

# ***Algebra & Number Theory***

Volume 3  
2009

No. 2



mathematical sciences publishers

# EDITORS

MANAGING EDITOR  
Bjorn Poonen  
Massachusetts Institute of Technology  
Cambridge, USA

EDITORIAL BOARD CHAIR  
David Eisenbud  
University of California  
Berkeley, USA

# BOARD OF EDITORS

Georgia Benkart	University of Wisconsin, Madison, USA	Susan Montgomery	University of Southern California, USA
Dave Benson	University of Aberdeen, Scotland	Shigefumi Mori	RIMS, Kyoto University, Japan
Richard E. Borcherds	University of California, Berkeley, USA	Andrei Okounkov	Princeton University, USA
John H. Coates	University of Cambridge, UK	Raman Parimala	Emory University, USA
J.-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Victor Reiner	University of Minnesota, USA
Brian D. Conrad	University of Michigan, USA	Karl Rubin	University of California, Irvine, USA
Hélène Esnault	Universität Duisburg-Essen, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Ronald Solomon	Ohio State University, USA
Andrew Granville	Université de Montréal, Canada	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Joseph Gubeladze	San Francisco State University, USA	J. Toby Stafford	University of Michigan, USA
Ehud Hrushovski	Hebrew University, Israel	Bernd Sturmfels	University of California, Berkeley, USA
Craig Huneke	University of Kansas, USA	Richard Taylor	Harvard University, USA
Mikhail Kapranov	Yale University, USA	Ravi Vakil	Stanford University, USA
Yujiro Kawamata	University of Tokyo, Japan	Michel van den Bergh	Hasselt University, Belgium
János Kollár	Princeton University, USA	Marie-France Vignéras	Université Paris VII, France
Hendrik W. Lenstra	Universiteit Leiden, The Netherlands	Kei-Ichi Watanabe	Nihon University, Japan
Yuri Manin	Northwestern University, USA	Andrei Zelevinsky	Northeastern University, USA
Barry Mazur	Harvard University, USA	Efim Zelmanov	University of California, San Diego, USA

# PRODUCTION

ant@mathscipub.org  
Paulo Ney de Souza, Production Manager      Silvio Levy, Senior Production Editor

---

See inside back cover or [www.jant.org](http://www.jant.org) for submission instructions.


---

Regular subscription rate for 2009: \$200.00 a year (\$140.00 electronic only).  
Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

---

Algebra & Number Theory, ISSN 1937-0652, at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

---

PUBLISHED BY  
 **mathematical sciences publishers**  
<http://www.mathscipub.org>  
A NON-PROFIT CORPORATION  
Typeset in L<sup>A</sup>T<sub>E</sub>X  
Copyright ©2009 by Mathematical Sciences Publishers

# A jeu de taquin theory for increasing tableaux, with applications to $K$ -theoretic Schubert calculus

Hugh Thomas and Alexander Yong

We introduce a theory of *jeu de taquin* for *increasing tableaux*, extending fundamental work of Schützenberger (1977) for standard Young tableaux. We apply this to give a new combinatorial rule for the  $K$ -theory Schubert calculus of Grassmannians via  *$K$ -theoretic jeu de taquin*, providing an alternative to the rules of Buch and others. This rule naturally generalizes to give a conjectural root-system uniform rule for any minuscule flag variety  $G/P$ , extending recent work of Thomas and Yong. We also present analogues of results of Fomin, Haiman, Schensted and Schützenberger.

1. Introduction	121
2. Growth diagrams	126
3. The infusion involution	128
4. A generalization of Schützenberger’s evacuation involution	130
5. Proof of the $K$ jd $t$ rule	132
6. Proof of the $K$ rect theorem	134
7. Minuscule Schubert calculus conjectures	138
8. Counterexamples	141
9. Concluding remarks	143
Appendix: Grothendieck polynomials	144
Acknowledgments	146
References	146

## 1. Introduction

In this paper, we introduce a *jeu de taquin* type theory for *increasing tableaux*, extending Schützenberger’s fundamental framework [1977] to the ( $K$ -theoretic) *Grothendieck polynomial* context introduced a few years later by Lascoux and Schützenberger [1982].

---

*MSC2000:* primary 05E10; secondary 14M15.

*Keywords:* Schubert calculus,  $K$ -theory, jeu de taquin.

Thomas was supported by an NSERC Discovery grant. Yong was supported by NSF grant 0601010.

One motivation and application for this work comes from Schubert calculus. Let  $X = \text{Gr}(k, \mathbb{C}^n)$  be the Grassmannian of  $k$ -planes in  $\mathbb{C}^n$  and let  $K(X)$  be the *Grothendieck ring* of algebraic vector bundles over  $X$ ; see, for example, the expositions [Brion 2005; Buch 2005b] for definitions and discussion. To each partition, as identified with its *Young shape*  $\lambda \subseteq \Lambda := k \times (n - k)$ , let  $X_\lambda$  be the associated Schubert variety and  $\mathcal{O}_{X_\lambda}$  its structure sheaf. The classes  $\{[\mathcal{O}_{X_\lambda}]\} \subseteq K(X)$  form an additive  $\mathbb{Z}$ -basis of  $K(X)$ . The (*K-theoretic*) *Schubert structure constants*  $C_{\lambda, \mu}^v$  are defined by

$$[\mathcal{O}_{X_\lambda}] \cdot [\mathcal{O}_{X_\mu}] = \sum_{v \subseteq \Lambda} C_{\lambda, \mu}^v [\mathcal{O}_{X_v}].$$

Buch's rule [2002b] established alternation of sign, that is,

$$(-1)^{|v| - |\lambda| - |\mu|} C_{\lambda, \mu}^v \in \mathbb{N}.$$

In the *cohomology case*  $|\lambda| + |\mu| = |v|$  where  $|\lambda| = \sum_i \lambda_i$  is the *size* of  $\lambda$ , the numbers  $C_{\lambda, \mu}^v$  are the classical *Littlewood–Richardson coefficients*. Here,  $C_{\lambda, \mu}^v$  counts points in the intersection of three general Schubert varieties. These numbers determine the ring structure of the cohomology  $H^*(X, \mathbb{Q})$ . Combinatorially, they are governed by the tableau theory of Schur polynomials. Schützenberger's *jeu de taquin* theory [1977], by which the first modern statement and proof of a Littlewood–Richardson rule was constructed, has had a central impact here.

While  $H^*(X, \mathbb{Q})$  contains important geometric data about  $X$ , this is even more true of  $K(X)$ . The combinatorics of  $K(X)$  is encoded by the Grothendieck polynomials of Lascoux and Schützenberger [1982] (for more details, see Appendix). This richer environment parallels the Schur polynomial setting, as demonstrated by, for example, [Lenart 2000; Buch 2002b; Buch et al. 2008]. However, basic gaps in this comparison remain. In particular, one lacks an analogue of the *jeu de taquin* theory. This also raises questions of intrinsic combinatorial interest.

Indeed, there has been significant interest in the Grothendieck ring of  $X$  and of related varieties; see work on, for example, quiver loci [Buch 2002a; 2005a; Miller 2005; Buch et al. 2008], Hilbert series of determinantal ideals [Knutson and Miller 2005; Knutson et al. 2008; 2009], applications to invariants of matroids [Speyer 2006], and in relation to representation theory [Griffeth and Ram 2004; Lenart and Postnikov 2007; Willems 2006]. See also work of Lam and Pylyavskyy [2007] concerning combinatorial Hopf algebras.

Consequently, we aim to provide unifying foundational combinatorics in support of further such developments. Evidence of the efficacy of this approach is provided through our study of minuscule Schubert calculus; other uses are also suggested. In particular, as a *non*-algebraic geometric application, in a followup paper [Thomas and Yong 2008b], we relate the ideas in this paper to [Buch et al. 2008] and the study of longest strictly increasing subsequences in random words.

Specifically, we introduce a jeu de taquin construction, thereby allowing for  $K$ -theoretic generalizations of a number of results from algebraic combinatorics. In particular, we give an analogue of Schützenberger’s Littlewood–Richardson rule. In addition, we extend Fomin’s *growth diagrams*, allowing for, for example, a generalization of Schützenberger’s *evacuation involution*. On the other hand, it is interesting that natural generalizations of some results from the classical theory are *not* true, underlining some basic combinatorial obstructions.

One feature of our rule is that it has a natural conjectural generalization to any minuscule flag variety  $G/P$ , extending our earlier work [Thomas and Yong 2006; 2007]; this provides the first generalized Littlewood–Richardson formula (even conjectural) for  $K$ -theory, outside of the Grassmannians. (There are already a number of more specialized  $K$ -theoretic Schubert calculus formulas proven for any  $G/P$ , such as the Pieri-type formulas of [Lenart and Postnikov 2007] and others.)

**Main definitions.** An *increasing tableau*  $T$  of shape  $\nu/\lambda$  is a filling of the skew shape

$$\text{shape}(T) = \nu/\lambda$$

with  $\{1, 2, \dots, q\}$  where  $q \leq |\nu/\lambda|$  such that the entries of  $T$  strictly increase along each row and column. We write  $\max T$  for the maximum entry in  $T$ . In particular, when  $\max T = |\nu/\lambda|$  and each label appears exactly once,  $T$  is a *standard Young tableau*. Let  $\text{INC}(\nu/\lambda)$  be the set of these increasing tableaux and  $\text{SYT}(\nu/\lambda)$  be the set of standard Young tableaux for  $\nu/\lambda$ . Below we give an example of an increasing tableau and a standard Young tableau, each of shape  $\nu/\lambda = (5, 3, 1)/(2, 1)$ :

$$\begin{array}{|c|c|c|c|c|} \hline & & 1 & 2 & 3 \\ \hline & 1 & 3 & & \\ \hline 2 & & & & \\ \hline \end{array} \in \text{INC}((5, 3, 1)/(2, 1)), \quad \begin{array}{|c|c|c|c|c|} \hline & & 1 & 4 & 6 \\ \hline & 2 & 5 & & \\ \hline 3 & & & & \\ \hline \end{array} \in \text{SYT}((5, 3, 1)/(2, 1)).$$

We also need to define the *superstandard Young tableau*  $S_\lambda$  of shape  $\lambda$  to be the standard Young tableau that fills the first row with  $1, 2, \dots, \lambda_1$ , the second row with  $\lambda_1+1, \lambda_1+2, \dots, \lambda_1+\lambda_2$ , and so on. For example,

$$S_{(5,3,3,1)} = \begin{array}{|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 \\ \hline 6 & 7 & 8 & & \\ \hline 9 & 10 & 11 & & \\ \hline 12 & & & & \\ \hline \end{array}.$$

A *short ribbon*  $R$  is a connected skew shape that does not contain a  $2 \times 2$  subshape and where each row and column contains at most two boxes. A *alternating ribbon* is a filling of a short ribbon  $R$  with two symbols where adjacent boxes are filled differently. We define  $\text{switch}(R)$  to be the alternating ribbon of the same shape as  $R$  but where each box is instead filled with the other symbol. For example,

we have

$$R = \begin{array}{|c|c|c|} \hline & \circ & \bullet \\ \hline & \circ & \bullet \\ \hline \circ & \bullet & \\ \hline \bullet & & \\ \hline \end{array} \quad \text{and} \quad \text{switch}(R) = \begin{array}{|c|c|c|} \hline \bullet & \circ & \\ \hline \bullet & \circ & \\ \hline \bullet & \circ & \\ \hline \circ & & \\ \hline \end{array}.$$

By definition, if  $R$  is a ribbon consisting of a single box,  $\text{switch}$  does nothing to it. We define  $\text{switch}$  to act on a skew shape consisting of multiple connected components, each of which is an alternating ribbon, by acting on each separately.

Our starting point is the following new idea. Given  $T \in \text{INC}(\nu/\lambda)$ , an *inner corner* is any maximally southeast box  $x \in \lambda$ . Now fix a set  $\{x_1, \dots, x_s\}$  of inner corners and let each of these boxes is filled with a  $\bullet$ . Consider the union of short ribbons  $R_1$  which is made of boxes with entries  $\bullet$  or 1. Apply  $\text{switch}$  to  $R_1$ . Now let  $R_2$  be the union of short ribbons consisting of boxes with entries  $\bullet$  or 2, and proceed as before. Repeat this process  $\max T$  times, in other words, until the  $\bullet$ 's have been switched past all the entries of  $T$ . The final placement of the numerical entries gives  $K\text{jdt}_{\{x_i\}}(T)$ .

**Example 1.1.** Let  $T = \begin{array}{|c|c|c|c|} \hline & & 1 & 2 & 3 \\ \hline & 2 & 3 & & \\ \hline 2 & & & & \\ \hline \end{array}$  be as above and  $\{x_i\}$  as indicated below:

$$\begin{array}{|c|c|c|c|c|} \hline & \bullet & 1 & 2 & 3 \\ \hline \bullet & 2 & 3 & & \\ \hline 2 & & & & \\ \hline \end{array} \mapsto \begin{array}{|c|c|c|c|c|} \hline & 1 & \bullet & 2 & 3 \\ \hline \bullet & 2 & 3 & & \\ \hline 2 & & & & \\ \hline \end{array} \mapsto \begin{array}{|c|c|c|c|c|} \hline & 1 & 2 & \bullet & 3 \\ \hline 2 & \bullet & 3 & & \\ \hline \bullet & & & & \\ \hline \end{array} \mapsto \begin{array}{|c|c|c|c|c|} \hline & 1 & 2 & 3 & \bullet \\ \hline 2 & 3 & \bullet & & \\ \hline \bullet & & & & \\ \hline \end{array}$$

and therefore

$$K\text{jdt}_{\{x_i\}} = \begin{array}{|c|c|c|c|} \hline & 1 & 2 & 3 \\ \hline 2 & 3 & & \\ \hline \end{array}.$$

It is easy to see that  $K\text{jdt}_{\{x_i\}}(T)$  is an increasing tableau also. Moreover, if  $T$  is a standard Young tableau, and only one corner  $x$  is selected, the result is an *ordinary jeu de taquin slide*  $\text{jdt}_x(T)$ . Given  $T \in \text{INC}(\nu/\lambda)$  we can iterate applying  $K\text{jdt}$ -slides until no such moves are possible. The result  $K\text{rect}(T)$ , which we call a *K-rectification* of  $T$ , is an increasing tableau of straight shape, that is, one whose shape is given by some partition  $\lambda$ . We will refer to the choice of intermediate  $K\text{jdt}$  slides as a *rectification order*.

**Theorem 1.2.** *Let  $T \in \text{INC}(\nu/\lambda)$ . If  $K\text{rect}(T)$  is a superstandard tableau  $S_\mu$  for some rectification order, then  $K\text{rect}(T) = S_\mu$  for any rectification order.*

It will also be convenient to define *reverse slides*

$$K\text{revjdt}_{\{x_i\}}(T)$$

of  $T \in \text{INC}(\nu/\lambda)$ , where now each  $x_i$  is an *outer corner*, that is, a maximally north-west box  $x \in \Lambda \setminus \nu$ . We can similarly define *reverse rectification*  $K\text{rect}(T)$ .

Clearly, Theorem 1.2 also implies the “reverse version”. When we refer to *slides*, we mean either  $Kjdt$  or  $Krevjdt$  operations.

Theorem 1.2 may be compared to what is often called the “confluence theorem” or the “First Fundamental Theorem” in the original setting of [Schützenberger 1977]. There, the superstandard assumption is unnecessary and so rectification is always well-defined. However this is not true in our more general context.

**Example 1.3.** Consider the following two  $K$ -rectifications of the same skew tableau  $T$ :

$$T = \begin{array}{|c|c|c|c|} \hline & & \bullet & 2 \\ \hline & & 2 & \\ \hline 1 & 3 & 4 & \\ \hline \end{array} \mapsto \begin{array}{|c|c|c|} \hline & & 2 \\ \hline & \bullet & 4 \\ \hline 1 & 3 & \\ \hline \end{array} \mapsto \begin{array}{|c|c|c|} \hline & & 2 \\ \hline \bullet & 3 & 4 \\ \hline 1 & & \\ \hline \end{array} \mapsto \begin{array}{|c|c|c|} \hline & \bullet & 2 \\ \hline 1 & 3 & 4 \\ \hline & & \\ \hline \end{array} \mapsto \begin{array}{|c|c|c|} \hline \bullet & 2 & 4 \\ \hline 1 & 3 & \\ \hline & & \\ \hline \end{array} \mapsto \begin{array}{|c|c|c|} \hline 1 & 2 & 4 \\ \hline 3 & & \\ \hline & & \\ \hline \end{array}$$

and

$$T = \begin{array}{|c|c|c|c|} \hline & & & 2 \\ \hline & \bullet & 2 & \\ \hline 1 & 3 & 4 & \\ \hline \end{array} \mapsto \begin{array}{|c|c|c|} \hline & & \bullet & 2 \\ \hline & 2 & 4 & \\ \hline 1 & 3 & & \\ \hline \end{array} \mapsto \begin{array}{|c|c|c|} \hline & & 2 \\ \hline \bullet & 2 & 4 \\ \hline 1 & 3 & \\ \hline \end{array} \mapsto \begin{array}{|c|c|c|} \hline & \bullet & 2 \\ \hline 1 & 2 & 4 \\ \hline 3 & & \\ \hline \end{array} \mapsto \begin{array}{|c|c|c|} \hline \bullet & 2 & 4 \\ \hline 1 & 4 & \\ \hline 3 & & \\ \hline \end{array} \mapsto \begin{array}{|c|c|c|} \hline 1 & 2 & 4 \\ \hline 3 & 4 & \\ \hline & & \\ \hline \end{array}.$$

The two results (rightmost tableaux) are different. However, neither rectification is superstandard.

We need Theorem 1.2 to state our new combinatorial rule for  $C_{\lambda,\mu}^v$ :

**Theorem 1.4.**  $(-1)^{|v|-|\lambda|-|\mu|} C_{\lambda,\mu}^v$  counts the number of  $T \in \text{INC}(v/\lambda)$  where

$$K\text{rect}(T) = S_\mu.$$

**Example 1.5.** The computation  $C_{(2,2),(2,1)}^{(3,2,2,1)} = -2$  is witnessed by the increasing tableaux

$$\begin{array}{|c|c|c|} \hline & & 2 \\ \hline & & \\ \hline 1 & 3 & \\ \hline 3 & & \\ \hline \end{array} \quad \text{and} \quad \begin{array}{|c|c|c|} \hline & & 2 \\ \hline & & \\ \hline 1 & 2 & \\ \hline 3 & & \\ \hline \end{array},$$

which both rectify to  $\begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & \\ \hline \end{array}$ .

One can replace the superstandard assumption by some other classes  $\{C_\mu\}$  of tableau (most obviously the one where we consecutively number columns rather than rows), but we focus on the superstandard choice in this paper.

We will give a self-contained proof of Theorem 1.4, once granted Lenart’s Pieri rule [2000].

A short review of past work on  $K$ -theoretic Littlewood–Richardson rules is in order: The first rule for  $C_{\lambda,\mu}^v$  was given by Buch [2002b], who gave a generalization of the *reverse lattice word* formulation of the classical Littlewood–Richardson rule.





(3, 2, 1)	(3, 3, 2, 1)	(4, 3, 3, 2)	(4, 4, 3, 2)	(4, 4, 3, 3)
(2, 2)	(3, 2, 1)	(4, 3, 2, 1)	(4, 4, 2, 1)	(4, 4, 3, 2)
(2, 1)	(3, 1, 1)	(4, 2, 1, 1)	(4, 3, 1, 1)	(4, 3, 2, 1)
(1)	(2, 1)	(3, 2, 1)	(3, 3, 1)	(3, 3, 2)
$\emptyset$	(1)	(2, 1)	(3, 2)	(3, 2, 1)

**Table 1.** A  $K$ -theory growth diagram: the leftmost column describes the rectification order of the skew tableau represented by the top row. The bottom row gives the resulting  $K$ -rectification.

Now, consider the following choice of rectification order:

$$T = \begin{array}{|c|c|c|c|} \hline & & \bullet & 3 \\ \hline & & 1 & 2 \\ \hline \bullet & 1 & 2 & \\ \hline 1 & 2 & 4 & \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|c|} \hline & & 1 & 2 \\ \hline & \bullet & 2 & 3 \\ \hline 1 & 2 & 4 & \\ \hline 2 & 4 & & \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|c|} \hline & \bullet & 1 & 2 \\ \hline \bullet & 2 & 3 & \\ \hline 1 & 4 & & \\ \hline 2 & & & \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|} \hline \bullet & 1 & 2 \\ \hline 1 & 2 & 3 \\ \hline 2 & 4 & \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 2 & 3 & \\ \hline 4 & & \\ \hline \end{array},$$

where the  $\bullet$ 's indicate the set of boxes to use in each  $Kjdt$  step. Each of these increasing tableaux also has a shape sequence, which we put one atop of another so the shapes increase moving up and to the right. The result is a  $K$ -theory growth diagram; in our example, we have Table 1.

Consider the following local conditions on any  $2 \times 2$  subsquare

$$\begin{array}{|c|c|} \hline \alpha & \beta \\ \hline \gamma & \delta \\ \hline \end{array}$$

of such a grid of shapes, where by assumption  $\gamma \subseteq \alpha \subseteq \beta$  and  $\gamma \subseteq \delta \subseteq \beta$ , as in the example above:

- (G1)  $\alpha/\gamma$  is a collection of boxes no two in the same row or column, and similarly for  $\beta/\alpha$ ,  $\beta/\delta$ , and  $\delta/\gamma$ .
- (G2)  $\delta$  is the shape  $\alpha \cup \text{shape}(Kjdt_{\alpha/\gamma}(T))$ , where  $T$  is the skew tableau of shape  $\beta/\alpha$  filled with 1's. This uniquely determines  $\delta$  from  $\gamma$ ,  $\alpha$  and  $\beta$ . Similarly,  $\alpha$  is uniquely determined by  $\gamma$ ,  $\delta$  and  $\beta$ .

**Proposition 2.2.** *If*

$$\begin{array}{|c|c|} \hline \alpha & \beta \\ \hline \gamma & \delta \\ \hline \end{array}$$

*is a  $2 \times 2$  square in a  $K$ -theory growth diagram, then (G1) and (G2) hold. Also, if  $\mathcal{G}$  is a growth diagram, then so is  $\mathcal{G}$  reflected about its antidiagonal.*

*Proof.* These are straightforward verifications. The second statement uses the fact that (G1) and (G2) are symmetric in  $\alpha$  and  $\delta$ .  $\square$

Let  $K\text{GROWTH}(\lambda, \mu; \nu)$  be the set of  $K$ -theory growth diagrams such that

- the leftmost column encodes the superstandard tableau of shape  $\lambda$ ,
- the bottom-most row encodes the superstandard tableau of shape  $\mu$ , and
- the top right corner is the shape  $\nu$ .

The following fact is immediate from Theorem 1.4, and amounts to an alternative formulation for it:

**Corollary 2.3** (of Theorem 1.4).  $(-1)^{|\nu| - |\lambda| - |\mu|} C_{\lambda, \mu}^{\nu} = \#KGROWTH(\lambda, \mu; \nu)$ .

By the symmetry of growth diagrams, the roles of the  $\lambda$  and  $\mu$  can be interchanged, resulting in the same growth diagram (up to reflection). Therefore, the rule of Corollary 2.3 manifests the  $\mathbb{Z}_2$  *commutation symmetry*

$$C_{\lambda, \mu}^{\nu} = C_{\mu, \lambda}^{\nu}$$

coming from  $[\mathbb{O}_{X_{\lambda}}][\mathbb{O}_{X_{\mu}}] = [\mathbb{O}_{X_{\mu}}][\mathbb{O}_{X_{\lambda}}]$ .

Growth diagrams corresponding to the classical rectifications of a standard tableau (using only  $\text{jdt}$  moves) were first introduced by Fomin; see [Stanley 1999, Appendix 1] and the references therein. In that case, Proposition 2.2 simplifies. Specifically,

(F1) shapes increase by precisely one box in the “up” and “right” directions.

(F2) if  $\alpha$  is the unique shape containing  $\gamma$  and contained in  $\beta$ , then  $\delta = \alpha$ ; otherwise there is a unique such shape different than  $\alpha$ , and this shape is  $\delta$ .

(Similarly,  $\alpha$  is uniquely determined by  $\beta$ ,  $\gamma$  and  $\delta$ .)

Fomin’s growth diagrams provide further useful combinatorial ideas that we extend below to the  $K$ -theory setting. These diagrams also arise (along with other classical tableaux algorithms we generalize) in an elegant geometric context, due to work of van Leeuwen [2000]; there are reasons to hope that one can extend his work to the setting of this paper.

### 3. The infusion involution

Given  $T \in \text{INC}(\lambda/\alpha)$  and  $U \in \text{INC}(\nu/\lambda)$ , define

$\text{Kinfusion}(T, U)$

$$= (\text{Kinfusion}_1(T, U), \text{Kinfusion}_2(T, U)) \in \text{INC}(\gamma/\alpha) \times \text{INC}(\nu/\gamma)$$

(for some straight shape  $\gamma$ ) as follows: consider the largest label “ $m$ ” that appears in  $T$ , appearing at  $x_1, \dots, x_k$ . Apply the slide  $K\text{jdt}_{\{x_i\}}(U)$ , leaving some “holes” at the other side of  $\nu/\lambda$ . Place “ $m$ ” in these holes and repeat, moving the labels originally from  $U$  until all labels of  $T$  are exhausted. The resulting tableau of shape

$\gamma/\alpha$  and skew tableau of shape  $\nu/\gamma$  are the outputted tableaux. To define

$Krevinfusion(T, U)$

$$= (Krevinfusion_1(T, U), Krevinfusion_2(T, U)) \in INC(\gamma/\alpha) \times INC(\nu/\gamma),$$

we apply  $Krevjdt$  moves to  $T$ , moving into boxes of  $U$ . We begin by removing the labels “1” appearing in  $U$  at boxes  $\{x_i\} \in \nu/\lambda$ , apply  $revjdt_{\{x_i\}}(T)$ , and place the “1” in the vacated holes of  $\lambda$  and continuing with higher labels of  $U$ .

It is easy to show that

$$Kinfusion \quad \text{and} \quad Krevinfusion$$

are inverses of one another, by inductively applying the observation that if  $\{y_i\}$  are the boxes vacated by  $Kjdt_{\{x_i\}}(T)$  then

$$Krevjdt_{\{y_i\}}(Kjdt_{\{x_i\}}(T)) = T.$$

We will need the following fact (the “infusion involution”); compare [Haiman 1992; Benkart et al. 1996].

**Theorem 3.1.** *For any increasing tableaux  $T$  and  $U$  such that  $\text{shape}(U)$  extends (the possibly skew shape)  $\text{shape}(T)$  then*

$$Kinfusion(T, U) = Krevinfusion(T, U).$$

That is,  $Kinfusion(Kinfusion(T, U)) = (T, U)$ .

**Example 3.2.** If

$$T = \begin{array}{|c|c|c|} \hline \underline{1} & \underline{2} & \underline{3} \\ \hline \underline{2} & \underline{3} & \\ \hline 4 & & \\ \hline \end{array} \quad \text{and} \quad U = \begin{array}{|c|c|c|} \hline & & 2 \\ \hline & 1 & 3 \\ \hline & 1 & 3 \\ \hline 2 & 3 & 4 \\ \hline \end{array}$$

then we compute  $Kinfusion$  as follows:

$$\begin{array}{ccccccc} \begin{array}{|c|c|c|c|} \hline \underline{1} & \underline{2} & \underline{3} & 2 \\ \hline \underline{2} & \underline{3} & 1 & 3 \\ \hline 4 & 1 & 3 & \\ \hline 2 & 3 & 4 & \\ \hline \end{array} & \mapsto & \begin{array}{|c|c|c|c|} \hline \underline{1} & \underline{2} & \underline{3} & 2 \\ \hline \underline{2} & \underline{3} & 1 & 3 \\ \hline 1 & 4 & 3 & \\ \hline 2 & 3 & 4 & \\ \hline \end{array} & \mapsto & \begin{array}{|c|c|c|c|} \hline \underline{1} & \underline{2} & \underline{3} & 2 \\ \hline \underline{2} & \underline{3} & 1 & 3 \\ \hline 1 & 3 & 4 & \\ \hline 2 & 4 & 4 & \\ \hline \end{array} & \mapsto & \begin{array}{|c|c|c|c|} \hline \underline{1} & \underline{2} & \underline{3} & 2 \\ \hline \underline{2} & \underline{3} & 1 & 3 \\ \hline 1 & 3 & 4 & \\ \hline 2 & 4 & 4 & \\ \hline \end{array} & \mapsto & \begin{array}{|c|c|c|c|} \hline \underline{1} & \underline{2} & 1 & 2 \\ \hline \underline{2} & 1 & \underline{3} & 3 \\ \hline 1 & 3 & 4 & \\ \hline 2 & 4 & 4 & \\ \hline \end{array} \\ & \mapsto & \begin{array}{|c|c|c|c|} \hline \underline{1} & \underline{2} & 1 & 2 \\ \hline \underline{2} & 1 & 3 & \underline{3} \\ \hline 1 & 3 & 4 & \\ \hline 2 & 4 & 4 & \\ \hline \end{array} & \mapsto & \begin{array}{|c|c|c|c|} \hline \underline{1} & 1 & \underline{2} & 2 \\ \hline 1 & \underline{2} & 3 & \underline{3} \\ \hline \underline{2} & 3 & 4 & \\ \hline 2 & 4 & 4 & \\ \hline \end{array} & \mapsto & \begin{array}{|c|c|c|c|} \hline \underline{1} & 1 & 2 & \underline{2} \\ \hline 1 & \underline{2} & 3 & \underline{3} \\ \hline 2 & 3 & 4 & \\ \hline 2 & 4 & 4 & \\ \hline \end{array} & \mapsto & \begin{array}{|c|c|c|c|} \hline \underline{1} & 1 & 2 & \underline{2} \\ \hline 1 & 3 & \underline{2} & \underline{3} \\ \hline 2 & \underline{2} & 4 & \\ \hline 2 & 4 & 4 & \\ \hline \end{array} \\ & \mapsto & \begin{array}{|c|c|c|c|} \hline \underline{1} & 1 & 2 & \underline{2} \\ \hline 1 & 3 & 4 & \underline{3} \\ \hline 2 & 4 & \underline{2} & \\ \hline 4 & \underline{2} & 4 & \\ \hline \end{array} & \mapsto & \begin{array}{|c|c|c|c|} \hline 1 & 1 & 2 & \underline{2} \\ \hline \underline{1} & 3 & 4 & \underline{3} \\ \hline 2 & 4 & \underline{2} & \\ \hline 4 & \underline{2} & 4 & \\ \hline \end{array} & \mapsto & \begin{array}{|c|c|c|c|} \hline 1 & 2 & 1 & \underline{2} \\ \hline 2 & 3 & 4 & \underline{3} \\ \hline \underline{1} & 4 & \underline{2} & \\ \hline 4 & \underline{2} & 4 & \\ \hline \end{array} & \mapsto & \begin{array}{|c|c|c|c|} \hline 1 & 2 & 4 & \underline{2} \\ \hline 2 & 3 & \underline{1} & \underline{3} \\ \hline 4 & \underline{1} & \underline{2} & \\ \hline \underline{1} & \underline{2} & 4 & \\ \hline \end{array} \end{array}$$

Hence

$$\text{Kinfusion}(T, U) = \left( \begin{array}{|c|c|c|} \hline 1 & 2 & 4 \\ \hline 2 & 3 & \\ \hline 4 & & \\ \hline \end{array}, \begin{array}{|c|c|c|} \hline & & 2 \\ \hline & 1 & 3 \\ \hline & 1 & 2 \\ \hline 1 & 2 & 4 \\ \hline \end{array} \right).$$

The reader can check that applying  $\text{Kinfusion}$  to this pair returns  $(T, U)$ , in agreement with Theorem 3.1.

*Proof.* Construct the growth diagram for  $\text{Krect}(U)$  using the slides suggested by the entries of  $T$ . It is straightforward to check from the definitions that the bottom row represents  $\text{Kinfusion}_1(T, U)$  and the right column  $\text{Kinfusion}_2(T, U)$ . However, by the antidiagonal symmetry of growth diagrams (see Proposition 2.2), the growth diagram computing  $\text{Kinfusion}$  applied to  $\text{Kinfusion}(T, U)$  is simply the one for  $\text{Kinfusion}(T, U)$  reflected about the antidiagonal.  $\square$

Finally, the growth diagram formalism makes it straightforward to observe facts such as the following, which we will need in Section 6:

**Lemma 3.3.** *Let  $T \in \text{INC}(v/\lambda)$ ,  $R \in \text{INC}(\lambda)$  and fix  $a \in \mathbb{N}$ . If  $A$  is the increasing tableau consisting of entries from 1 to  $a$  of  $T$ , and  $B = T \setminus A$  is the remaining tableau, then*

$$\begin{aligned} \text{Kinfusion}_1(R, T) \\ = \text{Kinfusion}_1(R, A) \cup \text{Kinfusion}_1(\text{Kinfusion}_2(R, A), B). \end{aligned}$$

*Proof.* Draw the growth diagram for  $\text{Kinfusion}(R, T)$ , encoding  $R$  on the left and  $T$  on the top. The shape  $\text{shape}(R) \cup \text{shape}(A)$  appears on the top row. Draw a vertical line through the growth diagram at that point. The diagram to the left of this line encodes the rectification of  $A$  by  $R$ . The diagram to the right of the line encodes the infusion of  $B = T \setminus A$  with the tableau encoded along the dividing line, which is  $\text{Kinfusion}_2(R, A)$ .  $\square$

#### 4. A generalization of Schützenberger’s evacuation involution

While on the topic of growth diagrams, we take this opportunity to introduce a generalization of another classical result from tableau theory. This section will not be needed in the remainder of the paper.

For  $T \in \text{INC}(\lambda)$ , let  ${}^\circ T$  be obtained by erasing the (unique) entry 1 in the north-west corner  $c$  of  $T$  and subtracting 1 from the remaining entries. Let

$$\Delta(T) = \text{Kjdt}_{\{c\}}({}^\circ T).$$

The  $K$ -evacuation  $\text{Kevac}(T) \in \text{INC}(\lambda)$  is defined by the shape sequence

$$\emptyset = \text{shape}(\Delta^{\max T}(T)) - \text{shape}(\Delta^{\max T-1}(T)) - \dots - \text{shape}(\Delta^1(T)) - T.$$

$\emptyset$	(1)	(2, 1)	(3, 2)	(3, 3, 1)	(4, 3, 2)
	$\emptyset$	(1)	(2, 1)	(3, 2, 1)	(4, 2, 2)
		$\emptyset$	(1)	(2, 1)	(3, 2, 1)
			$\emptyset$	(1)	(2, 1)
				$\emptyset$	(1)
					$\emptyset$

**Table 2.** A triangular growth diagram for Example 4.2.

The following result extends Schützenberger’s classical theorem for  $T \in \text{SYT}(\lambda)$ .

**Theorem 4.1.**  $\text{Kevac} : \text{INC}(\lambda) \rightarrow \text{INC}(\lambda)$  is an involution, that is,

$$\text{Kevac}(\text{Kevac}(T)) = T.$$

**Example 4.2.** Let

$$T = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 5 \\ \hline 2 & 3 & 4 & \\ \hline 4 & 5 & & \\ \hline \end{array} \in \text{INC}((4, 3, 2)).$$

Then the  $K$ -evacuation is computed by

$$\Delta^1(T) = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 2 & 3 & & \\ \hline 3 & 4 & & \\ \hline \end{array} \mapsto \Delta^2(T) = \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 2 & 3 & \\ \hline 3 & & \\ \hline \end{array} \mapsto \Delta^3(T) = \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 2 & \\ \hline \end{array} \mapsto \Delta^4(T) = \begin{array}{|c|} \hline 1 \\ \hline \end{array} \mapsto \Delta^5(T) \mapsto \emptyset.$$

Thus

$$\text{Kevac}(T) = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 2 & 3 & 5 & \\ \hline 3 & 4 & & \\ \hline \end{array}.$$

One checks that applying  $\text{Kevac}$  to this tableau returns  $T$ .

*Proof of Theorem 4.1.* Express each of the increasing tableaux

$$T, \Delta^1(T), \dots, \Delta^{\max T-1}(T), \Delta^{\max T}(T) = \emptyset$$

as a shape sequence and place them right justified in a triangular growth diagram. In the example above, we have Table 2. Note that each “minor” of the table whose southwest corner contains a “ $\emptyset$ ” is in fact a growth diagram. It follows that the triangular growth diagram can be reconstructed using (G1) and (G2), by Proposition 2.2. Observe that the right column encodes  $\text{Kevac}(T)$ . By the symmetry of growth diagrams, it follows that applying the above procedure to  $\text{Kevac}(T)$  would give the same triangular growth diagram, after a reflection across the antidiagonal. Thus the result follows.  $\square$

### 5. Proof of the $Kjdt$ rule

The strategy of our proof is based on the following fact. In the cohomological context, this approach was utilized in [Knutson et al. 2004; Buch et al. 2004].

**Lemma 5.1.** *Let  $\{d_{\lambda,\mu}^v\}$  be integers indexed by shapes  $\lambda, \mu, v \subseteq \Lambda$  that*

(A) *define a commutative and associative ring  $(R, \circ)$  by*

$$a_\lambda \circ a_\mu = \sum_{v \subseteq \Lambda} d_{\lambda,\mu}^v a_v$$

*with  $\mathbb{Z}$ -basis  $\{a_\lambda\}$  indexed by shapes  $\lambda \subseteq \Lambda$ , and such that*

(B)  $d_{\lambda,\rho}^v = c_{\lambda,\rho}^v$  *whenever  $\rho = (t)$  for  $0 \leq t \leq n - k$ .*

*Then  $d_{\lambda,\mu}^v = c_{\lambda,\mu}^v$ .*

*Proof.* The class  $[\mathbb{O}_{X_\lambda}]$  can be expressed as a polynomial in  $[\mathbb{O}_{X_{(1)}}], \dots, [\mathbb{O}_{X_{(n-k)}}]$ . This follows by an easy downward induction on  $|\lambda|$  using the fact that such an expression exists in cohomology for  $[X_\lambda] \in H^*(X, \mathbb{Q})$  as a polynomial in the classes  $[X_{(t)}]$  (the *Jacobi–Trudi identity*) and the lowest order term in  $K$ -theory agrees with cohomology under the Chern isomorphism. Let this polynomial be  $P_\lambda(X_1, \dots, X_{n-k})$  (where above  $X_t = [\mathbb{O}_{X_{(t)}}]$ ). Now (A) and (B) imply

$$a_\lambda = P_\lambda(a_{(1)}, \dots, a_{(t)}).$$

Using (B) again, we see that the map from  $(R, \circ)$  to  $K(X)$  sending  $a_\lambda \mapsto [\mathbb{O}_{X_\lambda}]$  is a ring isomorphism, so the desired conclusion follows.  $\square$

To apply the lemma, let  $d_{\lambda,\mu}^v$  be the integers computed by the rule given in the statement of the theorem. It remains to check associativity and agreement with Pieri’s rule, which we do below. In our proof of associativity we *assume* that Theorem 1.2 is true — this latter result is actually proved in the following section, using some of the elements introduced in the proof of agreement with Pieri’s rule, which of course, do not use this assumption. We will also use the commutation symmetry, proved in Section 2 (see after Corollary 2.3), that is,  $d_{\lambda,\mu}^v = d_{\mu,\lambda}^v$ .

**Associativity.** Let  $\alpha, \beta, \gamma, v$  be straight shapes and fix superstandard tableaux  $S_\alpha, S_\beta, S_\gamma$  and  $S_v$ .

Associativity is the assertion that

$$\sum_{\sigma} d_{\alpha,\beta}^{\sigma} d_{\sigma,\gamma}^v = \sum_{\tau} d_{\alpha,\tau}^v d_{\beta,\gamma}^{\tau}. \quad (5-1)$$

The left-hand side of (5-1) counts pairs of tableaux  $(B, C)$  where  $B$  is of shape  $\sigma/\alpha$  such that  $Krect(B) = S_\beta$ , and  $C$  is of shape  $v/\sigma$  such that  $Krect(C) = S_\gamma$ .

Let  $Kinfusion(S_\alpha, B) = (S_\beta, A)$  where  $A$  is of shape  $\sigma/\beta$ , and  $Krect(A) = S_\alpha$ . Next compute  $Kinfusion(A, C) = (D, E)$ . We have that  $Krect(E) = S_\alpha$

(since this was the case with  $A$ ) and that  $\text{shape}(E) = v/\tau$  for some  $\tau$ , and similarly  $\text{Krect}(D) = S_\gamma$  (since this was the case for  $C$ ) and  $\text{shape}(D) = \tau/\beta$ .

By Theorem 3.1 it follows that the above process establishes a bijection

$$(B, C) \mapsto (E, D)$$

into the set of pairs of tableaux counted by the right-hand side of (5-1). (More precisely, for pairs counted by

$$\sum_{\tau} d_{\tau, \alpha}^v d_{\beta, \gamma}^{\tau} = \sum_{\tau} d_{\alpha, \tau}^v d_{\beta, \gamma}^{\tau}$$

where the equality  $d_{\tau, \alpha}^v = d_{\alpha, \tau}^v$  is the commutation symmetry.) Associativity follows.

**Agreement with Pieri's rule.** We prove our rule agrees with the following formula, due to Lenart [2000]:

**Theorem 5.2.** *Let  $r(v/\lambda)$  be the number of rows of  $v/\lambda$ . Then*

$$[\mathbb{O}_{X_\lambda}][\mathbb{O}_{X_{(t)}}] = \sum_v (-1)^{|v| - |\lambda| - t} \binom{r(v/\lambda) - 1}{|v/\lambda| - t} [\mathbb{O}_{X_v}],$$

where the sum ranges over all  $v \subseteq \Lambda$  obtained by adding a horizontal strip (no two added boxes are in the same column) to  $\lambda$  of size at least  $t$ .

Our task is to show that

$$d_{\lambda, (t)}^v = \binom{r(v/\lambda) - 1}{|v/\lambda| - t}$$

when  $v$  is of the form in the statement of Theorem 5.2 and is zero otherwise.

First assume  $v$  is of the desired form and that  $|v/\lambda| - t \leq r(v/\lambda) - 1$ . We proceed to construct the required number of increasing tableaux on  $v/\lambda$ , as follows. Select  $|v/\lambda| - t$  of the non-bottom-most  $r(v/\lambda) - 1$  rows of  $v/\lambda$ . Now fill the bottom row with consecutive entries  $1, 2, \dots, k$  where  $k$  is the number of boxes in that bottom row of  $v/\lambda$ . Proceed to fill the remaining boxes of  $v/\lambda$  from southwest to northeast. If the current row to be filled was one of the  $|v/\lambda| - t$  selected rows then begin with the last entry  $e$  used in the previously filled row. Otherwise use  $e + 1$ .

Call these fillings  $t$ -Pieri fillings.

**Example 5.3.** Suppose  $\lambda = (5, 3, 2)$ ,  $v = (6, 5, 2, 2)$  and  $t = 4$ . Then  $r(v/\lambda) = 3$  and  $|v/\lambda| - t = 1$ . Hence the two 4-Pieri fillings we construct are

$$\begin{array}{|c|c|c|c|c|} \hline & & & & 4 \\ \hline & & & 2 & 3 \\ \hline & & & & \\ \hline 1 & 2 & & & \\ \hline \end{array} \quad \text{and} \quad \begin{array}{|c|c|c|c|c|} \hline & & & & 4 \\ \hline & & & 3 & 4 \\ \hline & & & & \\ \hline 1 & 2 & & & \\ \hline \end{array},$$

which both rectify to  $\begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline \end{array}$ . (In the first tableau we selected the second row and in the second we selected the top row.)

**Lemma 5.4.** *For any rectification order, a  $t$ -Pieri filling  $K$ -rectifies to  $S_{(t)}$ . No other increasing tableau  $K$ -rectifies to  $S_{(t)}$  for any choice of rectification order.*

*Proof.* That the  $t$ -Pieri fillings all  $K$ -rectify (under any rectification order) to  $S_{(t)}$  follows from a straightforward induction on  $|\lambda| \geq 0$  where we show in fact that any  $Kjdt$  slide applied to a  $t$ -Pieri filling results in a  $t$ -Pieri filling.

A similar induction shows that no other increasing tableau from  $INC(\nu/\lambda)$   $K$ -rectifies to  $S_{(t)}$  (noting that any such tableau with entries in  $\{1, \dots, t\}$  has a pair of entries  $i < j$  where  $j$  is southwest of  $i$ ). Separately, but for similar reasons, when  $\nu/\lambda$  is not a horizontal strip, one more induction on  $|\lambda|$  proves no increasing tableau can  $K$ -rectify to  $S_{(t)}$ .

Finally, if  $|\nu/\lambda| - t > r(\nu/\lambda) - 1$ , then we similarly see that no  $t$ -Pieri fillings are possible and  $d_{\lambda, \mu}^\nu = 0$  as desired.  $\square$

This completes the proof of Theorem 1.4, assuming Theorem 1.2.

## 6. Proof of the $Krect$ theorem

We now prove Theorem 1.2. First define the *reading word* of a tableau  $T$  to be the word obtained by reading the rows of  $T$  from left to right, starting from the bottom and moving up. Let  $LIS(T)$  be the length of the longest strictly increasing subsequence of the reading word of  $T$ .

The following result is crucial to our proof of Theorem 1.2.

**Theorem 6.1.**  $LIS(Kjdt_{\{x_i\}}(T)) = LIS(T)$ . *In particular, any rectification order applied to  $T$  results in a straight shape whose first row has length equal to  $LIS(T)$ .*

**Example 6.2.** Consider the two (different) rectifications of the same tableau  $T$  performed in Example 1.3. The reading word of  $T$  is  $\underline{1} \ 3 \ 4 \ 2 \ 2$  (where the unique longest strictly increasing subsequence has been underlined) so  $LIS(T) = 3$ . Note that also  $LIS(T_1) = LIS(T_2) = 3$ , that is, the lengths of the first rows of  $T_1$  and  $T_2$  agree, although  $T_1 \neq T_2$ .

*Proof of Theorem 6.1.* We will show that if  $I$  is a set of boxes of  $T$  which forms a strictly increasing subsequence of the reading word of  $T$ , then there is a string of boxes of equal length in  $Kjdt_{\{x_i\}}(T)$  which also forms a strictly increasing subsequence of the reading word. A symmetric argument using reverse slides gives the other desired inequality, thereby implying the theorem.

Fix  $I$  as above. We will analyze the slide  $Kjdt_{\{x_i\}}(T)$ , switch by switch. Set  $T_0 := T$ , and let  $T_i$  be the result of switching the  $\bullet$ 's and the  $i$ 's of  $T_{i-1}$ . Initially set  $I_0 := I$ . In a moment, we will describe  $I_i$  as a collection of some of the boxes



of  $T_i$ . We emphasize that in what follows  $I_i$  does not refer to the actual *contents* of the boxes.

We will show that, at each step,  $I_i$  has the following properties:

- (P1) The labels of  $I_i$  are strictly increasing in the reading word order, except for perhaps one  $\bullet$  box.
- (P2) If  $I_i$  contains a  $\bullet$  box, then the labels in  $I_i$  preceding the  $\bullet$  box in the reading word order are weakly less than  $i$ , while the labels of boxes following the  $\bullet$  box are strictly greater than  $i$ .
- (P3) If there is a  $\bullet$  box  $y_i$  in  $I_i$ , then there must be some box  $z_i$  in  $I_i$ , in the same row as  $y_i$  and weakly to the right, such that the entry in the box  $a_i$  immediately below  $z_i$  contains a numerical label. Moreover, if there is a next box  $b_i$  in  $I_i$  after  $z_i$ , in the reading order, then it contains a numerical label strictly larger than the one in  $a_i$ .

**Example 6.3.** (P1) and (P2) are self explanatory. For (P3), a possible configuration that can arise in our discussion below is

<u>1</u>	$\bullet$	<u>2</u>	4	<u>5</u>	7	<u>9</u>
$\bullet$	2	3	6	8	9	

where the underlined labels indicate members of  $I_1$ . Here the role of  $z_1$  is played by the 5, so  $a_1$  is the 8 and  $b_i$  is the 9. Note that  $b_i$  need not be immediately to the right of the  $z_i$ . Also, we could have set  $z_i$  to be the box containing the 2, but not the  $\bullet$  nor 9. We emphasize that while it isn't true in the present example, one could have  $y_i = z_i$ .

**Example 6.4.** Note that in (P3),  $b_i$  need not exist. For example, this is the case in

<u>1</u>	$\bullet$
$\bullet$	2

which satisfies (P1)–(P3) with  $z_i = y_i$ .

We now proceed to define  $I_i$  inductively for  $i \geq 1$ . Assume that  $I_{i-1}$  satisfies (P1)–(P3). After performing the slide interchanging  $\bullet$  boxes with  $i$ 's we define  $I_i$  as follows:

- (i) If  $I_{i-1}$  has no box containing  $i$ , then  $I_i := I_{i-1}$ .
- (ii) If  $I_{i-1}$  has a box containing  $i$  and a  $\bullet$  box, then  $I_i := I_{i-1}$ .
- (iii) If  $I_{i-1}$  has a box containing  $i$ , but does not have a  $\bullet$  box, and the  $i$  in  $I_{i-1}$  does not move, then  $I_i := I_{i-1}$ .
- (iv) If  $I_{i-1}$  has a box containing  $i$ , but does not have a  $\bullet$  box, and there is a  $\bullet$  box (not in  $I_{i-1}$ ) immediately to the left of the  $i$  in  $I_{i-1}$ , then let  $I_i$  be  $I_{i-1}$  with

the box containing  $i$  in  $I_{i-1}$  replaced by the box to its left (into which  $i$  has moved).

- (v) If  $I_{i-1}$  has a box containing  $i$ , but does not have a  $\bullet$  box, there is a  $\bullet$  box (not in  $I_{i-1}$ ) immediately above the  $i$ , and we are not in case (iv), then let  $I_i$  be  $I_{i-1}$  with the box containing  $i$  in  $I_{i-1}$  and all the other boxes in  $I_{i-1}$  to the right of it in the same row, replaced by the boxes immediately above them.

Clearly (i)–(v) indeed enumerate all of the intermediate possibilities during a  $Kjdt$  slide.

We now prove that  $I_i$  satisfies (P1)–(P3).

Case (i): We split this case up into three subcases. First, we consider the case that  $I_{i-1}$  has no  $\bullet$  box. In this case, (P1) is trivially satisfied (since it held for  $I_{i-1}$ ), and (P2) and (P3) are vacuously true.

Next, we consider the subcase that  $I_{i-1}$  has a  $\bullet$  box into which an  $i$  (not in  $I_{i-1}$ ) moves. Since (P1) and (P2) are satisfied for  $I_{i-1}$ , (P1) will be satisfied after this, and (P2) and (P3) are vacuous since  $I_i$  has no  $\bullet$  box.

Finally, we consider the subcase where  $I_{i-1}$  has a  $\bullet$  box which stays as such in  $I_i$ . Since the contents of  $I_{i-1}$  and  $I_i$  are the same, (P1) and (P2) are satisfied. To show (P3) is satisfied, observe that the label in the box below  $z_{i-1}$  is strictly greater than  $i$  (otherwise  $z_{i-1}$  has a label weakly smaller than  $i - 1$  and is southeast of a  $\bullet$ , a contradiction), so it does not move, and thus we can take  $z_i := z_{i-1}$ .

For case (ii), we need the following:

**Lemma 6.5.** *If  $I_{i-1}$  satisfies (P1)–(P3) and contains a  $\bullet$  box and a box labelled  $i$  then the  $i$  is immediately to the right of the  $\bullet$  box.*

*Proof.* By (P2), the next box in  $I_{i-1}$  after the  $\bullet$  box  $y_{i-1}$  must be the box containing  $i$ . Suppose that that box is not in the same row as  $y_{i-1}$ . Then  $y_{i-1}$  is the last box in  $I_{i-1}$  in its row, so we must have  $z_{i-1} = y_{i-1}$ , and  $b_{i-1}$  must be the box from  $I_{i-1}$  containing  $i$ .

Observe that in  $T_{i-1}$ , there is no label  $\ell < i$  which is weakly southeast of a  $\bullet$ . Thus the entry in  $a_{i-1}$  is at least  $i$ , violating (P3). It follows that the box containing  $i$  is in the same row as  $y_{i-1}$ . Using the same observation again, we see that there are no possible labels for a box between  $y_{i-1}$  and the box containing  $i$ , and therefore, they are adjacent.  $\square$

Now, using Lemma 6.5, it is clear that case (ii) preserves (P1) and (P2). To check (P3), as in the previous case, we can take  $z_i := z_{i-1}$ . This would not work if  $z_{i-1} = y_{i-1}$ , but this is impossible, because the entry in the box below  $z_{i-1}$  should be less than the next entry in  $I_{i-1}$  after  $z_{i-1}$ , which is  $i$ . So the  $\bullet$  box is immediately above a box which is at most  $i - 1$ , and this can't happen in  $T_{i-1}$ .

Cases (iii) and (iv) are trivial: (P1) holds since the contents of  $I_{i-1}$  and  $I_i$  are the same, and (P2) and (P3) are vacuously true since  $I_i$  contains no  $\bullet$  box.

Now we consider case (v). (P1) is trivial, so if  $I_i$  has no  $\bullet$  box, then we are done. So assume it does. The only way a  $\bullet$  box could appear in  $I_i$  is in the following situation:

$$\begin{array}{|c|c|} \hline \bullet & i \\ \hline i & k \\ \hline \end{array} \mapsto \begin{array}{|c|c|} \hline i & \bullet \\ \hline \bullet & k \\ \hline \end{array},$$

where the box containing  $k$  is also in  $I_{i-1}$ .

In this situation the top two boxes will be in  $I_i$ , and so we will have introduced a  $\bullet$  box into  $I_i$ . (P2) is clearly satisfied. Set  $z_i$  to be the rightmost of the boxes that are in  $I_i$  but not in  $I_{i-1}$ . Now (P3) is satisfied because (P1) was satisfied for  $I_{i-1}$ .

This completes the proof that  $I_i$  satisfies (P1)–(P3). Thus after iteration, we eventually terminate with a set of boxes  $I_m$  in  $T_m := K\text{jdt}_{\{x_i\}}(T)$  which satisfies (P1)–(P3). We wish to show that  $I_m$  contains no  $\bullet$  box. Suppose that it did. This  $\bullet$  box of  $I_m$  must be an outer corner of  $T$  (by the way  $K\text{jdt}$  is defined). This contradicts (P3), since the square below  $z_i$  is southeast of the  $\bullet$  box, and thus contains no label. Thus  $I_m$  contains no  $\bullet$  box, so (P1) implies that there is a strictly increasing subsequence of the reading word of  $K\text{jdt}_{\{x_i\}}(T)$  whose length equals the length of  $I$ , as desired.  $\square$

**Remark 6.6.** Theorem 6.1 may be regarded as a generalization of the classical result of Schensted which asserts that the longest increasing subsequence of a permutation  $w = w_1 w_2 \dots w_n$  in the symmetric group  $S_n$  (written in one-line notation) is equal to the first row of the common shape of the corresponding insertion and recording tableaux under the Robinson–Schensted algorithm; see, for example, [Stanley 1999]. To see this, one needs to use the well-known fact that the insertion tableau of  $w$  is equal to the (classical) rectification of the “permutation tableau”  $T_w$  of skew shape

$$(n, n-1, n-2, \dots, 3, 2, 1)/(n-1, n-2, \dots, 3, 2, 1),$$

where  $w_1$  occupies the southwest-most box, followed by  $w_2$  in the box to its immediate northeast, and so on. In [Thomas and Yong 2008b] we further explore this observation, and connect  $K\text{rect}$  to the Hecke algorithm of [Buch et al. 2008].

Recall the definition of  $t$ -Pieri filling given in Section 5.

**Lemma 6.7.** *If an increasing tableau  $T$  rectifies (with respect to any rectification order) to a tableau  $V$  which has precisely  $1, 2, \dots, t$  in the first row and no labels weakly smaller than  $t$  elsewhere, then*

- (1) *the labels  $1, 2, \dots, t$  form a subtableau of  $T$  that is a  $t$ -Pieri filling, and*
- (2)  $\text{LIS}(T) = t$ .

*Proof.* By Lemma 3.3,  $V$  contains the rectification of the subtableau of  $T$  consisting of the entries between 1 and  $t$ ; by results of the previous section, it follows that these entries must form a  $t$ -Pieri filling; this proves that (1) holds.

By Theorem 6.1,  $\text{LIS}(T) = \text{LIS}(V) = t$ , proving (2).  $\square$

*Proof of Theorem 1.2.* Let  $R \in \text{INC}(\lambda)$  encode a rectification where

$$\text{Kinfusion}_1(R, T) = S_\mu.$$

Let us suppose that the first row of  $S_\mu$  is  $S_{(t)}$ . By Theorem 6.1,  $\text{LIS}(T) = t$ . By Lemma 6.7, the subtableau  $P$  of  $T$ , consisting of the boxes containing one of the labels  $1, 2, \dots, t$ , is a  $t$ -Pieri filling.

Suppose  $Q \in \text{INC}(\lambda)$  is another rectification order. Since the labels of  $P$  are weakly smaller than  $t$  and those of  $T \setminus P$  are strictly larger than  $t$ , by Lemma 3.3, we can compute  $V := \text{Kinfusion}_1(Q, T)$  in two stages. First, by Lemma 5.4,  $\text{Kinfusion}_1(Q, P)$  is simply  $S_{(t)}$ , because  $P$  is a  $t$ -Pieri filling. Secondly, we use  $\text{Kinfusion}_2(Q, P)$  to (partially) rectify  $T \setminus P$ . *A priori*, this could contribute extra boxes to first row of  $V$  but since, by Theorem 6.1,  $\text{LIS}(V) = \text{LIS}(T) = t$ , it does not. Thus the rectification of  $T$  by  $Q$  consists of the row  $S_{(t)}$  with a rectification of  $T \setminus P$  to a straight shape underneath it.

Now, by assumption  $T \setminus P$  has a (partial) rectification to a superstandard tableaux (using labels starting from  $t + 1$ ), namely  $S_\mu \setminus S_{(t)}$ . So by induction on the number of boxes of the starting shape, we can conclude that  $T \setminus P$  will (partially) rectify to  $S_\mu \setminus S_{(t)}$  under any rectification order. Therefore  $V = S_\mu$ , as desired.  $\square$

## 7. Minuscule Schubert calculus conjectures: example and discussion

In earlier work [Thomas and Yong 2006; 2007], we introduced root-system uniform combinatorial rules for minuscule Schubert calculus. Theorem 1.4 has the advantage that it admits a straightforward conjectural generalization to the minuscule setting. We state one form of our conjecture below; more details will appear in forthcoming work.

Let  $G$  be a complex, connected reductive Lie group with root system  $\Phi$ , positive roots  $\Phi^+$  and base of simple roots  $\Delta$ . To each subset of  $\Delta$  is associated a parabolic subgroup  $P$ . The *generalized flag variety*  $G/P$  has *Schubert varieties*

$$X_w := \overline{B_- w P / P}$$

for  $wW_P \in W/W_P$ , where  $W$  is the Weyl group of  $G$  and  $W_P$  is the parabolic subgroup of  $W$  corresponding to  $P$ . Let  $K(G/P)$  be the Grothendieck ring of  $G/P$ , with a basis of Schubert structure sheaves  $\{[\mathcal{O}_{X_w}]\}$ . Define Schubert structure constants  $C_{u,v}^w(G/P)$  as before, by

$$[\mathcal{O}_{X_u}] \cdot [\mathcal{O}_{X_v}] = \sum_{wW_P \in W/W_P} C_{u,v}^w(G/P) [\mathcal{O}_{X_w}].$$

Brion [2005] has established that

$$(-1)^{\ell(w)-\ell(u)-\ell(v)} C_{u,v}^w(G/P) \in \mathbb{N},$$

where  $\ell(w)$  is the *Coxeter length* of the minimal length coset representative of  $wW_P$ .

A maximal parabolic subgroup  $P$  is said to be *minuscule* if the associated fundamental weight  $\omega_P$  satisfies  $\langle \omega_P, \alpha^\vee \rangle \leq 1$  for all  $\alpha \in \Phi^+$  under the usual pairing between weights and coroots. The *minuscule flag varieties*  $G/P$  are classified into five infinite families and two exceptional cases (the type  $A_{n-1}$  cases are the Grassmannians  $\text{Gr}(k, \mathbb{C}^n)$ ).

Associated to each minuscule  $G/P$  is a planar poset  $(\Lambda_{G/P}, <)$ , obtained as a subposet of the poset of positive roots  $\Omega_{G^\vee}$  for the dual root system of  $G$ ; this fact has been known for some time, and recently has been exploited by various authors; see, for example, [Perrin 2007; Purbhoo and Sottile 2008] among others. In this context, *shapes*  $\lambda$  are lower order ideals in this poset. These shapes are in bijection with the cosets  $wW_P$  indexing the Schubert varieties; in particular, if  $wW_P \leftrightarrow v$  under this bijection,  $\ell(w) = |v|$ . Define a *skew shape*  $v/\lambda := v \setminus \lambda$  to be a set theoretic difference of two shapes. Define an *increasing tableau* of shape  $v/\lambda$  to be an assignment

$$\text{label} : v/\lambda \rightarrow \{1, 2, \dots, q\}$$

such that  $\text{label}(x) < \text{label}(y)$  whenever  $x < y$ , and where each label appears at least once. An *inner corner* of  $v/\lambda$  is a maximal element  $x \in \Lambda_{G/P}$  that is below some element in  $v/\lambda$ . With these definitions, we define notions of  $\text{INC}_{G/P}(v/\lambda)$ ,  $\text{Kjdt}_{G/P; \{x_i\}}$ ,  $\text{Krect}_{G/P}$ , superstandard  $S_\mu$ , and so on, in a manner analogous to those we have given for the Grassmannian. The following rule is new for all minuscule  $G/P$ :

**Conjecture 7.1.** *For any minuscule  $G/P$ ,  $(-1)^{|v|-|\lambda|-|\mu|} C_{\lambda,\mu}^v(G/P)$  equals the number of  $T \in \text{INC}_{G/P}(v/\lambda)$  such that  $\text{Krect}_{G/P}(T) = S_\mu$ .*

Implicit in this conjecture is the conjecture that an analogue of Theorem 1.2 holds. A weaker form of these conjectures is that there is a tableau  $C_\mu$  for each shape  $\mu$  such that the aforementioned conjectures hold after replacing  $S_\mu$  by  $C_\mu$ .

Briefly, using the ideas contained in this paper, together with those in [Thomas and Yong 2006; 2007] it is not hard to show that  $\text{Kjdt}_{G/P; \{x_i\}}$  is well-defined. The next aim is to establish the analogue of Theorem 1.2. Once this is achieved we can prove that our conjectural rule defines an associative, commutative ring with an additive  $\mathbb{Z}$ -basis indexed by shapes. It would then remain to show that such rules compute the correct geometric numbers.

The interested reader may find details compatible with the notation used here in [Thomas and Yong 2006]; in particular, there we concretely describe  $\Lambda_{G/P}$  in



associated to  $E_7$ , which while not exhaustive, left us convinced. In particular, our choice of definition of superstandard passes these checks (although we also expect that other choices of  $S_\mu$  would as well, such as the ones obtained by rastering by columns, rather than rows).

We emphasize that this rule agrees in type  $A$  with the correct product, and as well as in cohomology for all minuscule cases. We also have some computational evidence that our numbers agree with small known cases of Schubert structure constants in type  $B$  (as supplied to us by M. Shimozono in private correspondence), although admittedly this is not a convincing amount of evidence on its own. Part of the difficulty in checking Conjecture 7.1 is that it seems to be a challenging task to construct efficient software to compute the  $K$ -theory Schubert structure constants for the main cases of the minuscule  $G/P$ 's outside of type  $A$ . In principle, such an algorithm is linear algebra using torus-equivariant fixed-point localization methods such as [Willems 2006].

Granted associativity, the conjectures would follow if they agree with multiplication in  $K(G/P)$  whenever  $\mu$  is drawn from some set of multiplicative generators  $\mathcal{P}$  for  $K(G/P)$ . (That is, they agree with a ‘‘Pieri rule’’.)

We also mention that the results of Sections 2–4 also have straightforward minuscule generalizations in cohomology; see [Thomas and Yong 2007].

## 8. Counterexamples

It is interesting that natural analogues of a number of results valid in the standard Young tableau theory are actually false in our setting. We have already seen in the introduction that in general  $K\text{rect}$  is not well-defined. This aspect can also be blamed for the following two other situations where counterexamples exist:

**Haiman’s dual equivalence.** One can define  *$K$ -theoretic dual equivalence*, extending ideas in [Haiman 1992]. Two increasing tableaux are  *$K$ -dual equivalent* if any sequence of slides ( $\{x_{i_1}^{(1)}\}, \dots, \{x_{i_k}^{(k)}\}$ ) for  $T$  and  $U$  results in increasing tableaux of the same shape. In this case we write

$$T \equiv_D U.$$

By definition,  $T \equiv_D U$  implies

$$\text{shape}(T) = \text{shape}(U).$$

One application of this theory (in the classical setting) is that it leads to a proof of the fundamental theorem of jeu de taquin. For a minuscule (but not  $K$ -theoretic) generalization, see [Thomas and Yong 2007]. However, it is important for this application that all standard Young tableaux of the same shape are dual equivalent. In view of Theorem 1.2, it is not surprising that this is not true in our setting.

Consider the computations

$$\begin{aligned} \text{Kinfusion}_2 \left( \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & \\ \hline \end{array}, \begin{array}{|c|c|c|} \hline & & 2 \\ \hline & 1 & 4 \\ \hline 1 & 3 & \\ \hline \end{array} \right) &= \begin{array}{|c|c|c|} \hline & & 1 \\ \hline 2 & 3 & \\ \hline \end{array}, \\ \text{Kinfusion}_2 \left( \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & \\ \hline \end{array}, \begin{array}{|c|c|c|} \hline & & 2 \\ \hline & 1 & 4 \\ \hline 1 & 3 & \\ \hline \end{array} \right) &= \begin{array}{|c|c|c|} \hline & 1 & 2 \\ \hline 1 & 3 & \\ \hline \end{array}. \end{aligned}$$

These calculations represent two sequences of  $Kjdt$  slides applied to different tableaux of the same shape  $(2, 1)$ , but whose results are tableaux of different (skew) shapes.

**Cartons.** In an earlier paper [Thomas and Yong 2008a], we gave an  $S_3$ -symmetric Littlewood–Richardson rule in terms of *cartons*. This idea also has a minuscule extension (which we will report on elsewhere). However, the naïve  $K$ -theoretic generalization does not work.

Briefly, the *carton* of [Thomas and Yong 2008a] is a three-dimensional box with a grid drawn rectilinearly on the six faces of its surface, each of whose sides are growth diagrams. We fix at the outset standard Young tableaux of shape  $\lambda$ ,  $\mu$  and  $\nu$  along three edges. Shapes are associated to each vertex so that the Fomin growth conditions (F1) and (F2) reproduced in Section 2 hold. The number of such cartons (with fixed initial data) is equal to the classical Littlewood–Richardson number.

The temptation is to attempt to generalize this to  $K$ -theory by replacing the initial standard Young tableau with superstandard tableau of shapes  $\lambda$ ,  $\mu$  and  $\nu$ , and to instead utilize the growth conditions (G1) and (G2) we introduced in Section 2. This does not work: one computes using Theorem 1.4 that if  $k = n - k = 3$ ,  $\lambda = \mu = (2, 1)$  and  $\nu = (2)$  then the constant  $C_{(2,1),(2,1),(2)} := C_{(2,1),(2,1)}^{(3,3,1)} = -2$ . However one cannot consistently complete a legal filling of this  $K$ -carton.

**Remark 8.1.** These obstructions are closely related to failure of associativity of a certain tableau product defined in [Buch et al. 2008, Section 3.7].

An  $\mathbb{Z}_3$ -symmetric rule preserving the *triality symmetry*

$$C_{\lambda,\mu,\nu^\vee} = C_{\mu,\nu^\vee,\lambda} = C_{\nu^\vee,\lambda,\mu}$$

where  $C_{\lambda,\mu,\nu^\vee} := C_{\lambda,\mu}^\nu$  and so on exists in the form of *puzzles*; see [Vakil 2006]). (Unlike in cohomology, in  $K$ -theory, this latter symmetry is not immediate from the geometric definitions; for a proof see [Buch 2002b; Vakil 2006]. In fact, this symmetry is not expected to hold for general  $G/P$ , although A. Knutson has informed us, in private communication, that it holds in the minuscule setting.)



## 9. Concluding remarks

**Proctor's  $d$ -complete posets.** Proctor [2004] has studied the class of  $d$ -complete posets. These posets generalize those required in our discussion of minuscule  $G/P$  Schubert calculus; see also [Thomas and Yong 2006; 2007]. In particular,  $d$ -complete posets were shown by Proctor to have a well-defined *jeu de taquin* procedure.

It would be interesting to generalize our arguments to show that for any  $d$ -complete poset  $D$ , there is an associative ring  $K(D)$  with an additive  $\mathbb{Z}$ -basis indexed by lower order ideals of  $D$  and structure constants defined by a rule generalizing Theorem 1.4. Observing that our notions of  $Kjdt$ ,  $Krect$  *a priori* make sense in this more general context, we ask:

**Problem 9.1.** Fix a  $d$ -complete poset. For which classes of tableaux  $\mathcal{C} = \{C_\mu\}$  (indexed by lower order ideals  $\mu$  of  $D$ ) is it true that an analogous Theorem 1.2 holds (that is, if  $Krect(T) = C \in \mathcal{C}$  under one rectification order, this holds for any rectification order)?

It seems plausible that good classes  $\mathcal{C}$  that play the role of the superstandard tableaux of Theorem 1.2 always exist. As we have said, for the minuscule cases, we believe that the superstandard tableaux suffice. Perhaps this also holds more generally.

Assuming this plausible claim holds, one would also like to find a geometric origin to the ring  $K(D)$  (outside of the cases where it should be isomorphic to the  $K$ -theory ring of a minuscule  $G/P$ ).

**A product-differences conjecture.** Let  $\lambda, \mu \in \mathbb{Y}$ . Since this poset is in fact a lattice, we can speak of their *meet*  $\lambda \wedge \mu$  and *join*  $\lambda \vee \mu$ .

**Conjecture 9.2.** Suppose  $\lambda, \mu \subseteq \Lambda$ . Let

$$[\mathbb{O}_{X_{\lambda \wedge \mu}}][\mathbb{O}_{X_{\lambda \vee \mu}}] - [\mathbb{O}_{X_\lambda}][\mathbb{O}_{X_\mu}] = \sum_v d_v [\mathbb{O}_{X_v}].$$

Then

$$(-1)^{|v| - |\lambda| - |\mu|} d_v \geq 0.$$

This conjecture generalizes a theorem in the cohomological case [Lam et al. 2007]; see related work [Okounkov 2003; Fomin et al. 2005; Chindris et al. 2007]. (We also know of no counterexample for the corresponding minuscule conjecture, even in the cohomology case.)

**Example 9.3.** Let

$$\lambda = (4, 2, 1), \quad \mu = (3, 3, 2) \subseteq \Lambda = 4 \times 5.$$

The join is the unique minimal shape that contains  $\lambda$  and  $\mu$ , that is,  $\lambda \vee \mu = (4, 3, 2)$ . Similarly, the meet is the unique maximal shape contained in  $\lambda$  and  $\mu$ . Hence  $\lambda \wedge \mu = (3, 2, 1)$ . One computes using Theorem 1.4 (or otherwise), preferably with the help of a computer, that

$$\begin{aligned} [\mathbb{O}_{X_{(4,3,2)}}] \cdot [\mathbb{O}_{X_{(3,2,1)}}] - [\mathbb{O}_{X_{(4,2,1)}}] \cdot [\mathbb{O}_{X_{(3,3,2)}}] \\ = ([\mathbb{O}_{X_{(5,5,3,2)}}] + 2[\mathbb{O}_{X_{(5,5,4,1)}}] + [\mathbb{O}_{X_{5,5,5}}] + [\mathbb{O}_{X_{5,4,4,2}}]) \\ - (3[\mathbb{O}_{X_{(5,5,5,1)}}] + [\mathbb{O}_{X_{(5,5,3,3)}}] + 5[\mathbb{O}_{X_{(5,5,4,2)}}] + [\mathbb{O}_{X_{(5,4,4,3)}}]) \\ + (3[\mathbb{O}_{X_{(5,5,5,2)}}] + 3[\mathbb{O}_{X_{(5,5,4,3)}}]) \\ - ([\mathbb{O}_{X_{(5,5,5,3)}}]), \end{aligned}$$

in agreement with Conjecture 9.2.

**Hecke insertion and factor sequence formulae.** In [Buch et al. 2008] a generalization of the Robinson–Schensted and Edelman–Greene insertion algorithms was given. In fact, increasing tableaux also play a prominent role there, although in a different, but related way. As we have mentioned in Section 1, this is explored, in part, in [Thomas and Yong 2008b], in connection to longest strictly increasing subsequences in random words. There we show that the insertion tableau of a word under Hecke insertion can be alternatively computed as a  $K$ -rectification of a permutation tableau (for a particular choice of rectification order).

A related question: is there a “plactification map” in the sense of [Reiner and Shimozono 1995]?

We believe that further developing this connection may allow one to, for example, prove a  $K$ -theory analogue of the “factor sequence formula” conjectured in [Buch and Fulton 1999] and proved in [Knutson et al. 2006], which is a problem that has remained open in this topic; see [Buch 2002a; 2005a]. (In [Buch et al. 2008] a different factor sequence formula, generalizing the one given in [Buch 2005a], was given.)

## Appendix: Grothendieck polynomials

The goal of this appendix is to provide combinatorial background for the results of Sections 1–7, in terms of the Grothendieck polynomials of Lascoux and Schützenberger [1982]. This presentation is not needed for the paper.

Fix a shape  $\lambda$  and define a *set-valued tableau*  $T$  to be an assignment of nonempty sets of natural numbers to each box of  $\lambda$  [Buch 2002b]. Such a tableau is *semi-standard* if for every box, the largest entry is weakly smaller than the minimum entry of the box immediately to its right and strictly smaller than the minimum entry of the box immediately below it. The *ordinary* case is when  $T$  assigns a singleton to each box. The following are examples of an ordinary and a set-valued

semistandard tableau:

$$T_1 = \begin{array}{|c|c|c|c|c|} \hline 1 & 2 & 4 & 4 & 6 \\ \hline 2 & 3 & 5 & & \\ \hline 4 & & & & \\ \hline \end{array}, \quad T_2 = \begin{array}{|c|c|c|c|c|} \hline 1, 2 & 2, 3 & 4, 5, 6 & 6, 7 & 7, 8 \\ \hline 3, 4 & 4, 5 & 7 & & \\ \hline 6, 7, 8 & & & & \\ \hline \end{array}.$$

Associate to each semistandard tableau a *weight*

$$\omega(T) := (-1)^{|T| - |\lambda|} x^T$$

where here  $x^T = x_1^{i_1} x_2^{i_2} \cdots$  if  $i_j$  is the number of  $j$ 's appearing in  $T$ , and  $|T|$  is the number of entries of  $T$ . For example, we have

$$\omega(T_1) = x_1 x_2^2 x_3 x_4^3 x_5 x_6 \quad \text{and} \quad \omega(T_2) = (-1)^{19-9} x_1 x_2^2 x_3^2 x_4^3 x_5^2 x_6^3 x_7^4 x_8^2.$$

The *Grothendieck polynomial* is defined as

$$G_\lambda(x_1, x_2, \dots, x_k) := \sum_T \omega(T)$$

with the sum over all set-valued semistandard tableaux using the labels of size at most  $k$ . This is an inhomogeneous symmetric polynomial whose lowest degree ( $= |\lambda|$ ) homogeneous component is equal to the *Schur polynomial*  $s_\lambda(x_1, x_2, \dots, x_k)$ .

It is not immediately obvious from the definitions, but true [Buch 2002b] (for an alternative proof, see [Buch et al. 2008]) that the  $G_\lambda(x_1, \dots, x_k)$  (for  $\lambda$  with at most  $k$  parts) form a  $\mathbb{Z}$ -linear basis for the ring of symmetric polynomials in  $x_1, \dots, x_k$  (say, with coefficients in  $\mathbb{Q}$ ). Thus we can write

$$G_\lambda(x_1, \dots, x_k) G_\mu(x_1, \dots, x_k) = \sum_\nu C_{\lambda, \mu}^\nu G_\nu(x_1, \dots, x_k).$$

The coefficients  $C_{\lambda, \mu}^\nu$  agree with the  $K$ -theory structure constants for  $\text{Gr}(k, \mathbb{C}^n)$  whenever  $\nu \subseteq \Lambda$ .

There are more general Grothendieck polynomials  $\mathfrak{G}_\pi(x_1, \dots, x_n)$  defined in [Lascoux and Schützenberger 1982] for any permutation  $\pi \in S_n$ . The polynomials  $G_\lambda$  amount to the case that  $\pi$  is *Grassmannian*: it has a unique descent at position  $k$ . In [Buch et al. 2005] a formula was first given that expresses any  $\mathfrak{G}_\pi$  in terms of the  $G_\lambda$ 's. Other formulas for both  $\mathfrak{G}_\pi$  and  $G_\lambda$  are also available; see, for example, [Buch et al. 2008; Knutson and Yong 2004; Knutson et al. 2008; Lascoux 2001] and the references therein.

### Acknowledgments

This work was partially completed while Thomas was visiting the Norges Teknisk–Naturvitenskapelige Universitet; he would like to thank the Institutt for Matematiske Fag for its hospitality. Yong utilized the resources of the Fields Institute, Toronto, while a visitor there. We thank Allen Knutson, Victor Reiner and Mark Shimozono for helpful discussions, as well as Anders Buch for supplying us with software to independently compute the  $K$ -theoretic numbers  $C_{\lambda, \mu}^{\nu}$  (for Grassmannians). We also thank an anonymous referee for comments that led to an improvement of this paper.

### References

- [Benkart et al. 1996] G. Benkart, F. Sottile, and J. Stroomer, “Tableau switching: algorithms and applications”, *J. Combin. Theory Ser. A* **76**:1 (1996), 11–43. MR 97m:05261 Zbl 0858.05099
- [Brion 2005] M. Brion, “Lectures on the geometry of flag varieties”, pp. 33–85 in *Topics in cohomological studies of algebraic varieties*, edited by P. Pragacz, Birkhäuser, Basel, 2005. MR 2006f:14058
- [Buch 2002a] A. S. Buch, “Grothendieck classes of quiver varieties”, *Duke Math. J.* **115**:1 (2002), 75–103. MR 2003m:14018 Zbl 1052.14056
- [Buch 2002b] A. S. Buch, “A Littlewood–Richardson rule for the  $K$ -theory of Grassmannians”, *Acta Math.* **189**:1 (2002), 37–78. MR 2003j:14062 Zbl 1090.14015
- [Buch 2005a] A. S. Buch, “Alternating signs of quiver coefficients”, *J. Amer. Math. Soc.* **18**:1 (2005), 217–237. MR 2006d:14052 Zbl 1061.14050
- [Buch 2005b] A. S. Buch, “Combinatorial  $K$ -theory”, pp. 87–103 in *Topics in cohomological studies of algebraic varieties*, edited by P. Pragacz, Birkhäuser, Basel, 2005. MR 2007a:14056
- [Buch and Fulton 1999] A. S. Buch and W. Fulton, “Chern class formulas for quiver varieties”, *Invent. Math.* **135**:3 (1999), 665–687. MR 2000f:14087 Zbl 0942.14027
- [Buch et al. 2004] A. S. Buch, A. Kresch, and H. Tamvakis, “Littlewood–Richardson rules for Grassmannians”, *Adv. Math.* **185**:1 (2004), 80–90. MR 2005e:05154 Zbl 1053.05121
- [Buch et al. 2005] A. S. Buch, A. Kresch, H. Tamvakis, and A. Yong, “Grothendieck polynomials and quiver formulas”, *Amer. J. Math.* **127**:3 (2005), 551–567. MR 2007d:14018 Zbl 1084.14048
- [Buch et al. 2008] A. S. Buch, A. Kresch, M. Shimozono, H. Tamvakis, and A. Yong, “Stable Grothendieck polynomials and  $K$ -theoretic factor sequences”, *Math. Ann.* **340**:2 (2008), 359–382. MR 2368984 Zbl 05236726
- [Chindris et al. 2007] C. Chindris, H. Derksen, and J. Weyman, “Counterexamples to Okounkov’s log-concavity conjecture”, *Compos. Math.* **143**:6 (2007), 1545–1557. MR 2371381 Zbl 05223860
- [Fomin et al. 2005] S. Fomin, W. Fulton, C.-K. Li, and Y.-T. Poon, “Eigenvalues, singular values, and Littlewood–Richardson coefficients”, *Amer. J. Math.* **127**:1 (2005), 101–127. MR 2006e:05189 Zbl 1072.15010
- [Griffeth and Ram 2004] S. Griffeth and A. Ram, “Affine Hecke algebras and the Schubert calculus”, *European J. Combin.* **25**:8 (2004), 1263–1283. MR 2005h:14118 Zbl 1076.14068
- [Haiman 1992] M. D. Haiman, “Dual equivalence with applications, including a conjecture of Proctor”, *Discrete Math.* **99**:1-3 (1992), 79–113. MR 93h:05173 Zbl 0760.05093

- [Knutson and Miller 2005] A. Knutson and E. Miller, “Gröbner geometry of Schubert polynomials”, *Ann. of Math.* (2) **161**:3 (2005), 1245–1318. MR 2006i:05177 Zbl 1089.14007
- [Knutson and Yong 2004] A. Knutson and A. Yong, “A formula for  $K$ -theory truncation Schubert calculus”, *Int. Math. Res. Not.* **70** (2004), 3741–3756. MR 2005h:14119 Zbl 1072.14071
- [Knutson et al. 2004] A. Knutson, T. Tao, and C. Woodward, “A positive proof of the Littlewood–Richardson rule using the octahedron recurrence”, *Electron. J. Combin.* **11**:1 (2004), Research Paper 61, 18 pp. MR 2005j:05098 Zbl 1053.05119
- [Knutson et al. 2006] A. Knutson, E. Miller, and M. Shimozono, “Four positive formulae for type  $A$  quiver polynomials”, *Invent. Math.* **166**:2 (2006), 229–325. MR 2007k:14098 Zbl 1107.14046
- [Knutson et al. 2008] A. Knutson, E. Miller, and A. Yong, “Tableau complexes”, *Israel J. Math.* **163** (2008), 317–343. MR 2391134 Zbl 1145.05055
- [Knutson et al. 2009] A. Knutson, E. Miller, and A. Yong, “Gröbner geometry of vertex decompositions and of flagged tableaux”, *J. Reine Angew. Math.* (2009). arXiv math/0502144
- [Lam and Pylyavskyy 2007] T. Lam and P. Pylyavskyy, “Combinatorial Hopf algebras and  $K$ -homology of Grassmannians”, *Int. Math. Res. Not. IMRN* 24 (2007), Art. ID rnm125, 48 pp. MR 2377012 Zbl 1134.16017
- [Lam et al. 2007] T. Lam, A. Postnikov, and P. Pylyavskyy, “Schur positivity and Schur log-concavity”, *Amer. J. Math.* **129**:6 (2007), 1611–1622. MR 2369890 Zbl 1131.05096
- [Lascoux 2001] A. Lascoux, “Transition on Grothendieck polynomials”, pp. 164–179 in *Physics and combinatorics. 2000* (Nagoya, 2000), edited by A. N. Kirillov and N. Liskova, World Sci. Publ., River Edge, NJ, 2001. MR 2002k:14082 Zbl 1052.14059
- [Lascoux and Schützenberger 1982] A. Lascoux and M.-P. Schützenberger, “Structure de Hopf de l’anneau de cohomologie et de l’anneau de Grothendieck d’une variété de drapeaux”, *C. R. Acad. Sci. Paris Sér. I Math.* **295**:11 (1982), 629–633. MR 84b:14030 Zbl 0542.14030
- [van Leeuwen 2000] M. A. A. van Leeuwen, “Flag varieties and interpretations of Young tableau algorithms”, *J. Algebra* **224**:2 (2000), 397–426. MR 2001h:14063 Zbl 0979.14025
- [Lenart 2000] C. Lenart, “Combinatorial aspects of the  $K$ -theory of Grassmannians”, *Ann. Comb.* **4**:1 (2000), 67–82. MR 2001j:05124 Zbl 0958.05128
- [Lenart and Postnikov 2007] C. Lenart and A. Postnikov, “Affine Weyl groups in  $K$ -theory and representation theory”, *Int. Math. Res. Not. IMRN* 12 (2007), Art. ID rnm038, 65. MR 2008j:14105 Zbl 1137.14037
- [Manivel 1998] L. Manivel, *Fonctions symétriques, polynômes de Schubert et lieux de dégénérescence*, Cours Spécialisés **3**, Société Mathématique de France, Paris, 1998. Translated in English by John R. Swallow. MR 99k:05159 Zbl 0911.14023
- [Miller 2005] E. Miller, “Alternating formulas for  $K$ -theoretic quiver polynomials”, *Duke Math. J.* **128**:1 (2005), 1–17. MR 2006e:05181 Zbl 1099.05079
- [Okounkov 2003] A. Okounkov, “Why would multiplicities be log-concave?”, pp. 329–347 in *The orbit method in geometry and physics* (Marseille, 2000), edited by C. Duval et al., Progr. Math. **213**, Birkhäuser, Boston, 2003. MR 2004j:20022 Zbl 1063.22024
- [Perrin 2007] N. Perrin, “Small resolutions of minuscule Schubert varieties”, *Compos. Math.* **143**:5 (2007), 1255–1312. MR 2008m:14098 Zbl 1129.14069
- [Proctor 2004] R. Proctor, “ $d$ -Complete posets generalize Young diagrams for the jeu de taquin property”, preprint, 2004, Available at <http://www.math.unc.edu/Faculty/rap/>.
- [Purbhoo and Sottile 2008] K. Purbhoo and F. Sottile, “The recursive nature of cominuscule Schubert calculus”, *Adv. Math.* **217**:5 (2008), 1962–2004. MR 2388083 Zbl 1141.14032

- [Reiner and Shimozono 1995] V. Reiner and M. Shimozono, “Plactification”, *J. Algebraic Combin.* **4**:4 (1995), 331–351. MR 96i:05179 Zbl 0922.05049
- [Schützenberger 1977] M.-P. Schützenberger, “La correspondance de Robinson”, pp. 59–113 in *Combinatoire et représentation du groupe symétrique* (Strasbourg, 1976), edited by D. Foata, Lecture Notes in Math. **579**, Springer, Berlin, 1977. MR 58 #16863 Zbl 0398.05011
- [Speyer 2006] D. Speyer, “A matroid invariant via the K-theory of the Grassmannian”, preprint, 2006. arXiv math/0603551
- [Stanley 1999] R. P. Stanley, *Enumerative combinatorics*, vol. 2, Cambridge Studies in Advanced Mathematics **62**, Cambridge University Press, Cambridge, 1999. MR 2000k:05026 Zbl 0928.05001
- [Thomas and Yong 2006] H. Thomas and A. Yong, “A combinatorial rule for (co)minuscule Schubert calculus”, preprint, 2006. arXiv math/0608273
- [Thomas and Yong 2007] H. Thomas and A. Yong, “Cominuscule tableau combinatorics”, preprint, 2007. arXiv math/0701215
- [Thomas and Yong 2008a] H. Thomas and A. Yong, “An  $S_3$ -symmetric Littlewood–Richardson rule”, *Math. Res. Lett.* **15**:5 (2008), 1027–1037. MR 2443999
- [Thomas and Yong 2008b] H. Thomas and A. Yong, “Longest increasing subsequences, Plancherel-type measure and the Hecke insertion algorithm”, preprint, 2008. arXiv 0801.1319
- [Vakil 2006] R. Vakil, “A geometric Littlewood–Richardson rule”, *Ann. of Math. (2)* **164**:2 (2006), 371–421. MR 2007f:05184
- [Willems 2006] M. Willems, “ $K$ -théorie équivariante des tours de Bott. Application à la structure multiplicative de la  $K$ -théorie équivariante des variétés de drapeaux”, *Duke Math. J.* **132**:2 (2006), 271–309. MR 2007b:19009 Zbl 1118.19002

Communicated by Ravi Vakil

Received 2007-11-04

Revised 2008-09-17

Accepted 2008-11-29

hugh@math.unb.ca

*Tilley Hall 418, Department of Mathematics and Statistics,  
University of New Brunswick, Fredericton, New Brunswick  
E3B 5A3, Canada  
<http://www.math.unb.ca/~hugh/>*

ayong@uiuc.edu

*1409 W. Green Street, Department of Mathematics,  
University of Illinois at Urbana-Champaign,  
Urbana, IL 61801, United States  
<http://www.math.uiuc.edu/~ayong>*

# Weak Hopf monoids in braided monoidal categories

Craig Pastro and Ross Street

We develop the theory of weak bimonoids in braided monoidal categories and show that they are in one-to-one correspondence with quantum categories with a separable Frobenius object-of-objects. Weak Hopf monoids are shown to be quantum groupoids. Each separable Frobenius monoid  $R$  leads to a weak Hopf monoid  $R \otimes R$ .

Introduction	149
1. Weak bimonoids	153
2. Weak Hopf monoids	160
3. The monoidal category of $A$ -comodules	163
4. Frobenius monoid example	175
5. Quantum groupoids	177
6. Weak Hopf monoids and quantum groupoids	182
Appendix A. String diagrams and basic definitions	196
Appendix B. Proofs of the properties of $s$ , $t$ , and $r$	203
Acknowledgments	206
References	206

## Introduction

Weak Hopf algebras, introduced by Böhm, Nill, and Szlachányi in the papers [Böhm and Szlachányi 1996; Nill 1998; Szlachányi 1997; Böhm et al. 1999], are generalizations of Hopf algebras and were proposed as an alternative to weak quasi-Hopf algebras. A weak bialgebra is both an associative algebra and a coassociative coalgebra, but instead of requiring that the multiplication and unit morphism are

---

*MSC2000:* primary 16W30; secondary 18B40, 18D10.

*Keywords:* weak bimonoids (weak bialgebra), weak Hopf monoids (weak Hopf algebra), quantum category, quantum groupoid, monoidal category.

Pastro is partially supported by GCOE, Kyoto University. The majority of this work was completed while he was a PhD student at Macquarie University, Australia, and during that time was gratefully supported by an international Macquarie University Research Scholarship and a Scott Russell Johnson Memorial Scholarship. Street gratefully acknowledges the support of the Australian Research Council Discovery Grant DP0771252.

coalgebra morphisms (or equivalently that the comultiplication and the counit are algebra morphisms), other “weakened” axioms are imposed. The multiplication is still required to be comultiplicative (equivalently, the comultiplication is still required to be multiplicative), but the counit is no longer required to be an algebra morphism and the unit is no longer required to be a coalgebra morphism. Instead, these requirements are replaced by weakened versions (see Equations (v) and (w) below). As the name suggests, any bialgebra satisfies these weakened axioms and is therefore a weak bialgebra.

For a given a weak bialgebra  $A$ , one may define source and target morphisms  $s, t : A \rightarrow A$  whose images  $s(A)$  and  $t(A)$  are called the source and target (counital) subalgebras. Nill [1998] has shown that Hayashi’s face algebras [1998] are special cases of weak bialgebras for which the, say, target subalgebra is commutative.

A weak Hopf algebra is a weak bialgebra  $H$  that is equipped with an antipode  $\nu : H \rightarrow H$  satisfying the axioms<sup>1</sup>

$$\mu(\nu \otimes 1)\delta = t, \quad \mu(1 \otimes \nu)\delta = s, \quad \text{and} \quad \mu_3(\nu \otimes 1 \otimes \nu)\delta_3 = \nu,$$

where  $\mu_3 = \mu(\mu \otimes 1)$  and  $\delta_3 = (\delta \otimes 1)\delta$ . Again, any Hopf algebra satisfies these weakened axioms and so is a weak Hopf algebra. Nill [1998] has also shown that the (finite-dimensional) generalized Kac algebras of Yamanouchi [1994] are examples of weak Hopf algebras with involutive antipode. Weak Hopf algebras have also been called “quantum groupoids” [Nikshych and Vainerman 2002], but in this paper this is *not* what we mean by quantum groupoid.

Perhaps the simplest examples of weak bialgebras and weak Hopf algebras are category algebras and groupoid algebras, respectively. Suppose that  $k$  is a field, and let  $\mathcal{C}$  be a category with set of objects  $\mathcal{C}_0$  and set of morphisms  $\mathcal{C}_1$ . The *category algebra*  $k[\mathcal{C}]$  is the vector space  $k[\mathcal{C}_1]$  over  $k$  with basis  $\mathcal{C}_1$ . Elements are formal linear combinations of the elements of  $\mathcal{C}_1$  with coefficients in  $k$ , that is,

$$\alpha f + \beta g + \cdots \quad \text{with } \alpha, \beta \in k \text{ and } f, g \in \mathcal{C}_1.$$

An associative multiplication on  $k[\mathcal{C}]$  is defined by

$$\mu(f, g) = f \cdot g = \begin{cases} g \circ f & \text{if } g \circ f \text{ exists,} \\ 0 & \text{otherwise} \end{cases}$$

and extended by linearity to  $k[\mathcal{C}]$ . This algebra does not have a unit unless  $\mathcal{C}_0$  is finite, in which case the unit is

$$\eta(1) = e = \sum_{A \in \mathcal{C}_0} 1_A,$$

---

<sup>1</sup>There may be some discrepancy with what we call the source and target morphisms and what exists in the literature. This arises from our convention of taking multiplication in the groupoid algebra to be  $f \cdot g = g \circ f$  (whenever  $g \circ f$  is defined).



making  $k[\mathcal{C}]$  into a unital algebra; all algebras (monoids) considered in this paper will be unital. A comultiplication and counit may be defined on  $k[\mathcal{C}]$  as

$$\delta(f) = f \otimes f, \quad \epsilon(f) = 1,$$

making  $k[\mathcal{C}]$  into a coalgebra. Note that  $k[\mathcal{C}]$  equipped with this algebra and coalgebra structure will not satisfy any of the following usual bialgebra axioms:

$$\epsilon\mu = \epsilon \otimes \epsilon, \quad \delta\eta = \eta \otimes \eta, \quad \epsilon\eta = 1_k.$$

The one bialgebra axiom that does hold is  $\delta\mu = (\mu \otimes \mu)(1 \otimes c \otimes 1)(\delta \otimes \delta)$ . Equipped with this algebra and coalgebra structure,  $k[\mathcal{C}]$  does, however, satisfy the axioms of a weak bialgebra. Furthermore, if  $\mathcal{C}$  is a groupoid, then  $k[\mathcal{C}]$ , which is then called the *groupoid algebra*, is an example of a weak Hopf algebra with antipode  $\nu : k[\mathcal{C}] \rightarrow k[\mathcal{C}]$  defined by  $\nu(f) = f^{-1}$  and extended by linearity. If  $f : A \rightarrow B \in \mathcal{C}$ , the source and target morphisms  $s, t : k[\mathcal{C}] \rightarrow k[\mathcal{C}]$  are given by  $s(f) = 1_A$  and  $t(f) = 1_B$ , as one would expect.

In this paper we define weak bialgebras and weak Hopf algebras in a braided monoidal category  $\mathcal{V}$ , where we prefer to call them “weak bimonoids” and “weak Hopf monoids”. The only difference between our definition of a weak bimonoid in  $\mathcal{V}$  and the one given by Böhm, Nill, and Szlachányi [Böhm et al. 1999] is that a choice of “crossing” must be made in the axioms. Our definition is not as general as the one given by J. N. Alonso, J. M. Fernández, and R. González in [Alonso Álvarez et al. 2008a; 2008b], but, in the case that their weak Yang–Baxter operator  $t_{A,A}$  is the braiding  $c_{A,A}$  and their idempotent  $\nabla_{A \otimes A} = 1_{A \otimes A}$ , our choices of crossings are the same. Our difference in defining weak bimonoids occurs in the choice of source and target morphisms. We have chosen  $s : A \rightarrow A$  and  $t : A \rightarrow A$  so that

- (1) the “globular” identities  $ts = s$  and  $st = t$  hold,
- (2) the source subcomonoid and target subcomonoid coincide (up to isomorphism) and are denoted by  $C$ ; and
- (3)  $s : A \rightarrow C^\circ$  and  $t : A \rightarrow C$  are comonoid morphisms.

These properties of the source and target morphisms are essential for our point of view of quantum categories. These are  $s = \bar{\Pi}_A^L$  and  $t = \Pi_A^R$  in the notation of [Alonso Álvarez et al. 2008a; 2008b] and  $s = \epsilon'_s$  and  $t = \epsilon_s$  in the notation of [Schauenburg 2003], with the appropriate choice of crossings.

We choose to work in the Cauchy completion  $\mathcal{QV}$  of  $\mathcal{V}$ . The category  $\mathcal{QV}$  is also called the “completion under idempotents” of  $\mathcal{V}$  or the “Karoubi envelope” of  $\mathcal{V}$ . We do this rather than assume that idempotents split in  $\mathcal{V}$ . Suppose  $A$  is a weak bimonoid in  $\mathcal{QV}$ . In this case we find  $C$  by splitting either the source or target morphism. As in [Schauenburg 2003, Proposition 4.2],  $C$  is a separable Frobenius monoid in  $\mathcal{QV}$ , meaning that  $(C, \mu, \eta, \delta, \epsilon)$  is a Frobenius monoid with  $\mu\delta = 1_C$ .

Our definition of weak Hopf monoid is the same as the one proposed in [Böhm et al. 1999] for the symmetric case and as in [Alonso Álvarez et al. 2008a; 2008b] when restricted to the braided case. A weak bimonoid  $H$  is a weak Hopf monoid if it is equipped with an antipode  $\nu : H \rightarrow H$  satisfying

$$\mu(\nu \otimes 1)\delta = t, \quad \mu(1 \otimes \nu)\delta = r, \quad \text{and} \quad \mu_3(\nu \otimes 1 \otimes \nu)\delta_3 = \nu,$$

where  $r = \nu s$ . This  $r : H \rightarrow H$  turns out to be the “usual” source morphism, that is,  $\Pi_H^L$  in the notation of [Alonso Álvarez et al. 2008a; 2008b]. Ignoring crossings  $r$  is  $\epsilon_t$  in the notation of [Schauenburg 2003], and our  $r$  and  $t$  correspond respectively to  $\sqcap^L$  and  $\sqcap^R$  in the notation of [Böhm et al. 1999], wherein the morphism  $s$  does not appear. Usually, in the second axiom above,  $\mu(1 \otimes \nu)\delta = r$ , the right side is equal to the chosen source map  $s$  of the weak bimonoid  $H$ . The reason that this  $r$  does not work for us as a source morphism is that it does not satisfy all three requirements for the source morphism mentioned above. This choice of  $r$  allows us to show that any Frobenius monoid in  $\mathcal{V}$  yields a weak Hopf monoid  $R \otimes R$  with bijective antipode; see [Böhm et al. 1999, example in the appendix].

There are a number of generalizations of bialgebras and Hopf algebras to their “many object” versions, for example, Sweedler’s generalized bialgebras [1974], which were later generalized by Takeuchi to  $\times_R$ -bialgebras [1977]; the quantum groupoids of Lu [1996] and Xu [2001]; Schauenburg’s  $\times_R$ -Hopf algebras [2000]; the bialgebroids and Hopf algebroids of Böhm and Szlachányi [2004]; the face algebras [Hayashi 1998] and generalized Kac algebras [Yamanouchi 1994]; and the ones of interest in this paper, the quantum categories and quantum groupoids of Day and Street [2004]. Brzeziński and Militaru [2002, Theorem 3.1] have shown that the quantum groupoids of Lu and Xu are equivalent to Takeuchi’s  $\times_R$ -bialgebras. Schauenburg [1998] has shown that face algebras are an example of  $\times_R$ -bialgebras for which  $R$  is commutative and separable. In [2003, Theorem 5.1], Schauenburg shows that weak bialgebras are also examples of  $\times_R$ -bialgebras for which  $R$  is separable Frobenius (there called Frobenius-separable). Schauenburg also shows in [2003, Theorem 6.1] that a weak Hopf algebra may be characterized as a weak bialgebra  $H$  for which a certain canonical map  $H \otimes_C H \rightarrow \mu(\delta(\eta(1)), H \otimes H)$  is a bijection. As a corollary he shows that the  $\times_R$ -bialgebra associated to the weak Hopf algebra is actually a  $\times_R$ -Hopf algebra.

While bialgebras are self dual, bialgebroids are not. The dual of a bialgebroid is called a “bicoalgebroid” by Brzeziński and Militaru [2002] and further studied by Bálint [2008b]. In the terminology of [Day and Street 2004], these structures are quantum categories in the monoidal category of vector spaces.

According to [Day and Street 2004], a quantum category in  $\mathcal{V}$  consists of two comonoids  $A$  and  $C$  in  $\mathcal{V}$ , with  $A$  playing the role of the object of morphisms, and  $C$  the object-of-objects. There are source and target morphisms  $s, t : A \rightarrow C$ ,

a “composition” morphism  $\mu : A \otimes_C A \rightarrow A$ , and a “unit” morphism  $\eta : C \rightarrow A$ , all in  $\mathcal{V}$ . These data must satisfy a number of axioms. Indeed, ordinary categories are quantum categories in the category of sets.

Motivated by the duality present in  $*$ -autonomous categories [Barr 1995], Day and Street define a quantum groupoid to be a quantum category equipped with a generalized antipode coming from a  $*$ -autonomous structure.

In this paper we show there is a bijection between weak bimonoids and quantum categories for which the object-of-objects is a separable Frobenius monoid. In the case that the weak bimonoid is equipped with an invertible antipode, making it a weak Hopf monoid, we show how to yield a quantum groupoid.

The outline of this paper is as follows: In Section 1, we provide the definition of a weak bimonoid  $A$  in a braided monoidal category  $\mathcal{V}$  and define the source and target morphisms. We then move to the Cauchy completion  $\mathcal{Q}\mathcal{V}$  and prove the three required properties of our source and target morphisms. In this section we also prove that  $C$ , the object-of-objects of  $A$ , is a separable Frobenius monoid.

In Section 2, we introduce Weak Hopf monoids in braided monoidal categories.

In Section 3, we describe a monoidal structure on the categories  $\mathbf{Bicomod}(C)$  of  $C$ -bicomodules in  $\mathcal{V}$ , and  $\mathbf{Comod}(A)$  of right  $A$ -comodules in  $\mathcal{V}$ , such that the underlying functor  $U : \mathbf{Comod}(A) \rightarrow \mathbf{Bicomod}(C)$  is strong monoidal. If  $H$  is a weak Hopf monoid, we are then able to show that the category  $\mathbf{Comod}_f(H)$ , consisting of the dualizable objects of  $\mathbf{Comod}(H)$ , is left autonomous.

In Section 4, we prove that any separable Frobenius monoid  $R$  in a braided monoidal category  $\mathcal{V}$  yields an example of a weak Hopf monoid  $R \otimes R$  with invertible antipode in  $\mathcal{V}$ .

In Section 5, we recall the definitions of quantum categories and of quantum groupoids, and in Section 6, we show the correspondence between weak bimonoids and quantum categories with separable Frobenius object-of-objects. In Section 6, we also show that a weak Hopf monoid with invertible antipode yields a quantum groupoid.

This paper depends heavily on the string diagrams in braided monoidal categories of Joyal and Street [1993], which were shown to be rigorous in [1991]. The reader unfamiliar with string diagrams may first want to read Appendix A, where we review some preliminary concepts using these diagrams. Many string proofs also appear in Appendix B.

## 1. Weak bimonoids

A weak bialgebra [Böhm and Szlachányi 1996; Nill 1998; Szlachányi 1997; Böhm et al. 1999] is a generalization of a bialgebra with weakened axioms. These weakened axioms replace the three that follow by requiring that the unit be a coalgebra

morphism and the counit be an algebra morphism. With the appropriate choices of under and over crossings, the definition of a weak bialgebra carries over rather straightforwardly into braided monoidal categories, where we prefer to call it a “weak bimonoid”.

**1.1. Weak bimonoids.** Suppose that  $\mathcal{V} = (\mathcal{V}, \otimes, I, c)$  is a braided monoidal category.

**Definition 1.1.** A *weak bimonoid*  $A = (A, \mu, \eta, \delta, \epsilon)$  in  $\mathcal{V}$  is an object  $A \in \mathcal{V}$  equipped with the structure of a monoid  $(A, \mu, \eta)$  and a comonoid  $(A, \delta, \epsilon)$  satisfying the following equations.

$$\begin{array}{c} \text{Y-shape} \\ \text{=} \\ \text{Braid} \end{array} \quad (b)$$

$$\begin{array}{c} \text{Y-shape} \\ \text{=} \\ \text{Braid} \\ \text{=} \\ \text{Braid} \end{array} \quad (v)$$

$$\begin{array}{c} \text{Y-shape} \\ \text{=} \\ \text{Braid} \\ \text{=} \\ \text{Braid} \end{array} \quad (w)$$

Suppose  $A$  is a weak bimonoid, and define the *source* and *target* morphisms  $s, t : A \rightarrow A$  of  $A$  as

$$s = \begin{array}{c} \circ \\ \diagup \quad \diagdown \\ \circ \end{array}, \quad \text{and} \quad t = \begin{array}{c} \diagup \quad \diagdown \\ \circ \end{array}.$$

Notice that  $s : A \rightarrow A$  is invariant under rotation by  $\pi$ , while  $t : A \rightarrow A$  is invariant under horizontal reflection and the inverse braiding. Importantly, under either of these transformations

- (m) and (c) are interchanged,<sup>2</sup>
- (b) is invariant, and
- (v) and (w) are interchanged.

Note that these are not the “usual” source and target morphisms. They were chosen, as mentioned in the introduction, precisely because we need them to satisfy the following three properties:

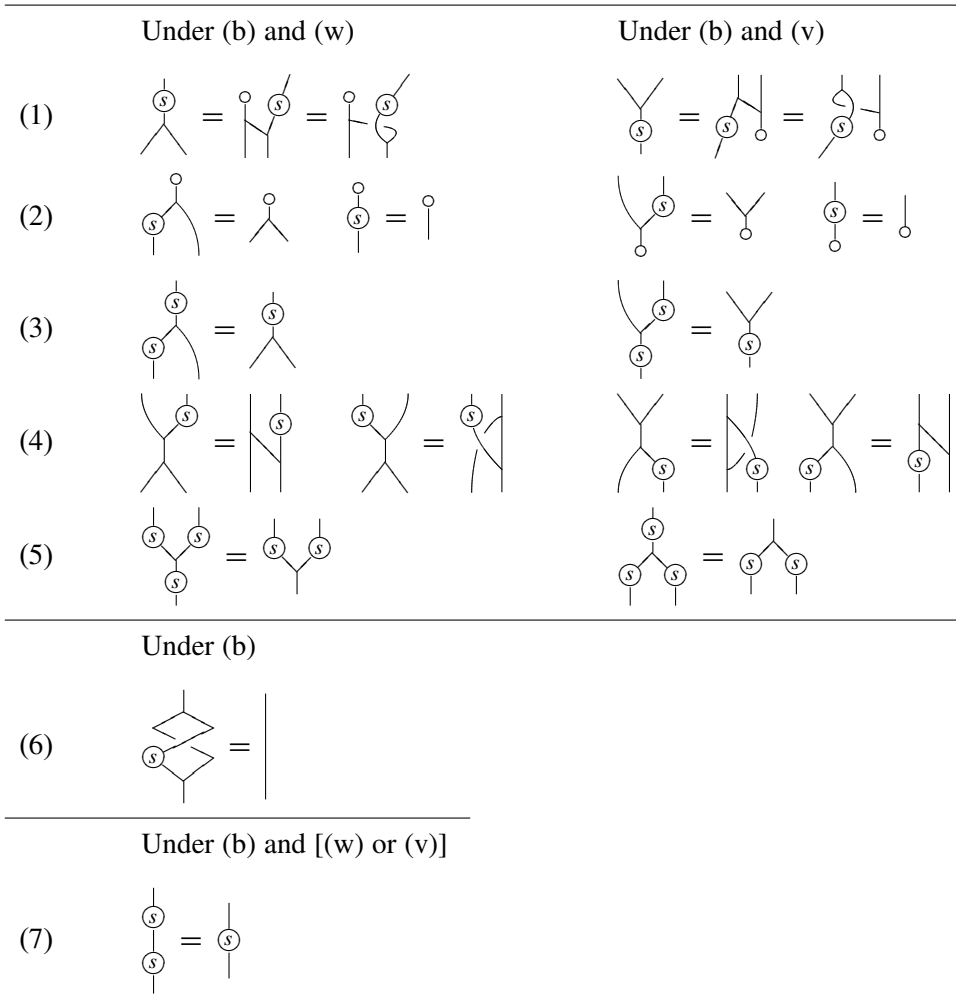
- (i) the “globular” identities  $ts = s$  and  $st = t$  hold;
- (ii) the source subcomonoid and target subcomonoid coincide (up to isomorphism), and are denoted by  $C$ ;
- (iii)  $s : A \rightarrow C^\circ$  and  $t : A \rightarrow C$  are comonoid morphisms.

<sup>2</sup>The (m) and (c) refer to the monoid and comonoid identities found in Appendix A.

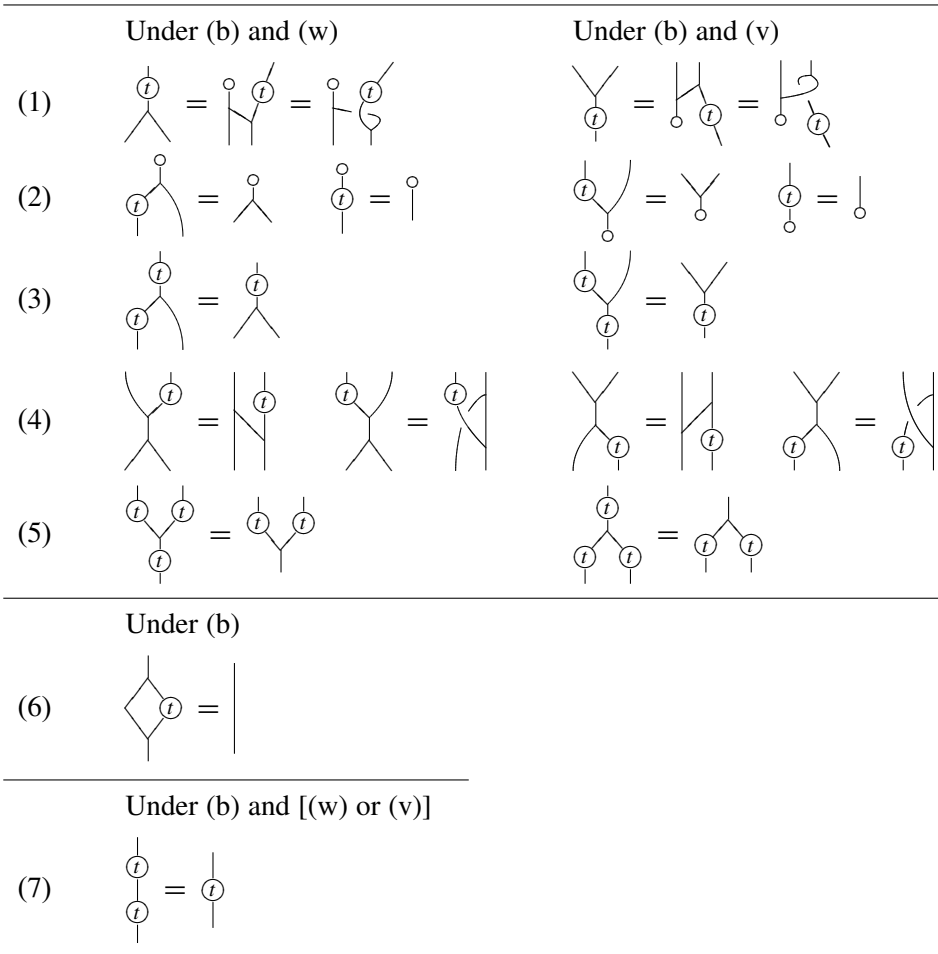
These properties will be proved in this section. Note that we will run into the usual source morphism (which we call  $r$ ) in Definition 2.1, which defines weak Hopf monoids.

We tabulate properties of the source morphism  $s$  in Figure 1, properties of the target morphism  $t$  in Figure 2, and properties involving the interaction of  $s$  and  $t$  in Figure 3. Proofs of these properties may be found in Appendix B.

Suppose  $A$  and  $B$  are weak bimonoids in  $\mathcal{V}$ . A *morphism of weak bimonoids*  $f : A \rightarrow B$  is a morphism  $f : A \rightarrow B$  in  $\mathcal{V}$  that is both a monoid morphism and a comonoid morphism.



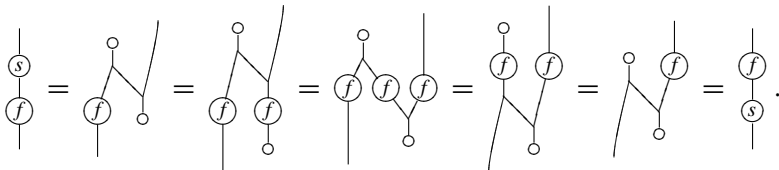
**Figure 1.** Properties of  $s$ .

**Figure 2.** Properties of  $t$ .

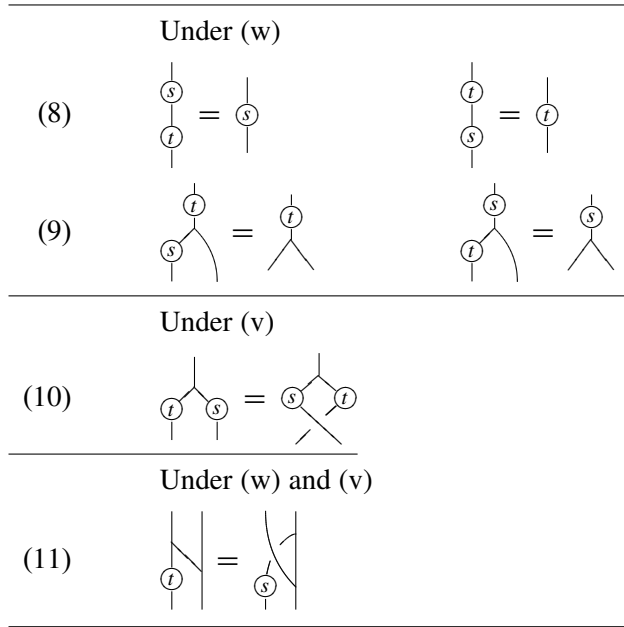
**Lemma 1.2.** Suppose  $A$  and  $B$  are weak bimonoids in  $\mathcal{V}$  each with source and target morphisms  $s$  and  $t$ . If  $f : A \rightarrow B$  is a morphism of weak bimonoids, then

$$fs = sf \quad \text{and} \quad ft = tf.$$

*Proof.* The proof of the first statement is



The second statement follows from a similar proof. □

**Figure 3.** Interactions of  $s$  and  $t$ .

In what follows  $A = (A, \mu, \eta, \delta, \epsilon)$  will always denote a weak bimonoid and  $s, t : A \rightarrow A$  will always denote the source and target morphisms.

From properties (7) and (7) in Figures 1 and 2 respectively,  $s$  and  $t$  are idempotents. In the following we will work in the Cauchy completion (= completion under idempotents = Karoubi envelope)  $\mathcal{Q}\mathcal{V}$  of  $\mathcal{V}$ . We do this rather than assume that idempotents split in  $\mathcal{V}$ .

**1.2. Cauchy completion.** Given a category  $\mathcal{V}$ , its *Cauchy completion*  $\mathcal{Q}\mathcal{V}$  is the category whose objects are pairs  $(X, e)$  with  $X \in \mathcal{V}$  and  $e : X \rightarrow X \in \mathcal{V}$  an idempotent. A morphism  $(X, e) \rightarrow (X', e')$  in  $\mathcal{Q}\mathcal{V}$  is a morphism  $f : X \rightarrow X' \in \mathcal{V}$  such that  $e'fe = f$ . Note that the identity morphism of  $(X, e)$  is  $e$  itself.

The point of working in the Cauchy completion is that every idempotent  $f : (X, e) \rightarrow (X, e)$  in  $\mathcal{Q}\mathcal{V}$  has a splitting, namely,

$$\begin{array}{ccc}
 (X, e) & \xrightarrow{f} & (X, e) \\
 & \searrow f \quad \nearrow f & \\
 & (X, f) &
 \end{array}$$

If  $\mathcal{V}$  is a monoidal category, then  $\mathcal{Q}\mathcal{V}$  is a monoidal category via

$$(X, e) \otimes (X', e') = (X \otimes X', e \otimes e').$$

The category  $\mathcal{V}$  may be fully embedded in  $\mathcal{QV}$  by sending  $X \in \mathcal{V}$  to  $(X, 1) \in \mathcal{QV}$  and  $f : X \rightarrow Y \in \mathcal{V}$  to  $f : (X, 1) \rightarrow (Y, 1)$ , which is obviously a morphism in  $\mathcal{QV}$ . When working in  $\mathcal{QV}$  we will often identify an object  $X \in \mathcal{V}$  with  $(X, 1) \in \mathcal{QV}$ .

**1.3. Properties of the source and target morphisms.** Let  $A = (A, 1)$  be a weak bimonoid in  $\mathcal{QV}$ . From the definition of the Cauchy completion, the result of splitting the source morphism  $s$  is  $(A, s)$ , and similarly, the result of splitting the target morphism  $t$  is  $(A, t)$ . The following proposition shows that these two objects are isomorphic.

**Proposition 1.3.** *The idempotent  $t : (A, 1) \rightarrow (A, 1)$  has the two splittings*

$$\begin{array}{ccc} (A, 1) & \xrightarrow{t} & (A, 1) \\ & \searrow t \quad \nearrow t & \\ & (A, t) & \end{array} \quad \text{and} \quad \begin{array}{ccc} (A, 1) & \xrightarrow{t} & (A, 1) \\ & \searrow t \quad \nearrow s & \\ & (A, s) & \end{array}$$

In this case  $s : (A, s) \rightarrow (A, t)$  and  $t : (A, t) \rightarrow (A, s)$  are inverse morphisms, and hence  $(A, t) \cong (A, s)$ .

*Proof.* This result follows from the identities  $ts = s$  and  $st = t$  (property (8) in Figure 3).  $\square$

We will denote this object by  $C = (A, t)$  and call it the *object-of-objects* of  $A$ . In the propositions next we will show that  $C$  is a comonoid and that it is a separable Frobenius monoid; this is similar to what was done in [Schauenburg 2003] (where it was called Frobenius-separable).

**Proposition 1.4.** *The object  $C = (A, t)$  equipped with*

$$\delta = (C \xrightarrow{\delta} C \otimes C \xrightarrow{t \otimes t} C \otimes C) \quad \text{and} \quad \epsilon = C \xrightarrow{\epsilon} I$$

*is a comonoid in  $\mathcal{QV}$ . If  $C$  is furthermore equipped with*

$$\mu = (C \otimes C \xrightarrow{t \otimes t} C \otimes C \xrightarrow{\mu} C) \quad \text{and} \quad \eta = I \xrightarrow{\eta} C,$$

*then  $C$  is a separable Frobenius monoid in  $\mathcal{QV}$  (see Definition A.5).*

*Proof.* We first observe that  $(t \otimes t)\delta : C \rightarrow C \otimes C$  and  $\epsilon : C \rightarrow I$  are in  $\mathcal{QV}$ , which follows respectively from (5) and (2).

The comonoid identities are given as



and

$$\begin{array}{c} \text{Diagram 1} \end{array} \stackrel{(2)}{=} \begin{array}{c} \text{Diagram 2} \end{array} \stackrel{(c)}{=} \begin{array}{c} \text{Diagram 3} \end{array} \stackrel{(c)}{=} \begin{array}{c} \text{Diagram 4} \end{array} \stackrel{(2)}{=} \begin{array}{c} \text{Diagram 5} \end{array}.$$

To see that  $C$  is a separable Frobenius monoid we first observe that  $\mu$  and  $\eta$  are morphisms in  $\mathcal{W}$  from (5) and (2), and the monoid identities are dual to the comonoid identities. The following calculation proves that the Frobenius condition holds.

$$\begin{array}{c} \text{Diagram 1} \end{array} \stackrel{(7)}{=} \begin{array}{c} \text{Diagram 2} \end{array} \stackrel{(5)}{=} \begin{array}{c} \text{Diagram 3} \end{array} \stackrel{(3)}{=} \begin{array}{c} \text{Diagram 4} \end{array} \stackrel{(4)}{=} \begin{array}{c} \text{Diagram 5} \end{array} \stackrel{(4)}{=} \begin{array}{c} \text{Diagram 6} \end{array} \stackrel{(3)}{=} \begin{array}{c} \text{Diagram 7} \end{array} \stackrel{(5)}{=} \begin{array}{c} \text{Diagram 8} \end{array} \stackrel{(7)}{=} \begin{array}{c} \text{Diagram 9} \end{array}$$

Finally, that this is a separable Frobenius monoid follows from

$$\mu\delta = \begin{array}{c} \text{Diagram 1} \end{array} \stackrel{(7)}{=} \begin{array}{c} \text{Diagram 2} \end{array} \stackrel{(5)}{=} \begin{array}{c} \text{Diagram 3} \end{array} \stackrel{(3)}{=} \begin{array}{c} \text{Diagram 4} \end{array} \stackrel{(6)}{=} \begin{array}{c} \text{Diagram 5} \end{array} = 1_C. \quad \square$$

**Corollary 1.5.** *Every morphism of weak bimonoids induces an isomorphism on the objects-of-objects. That is, if  $(A, 1)$  and  $(B, 1)$  are weak bimonoids, and  $f : (A, 1) \rightarrow (B, 1)$  is a morphism of weak bimonoids, then the induced morphism  $tft : (A, t) \rightarrow (B, t)$  is an isomorphism.*

*Proof.* If  $f : A \rightarrow B$  is a morphism of weak bimonoids, then by Lemma 1.2  $ft = tf$  and  $fs = st$ . The corollary now follows from Propositions 1.4 and A.3.  $\square$

**Proposition 1.6.** *If we write  $C^\circ$  for the comonoid  $C$  with the “opposite” comultiplication defined via*

$$C \xrightarrow{\delta} C \otimes C \xrightarrow{t \otimes t} C \otimes C \xrightarrow{c} C \otimes C = \begin{array}{c} \text{Diagram 1} \end{array},$$

*then  $s : A \rightarrow C^\circ$  and  $t : A \rightarrow C$  are comonoid morphisms. That is, the diagrams*

$$\begin{array}{ccc} A & \xrightarrow{s} & C \\ \delta \downarrow & & \downarrow c(t \otimes t)\delta \\ A \otimes A & \xrightarrow{s \otimes s} & C \otimes C \end{array} \quad \text{and} \quad \begin{array}{ccc} A & \xrightarrow{t} & C \\ \delta \downarrow & & \downarrow (t \otimes t)\delta \\ A \otimes A & \xrightarrow{t \otimes t} & C \otimes C \end{array}$$

*commute.*

*Proof.* The second diagram expresses

$$\begin{array}{c} \textcircled{t} \\ | \\ \textcircled{t} \text{ --- } \textcircled{t} \end{array} = \begin{array}{c} \textcircled{t} \text{ --- } \textcircled{t} \\ | \quad | \end{array},$$

which is exactly (5), and the calculation

$$\begin{array}{c} \textcircled{s} \text{ --- } \textcircled{s} \\ | \quad | \end{array} \stackrel{(5)}{=} \begin{array}{c} \textcircled{s} \\ | \\ \textcircled{s} \text{ --- } \textcircled{s} \\ | \quad | \end{array} \stackrel{(8)}{=} \begin{array}{c} \textcircled{s} \\ | \\ \textcircled{s} \text{ --- } \textcircled{s} \\ | \quad | \\ \textcircled{t} \end{array} \stackrel{(3)}{=} \begin{array}{c} \textcircled{s} \\ | \\ \textcircled{t} \text{ --- } \textcircled{s} \\ | \quad | \end{array} \stackrel{(10)}{=} \begin{array}{c} \textcircled{s} \\ | \\ \textcircled{s} \text{ --- } \textcircled{t} \\ | \quad | \end{array} \stackrel{(9)}{=} \begin{array}{c} \textcircled{s} \\ | \\ \textcircled{t} \text{ --- } \textcircled{t} \\ | \quad | \\ \textcircled{s} \end{array} \stackrel{(8)}{=} \begin{array}{c} \textcircled{s} \\ | \\ \textcircled{t} \text{ --- } \textcircled{t} \\ | \quad | \end{array}$$

shows that the first diagram commutes.  $\square$

## 2. Weak Hopf monoids

In this section we introduce weak Hopf monoids. A weak Hopf monoid is a weak bimonoid  $H$  equipped with an antipode  $\nu : H \rightarrow H$  satisfying the three axioms

$$\nu * 1 = t, \quad 1 * \nu = r, \quad \text{and} \quad \nu * 1 * \nu = \nu,$$

where  $f * g = \mu(f \otimes g)\delta$  is the convolution product, and the morphism  $r : H \rightarrow H$  is introduced below. This turns out to be the usual definition of weak Hopf monoids as found in the literature; in the symmetric case see [Böhm et al. 1999], and in the braided case see [Alonso Álvarez et al. 2008a; 2008b]. Note property (15), which says that  $r = \nu s$ .

**2.1. The endomorphism  $r$  and weak Hopf monoids.** Define an endomorphism  $r : A \rightarrow A$  by rotating the target morphism  $t : A \rightarrow A$  by  $\pi$ , that is,

$$r = \begin{array}{c} \circ \\ | \\ \circ \end{array} \begin{array}{c} \diagup \\ \diagdown \end{array}.$$

Since  $r$  is just  $t$  rotated by  $\pi$ , all the identities for  $t$  in Figure 2 rotated by  $\pi$  hold for  $r$ . We list some additional identities of  $r$  interacting with  $s$  and  $t$ .

$$\begin{array}{c} \textcircled{r} \\ | \\ \textcircled{s} \end{array} = \begin{array}{c} \textcircled{s} \\ | \end{array} \quad (12)$$

$$\begin{array}{c} \textcircled{t} \text{ --- } \textcircled{r} \\ | \quad | \end{array} = \begin{array}{c} \textcircled{r} \text{ --- } \textcircled{t} \\ | \quad | \end{array} \quad (13)$$

$$\begin{array}{c} \textcircled{r} \\ | \\ \textcircled{s} \end{array} = \begin{array}{c} \textcircled{s} \\ | \end{array} \quad (14)$$

**Definition 2.1.** A weak bimonoid  $H$  is called a *weak Hopf monoid* if it is equipped with an endomorphism  $\nu : H \rightarrow H$ , called the *antipode*, satisfying

$$v = \begin{array}{c} | \\ \circlearrowleft t \quad \circlearrowright v \\ | \end{array} = \begin{array}{c} | \\ \circlearrowleft v \quad \circlearrowright r \\ | \end{array}.$$
$$\nu' \equiv \nu' * 1 * \nu' \equiv t * \nu' \equiv \nu * 1 * \nu' \equiv \nu * r \equiv \nu * 1 * \nu \equiv \nu.$$

The proof is also due to the authors of [Alonso Álvarez et al. 2003], where a similar proof may be found. We include it here for completeness.

We list some properties of the antipode  $\nu : H \rightarrow H$ .

**Proposition 2.3.**

$$\begin{array}{c} \textcircled{s} \\ | \\ \textcircled{v} \\ | \end{array} = \begin{array}{c} | \\ \textcircled{r} \\ | \end{array} \quad (15)$$

$$\begin{array}{c} \textcircled{v} \\ | \\ \textcircled{t} \end{array} = \begin{array}{c} \textcircled{r} \\ | \\ \textcircled{v} \end{array} = \begin{array}{c} \textcircled{r} \\ | \\ \textcircled{t} \end{array} \quad \begin{array}{c} \textcircled{v} \\ | \\ \textcircled{r} \end{array} = \begin{array}{c} \textcircled{t} \\ | \\ \textcircled{v} \end{array} = \begin{array}{c} \textcircled{t} \\ | \\ \textcircled{r} \end{array} \quad (16)$$

$$\begin{array}{c} \textcircled{v} \\ | \\ \circ \end{array} = \begin{array}{c} | \\ \circ \end{array} \quad \begin{array}{c} \textcircled{v} \\ / \quad \backslash \\ \text{---} \end{array} = \begin{array}{c} \textcircled{v} \quad \textcircled{v} \\ / \quad \backslash \\ \text{---} \end{array} \quad (17)$$

$$\begin{array}{c} \circ \\ | \\ \textcircled{v} \\ | \end{array} = \begin{array}{c} \circ \\ | \end{array} \quad \begin{array}{c} \text{---} \\ / \quad \backslash \\ \textcircled{v} \end{array} = \begin{array}{c} \text{---} \\ / \quad \backslash \\ \textcircled{v} \quad \textcircled{v} \end{array}$$

The last identity (17) states that  $v : H \rightarrow H$  is both an anticomonoid morphism and an antimonoid morphism.

*Proof.* The calculation

$$\begin{array}{c} \textcircled{s} \\ | \\ \textcircled{v} \end{array} \stackrel{v}{=} \begin{array}{c} \textcircled{s} \\ / \quad \backslash \\ \textcircled{t} \quad \textcircled{v} \\ \backslash \quad / \\ \text{---} \end{array} \stackrel{(9)}{=} \begin{array}{c} \textcircled{s} \\ | \\ \textcircled{v} \end{array} \stackrel{v}{=} \begin{array}{c} \textcircled{s} \\ | \\ \textcircled{r} \end{array} \stackrel{(12)}{=} \begin{array}{c} | \\ \textcircled{r} \\ | \end{array}$$

verifies the identity (15), and

$$\begin{array}{c} \textcircled{v} \\ | \\ \textcircled{t} \end{array} \stackrel{v}{=} \begin{array}{c} \textcircled{t} \quad \textcircled{v} \\ / \quad \backslash \\ \text{---} \\ \backslash \quad / \\ \textcircled{t} \end{array} \stackrel{(3)}{=} \begin{array}{c} \text{---} \\ / \quad \backslash \\ \textcircled{v} \end{array} \stackrel{v}{=} \begin{array}{c} \textcircled{r} \\ | \\ \textcircled{t} \end{array} \stackrel{v}{=} \begin{array}{c} \textcircled{r} \\ | \\ \textcircled{v} \end{array} \stackrel{(3)}{=} \begin{array}{c} \textcircled{r} \quad \textcircled{v} \\ / \quad \backslash \\ \text{---} \\ \backslash \quad / \\ \textcircled{v} \end{array} \stackrel{v}{=} \begin{array}{c} \textcircled{r} \\ | \\ \textcircled{v} \end{array}$$

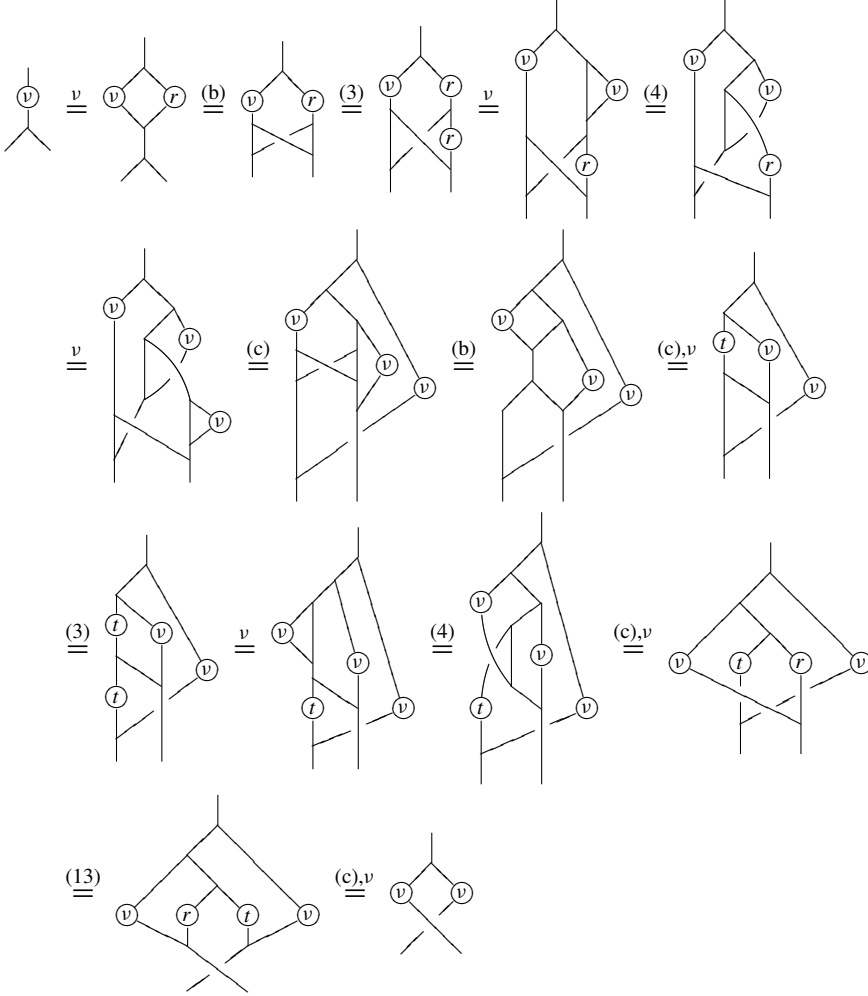
verifies the first identity of (16). The second follows from a similar calculation.

We prove the first two properties of (17), which show that  $v$  is an anticomonoid morphism. The remaining two properties of (17), which show that  $v$  is an antimonoid morphism, following from rotating the diagrams by  $\pi$ .

The proof of the counit property is easy enough:

$$\begin{array}{c} \textcircled{v} \\ | \\ \circ \end{array} \stackrel{v}{=} \begin{array}{c} \textcircled{t} \quad \textcircled{v} \\ / \quad \backslash \\ \text{---} \\ \backslash \quad / \\ \circ \end{array} \stackrel{(2)}{=} \begin{array}{c} \text{---} \\ / \quad \backslash \\ \textcircled{v} \end{array} \stackrel{v}{=} \begin{array}{c} \textcircled{r} \\ | \\ \circ \end{array} \stackrel{(2)}{=} \begin{array}{c} | \\ \circ \end{array}$$

The following calculation proves that the antipode is anticomultiplicative.



### 3. The monoidal category of $A$ -comodules

Suppose  $A = (A, 1)$  is a weak bimonoid in  $\mathcal{V}$  and let  $C = (A, t)$ , which we recall is a separable Frobenius monoid. In this section we describe a monoidal structure on the categories  $\mathbf{Bicomod}(C)$  of  $C$ -bicomodules in  $\mathcal{V}$ , and  $\mathbf{Comod}(A)$  of right  $A$ -comodules in  $\mathcal{V}$ , such that the underlying functor

$$U : \mathbf{Comod}(A) \rightarrow \mathbf{Bicomod}(C)$$

is strong monoidal. If  $A$  is a weak Hopf monoid then we show that  $\mathbf{Comod}_f(A)$ , the subcategory consisting of the dualizable objects, is left autonomous.

This section is fairly standard in the  $\mathcal{V} = \mathbf{Vect}$  case—see for example [Böhm and Szlachányi 2000; Nill 1998; Nikshych and Vainerman 2002]—and carries over rather straightforwardly to the general braided  $\mathcal{V}$  case; see [Day et al. 2003].

**3.1. The monoidal structure on  $C$ -bicomodules.** Suppose, for this section, that idempotents split in  $\mathcal{V}$ , that  $C \in \mathcal{V}$  is a separable Frobenius monoid, and that  $M \in \mathcal{V}$  is a  $C$ -bicomodule with coaction

$$\gamma : M \rightarrow C \otimes M \otimes C.$$

A left  $C$ -coaction and a right  $C$ -coaction are obtained from  $\gamma$  by involving the counit  $\epsilon$  as follows:

$$\begin{aligned} \gamma_l &= (M \xrightarrow{\gamma} C \otimes M \otimes C \xrightarrow{1 \otimes 1 \otimes \epsilon} C \otimes M), \\ \gamma_r &= (M \xrightarrow{\gamma} C \otimes M \otimes C \xrightarrow{\epsilon \otimes 1 \otimes 1} M \otimes C). \end{aligned}$$

Suppose now that  $N$  is another  $C$ -bicomodule. We now wish to define the tensor product of  $M$  and  $N$ . Before doing so we will need the following definition.

**Definition 3.1.** Let  $f, g : X \rightarrow Y$  be a parallel pair in  $\mathcal{V}$ . This pair is called *cosplit* when there is an arrow  $d : Y \rightarrow X$  such that

$$df = 1_X \quad \text{and} \quad fdg = gdg.$$

It is not hard to see that, in this case,  $dg : X \rightarrow X$  is an idempotent and a splitting of  $dg$ , that is,

$$\begin{array}{ccc} X & \xrightarrow{dg} & X \\ & \searrow x & \nearrow y \\ & Q & \end{array} \qquad \begin{array}{ccc} Q & \xrightarrow{1} & Q \\ & \searrow y & \nearrow x \\ & X & \end{array}$$

provides an absolute equalizer  $(Q, y)$  for  $f$  and  $g$ .

Now  $M$  and  $N$  are  $C$ -bicomodules and we have two morphisms

$$M \otimes N \xrightleftharpoons[1 \otimes \gamma_l]{\gamma_r \otimes 1} M \otimes C \otimes N.$$

**Proposition 3.2.** *The pair  $\gamma_r \otimes 1$  and  $1 \otimes \gamma_l$  are cosplit by*

$$d = (1 \otimes \epsilon \otimes 1)(1 \otimes \mu \otimes 1)(\gamma_r \otimes 1 \otimes 1) : M \otimes C \otimes N \rightarrow M \otimes N.$$

*Proof.* Here we barely sketch the proof and note that we prove a very similar statement in greater detail in Proposition 3.3.

That  $d(\gamma_r \otimes 1) = 1$  follows from the separable property of the Frobenius monoid, and  $(\gamma_r \otimes 1)d(1 \otimes \gamma_l) = (1 \otimes \gamma_l)d(1 \otimes \gamma_l)$  follows from the Frobenius property.  $\square$

That this defines a monoidal structure on the category  $\mathbf{Bicomod}(C)$  with tensor product  $\otimes_C$  and unit  $C$  is yet to be proved. However, we thought it better to write the next section more explicitly from which the details here may be filled in.

Suppose that  $M$  is a right  $A$ -comodule. We know that  $s : A \rightarrow C^\circ$  and  $t : A \rightarrow C$  are comonoid morphisms and that property (10) holds, recalling that property (10) expresses the commutativity of the diagram

$$\begin{array}{ccccc}
 & & A \otimes A & \xrightarrow{s \otimes t} & C \otimes C \\
 & \nearrow \delta & & & \downarrow c \\
 A & & & & \\
 & \searrow \delta & A \otimes A & \xrightarrow{t \otimes s} & C \otimes C
 \end{array}$$

$$\gamma = (M \xrightarrow{\gamma} M \otimes A \xrightarrow{1 \otimes \delta} M \otimes A \otimes A \xrightarrow{c^{-1} \otimes 1} A \otimes M \otimes A \xrightarrow{s \otimes 1 \otimes t} C \otimes M \otimes C),$$

$\gamma =$

```

      M
     /|\
    s | A
   ( )| ( )
   C  | C
      /|\
     s | t
    ( )|( )
    C  |C
  
```

$$\gamma_l = \text{diagram of a source node } s \text{ connected to a vertical line} \quad \text{and} \quad \gamma_r = \text{diagram of a target node } t \text{ connected to a vertical line}.$$
$$\gamma_r \otimes 1 = \begin{array}{c} M \quad N \\ \diagdown \quad | \\ A \quad I \\ \diagup \quad | \\ M \quad C \quad N \end{array} \quad \text{and} \quad 1 \otimes \gamma_l = \begin{array}{c} M \quad N \\ | \quad \diagup \\ \quad A \\ | \quad \diagdown \\ S \quad \quad \\ M \quad C \quad N \end{array}$$

**Proposition 3.3.** *The pair  $\gamma_r \otimes 1$  and  $1 \otimes \gamma_l$  are cosplit by*

$$d = \begin{array}{c} M \quad C \quad N \\ \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} t \\ | \\ \circ \end{array} \begin{array}{c} | \\ | \\ | \end{array} \\ M \quad N \end{array}.$$

*Proof.* That  $d$  is a morphism in  $\mathcal{V}$  follows immediately as  $t$  is idempotent. The calculation

$$d(\gamma_r \otimes 1) = \begin{array}{c} \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} t \\ | \\ t \\ | \\ \circ \end{array} \end{array} \stackrel{(7)}{=} \begin{array}{c} \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} t \\ | \\ \circ \end{array} \end{array} \stackrel{(c)}{=} \begin{array}{c} \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} t \\ | \\ \circ \end{array} \end{array} \stackrel{(6)}{=} \begin{array}{c} \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} \circ \end{array} \end{array} \stackrel{(c)}{=} \begin{array}{c} | \\ | \\ | \end{array} = 1_{M \otimes N}$$

shows that  $d(\gamma_r \otimes 1) = 1$ , and the identity

$$(\gamma_r \otimes 1)d(1 \otimes \gamma_l) = (1 \otimes \gamma_l)d(1 \otimes \gamma_l)$$

follows from

$$\begin{aligned} (\gamma_r \otimes 1)d(1 \otimes \gamma_l) &= \begin{array}{c} \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} s \\ | \\ t \\ | \\ \circ \end{array} \end{array} \stackrel{(8)}{=} \begin{array}{c} \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} s \\ | \\ t \\ | \\ \circ \end{array} \end{array} \stackrel{(2)}{=} \begin{array}{c} \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} \circ \end{array} \end{array} \stackrel{(c)}{=} \begin{array}{c} \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} t \\ | \\ \circ \end{array} \end{array} \stackrel{(12)}{=} \begin{array}{c} \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} s \\ | \\ \circ \end{array} \end{array} \\ &\stackrel{(2)}{=} \begin{array}{c} \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} s \\ | \\ s \\ | \\ \circ \end{array} \end{array} \stackrel{(c)}{=} \begin{array}{c} \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} s \\ | \\ \circ \end{array} \end{array} \stackrel{(8)}{=} \begin{array}{c} \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} s \\ | \\ t \\ | \\ \circ \end{array} \end{array} \\ &= (1 \otimes \gamma_l)d(1 \otimes \gamma_l). \end{aligned}$$

□

The idempotent  $d(1 \otimes \gamma_l)$  will be denoted by  $m$ , which gains a simpler representation from the calculation

$$\begin{array}{c} \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} s \\ | \\ t \\ | \\ \circ \end{array} \end{array} \stackrel{(8)}{=} \begin{array}{c} \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} s \\ | \\ \circ \end{array} \end{array} \stackrel{(2)}{=} \begin{array}{c} \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array} \begin{array}{c} \circ \end{array} \end{array} = m.$$



A splitting of  $m$ , that is,

$$\begin{array}{ccc}
 (M \otimes N, 1) & \xrightarrow{m} & (M \otimes N, 1) \\
 \searrow m & & \nearrow m \\
 & (M \otimes N, m) &
 \end{array}
 \quad
 \begin{array}{ccc}
 (M \otimes N, m) & \xrightarrow{m} & (M \otimes N, m) \\
 \searrow m & & \nearrow m \\
 & (M \otimes N, 1) &
 \end{array}$$

provides an absolute equalizer  $(M \otimes N, m)$  of  $(\gamma_r \otimes 1)$  and  $(1 \otimes \gamma_l)$ . Thus, the tensor product of  $M$  and  $N$  over  $C$  is

$$M \otimes_C N = (M \otimes N, m).$$

**3.3. The coaction on the tensor product.** If  $\mathbf{Comod}(A)$  is to be a monoidal category with underlying functor  $U : \mathbf{Comod}(A) \rightarrow \mathbf{Bicomod}(C)$  strong monoidal, then the tensor product of two  $A$ -comodules must also be an  $A$ -comodule. In this section we show that the obvious coaction on  $M \otimes_C N$ , namely,

$$\gamma = \begin{array}{c} | \\ \diagdown \\ | \end{array} : M \otimes_C N \rightarrow M \otimes_C N \otimes A,$$

does the job.

**Lemma 3.4.** *The coaction  $\gamma : M \otimes_C N \rightarrow M \otimes_C N \otimes A$ , as defined above, is a morphism in  $\mathcal{V}$ . That is,*

$$\begin{array}{c} | \\ \diagdown \\ | \end{array} = \begin{array}{c} | \\ \diagdown \\ | \end{array} = \begin{array}{c} | \\ \diagdown \\ | \end{array}.$$

*Proof.* The first equality is given by

$$\begin{array}{c} | \\ \diagdown \\ | \end{array} \stackrel{(c)}{=} \begin{array}{c} | \\ \diagdown \\ | \end{array} \stackrel{(b)}{=} \begin{array}{c} | \\ \diagdown \\ | \end{array} \stackrel{(c)}{=} \begin{array}{c} | \\ \diagdown \\ | \end{array},$$

and the second by the similar calculation:

$$\begin{array}{c} | \\ \diagdown \\ | \end{array} \stackrel{(c)}{=} \begin{array}{c} | \\ \diagdown \\ | \end{array} \stackrel{(b)}{=} \begin{array}{c} | \\ \diagdown \\ | \end{array} \stackrel{(c)}{=} \begin{array}{c} | \\ \diagdown \\ | \end{array}.$$

□

**Proposition 3.5.**  $(M \otimes_C N, \gamma)$  is an  $A$ -comodule.

*Proof.* Coassociativity is proved as usual, by

$$\begin{array}{c} \text{Diagram 1} \\ \text{Diagram 2} \end{array} \stackrel{(b)}{=} \begin{array}{c} \text{Diagram 3} \\ \text{Diagram 4} \end{array} \stackrel{(c)}{=} \begin{array}{c} \text{Diagram 5} \\ \text{Diagram 6} \end{array},$$

and the counit condition is proved as

$$\begin{array}{c} \text{Diagram 1} \\ \text{Diagram 2} \end{array} \stackrel{\text{Lemma 3.4}}{=} \begin{array}{c} \text{Diagram 3} \\ \text{Diagram 4} \end{array} \stackrel{(c)}{=} \begin{array}{c} \text{Diagram 5} \\ \text{Diagram 6} \end{array} \stackrel{(b)}{=} \begin{array}{c} \text{Diagram 7} \\ \text{Diagram 8} \end{array} \stackrel{(c)}{=} \begin{array}{c} \text{Diagram 9} \\ \text{Diagram 10} \end{array} = 1_{M \otimes_C N}. \quad \square$$

**3.4.  $\mathbf{Comod}(A)$  is a monoidal category.** We now set out to prove the claim, at the beginning of this section, that  $(\mathbf{Comod}(A), \otimes_C, C)$  is a monoidal category. It will turn out that associativity is a strict equality (if it is so in  $\mathcal{V}$ ) and the unit conditions are only up to isomorphism.

We state this as a theorem and devote the remainder of this section to its proof.

**Theorem 3.6.**  $\mathbf{Comod}(A) = (\mathbf{Comod}(A), \otimes_C, C)$  is a monoidal category.

First note that  $C$  itself is an  $A$ -comodule with coaction

$$\begin{array}{c} C \\ \downarrow \\ \text{Coaction} \\ \swarrow \searrow \\ C \quad A \end{array}.$$

The following lemma will be useful.

**Lemma 3.7.** *The following identities hold.*

$$\begin{array}{c} \text{Diagram 1} \\ \text{Diagram 2} \end{array} = \begin{array}{c} \text{Diagram 3} \\ \text{Diagram 4} \end{array} \quad \begin{array}{c} \text{Diagram 5} \\ \text{Diagram 6} \end{array} = \begin{array}{c} \text{Diagram 7} \\ \text{Diagram 8} \end{array}$$

*Proof.* The first identity is proved by

$$\begin{array}{c} \text{Diagram 1} \\ \text{Diagram 2} \end{array} \stackrel{(9)}{=} \begin{array}{c} \text{Diagram 3} \\ \text{Diagram 4} \end{array} \stackrel{(11)}{=} \begin{array}{c} \text{Diagram 5} \\ \text{Diagram 6} \end{array} \stackrel{(c)}{=} \begin{array}{c} \text{Diagram 7} \\ \text{Diagram 8} \end{array},$$

and the second is proved by

$$\begin{array}{c} \textcircled{t} \\ | \\ \text{---} \diagup \text{---} \diagdown \\ | \end{array} \stackrel{(3)}{=} \begin{array}{c} \textcircled{t} \\ | \\ \text{---} \diagup \text{---} \diagdown \\ | \textcircled{t} \end{array} \stackrel{(11)}{=} \begin{array}{c} \textcircled{t} \\ | \\ \text{---} \diagup \text{---} \diagdown \\ | \textcircled{s} \end{array} \stackrel{(c)}{=} \begin{array}{c} \textcircled{t} \\ | \\ \text{---} \diagup \text{---} \diagdown \\ | \textcircled{s} \end{array} . \quad \square$$

*Proof of Theorem 3.6.* Consider  $(M \otimes_C N) \otimes_C P$  and  $M \otimes_C (N \otimes_C P)$  in  $\mathfrak{V}$ . The former is  $(M \otimes N \otimes P, u)$  and the latter is  $(M \otimes N \otimes P, v)$ , where

$$u = \begin{array}{c} | \\ | \\ \text{---} \diagup \text{---} \diagdown \\ | \textcircled{t} \end{array} \quad \text{and} \quad v = \begin{array}{c} | \\ | \\ \text{---} \diagup \text{---} \diagdown \\ | \textcircled{s} \end{array} .$$

Since, by Lemma 3.4,  $\gamma$  is a morphism in  $\mathfrak{V}$ , both  $u$  and  $v$  may be rewritten as

$$\begin{array}{c} | \\ | \\ \text{---} \diagup \text{---} \diagdown \\ | \textcircled{t} \end{array} ,$$

proving the (strict) equality  $(M \otimes_C N) \otimes_C P = M \otimes_C (N \otimes_C P)$  in  $\mathfrak{V}$  (since we are writing as if  $\mathfrak{V}$  were strict).

It remains to prove  $M \otimes_C C \cong M \cong C \otimes_C M$ . By definition

$$M \otimes_C C = (M \otimes C, \begin{array}{c} \textcircled{t} \\ | \\ \text{---} \diagup \text{---} \diagdown \\ | \textcircled{t} \end{array}) \quad \text{and} \quad C \otimes_C M = (C \otimes M, \begin{array}{c} \textcircled{t} \\ | \\ \text{---} \diagup \text{---} \diagdown \\ | \textcircled{t} \end{array}) .$$

We will show that the morphisms

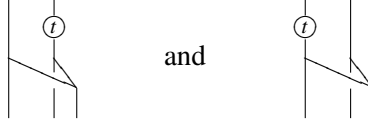
$$\begin{array}{c} \textcircled{t} \\ | \\ \text{---} \diagup \text{---} \diagdown \\ | \textcircled{t} \end{array} : M \otimes_C C \rightarrow M \quad \text{and} \quad \begin{array}{c} | \\ | \\ \text{---} \diagup \text{---} \diagdown \\ | \textcircled{t} \end{array} : M \rightarrow M \otimes_C C$$

will establish the isomorphism  $M \otimes_C C \cong M$ , and

$$\begin{array}{c} \textcircled{t} \\ | \\ \text{---} \diagup \text{---} \diagdown \\ | \textcircled{t} \end{array} : C \otimes_C M \rightarrow M \quad \text{and} \quad \begin{array}{c} | \\ | \\ \text{---} \diagup \text{---} \diagdown \\ | \textcircled{s} \end{array} : M \rightarrow C \otimes_C M$$

will establish the isomorphism  $M \cong C \otimes_C M$ . These morphisms are easily seen to be in  $\mathfrak{V}$ , and the fact that they are mutually inverse pairs is given in one direction by Lemma 3.7, and in the other by an easy string calculation making use of the identity (6) in Figure 1 or (6) in Figure 2.

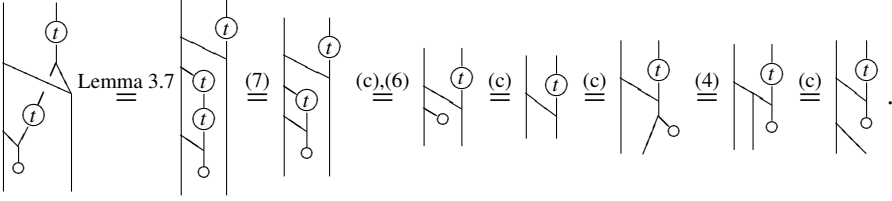
It now remains to show that these four morphisms are  $A$ -comodule morphisms, that is, that they are in  $\mathbf{Comod}(A)$ . Note that  $M \otimes_C C$  and  $C \otimes_C M$  are  $A$ -comodules via the coactions



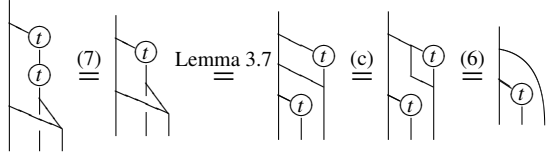
and

respectively. We then have these facts:

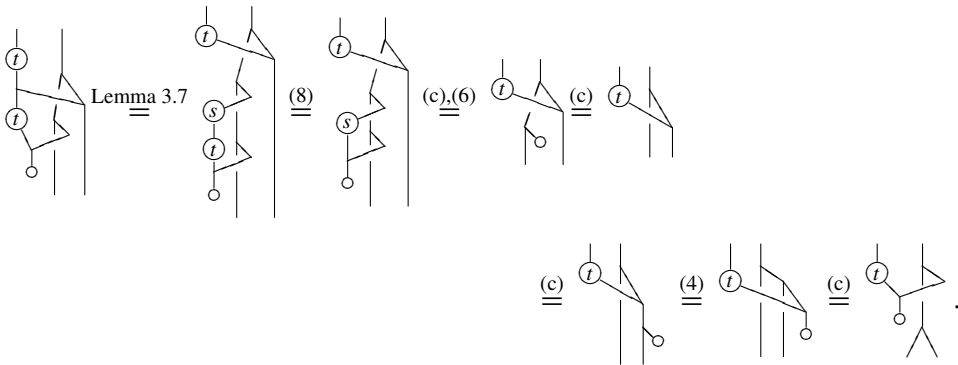
- $\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} : M \otimes_C C \rightarrow M$  is an  $A$ -comodule morphism since




- $\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} : M \rightarrow M \otimes_C C$  is an  $A$ -comodule morphism since



- $\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} : C \otimes_C M \rightarrow M$  is an  $A$ -comodule morphism since



-  :  $M \rightarrow C \otimes_C M$  is an  $A$ -comodule morphism since

$$\begin{array}{c}
 \begin{array}{c} \text{Diagram 1: } s \text{ followed by a triangle and a vertical line.} \\ \text{Diagram 2: } s \text{ followed by a triangle and a vertical line, with a circle labeled 't' below the triangle.} \\ \text{Diagram 3: } s \text{ followed by a triangle and a vertical line, with a circle labeled 't' below the triangle.} \\ \text{Diagram 4: } s \text{ followed by a triangle and a vertical line, with a circle labeled 't' below the triangle.} \end{array}
 \end{array}
 \begin{array}{l}
 \text{Lemma 3.7} \\
 \equiv \\
 \text{(8)} \\
 \equiv \\
 \text{(c),(6)} \\
 \equiv
 \end{array}
 \begin{array}{c}
 \text{Diagram 5: } s \text{ followed by a triangle and a vertical line.}
 \end{array}$$

Thus,  $M \otimes_C C \cong M \cong C \otimes_C M$  in  $\mathcal{V}$ . □

Thus,  $\mathbf{Comod}(A) = (\mathbf{Comod}(A), \otimes_C, C)$  is a monoidal category.

**3.5. The forgetful functor from  $A$ -comodules to  $C$ -bicomodules.** There is a forgetful functor  $U : \mathbf{Comod}(A) \rightarrow \mathbf{Bicomod}(C)$  that assigns to each  $A$ -comodule  $M$  a  $C$ -bicomodule  $UM$  that is  $M$  itself with coaction

$$\begin{array}{c}
 M \\
 | \\
 \begin{array}{c} \text{Diagram: A triangle with a circle labeled 's' on the left and a circle labeled 't' on the right. The triangle is labeled 'A' above it. Below the triangle are three vertical lines labeled 'C', 'M', and 'C' respectively.} \end{array}
 \end{array}$$

Obviously a morphism of  $A$ -comodules  $f : M \rightarrow N$  is automatically a morphism of the underlying  $C$ -bicomodules  $f : UM \rightarrow UN$ .

**Proposition 3.8.** *The forgetful functor  $U : \mathbf{Comod}(A) \rightarrow \mathbf{Bicomod}(C)$  is strong monoidal.*

*Proof.* We must establish the  $C$ -bicomodule isomorphisms

$$C \cong UC \quad \text{and} \quad UM \otimes_C UN \cong U(M \otimes_C N).$$

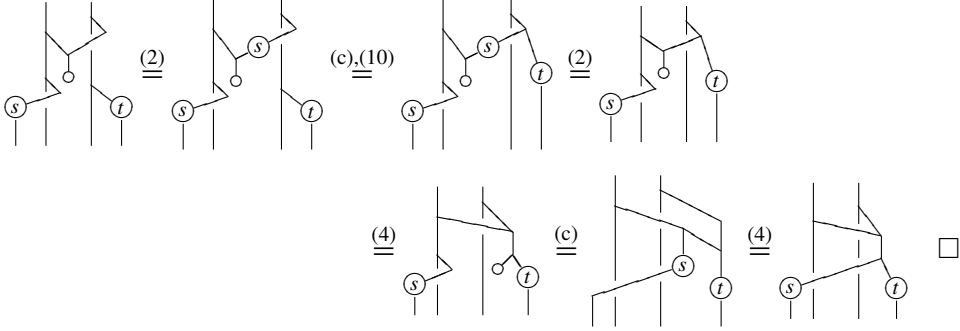
The first is obvious. To establish the second we observe that the object  $UM \otimes_C UN$  is  $(M \otimes_C N, m)$  with coaction

$$\begin{array}{c}
 \text{Diagram: A triangle with a circle labeled 's' on the left and a circle labeled 't' on the right. The triangle is labeled 'A' above it. Below the triangle are three vertical lines labeled 'C', 'M', and 'C' respectively.}
 \end{array}$$

and  $U(M \otimes_C N)$  is also  $(M \otimes_C N, m)$  but with coaction

$$\begin{array}{c}
 \text{Diagram: A triangle with a circle labeled 's' on the left and a circle labeled 't' on the right. The triangle is labeled 'A' above it. Below the triangle are three vertical lines labeled 'C', 'M', and 'C' respectively.}
 \end{array}$$

The following calculation shows that these two coactions are the same, and hence the isomorphism  $U(M \otimes_C N) \cong UM \otimes_C UN$ .



This may seem to be a strict equality, but as tensor products are really only defined up to isomorphism, we prefer “strong”.

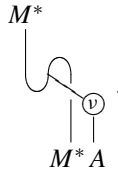
**3.6.  $\mathbf{Comod}_f(H)$  is left autonomous.** Let  $\mathcal{V}_f$  denote the subcategory of  $\mathcal{V}$  consisting of the objects with a left dual (since  $\mathcal{V}$  is braided, left duals are right duals), and suppose that  $H$  is a weak Hopf monoid. There is a forgetful functor  $U_l : \mathbf{Comod}(H) \rightarrow \mathcal{V}$  defined as the composite of the two forgetful functors  $\mathbf{Comod}(H) \rightarrow \mathbf{Bicomod}(C)$  and  $\mathbf{Bicomod}(C) \rightarrow \mathcal{V}$ . Sometimes this composite  $U_l : \mathbf{Comod}(H) \rightarrow \mathcal{V}$  is called the *long forgetful functor*, as opposed to the *short forgetful functor*  $U : \mathbf{Comod}(H) \rightarrow \mathbf{Bicomod}(C)$ .

Let us say an object  $M \in \mathbf{Comod}(H)$  is *dualizable* if  $U_l M$  has a left dual in  $\mathcal{V}$ , that is,  $U_l M \in \mathcal{V}_f$ . Denote by  $\mathbf{Comod}_f(H)$  the subcategory of  $\mathbf{Comod}(H)$  consisting of the dualizable objects.

The goal of this section is to prove the following proposition.

**Proposition 3.9.** *If  $H$  is a weak Hopf monoid, then the category  $\mathbf{Comod}_f(H)$  is left autonomous (= left compact = left rigid).*

Suppose  $M \in \mathbf{Comod}_f(H)$  has a left dual  $M^*$  in  $\mathcal{V}$ . Using the antipode of  $H$ , a coaction on  $M^*$  is defined as



By (17) it is easy to see that this defines a comodule structure on  $M^*$ . We claim that  $M^*$  is the left dual of  $M$  in  $\mathbf{Comod}_f(H)$ . Define morphisms  $e : M^* \otimes_C M \rightarrow C$

and  $n : C \rightarrow M \otimes_C M^*$  via

$$e = \text{diagram} \quad \text{and} \quad n = \text{diagram}.$$

**Proposition 3.10.** *Suppose  $M \in \mathbf{Comod}_f(H)$  with underlying left dual  $M^*$ . Then  $M^*$  with evaluation and coevaluation morphisms  $e$  and  $n$  respectively is the left dual of  $M$  in  $\mathbf{Comod}_f(H)$ . That is,  $\mathbf{Comod}_f(H)$  is left autonomous.*

*Proof.* Let  $M$ ,  $M^*$ ,  $e$ , and  $n$  be as above. We will first show that  $e$  and  $n$  are comodule morphisms, and secondly that they satisfy the triangle identities.

The following calculation shows that  $e$  is a comodule morphism.

$$\text{diagram} \stackrel{\text{tri}}{=} \text{diagram} \stackrel{(c)}{=} \text{diagram} \stackrel{(4)}{=} \text{diagram} \stackrel{v}{=} \text{diagram} \stackrel{(3),(7)}{=} \text{diagram}$$

To show that  $n$  is a comodule morphism, we must establish the equality

$$\text{diagram} = \text{diagram},$$

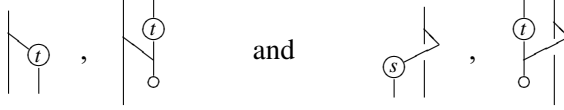
which is proved by the calculation

$$\begin{aligned} \text{diagram} &\stackrel{\text{tri}}{=} \text{diagram} \stackrel{v, (c)}{=} \text{diagram} \stackrel{(17)}{=} \text{diagram} \\ &\stackrel{(b)}{=} \text{diagram} \stackrel{v}{=} \text{diagram} \stackrel{(4)}{=} \text{diagram} \stackrel{(4)}{=} \text{diagram} \stackrel{(4)}{=} \text{diagram}. \end{aligned}$$

It remains to show that  $e$  and  $n$  satisfy the triangle identities, that is, that the following composites are the identity:

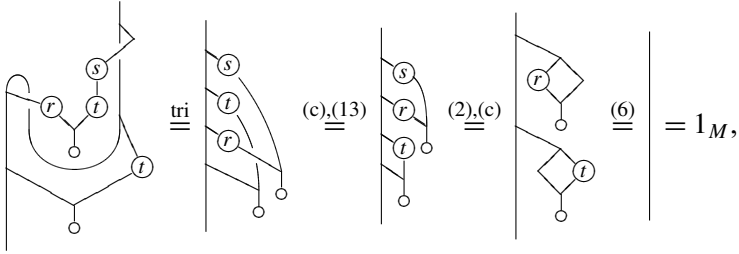
- (i)  $M \cong C \otimes_C M \xrightarrow{n \otimes 1} M \otimes_C M^* \otimes_C M \xrightarrow{1 \otimes e} M \otimes_C C \cong M$  ;
- (ii)  $M^* \cong M^* \otimes_C C \xrightarrow{1 \otimes n} M^* \otimes_C M \otimes_C M^* \xrightarrow{e \otimes 1} C \otimes_C M^* \cong M^*$  .

Recall that  $M \cong M \otimes_C C$  and  $M \cong C \otimes_C M$  via

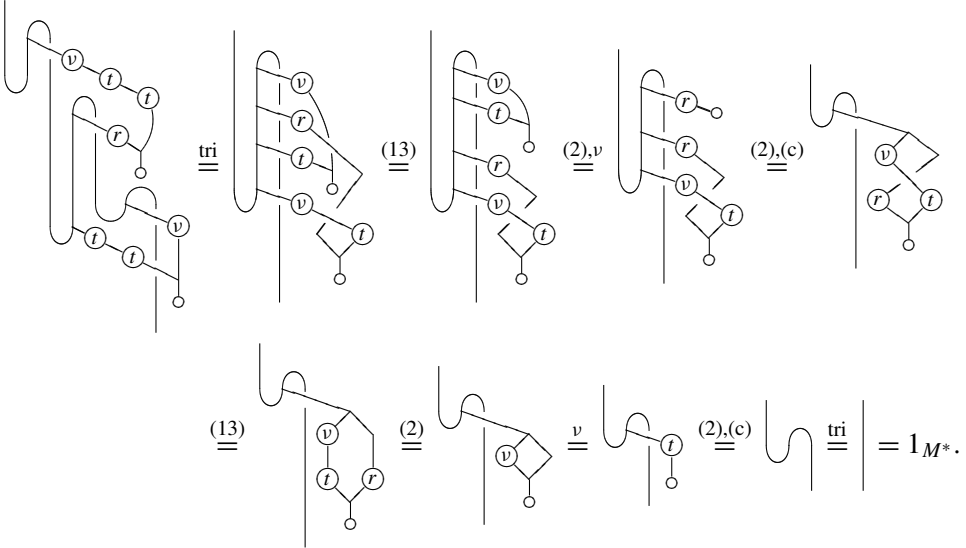


respectively.

The calculation



proves (i), and (ii) is given by



This completes the proof that  $M^*$  is the left dual of  $M$  in  $\mathbf{Comod}_f(H)$ , and hence that  $\mathbf{Comod}_f(H)$  is left autonomous.  $\square$



Let  $R$  be a separable Frobenius monoid in  $\mathcal{V}$ . In this section we prove that  $R \otimes R$  is an example of a weak Hopf monoid with an invertible antipode. In the case  $\mathcal{V} = \mathbf{Vect}$ , this example is essentially the same as in [Böhm et al. 1999, Appendix].

$$\delta = \text{[diagram of a pair of pants]} \quad \text{and} \quad \epsilon = \cup.$$
$$\begin{array}{c} \circ \\ \diagup \quad \diagdown \end{array} = \cap \quad \text{and} \quad \begin{array}{c} \diagup \quad \diagdown \\ \circ \end{array} = \cup,$$
$$\mu = \text{[diagram: a vertex with two incoming lines from the left and two outgoing lines to the right, one solid and one dashed]} \quad \text{and} \quad \eta = \text{[diagram: two separate vertices, each with one incoming line from the left and one outgoing line to the right, both solid]}.$$

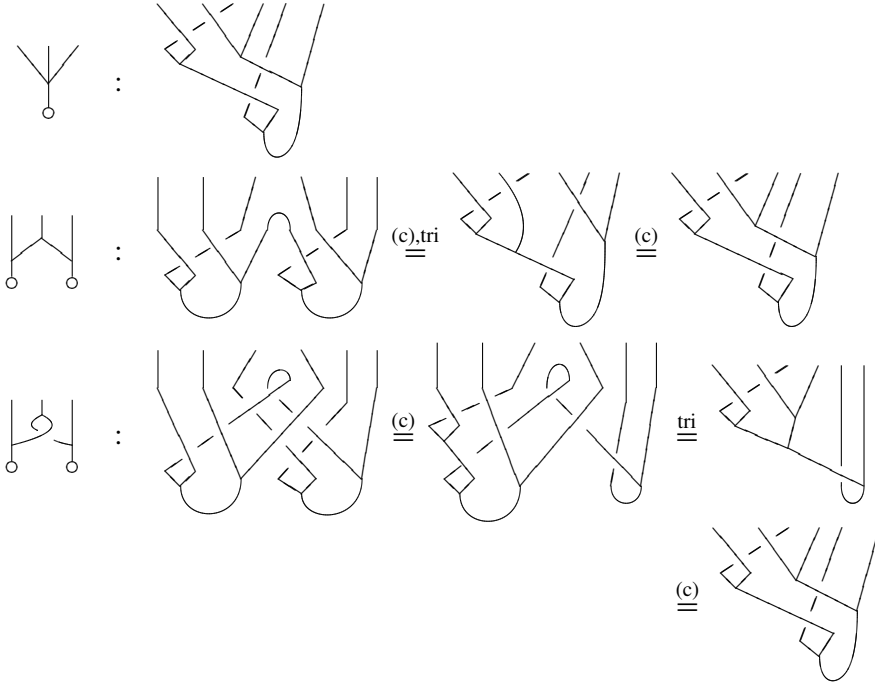
**Proposition 4.1.** *If  $R$  is separable, meaning  $\mu\delta = 1_R$ , then  $R \otimes R$  is a weak bi-monoid. An invertible antipode  $\nu$  on  $R \otimes R$  is given by*

$$v = \text{[diagram of a vertex with two incoming lines and one outgoing line]},$$

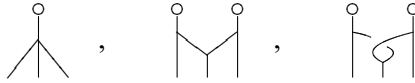
The next three sets of calculations establish the axioms (b), (v), and (w), and hence the first claim.

$$(\mu \otimes \mu)(1 \otimes c \otimes 1)(\delta \otimes \delta) = \text{nat} = \text{sep} = \delta\mu.$$

Axiom (v) is seen from the diagrams



For (w), by the naturality of the braiding and the counit property of  $R$ , each equation in (w), that is,



is easily seen to be equal to the diagram



Thus,  $R \otimes R$  is a weak bimonoid. We next prove that  $R \otimes R$  is a weak Hopf monoid with invertible antipode

$$\nu = \text{diagram of a crossing with a loop on the left strand}.$$

An inverse to  $\nu$  is easily seen to be given by

$$\nu^{-1} = \text{diagram of a crossing with a loop on the right strand}.$$

and so the antipode is invertible. We note that (in simplified form)

$$r = \text{diagram} \quad \text{and} \quad t = \text{diagram}.$$

The following calculations then prove the antipode axioms.

$$\mu(v \otimes 1)\delta = \text{diagram} \stackrel{\text{tri}}{=} \text{diagram} \stackrel{\text{sep}}{=} \text{diagram} = t$$

$$\mu(1 \otimes v)\delta = \text{diagram} \stackrel{\text{nat}}{=} \text{diagram} \stackrel{\text{sep}}{=} \text{diagram} = r$$

$$\mu_3(v \otimes 1 \otimes v)\delta_3 = \text{diagram} \stackrel{\text{sep}}{=} \text{diagram} \stackrel{\text{sep}}{=} \text{diagram} \stackrel{(c)}{=} \text{diagram} = v$$

Thus,  $R \otimes R$  is a weak Hopf monoid with invertible antipode.

## 5. Quantum groupoids

In this section we recall the quantum categories and quantum groupoids of Day and Street [2004], where there is a succinct definition on [page 216] in terms of “basic data” and “Hopf basic data”. Here we give the unpacked definition of quantum category and quantum groupoid which is essentially found in [page 221]; however, we do make a correction.

Our setting is a braided monoidal category  $\mathcal{V} = (\mathcal{V}, \otimes, I, c)$  in which the functors

$$A \otimes - : \mathcal{V} \rightarrow \mathcal{V}$$

with  $A \in \mathcal{V}$ , preserve coreflexive equalizers, that is, equalizers of pairs of morphisms with a common left inverse.

**5.1. Quantum categories.** Suppose  $A$  and  $C$  are comonoids in  $\mathcal{V}$  and  $s : A \rightarrow C^\circ$  and  $t : A \rightarrow C$  are comonoid morphisms such that the diagram

$$\begin{array}{ccc} & A \otimes A & \xrightarrow{s \otimes t} C \otimes C \\ & \delta \nearrow & \downarrow c \\ A & & \\ & \delta \searrow & \\ & A \otimes A & \xrightarrow{t \otimes s} C \otimes C \end{array}$$

commutes. Then  $A$  may be viewed as a  $C$ -bicomodule with left and right coactions defined respectively via

$$\begin{aligned} \gamma_l &= (A \xrightarrow{\delta} A \otimes A \xrightarrow{1 \otimes s} A \otimes C \xrightarrow{c^{-1}} C \otimes A), \\ \gamma_r &= (A \xrightarrow{\delta} A \otimes A \xrightarrow{1 \otimes t} A \otimes C). \end{aligned}$$

Recall that the tensor product  $P = A \otimes_C A$  of  $A$  with itself over  $C$  is defined as the equalizer

$$P \xrightarrow{\iota} A \otimes A \xrightarrow[1 \otimes \gamma_l]{\gamma_r \otimes 1} A \otimes C \otimes A.$$

The diagrams

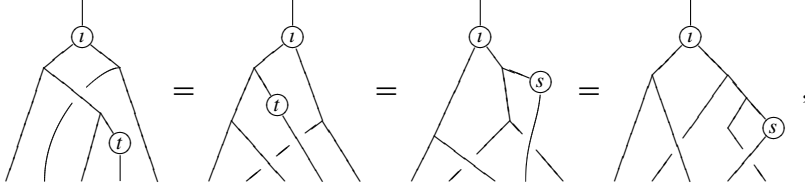
$$\begin{aligned} P &\xrightarrow{\iota} A \otimes A \xrightarrow{\gamma_l \otimes 1} C \otimes A \otimes A \xrightarrow[1 \otimes 1 \otimes \gamma_l]{1 \otimes \gamma_r \otimes 1} C \otimes A \otimes C \otimes A, \\ P &\xrightarrow{\iota} A \otimes A \xrightarrow{1 \otimes \gamma_r} A \otimes A \otimes C \xrightarrow[1 \otimes \gamma_l \otimes 1]{\gamma_r \otimes 1 \otimes 1} A \otimes C \otimes A \otimes C \end{aligned}$$

may be seen to commute and therefore induce respectively a left  $C$ - and right  $C$ -coaction on  $P$ . These coactions make  $P$  into a  $C$ -bicomodule.

The commutativity of the diagram

$$P \xrightarrow{\iota} A \otimes A \xrightarrow{\delta \otimes \delta} A^{\otimes 4} \xrightarrow{1 \otimes c \otimes 1} A^{\otimes 4} \xrightarrow[1 \otimes 1 \otimes 1 \otimes \gamma_l]{1 \otimes 1 \otimes \gamma_r \otimes 1} A \otimes A \otimes A \otimes C \otimes A$$

may be seen from



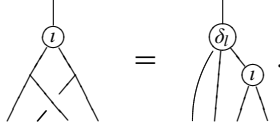
and since  $1 \otimes 1 \otimes \iota$  is the equalizer of  $1 \otimes 1 \otimes \gamma_r \otimes 1$  and  $1 \otimes 1 \otimes 1 \otimes \gamma_l$ , there is a unique morphism

$$\delta_l : P \rightarrow A \otimes A \otimes P$$

making the diagram

$$\begin{array}{ccc} P & \xrightarrow{\iota} & A \otimes A \xrightarrow{\delta \otimes \delta} A \otimes A \otimes A \otimes A \\ \delta_l \downarrow & & \downarrow 1 \otimes c \otimes 1 \\ A \otimes A \otimes P & \xrightarrow{1 \otimes 1 \otimes \iota} & A \otimes A \otimes A \otimes A \end{array}$$

commute. In strings,



It is easy to see (postcompose with the monomorphism  $1 \otimes 1 \otimes 1 \otimes 1 \otimes \iota$ ) that the morphism  $\delta_l$  is the left coaction of the comonoid  $A \otimes A$  on  $P$  that makes  $P$  into a (left)  $A \otimes A$ -comodule. This means that the diagrams

$$\begin{array}{ccc} P & \xrightarrow{\delta_l} & A \otimes A \otimes P \\ \delta_l \downarrow & & \downarrow 1 \otimes 1 \otimes \delta_l \\ A \otimes A \otimes P & & \\ \delta \otimes \delta \otimes 1 \downarrow & & \downarrow 1 \otimes c \otimes 1 \otimes 1 \\ A \otimes A \otimes A \otimes A \otimes P & \xrightarrow{1 \otimes c \otimes 1 \otimes 1} & A \otimes A \otimes A \otimes A \otimes P \end{array} \quad \begin{array}{ccc} P & \xrightarrow{\delta_l} & A \otimes A \otimes P \\ & \searrow 1 & \downarrow \epsilon \otimes \epsilon \otimes 1 \\ & & P \end{array}$$

commute.

**5.2. The definition.** We are now ready to state the definition. A *quantum category* in  $\mathcal{V}$  consists of the data  $\mathbf{A} = (A, C, s, t, \mu, \eta)$  where  $A, C, s, t$  are as above, and  $\mu : P = A \otimes_C A \rightarrow A$  and  $\eta : C \rightarrow A$  are morphisms in  $\mathcal{V}$ , called the *composition morphism* and *unit morphism*, respectively. This data must satisfy axioms (B1) through (B6) below.

(B1)  $(A, \mu, \eta)$  is a monoid in  $\mathbf{Bicomod}(C)$ .

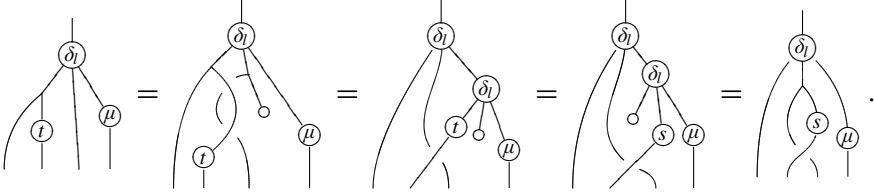
(B2) The following diagram commutes.

$$P \xrightarrow{\delta_l} A \otimes A \otimes P \xrightarrow[\epsilon \otimes s \otimes 1]{t \otimes \epsilon \otimes 1} C \otimes P \xrightarrow{1 \otimes \mu} C \otimes A$$

Before stating (B3), we use (B2) to show that the diagram

$$P \xrightarrow{\delta_l} A \otimes A \otimes P \xrightarrow{1 \otimes 1 \otimes \mu} A \otimes A \otimes A \xrightarrow[1 \otimes \gamma_l \otimes 1]{\gamma_r \otimes 1 \otimes 1} A \otimes C \otimes A \otimes A$$

commutes, as seen by the calculation



Since  $\iota \otimes 1$  is the equalizer of  $\gamma_r \otimes 1 \otimes 1$  and  $1 \otimes \gamma_l \otimes 1$ , there is a unique morphism  $\delta_r : P \rightarrow P \otimes A$  making the square

$$\begin{array}{ccc} P & \xrightarrow{\delta_l} & A \otimes A \otimes P \\ \delta_r \downarrow & & \downarrow 1 \otimes 1 \otimes \mu \\ P \otimes A & \xrightarrow{\iota \otimes 1} & A \otimes A \otimes A \end{array}$$

commute. We can now state (B3).

(B3) The following diagram commutes.

$$\begin{array}{ccc} P & \xrightarrow{\mu} & A \\ \delta_r \downarrow & & \downarrow \delta \\ P \otimes A & \xrightarrow{\mu \otimes 1} & A \otimes A \end{array}$$

(B4) The following diagram commutes.

$$\begin{array}{ccc} P & \xrightarrow{\mu} & A \\ \iota \downarrow & & \downarrow \epsilon \\ A \otimes A & \xrightarrow{\epsilon \otimes \epsilon} & I \end{array}$$

(B5) The following diagram commutes.

$$\begin{array}{ccc} C & & \\ \eta \downarrow & \searrow \epsilon & \\ A & \xrightarrow{\epsilon} & I \end{array}$$

(B6) The following diagram commutes.

$$\begin{array}{ccccc}
 & & A & \xrightarrow{\delta} & A \otimes A & \xrightarrow{s \otimes 1} & C \otimes A & & \\
 & \nearrow \eta & & & & & & \searrow \eta \otimes 1 & \\
 C & \xrightarrow{\eta} & A & \xrightarrow{\delta} & A \otimes A & & & & A \otimes A \\
 & \searrow \eta & & & & & & \nearrow \eta \otimes 1 & \\
 & & A & \xrightarrow{\delta} & A \otimes A & \xrightarrow{t \otimes 1} & C \otimes A & & 
 \end{array}$$

A consequence of these axioms is that  $P$  becomes a left  $A \otimes A$ -, right  $A$ -bicomodule.

The axiom (B6) makes  $C$  into a right  $A$ -comodule via

$$C \xrightarrow{\eta} A \xrightarrow{\delta} A \otimes A \xrightarrow{s \otimes 1} C \otimes A .$$

We refer to  $A$  as the *object-of-arrows* and  $C$  as the *object-of-objects*.

**5.3. Quantum groupoids.** Suppose we have comonoid isomorphisms

$$v : C^\circ \xrightarrow{\cong} C \quad \text{and} \quad v : A^\circ \xrightarrow{\cong} A .$$

Denote by  $P_l$  the left  $A^{\otimes 3}$ -comodule  $P$  with coaction defined by

$$P \xrightarrow{\delta} A \otimes A \otimes P \otimes A \xrightarrow{1 \otimes 1 \otimes 1 \otimes v} A \otimes A \otimes P \otimes A \xrightarrow{1 \otimes 1 \otimes c_{P,A}} A \otimes A \otimes A \otimes P ,$$

and by  $P_r$  the left  $A^{\otimes 3}$ -comodule  $P$  with coaction defined by

$$P \xrightarrow{\delta} A \otimes A \otimes P \otimes A \xrightarrow{1 \otimes 1 \otimes 1 \otimes v^{-1}} A \otimes A \otimes P \otimes A \xrightarrow{c_{A \otimes A \otimes P, A}^{-1}} A \otimes A \otimes A \otimes P .$$

Furthermore, suppose that  $\theta : P_l \rightarrow P_r$  is a left  $A^{\otimes 3}$ -comodule isomorphism. We define a *quantum groupoid* in  $\mathcal{V}$  to be a quantum category  $\mathbf{A}$  in  $\mathcal{V}$  equipped with an  $v$ ,  $\nu$ , and  $\theta$  satisfying (G1) through (G3) below.

(G1)  $sv = t$ ,

(G2)  $t\nu = \nu s$ , and

(G3) the diagram<sup>3</sup>

$$\begin{array}{ccc}
 P & \xrightarrow{\varsigma} & C \otimes C \otimes C & \xrightarrow{c_{C,C \otimes C}} & C \otimes C \otimes C \\
 \theta \downarrow & & & & \downarrow 1 \otimes 1 \otimes v \\
 P & \xrightarrow{\varsigma} & C \otimes C \otimes C & & 
 \end{array}$$

<sup>3</sup>This corrects [Day and Street 2004, Section 12, page 223].

commutes, where the morphism  $\varsigma : P \rightarrow C^{\otimes 3}$  is defined by taking either of the equal routes

$$P \xrightarrow{t} A \otimes A \xrightleftharpoons[1 \otimes \gamma_l]{\gamma_r \otimes 1} A \otimes C \otimes A \xrightarrow{s \otimes 1 \otimes t} C^{\otimes 3}.$$

## 6. Weak Hopf monoids and quantum groupoids

The goal of this section is to prove the following theorem.

**Theorem 6.1.** *There is a bijection in  $\mathbb{Q}\mathcal{V}$  between weak bimonoids and quantum categories with separable Frobenius object-of-objects. Also, if the weak bimonoid is equipped with an invertible antipode, making it a weak Hopf monoid, then the quantum category becomes a quantum groupoid.*

In the case  $\mathcal{V} = \mathbf{Vect}$ , it has been shown in [Brzeziński and Militaru 2002, Proposition 5.2] that a weak Hopf monoid with invertible antipode yields a quantum groupoid.

Concerning the converse, we would like to warmly thank Gabriella Böhm for not only suggesting that it may be true, and pointing out that the  $\mathcal{V} = \mathbf{Vect}$  case appears in the PhD thesis of Imre Bálint [2008a], but for also helping us with the proof.

The theorem has an obvious corollary.

**Corollary 6.2.** *Any Frobenius monoid in  $\mathcal{V}$  yields a quantum groupoid in  $\mathcal{V}$ .*

*Proof.* By Proposition 4.1, every Frobenius monoid  $R$  in  $\mathcal{V}$  leads to a weak Hopf monoid with invertible antipode  $R \otimes R$ . Apply Theorem 6.1 to this weak Hopf monoid with invertible antipode to get a quantum groupoid in  $\mathcal{V}$ .  $\square$

Now let us discuss the necessary data for the theorem. The proof involves many string calculations, which may be found in Sections 6.1 and 6.2.

Suppose  $A = (A, 1)$  is a weak bimonoid in  $\mathcal{V}$  with source morphism  $s$  and target morphism  $t$ , and put  $C = (A, t)$ . Our claim is that this data along with

$$\mu = \begin{array}{c} \diagup \quad \diagdown \\ | \end{array} : P \rightarrow A, \quad \eta = t : C \rightarrow A$$

forms a quantum category in  $\mathcal{V}$ . If moreover  $A$  is a weak Hopf monoid in  $\mathcal{V}$  with an invertible antipode  $\nu : A \rightarrow A$ , then setting

$$v = t\nu\nu t : C^{\circ\circ} \rightarrow C, \quad \nu = \nu : A^{\circ} \rightarrow A, \quad \theta = \begin{array}{c} \diagup \quad \diagdown \\ | \quad \bigcirc \nu \end{array} : P \rightarrow P.$$

yields a quantum groupoid in  $\mathcal{V}$ . The details will be proved in Section 6.1.



For the other direction, recall from Section 3.1 that, if  $C$  is a separable Frobenius monoid and  $M$  and  $N$  are  $C$ -comodules, we may form  $M \otimes_C N$ , the tensor product over  $C$  of  $M$  and  $N$ . Moreover, the tensor product over  $C$  is a retract of the tensor product in  $\mathcal{V}$  so that

$$M \otimes_C N \xrightarrow{\iota} M \otimes N$$

has a retraction  $m : M \otimes N \rightarrow M \otimes_C N$ . Again, from Section 3.1, we see that we may explicitly write  $\iota m$  as

$$\iota m = (M \otimes N \xrightarrow{\delta_r \otimes \delta_l} M \otimes C \otimes C \otimes N \xrightarrow{1 \otimes \mu \otimes 1} M \otimes C \otimes N \xrightarrow{1 \otimes \epsilon \otimes 1} M \otimes N).$$

Graphically,

$$\begin{array}{c} M \quad N \\ \diagdown \quad \diagup \\ \textcircled{m} \\ \diagup \quad \diagdown \\ M \otimes_C N \\ \diagdown \quad \diagup \\ \textcircled{\iota} \\ \diagup \quad \diagdown \\ M \quad N \end{array} = \begin{array}{c} M \quad N \\ \diagdown \quad \diagup \\ C \quad C \\ \diagup \quad \diagdown \\ M \quad N \end{array} \quad \text{and} \quad \begin{array}{c} M \otimes_C N \\ \textcircled{\iota} \\ M \quad N \\ \textcircled{m} \end{array} = \begin{array}{c} M \otimes_C N \\ | \end{array}. \quad (@)$$

Now suppose  $\mathbf{A} = (A, C, s, t, \mu, \eta)$  is a quantum category in  $\mathcal{V}$ , in which  $C = (C, \mu, \eta, \delta, \epsilon)$  is a separable Frobenius monoid. The comonoid  $A$  is therefore a  $C$ -bicomodule, so that  $\iota : P \rightarrow A \otimes A$  has a retraction  $m : A \otimes A \rightarrow P$ . This is such that

$$\iota m = \begin{array}{c} \diagup \quad \diagdown \\ \textcircled{\iota} \quad \textcircled{s} \\ \diagdown \quad \diagup \\ \textcircled{m} \end{array} \quad \text{and} \quad m \iota = 1_P.$$

If we then define a multiplication and unit for  $A$  as

$$\mu = (A \otimes A \xrightarrow{m} P \xrightarrow{\mu} A), \quad \eta = (I \xrightarrow{\eta} C \xrightarrow{\eta} A),$$

where  $\eta : I \rightarrow C$  comes from the fact that  $C$  is a Frobenius module, then we have the data for a weak bimonoid  $A$ . That this is actually a weak bimonoid will be proved in Section 6.2.

Let us see that this correspondence between weak bimonoids and quantum categories with separable Frobenius object-of-objects is one-to-one. Suppose we have a weak bimonoid  $A = (A, \mu, \eta, \delta, \epsilon)$  in  $\mathcal{V}$ . It becomes a quantum category in  $\mathcal{V}$  by setting

$$C := (A, t), \quad s := s, \quad t := t, \quad \eta := t, \quad \text{and} \quad \mu := \mu.$$

This quantum category then becomes a weak bimonoid by setting

$$\mu := \mu \circ m \quad \text{and} \quad \eta := t \circ \eta$$

where, in this case,

$$m = \begin{array}{c} \text{---} \circlearrowleft \text{---} \circlearrowright \text{---} \\ | \quad | \\ \text{---} \circ \text{---} \end{array} \stackrel{(2)}{=} \begin{array}{c} \text{---} \text{---} \text{---} \\ | \quad | \\ \text{---} \circ \text{---} \end{array}$$

and, as we see from the first paragraph of Section 6.1,  $\mu \circ m = \mu$ , and moreover, the morphism  $t \circ \eta = \eta$  by axiom (2) for weak bimonoids. Thus, we have ended up with the weak bimonoid  $A$  that we started with.

Let us now go in the other direction. Suppose that we have a quantum category  $\mathbf{A} = (A, C, s, t, \mu, \eta)$  with  $(A, \delta, \epsilon)$  a comonoid, and  $C = (C, \mu_C, \eta_C, \delta_C, \epsilon_C)$  a separable Frobenius monoid. Then  $A$  becomes a weak bimonoid with

$$\mu' := \mu \circ m, \quad \text{where } m : A \otimes A \rightarrow P, \quad \text{and} \quad \eta' := \eta \circ \eta_C.$$

We note that the source and target morphisms for the weak bimonoid are given by

$$s' := \eta \circ s \quad \text{and} \quad t' := \eta \circ t.$$

First, we observe that  $C \cong (A, t)$  and  $P \cong (A \otimes A, \iota m)$  respectively via

$$(A, t') \xrightarrow[t]{} (C, 1) \quad \text{and} \quad (P, 1) \xleftarrow[m]{} (A \otimes A, \iota m).$$

The first isomorphism is established in one direction by definition and in the other by

$$\begin{aligned} t\eta &= (1 \otimes t)(\epsilon \otimes 1)\delta\eta \\ &= (\epsilon \otimes 1)(\eta \otimes 1)\delta_C && \text{since } \eta \text{ is a } C\text{-comodule morphism} \\ &= (\epsilon_C \otimes 1)\delta_C && \text{by (B5)} \\ &= 1_C. \end{aligned}$$

The second isomorphism is again established in one direction by definition and in the other by the fact that  $m$  is a retract of  $\iota$ . This weak bimonoid becomes a quantum category by stripping off the  $m$  from  $\mu'$  so that we are left with the original  $\mu$ . Since  $t'$  is a morphism from  $(A, t)$  to  $(A, 1)$ , if we wish to consider it as a morphism from  $C$  to  $A$ , we must precompose with  $\eta : (C, 1) \rightarrow (A, t)$ . This gives  $t' \circ \eta = \eta \circ t \circ \eta = \eta$ , and so we are left with the original  $\eta$ . We have already seen that  $C \cong (A, t)$ , so we are left with our original quantum category.

This establishes the bijection one-to-one correspondence between quantum categories and weak bimonoids, and moreover shows how to construct a quantum groupoid from a weak Hopf monoid.

The remainder of this section is devoted to proving the details of the theorem.

**6.1. Weak bimonoids yield quantum categories.** In this section, we prove that a weak bimonoid in  $\mathcal{QV}$  yields a quantum category in  $\mathcal{QV}$ . Suppose that  $A = (A, 1)$  is a weak bimonoid with source and target morphisms  $s$  and  $t$ , respectively. Set  $C = (A, t)$  as usual. The morphisms  $s$  and  $t$  are obviously in  $\mathcal{QV}$ , hence so is  $\eta = t$ , and

$$\begin{array}{c} \text{Diagram 1} \end{array} \stackrel{\text{nat}}{=} \begin{array}{c} \text{Diagram 2} \end{array} \stackrel{\text{(b)}}{=} \begin{array}{c} \text{Diagram 3} \end{array} = \mu$$

shows that  $\mu$  is as well. Recall that

$$P = (A \otimes A, \begin{array}{c} \text{Diagram 4} \end{array}).$$

The morphisms  $\delta_l : P \rightarrow A \otimes A \otimes P$  and  $\delta_r : P \rightarrow P \otimes A$  are given by

$$\delta_l = \begin{array}{c} \text{Diagram 5} \end{array} \quad \text{and} \quad \delta_r = \begin{array}{c} \text{Diagram 6} \end{array}.$$

The two calculations

$$\begin{array}{c} \text{Diagram 7} \end{array} \stackrel{\text{(c)}}{=} \begin{array}{c} \text{Diagram 8} \end{array} = \begin{array}{c} \text{Diagram 9} \end{array}$$

and

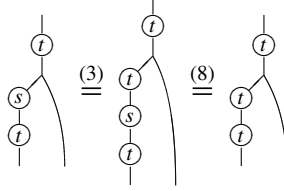
$$\begin{array}{c} \text{Diagram 10} \end{array} \stackrel{\text{(c)}}{=} \begin{array}{c} \text{Diagram 11} \end{array} \stackrel{\text{(b)}}{=} \begin{array}{c} \text{Diagram 12} \end{array}$$

show that these are morphisms in  $\mathcal{QV}$ .

To see that  $(A, \mu, \eta)$  is a comonoid in  $\mathbf{Bicomod}(C)$ , notice that associativity follows from that of  $\mu$  viewed as a weak bimonoid, and the counit property may be seen from property (6), that is,

$$\mu(1 \otimes t)\delta = 1_A \quad \text{and} \quad \mu(s \otimes 1)c^{-1}\delta = 1_A,$$

and so (B1) holds. (B2) follows from one application of (12), (B3) follows from (b), (B4) from (c), and (B5) follows from (2). The calculation

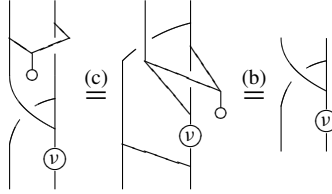


verifies (B6). Thus,  $\mathbf{A} = (A, C, s, t, \mu, \eta)$  is a quantum category in  $\mathcal{QV}$ .

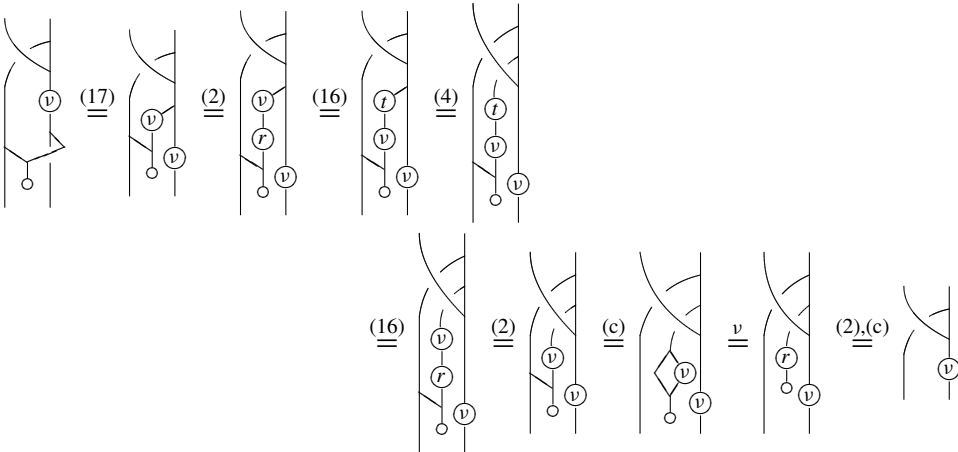
We now wish to show that a weak Hopf monoid with invertible antipode yields a quantum groupoid. So suppose that our weak bimonoid  $A$  is equipped with an invertible antipode  $\nu : A \rightarrow A$ , and set

$$v = tvvt : C^{\circ\circ} \rightarrow C, \quad \nu = \nu : A^\circ \rightarrow A, \quad \theta = \begin{array}{c} \diagup \\ \diagdown \\ \bigcirc \nu \end{array} : P \rightarrow P.$$

The morphisms  $v$  and  $\nu$  are obviously morphisms in  $\mathcal{QV}$ , and the two calculations



and



show that  $\theta$  is as well.

**Lemma 6.3.** *An inverse for  $\theta$  is given by*

$$\theta^{-1} = \text{diagram},$$

*Proof.* Since

$$\text{diagram} \stackrel{(c)}{=} \text{diagram} \stackrel{(b)}{=} \text{diagram},$$

it is clear that  $\theta^{-1}$  is a morphism in  $\mathcal{V}$ . That  $\theta^{-1}$  is an inverse for  $\theta$  may be seen in one direction from

$$\begin{aligned} \theta^{-1}\theta &= \text{diagram} \stackrel{(17)}{=} \text{diagram} = \text{diagram} \stackrel{(c)}{=} \text{diagram} \\ &\stackrel{(\dagger)}{=} \text{diagram} \stackrel{(4)}{=} \text{diagram} \stackrel{(2)}{=} \text{diagram} \\ &= 1_P, \end{aligned}$$

where  $(\dagger)$  is given by

$$\text{diagram} = \text{diagram} \stackrel{(17)}{=} \text{diagram} \stackrel{v}{=} \text{diagram} \stackrel{(15)}{=} \text{diagram},$$

and in the other direction by

$$\begin{aligned}
 \theta\theta^{-1} &= \text{diagram 1} \stackrel{(\ddagger)}{=} \text{diagram 2} \stackrel{(c)}{=} \text{diagram 3} \stackrel{(17)}{=} \text{diagram 4} \\
 &= \text{diagram 5} \stackrel{(c), v}{=} \text{diagram 6} \stackrel{(4)}{=} \text{diagram 7} \stackrel{(2)}{=} \text{diagram 8} = 1_P,
 \end{aligned}$$

for which the first step  $(\ddagger)$  holds because  $\theta$  is a morphism in  $\mathcal{QV}$ . □

That the antipode  $v : A^\circ \rightarrow A$  is a comonoid isomorphism is our assumption. That  $v : C^{\circ\circ} \rightarrow C$  is as well may be seen from the calculation

$$\begin{aligned}
 (t \otimes t)\delta v &= (t \otimes t)\delta t v v t \\
 &= (t \otimes t)\delta v v t && \text{by (3)} \\
 &= (t \otimes t)c(v \otimes v)\delta v t && \text{by (17)} \\
 &= (t \otimes t)c(v \otimes v)c(v \otimes v)\delta t && \text{by (17)} \\
 &= (t \otimes t)(v \otimes v)(v \otimes v)cc\delta t && \text{by nat} \\
 &= (t \otimes t)(t \otimes t)(v \otimes v)(v \otimes v)cc\delta t && \text{by (7)} \\
 &= (t \otimes t)(v \otimes v)(r \otimes r)(v \otimes v)cc\delta t && \text{by (16)} \\
 &= (t \otimes t)(v \otimes v)(v \otimes v)(t \otimes t)cc\delta t && \text{by (16)} \\
 &= (t \otimes t)(v \otimes v)(v \otimes v)(t \otimes t)cc\delta && \text{by (5)} \\
 &= (v \otimes v)cc\delta && \text{by (5).}
 \end{aligned}$$

An inverse for  $v$  is given by the morphism  $v^{-1} = tv^{-1}v^{-1}t$ , as may be seen in one direction by the calculation

$$\begin{aligned}
 v^{-1}v &= tv^{-1}v^{-1}ttvvt \\
 &= ttv^{-1}v^{-1}vvtt && \text{by (16)} \\
 &= tv^{-1}v^{-1}vv t && \text{by (7)} \\
 &= tt \\
 &= t = 1_C && \text{by (7).}
 \end{aligned}$$

The other direction is similar.

Recall that the left  $A \otimes A$ -, right  $A$ -coaction  $\delta$  on  $P$  is defined by taking the diagonal of the commutative square

$$\begin{array}{ccc} P & \xrightarrow{\delta_l} & A \otimes A \otimes P \\ \delta_r \downarrow & & \downarrow 1 \otimes 1 \otimes \delta_r \\ P \otimes A & \xrightarrow{\delta_l \otimes 1} & A \otimes A \otimes P \otimes A. \end{array}$$

We note that  $\delta$  may be written as

We must show that  $\theta$  is a left  $A^{\otimes 3}$ -comodule isomorphism  $P_l \rightarrow P_r$ . That is, we must prove the commutativity of the square

$$\begin{array}{ccc} P_l & \xrightarrow{\gamma} & A^{\otimes 3} \otimes P_l \\ \theta \downarrow & & \downarrow 1 \otimes \theta \\ P_r & \xrightarrow{\gamma} & A^{\otimes 3} \otimes P_r, \end{array}$$

where the left  $A^{\otimes 3}$ -coactions on  $P_l$  and  $P_r$  were defined using  $\delta$  (see Section 5.3). The clockwise direction around the square is

where the last step (§) is given by the calculation

The counterclockwise direction is

Thus,  $\theta$  is a left  $A^{\otimes 3}$ -comodule morphism  $P_l \rightarrow P_r$ . The inverse of  $\theta$  then is a left  $A^{\otimes 3}$ -comodule morphism  $P_r \rightarrow P_l$ .

We now prove the properties (G1) through (G3) required of a quantum groupoid. The calculation



verifies (G1), and (G2) is established by

$$\begin{array}{c} \textcircled{v} \\ | \\ \textcircled{t} \end{array} \stackrel{(7)}{=} \begin{array}{c} \textcircled{v} \\ | \\ \textcircled{t} \\ | \\ \textcircled{t} \end{array} \stackrel{(16)}{=} \begin{array}{c} \textcircled{r} \\ | \\ \textcircled{v} \\ | \\ \textcircled{t} \end{array} \stackrel{(15)}{=} \begin{array}{c} \textcircled{s} \\ | \\ \textcircled{v} \\ | \\ \textcircled{v} \\ | \\ \textcircled{t} \end{array} \stackrel{(8)}{=} \begin{array}{c} \textcircled{s} \\ | \\ \textcircled{t} \\ | \\ \textcircled{v} \\ | \\ \textcircled{v} \\ | \\ \textcircled{t} \end{array} \stackrel{\text{def}}{=} \begin{array}{c} \textcircled{s} \\ | \\ \textcircled{v} \end{array} .$$

It remains to prove (G3), that is, we must show that  $\theta$  makes the square

$$\begin{array}{ccc} P & \xrightarrow{\varsigma} & C^{\otimes 3} \xrightarrow{c_C, C \otimes C} C^{\otimes 3} \\ \theta \downarrow & & \downarrow 1 \otimes 1 \otimes v \\ P & \xrightarrow{\varsigma} & C^{\otimes 3} \end{array}$$

commute. The clockwise direction around the square is

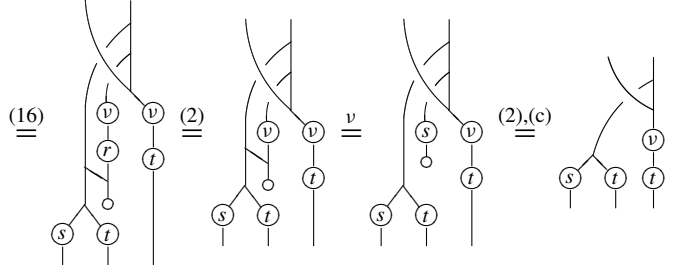
$$\begin{array}{c} \textcircled{s} \textcircled{s} \textcircled{t} \\ \diagdown \quad \diagup \\ \textcircled{t} \textcircled{v} \textcircled{v} \textcircled{t} \end{array} \stackrel{(10)}{=} \begin{array}{c} \textcircled{s} \textcircled{s} \textcircled{t} \\ \diagdown \quad \diagup \\ \textcircled{t} \textcircled{v} \textcircled{v} \textcircled{t} \end{array} \stackrel{(4)}{=} \begin{array}{c} \textcircled{s} \textcircled{s} \textcircled{t} \\ \diagdown \quad \diagup \\ \textcircled{t} \textcircled{v} \textcircled{v} \textcircled{t} \end{array} = \begin{array}{c} \textcircled{s} \textcircled{t} \textcircled{v} \end{array}$$

for which the last step holds since

$$\begin{aligned} tvvts &= tvvs && \text{by (8)} \\ &= tvr && \text{by (15)} \\ &= ttv && \text{by (16)} \\ &= tv && \text{by (7)}. \end{aligned}$$

The counterclockwise direction is

$$\begin{array}{c} \textcircled{s} \textcircled{t} \textcircled{v} \end{array} \stackrel{(17)}{=} \begin{array}{c} \textcircled{s} \textcircled{t} \textcircled{v} \end{array} \stackrel{(2)}{=} \begin{array}{c} \textcircled{s} \textcircled{t} \textcircled{v} \end{array} \stackrel{(16)}{=} \begin{array}{c} \textcircled{s} \textcircled{t} \textcircled{v} \end{array} \stackrel{(4)}{=} \begin{array}{c} \textcircled{s} \textcircled{t} \textcircled{v} \end{array}$$



This establishes the commutativity of the square.

**6.2. Quantum categories are weak bimonoids.** In this section we prove that a quantum category with a separable Frobenius object-of-objects yields a weak bimonoid. Thus, suppose that  $\mathbf{A} = (A, C, s, t, \mu, \eta)$  is a quantum category in  $\mathcal{V}$  with  $C = (C, \mu, \eta, \delta, \epsilon)$  a separable Frobenius monoid. The object  $A$  is a comonoid in  $\mathcal{V}$ , and our goal here is to show that equipping it with a multiplication and unit as

$$\mu = (A \otimes A \xrightarrow{m} P \xrightarrow{\mu} A), \quad \eta = (I \xrightarrow{\eta} C \xrightarrow{\eta} A)$$

then yields a weak bimonoid  $A$  in  $\mathcal{V}$  (and hence in  $\mathcal{QV}$ ).

Let us begin by establishing that the multiplication and unit defined here give a monoid structure on  $A$ . Note that the morphisms

$$\eta \otimes_C 1 : C \otimes_C A \rightarrow A \otimes_C A \quad \text{and} \quad 1 \otimes_C \eta : A \otimes_C C \rightarrow A \otimes_C A$$

are the unique morphisms such that  $(\eta \otimes 1)\iota = \iota(\eta \otimes_C 1) : C \otimes_C A \rightarrow A \otimes A$  and  $(1 \otimes \eta)\iota = \iota(1 \otimes_C \eta) : A \otimes C \rightarrow A \otimes A$ , respectively. Thus, we have

$$\eta \otimes_C 1 = m(\eta \otimes 1)\iota \quad \text{and} \quad 1 \otimes_C \eta = m(1 \otimes \eta)\iota,$$

so that

$$(\eta \otimes_C 1)\lambda = m(\eta \otimes 1)\delta_l \quad \text{and} \quad (1 \otimes_C \eta)\rho = m(1 \otimes \eta)\delta_r,$$

where  $\lambda : A \rightarrow C \otimes_C A$  and  $\rho : A \rightarrow A \otimes_C C$  are the left and right unit isomorphisms, respectively.

Also,  $\mu \otimes_C 1$  and  $1 \otimes_C \mu$  are the unique morphisms such that  $(\mu \otimes 1)\iota = \iota(\mu \otimes_C 1)$  and  $(1 \otimes \mu)\iota = \iota(1 \otimes_C \mu)$ . Thus,

$$1 \otimes_C \mu = m(1 \otimes \mu)\iota \quad \text{and} \quad \mu \otimes_C 1 = m(\mu \otimes 1)\iota.$$

Given these identities, one of the unit conditions is seen from the calculation

The third equality uses the fact that  $\eta$  is a  $C$ -comodule morphism. The other unit condition may be calculated similarly.

To establish associativity, we first prove the following lemma.

**Lemma 6.4.**

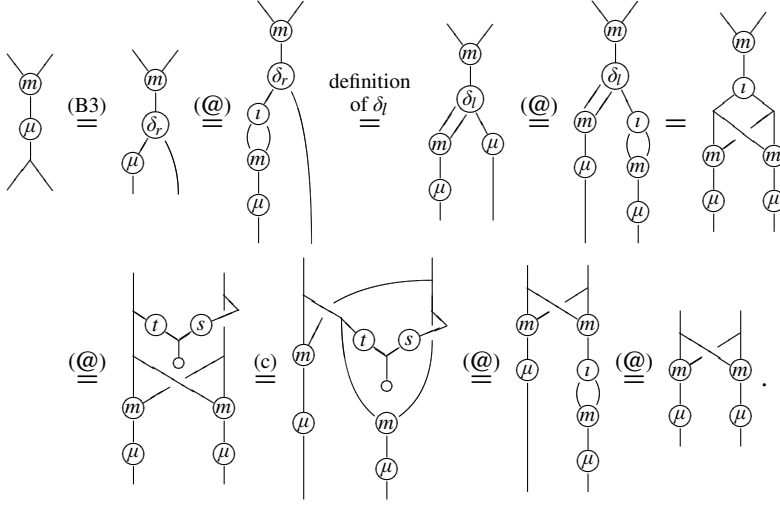
*Proof.* We prove the first equality. The second is similar.

where the second step follows since  $\mu$  is a  $C$ -comodule morphism. □

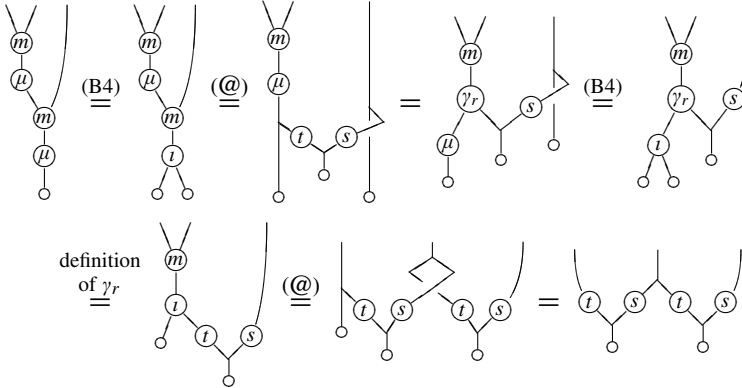
The following calculation then shows that associativity holds.

This then proves that  $(A, \mu, \eta)$  is a monoid in  $\mathcal{V}$ . We now prove the remaining axioms for a weak bimonoid.

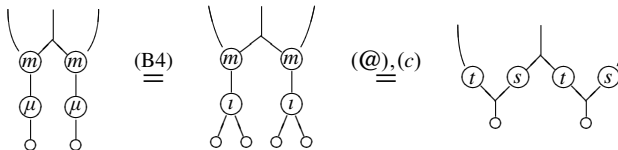
Axiom (b) is given by the calculation



Axiom (v) is established with three calculations. The first is given as follows, where the third equality below follows from the fact that  $\mu$  is a  $C$ -comodule morphism.



The second:



The third:

$$\begin{array}{c} \text{Diagram 1} \end{array} \stackrel{(B4)}{=} \begin{array}{c} \text{Diagram 2} \end{array} \stackrel{(@),(c)}{=} \begin{array}{c} \text{Diagram 3} \end{array} = \begin{array}{c} \text{Diagram 4} \end{array}$$

The diagrams represent string rewrites involving multiplication  $m$ , comultiplication  $\mu$ , comultiplication  $\iota$ , and comultiplication  $s$ . Diagram 1 shows  $m$  and  $\mu$  with a crossing. Diagram 2 shows  $m$  and  $\iota$  with a crossing. Diagram 3 shows  $\iota$  and  $s$  with a crossing. Diagram 4 shows  $\iota$  and  $s$  with a crossing.

To prove the final axiom (w) for a weak bimonoid, we need a lemma.

**Lemma 6.5.**

$$\begin{array}{c} \text{Diagram 1} \end{array} = \begin{array}{c} \text{Diagram 2} \end{array} \quad \text{and} \quad \begin{array}{c} \text{Diagram 3} \end{array} = \begin{array}{c} \text{Diagram 4} \end{array}$$

The diagrams represent string rewrites involving multiplication  $m$ , comultiplication  $\eta$ , and comultiplication  $\iota$ . Diagram 1 shows  $m$  and  $\eta$  with a crossing. Diagram 2 shows  $m$  and  $\iota$  with a crossing. Diagram 3 shows  $m$  and  $\eta$  with a crossing. Diagram 4 shows  $m$  and  $\iota$  with a crossing.

*Proof.* The first property of the lemma may be seen as follows. (The second equality below holds since  $\eta$  is a  $C$ -comodule morphism.)

$$\begin{array}{c} \text{Diagram 1} \end{array} \stackrel{(@)}{=} \begin{array}{c} \text{Diagram 2} \end{array} = \begin{array}{c} \text{Diagram 3} \end{array} \stackrel{(f)}{=} \begin{array}{c} \text{Diagram 4} \end{array} \stackrel{(B6)}{=} \begin{array}{c} \text{Diagram 5} \end{array} = \begin{array}{c} \text{Diagram 6} \end{array} \stackrel{(B6)}{=} \begin{array}{c} \text{Diagram 7} \end{array}$$

The diagrams represent string rewrites involving multiplication  $m$ , comultiplication  $\eta$ , and comultiplication  $\iota$ . Diagram 1 shows  $m$  and  $\eta$  with a crossing. Diagram 2 shows  $m$  and  $\iota$  with a crossing. Diagram 3 shows  $m$  and  $\eta$  with a crossing. Diagram 4 shows  $m$  and  $\iota$  with a crossing. Diagram 5 shows  $m$  and  $\eta$  with a crossing. Diagram 6 shows  $m$  and  $\iota$  with a crossing. Diagram 7 shows  $m$  and  $\eta$  with a crossing.

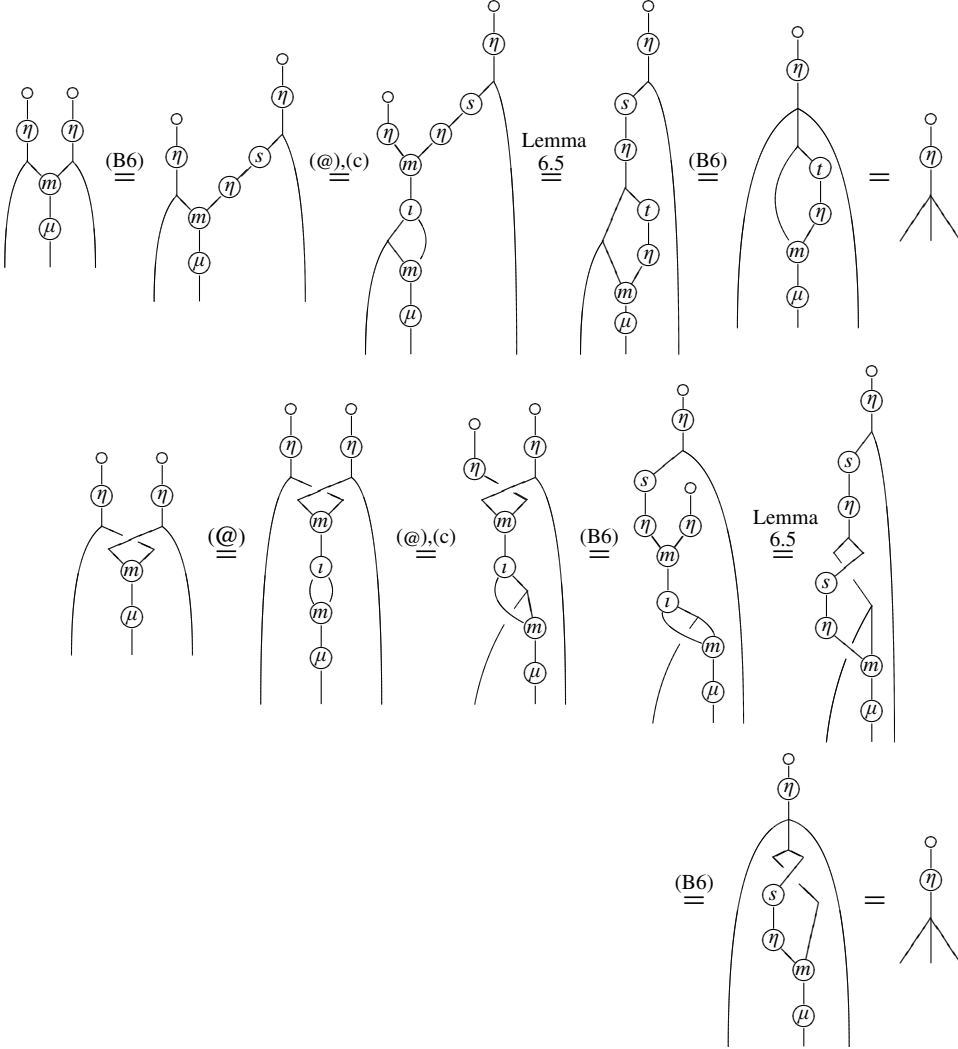
The second property of the lemma is proven as

$$\begin{array}{c} \text{Diagram 1} \end{array} \stackrel{(@)}{=} \begin{array}{c} \text{Diagram 2} \end{array} = \begin{array}{c} \text{Diagram 3} \end{array} \stackrel{(f)}{=} \begin{array}{c} \text{Diagram 4} \end{array} = \begin{array}{c} \text{Diagram 5} \end{array},$$

The diagrams represent string rewrites involving multiplication  $m$ , comultiplication  $\eta$ , and comultiplication  $\iota$ . Diagram 1 shows  $m$  and  $\eta$  with a crossing. Diagram 2 shows  $m$  and  $\iota$  with a crossing. Diagram 3 shows  $m$  and  $\eta$  with a crossing. Diagram 4 shows  $m$  and  $\iota$  with a crossing. Diagram 5 shows  $m$  and  $\eta$  with a crossing.

where the second equality holds again since  $\eta$  is a  $C$ -comodule morphism and the last equality follows from the proof of the first part.  $\square$

The following two calculations prove the axiom (w). In both calculations the last equality follows from the monoid structure on  $A$ .



This completes the proof. Thus, a quantum category with a separable Frobenius object-of-objects yields a weak bimonoid.

## Appendix A. String diagrams and basic definitions

In this appendix we give a quick introduction to string diagrams in a braided monoidal category  $\mathcal{V} = (\mathcal{V}, \otimes, I, c)$  [Joyal and Street 1993] and use these to define monoid, module, comonoid, comodule, and separable Frobenius monoid in  $\mathcal{V}$ . The string calculus was shown to be rigorous in [Joyal and Street 1991].

**A.1. String diagrams.** Suppose that  $\mathcal{V} = (\mathcal{V}, \otimes, I, c)$  is a braided (strict) monoidal category. In a string diagram, objects label edges and morphisms label nodes. For example, if  $f : A \otimes B \rightarrow C \otimes D \otimes E$  is a morphism in  $\mathcal{V}$ , it is represented as

$$f = \begin{array}{c} A \quad B \\ \diagdown \quad \diagup \\ \circlearrowleft f \\ \diagup \quad \diagdown \\ C \quad D \quad E \end{array},$$

where this diagram is meant to be read top to bottom. The identity morphism on an object will be represented as the object itself, as in

$$A = \begin{array}{c} A \\ | \\ \hline \end{array}.$$

A special case is the object  $I \in \mathcal{V}$ , which is represented as the empty string.

If, in  $\mathcal{V}$ , there are morphisms  $f : A \otimes B \rightarrow C \otimes D \otimes E$  and  $g : D \otimes E \otimes F \rightarrow G \otimes H$ , then they may be composed as

$$A \otimes B \otimes F \xrightarrow{f \otimes 1} C \otimes D \otimes E \otimes F \xrightarrow{1 \otimes g} C \otimes G \otimes H,$$

which may be represented as vertical concatenation

$$(1 \otimes g)(f \otimes 1) = \begin{array}{c} \diagup \quad \diagdown \\ \circlearrowleft f \\ \diagdown \quad \diagup \\ \diagup \quad \diagdown \\ \circlearrowleft g \\ \diagdown \quad \diagup \end{array}$$

(where we have left off the objects). The tensor product of morphisms, say

$$\begin{array}{c} \diagup \quad \diagdown \\ \circlearrowleft f \\ \diagdown \quad \diagup \end{array} \quad \text{and} \quad \begin{array}{c} \diagup \quad \diagdown \\ \circlearrowleft g \\ \diagdown \quad \diagup \end{array},$$

is represented by horizontal juxtaposition:

$$f \otimes g = \begin{array}{c} \diagup \quad \diagdown \\ \circlearrowleft f \\ \diagdown \quad \diagup \end{array} \quad \begin{array}{c} \diagup \quad \diagdown \\ \circlearrowleft g \\ \diagdown \quad \diagup \end{array}$$

(again leaving off the objects).

The braiding  $c_{A,B} : A \otimes B \rightarrow B \otimes A$  is represented as a left-over-right crossing. The inverse braiding is then represented as a right-over-left crossing:

$$c_{A,B} = \begin{array}{c} A \quad B \\ \diagdown \quad \diagup \\ B \quad A \end{array}, \quad c_{A,B}^{-1} = \begin{array}{c} B \quad A \\ \diagdown \quad \diagup \\ A \quad B \end{array}.$$

Suppose  $A \in \mathcal{V}$  has a chosen left dual  $A^*$ , which we denote by  $A^* \dashv A$  (it would be an adjunction if we were to view  $\mathcal{V}$  as a one object bicategory). The evaluation and coevaluation morphisms  $e_A : A^* \otimes A \rightarrow I$  and  $n_A : I \rightarrow A \otimes A^*$  are represented as

$$e_A = \begin{array}{c} A^* \quad A \\ \diagdown \quad \diagup \\ I \end{array} \quad \text{and} \quad n_A = \begin{array}{c} I \\ \diagup \quad \diagdown \\ A \quad A^* \end{array}.$$

The triangle equalities become

$$\begin{array}{c} A \\ \diagup \\ A^* \\ \diagdown \\ A \end{array} = \begin{array}{c} A \\ | \\ I \end{array} \quad \text{and} \quad \begin{array}{c} A^* \\ \diagdown \\ A \\ \diagup \\ A^* \end{array} = \begin{array}{c} A^* \\ | \\ I \end{array}.$$

To simplify the string diagrams in what follows, we will omit the nodes from certain morphisms (for example, multiplication and comultiplication morphisms) or simplify them (for example, unit and counit morphisms).

**A.2. Monoids and modules.** A monoid  $A = (A, \mu, \eta)$  in  $\mathcal{V}$  is an object  $A \in \mathcal{V}$  equipped with morphisms

$$\mu = \begin{array}{c} \diagup \quad \diagdown \\ | \end{array} : A \otimes A \rightarrow A \quad \text{and} \quad \eta = \begin{array}{c} \circ \\ | \end{array} : I \rightarrow A,$$

called the *multiplication* and *unit* of the monoid respectively, satisfying

$$\begin{array}{c} \diagup \quad \diagdown \\ | \end{array} = \begin{array}{c} \diagup \quad \diagdown \\ \diagup \quad \diagdown \\ | \end{array} = \begin{array}{c} \diagup \quad \diagdown \\ \diagup \quad \diagdown \\ \diagup \quad \diagdown \\ | \end{array} \quad \text{and} \quad \begin{array}{c} \circ \\ | \end{array} = \begin{array}{c} | \\ | \end{array} = \begin{array}{c} \diagup \quad \diagdown \\ \circ \end{array}. \quad (\text{m})$$

If  $A$  and  $B$  are monoids, a *monoid morphism*  $f : A \rightarrow B$  is a morphism in  $\mathcal{V}$  satisfying

$$\begin{array}{c} A \quad A \\ \diagdown \quad \diagup \\ \circ \\ | \end{array} = \begin{array}{c} A \quad A \\ \diagdown \quad \diagup \\ \circ \\ | \end{array} \quad \text{and} \quad \begin{array}{c} A \\ \circ \\ | \end{array} = \begin{array}{c} B \\ \circ \\ | \end{array}.$$

Monoids make sense in any monoidal category, however, in order that the tensor product  $A \otimes B$  of monoids  $A, B \in \mathcal{V}$  should again be a monoid, there must be a



“switch” morphism  $c_{A,B} : A \otimes B \rightarrow B \otimes A$  in  $\mathcal{V}$  given by, say, a braiding. In this case,  $A \otimes B$  becomes a monoid in  $\mathcal{V}$  via

$$\mu = \begin{array}{c} \diagup \quad \diagdown \\ \diagdown \quad \diagup \\ \text{---} \end{array} \quad \text{and} \quad \eta = \begin{array}{c} \circ \quad \circ \\ | \quad | \end{array}.$$

Suppose that  $A$  is a monoid in  $\mathcal{V}$ . A *right  $A$ -module* in  $\mathcal{V}$  is an object  $M \in \mathcal{V}$  equipped with a morphism

$$\mu = \begin{array}{c} M \quad A \\ \diagdown \quad \diagup \\ \text{---} \\ M \end{array} : M \otimes A \rightarrow M,$$

called the *action of  $A$  on  $M$* , satisfying

$$\begin{array}{c} M \quad A \quad A \\ \diagdown \quad \diagup \quad \diagup \\ \text{---} \\ M \end{array} = \begin{array}{c} M \quad A \quad A \\ \diagdown \quad \diagup \quad \diagup \\ \text{---} \\ M \end{array} \quad \text{and} \quad \begin{array}{c} M \\ \diagdown \quad \circ_A \\ \text{---} \\ M \end{array} = \begin{array}{c} M \\ | \\ \text{---} \end{array}. \quad (\text{m})$$

Notice that we use the same label “(m)” as in the monoid axioms (and “(c)” below for the comodule axioms). This should not cause any confusion as the labeling of strings disambiguates a multiplication and an action; however, the labeling will usually be left off.

If  $M$  and  $N$  are modules, a *module morphism*  $f : M \rightarrow N$  is a morphism in  $\mathcal{V}$  satisfying

$$\begin{array}{c} M \quad A \\ \diagdown \quad \diagup \\ \text{---} \\ \circ_f \\ N \end{array} = \begin{array}{c} M \quad A \\ \diagdown \quad \diagup \\ \text{---} \\ \circ_f \\ N \end{array}.$$

**A.3. Comonoids and comodules.** Comonoids and comodules are dual to monoids and modules. Explicitly, a *comonoid*  $C = (C, \delta, \epsilon)$  in  $\mathcal{V}$  is an object  $C \in \mathcal{V}$  equipped with morphisms

$$\delta = \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \end{array} : C \rightarrow C \otimes C \quad \text{and} \quad \epsilon = \begin{array}{c} \text{---} \\ \circ \end{array} : C \rightarrow I,$$

called the *comultiplication* and *counit* of the comonoid respectively, satisfying

$$\begin{array}{c} \text{---} \\ \diagdown \quad \diagup \end{array} = \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \end{array} = \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \end{array} \quad \text{and} \quad \begin{array}{c} \text{---} \\ \diagdown \quad \circ \end{array} = \begin{array}{c} \text{---} \\ | \end{array} = \begin{array}{c} \text{---} \\ \diagdown \quad \circ \end{array}. \quad (\text{c})$$

If  $C, D$  are comonoids, a *comonoid morphism*  $f : C \rightarrow D$  is a morphism in  $\mathcal{V}$  satisfying

$$\begin{array}{c} A \\ | \\ \textcircled{f} \\ / \quad \backslash \\ B \quad B \end{array} = \begin{array}{c} A \\ / \quad \backslash \\ \textcircled{f} \quad \textcircled{f} \\ | \quad | \\ B \quad B \end{array} \quad \text{and} \quad \begin{array}{c} A \\ | \\ \textcircled{f} \\ | \\ \textcircled{B} \end{array} = \begin{array}{c} A \\ | \\ \textcircled{B} \end{array}.$$

Similarly here,  $\mathcal{V}$  must contain a switch morphism  $c_{C,D} : C \otimes D \rightarrow D \otimes C$  in order that the tensor product  $C \otimes D$  of comonoids  $C, D \in \mathcal{V}$  should again be a comonoid. In this case the comultiplication and counit are given by

$$\delta = \begin{array}{c} \diagup \quad \diagdown \\ | \quad | \\ \diagdown \quad \diagup \end{array} \quad \text{and} \quad \epsilon = \begin{array}{c} | \quad | \\ \textcircled{\phantom{A}} \quad \textcircled{\phantom{A}} \end{array}.$$

Suppose that  $C$  is a comonoid in  $\mathcal{V}$ . A *right  $C$ -comodule* in  $\mathcal{V}$  is an object  $M \in \mathcal{V}$  equipped with a morphism

$$\gamma = \begin{array}{c} M \\ | \\ \diagdown \quad \diagup \\ M \quad C \end{array} : M \rightarrow M \otimes C,$$

called the *coaction of  $A$  on  $M$* , satisfying

$$\begin{array}{c} M \\ | \\ \diagdown \quad \diagup \\ M \quad C \quad C \end{array} = \begin{array}{c} M \\ | \\ \diagdown \quad \diagup \\ M \quad C \quad C \end{array} \quad \text{and} \quad \begin{array}{c} M \\ | \\ \diagdown \quad \diagup \\ M \quad \textcircled{C} \end{array} = \begin{array}{c} M \\ | \\ \textcircled{M} \end{array}. \quad (\text{c})$$

If  $M$  and  $N$  are  $C$ -comodules, a *comodule morphism*  $f : M \rightarrow N$  is a morphism in  $\mathcal{V}$  satisfying

$$\begin{array}{c} M \\ | \\ \textcircled{f} \\ | \\ \diagdown \quad \diagup \\ N \quad C \end{array} = \begin{array}{c} M \\ | \\ \diagdown \quad \diagup \\ \textcircled{f} \quad \diagup \\ N \quad C \end{array}.$$

In this paper we also make use of  $C$ -bicomodules. Suppose that  $M$  is both a left  $C$ -comodule and a right  $C$ -comodule with coactions

$$\gamma_l : M \rightarrow C \otimes M \quad \text{and} \quad \gamma_r : M \rightarrow M \otimes C.$$

If the square

$$\begin{array}{ccc} M & \xrightarrow{\gamma_l} & C \otimes M \\ \gamma_r \downarrow & & \downarrow 1 \otimes \gamma_r \\ M \otimes C & \xrightarrow{\gamma_l \otimes 1} & C \otimes M \otimes C \end{array}$$

commutes, meaning

$$\begin{array}{c} C \\ \diagup \quad \diagdown \\ M \quad C \quad M \end{array} = \begin{array}{c} C \\ \diagup \quad \diagdown \\ M \quad C \quad M \end{array}$$

in string diagrams, then  $M$  is called a  $C$ -bicomodule. The diagonal of the square will be denoted by  $\gamma : M \rightarrow C \otimes M \otimes C$ .

**A.4. Frobenius monoids.** A Frobenius monoid  $R$  in  $\mathcal{V}$  is both a monoid and a comonoid in  $\mathcal{V}$  that additionally satisfies the “Frobenius condition”:

$$\begin{array}{ccc} R \otimes R & \xrightarrow{\delta \otimes 1} & R \otimes R \otimes R \\ 1 \otimes \delta \downarrow & & \downarrow 1 \otimes \mu \\ R \otimes R \otimes R & \xrightarrow{\mu \otimes 1} & R \otimes R. \end{array}$$

In strings the Frobenius condition is displayed as

$$\begin{array}{c} | \\ \diagdown \\ | \\ \diagup \\ | \end{array} = \begin{array}{c} | \\ \diagup \\ | \\ \diagdown \\ | \end{array}. \quad (\text{f})$$

We will now review some basic facts about Frobenius monoids.

**Lemma A.1.**  $(1 \otimes \mu)(\delta \otimes 1) = \delta\mu = (\mu \otimes 1)(1 \otimes \delta) : R \otimes R \rightarrow R \otimes R$ .

*Proof.* The left equality is proved by the string calculation

$$\begin{array}{c} | \\ \diagdown \\ | \end{array} \stackrel{(c)}{=} \begin{array}{c} | \\ \diagdown \\ | \circ \end{array} \stackrel{(f)}{=} \begin{array}{c} | \\ \diagdown \\ | \circ \end{array} \stackrel{(c)}{=} \begin{array}{c} | \\ \diagdown \\ | \circ \end{array} \stackrel{(f)}{=} \begin{array}{c} | \\ \diagup \\ | \circ \end{array} \stackrel{(c)}{=} \begin{array}{c} | \\ \diagup \\ | \end{array}.$$

The right equality follows from a similar calculation. □

Define morphisms  $\rho$  and  $\sigma$  by

$$\begin{aligned} \rho &= (I \xrightarrow{\eta} R \xrightarrow{\delta} R \otimes R) = \begin{array}{c} \circ \\ \diagup \quad \diagdown \\ | \quad | \end{array}, \\ \sigma &= (R \otimes R \xrightarrow{\mu} R \xrightarrow{\epsilon} I) = \begin{array}{c} | \quad | \\ \diagdown \quad \diagup \\ \circ \end{array}. \end{aligned}$$

**Proposition A.2.** The morphisms  $\rho$  and  $\sigma$  respectively form the unit and counit of an adjunction  $R \dashv R$ .

*Proof.* One of the triangle identities is given as

$$\begin{array}{c} | \\ \diagup \\ | \circ \end{array} \stackrel{(f)}{=} \begin{array}{c} | \\ \diagup \\ | \circ \end{array} \stackrel{(m),(c)}{=} \begin{array}{c} | \\ \diagup \\ | \end{array},$$



### Appendix B. Proofs of the properties of $s$ , $t$ , and $r$

As we have noted in Section 1, the source morphism  $s : A \rightarrow A$  is invariant under rotation by  $\pi$ , the target  $t : A \rightarrow A$  is invariant under horizontal reflection, and the endomorphism  $r$  is  $t$  rotated by  $\pi$ . This reduces the number of proofs we present, since the others are derivable.

$$\begin{array}{l}
 \begin{array}{c} \textcircled{s} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \stackrel{(c)}{=} \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \stackrel{(w)}{=} \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \textcircled{s} \quad (1) \\
 \begin{array}{c} \textcircled{s} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \stackrel{(c)}{=} \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \stackrel{(w)}{=} \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \textcircled{s} \\
 \begin{array}{c} \textcircled{t} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \stackrel{(c)}{=} \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \stackrel{(w)}{=} \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \textcircled{t} \\
 \begin{array}{c} \textcircled{t} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \stackrel{(c)}{=} \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \stackrel{(w)}{=} \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \textcircled{t}
 \end{array}$$

$$\begin{array}{l}
 \begin{array}{c} \textcircled{s} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \stackrel{\text{nat}}{=} \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \stackrel{(w)}{=} \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \stackrel{(c)}{=} \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \quad (2) \\
 \begin{array}{c} \textcircled{s} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \stackrel{(m)}{=} \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \stackrel{(c)}{=} \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \\
 \begin{array}{c} \textcircled{t} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \stackrel{\text{nat}}{=} \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \stackrel{(w)}{=} \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \stackrel{(c)}{=} \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \\
 \begin{array}{c} \textcircled{t} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \stackrel{(m)}{=} \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \stackrel{(c)}{=} \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array}
 \end{array}$$

$$\begin{array}{l}
 \begin{array}{c} \textcircled{s} \\ | \\ \text{---} \end{array} \stackrel{(1)}{=} \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \stackrel{(2)}{=} \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \stackrel{(1)}{=} \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \textcircled{s} \quad (3) \\
 \begin{array}{c} \textcircled{t} \\ | \\ \text{---} \end{array} \stackrel{(1)}{=} \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \stackrel{(2)}{=} \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \stackrel{(1)}{=} \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \textcircled{t}
 \end{array}$$

$$\begin{array}{c}
 \text{Diagram 1} \stackrel{(b)}{=} \text{Diagram 2} \stackrel{(1)}{=} \text{Diagram 3} \stackrel{(m)}{=} \text{Diagram 4} \stackrel{(b)}{=} \text{Diagram 5}
 \end{array} \quad (4)$$

$$\begin{array}{c}
 \text{Diagram 6} \stackrel{(b)}{=} \text{Diagram 7} \stackrel{(1)}{=} \text{Diagram 8} \stackrel{(m)}{=} \text{Diagram 9} \stackrel{(b)}{=} \text{Diagram 10}
 \end{array}$$

$$\begin{array}{c}
 \text{Diagram 11} \stackrel{(b)}{=} \text{Diagram 12} \stackrel{(1)}{=} \text{Diagram 13} \stackrel{(m)}{=} \text{Diagram 14} \stackrel{(b)}{=} \text{Diagram 15}
 \end{array}$$

$$\begin{array}{c}
 \text{Diagram 16} \stackrel{(b)}{=} \text{Diagram 17} \stackrel{(1)}{=} \text{Diagram 18} \stackrel{(m)}{=} \text{Diagram 19} \stackrel{(b)}{=} \text{Diagram 20}
 \end{array}$$

$$\begin{array}{c}
 \text{Diagram 21} \stackrel{(4)}{=} \text{Diagram 22} \stackrel{(3)}{=} \text{Diagram 23} \stackrel{(4)}{=} \text{Diagram 24}
 \end{array} \quad (5)$$

$$\begin{array}{c}
 \text{Diagram 25} \stackrel{(4)}{=} \text{Diagram 26} \stackrel{(3)}{=} \text{Diagram 27} \stackrel{(4)}{=} \text{Diagram 28}
 \end{array}$$

$$\begin{array}{c}
 \text{Diagram 29} \stackrel{s}{=} \text{Diagram 30} \stackrel{\text{nat}}{=} \text{Diagram 31} \stackrel{(b)}{=} \text{Diagram 32} \stackrel{(m),(c)}{=} \text{Diagram 33}
 \end{array} \quad (6)$$

$$\begin{array}{c}
 \text{Diagram 34} \stackrel{t}{=} \text{Diagram 35} \stackrel{(b)}{=} \text{Diagram 36} \stackrel{(m),(c)}{=} \text{Diagram 37}
 \end{array}$$

$$\begin{array}{c}
 \text{Diagram 38} \stackrel{s}{=} \text{Diagram 39} \stackrel{(2)}{=} \text{Diagram 40} \stackrel{s}{=} \text{Diagram 41} \quad \text{Diagram 42} \stackrel{t}{=} \text{Diagram 43} \stackrel{(2)}{=} \text{Diagram 44} \stackrel{t}{=} \text{Diagram 45}
 \end{array} \quad (7)$$

$$\begin{array}{c}
 \text{Diagram 46} \stackrel{s}{=} \text{Diagram 47} \stackrel{(2)}{=} \text{Diagram 48} \stackrel{s}{=} \text{Diagram 49} \quad \text{Diagram 50} \stackrel{t}{=} \text{Diagram 51} \stackrel{(2)}{=} \text{Diagram 52} \stackrel{t}{=} \text{Diagram 53}
 \end{array} \quad (8)$$

(9)

[illegible]

$$\begin{array}{c}
\text{Diagram 1} \\
\equiv \text{(m)} \\
\text{Diagram 2} \\
\equiv \text{(4)} \\
\text{Diagram 3} \\
\equiv \text{(m)} \\
\text{Diagram 4} \\
\equiv \text{(2)} \\
\text{Diagram 5} \\
\equiv \text{(2)} \\
\text{Diagram 6} \\
\equiv \text{(4)} \\
\text{Diagram 7}
\end{array} \quad (11)$$

$$\begin{array}{c} \textcircled{r} \\ \textcircled{s} \end{array} \stackrel{r,s}{=} \begin{array}{c} \textcircled{\phantom{r}} \\ \textcircled{\phantom{s}} \end{array} \stackrel{\text{nat}}{=} \begin{array}{c} \textcircled{\phantom{r}} \\ \textcircled{\phantom{s}} \end{array} \stackrel{(v)}{=} \begin{array}{c} \textcircled{\phantom{r}} \\ \textcircled{\phantom{s}} \end{array} \stackrel{(c)}{=} \begin{array}{c} \textcircled{\phantom{r}} \\ \textcircled{\phantom{s}} \end{array} \stackrel{s}{=} \begin{array}{c} \textcircled{s} \end{array} \quad (12)$$

$$\begin{array}{c} \textcircled{i} \\ | \\ \textcircled{r} \end{array} \stackrel{t,r}{=} \begin{array}{c} \diagup \quad \diagdown \\ | \qquad | \\ \textcircled{\phantom{i}} \quad \textcircled{\phantom{r}} \end{array} \stackrel{\text{nat}}{=} \begin{array}{c} \diagup \quad \diagdown \\ | \qquad | \\ \textcircled{\phantom{i}} \quad \textcircled{\phantom{r}} \end{array} \stackrel{(v)}{=} \begin{array}{c} \diagup \quad \diagdown \\ | \qquad | \\ \textcircled{\phantom{i}} \quad \textcircled{\phantom{r}} \end{array} \stackrel{t,r}{=} \begin{array}{c} \textcircled{r} \quad \textcircled{i} \end{array} \quad (13)$$

$$\begin{array}{c}
\begin{array}{c} \text{Diagram 1: } \text{Y-junction with } r \text{ on top-left, } s \text{ on bottom-left, and } s \text{ on bottom-right.} \\ \text{Diagram 2: } \text{Y-junction with } r \text{ on top-left, } s \text{ on top-right, and } s \text{ on bottom-left.} \end{array} \stackrel{(3)}{=} \begin{array}{c} \text{Diagram 3: } \text{Y-junction with } r \text{ on top-left, } s \text{ on top-right, and } s \text{ on bottom-right.} \\ \text{Diagram 4: } \text{Y-junction with } r \text{ on top-left, } s \text{ on top-right, and } s \text{ on bottom-left.} \end{array} \stackrel{(12)}{=} \begin{array}{c} \text{Diagram 5: } \text{Y-junction with } s \text{ on top-left, } s \text{ on top-right, and } s \text{ on bottom-left.} \\ \text{Diagram 6: } \text{Y-junction with } s \text{ on top-left, } s \text{ on top-right, and } s \text{ on bottom-right.} \end{array} \stackrel{(3)}{=} \begin{array}{c} \text{Diagram 7: } \text{Y-junction with } s \text{ on top-left, } s \text{ on top-right, and } s \text{ on bottom-left.} \\ \text{Diagram 8: } \text{Y-junction with } s \text{ on top-left, } s \text{ on top-right, and } s \text{ on bottom-right.} \end{array}
\end{array}
\quad (14)$$

## Acknowledgments

We would like to thank Gabriella Böhm for her helpful comments and suggestions, and particularly for her help with Theorem 6.1, both for its statement and also for helping with the proof. We would also like to thank J. N. Alonso, J. M. Fernández, and R. González for sending us copies of their preprints [Alonso Álvarez et al. 2008a; 2008b], and an anonymous referee for helpful comments and suggestions.

## References

- [Alonso Álvarez et al. 2003] J. N. Alonso Álvarez, R. González Rodríguez, J. M. Fernández Vilaboa, M. P. López López, and E. Villanueva Novoa, “Weak Hopf algebras with projection and weak smash bialgebra structures”, *J. Algebra* **269**:2 (2003), 701–725. MR 2005b:16062 Zbl 1042.16020
- [Alonso Álvarez et al. 2008a] J. N. Alonso Álvarez, J. M. Fernández Vilaboa, and R. González Rodríguez, “Weak braided Hopf algebras”, preprint, 2008. To appear in *Indiana University Math. J.*
- [Alonso Álvarez et al. 2008b] J. N. Alonso Álvarez, J. M. Fernández Vilaboa, and R. González Rodríguez, “Weak Hopf algebras and weak Yang–Baxter operators”, *J. Algebra* **320**:5 (2008), 2101–2143. MR 2437645 Zbl 1142.18006
- [Bálint 2008a] I. Bálint, *Quantum groupoid symmetry in low dimensional quantum field theory*, Ph.D. thesis, Eötvös Loránd University, Budapest, 2008.
- [Bálint 2008b] I. Bálint, “Scalar extension of bicoalgebroids”, *Appl. Categ. Structures* **16**:1-2 (2008), 29–55. MR 2383276 Zbl 05265525
- [Barr 1995] M. Barr, “Nonsymmetric \*-autonomous categories”, *Theoret. Comput. Sci.* **139**:1-2 (1995), 115–130. MR 96e:03077 Zbl 0874.18004
- [Böhm and Szlachányi 1996] G. Böhm and K. Szlachányi, “A coassociative  $C^*$ -quantum group with nonintegral dimensions”, *Lett. Math. Phys.* **38**:4 (1996), 437–456. MR 97k:46080 Zbl 0872.16022
- [Böhm and Szlachányi 2000] G. Böhm and K. Szlachányi, “Weak Hopf algebras, II: Representation theory, dimensions, and the Markov trace”, *J. Algebra* **233**:1 (2000), 156–212. MR 2001m:16059 Zbl 0980.16028
- [Böhm and Szlachányi 2004] G. Böhm and K. Szlachányi, “Hopf algebroids with bijective antipodes: axioms, integrals, and duals”, *J. Algebra* **274**:2 (2004), 708–750. MR 2004m:16047 Zbl 1080.16035
- [Böhm et al. 1999] G. Böhm, F. Nill, and K. Szlachányi, “Weak Hopf algebras, I: Integral theory and  $C^*$ -structure”, *J. Algebra* **221**:2 (1999), 385–438. MR 2001a:16059 Zbl 0949.16037
- [Brzeziński and Militaru 2002] T. Brzeziński and G. Militaru, “Bialgebroids,  $\times_A$ -bialgebras and duality”, *J. Algebra* **251**:1 (2002), 279–294. MR 2003c:16044 Zbl 1003.16033
- [Day and Street 2004] B. Day and R. Street, “Quantum categories, star autonomy, and quantum groupoids”, pp. 187–225 in *Galois theory, Hopf algebras, and semiabelian categories*, edited by G. Janelidze et al., Fields Institute Communications **43**, Amer. Math. Soc., Providence, RI, 2004. MR 2005f:18006 Zbl 1067.18006
- [Day et al. 2003] B. Day, P. McCrudden, and R. Street, “Dualizations and antipodes”, *Appl. Categ. Structures* **11**:3 (2003), 229–260. MR 2004b:18013 Zbl 1137.18302
- [Hayashi 1998] T. Hayashi, “Face algebras, I: A generalization of quantum group theory”, *J. Math. Soc. Japan* **50**:2 (1998), 293–315. MR 99d:16043 Zbl 0908.16032
- [Joyal and Street 1991] A. Joyal and R. Street, “The geometry of tensor calculus, I”, *Adv. Math.* **88**:1 (1991), 55–112. MR 92d:18011 Zbl 0738.18005



- [Joyal and Street 1993] A. Joyal and R. Street, “Braided tensor categories”, *Adv. Math.* **102**:1 (1993), 20–78. MR 94m:18008 Zbl 0817.18007
- [Lu 1996] J.-H. Lu, “Hopf algebroids and quantum groupoids”, *Internat. J. Math.* **7**:1 (1996), 47–70. MR 97a:16073 Zbl 0884.17010
- [Nikshych and Vainerman 2002] D. Nikshych and L. Vainerman, “Finite quantum groupoids and their applications”, pp. 211–262 in *New directions in Hopf algebras*, edited by S. Montgomery and H.-J. Schneider, Math. Sci. Res. Inst. Publ. **43**, Cambridge Univ. Press, 2002. MR 2004d:16071 Zbl 1026.17017
- [Nill 1998] F. Nill, “Axioms for weak bialgebras”, preprint, 1998. arXiv math/9805104
- [Schauenburg 1998] P. Schauenburg, “Face algebras are  $\times_R$ -bialgebras”, pp. 275–285 in *Rings, Hopf algebras, and Brauer groups* (Antwerp/Brussels, 1996), edited by S. Caenepeel and A. Verschoren, Lecture Notes in Pure and Appl. Math. **197**, Dekker, New York, 1998. MR 99k:16086 Zbl 0905.16019
- [Schauenburg 2000] P. Schauenburg, “Duals and doubles of quantum groupoids ( $\times_R$ -Hopf algebras)”, pp. 273–299 in *New trends in Hopf algebra theory* (La Falda, 1999), edited by N. Andruskiewitsch et al., Contemporary Mathematics **267**, Amer. Math. Soc., Providence, RI, 2000. MR 2001i:16073 Zbl 0974.16036
- [Schauenburg 2003] P. Schauenburg, “Weak Hopf algebras and quantum groupoids”, pp. 171–188 in *Noncommutative geometry and quantum groups* (Warsaw, 2001), edited by P. M. Hajac and W. Pusz, Banach Center Publ. **61**, Polish Acad. Sci., Warsaw, 2003. MR 2004j:16042 Zbl 1064.16041
- [Sweedler 1974] M. E. Sweedler, “Groups of simple algebras”, *Inst. Hautes Études Sci. Publ. Math.* **44** (1974), 79–189. MR 51 #587 Zbl 0314.16008
- [Szlachányi 1997] K. Szlachányi, “Weak Hopf algebras”, pp. 621–632 in *Operator algebras and quantum field theory* (Rome, 1996), edited by S. Doplicher et al., Int. Press, Cambridge, MA, 1997. MR 99a:46105 Zbl 1098.16504
- [Takeuchi 1977] M. Takeuchi, “Groups of algebras over  $A \otimes \overline{A}$ ”, *J. Math. Soc. Japan* **29**:3 (1977), 459–492. MR 58 #22151 Zbl 0349.16012
- [Xu 2001] P. Xu, “Quantum groupoids”, *Communications in Mathematical Physics* **216**:3 (2001), 539–581. MR 2002f:17033 Zbl 0986.17003
- [Yamanouchi 1994] T. Yamanouchi, “Duality for generalized Kac algebras and a characterization of finite groupoid algebras”, *J. Algebra* **163**:1 (1994), 9–50. MR 95c:22010 Zbl 0830.46047

Communicated by Susan Montgomery

Received 2008-01-26

Revised 2008-11-14

Accepted 2008-12-23

craig@kurims.kyoto-u.ac.jp

Research Institute for the Mathematical Sciences,  
Kyoto University, Kyoto 606-8502, Japan  
www.kurims.kyoto-u.ac.jp/~craig/

street@ics.mq.edu.au

Department of Mathematics, Macquarie University,  
New South Wales 2109, Australia  
www.maths.mq.edu.au/~street

# Chabauty for symmetric powers of curves

Samir Siksek

Let  $C$  be a smooth projective absolutely irreducible curve of genus  $g \geq 2$  over a number field  $K$ , and denote its Jacobian by  $J$ . Let  $d \geq 1$  be an integer and denote the  $d$ -th symmetric power of  $C$  by  $C^{(d)}$ . In this paper we adapt the classic Chabauty–Coleman method to study the  $K$ -rational points of  $C^{(d)}$ . Suppose that  $J(K)$  has Mordell–Weil rank at most  $g - d$ . We give an explicit and practical criterion for showing that a given subset  $\mathcal{L} \subseteq C^{(d)}(K)$  is in fact equal to  $C^{(d)}(K)$ .

## 1. Introduction

Let  $C$  be a smooth projective absolutely irreducible curve of genus  $g \geq 2$  defined over a number field  $K$ , and write  $J$  for the Jacobian of  $C$ . Suppose that the rank of the Mordell–Weil group  $J(K)$  is at most  $g - 1$ . In a pioneering paper, Chabauty [1941] proved the finiteness of the set of  $K$ -rational points on  $C$ . This has since been superseded by Faltings’s proof [1983] of the Mordell conjecture, which gives the finiteness of  $C(K)$  without any assumption on the rank of  $J(K)$ . Chabauty’s approach, where applicable, does however have two considerable advantages:

The first is that Chabauty can be refined to give explicit bounds for the cardinality of  $C(K)$ , as shown by Coleman [1985a]. Coleman’s bounds are realistic, and occasionally even sharp; see for example [Grant 1994; Flynn 1995]. Coleman’s approach has been adapted to give bounds (assuming some reasonable conditions) for the number of solutions of Thue equations [Lorenzini and Tucker 2002], the number of rational points on Fermat’s curves [McCallum 1992; 1994], the number of points on curves of the form  $y^2 = x^5 + A$  [Stoll 2006b], and the number of rational points on twists of a given curve [Stoll 2006a].

The second is that the Chabauty–Coleman strategy can often be adapted to compute  $C(K)$ , as in [Bruin 2002; 2003, Flynn 1997; Flynn and Wetherell 1999; 2001; McCallum and Poonen 2006; Wetherell 1997].

---

*MSC2000:* primary 11G30; secondary 11G35, 14K20, 14C20.

*Keywords:* Chabauty, Coleman, curves, Jacobians, symmetric powers, divisors, differentials, abelian integrals.

The author is supported by an UK EPSRC grant and by a Marie Curie International Reintegration Grant.

One can ask if it is sensible to apply Chabauty to varieties  $X/K$  of dimension at least 2, where the Albanese variety  $\text{Alb}(X)$  plays the role of the Jacobian. Of course, even when a  $K$ -rational degree 1 zero-cycle on  $X$  exists, the associated Albanese map  $j : X \rightarrow \text{Alb}(X)$  is often not injective. Indeed  $\text{Alb}(X)$  can have smaller dimension than  $X$ . However, if  $j$  is injective, or even if  $j(X)$  is merely birational to  $X$ , there is a hope that Chabauty might enable us to determine the rational points on  $X$ . Alas, for a general variety  $X$  there are as of yet no algorithms for studying the arithmetic of  $\text{Alb}(X)$ . A sensible starting point for the investigation of Chabauty in higher dimension is the symmetric powers of curves. Here the Albanese variety is also the Jacobian of the curve.

Suppose  $d$  is a positive integer, and denote the  $d$ -th symmetric power of  $C$  by  $C^{(d)}$ . The elements of  $C^{(d)}(K)$  correspond to effective  $K$ -rational divisors on  $C$  of degree  $d$ . Suppose  $C^{(d)}(K)$  is nonempty, and let  $j : C^{(d)} \rightarrow J$  be the Abel–Jacobi map corresponding to some fixed element of  $C^{(d)}(K)$ . We shall write  $\gamma$  for the gonality of  $C$ ; this is defined to be the least possible degree of any nonconstant morphism  $C \rightarrow \mathbb{P}^1$ . If  $d < \gamma$ , then  $C^{(d)}$  is isomorphic to its image in  $J$  (denoted by  $W^{(d)}$ ), and if  $d \leq g$ , then  $C^{(d)}$  is birational to  $W^{(d)}$ . Another theorem of Faltings [1991; 1994] states that any proper subvariety of an abelian variety has finitely many  $K$ -rational points provided this subvariety does not contain a translate of any nontrivial proper abelian subvariety of  $J$ . If  $d < \gamma$  and  $W^{(d)}$  does not contain the translate of any proper abelian subvariety—this would be the case if  $J$  is simple—then it follows from Faltings’s theorem that  $C^{(d)}(K)$  is finite. This idea is used by Klassen [1993], by Debarre and Klassen [1994], and by Harris and Silverman [1991] to give sufficient conditions for  $C^{(d)}(K)$  to be finite in many cases. For example, Harris and Silverman show that if  $C$  is neither hyperelliptic nor bielliptic, then the set  $C^{(2)}(K)$  is finite. This result fails if  $C$  is hyperelliptic or bielliptic.

We are naturally led to the question, if  $C^{(d)}(K)$  is finite, can we adapt Chabauty–Coleman to compute it? Klassen makes a first attempt at this question in his PhD thesis [1993]. His main result on Chabauty–Coleman can be summarized as follows. Let  $K = \mathbb{Q}$  and  $1 < d < \gamma$ . Suppose that the rank of  $J(\mathbb{Q})$  is at most  $g - d$ . Let  $p$  be an odd prime of good reduction, and let  $\text{red} : C^{(d)}(\mathbb{Q}) \rightarrow \tilde{C}^{(d)}(\mathbb{F}_p)$  denote the reduction map. Klassen shows the existence of a canonical divisor  $M$  on  $C^{(d)}$  such that  $C^{(d)}(\mathbb{Q}) \setminus \text{red}^{-1}(M(\mathbb{F}_p))$  is finite. In essence he shows that any fibre of the reduction map contains at most one element of  $C^{(d)}(\mathbb{Q}) \setminus \text{red}^{-1}(M(\mathbb{F}_p))$ .

Our broad objective here is to refine the method of Chabauty–Coleman so that we can compute  $C^{(d)}(K)$  in many cases. Our achievements can be summarized as follows:

(I) Let  $v$  be a nonarchimedean prime of the number field  $K$ . Inspired by the aforementioned work of Klassen, we give an explicit criterion for an element

of  $C^{(d)}(K)$  to be the unique  $K$ -rational element in its residue class, for a given prime  $v$  (the residue classes are defined to be the fibres of the reduction map  $C^{(d)}(K_v) \rightarrow C^{(d)}(k_v)$ ). Here, unlike Klassen, we do not assume that  $d < \gamma$ . Just as in classical Chabauty, we need an assumption on the rank of the Mordell–Weil group: Our criterion requires that  $\text{rank } J(K) \leq g - d$ .

(II) We often expect, by applying the criterion of (I), to show that the fibres containing a  $K$ -rational element do not contain any other. This criterion however does not tell us anything about fibres that do not seem to contain  $K$ -rational elements. Thus, if the reduction map  $C^{(d)}(K) \rightarrow C^{(d)}(k_v)$  happens to be surjective, then it might be possible to use (I) to show that the known elements of  $C^{(d)}(K)$  are the only ones. But experience suggests that the reduction map is rarely surjective for  $d > 1$ . To prove that the known elements of  $C^{(d)}(K)$  are all its elements, we combine information given by our criterion using several well-chosen primes  $v_1, \dots, v_t$ .

(III) Suppose  $\varrho : C \rightarrow C'$  is a degree- $d$  morphism defined over  $K$ . Then  $\varrho^*C'(K)$  is a subset of  $C^{(d)}(K)$ . If  $C'$  has genus 0 or 1, then  $C'(K)$  can be infinite, and in this case  $\varrho^*C'(K)$  is an infinite subset of  $C^{(d)}(K)$ , and undoubtedly, the strategy of (I) and (II) fails. In this case we explain how the strategy of (I) and (II) can be suitably modified to compute  $C^{(d)}(K) \setminus \varrho^*C'(K)$ . Again we need a condition on the ranks of the Mordell–Weil groups; in the obvious notation, we require that  $\text{rank } J_C(K) - \text{rank } J_{C'}(K) \leq g_C - g_{C'} - d + 1$ .

Although we do not give theoretical bounds for  $C^{(d)}(K)$  in the way that Coleman [1985a] does for  $C(K)$ , we believe that our simplified explicit approach in (I) is a useful first step in this direction.

In the spirit of modern computations on curves of higher genus, we will not require explicit equations for  $C^{(d)}$ , but rather represent  $K$ -rational points on  $C^{(d)}$  as effective  $K$ -rational divisors of degree  $d$ . We suppose we have been supplied with a basis  $D_1, \dots, D_r$  for a subgroup of  $J(K)$  of full rank and hence finite index — the elements of this basis are represented as degree 0 divisors on  $C$  (modulo linear equivalence). Obtaining a basis for a subgroup of full rank is often the happy outcome of a successful descent calculation; see for example [Cassels and Flynn 1996; Flynn 1994; Poonen and Schaefer 1997; Schaefer 1995; Schaefer and Wetherell 2005; Stoll 1998; 2001; 2002]. Obtaining a basis for the full Mordell–Weil group is often time consuming for curves of genus 2 and simply not feasible in the present state of knowledge for curves of higher genus.

We illustrate our method by computing  $C^{(2)}(\mathbb{Q})$  for two curves  $C$  of genus 3. The first is a hyperelliptic curve, and the second a nonhyperelliptic plane quartic curve. It is noteworthy that in both examples  $C^{(2)}$  is a surface of general type, being birational to a  $\Theta$ -divisor on the Jacobian. Much less is known about the arithmetic of surfaces of general type than that of other surfaces.

Examples of papers that study rational points on symmetric powers of modular curves are [Kamienny 1986a; 1986b; 1992; Merel 1996; Parent 2000; 2003]; some that study rational points on symmetric powers of Fermat curves are [Debarre and Klassen 1994; Gross and Rohrlich 1978; Klassen and Tzermias 1997; Tzermias 1998, 2003; 2004; 2005]. It is our hope that the techniques explained in this paper will lead to useful progress in these directions.

## 2. Preliminaries

In this section we summarize various results on  $p$ -adic integration. The definitions and proofs can be found in [Coleman 1985b; Colmez 1998]. For an introduction to the ideas involved in Chabauty's method we warmly recommend Wetherell's thesis [1997] and the survey paper of McCallum and Poonen [2006], as well as Coleman's paper [1985a].

**Integration.** Let  $p$  be a rational prime and  $K_v$  be a finite extension of  $\mathbb{Q}_p$ . Let  $\mathbb{O}_v$  be the ring of integers in  $K_v$ , and let  $\mathbb{C}_v$  be the completion of its algebraic closure. Let  $\mathcal{W}$  be a smooth, proper connected scheme of finite type over  $\mathbb{O}_v$ , and write  $W$  for the generic fibre. Coleman [1985b, Section II] describes how to integrate “differentials of the second kind” on  $W$ . We shall however only be concerned with global 1-forms (that is, differentials of the first kind) and so shall restrict our attention to these. Among the properties of integration [loc. cit.] we shall need are

$$\begin{aligned} \int_P^Q \omega &= - \int_Q^P \omega, & \int_Q^P \omega + \int_P^R \omega &= \int_Q^R \omega, \\ \int_Q^P \alpha \omega &= \alpha \int_Q^P \omega, & \int_Q^P \omega + \int_Q^P \omega' &= \int_Q^P (\omega + \omega') \end{aligned} \quad (1)$$

for  $P, Q, R \in W(\mathbb{C}_v)$ , global 1-forms  $\omega, \omega'$  on  $W \times \mathbb{C}_v$ , and  $\alpha \in \mathbb{C}_v$ . We shall also need the “change of variables formula” [Coleman 1985b, Theorem 2.7]: If  $\mathcal{W}_1$  and  $\mathcal{W}_2$  are smooth, proper connected schemes of finite type over  $\mathbb{O}_v$  and  $\varrho : \mathcal{W}_1 \rightarrow \mathcal{W}_2$  is a morphism of their generic fibres, then

$$\int_Q^P \varrho^* \omega = \int_{\varrho(Q)}^{\varrho(P)} \omega \quad (2)$$

for all global 1-forms  $\omega$  on  $\mathcal{W}_2 \times \mathbb{C}_v$  and  $P, Q \in \mathcal{W}_1(\mathbb{C}_v)$ .

Now let  $A$  be an abelian variety of dimension  $g$  over  $K_v$ , and write  $\Omega_A$  for the  $K_v$ -space of global 1-forms on  $A$ . Consider the pairing

$$\Omega_A \times A(K_v) \rightarrow K_v, \quad (\omega, P) \mapsto \int_0^P \omega. \quad (3)$$

This pairing is bilinear. It is  $K_v$ -linear on the left by the bottom two equalities in (1). That it is also  $\mathbb{Z}$ -linear on the right is a straightforward consequence of the change of variables formula (2); see [Coleman 1985b, Theorem 2.8]. The kernel on the left is 0 and on the right is the torsion subgroup of  $A(K_v)$ ; see [Bourbaki 1989, III.7.6].

**Notation.** Henceforth we shall be concerned with curves over number fields and their Jacobians. Once and for all, we fix

$K$	a number field,
$C$	a smooth projective absolutely irreducible curve defined over $K$ , of genus $\geq 2$ ,
$C^{(d)}$	the $d$ -th symmetric power of $C$ ,
$J$	the Jacobian of $C$ ,
$v$	a nonarchimedean prime of $K$ , of good reduction for $C$ ,
$K_v$	the completion of $K$ at $v$ ,
$k_v$	the residue field of $K$ at $v$ ,
$\mathbb{O}_v$	the ring of integers in $K_v$ ,
$\mathcal{C}$	a minimal regular proper model for $C$ over $\mathbb{O}_v$ ,
$\tilde{C}$	the special fibre of $\mathcal{C}$ at $v$ ,
$\Omega_{C/K_v}$	the $K_v$ -vector space of global 1-forms on $C$ .

**Global 1-forms on curves and Jacobians.** For any field extension  $M/K$  (not necessarily finite), we shall write  $\Omega_{C/M}$  and  $\Omega_{J/M}$  for the  $M$ -vector spaces of global 1-forms on  $C/M$  and  $J/M$ , respectively. Corresponding to any  $P_0 \in C(\bar{K})$  is the Abel–Jacobi map

$$J : C \hookrightarrow J, \quad P \mapsto [P - P_0].$$

It is well known that the pull-back  $j^* : \Omega_{J/\bar{K}} \rightarrow \Omega_{C/\bar{K}}$  is an isomorphism; see [Milne 1986, Proposition 2.2]. Moreover any two Abel–Jacobi maps differ by a translation on  $J$ . Since 1-forms on  $J$  are translation invariant, the map  $j^*$  is independent of the choice of  $P_0$ ; see [Wetherell 1997, Section 1.4]. It is clear that  $j^*$  is defined over  $K$  if there is some  $K$ -rational point  $P_0$  on  $C$ . We however do not want to assume the existence of a  $K$ -rational point on  $C$ . Instead we shall make use of the following (well-known) result, for which we cannot find a reference.

**Proposition 2.1.** *With notation as above, the pull-back  $j^*$  induces an isomorphism  $\Omega_{J/K} \rightarrow \Omega_{C/K}$ .*

*Proof.* By smoothness there is a rational point on  $C$  defined over some finite Galois extension  $M/K$ . This induces an isomorphism  $j^* : \Omega_{J/M} \rightarrow \Omega_{C/M}$ . However, by independence of the choice of  $M$ -rational point, the isomorphism  $j^*$  is equivariant

under the action of  $\text{Gal}(M/K)$ , and hence descends to an isomorphism over the ground field  $K$ .  $\square$

**Integration on curves and Jacobians.** Suppose  $v$  is a nonarchimedean place for  $K$  of good reduction for  $C$ . Let  $J$  be the Abel–Jacobi corresponding to any  $P_0 \in C(\bar{K})$ . Proposition 2.1 asserts that the pull-back induces an isomorphism  $J^* : \Omega_{J/K} \rightarrow \Omega_{C/K}$  of global 1-forms defined over  $K$  (and independent of  $P_0$ ). This extends to an isomorphism  $\Omega_{J/K_v} \rightarrow \Omega_{C/K_v}$ , which we also denote by  $J^*$ . For any global 1-form  $\omega \in \Omega_{J/K_v}$  and any two points  $P, Q \in C(\mathbb{C}_v)$ , we have

$$\int_Q^P J^* \omega = \int_{JQ}^{JP} \omega = \int_0^{[P-Q]} \omega,$$

using the integration properties (1). We shall henceforth use  $J^*$  to identify  $\Omega_{C/K_v}$  with  $\Omega_{J/K_v}$ . With this identification, the pairing (3) with  $J = A$  gives the bilinear pairing

$$\Omega_{C/K_v} \times J(K_v) \rightarrow K_v, \quad (\omega, [\sum P_i - \sum Q_i]) \mapsto \sum \int_{Q_i}^{P_i} \omega, \quad (4)$$

whose kernel on the right is 0 and on the left is the torsion subgroup of  $J(K_v)$ . We ease notation a little by defining, for divisor class  $D = \sum P_i - Q_i$  of degree 0, the integral

$$\int_D \omega = \sum \int_{Q_i}^{P_i} \omega.$$

Note that this integral depends on the equivalence class of  $D$  and not on the decomposition as  $D = \sum P_i - Q_i$ . We shall need the following functorial property of integration of curves, for which we are unable to find a reference:

**Lemma 2.2.** *Suppose  $\varrho : C \rightarrow C'$  is a nonconstant morphism of curves defined over  $K$ , and let  $v$  be a nonarchimedean place of good reduction for both curves. Denote by  $\text{Tr}$  the corresponding trace map  $\Omega_{C/K_v} \rightarrow \Omega_{C'/K_v}$  on global 1-forms. If  $D$  is a degree 0 divisor on  $C'$  and  $\omega \in \Omega_{C/K_v}$  then*

$$\int_{\varrho^* D} \omega = \int_D \text{Tr } \omega.$$

*Proof.* First we assume that  $C/C'$  is geometrically Galois. Replacing  $K_v$  by a finite extension if necessary, we can assume that  $K_v(C)/K_v(C')$  is in fact Galois and contains the fields of definition of the points in  $\varrho^* D$ . Suppose that  $\varrho$  has degree  $d$ . Then the Galois group of  $C/C'$  is some set of automorphisms  $\{\sigma_1, \dots, \sigma_d\}$  where  $\sigma_i : C \rightarrow C$  is defined over  $K_v$  and commutes with  $\varrho$ . The virtue of assuming that  $C/C'$  is Galois is that the trace has a very simple formula in terms of the Galois group:  $\varrho^* \text{Tr } \omega = \sum \sigma_i^* \omega$ .

Now fix a degree 0 divisor  $D_0$  on  $C$  such that  $\varrho D_0 = D$ . Then  $\varrho^* D = \sum \sigma_i D_0$ , and

$$\int_{\varrho^* D} \omega = \sum_{i=1}^d \int_{\sigma_i D_0} \omega = \sum_{i=1}^d \int_{D_0} \sigma_i^* \omega = \int_{D_0} \varrho^* \text{Tr } \omega = \int_D \text{Tr } \omega.$$

where the second and fourth equalities use the change of variables formula (2). This proves the lemma in the geometrically Galois case. For the general case, we will need to work with the (geometric) Galois closure  $C''/C$  of  $C'/C$ . This is necessarily defined over some finite extension of  $K_v$ , so we again replace  $K_v$  by this finite extension. Consider now the following commutative diagram of curves.

$$\begin{array}{ccc} C'' & \xrightarrow{\epsilon} & C \\ & \searrow \delta & \downarrow \varrho \\ & & C' \end{array}$$

Both  $\epsilon$  and  $\delta$  are geometrically Galois and we may apply the lemma to them. Let  $D$  be a degree 0 divisor on  $C'$  and  $\omega$  a global 1-form on  $C$ . Applying the lemma to  $\delta$ , we see

$$\int_{\delta^* D} \epsilon^* \omega = \int_D \text{Tr}_{C''/C'}(\epsilon^* \omega) = \deg(\epsilon) \int_D \text{Tr}_{C/C'} \omega.$$

Likewise, applying the lemma to  $\epsilon$ , we get

$$\int_{\delta^* D} \epsilon^* \omega = \int_{\epsilon^* \varrho^* D} \epsilon^* \omega = \int_{\varrho^* D} \text{Tr}_{C''/C}(\epsilon^* \omega) = \deg(\epsilon) \int_{\varrho^* D} \omega.$$

Comparing the results of the last two calculations yields the desired conclusion.  $\square$

**Uniformizers.** The usual Chabauty approach when studying rational points in a residue class is to work with a local coordinate (defined shortly) and create power series equations in terms of the local coordinate whose solutions, roughly speaking, contain the rational points. In our situation we find it more convenient to shift the local coordinate so that it becomes a uniformizer at a rational point in the residue class. Fix a nonarchimedean prime  $v$  of good reduction for  $C$ , and a minimal regular proper model  $\mathcal{C}$  for  $C$  over  $v$ . Let  $Q \in C(K)$  and let  $\tilde{Q}$  be its reduction on the special fibre  $\tilde{C}$ . Choose a rational function  $s_Q \in K(C)$  so that its extension to a rational function on  $\mathcal{C}$  is a generator of the maximal ideal in  $\mathbb{O}_{\mathcal{C}, \tilde{Q}}$ ; the function  $s_Q$  is called in [Lorenzini and Tucker 2002, Section 1] a *local coordinate* at  $Q$ . Let  $t_Q = s_Q - s_Q(Q)$ .

**Lemma 2.3.** (i)  $t_Q$  is a uniformizer at  $Q$ .

(ii)  $\tilde{t}_Q$  is a uniformizer at  $\tilde{Q}$ .



- (iii) Let  $L_v$  be a finite extension of  $K_v$  with valuation ring  $\mathbb{O}_{L_v}$  and uniformizing element  $\pi$ . Then  $t_Q$  is regular and injective on  $\{P \in C(L_v) : \tilde{P} = \tilde{Q}\}$ . Indeed,  $t_Q$  defines a bijection between  $\{P \in C(L_v) : \tilde{P} = \tilde{Q}\}$  and  $\pi\mathbb{O}_{L_v}$ , given by  $P \mapsto t_Q(P)$ .

*Proof.* Parts (i) and (ii) are clear from the construction. Part (iii) is standard; see for example [Lorenzini and Tucker 2002, Section 1] or [Wetherell 1997, Sections 1.7 and 1.8].  $\square$

We shall refer to  $t_Q$ , constructed as above, as a *well-behaved uniformizer* at  $Q$ .

Now let  $Q \in C(\bar{K})$  and fix an extension of  $v$  to  $K(Q)$ . By a *well-behaved uniformizer*  $t_Q$  at  $Q$ , we mean an element  $t_Q \in K(Q)(C)$  that is a well-behaved uniformizer for the point  $Q$  on the curve  $C \times K(Q)$ .

**Evaluating integrals on curves.** Inside  $\Omega_{C/K_v}$  is the lattice  $\Omega_{\mathbb{C}/\mathbb{O}_v}$ . Let  $P$  and  $Q$  belong to  $C(K)$  and satisfy  $\tilde{P} = \tilde{Q}$ . Let  $\omega \in \Omega_{\mathbb{C}/\mathbb{O}_v}$ . Let  $t_Q \in K(C)$  be a well-behaved uniformizer at  $Q$ . We can expand  $\omega$  (after viewing it as an element in  $\Omega_{\hat{\mathbb{C}}_Q}$ ) as a formal power series as

$$\omega = (a_0 + a_1 t_Q + a_2 t_Q^2 + \cdots) dt_Q, \quad (5)$$

where the coefficients  $a_i$  are all integers in  $K_v$  (see for example [Lorenzini and Tucker 2002, Proposition 1.6] or [Wetherell 1997, Sections 1.7 and 1.8]); here we have not used the assumption that  $t_Q(Q) = 0$ , but instead merely that  $t_Q$  is a local coordinate at  $Q$ . We can now evaluate the integral (see for example [Lorenzini and Tucker 2002, Proposition 1.3])

$$\int_Q^P \omega = \sum_{i=0}^{\infty} \frac{a_{i+1}}{i+1} t_Q(P)^{i+1},$$

where the infinite series converges since  $|t_Q(P)| < 1$  by Lemma 2.3(iii).

### 3. Chabauty for a single residue class

As an algebraic variety, the  $d$ -th symmetric power  $C^{(d)}$  is the quotient of the  $d$ -th Cartesian power  $C^d$  by the action of the  $d$ -th symmetric group. We represent points of  $C^{(d)}(K)$  as unordered  $d$ -tuples  $\mathcal{P} = \{P_1, \dots, P_d\}$  such that  $P_i \in C(\bar{K})$  and  $\{P_1, \dots, P_d\}$  is invariant under the action of  $\text{Gal}(\bar{K}/K)$ . It is often useful to think of  $\mathcal{P} = \{P_1, \dots, P_d\}$  as a positive  $K$ -rational divisor on  $C$  of degree  $d$ . A useful reference on the geometry of symmetric powers of curves is [Milne 1986].

Let  $\text{red}_v : C^{(d)}(K_v) \rightarrow C^{(d)}(k_v)$  denote the reduction map. The *residue class* of  $\mathcal{P}$  in  $C^{(d)}(K_v)$  is defined as the fibre of the reduction map containing this  $d$ -tuple; in other words, it is the set  $\text{red}_v^{-1}(\text{red}_v(\mathcal{P}))$ . There are clearly only finitely many residue classes.

This section gives a criterion for a given  $\mathfrak{Q} \in C^{(d)}(K)$  to be the unique  $K$ -rational point in its residue class. Let  $V \subset \Omega_{C/K_v}$  be the annihilator of  $J(K) \subset J(K_v)$  under the pairing (4). Write

$$\mathcal{V} = V \cap \Omega_{\mathbb{C}/\mathbb{C}_v}.$$

**Lemma 3.1.**  $\mathcal{V}$  is a free  $\mathbb{C}_v$ -module of rank at least  $g - \text{rank } J(K)$ .

*Proof.* This is a standard observation. It suffices to show that  $\dim_{K_v} V \geq g - s$ , where  $s$  is the rank of  $J(K)$ . Recall that torsion belongs to the kernel of the pairing (4) on the right. Let  $D_1, \dots, D_s$  be a Mordell–Weil basis for  $J(K)$  modulo torsion. Then a global 1-form  $\omega \in \Omega_{C/K_v}$  belongs to  $V$  if and only if it annihilates  $D_1, \dots, D_s$ . Thus  $V$  is a subspace of  $\Omega_{C/K_v}$  defined by  $s$  (not necessarily independent)  $K_v$ -linear conditions. Since the dimension of  $\Omega_{C/K_v}$  is  $g$ , the lemma follows.  $\square$

Let  $\omega \in \Omega_{\mathbb{C}/\mathbb{C}_v}$ . Let  $Q \in C(\bar{K})$ ; fix an extension of  $v$  to  $K(Q)$  and denote it also by  $v$ . Let  $t_Q \in K(Q)(C)$  be a well-behaved uniformizer at the point  $Q$ . Expand  $\omega$  as in (5), where the coefficients  $a_i$  are integers in  $K(Q)_v$ . For a positive integer  $m$ , define

$$\mathbf{v}(\omega, t_Q, m) = (a_0, \tfrac{1}{2}a_1, \tfrac{1}{3}a_2, \dots, \tfrac{1}{m}a_{m-1}). \quad (6)$$

Now let  $\omega_1, \dots, \omega_r$  be an  $\mathbb{C}_v$ -basis for  $\mathcal{V}$ , and let  $\mathfrak{Q}$  be an element of  $C^{(d)}(K)$ . The unordered  $d$ -tuple  $\mathfrak{Q}$  may have some repetition in it, and we need to take a careful account of that possibility. At this point it will be convenient to identify  $C^{(d)}(K)$  with the set of effective  $K$ -rational divisors of degree  $d$ . Thus we can write

$$\mathfrak{Q} = \sum_{j=1}^l d_j Q_j, \quad (7)$$

where  $Q_1, Q_2, \dots, Q_l$  are distinct and  $d_j > 0$ . We call  $d_j$  the *multiplicity* of  $Q_j$  in  $\mathfrak{Q}$ . Note that  $d = d_1 + d_2 + \dots + d_l$ . Let  $L = K(Q_1, \dots, Q_l)$  and fix an extension of  $v$  to  $L$ , which we also denote by  $v$ . Let  $\mathcal{A}$  be the  $r \times d$  matrix

$$\mathcal{A} = \begin{pmatrix} \mathbf{v}(\omega_1, t_{Q_1}, d_1) & \mathbf{v}(\omega_1, t_{Q_2}, d_2) & \cdots & \mathbf{v}(\omega_1, t_{Q_l}, d_l) \\ \mathbf{v}(\omega_2, t_{Q_1}, d_1) & \mathbf{v}(\omega_2, t_{Q_2}, d_2) & \cdots & \mathbf{v}(\omega_2, t_{Q_l}, d_l) \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}(\omega_r, t_{Q_1}, d_1) & \mathbf{v}(\omega_r, t_{Q_2}, d_2) & \cdots & \mathbf{v}(\omega_r, t_{Q_l}, d_l) \end{pmatrix}. \quad (8)$$

The main objective of this section is to prove the following theorem.

**Theorem 3.2.** Suppose  $C$  is a smooth projective curve of genus  $g \geq 2$  over a number field  $K$ , and write  $J$  for the Jacobian of  $C$ . Let  $d$  be a positive integer and  $\mathfrak{Q}$  an element of  $C^{(d)}(K)$ . Write  $\mathfrak{Q}$  as in (7) with  $Q_1, Q_2, \dots, Q_l$  distinct, having positive multiplicities  $d_1, d_2, \dots, d_l$ . Let  $v$  be a nonarchimedean prime of  $K$ , and let  $p$  be the rational prime below  $v$ . Write  $k_v$  for the residue field of  $v$ . Write  $e$  for

the ramification index of  $v/p$  in  $K/\mathbb{Q}$ . Fix an extension of  $v$  to  $K(Q_1, \dots, Q_l)$ , which we also denote by  $v$ . Write  $e_j$  for the ramification index of  $v$  in  $K(Q_j)/K$ , and let  $f_j := [k_v(\tilde{Q}_j) : k_v]$ . Let

$$N = e \cdot \max\{\text{lcm}(e_j, b) : 1 \leq j \leq l, 1 \leq b \leq d/f_j\}. \quad (9)$$

Suppose

- (i)  $v$  is a prime of good reduction for  $C$ ,
- (ii)  $p > d_1, d_2, \dots, d_l$ , and
- (iii)  $\text{ord}_p(d_j + i + 1) \leq i/N$  for all  $i \geq 0$  and  $1 \leq j \leq l$ .

Let  $\omega_1, \dots, \omega_r$  be an  $\mathbb{O}_v$ -basis for  $\mathcal{V}$  (defined as above), and  $\mathcal{A}$  be the  $r \times d$  matrix associated with the  $\omega_i$  and  $\mathcal{Q}$  as in (8). Write  $\tilde{\mathcal{A}}$  for the reduction of  $\mathcal{A}$  with entries in  $\bar{k}_v$ . If  $\tilde{\mathcal{A}}$  has rank  $d$ , then the point  $\mathcal{Q}$  is the unique element in its residue class belonging to  $C^{(d)}(K)$ .

**Remarks.** (a) The matrix  $\tilde{\mathcal{A}}$  has dimension  $r \times d$ , where  $r$  is the  $\mathbb{O}_v$ -rank of  $\mathcal{V}$ . It is evident that a necessary condition for the success of the criterion in the theorem is  $r \geq d$ . Evaluating the precise value of  $r$  is difficult, though by Lemma 3.1 we know that  $r \geq g - \text{rank } J(K)$ . Hence it is sensible to apply the theorem when  $\text{rank } J(K) \leq g - d$ .

(b) We note the following useful simplification in the case where  $d_1 = d_2 = \dots = d_l = 1$  (that is  $\mathcal{Q} = \{Q_1, Q_2, \dots, Q_d\}$  with the  $Q_j$  distinct). Then  $\mathcal{A} = (\alpha_{ij})$  is the  $r \times d$  matrix with entries given by

$$\alpha_{ij} = \frac{\omega_i}{dt_{Q_j}} \Big|_{t_{Q_j}=0}.$$

(c) At first glance it seems that hypothesis (iii) of the theorem requires checking an infinite list of inequalities, though this is not the case. To see this, fix  $1 \leq j \leq l$  and let  $i_0$  be the first value of  $i$  such that

$$u(i) := \frac{i}{N} - \log_p(d_j + i + 1) \geq 0 \quad \text{and} \quad v(i) := \frac{1}{N} - \frac{1}{(d_j + i + 1) \log p} \geq 0.$$

But  $v = du/di$ ; thus  $u$  is a nondecreasing function on  $i \geq i_0$ . So

$$\frac{i}{N} \geq \log_p(d_j + i + 1) \geq \text{ord}_p(d_j + i + 1) \quad \text{for all } i \geq i_0.$$

Hence we need only check the inequality  $i/N \geq \text{ord}_p(d_j + i + 1)$  for  $0 \leq i < i_0$ .

(d) Our theorem should be related to [Klassen 1993, Proposition 11]. Klassen assumes that  $d$  is strictly less than the gonality, and so he is able to identify  $C^{(d)}$  with its image  $W^{(d)}$  on the Jacobian. He works with local parameters on  $W^{(d)}$  instead of local parameters on the curve as we do. Moreover he phrases his criterion

in terms of wedge products of 1-forms. We have not attempted to evaluate the precise overlap between our theorem and Klassen's. We expect that in the case where  $d$  is strictly less than the gonality and the multiplicities of  $\mathcal{Q}$  are all 1, some variant of our theorem above may be deduced from Klassen's result. We are not at all confident that such a deduction is possible if these restrictions are not assumed.

(e) There is one striking difference between our approach and Klassen's: power series obtained through our method do not contain any mixed terms. Our power series equations are of the form  $\sum_{j=1}^d f_{i,j}(z_j) = 0$  for  $i = 1, \dots, r$ , with  $f_{i,j}(z_j)$  being a power series in  $z_j$ . By the absence of mixed terms, we mean that our power series do not contain any terms that involve more than one unknown. We believe that these simpler power series should be useful in proving effective bounds for the number of points on  $C^{(d)}(K)$ , similar to Coleman's bounds [1985a] for  $C(K)$ .

*Proof of Theorem 3.2.* We continue with the notation of Theorem 3.2. Suppose that  $\mathcal{Q}$  shares its residue class with  $\mathcal{P} \in C^{(d)}(K)$ . Our objective is to show that the two  $d$ -tuples are equal. Let  $L$  be the extension of  $K$  generated by the supports of the divisors  $\mathcal{P}$  and  $\mathcal{Q}$ . In the statement of the theorem we fixed an extension  $v$  to  $K(Q_1, \dots, Q_l)$ , which we denoted also by  $v$ . We now fix a further extension of  $v$  to  $L$  (compatible with the earlier extension to  $K(Q_1, \dots, Q_l)$ ), and also denote it by  $v$ . Let  $L_v/K_v$  be the corresponding extension of local fields, and write  $\mathbb{O}_{L,v}$  for the integers of  $L_v$ . We normalize  $|\cdot|_v$  in the usual way, requiring  $|p|_v = p^{-1}$ . Without loss of generality we can rewrite

$$\mathcal{P} = \sum_{j=1}^l \sum_{j'=1}^{d_j} P_{j,j'}, \quad \text{where } \tilde{P}_{j,j'} = \tilde{Q}_j \text{ for } j = 1, \dots, l.$$

Suppose  $\omega \in \mathcal{V}$ . Then  $\mathcal{P} - \mathcal{Q}$  is a divisor of degree 0 and yields an element of  $J(K)$ . Since  $\mathcal{V}$  is orthogonal to  $J(K)$  with respect to the pairing (4), we obtain  $\int_{\mathcal{P}-\mathcal{Q}} \omega = 0$ . We may rewrite this as

$$\sum_{j=1}^l \sum_{j'=1}^{d_j} \int_{Q_j}^{P_{j,j'}} \omega = 0. \quad (10)$$

As before, we choose  $t_{Q_j} \in K(Q_j)(C)$  to be well-behaved uniformizers at  $Q_j$ . Let  $z_{j,j'} = t_{Q_j}(P_{j,j'})$ . We note the following:

- (a)  $|z_{j,j'}|_v < 1$ . This follows from Lemma 2.3(iii) as  $P_{j,j'}$  belongs to the residue class of  $Q_j$ .
- (b)  $|z_{j,j'}|_v \leq 1/p^{1/N}$ , where  $N$  is given by (9). Let  $L_{j,j'} = K(Q_j, P_{j,j'})$ , which contains  $z_{j,j'}$ . Since  $|z_{j,j'}|_v < 1$ , all we have to show is that  $v$  has ramification index at most  $N$  in  $L_{j,j'}/\mathbb{Q}$ . Recall that the ramification index for  $v$  in  $K/\mathbb{Q}$

is  $e$ . Hence it is enough to show that the ramification index of  $v$  in  $L_{j,j'}/K$  is at most  $\text{lcm}(e_j, b)$  for some  $1 \leq b \leq d/f_j$ . The ramification index for  $v$  in  $L_{j,j'}/K$  is at most the least common multiple of the ramification indices for  $v$  in  $K(Q_j)/K$  and  $K(P_{j,j'})/K$ . The former is denoted by  $e_j$  in the theorem. The latter is at most  $d/f_j$  since the extension  $K(P_{j,j'})/K$  has degree at most  $d$ , and the corresponding residue field extension is  $k_v(\tilde{Q}_j)/k_v$ , whose degree was denoted by  $f_j$ .

(c)  $z_{j,j'} = 0$  if and only if  $Q_j = P_{j,j'}$ . This again follows from Lemma 2.3(iii).

We will show that all  $z_{j,j'} = 0$ , and then  $\mathcal{P} = \mathcal{Q}$  as required. Now fix some  $j$  and expand  $\omega$  in terms of  $t_{Q_j}$  to obtain

$$\omega = (a_0 + a_1 t_{Q_j} + a_2 t_{Q_j}^2 + \cdots) dt_{Q_j},$$

where the  $a_i$  lie in  $\mathbb{O}_{L,v}$  (page 216, middle). Integrating, we obtain

$$\begin{aligned} \int_{Q_j}^{P_{j,j'}} \omega &= \int_0^{z_{j,j'}} (a_0 + a_1 t_{Q_j} + a_2 t_{Q_j}^2 + \cdots) dt_{Q_j} = a_0 z_{j,j'} + \frac{1}{2} a_1 z_{j,j'}^2 + \cdots \\ &= \mathbf{v}(\omega, t_{Q_j}, d_j) \cdot \begin{pmatrix} z_{j,j'} \\ z_{j,j'}^2 \\ \vdots \\ d_j \\ z_{j,j'} \end{pmatrix} + z_{j,j'}^{d_j+1} \left( \frac{a_{d_j}}{d_j+1} + \frac{a_{d_j+1} z_{j,j'}}{d_j+2} + \cdots \right). \end{aligned} \quad (11)$$

where  $\mathbf{v}(\omega, t_{Q_j}, d_j)$  is as in (6). Note that hypothesis (ii) of the theorem ensures that the entries of  $\mathbf{v}(\omega, t_{Q_j}, d_j)$  belong to  $\mathbb{O}_{L,v}$ . Moreover, by hypothesis (iii) and observation (b) above, we see that

$$\left( \frac{a_{d_j}}{d_j+1} + \frac{a_{d_j+1} z_{j,j'}}{d_j+2} + \cdots \right) \in \mathbb{O}_{L,v}.$$

Let  $\pi$  be a uniformizing element of  $L_v$ . Let  $\text{ord}_\pi : L_v \rightarrow \mathbb{Z} \cup \{\infty\}$  be the normalized valuation corresponding to  $\pi$ . Write

$$m_j = \min_{j'=1, \dots, d_j} \text{ord}_\pi(z_{j,j'}) \quad \text{for } j = 1, \dots, l. \quad (12)$$

Without loss of generality, we may suppose that

$$m_1(d_1+1) \leq m_2(d_2+1) \leq \cdots \leq m_l(d_l+1).$$

We will show that  $m_1 = \infty$ ; thus all  $m_j = \infty$  and so all  $z_{j,j'} = 0$ , completing our proof. Thus suppose that  $m_1 < \infty$ .

We obtain from (11)

$$\int_{Q_j}^{P_{j,j'}} \omega \equiv \mathbf{v}(\omega, t_{Q_j}, d_j) \cdot \begin{pmatrix} z_{j,j'} \\ z_{j,j'}^2 \\ \vdots \\ z_{j,j'}^{d_j} \end{pmatrix} \pmod{\pi^{m_1(d_1+1)}}, \quad (13)$$

for all  $j, j'$ . Write

$$\mathbf{z}_j = \begin{pmatrix} z_{j,1} + z_{j,2} + \cdots + z_{j,d_j} \\ z_{j,1}^2 + z_{j,2}^2 + \cdots + z_{j,d_j}^2 \\ \vdots \\ z_{j,1}^{d_j} + z_{j,2}^{d_j} + \cdots + z_{j,d_j}^{d_j} \end{pmatrix} \quad \text{for } j = 1, \dots, l.$$

From (10) and (13) we deduce that

$$\sum_{j=1}^l \mathbf{v}(\omega, t_{Q_j}, d_j) \cdot \mathbf{z}_j \equiv 0 \pmod{\pi^{m_1(d_1+1)}}. \quad (14)$$

For  $\mathbf{z} \in (\mathbb{O}_{L,v})^d$ , write  $\mathbf{z} = (z_1 \ z_2 \ \cdots \ z_l)^T$ . From (14) we obtain

$$(\mathbf{v}(\omega, t_{Q_1}, d_1), \dots, \mathbf{v}(\omega, t_{Q_l}, d_l)) \cdot \mathbf{z} \equiv 0 \pmod{\pi^{m_1(d_1+1)}}.$$

This is true for  $\omega_1, \omega_2, \dots, \omega_r$  in place of  $\omega$ . So plainly (from the definition of  $\mathcal{A}$  in (8)) we have  $\mathcal{A}\mathbf{z} \equiv \mathbf{0} \pmod{\pi^{m_1(d_1+1)}}$ . However,  $\mathbf{z} \in (\mathbb{O}_{L,v})^d$ , where  $\mathbb{O}_{L,v}$  are the integers of  $L_v$ . Moreover, we assume in the statement of the theorem that the reduction  $\tilde{\mathcal{A}}$  of  $\mathcal{A}$  modulo  $\pi$  has rank  $d$ . Hence  $\mathbf{z} \equiv \mathbf{0} \pmod{\pi^{m_1(d_1+1)}}$ . From the definition of  $\mathbf{z}$  we obtain  $z_1 \equiv \mathbf{0} \pmod{\pi^{m_1(d_1+1)}}$  or equivalently

$$\begin{aligned} z_{1,1} + z_{1,2} + \cdots + z_{1,d_1} &\equiv 0 \pmod{\pi^{m_1(d_1+1)}}, \\ z_{1,1}^2 + z_{1,2}^2 + \cdots + z_{1,d_1}^2 &\equiv 0 \pmod{\pi^{m_1(d_1+1)}}, \\ &\vdots \\ z_{1,1}^{d_1} + z_{1,2}^{d_1} + \cdots + z_{1,d_1}^{d_1} &\equiv 0 \pmod{\pi^{m_1(d_1+1)}}. \end{aligned}$$

By Lemma 3.4 below, we see that  $z_{1,1} \equiv z_{1,2} \equiv \cdots \equiv z_{1,d_1} \equiv 0 \pmod{\pi^{m_1+1}}$ ; in applying Lemma 3.4 we needed that  $p > d_1$ , which is given by hypothesis (ii) of the theorem. This contradicts the definition of  $m_1$  in (12). The source of the contradiction is our assumption that  $m_1 < \infty$ . Thus  $m_1 = \infty$ .  $\square$

**Lemma 3.3.** *Suppose  $L_\kappa$  is a nonarchimedean local field of characteristic 0 with ring of integers  $\mathbb{O}_\kappa$  and uniformizing element  $\pi$ . Suppose  $\pi \mid p$  for a rational*

prime  $p$ . Let  $h < p$  be a positive integer, and suppose that  $z_1, \dots, z_h \in \mathbb{O}_\kappa$  satisfy

$$\begin{aligned} z_1 + z_2 + \dots + z_h &\equiv 0 \pmod{\pi}, \\ z_1^2 + z_2^2 + \dots + z_h^2 &\equiv 0 \pmod{\pi}, \\ &\vdots \\ z_1^h + z_2^h + \dots + z_h^h &\equiv 0 \pmod{\pi}. \end{aligned}$$

Then  $z_1 \equiv z_2 \equiv \dots \equiv z_h \equiv 0 \pmod{\pi}$ .

*Proof.* The proof is by easy induction on  $h$ . The keys to the proof are Newton's identities [Garling 1986, page 113], which imply that  $hz_1z_2\dots z_h \equiv 0 \pmod{\pi}$ . Since  $h < p$  we obtain that  $z_j \equiv 0 \pmod{\pi}$  for some  $j$ , allowing us to reduce to the  $h - 1$  case.  $\square$

**Lemma 3.4.** Suppose  $L_\kappa$  is a nonarchimedean local field of characteristic 0 with ring of integers  $\mathbb{O}_\kappa$  and uniformizing element  $\pi$ . Suppose  $\pi \mid p$  for a rational prime  $p$ . Let  $h < p$  be a positive integer, and suppose that  $z_1, \dots, z_h \in \mathbb{O}_\kappa$  satisfy

$$\begin{aligned} z_1 + z_2 + \dots + z_h &\equiv 0 \pmod{\pi^{m+1}}, \\ z_1^2 + z_2^2 + \dots + z_h^2 &\equiv 0 \pmod{\pi^{2m+1}}, \\ &\vdots \\ z_1^h + z_2^h + \dots + z_h^h &\equiv 0 \pmod{\pi^{hm+1}}, \end{aligned}$$

where  $m \geq 0$ . Then  $z_1 \equiv z_2 \equiv \dots \equiv z_h \equiv 0 \pmod{\pi^{m+1}}$ .

*Proof.* By the previous lemma,  $z_1 \equiv z_2 \equiv \dots \equiv z_h \equiv 0 \pmod{\pi}$ . Suppose that  $z_1 \equiv z_2 \equiv \dots \equiv z_h \equiv 0 \pmod{\pi^r}$  where  $1 \leq r \leq m$ . Let  $z'_i = \pi^{-r}z_i$ . Then  $z'_i \in \mathbb{O}_\kappa$ , and the previous lemma again applies with  $z'_i$  in place of the  $z_i$ . Hence  $z'_i \equiv 0 \pmod{\pi}$ , giving  $z_i \equiv 0 \pmod{\pi^{r+1}}$ .  $\square$

#### 4. A relative version of Chabauty for covers of curves

Suppose that  $\varrho : C \rightarrow C'$  is a morphism of curves of degree  $d$  defined over a number field  $K$ . Then  $\varrho^*C'(K)$  is subset of  $C^{(d)}(K)$ . If  $C'(K)$  is infinite, then so is  $C^{(d)}(K)$ . We know, thanks to Faltings's theorem, that  $C'(K)$  can be infinite only if the genus of  $C'$  is 0 or 1. If  $C'(K)$  is infinite, then some residue classes of  $C^{(d)}$  will contain infinitely many  $K$ -rational points, and the criterion of Theorem 3.2 is bound to fail for these residue classes. In this situation it is indeed more natural to ask if a given residue class of  $C^{(d)}$  contains  $K$ -rational points not belonging to  $\varrho^*C'(K)$ . In this section we give a criterion for a given residue class in  $C^{(d)}(K)$  to contain only elements of  $\varrho^*C'(K)$ .

Let  $v$  be a nonarchimedean prime of good reduction for both  $C$  and  $C'$ . To ease notation we shall write  $\Omega_C$  and  $\Omega_{C'}$  for the global 1-forms on  $C/K_v$  and  $C'/K_v$ , and let  $\text{Tr} : \Omega_C \rightarrow \Omega_{C'}$  be the trace map. Write  $\Omega_0$  for the kernel of this trace map.

**Lemma 4.1.**  $\Omega_0$  has dimension  $g_C - g_{C'}$ , where  $g_C$  (respectively  $g_{C'}$ ) is the genus of  $C$  (respectively  $C'$ ). Moreover,  $\Omega_C = \varrho^*(\Omega_{C'}) \oplus \Omega_0$ .

*Proof.* The lemma follows from the fact that the trace map is surjective: if  $\omega \in \Omega_{C'}$ , then  $\text{Tr}((1/d)\varrho^*\omega) = \omega$ .  $\square$

Let  $\mathcal{V}$  be as in the previous section, and let  $\mathcal{V}_0 = \Omega_0 \cap \mathcal{V}$ . Thus the 1-forms belonging to  $\mathcal{V}_0$  enjoy two properties; the first is that their trace is 0 with respect to  $\varrho$ , and the second is that they are orthogonal to the Mordell–Weil group  $J(K)$  with respect to the pairing (4).

**Lemma 4.2.** With notation as above,  $\mathcal{V}_0$  is a free  $\mathbb{O}_v$ -module satisfying

$$\text{rank}_{\mathbb{O}_v} \mathcal{V}_0 \geq (g_C - g_{C'}) - (\text{rank } J_C(K) - \text{rank } J_{C'}(K)).$$

*Proof.* The pairing (4) restricts to a bilinear pairing  $\Omega_0 \times J_C(K_v) \rightarrow K_v$ . Let  $\Omega'$  be the annihilator of  $J_C(K)$  with respect to this pairing. Then  $\mathcal{V}_0 = \Omega' \cap \Omega_{\mathbb{C}/\mathbb{O}_v}$ . It is sufficient to show that

$$\dim_{K_v} \Omega' \geq (g_C - g_{C'}) - (\text{rank } J_C(K) - \text{rank } J_{C'}(K)).$$

However, by Lemma 2.2 the pairing is trivial on  $\varrho^*J_{C'}(K)$ . By Lemma 4.1, the  $K_v$ -dimension of  $\Omega_0$  is  $g_C - g_{C'}$ . Thus

$$\dim_{K_v} \Omega' \geq (g_C - g_{C'}) - \text{rank}(J_C(K)/\varrho^*J_{C'}(K)).$$

The lemma follows at once by observing that the kernel of  $\varrho^* : J_{C'} \rightarrow J_C$  contains only torsion (since  $\varrho_* \circ \varrho^* = \deg(\varrho)$ ), so that

$$\text{rank}(J_C(K)/\varrho^*J_{C'}(K)) = \text{rank } J_C(K) - \text{rank } J_{C'}(K). \quad \square$$

**Theorem 4.3.** With notation as above, let  $\mathcal{Q} = \sum_{j=1}^d \mathcal{Q}_j$  be an element of  $\varrho^*C'(K)$ . Let  $v$  be a nonarchimedean prime of  $K$ , of good reduction for  $C$  and  $C'$ , and let  $p$  be the rational prime below  $v$ . Write  $k_v$  for the residue field of  $v$ . Write  $e$  for the ramification index of  $v/p$  in  $K/\mathbb{Q}$ . Fix an extension of  $v$  to  $K(Q_1, \dots, Q_d)$ , which we also denote by  $v$ . Write  $e_j$  for the ramification index of  $v$  in  $K(Q_j)/K$ , and let  $f_j := [k_v(\tilde{Q}_j) : k_v]$ . Let

$$N' = e \cdot \max \{ \text{lcm}(e_j, b) : 1 \leq j \leq d, 1 \leq b \leq d(d-1)/f_j \}. \quad (15)$$

Suppose  $\text{ord}_p(i+1) < i/N'$  for all  $i \geq 0$ . Let  $t_j \in K(Q_j)(C)$  be a well-behaved uniformizer at  $Q_j$ . Let  $\omega_1, \omega_2, \dots, \omega_s$  be a basis for  $\mathcal{V}_0$ . Let  $\mathcal{A} = (\alpha_{i,j})$  be the



$s \times (d-1)$  matrix with entries

$$\alpha_{i,j} = \frac{\omega_i}{dt_j} \Big|_{t_j=0}, \quad \text{for } i = 1, \dots, s \text{ and } j = 2, \dots, d.$$

If the reduced matrix  $\tilde{\mathcal{A}}$  with entries in  $\bar{k}_v$  has rank  $d-1$ , then any element of  $C^{(d)}(K)$  belonging to the residue class of  $\mathcal{Q}$  does in fact belong to  $\varrho^* C'(K)$ .

**Remark.** For the criterion in the theorem to succeed, a necessary condition is  $s \geq d-1$ , where  $s$  is the  $\mathbb{O}_v$ -rank of  $\mathcal{V}_0$ . Considering Lemma 4.2, it is sensible to apply the theorem when

$$\text{rank } J_C(K) - \text{rank } J_{C'}(K) \leq g_C - g_{C'} - d + 1.$$

*Proof of Theorem 4.3.* We are supposing  $\mathcal{Q} = \sum_{j=1}^d Q_j$  is some element of  $\varrho^* C'(K)$  and  $\mathcal{P} = \sum_{j=1}^d P_j$  shares its residue class. We reorder the  $P_j$  so that  $\tilde{P}_j = \tilde{Q}_j$ . Let  $\mathcal{P}' = \varrho^* \varrho P_1$  and write  $\mathcal{P}' = \sum_{j=1}^d P'_j$ , where  $P'_1 = P_1$  and  $\tilde{P}'_j = \tilde{P}_j = \tilde{Q}_j$  for  $j = 2, \dots, d$ .

We want to show that  $\mathcal{P} \in \varrho^* C'(K)$ . We claim it suffices to show that  $P_j = P'_j$  for  $j = 2, \dots, d$ . Suppose for the moment this holds. Then  $\varrho P_j = \varrho P_1$  for  $j = 1, \dots, d$ . But the set  $\{P_1, \dots, P_d\}$  is stable under the action of  $\text{Gal}(\bar{K}/K)$ . Hence  $\varrho P_1$  is fixed by the action of Galois and so is in  $C'(K)$ , establishing our claim.

To show that  $P_j = P'_j$  for  $j = 2, \dots, d$ , we need to modify the Chabauty strategy used in the proof of Theorem 3.2. Let  $\omega \in \mathcal{V}_0$ . As before

$$\int_{\mathcal{P}-\mathcal{Q}} \omega = 0, \quad \text{so} \quad 0 = \int_{\mathcal{P}-\mathcal{P}'} \omega + \int_{\mathcal{P}'-\mathcal{Q}} \omega.$$

However,

$$\int_{\mathcal{P}'-\mathcal{Q}} \omega = \int_{\varrho^*(\varrho P_1 - \varrho Q_1)} \omega = \int_{\varrho P_1 - \varrho Q_1} \text{Tr } \omega = 0,$$

where we have used Lemma 2.2 and the fact that  $\omega \in \mathcal{V}_0 \subset \Omega_0$ , so its trace vanishes.

We deduce that

$$0 = \int_{\mathcal{P}-\mathcal{P}'} \omega = \sum_{j=2}^d \int_{P'_j}^{P_j} \omega.$$

Recall that  $t_j$  was chosen as a well-behaved uniformizer at  $Q_j$  and that  $P_j$  and  $P'_j$  belong to the residue class at  $Q_j$ . Let  $z_j = t_j(P_j)$  and  $z'_j = t_j(P'_j)$ . We will show that  $z_j = z'_j$  for  $j = 2, \dots, d$ . Once this is done, Lemma 2.3 implies that  $P_j = P'_j$ , as required.

Now we may as before expand  $\omega = (\alpha_j + \beta_j t_j + \gamma_j t_j^2 + \dots) dt_j$ , where the coefficients are integral. We obtain

$$0 = \sum_{j=2}^d \int_{P'_j}^{P_j} \omega = \sum_{j=2}^d \alpha_j (z_j - z'_j) + \frac{1}{2} \beta_j (z_j^2 - z'^2_j) + \frac{1}{3} \gamma_j (z_j^3 - z'^3_j) + \dots,$$

and so

$$\sum_{j=2}^d \alpha_j(z_j - z'_j) = \sum_{j=2}^d (z'_j - z_j) \left( \frac{1}{2} \beta_j(z_j + z'_j) + \frac{1}{3} \gamma_j(z_j^2 + z_j z'_j + z_j'^2) + \cdots \right). \quad (16)$$

Let  $L$  be the finite extension of  $K$  generated by the  $Q_j$ ,  $P_j$  and  $P'_j$ . In the statement of the theorem, we chose an extension of  $v$  to  $K(Q_1, \dots, Q_d)$ , which we also denoted by  $v$ . We now extend  $v$  to  $L$  in a way that is compatible with the earlier extension to  $K(Q_1, \dots, Q_d)$ , and we continue to denote it by  $v$ . Let  $\pi$  be a uniformizing element of  $L_v$ . Let

$$m = \min_{j=2, \dots, d} \text{ord}_\pi(z_j - z'_j).$$

We would like to show that  $m = \infty$  and so  $z_j = z'_j$  for all  $j$ . We suppose  $m < \infty$ , aiming for a contradiction. We will show shortly that

$$|z_j|_v \leq 1/p^{1/N'}, \quad |z'_j|_v \leq 1/p^{1/N'} \quad \text{for } j = 2, \dots, d, \quad (17)$$

where  $N'$  is given by (15); let us assume this for the moment. One of the hypotheses of the theorem is that  $\text{ord}_p(i+1) < i/N'$  for all  $i \geq 0$ . Hence

$$|z_j^i/(i+1)|_v < 1, \quad |z'_j{}^i/(i+1)|_v < 1 \quad \text{for } i \geq 0 \text{ and } j = 2, \dots, d.$$

Hence  $\frac{1}{2}(z_j + z'_j) \equiv \frac{1}{3}(z_j^2 + z_j z'_j + z_j'^2) \equiv \cdots \equiv 0 \pmod{\pi}$ . Since  $z_j \equiv z'_j \pmod{\pi^m}$ , Equation (16) shows that

$$\sum_{j=2}^d \alpha_j(z_j - z'_j) \equiv 0 \pmod{\pi^{m+1}}.$$

If  $\omega = \omega_i$ , we see that  $\alpha_j$  is precisely what is called  $\alpha_{i,j}$  in the statement of the theorem. Hence we obtain

$$\sum_{j=2}^d \alpha_{i,j}(z_j - z'_j) \equiv 0 \pmod{\pi^{m+1}} \quad \text{for } i = 1, \dots, s.$$

Let  $w_j = (z_j - z'_j)/\pi^m$ . Then  $w_j \in \mathbb{G}_{L,v}$ . Also  $\mathcal{A}(w_2 \cdots w_d)^T \equiv 0 \pmod{\pi}$ . Because  $\tilde{\mathcal{A}}$  has rank  $d-1$ , we see that all the  $w_j \equiv 0 \pmod{\pi}$ , and therefore  $z_j \equiv z'_j \pmod{\pi^{m+1}}$  for all  $j$ . This contradicts the definition of  $m$  above, and shows that  $m = \infty$  as required.

Our proof is complete except for claim (17). Naturally  $|z_j|_v < 1$  and  $|z'_j|_v < 1$ . Also,  $z_j$  and  $z'_j$  are contained in  $L_j = K(Q_j, P_j)$  and  $L'_j = K(Q_j, P'_j)$ . Thus it is sufficient to show that the ramification index in these fields is at most  $N'$ . Let us do this for  $L'_j$ ; the corresponding proof for  $L_j$  is easier. The ramification index for  $v$  in  $K/\mathbb{Q}$  is  $e$ . The ramification index of  $v$  in  $L'_j/K$  is the least common multiple of

its ramification index in  $K(Q_j)/K$  and  $K(P'_j)/K$ . The former ramification index is denoted by  $e_j$  in the statement of the theorem. We will see shortly that the field extension  $K(P'_j)/K$  has degree at most  $d(d-1)$ ; we know that the corresponding residue field extension is simply  $k_v(\tilde{Q}_j)/k_v$ , whose degree was denoted by  $f_j$ . Hence the ramification index for  $K(P'_j)/K$  is at most  $d(d-1)/f_j$ . Putting this together, it only remains to show that the degree  $[K(P'_j) : K]$  is at most  $d(d-1)$ . Now  $[K(P_1) : K] \leq d$  since  $P_1$  belongs to the rational  $d$ -tuple  $\mathcal{P}$ . The  $P'_j$  are obtained by solving for  $P$  the degree  $d$  equation  $\varrho P = \varrho P_1$ . Clearly any solution must live in some extension of  $K(P_1)$  of degree at most  $d-1$ .  $\square$

### 5. Chabauty using several primes

Let  $\mathcal{L}$  be a (known) nonempty subset of  $C^{(d)}(K)$ . We next give a criterion for showing that  $\mathcal{L}$  is equal to  $C^{(d)}(K)$ . This criterion involves using several well-chosen nonarchimedean primes  $v_1, \dots, v_t$  of good reduction, applying Theorem 3.2 (and Theorem 4.3 in the case of a cover  $C \rightarrow C'$ ) at each prime separately, and finally combining the information so obtained to show that  $\mathcal{L}$  is equal to  $C^{(d)}(K)$ . Our method resembles the Mordell–Weil sieve [Bruin and Elkies 2002], which is often applied to show that a given curve has no rational points [Bruin and Stoll 2008]. We have found the Mordell–Weil sieve to yield very poor information in our situation; not only are we dealing with a variety  $C^{(d)}$  which has rational points, we also have many points locally because of the dimension. We improve the situation dramatically by using Chabauty to remove the image under reduction maps of the known rational points, and then merely sieve for unknown rational points. If we obtain a contradiction, then we know there are no unknown rational points and we have provably determined all the rational points.

We shall make some assumptions:

- We know a subset  $D_1, \dots, D_n$  of  $J(K)$  that generates a subgroup  $G$  of finite index in  $J(K)$ . Such a subset can often be obtained using a descent argument; see for example [Cassels and Flynn 1996; Flynn 1994; Poonen and Schaefer 1997; Schaefer 1995; Schaefer and Wetherell 2005; Stoll 1998; 2001; 2002].
- The orders of the finite groups  $J(k_{v_1}), \dots, J(k_{v_t})$  are coprime to the index of  $G$  in  $J(K)$ . This assumption can be verified using the standard method of checking  $p$ -saturation, as explained in [Flynn and Smart 1997, page 345], [Siksek 1995b, page 1526] and [Siksek 1995a].
- If  $\varrho : C \rightarrow C'$  is a morphism of degree  $d$ , and  $C'(K)$  is known, we also suppose  $\varrho^*C'(K) \subseteq \mathcal{L}$ .

Fix  $v$  to be one of these primes of good reduction  $v_1, \dots, v_t$ . Let  $N_{i,v}$  be the order of the reduction of  $\tilde{D}_i$  in  $J(k_v)$ . Fix once and for all an element  $\varrho_0 \in \mathcal{L}$ , and denote

by  $J : C^{(d)}(K) \rightarrow J(K)$  the Abel–Jacobi map corresponding to  $\mathfrak{Q}_0$ . We also lazily denote by  $J$  the Abel–Jacobi map  $J : C^{(d)}(k_v) \rightarrow J(k_v)$  corresponding to  $\tilde{\mathfrak{Q}}_0$ . Let

$$\phi : \mathbb{Z}^n \rightarrow J(K), \quad (b_1, \dots, b_n) \mapsto \sum b_i D_i.$$

This induces a well-defined map

$$\tilde{\phi} : \prod_{i=1}^n \mathbb{Z}/N_{i,v} \mathbb{Z} \rightarrow J(k_v), \quad (\tilde{b}_1, \dots, \tilde{b}_n) \mapsto \sum b_i \tilde{D}_i.$$

These maps fit together in the commutative diagram

$$\begin{array}{ccccccc} \mathcal{L} & \hookrightarrow & C^{(d)}(K) & \xrightarrow{J} & J(K) & \xleftarrow{\phi} & \mathbb{Z}^n \\ & \searrow \text{red} & \downarrow \text{red} & & \downarrow \text{red} & & \downarrow \\ & & C^{(d)}(k_v) & \xrightarrow{J} & J(k_v) & \xleftarrow{\tilde{\phi}} & \prod_{i=1}^n \mathbb{Z}/N_{i,v} \mathbb{Z}. \end{array}$$

We immediately notice that  $\text{red}(C^{(d)}(K)) \subseteq J^{-1} \text{red}(J(K))$ . By assumption, the order of  $J(k_v)$  is coprime to the index  $[J(K) : G]$ . Thus  $\text{red}(J(K)) = \text{red}(G)$ . We deduce that  $\text{red}(C^{(d)}(K)) \subset J^{-1} \text{im } \tilde{\phi}$ . The set  $J^{-1} \text{im } \tilde{\phi}$  is finite and computable. Recall that our objective is to show, somehow, that  $C^{(d)}(K) = \mathcal{L}$ . Assume the existence of some element  $\mathcal{P} = \{P_1, \dots, P_d\}$  of  $C^{(d)}(K)$  that *does not* belong to  $\mathcal{L}$ . We would like to say something about the reduction  $\tilde{\mathcal{P}}$  in  $C^{(d)}(k_v)$ . Suppose now that  $\mathfrak{Q} = \{Q_1, \dots, Q_d\} \in \mathcal{L}$  satisfies the criterion of Theorem 3.2. Then  $\mathfrak{Q}$  is the only element in its residue class. Hence  $\tilde{\mathcal{P}} \neq \tilde{\mathfrak{Q}}$ . Likewise in the case of a morphism  $\varrho : C \rightarrow C'$  of degree  $d$ , if  $\mathfrak{Q}$  belongs to  $\varrho^* C'(K) \subseteq \mathcal{L}$  and satisfies the criterion of Theorem 4.3, then  $\tilde{\mathcal{P}} \neq \tilde{\mathfrak{Q}}$ . Now let  $\mathcal{M}_v$  be the subset of those  $\tilde{\mathcal{R}}$  in  $J^{-1} \text{im } \tilde{\phi}$  satisfying either

- $\tilde{\mathcal{R}} \notin \text{red}(\mathcal{L})$ , or
- $\tilde{\mathcal{R}} = \tilde{\mathfrak{Q}}$  for some  $\mathfrak{Q} \in \mathcal{L}$  that *does not* satisfy the criterion of Theorem 3.2, or
- we are in the case of a degree  $d$  cover  $\varrho : C \rightarrow C'$  and  $\tilde{\mathcal{R}} = \tilde{\mathfrak{Q}}$  for some  $\mathfrak{Q} \in \varrho^* C'(K)$  that *does not* satisfy the criterion of Theorem 4.3.

It is plain that the reduction  $\tilde{\mathcal{P}}$  of our hypothetical point  $\mathcal{P} \in C^{(d)}(K) \setminus \mathcal{L}$  belongs to  $\mathcal{M}_v$ . Define

$$\mathcal{N}_v = \tilde{\phi}^{-1} J(\mathcal{M}_v) \subseteq \prod_{i=1}^n \mathbb{Z}/N_{i,v} \mathbb{Z}.$$

The set  $\mathcal{N}_v$  carries some information about the hypothetical point  $\mathcal{P}$ . This information was obtained by considering only one nonarchimedean prime  $v$ . We would like to combine the information coming from each of our chosen primes  $v_1, \dots, v_t$ . We let

$$N_i = \text{lcm}(N_{i,v_1}, N_{i,v_2}, \dots, N_{i,v_t}) \quad \text{for } i = 1, \dots, n.$$

For each  $v = v_1, \dots, v_t$ , there is a natural projection

$$\sigma_v : \prod_{i=1}^n \mathbb{Z}/N_i\mathbb{Z} \rightarrow \prod_{i=1}^n \mathbb{Z}/N_{i,v}\mathbb{Z}.$$

We are now ready to state our main result of this section.

**Theorem 5.1.** *Under the hypotheses above, suppose that*

$$\bigcap_{v=v_1}^{v_t} \sigma_v^{-1} \mathcal{N}_v = \emptyset.$$

*Then  $C^{(d)}(K) = \mathcal{L}$ .*

*Proof.* Suppose  $\mathcal{P} \in C^{(d)}(K) \setminus \mathcal{L}$ . From the discussion above, we know that

$$\tilde{\mathcal{P}} \in \mathcal{M}_v \quad \text{for } v = v_1, \dots, v_t.$$

Now  $j\mathcal{P} \in J(K)$  and  $D_1, \dots, D_n$  generate a subgroup  $G$  of  $J(K)$  of finite index  $m = [J(K) : G]$ . Thus

$$m \cdot j\mathcal{P} = a_1 D_1 + a_2 D_2 + \dots + a_n D_n \quad \text{for some } a_1, \dots, a_n \in \mathbb{Z}.$$

The index  $m$  is coprime to  $\#J(k_v)$  for  $v = v_1, \dots, v_t$ . Hence there is some  $m^* \in \mathbb{Z}$  such that

$$m^* m \equiv 1 \pmod{\text{lcm}\{\#J(k_v) : v = v_1, \dots, v_t\}}.$$

The equality  $m^* m \cdot j\mathcal{P} = (m^* a_1) D_1 + (m^* a_2) D_2 + \dots + (m^* a_n) D_n$  takes place in  $J(K)$ , with the coefficients  $m^* a_i$  belonging to  $\mathbb{Z}$ . Applying  $\text{red}_v : J(K) \rightarrow J(k_v)$ , and recalling that  $m^* m \equiv 1 \pmod{\#J(k_v)}$ , we get

$$j\tilde{\mathcal{P}} = (m^* a_1) \tilde{D}_1 + (m^* a_2) \tilde{D}_2 + \dots + (m^* a_n) \tilde{D}_n.$$

Recall our observation at the beginning of the proof that  $\tilde{\mathcal{P}} \in \mathcal{M}_v$ . Hence the image of  $(m^* a_1, \dots, m^* a_n) \in \mathbb{Z}^n$  in  $\prod_{i=1}^n \mathbb{Z}/N_{i,v}\mathbb{Z}$  belongs to  $\mathcal{N}_v = \tilde{\phi}^{-1} j\mathcal{M}_v$ . Thus the image of  $(m^* a_1, \dots, m^* a_n) \in \mathbb{Z}^n$  in  $\prod_{i=1}^n \mathbb{Z}/N_i\mathbb{Z}$  belongs to  $\bigcap \sigma_v^{-1} \mathcal{N}_v$ . This contradicts the assumption that  $\bigcap \sigma_v^{-1} \mathcal{N}_v = \emptyset$  and completes our proof.  $\square$

## 6. Examples

In this section we use our method to compute  $C^{(2)}(\mathbb{Q})$  for two genus 3 curves, both with Jacobians having rank 1. The first example is hyperelliptic and the second is a nonsingular plane quartic. All computations are done using the MAGMA package [Bosma et al. 1997; MAGMA 2009].

**A hyperelliptic example.** Let  $C$  be the smooth projective curve over  $\mathbb{Q}$  with affine chart

$$C : y^2 = x(x^2 + 2)(x^2 + 43)(x^2 + 8x - 6), \quad (18)$$

and write  $f$  for the polynomial on the right. Being hyperelliptic,  $C$  is of course a double cover of the projective line. In our earlier notation, the map  $\varrho : C \rightarrow C'$  is just the map

$$C \rightarrow \mathbb{P}^1, \quad (x, y) \mapsto x, \quad \infty \mapsto \infty.$$

Thus

$$\varrho^* \mathbb{P}^1(\mathbb{Q}) = \{(x, \sqrt{f(x)}), (x, -\sqrt{f(x)}) : x \in \mathbb{Q}\} \cup \{\{\infty, \infty\}\}.$$

Note that the hyperelliptic involution  $\iota : C \rightarrow C$  extends to an involution on  $C^{(2)}$ , which we will also denote by  $\iota$ . Thus

$$\iota : C^{(2)} \rightarrow C^{(2)}, \quad \{(x_1, y_1), (x_2, y_2)\} \mapsto \{(x_1, -y_1), (x_2, -y_2)\}.$$

Let

$$\mathcal{L} = \varrho^* \mathbb{P}^1(\mathbb{Q}) \cup \{\mathfrak{Q}_i : i = 1, \dots, 10\} \subseteq C^{(2)}(\mathbb{Q})$$

where

$$\mathfrak{Q}_1 = \{(\sqrt{6}, 56\sqrt{6}), (-\sqrt{6}, -56\sqrt{6})\},$$

$$\mathfrak{Q}_2 = \{(0, 0), \infty\},$$

$$\mathfrak{Q}_3 = \{(\sqrt{-2}, 0), (-\sqrt{-2}, 0)\},$$

$$\mathfrak{Q}_4 = \{(\sqrt{-43}, 0), (-\sqrt{-43}, 0)\},$$

$$\mathfrak{Q}_5 = \{(-4 + \sqrt{22}, 0), (-4 - \sqrt{22}, 0)\},$$

$$\mathfrak{Q}_6 = \left\{ \left( \frac{41 + \sqrt{1509}}{2}, -222999 - 5740\sqrt{1509} \right), \text{conjugate} \right\}$$

$$\mathfrak{Q}_7 = \left\{ \left( \frac{-164 + \sqrt{22094}}{49}, \frac{257704352 - 1648200\sqrt{22094}}{823543} \right), \text{conjugate} \right\},$$

$$\mathfrak{Q}_8 = \iota \mathfrak{Q}_1,$$

$$\mathfrak{Q}_9 = \iota \mathfrak{Q}_6,$$

$$\mathfrak{Q}_{10} = \iota \mathfrak{Q}_7.$$

We want to show that  $C^{(2)}(\mathbb{Q}) = \mathcal{L}$ . First we need some information about the Mordell–Weil group  $J(\mathbb{Q})$ , where  $J$  is the Jacobian of  $C$ . Using the MAGMA routine for 2-descent on Jacobians of hyperelliptic curves, we find  $J(\mathbb{Q})$  has Mordell–Weil rank 1; this routine is an implementation of the algorithm in [Stoll 2001].

Write  $j : C^{(2)} \rightarrow J$  for the Abel–Jacobi map given by  $\mathcal{P} \mapsto \mathcal{P} - 2\infty$ . Write  $D_i = j \mathfrak{Q}_i$ , where  $i = 1, \dots, 10$ . Then  $D_1$  has infinite order, and  $D_2, D_3, D_4$  are a

basis for the 2-torsion. We note the relations

$$\begin{aligned} D_5 &= D_2 + D_3 + D_4, & D_6 &= D_1 + D_2 + D_3, & D_7 &= D_1 + D_2 + D_4, \\ D_8 &= -D_1, & D_9 &= -D_7, & D_{10} &= -D_8. \end{aligned}$$

We believe that  $D_1, D_2, D_3, D_4$  is a Mordell–Weil basis for  $J(\mathbb{Q})$ , although we are unable to prove this. However,  $D_1, D_2, D_3, D_4$  generates a subgroup  $G$  of full rank and hence finite index. Using our implementation of the  $p$ -saturation method (from [Flynn and Smart 1997, page 345], [Siksek 1995b, page 1526] and [Siksek 1995a]) we verified that this index is not divisible by any prime  $l \leq 100$ ; this verification took just a few seconds.

The primes of bad reduction for  $C$  are 2, 3, 11, 41, 43, 5153. We shall work with primes  $p = 5, 7, 13$  of good reduction. Note that

$$\#J(\mathbb{F}_5) = 2^6 \times 3, \quad \#J(\mathbb{F}_7) = 2^5 \times 5, \quad \#J(\mathbb{F}_{13}) = 2^{10}.$$

It follows that the index of  $G$  in  $J(\mathbb{Q})$  is coprime to the orders of these groups. To use our theorems we must, for each of our chosen primes  $p$ , compute a  $\mathbb{Z}_p$ -basis for the global 1-forms  $\mathcal{V}$  that kill off  $J(\mathbb{Q})$ . Of course  $\mathcal{V}$  is a submodule of the  $\mathbb{Z}_p$ -module spanned by the basis for global 1-forms:  $dx/y, xdx/y, x^2dx/y$ .

Work first with  $p = 5$ . Now  $D = 3D_1 + D_3 + D_4$  is in the kernel of reduction. We compute (see [McCallum and Poonen 2006] and [Wetherell 1997] for hints on computing  $p$ -adic integrals):

$$\begin{aligned} \int_D \frac{dx}{y} &\equiv 5 \times 1471729 \pmod{5^{10}}, \\ \int_D \frac{xdx}{y} &\equiv 5 \times 1174134 \pmod{5^{10}}, \\ \int_D \frac{x^2dx}{y} &\equiv 5 \times 1135401 \pmod{5^{10}}. \end{aligned}$$

We can take

$$\omega_1 = \frac{dx}{y} + \epsilon \frac{x^2dx}{y} \quad \text{and} \quad \omega_2 = \frac{xdx}{y} + \delta \frac{x^2dx}{y}$$

as a  $\mathbb{Z}_5$ -basis for  $\mathcal{V}$ , where

$$\epsilon \equiv 510496 \pmod{5^9} \quad \text{and} \quad \delta \equiv 395091 \pmod{5^9}.$$

Since  $\mathbb{P}^1$  has genus 0, Lemma 4.1 shows that  $\Omega_0 = \Omega$  (in the notation of Section 4) and hence  $\mathcal{V}_0 = \mathcal{V}$ .

Although we programmed our criteria for Theorems 3.2, 4.3 and 5.1 in MAGMA, we will however carry out some of the calculations explicitly to give the reader a taste for these. Consider for example  $\mathfrak{D}_0 = \{(0, 0), (0, 0)\} \in \mathcal{Q}^*\mathbb{P}^1(\mathbb{Q})$ . Let us show

that  $\mathfrak{Q}_0$  does not share its residue class with any element of  $C^{(2)}(\mathbb{Q})$  not belonging to  $\varrho^*\mathbb{P}^1(\mathbb{Q})$ . We apply the criterion of Theorem 4.3. We take  $y$  as the uniformizer at the point  $(0, 0)$ . From  $y^2 = f(x)$ , we see that  $2ydy = f'(x)dx$ . Hence

$$\left(\frac{1}{y} \frac{dx}{dy}\right)\Big|_{y=0} = \frac{2}{f'(x)}\Big|_{y=0} = \frac{2}{f'(0)} = \frac{-1}{258}.$$

Hence

$$\frac{\omega_1}{dy}\Big|_{y=0} \equiv 3 \pmod{5}$$

and so by Theorem 4.3,  $\mathfrak{Q}_0$  does not share its residue class with any element of  $C^{(2)}(\mathbb{Q})$  not belonging to  $\varrho^*\mathbb{P}^1(\mathbb{Q})$ . The reader may care to repeat this calculation with  $\{\infty, \infty\}$ , and  $\{(a, \sqrt{f(a)}), (a, -\sqrt{f(a)})\}$  for  $a = 1, \dots, 4$ . The outcome of such a calculation is that no element in  $\varrho^*\mathbb{P}^1(\mathbb{Q})$  shares its residue class with an element of  $C^{(2)}(\mathbb{Q})$  not belonging to  $\varrho^*\mathbb{P}^1(\mathbb{Q})$ .

We now apply Theorem 3.2 to  $\mathfrak{Q}_1$ . We can take  $t_1 = x - \sqrt{6}$  as a uniformizer at  $(\sqrt{6}, 56\sqrt{6})$ . Note that  $dt_1 = dx$ . Thus

$$\frac{x^i}{y} \frac{dx}{dt_1}\Big|_{t_1=0} = \frac{\sqrt{6}^i}{56\sqrt{6}}.$$

We see that

$$\frac{\omega_1}{dt_1}\Big|_{t_1=0} = \frac{1+6\epsilon}{56\sqrt{6}} \quad \text{and} \quad \frac{\omega_2}{dt_1}\Big|_{t_1=0} = \frac{\sqrt{6}+6\delta}{56\sqrt{6}}.$$

For  $(-\sqrt{6}, -56\sqrt{6})$ , we take  $t_2 = x + \sqrt{6}$  as a uniformizer. We get

$$\frac{\omega_1}{dt_2}\Big|_{t_2=0} = \frac{1+6\epsilon}{-56\sqrt{6}} \quad \text{and} \quad \frac{\omega_2}{dt_2}\Big|_{t_2=0} = \frac{-\sqrt{6}+6\delta}{-56\sqrt{6}}.$$

We compute the determinant

$$\begin{vmatrix} \frac{1+6\epsilon}{56\sqrt{6}} & \frac{\sqrt{6}+6\delta}{56\sqrt{6}} \\ \frac{1+6\epsilon}{-56\sqrt{6}} & \frac{-\sqrt{6}+6\delta}{-56\sqrt{6}} \end{vmatrix} = \frac{2(1+6\epsilon)}{56^2\sqrt{6}} \equiv 4 \pmod{5},$$

where in the last step we chose  $\sqrt{6} = 1 + 3 \times 5 + 4 \times 5^3 + \dots$ . By Theorem 3.2,  $\mathfrak{Q}_1$  does not share its residue class with any other element of  $C^{(2)}(\mathbb{Q})$ . By similar arguments, the same is true of  $\mathfrak{Q}_i$  for  $i = 2, \dots, 10$ .

Suppose now that  $\mathcal{P} \in C^{(2)}(\mathbb{Q}) \setminus \mathcal{L}$ . We would like to deduce a contradiction. The argument at the end of the proof of Theorem 5.1 shows that there are integers  $n_1, n_2, n_3, n_4$  such that simultaneously in each of  $J(\mathbb{F}_p)$  with  $p = 5, 7, 13$  we have

$${}_J\tilde{\mathcal{P}} = n_1\tilde{D}_1 + n_2\tilde{D}_2 + n_3\tilde{D}_3 + n_4\tilde{D}_4.$$



In  $J(\mathbb{F}_5)$ , the order of  $\tilde{D}_1$  is 6 while  $\tilde{D}_2, \tilde{D}_3, \tilde{D}_4$  are of order 2. Consider the maps

$$C^{(2)}(\mathbb{F}_5) \xrightarrow{J} J(\mathbb{F}_5) \xleftarrow{\tilde{\phi}} \mathbb{Z}/6\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3.$$

We see that  $(n_1, n_2, n_3, n_4) \bmod (6, 2, 2, 2)$  belongs to  $\tilde{\phi}^{-1}(JC^{(2)}(\mathbb{F}_5))$ . Using our MAGMA program, we wrote down the set  $\tilde{\phi}^{-1}(JC^{(2)}(\mathbb{F}_5))$  and found that it has 22 elements. In the notation of Section 5, we want to write down the set  $\mathcal{N}_5$ . This is the subset of  $\tilde{\phi}^{-1}(JC^{(2)}(\mathbb{F}_5))$  containing all quadruples that, on the basis of our Chabauty calculations above, cannot be  $(n_1, n_2, n_3, n_4) \bmod (6, 2, 2, 2)$ . For example, the quadruple  $(0, 0, 0, 0)$  is in  $\tilde{\phi}^{-1}(JC^{(2)}(\mathbb{F}_5))$ . However, if  $(n_1, n_2, n_3, n_4) \equiv (0, 0, 0, 0) \bmod (6, 2, 2, 2)$ , then  $\mathcal{P}$  shares its residue class with some element of  $J^{-1}\mathbb{P}^1(\mathbb{Q})$ , contradicting our computations above. Therefore  $(0, 0, 0, 0) \notin \mathcal{N}_5$ . Similarly we can exclude another 10 elements corresponding to  $\mathfrak{Q}_1, \dots, \mathfrak{Q}_{10}$ . This leaves us with 11 elements in  $\mathcal{N}_5$ :

$$\begin{aligned} \mathcal{N}_5 = \{ & (2, 0, 1, 1), (2, 1, 0, 1), (2, 1, 1, 0), (3, 0, 0, 1), (3, 0, 1, 0), (3, 0, 1, 1), \\ & (3, 1, 0, 0), (3, 1, 1, 1), (4, 0, 1, 1), (4, 1, 0, 1), (4, 1, 1, 0) \} \\ & \subset \mathbb{Z}/6\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3. \end{aligned}$$

We know that  $(n_1, n_2, n_3, n_4)$  is equivalent modulo  $(6, 2, 2, 2)$  to one of these 11 elements of  $\mathcal{N}_5$ .

Next we repeat the calculation with  $p = 7$ . Our Chabauty arguments, Theorems 3.2 and 4.3, succeed for  $J^{-1}\mathbb{P}^1(\mathbb{Q})$  and  $\mathfrak{Q}_3$  and fail for all other  $\mathfrak{Q}_i$ . There are good reasons for these failures. It turns out that  $\mathfrak{Q}_1, \mathfrak{Q}_4$  and  $\mathfrak{Q}_8$  share the same residue class, likewise for  $\mathfrak{Q}_5, \mathfrak{Q}_6$  and  $\mathfrak{Q}_9$ , and for  $\mathfrak{Q}_2, \mathfrak{Q}_7$  and  $\mathfrak{Q}_{10}$ . Despite this, the information given by  $p = 7$  is still useful, this time because the set  $\tilde{\phi}^{-1}(JC^{(2)}(\mathbb{F}_7))$  is small, having only 10 elements. We have excluded two of them, those corresponding to  $J^{-1}\mathbb{P}^1(\mathbb{Q})$  and  $\mathfrak{Q}_3$ . We are left with

$$\begin{aligned} \mathcal{N}_7 = \{ & (0, 0, 0, 1), (0, 1, 0, 0), (0, 1, 1, 1), (1, 0, 0, 0), \\ & (1, 0, 0, 1), (1, 0, 1, 1), (1, 1, 0, 1), (1, 1, 1, 0) \} \subset (\mathbb{Z}/2\mathbb{Z})^4. \end{aligned}$$

We know that  $(n_1, n_2, n_3, n_4)$  is equivalent modulo  $(2, 2, 2, 2)$  to one of these eight elements of  $\mathcal{N}_7$ . Combining the information from  $\mathcal{N}_5$  and  $\mathcal{N}_7$ , we see that

$$(n_1, n_2, n_3, n_4) \equiv (3, 0, 0, 1) \text{ or } (3, 0, 1, 1) \pmod{(6, 2, 2, 2)}. \quad (19)$$

We still have not obtained a contradiction. Finally we let  $p = 13$ . This time we find

$$\begin{aligned} \mathcal{N}_{13} = \{ & (3, 1, 0, 1), (8, 0, 1, 0), (8, 0, 1, 1), (8, 1, 0, 0), (8, 1, 0, 1), (13, 1, 0, 1) \} \\ & \subset \mathbb{Z}/16\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3. \end{aligned}$$

Again we know that  $(n_1, n_2, n_3, n_4)$  is equivalent modulo  $(16, 2, 2, 2)$  to one of these six elements of  $\mathcal{N}_{13}$ . This contradicts the congruences in (19). We deduce that  $C^{(2)}(\mathbb{Q}) = \mathcal{L}$  as required.

**A plane quartic example.** Let  $C$  be the smooth plane quartic (genus 3) curve with affine equation

$$C : x^4 + (y^2 + 1)(x + y) = 0,$$

and let  $J$  be its Jacobian. Schaefer and Wetherell [2005] observe that it has a trivial automorphism group, and that its  $J$  is absolutely simple and not modular. Using a deep descent argument, they show that  $J(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ . They apply Chabauty to conclude that  $C(\mathbb{Q}) = \{(0, 0), (-1, 0), \infty\}$ .

Using our method we showed that  $C^{(2)}(\mathbb{Q}) = \{\mathfrak{Q}_1, \dots, \mathfrak{Q}_{10}\}$ , where

$$\mathfrak{Q}_1 = \{(-17 + \sqrt{259}, -48 + 3\sqrt{259}), (-17 - \sqrt{259}, -48 - 3\sqrt{259})\},$$

$$\mathfrak{Q}_2 = \{(-1, \tfrac{1}{2}(1 + \sqrt{-3})), (-1, \tfrac{1}{2}(1 - \sqrt{-3}))\},$$

$$\mathfrak{Q}_3 = \{(\tfrac{1}{2}(1 + \sqrt{-3}), 0), (\tfrac{1}{2}(1 - \sqrt{-3}), 0)\},$$

$$\mathfrak{Q}_4 = \{(0, 0), \infty\},$$

$$\mathfrak{Q}_5 = \{(0, 0), (0, 0)\},$$

$$\mathfrak{Q}_6 = \{(0, i), (0, -i)\},$$

$$\mathfrak{Q}_7 = \{(-1, 0), \infty\},$$

$$\mathfrak{Q}_8 = \{(-1, 0), (0, 0)\},$$

$$\mathfrak{Q}_9 = \{(-1, 0), (-1, 0)\},$$

$$\mathfrak{Q}_{10} = \{\infty, \infty\}.$$

## Acknowledgments

We thank the referees for carefully reading the manuscript and suggesting many improvements and corrections. We are indebted to Nils Bruin, Bjorn Poonen, Michael Stoll and Joseph Wetherell for helpful conversations about Chabauty, and to Miles Reid for useful algebraic geometry discussions. In particular, we are aware of some earlier Chabauty computations on symmetric squares of hyperelliptic genus 3 curves by Wetherell, although no details of such computations have been published.

## References

- [Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, “The Magma algebra system, I, The user language”, *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR 1484478 Zbl 0898.68039
- [Bourbaki 1989] N. Bourbaki, *Lie groups and Lie algebras, Chapters 1–3*, Springer, Berlin, 1989. MR 89k:17001 Zbl 0672.22001

- [Bruin 2002] N. R. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, CWI Tract **133**, Centrum voor Wiskunde en Informatica, Amsterdam, 2002. MR 2003i:11042 Zbl 1043.11029
- [Bruin 2003] N. Bruin, “Chabauty methods using elliptic curves”, *J. Reine Angew. Math.* **562** (2003), 27–49. MR 2004j:11051 Zbl 1135.11320
- [Bruin and Elkies 2002] N. Bruin and N. D. Elkies, “Trinomials  $ax^7 + bx + c$  and  $ax^8 + bx + c$  with Galois groups of order 168 and  $8 \cdot 168$ ”, pp. 172–188 in *Algorithmic number theory* (Sydney, 2002), edited by C. Fieker and D. R. Kohel, Lecture Notes in Comput. Sci. **2369**, Springer, Berlin, 2002. MR 2005d:11094 Zbl 1058.11044
- [Bruin and Stoll 2008] N. Bruin and M. Stoll, “Deciding existence of rational points on curves: An experiment”, *Experiment. Math.* **17**:2 (2008), 181–189. MR 2433884
- [Cassels and Flynn 1996] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Mathematical Society Lecture Note Series **230**, Cambridge University Press, 1996. MR 97i:11071 Zbl 0857.14018
- [Chabauty 1941] C. Chabauty, “Sur les points rationnels des variétés algébriques dont l’irrégularité est supérieure à la dimension”, *C. R. Acad. Sci. Paris* **212** (1941), 1022–1024. MR 6,102e Zbl 0025.24903
- [Coleman 1985a] R. F. Coleman, “Effective Chabauty”, *Duke Mathematical J.* **52**:3 (1985), 765–770. MR 87f:11043 Zbl 0588.14015
- [Coleman 1985b] R. F. Coleman, “Torsion points on curves and  $p$ -adic abelian integrals”, *Ann. of Math.* (2) **121**:1 (1985), 111–168. MR 86j:14014 Zbl 0578.14038
- [Colmez 1998] P. Colmez, *Intégration sur les variétés  $p$ -adiques*, Astérisque **248**, Société Mathématique de France, Paris, 1998. MR 2000e:14026 Zbl 0930.14013
- [Debarre and Klassen 1994] O. Debarre and M. J. Klassen, “Points of low degree on smooth plane curves”, *J. Reine Angew. Math.* **446** (1994), 81–87. MR 95f:14052 Zbl 0784.14014
- [Faltings 1983] G. Faltings, “Endlichkeitssätze für abelsche Varietäten über Zahlkörpern”, *Invent. Math.* **73**:3 (1983), 349–366. MR 85g:11026a Zbl 0588.14026
- [Faltings 1991] G. Faltings, “Diophantine approximation on abelian varieties”, *Ann. of Math.* (2) **133**:3 (1991), 549–576. MR 93d:11066 Zbl 0734.14007
- [Faltings 1994] G. Faltings, “The general case of S. Lang’s conjecture”, pp. 175–182 in *Barsotti Symposium in Algebraic Geometry* (Abano Terme, 1991), edited by V. Cristante and W. Messing, Perspect. Math. **15**, Academic Press, San Diego, CA, 1994. MR 95m:11061 Zbl 0823.14009
- [Flynn 1994] E. V. Flynn, “Descent via isogeny in dimension 2”, *Acta Arith.* **66**:1 (1994), 23–43. MR 95g:11057 Zbl 0835.14009
- [Flynn 1995] E. V. Flynn, “On a theorem of Coleman”, *Manuscripta Math.* **88**:4 (1995), 447–456. MR 97b:11082 Zbl 0865.14012
- [Flynn 1997] E. V. Flynn, “A flexible method for applying Chabauty’s theorem”, *Compositio Math.* **105**:1 (1997), 79–94. MR 97m:11083 Zbl 0882.14009
- [Flynn and Smart 1997] E. V. Flynn and N. P. Smart, “Canonical heights on the Jacobians of curves of genus 2 and the infinite descent”, *Acta Arith.* **79**:4 (1997), 333–352. MR 98f:11066 Zbl 0895.11026
- [Flynn and Wetherell 1999] E. V. Flynn and J. L. Wetherell, “Finding rational points on bielliptic genus 2 curves”, *Manuscripta Math.* **100**:4 (1999), 519–533. MR 2001g:11098 Zbl 1029.11024
- [Flynn and Wetherell 2001] E. V. Flynn and J. L. Wetherell, “Covering collections and a challenge problem of Serre”, *Acta Arith.* **98**:2 (2001), 197–205. MR 2002b:11088 Zbl 1049.11066

- [Garling 1986] D. J. H. Garling, *A course in Galois theory*, Cambridge University Press, 1986. MR 88d:12007 Zbl 0608.12025
- [Grant 1994] D. Grant, “A curve for which Coleman’s effective Chabauty bound is sharp”, *Proc. Amer. Math. Soc.* **122**:1 (1994), 317–319. MR 94k:14019 Zbl 0834.14015
- [Gross and Rohrlich 1978] B. H. Gross and D. E. Rohrlich, “Some results on the Mordell–Weil group of the Jacobian of the Fermat curve”, *Invent. Math.* **44**:3 (1978), 201–224. MR 58 #10911 Zbl 0369.14011
- [Harris and Silverman 1991] J. Harris and J. Silverman, “Bielliptic curves and symmetric products”, *Proc. Amer. Math. Soc.* **112**:2 (1991), 347–356. MR 91i:11067 Zbl 0727.11023
- [Kamienny 1986a] S. Kamienny, “Torsion points on elliptic curves over all quadratic fields”, *Duke Mathematical J.* **53**:1 (1986), 157–162. MR 87g:11068 Zbl 0599.14029
- [Kamienny 1986b] S. Kamienny, “Torsion points on elliptic curves over all quadratic fields, II”, *Bull. Soc. Math. France* **114**:1 (1986), 119–122. MR 87j:11051 Zbl 0599.14030
- [Kamienny 1992] S. Kamienny, “Torsion points on elliptic curves and  $q$ -coefficients of modular forms”, *Invent. Math.* **109**:2 (1992), 221–229. MR 93h:11054 Zbl 0773.14016
- [Klassen 1993] M. J. Klassen, *Algebraic points of low degree on curves of low rank*, thesis, University of Arizona, 1993.
- [Klassen and Tzermias 1997] M. Klassen and P. Tzermias, “Algebraic points of low degree on the Fermat quintic”, *Acta Arith.* **82**:4 (1997), 393–401. MR 98k:11086 Zbl 0917.11022
- [Lorenzini and Tucker 2002] D. Lorenzini and T. J. Tucker, “Thue equations and the method of Chabauty–Coleman”, *Invent. Math.* **148**:1 (2002), 47–77. MR 2003d:11088 Zbl 1048.11023
- [MAGMA 2009] “MAGMA Computational Algebra System”, web site, University of Sydney, 2009, Available at <http://magma.maths.usyd.edu.au/magma/>.
- [McCallum 1992] W. G. McCallum, “The arithmetic of Fermat curves”, *Math. Ann.* **294**:3 (1992), 503–511. MR 93j:11037 Zbl 0766.14013
- [McCallum 1994] W. G. McCallum, “On the method of Coleman and Chabauty”, *Math. Ann.* **299**:3 (1994), 565–596. MR 95c:11079 Zbl 0824.14017
- [McCallum and Poonen 2006] W. McCallum and B. Poonen, “The method of Chabauty and Coleman”, preprint, 2006, Available at <http://math.arizona.edu/~wmc/Research/Chabauty.pdf>.
- [Merel 1996] L. Merel, “Bornes pour la torsion des courbes elliptiques sur les corps de nombres”, *Invent. Math.* **124**:1-3 (1996), 437–449. MR 96i:11057 Zbl 0936.11037
- [Milne 1986] J. S. Milne, “Jacobian varieties”, pp. 167–212 in *Arithmetic geometry* (Storrs, CT, 1984), edited by G. Cornell and J. H. Silverman, Springer, New York, 1986. MR 86i:14018 Zbl 0604.14018
- [Parent 2000] P. Parent, “Torsion des courbes elliptiques sur les corps cubiques”, *Ann. Inst. Fourier (Grenoble)* **50**:3 (2000), 723–749. MR 2001i:11067 Zbl 0971.11030
- [Parent 2003] P. Parent, “No 17-torsion on elliptic curves over cubic number fields”, *J. Théor. Nombres Bordeaux* **15**:3 (2003), 831–838. MR 2006a:11071 Zbl 1072.11037
- [Poonen and Schaefer 1997] B. Poonen and E. F. Schaefer, “Explicit descent for Jacobians of cyclic covers of the projective line”, *J. Reine Angew. Math.* **488** (1997), 141–188. MR 98k:11087 Zbl 0888.11023
- [Schaefer 1995] E. F. Schaefer, “2-descent on the Jacobians of hyperelliptic curves”, *J. Number Theory* **51**:2 (1995), 219–232. MR 96c:11066 Zbl 0832.14016

- [Schaefer and Wetherell 2005] E. F. Schaefer and J. L. Wetherell, “Computing the Selmer group of an isogeny between abelian varieties using a further isogeny to a Jacobian”, *J. Number Theory* **115**:1 (2005), 158–175. MR 2006g:11116 Zbl 1095.11033
- [Siksek 1995a] S. Siksek, *Descents on curves of genus 1*, thesis, University of Exeter, 1995.
- [Siksek 1995b] S. Siksek, “Infinite descent on elliptic curves”, *Rocky Mountain J. Math.* **25**:4 (1995), 1501–1538. MR 97g:11053 Zbl 0852.11028
- [Stoll 1998] M. Stoll, “On the arithmetic of the curves  $y^2 = x^l + A$  and their Jacobians”, *J. Reine Angew. Math.* **501** (1998), 171–189. MR 99h:11069 Zbl 0902.11024
- [Stoll 2001] M. Stoll, “Implementing 2-descent for Jacobians of hyperelliptic curves”, *Acta Arith.* **98**:3 (2001), 245–277. MR 2002b:11089 Zbl 0972.11058
- [Stoll 2002] M. Stoll, “On the arithmetic of the curves  $y^2 = x^l + A$ , II”, *J. Number Theory* **93**:2 (2002), 183–206. MR 2003d:11090 Zbl 1004.11038
- [Stoll 2006a] M. Stoll, “Independence of rational points on twists of a given curve”, *Compos. Math.* **142**:5 (2006), 1201–1214. MR 2007m:14025 Zbl 1128.11033
- [Stoll 2006b] M. Stoll, “On the number of rational squares at fixed distance from a fifth power”, *Acta Arith.* **125**:1 (2006), 79–88. MR 2007g:11039
- [Tzermias 1998] P. Tzermias, “Algebraic points of low degree on the Fermat curve of degree seven”, *Manuscripta Math.* **97**:4 (1998), 483–488. MR 99j:11075 Zbl 0952.11017
- [Tzermias 2003] P. Tzermias, “Parametrization of low-degree points on a Fermat curve”, *Acta Arith.* **108**:1 (2003), 25–35. MR 2004b:11091 Zbl 1056.11040
- [Tzermias 2004] P. Tzermias, “Low-degree points on Hurwitz-Klein curves”, *Trans. Amer. Math. Soc.* **356**:3 (2004), 939–951. MR 2004j:11061 Zbl 1116.14017
- [Tzermias 2005] P. Tzermias, “Improved bounds on the number of low-degree points on certain curves”, *Acta Arith.* **117**:3 (2005), 277–282. MR 2006m:11093 Zbl 1079.11032
- [Wetherell 1997] J. L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, thesis, University of California at Berkeley, 1997.

Communicated by Bjorn Poonen

Received 2008-04-02

Revised 2009-01-20

Accepted 2009-02-17

s.siksek@warwick.ac.uk

*Institute of Mathematics, University of Warwick,  
Coventry CV4 7AL, United Kingdom  
<http://www.warwick.ac.uk/~maseap/>*

# Obstruction de descente et obstruction de Brauer–Manin étale

Cyril Demarche

Soit  $X$  une variété projective lisse géométriquement intègre sur un corps de nombres. On considère deux obstructions au principe de Hasse sur  $X$  : l'obstruction de Brauer–Manin appliquée aux revêtements étales de  $X$  et l'obstruction de descente sur  $X$ . On démontre que la première est plus forte que la seconde. On en déduit, grâce à un exemple récent de Poonen, que l'obstruction de descente est insuffisante pour expliquer tous les contre-exemples au principe de Hasse.

Let  $X$  be a smooth, projective and geometrically integral variety over a number field. We consider two obstructions to the Hasse principle on  $X$ : the Brauer–Manin obstruction applied to étale covers of  $X$  and the descent obstruction on  $X$ . We prove that the first one is at least as strong as the second. Combining this with a recent example of Poonen shows that the descent obstruction is not sufficient to explain all counterexamples to the Hasse principle.

## 1. Introduction

Dans tout ce texte, une variété est un schéma séparé de type fini sur un corps, et un groupe algébrique est un schéma en groupes séparé de type fini sur un corps. Si  $k$  est un corps de caractéristique 0, et  $\bar{k}$  une clôture algébrique de  $k$ , un  $k$ -groupe algébrique  $G$  est dit fini si  $G(\bar{k})$  est fini (c'est-à-dire si  $G$  est fini comme  $k$ -schéma).

Soit  $k$  un corps de nombres ; si  $S$  est un ensemble fini de places de  $k$ ,  $\mathbb{O}_{k,S}$  désigne l'ensemble des éléments de  $k$  entiers hors de  $S$ . Pour toute  $k$ -variété  $Y$ , on notera  $Y(\mathbb{A}_k)$  l'ensemble de ses points adéliques, défini de la façon suivante : si  $\mathcal{Y}$  est un modèle de  $Y$  sur un ouvert  $U = \text{Spec}(\mathbb{O}_{k,S})$  du spectre de l'anneau des entiers de  $k$ ,  $Y(\mathbb{A}_k)$  est défini comme étant le produit restreint  $\prod'_v Y(k_v)$  par rapport aux sous-ensembles  $\mathcal{Y}(\mathbb{O}_v)$ ,  $v \notin S$ . Cet ensemble est muni de la topologie produit restreint (chaque  $Y(k_v)$  étant muni de la topologie  $v$ -adique). Si  $Y$  est propre, cet ensemble coïncide avec le produit direct des  $Y(k_v)$ .

*MSC2000:* primary 11G35; secondary 14G05, 11E72.

*Mots-clefs:* principe de Hasse, obstruction de Brauer–Manin, obstruction de descente, cohomologie galoisienne, toseurs, Hasse principle, Brauer–Manin obstruction, descent obstruction, Galois cohomology, torsors.

On rappelle l'existence de l'accouplement dit de Brauer–Manin

$$\begin{aligned} Y(\mathbb{A}_k) \times \mathrm{Br}(Y) &\longrightarrow \mathbb{Q}/\mathbb{Z} \\ (P, A) &\longmapsto \langle A, P \rangle_{\mathrm{BM}} := \sum_{v \in \Omega_k} j_v(A(P_v)) \end{aligned}$$

(voir par exemple [Skorobogatov 2001, section 5.2]), où  $\mathrm{Br}(Y) := H_{\mathrm{\acute{e}t}}^2(Y, \mathbb{G}_m)$  désigne le groupe de Brauer cohomologique de la variété  $Y$ ,  $j_v : \mathrm{Br}(k_v) \rightarrow \mathbb{Q}/\mathbb{Z}$  est l'invariant donné par la théorie du corps de classes local et  $A(P_v) \in \mathrm{Br}(k_v)$  est l'évaluation de  $A \in \mathrm{Br}(Y)$  en  $P_v \in Y(k_v)$ . On peut alors définir l'ensemble de Brauer–Manin

$$Y(\mathbb{A}_k)^{\mathrm{Br}} := \{P \in Y(\mathbb{A}_k) : \langle A, P \rangle_{\mathrm{BM}} = 0, \forall A \in \mathrm{Br}(Y)\}$$

Grâce à la loi de réciprocité de la théorie du corps de classes global, on sait que  $Y(k) \subset Y(\mathbb{A}_k)^{\mathrm{Br}}$ .

Désormais,  $X$  est une  $k$ -variété projective.

Pour tout groupe algébrique  $G$  sur  $k$ , pour tout  $X$ -torseur  $f : Y \xrightarrow{G} X$  sous  $G$ , et tout cocycle  $\sigma \in Z^1(k, G)$ , on notera

$$f^\sigma : Y^\sigma \xrightarrow{G^\sigma} X$$

le  $X$ -torseur  $f$  tordu par le cocycle  $\sigma$  (voir par exemple [Skorobogatov 2001, p. 20] ou la définition 1) ; on notera également  $[Y]$  la classe d'un tel torseur dans l'ensemble de cohomologie étale  $H^1(X, G)$ , et pour tout point  $P \in X(K)$ , où  $K$  est un corps contenant  $k$ , on notera  $[Y](P) \in H^1(K, G)$  la classe de la fibre  $Y_P := f^{-1}(P) \rightarrow K$  (qui est un  $K$ -torseur sous  $G$ ) dans  $H^1(K, G)$ . En outre, si  $\sigma$  est un 1-cocycle à valeurs dans  $G$ , on notera  $[\sigma]$  sa classe dans  $H^1(k, G)$ . Soit  $f : Y \xrightarrow{G} X$  un torseur sous un  $k$ -groupe  $G$  ; on considérera l'ensemble de descente de  $f$  défini par

$$X(\mathbb{A}_k)^f := \bigcup_{[\sigma] \in H^1(k, G)} f^\sigma(Y^\sigma(\mathbb{A}_k)).$$

**Remarque.** Une définition équivalente de l'ensemble de descente  $X(\mathbb{A}_k)^f$  est donnée par exemple dans [Harari et Skorobogatov 2002, définition 4.2] :  $X(\mathbb{A}_k)^f$  est l'ensemble des points adéliques  $(P_v)$  de  $X$  tels que l'évaluation  $([Y](P_v)) \in \prod_v H^1(k_v, G)$  provienne d'une classe globale dans  $H^1(k, G)$ , c'est-à-dire que  $([Y](P_v)) \in \mathrm{Im}(H^1(k, G) \rightarrow \prod_v H^1(k_v, G))$ . L'équivalence de ces deux définitions est une conséquence immédiate de [Skorobogatov 2008, proposition 2.4].

On définit alors, comme dans [Poonen 2008, sections 3.2 et 3.3], les ensembles

$$X(\mathbb{A}_k)^{\mathrm{\acute{e}t}, \mathrm{Br}} := \bigcap_{\substack{f: Y \xrightarrow{G} X \\ G \text{ fini}}} \bigcup_{[\sigma] \in H^1(k, G)} f^\sigma(Y^\sigma(\mathbb{A}_k)^{\mathrm{Br}})$$

et

$$X(\mathbb{A}_k)^{\text{desc}} := \bigcap_{\substack{f: Y \xrightarrow{G} X \\ G \text{ linéaire}}} X(\mathbb{A}_k)^f = \bigcap_{\substack{f: Y \xrightarrow{G} X \\ G \text{ linéaire}}} \bigcup_{[\sigma] \in H^1(k, G)} f^\sigma(Y^\sigma(\mathbb{A}_k)).$$

On cherche à comparer ces deux ensembles, qui définissent tous les deux des obstructions au principe de Hasse pour la variété  $X$ , appelées respectivement obstruction de Brauer–Manin étale et obstruction de descente. En effet, on sait que pour tout  $X$ -torseur  $f : Y \xrightarrow{G} X$ , on a (voir par exemple [Skorobogatov 2001, p. 22]) :

$$X(k) = \bigcup_{[\sigma] \in H^1(k, G)} f^\sigma(Y^\sigma(k))$$

Cela implique bien en particulier que l'on a des inclusions  $X(k) \subset X(\mathbb{A}_k)^{\text{desc}}$  et  $X(k) \subset X(\mathbb{A}_k)^{\text{ét, Br}}$ . Cela permet de définir des obstructions au principe de Hasse, qui sont plus fines que l'obstruction de Brauer–Manin : les ensembles  $X(\mathbb{A}_k)^{\text{ét, Br}}$  et  $X(\mathbb{A}_k)^{\text{desc}}$  sont en effet contenus dans  $X(\mathbb{A}_k)^{\text{Br}}$  (pour le premier, c'est évident, et pour le second, c'est le lemme 2.8 de [Skorobogatov 2008], qui est une conséquence d'un résultat de Gabber, également prouvé par de Jong [2005, théorème 1.1]).

Skorobogatov [1999] a construit un contreexemple  $X$  au principe de Hasse pour lequel  $X(\mathbb{A}_k)^{\text{Br}} \neq \emptyset$ , mais  $X(\mathbb{A}_k)^{\text{ét, Br}} = X(\mathbb{A}_k)^{\text{desc}} = \emptyset$ . Plus récemment, Poonen [2008] a fabriqué des exemples de variétés  $X$  pour lesquelles l'obstruction de Brauer–Manin étale est insuffisante pour expliquer la vacuité de  $X(\mathbb{A}_k)$  : pour ces variétés, l'ensemble  $X(k)$  est vide, mais  $X(\mathbb{A}_k)^{\text{ét, Br}}$  (et a fortiori  $X(\mathbb{A}_k)^{\text{Br}}$ ) ne l'est pas.

On cherche ici à répondre à une question de Poonen [2008, question 3.1], ainsi qu'à une question similaire de Stoll [2007, p. 134 en bas et 135 en haut] : a-t-on toujours une inclusion  $X(\mathbb{A}_k)^{\text{ét, Br}} \subset X(\mathbb{A}_k)^{\text{desc}}$  ?

On se propose de démontrer le résultat suivant, qui répond à cette question par l'affirmative :

*Soit  $X$  une  $k$ -variété projective, lisse et géométriquement intègre. Alors*

$$X(\mathbb{A}_k)^{\text{ét, Br}} \subset X(\mathbb{A}_k)^{\text{desc}}.$$

Cet énoncé permet de répondre à la question de Poonen, ce qui assure que l'obstruction de descente est insuffisante pour expliquer les contreexemples au principe de Hasse que sont les variétés considérées dans [Poonen 2008] (voir corollaire 2).

**Remarque.** Un résultat récent de Skorobogatov [2008, corollaire 1.2] assure que l'inclusion inverse  $X(\mathbb{A}_k)^{\text{desc}} \subset X(\mathbb{A}_k)^{\text{ét, Br}}$  est également vérifiée. Cela démontre donc que l'obstruction de descente et l'obstruction de Brauer–Manin étale sont en fait équivalentes.



## 2. Énoncé du résultat et structure de la preuve

**2.1. Notations et rappels.** Avant d'énoncer et de démontrer le résultat principal de ce texte, on rappelle d'abord quelques définitions et quelques notations qui seront utiles pour la suite.

Soit  $k$  un corps de caractéristique nulle. Fixons une clôture algébrique  $\bar{k}$  de  $k$ . Dans tout le texte, si  $Y$  est une  $k$ -variété, on notera  $\bar{Y}$  la  $\bar{k}$ -variété déduite de  $Y$  par extension des scalaires, c'est-à-dire  $\bar{Y} := Y \times_k \bar{k}$ . On notera aussi  $\Gamma_k := \text{Gal}(\bar{k}|k)$  le groupe de Galois absolu de  $k$ . Les ensembles de cohomologie considérés dans ce texte sont tous des ensembles de cohomologie étale (ou galoisienne). Tous les torseurs considérés ici seront, sauf mention explicite du contraire, des torseurs à droite.

On rappelle d'abord la définition de la torsion d'un torseur par un 1-cocycle (voir par exemple [Harari et Skorobogatov 2002, définitions 1.7 et 1.8]) :

**Définition 1.** Soit  $G$  un  $k$ -groupe algébrique, soit  $\sigma \in Z^1(k, G)$  un 1-cocycle.

- Le  $k$ -groupe algébrique  $G^\sigma$  est la  $k$ -forme intérieure de  $G$  obtenue en quotientant  $\bar{G}$  par l'action tordue de  $\Gamma_k$  définie par  $(\gamma, \bar{g}) \mapsto \sigma_\gamma(\gamma \bar{g}) \sigma_\gamma^{-1}$  pour tout  $\gamma \in \Gamma_k$  et tout  $\bar{g} \in \bar{G}$ .
- Soit  $f : Y \xrightarrow{G} X$  un  $X$ -torseur (à droite) sous  $G$ . On suppose que  $Y$  est une  $k$ -variété quasi-projective. Alors la forme tordue de  $f$  par  $\sigma$  est la  $k$ -variété quotient  $Y^\sigma$  de  $\bar{Y}$  par l'action de  $\Gamma_k$  définie par  $(\gamma, \bar{y}) \mapsto \gamma \cdot \bar{y} \cdot \sigma_\gamma^{-1}$ . Cette variété est munie d'un morphisme canonique  $f^\sigma : Y^\sigma \rightarrow X$  qui munit  $Y^\sigma$  d'une structure de  $X$ -torseur (à droite) sous  $G^\sigma$ .

Dans le cas où  $k$  est un corps de nombres et  $X$  est une  $k$ -variété projective, cette définition permet ensuite de définir les ensembles  $X(\mathbb{A}_k)^{\text{desc}}$  et  $X(\mathbb{A}_k)^{\text{ét, Br}}$  comme dans l'introduction (on notera que dans la construction de ces ensembles, les hypothèses de la définition 1 sont vérifiées, à savoir que les torseurs considérés sont quasi-projectifs).

Dans la preuve du résultat principal, on va utiliser quelques notions de cohomologie non-abélienne. On rappelle ici quelques définitions sur le sujet. Pour davantage de précisions, on pourra consulter [Flicker et al. 1998, section 1] ou [Borovoi 1993].

On commence par définir un automorphisme semi-linéaire (voir [Harari et Skorobogatov 2002, définition 1.1]) : soit  $\bar{f} : \bar{Y} \rightarrow \text{Spec } \bar{k}$  une  $\bar{k}$ -variété. Soit  $\varphi \in \text{Aut}(\bar{Y}/k)$ . L'automorphisme  $\varphi$  est dit *semi-linéaire* s'il existe un élément (nécessairement unique)  $\gamma \in \Gamma_k$  tel que  $\bar{f} \circ \varphi = (\gamma^*)^{-1} \circ \bar{f}$ , où  $\gamma^* : \text{Spec } \bar{k} \rightarrow \text{Spec } \bar{k}$  est induit par l'action de  $\gamma$  sur  $\bar{k}$ . On notera  $\text{SAut}(\bar{Y}/k)$  le groupe des automorphismes semi-linéaires de  $\bar{Y}$ . On notera aussi  $q : \text{SAut}(\bar{Y}/k) \rightarrow \Gamma_k$  le morphisme défini par  $q(\varphi) = \gamma$ . Enfin, si  $\bar{Y}$  est un  $\bar{k}$ -groupe algébrique, on notera  $\text{SAut}^{\text{gr}}(\bar{Y}/k)$  le

groupe des automorphismes semi-linéaires compatibles avec la structure de groupe de  $\bar{Y}$ , et  $\text{SOut}(\bar{Y}/k)$  le quotient de  $\text{SAut}^{\text{gr}}(\bar{Y}/k)$  par le sous-groupe  $\text{Int}(\bar{Y})$  des automorphismes intérieurs de  $\bar{Y}$ ; de même, on note  $\text{Out}(\bar{Y}/k)$  le quotient du groupe  $\text{Aut}^{\text{gr}}(\bar{Y}/k)$  (formé des éléments de  $\text{Aut}(\bar{Y}/k)$  respectant la structure de groupe) par les automorphismes intérieurs. Si  $y \in \bar{Y}(k)$ , on notera  $\text{int}(y)$  l'automorphisme intérieur de  $\bar{Y}$  défini par  $g \mapsto ygy^{-1}$ .

Plus généralement, si  $X$  est une  $k$ -variété,  $\bar{Y}$  une  $\bar{k}$ -variété et  $\bar{Y} \rightarrow \bar{X}$  un morphisme, on définit  $\text{SAut}(\bar{Y}/X) := \text{Aut}(\bar{Y}/X) \cap \text{SAut}(\bar{Y}/k)$  (voir [Harari et Skorobogatov 2002, définition 1.3]). Enfin, ces groupes d'automorphismes linéaires sont munis d'une topologie faible (voir [Harari et Skorobogatov 2002, définition 1.3]), et on munit l'ensemble  $\bar{Y}(\bar{k})$  de la topologie discrète.

On peut alors définir la notion de  $k$ -lien : si  $\bar{G}$  est un  $\bar{k}$ -groupe algébrique, un  $k$ -lien sur  $\bar{G}$  est un morphisme de groupes  $\kappa : \Gamma_k \rightarrow \text{SOut}(\bar{G}/k)$  qui scinde le morphisme  $\text{SOut}(\bar{G}/k) \rightarrow \Gamma_k$  et qui se relève en une section continue du morphisme  $q : \text{SAut}^{\text{gr}}(\bar{G}/k) \rightarrow \Gamma_k$ . Par exemple, si  $\bar{G}$  est commutatif, la donnée d'un  $k$ -lien sur  $\bar{G}$  équivaut à la donnée d'une section de  $q$  qui soit un morphisme de groupes, ce qui équivaut à la donnée d'une  $k$ -forme de  $\bar{G}$ . À l'aide de ces notions, on peut enfin définir un  $H^2$  non-abélien en termes de cocycles :

**Définition 2.** Soit  $L := (\bar{G}, \kappa)$  un  $k$ -lien sur un  $\bar{k}$ -groupe algébrique  $\bar{G}$ .

– Un 2-cocycle à coefficients dans  $L$  est un couple  $(f, g)$  d'applications continues

$$f : \begin{cases} \Gamma_k \longrightarrow \text{SAut}^{\text{gr}}(\bar{G}/k) \\ s \longmapsto f_s \end{cases} \quad \text{et} \quad g : \begin{cases} \Gamma_k \times \Gamma_k \longrightarrow \bar{G}(\bar{k}) \\ (s, t) \longmapsto g_{s,t} \end{cases}$$

vérifiant les conditions suivantes :

$$f \bmod \text{Int}(\bar{G}) = \kappa, \quad f_s \circ f_t = \text{int}(g_{s,t}) \circ f_{st}, \quad f_s(g_{t,u})g_{s,tu} = g_{s,t}g_{st,u}.$$

On note  $Z^2(k, L)$  l'ensemble des 2-cocycles à coefficients dans  $L$ .

– Deux 2-cocycles  $(f, g)$  et  $(f', g')$  sont dits équivalents s'il existe une application continue  $h : \Gamma_k \rightarrow \bar{G}(\bar{k})$  telle que

$$f'_s = \text{int}(h_s) \circ f_s \quad \text{et} \quad g'_{s,t} = h_s f_s(h_t) g_{s,t} h_{st}^{-1}.$$

La classe d'équivalence d'un élément  $(f, g) \in Z^2(k, L)$  est notée  $[(f, g)]$ . L'ensemble des classes d'équivalence est noté  $H^2(k, L)$ .

– Un 2-cocycle  $(f, g)$  est dit neutre si  $g_{s,t} = 1$  pour tout  $s, t \in \Gamma_k$ . Une classe  $\alpha \in H^2(k, L)$  est dite neutre si elle est représentée par un 2-cocycle neutre.

En particulier, si  $\bar{G}$  est commutatif, et si  $L$  est un  $k$ -lien sur  $\bar{G}$ , alors  $H^2(k, L)$  s'identifie au groupe abélien usuel  $H^2(k, G)$  où  $G$  est la  $k$ -forme de  $\bar{G}$  associée au  $k$ -lien  $L$ .

Pour finir, on rappelle la définition du type d'un toreur sous un tore (voir par exemple [Skorobogatov 2001, section 2.3]) : soit  $T$  un  $k$ -tore,

$$M := \text{Hom}_{\bar{k}\text{-groupes}}(\bar{T}, \overline{\mathbb{G}_m})$$

son module des caractères et  $Y \xrightarrow{T} X$  un  $X$ -torseur sous  $T$ . On appelle *type* du toreur  $Y \rightarrow X$  le morphisme  $\lambda : M \rightarrow \text{Pic}(\bar{X})$  défini de la façon suivante : si  $\chi : \bar{T} \rightarrow \overline{\mathbb{G}_m}$  est un élément de  $M$ ,  $\lambda(\chi)$  est la classe dans  $\text{Pic}(\bar{X})$  du  $\bar{X}$ -torseur sous  $\overline{\mathbb{G}_m}$  obtenu en poussant en avant le toreur  $Y \xrightarrow{T} X$  par le caractère  $\chi : \bar{T} \rightarrow \overline{\mathbb{G}_m}$ .

**2.2. Énoncé du résultat et structure de la preuve.** L'objectif de ce texte est donc de prouver le théorème suivant :

**Théorème 1.** *Soit  $k$  un corps de nombres, soit  $X$  une  $k$ -variété projective, lisse et géométriquement intègre. Alors  $X(\mathbb{A}_k)^{\text{ét}, \text{Br}} \subset X(\mathbb{A}_k)^{\text{desc}}$ .*

Comme mentionné dans l'introduction, ce résultat permet de répondre à la question posée dans [Poonen 2008] :

**Corollaire 2.** *Soit  $k$  un corps de nombres, soit  $X/k$  la variété construite dans [Poonen 2008]. Alors  $X$  est un contreexemple au principe de Hasse qui ne peut être expliqué par l'obstruction de descente, c'est-à-dire que l'on a  $X(\mathbb{A}_k)^{\text{desc}} \neq \emptyset$  alors que  $X(k) = \emptyset$ .*

*Preuve du théorème 1.* Soit  $(P_v) \in X(\mathbb{A}_k)^{\text{ét}, \text{Br}}$ . Soit  $G$  un  $k$  groupe algébrique linéaire. On se donne un  $X$ -torseur sous  $G$  :

$$f : Y \rightarrow X$$

L'objectif est de montrer que le point  $(P_v)$  se relève en un point de  $Y^\tau(\mathbb{A}_k)$ , pour un certain cocycle  $\tau$  à valeurs dans  $G$ . On remarque que dans le cas extrême où  $G$  est fini, ce résultat est évident puisque  $(P_v) \in X(\mathbb{A}_k)^{\text{ét}, \text{Br}}$  ; dans l'autre cas extrême où  $G$  est connexe, en utilisant l'inclusion évidente  $X(\mathbb{A}_k)^{\text{ét}, \text{Br}} \subset X(\mathbb{A}_k)^{\text{Br}}$ , c'est un résultat de Harari que l'on rappelle ici :

**Théorème 3** [Harari 2002, théorème 2(2)]. *Soit  $X$  une  $k$ -variété géométriquement intègre et  $G$  un  $k$ -groupe linéaire connexe. Si  $f : Y \rightarrow X$  est un  $X$ -torseur sous  $G$ , alors on a  $X(\mathbb{A}_k)^{\text{Br}} \subset X(\mathbb{A}_k)^f$ .*

Le principe de la preuve du théorème 1 consiste à ramener en quelque sorte le cas général au cas connexe et au théorème 3, grâce à la proposition 5 qui suit.

On commence par rappeler un résultat de Stoll :

**Lemme 4** (Stoll). *Soit  $X$  une  $k$ -variété projective lisse géométriquement intègre. Soit  $(P_v) \in X(\mathbb{A}_k)^{\text{ét}, \text{Br}}$  et soit  $g : Z \xrightarrow{F} X$  un  $X$ -torseur sous un  $k$ -groupe fini  $F$ . Alors il existe un  $k$ -groupe fini  $F'$ , un cocycle  $\sigma \in Z^1(k, F)$ , un  $X$ -torseur  $X' \xrightarrow{F'} X$  sous  $F'$ , un morphisme  $p : F' \rightarrow F^\sigma$  et un morphisme  $\psi : X' \rightarrow Z^\sigma$  faisant commuter le*

diagramme suivant (où les deux flèches verticales du carré supérieur sont données par les actions respectives de  $F'$  et  $F^\sigma$  sur  $X'$  et  $Z^\sigma$ ) :

$$\begin{array}{ccc}
 X' \times_k F' & \xrightarrow{\psi \times p} & Z^\sigma \times_k F^\sigma \\
 \downarrow & & \downarrow \\
 X' & \xrightarrow{\psi} & Z^\sigma \\
 \downarrow & & \downarrow \\
 X & \xrightarrow{=} & X
 \end{array}$$

et tels que la variété  $X'$  soit géométriquement intègre et  $(P_v)$  se relève en un point  $(Q'_v) \in X'(\mathbb{A}_k)^{\text{Br}}$ .

*Démonstration.* On considère le  $\bar{X}$ -torseur  $\bar{Z} \xrightarrow{\bar{F}} \bar{X}$ . Suivant [Stoll 2007, remarque précédant le lemme 5.6 et preuve du lemme 5.7], il existe un  $k$ -groupe fini  $F'$ , un  $X$ -torseur  $X' \xrightarrow{F'} X$  avec  $X'$  connexe (sur  $k$ ), un morphisme de groupes  $\bar{F}' \rightarrow \bar{F}$  et un diagramme commutatif

$$\begin{array}{ccc}
 \bar{X}' & \xrightarrow{\bar{\psi}} & \bar{Z} \\
 \searrow \bar{F}' & & \swarrow \bar{F} \\
 & \bar{X} &
 \end{array}$$

de sorte que le morphisme  $\bar{\psi}$  soit compatible aux actions respectives de  $\bar{F}'$  sur  $\bar{X}'$  et  $\bar{F}$  sur  $\bar{Z}$ . Quitte à tordre  $X' \rightarrow X$ , on peut supposer que  $(P_v)$  se relève dans  $X'(\mathbb{A}_k)^{\text{Br}}$  (puisque  $(P_v) \in X(\mathbb{A}_k)^{\text{ét, Br}}$ ). Dans ce cas, par le lemme 5.5 de [Stoll 2007], la variété  $X'$  est géométriquement intègre. On applique alors le lemme 5.6 du même article : il existe un cocycle  $\sigma \in Z^1(k, F)$ , un morphisme de  $k$ -groupes algébriques  $F' \rightarrow F^\sigma$  et un morphisme  $\psi$  s'insérant dans le diagramme commutatif

$$\begin{array}{ccc}
 X' & \xrightarrow{\psi} & Z^\sigma \\
 \searrow F' & & \swarrow F^\sigma \\
 & X &
 \end{array}$$

et tel que  $\psi$  soit compatible aux actions de  $F'$  et  $F^\sigma$ , via le morphisme  $F' \rightarrow F^\sigma$ . Cela conclut la preuve du lemme.  $\square$

Le point principal de la preuve du théorème 1 est résumé dans la proposition suivante, qui sera démontrée dans le paragraphe 3 :

**Proposition 5.** *Soit  $X$  une  $k$ -variété projective lisse géométriquement intègre. Soit  $(P_v) \in X(\mathbb{A}_k)^{\text{ét, Br}}$  et soit  $f : Y \xrightarrow{G} X$  un  $X$ -torseur sous un  $k$ -groupe algébrique*

linéaire  $G$ . Soit

$$1 \rightarrow H \rightarrow G \rightarrow F \rightarrow 1$$

une suite exacte de  $k$ -groupes linéaires, avec  $H$  connexe et  $F$  fini. On note  $Z \xrightarrow{F} X$  le poussé en avant de  $Y \rightarrow X$  par le morphisme  $G \rightarrow F$ . Soit alors  $\sigma \in Z^1(k, F)$  un 1-cocycle donné par le lemme 4 appliqué au torseur  $Z \rightarrow X$  et au point  $(P_v)$ .

Alors le cocycle  $\sigma \in Z^1(k, F)$  se relève en un cocycle  $\tau \in Z^1(k, G)$ .

Supposons la proposition 5 démontrée, et déduisons-en le théorème 1, à l'aide du lemme 4 et du théorème 3. Soit  $(P_v) \in X(\mathbb{A}_k)^{\text{ét}, \text{Br}}$ . Soit  $G$  un  $k$  groupe algébrique linéaire. On note  $H := G^\circ$  sa composante neutre. On a une suite exacte de groupes algébriques

$$1 \rightarrow H \rightarrow G \rightarrow F \rightarrow 1,$$

$F$  étant un  $k$ -groupe algébrique fini, et  $H$  étant linéaire connexe. On se donne un  $X$ -torseur sous  $G$  :

$$f : Y \rightarrow X$$

On peut décomposer ce torseur en deux torseurs, l'un sous le groupe connexe  $H$  et l'autre sous le groupe fini  $F$  : on a un dessin de la forme

$$\begin{array}{ccc} Y & & \\ \downarrow H & \searrow G & \\ Z & & \\ \downarrow F & \swarrow & \\ X & & \end{array}$$

L'objectif est de montrer que le point  $(P_v)$  se relève en un point de  $Y^\tau(\mathbb{A}_k)$ , pour un certain cocycle  $\tau$  à valeurs dans  $G$ .

On applique d'abord la proposition 5 au torseur  $f : Y \xrightarrow{G} X$ , au point  $(P_v)$  et à la suite exacte  $1 \rightarrow H \rightarrow G \rightarrow F \rightarrow 1$ . On obtient alors un cocycle  $\sigma \in Z^1(k, F)$  et un diagramme

$$\begin{array}{ccc} X' & \xrightarrow{\psi} & Z^\sigma \\ & \searrow F' & \swarrow F^\sigma \\ & X & \end{array}$$

satisfaisant les propriétés du lemme 4, et par la proposition 5, on sait que le cocycle  $\sigma \in Z^1(k, F)$  ainsi défini se relève en un cocycle  $\tau \in Z^1(k, G)$ . On considère alors le  $X$ -torseur tordu  $Y^\tau \xrightarrow{G^\tau} X$ . Ce torseur est naturellement muni d'une structure de

$Z^\sigma$ -torseur sous  $H^\tau$ , c'est-à-dire que l'on a un dessin de la forme

$$\begin{array}{ccc}
 R & \longrightarrow & Y^\tau \\
 \downarrow H^\tau & & \downarrow H^\tau \\
 X' & \xrightarrow{\psi} & Z^\sigma \\
 \downarrow F' & & \downarrow F^\sigma \\
 X & \xrightarrow{=} & X
 \end{array}
 \quad G^\tau$$

où  $R$  est défini comme le produit fibré de  $X'$  et  $Y^\tau$  au-dessus de  $Z^\sigma$ .

Le groupe  $H^\tau$  étant une  $k$ -forme de  $H$ , il est linéaire connexe. On peut donc lui appliquer le théorème 3 (on rappelle que  $X'$  est géométriquement intègre) : l'ensemble  $X'(\mathbb{A}_k)^{\text{Br}}$  est contenu dans l'ensemble de descente du toseur  $R \xrightarrow{H^\tau} X'$ , donc en particulier le point  $(Q'_v) \in X'(\mathbb{A}_k)^{\text{Br}}$  fourni par le lemme 4 et relevant  $(P_v)$  est l'image d'un point  $(R'_v) \in R^\mu(\mathbb{A}_k)$  pour un certain  $\mu \in Z^1(k, H^\tau)$ . Poussons alors le point  $(R'_v)$  dans  $(Y^\tau)^\mu$ . On obtient ainsi un point  $(R_v) \in (Y^\tau)^\mu(\mathbb{A}_k)$  au-dessus de  $(Q_v) := (\psi(Q'_v)) \in Z^\sigma(\mathbb{A}_k)$  et de  $(P_v) \in X(\mathbb{A}_k)$ . Notons  $\nu \in Z^1(k, G^\tau)$  l'image de  $\mu \in Z^1(k, H^\tau)$ ; alors  $(Y^\tau)^\mu = (Y^\tau)^\nu$ . Considérons alors la bijection de torsion par  $\tau$ ,  $t_\tau : Z^1(k, G^\tau) \rightarrow Z^1(k, G)$  (voir par exemple [Serre 1973, section I.5.3, proposition 35 bis]) et posons  $\rho := t_\tau(\nu) \in Z^1(k, G)$ . Alors un calcul simple assure que  $(Y^\tau)^\nu = Y^\rho$ , et donc  $(Y^\tau)^\mu = Y^\rho$ . Par conséquent, on a montré que  $(R_v)$  était dans  $Y^\rho(\mathbb{A}_k)$ , et par construction on a  $f^\rho((R_v)) = (P_v)$ . Donc  $(P_v) \in X(\mathbb{A}_k)^f$ , ce qui conclut la preuve du théorème 1, en admettant la proposition 5.  $\square$

**Remarque.** Avec les notations de la preuve, l'approche naïve pour montrer «directement» le théorème 1 sans le lemme 4 et la proposition 5 consisterait à appliquer le théorème 3 à un certain toseur  $Y^\tau \rightarrow Z^\sigma$  sous une  $k$ -forme du groupe connexe  $H$ , où  $(P_v) \in X(\mathbb{A}_k)^{\text{Br}}$  et  $\tau \in Z^1(k, G)$  relève  $\sigma$ . Cependant, cette approche se heurte à deux problèmes majeurs : d'abord on ne sait pas a priori si  $\sigma$  se relève ou non dans  $Z^1(k, G)$ , et ensuite il se peut que  $Z^\sigma$  ne soit pas géométriquement intègre (ce dont on a besoin pour appliquer le théorème 3). L'approche naïve ne suffit donc pas : on a besoin du lemme 4 pour remplacer  $Z^\sigma$  par une variété géométriquement intègre, ainsi que de la proposition 5 pour relever  $\sigma$  dans  $Z^1(k, G)$ .

### 3. Preuve de la proposition 5

On se place sous les hypothèses de la proposition 5, avec les mêmes notations. Pour tout  $k$ -groupe algébrique linéaire connexe  $H$ , on notera  $H^{\text{red}}$  le quotient de  $H$  par son radical unipotent  $R_u(H)$ ,  $H^{\text{ss}}$  le sous-groupe dérivé de  $H^{\text{red}}$ , et  $H^{\text{tor}}$  le quotient de  $H^{\text{red}}$  par  $H^{\text{ss}}$ . Ainsi,  $H^{\text{red}}$  est un groupe réductif (connexe),  $H^{\text{ss}}$  est un groupe semi-simple et  $H^{\text{tor}}$  est un  $k$ -tore.

Considérons pour commencer la suite exacte de la proposition 5 :

$$1 \rightarrow H \rightarrow G \rightarrow F \rightarrow 1$$

En quotientant  $H$  et  $G$  par le radical unipotent de  $H$ , puis en quotientant à nouveau par le sous-groupe dérivé  $H^{\text{ss}}$  ( $R_u(G)$  et  $H^{\text{ss}}$  sont des sous-groupes caractéristiques de  $H$  et  $H^{\text{red}}$  respectivement), on obtient le diagramme exact suivant :

$$\begin{array}{ccccccc} 1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & F \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow = \\ 0 & \longrightarrow & H^{\text{tor}} & \longrightarrow & G' & \longrightarrow & F \longrightarrow 1 \end{array}$$

Dans toute la suite, on notera  $T := H^{\text{tor}}$  le quotient torique de  $H$ .

Le groupe  $T$  étant abélien, la suite exacte ainsi obtenue induit une action par conjugaison de  $F$  sur  $T$ . On peut donc faire agir  $\Gamma_k$  sur  $T(\bar{k})$  via le cocycle  $\sigma$ , et on obtient ainsi l'action tordue suivante :  $\gamma.h := \tilde{\sigma}_\gamma \cdot {}^\gamma h \cdot \tilde{\sigma}_\gamma^{-1}$  pour  $\gamma \in \Gamma_k$  et  $h \in T(\bar{k})$ ,  $\tilde{\sigma}_\gamma$  désignant un relevé quelconque de  $\sigma_\gamma$  dans  $G'$ . On notera alors  $T^\sigma$  le  $k$ -tore ainsi obtenu, en tordant  $T$  par cette action de  $\sigma$ .

Voyons désormais le cocycle  $\sigma$  (défini dans l'énoncé de la proposition 5, à partir du lemme 4) comme un espace principal homogène (à droite) de  $F$  sur  $k$ , que l'on notera  $U \xrightarrow{F} \text{Spec } k$ . La  $k$ -variété  $U$  est définie de la façon suivante :  $U(\bar{k}) := F(\bar{k})$  et l'action de  $\Gamma_k$  sur  $U(\bar{k})$  est donnée par  $(\gamma, f) \mapsto \sigma_\gamma \cdot ({}^\gamma f)$  pour  $\gamma \in \Gamma_k$  et  $f \in U(\bar{k}) = F(\bar{k})$ , le produit désignant le produit dans le groupe  $F(\bar{k})$ . La variété  $U$  est ainsi un  $k$ -torseur (à droite) sous  $F$ , dont la classe dans  $H^1(k, F)$  est exactement  $[\sigma]$ . Le morphisme quotient  $G \rightarrow F$  munit  $U$  d'une structure d'espace homogène de  $G$  sur  $k$ , à stabilisateur géométrique connexe  $\bar{H}$ .

Dans une telle situation, Springer a construit un  $k$ -lien  $\kappa_\sigma$  sur  $\bar{H}$  et une classe  $\eta_\sigma \in H^2(k, \kappa_\sigma)$  associés à l'espace homogène  $U$ . On rappelle brièvement cette construction (voir par exemple [Flicker et al. 1998, (5.1)] ou [Borovoi 1993, 7.7]) : on fixe un point  $u_0 \in U(\bar{k})$  (dans toute la suite, on choisira pour  $u_0$  le point de  $U(\bar{k})$  correspondant au neutre  $1 \in F(k)$ ), son stabilisateur dans  $\bar{G}$  est le sous-groupe  $\bar{H}$ . Il existe alors une application localement constante

$$\begin{array}{ccc} \Gamma_k & \longrightarrow & \bar{G}(\bar{k}) \\ \gamma & \longmapsto & g_\gamma \end{array}$$

telle que pour tout  $\gamma \in \Gamma_k$ , on ait  ${}^\gamma u_0 = u_0 \cdot g_\gamma$ . On vérifie alors que pour  $\gamma \in \Gamma_k$ , l'application  $\text{int}(g_\gamma) \circ \gamma^*$  est un automorphisme semi-linéaire de  $\bar{G}$  qui laisse  $\bar{H}$  invariant. On note  $f_\gamma \in \text{SAut}^{\text{gr}}(\bar{H}/k)$  sa restriction à  $\bar{H}$ . Alors l'application  $\kappa_\sigma : \gamma \mapsto f_\gamma \bmod \text{Int}(\bar{H})$  définit un  $k$ -lien sur  $\bar{H}$ , et si  $g_{\gamma, \tau} := g_\gamma ({}^\gamma g_\tau) g_{\gamma, \tau}^{-1}$ , la classe de Springer  $\eta_\sigma$  est par définition la classe du 2-cocycle  $(f, g)$  dans  $H^2(k, \kappa_\sigma)$ . La principale propriété de la classe  $\eta_\sigma$  est la suivante [Flicker et al. 1998, (5.1)] :  $\eta_\sigma$  est neutre dans  $H^2(k, \kappa_\sigma)$  si et seulement si l'espace homogène  $U$  de  $G$  est dominé

par un espace principal homogène de  $G$ , c'est-à-dire si et seulement si il existe un espace principal homogène  $V$  de  $G$  et un morphisme  $V \rightarrow U$  qui est  $G$ -équivariant. En particulier,  $\eta_\sigma$  est neutre si et seulement si  $[\sigma] \in H^1(k, F)$  se relève dans  $H^1(k, G)$ . Enfin, on remarque que puisque le morphisme de groupes algébriques  $G \rightarrow F$  est surjectif, le fait que  $[\sigma]$  se relève dans  $H^1(k, G)$  est équivalent au fait que le cocycle  $\sigma$  se relève dans  $Z^1(k, G)$ . Par conséquent il suffit, pour montrer la proposition 5, de montrer que la classe  $\eta_\sigma$  est neutre dans  $H^2(k, \kappa_\sigma)$ .

Suivant [Borovoi 1993, 6.1.2], on dispose alors des morphismes d'abélianisation suivants :

$$H^2(k, \kappa_\sigma) \xrightarrow{\text{ab}^2} H_{\text{ab}}^2(k, \kappa_\sigma) \xrightarrow{t_{\text{ab}}} H^2(k, S^\sigma)$$

où  $S^\sigma$  est la  $k$ -forme de  $\bar{T}$  canoniquement associée au  $k$ -lien sur  $\bar{T}$  induit par le lien  $\kappa_\sigma$ . On notera  $\eta'_\sigma \in H^2(k, S^\sigma)$  l'image de  $\eta_\sigma$  par la composée de ces morphismes. On dispose alors du lemme suivant :

**Lemme 6.** *Sous les hypothèses de la proposition 5, et avec les notations précédentes :*

- (1) *La classe de Springer  $\eta_\sigma \in H^2(k, \kappa_\sigma)$  associée au cocycle  $\sigma$  est une classe localement neutre en toute place  $v$  de  $k$ .*
- (2) *Les  $k$ -tores  $S^\sigma$  et  $T^\sigma$  sont isomorphes.*

*Preuve du lemme 6.* (1) Pour toute place  $v$  de  $k$ , le fait que  $Z^\sigma$  admette un  $k_v$ -point  $Q_v$  assure que  $[\sigma_v] \in H^1(k_v, F)$  coïncide avec la classe de  $[Z](P_v)$ . Or cette dernière est l'image de  $[Y](P_v) \in H^1(k_v, G)$ , donc  $[\sigma_v]$  se relève dans  $H^1(k_v, G)$ , donc  $(\eta_\sigma)_v \in H^2(k_v, \kappa_\sigma)$  est une classe neutre.

(2) Revenons à la construction de  $S^\sigma$  : on fixe  $u_0 \in U(\bar{k})$ , correspondant à l'élément neutre  $1 \in F(\bar{k}) = U(\bar{k})$ , et pour tout  $\gamma \in \Gamma_k$ , un élément  $g_\gamma \in \bar{G}$  tel que  ${}^\gamma u_0 = u_0 \cdot g_\gamma$  dans  $\bar{U}$ , de sorte que l'application  $\gamma \mapsto g_\gamma$  soit localement constante. Le lien  $\kappa_\sigma$  induit, via la surjection  $H \rightarrow T$ , un  $k$ -lien  $\kappa'_\sigma$  sur  $\bar{T}$ , défini par

$$\begin{aligned} \Gamma_k &\longrightarrow \text{SAut}^{\text{gr}}(\bar{T}/k) \\ \gamma &\longmapsto (\bar{h} \mapsto \overline{g_\gamma \cdot ({}^\gamma h) \cdot g_\gamma^{-1}}) \end{aligned}$$

où  $\bar{h}$  désigne l'image de l'élément  $h \in H$  dans  $T$ . Ce morphisme définit la  $k$ -forme  $S^\sigma$ , alors que  $T^\sigma$  est quant à lui défini par le morphisme

$$\begin{aligned} \Gamma_k &\longrightarrow \text{SAut}^{\text{gr}}(\bar{T}/k) \\ \gamma &\longmapsto (\bar{h} \mapsto \overline{\tilde{\sigma}_\gamma \cdot ({}^\gamma h) \cdot \tilde{\sigma}_\gamma^{-1}}) \end{aligned}$$

Il suffit donc de vérifier que pour tout  $\gamma \in \Gamma_k$ ,  $g_\gamma \in \bar{G}$  s'envoie sur  $\sigma_\gamma \in \bar{F}$  par le morphisme quotient  $G \xrightarrow{\pi} F$ . Or ceci est clair par la formule qui définit les  $g_\gamma$  : on a  ${}^\gamma u_0 = \sigma_\gamma \cdot 1 = \sigma_\gamma$  dans  $F(\bar{k})$  (c'est la définition de l'action de  $\Gamma_k$  sur  $\bar{U}$ , sachant



que  $1 \in F(k)$ , et par ailleurs  ${}^{\gamma}u_0 = u_0 \cdot g_{\gamma} = 1 \cdot \pi(g_{\gamma}) = \pi(g_{\gamma})$  dans  $F(\bar{k})$  (le premier produit est l'action de  $G$  sur  $U$  et le second est le produit dans  $F(\bar{k})$ ). Cette formule assure que  $\pi(g_{\gamma}) = \sigma_{\gamma}$ , ce qui prouve le  $k$ -isomorphisme  $S^{\sigma} \cong T^{\sigma}$ .  $\square$

En résumé, on a donc montré que la classe de Springer  $\eta_{\sigma} \in H^2(k, \kappa_{\sigma})$  s'envoyait par la flèche d'abélianisation sur  $\eta'_{\sigma} \in \text{III}^2(k, T^{\sigma})$ , où

$$\text{III}^2(k, T^{\sigma}) := \{ \alpha \in H^2(k, T^{\sigma}) : \alpha_v = 0 \in H^2(k_v, T^{\sigma}) \text{ pour toute place } v \text{ de } k \}.$$

On cherche désormais à identifier cette classe  $\eta'_{\sigma}$ . Pour cela, on remarque que le toreur  $Y \xrightarrow{H} Z$  fournit un toreur intermédiaire  $\varpi : W \xrightarrow{T} Z$  après quotient par le radical unipotent  $R_u(H)$  de  $H$ , puis par le sous-groupe dérivé  $H^{\text{ss}}$  de  $H/R_u(H)$ . On note  $\lambda : M \rightarrow \text{Pic}(\bar{Z})$  le type de ce toreur, où  $M$  désigne le module des caractères du tore  $T = H^{\text{tor}}$  (voir paragraphe 2.1, ou [Skorobogatov 2001, paragraphe 2.3], pour la définition du type d'un toreur sous un tore). L'application  $\lambda$  est un morphisme de  $\Gamma_k$ -modules. Notons  $M^{\sigma}$  le module des caractères du tore  $T^{\sigma}$ . Alors  $M$  et  $M^{\sigma}$  sont canoniquement isomorphes comme groupes abéliens, et il en est de même pour  $\text{Pic}(\bar{Z})$  et  $\text{Pic}(\bar{Z}^{\sigma})$ . Donc  $\lambda$  induit un morphisme de groupes abéliens  $\lambda^{\sigma} : M^{\sigma} \rightarrow \text{Pic}(\bar{Z}^{\sigma})$ .

**Lemme 7.** *Sous les hypothèses de la proposition 5, et avec les mêmes notations, l'application  $\lambda^{\sigma} : M^{\sigma} \rightarrow \text{Pic}(\bar{Z}^{\sigma})$  est un morphisme de  $\Gamma_k$ -modules.*

*Preuve du lemme 7.* Le groupe  $\bar{F}$  agit sur  $\bar{T}$ , sur  $M$ , sur  $\bar{Z}$  et sur  $\text{Pic}(\bar{Z})$  de la façon suivante :

- $F$  agit à gauche sur  $T$  par conjugaison :  $(f, t) \mapsto gtg^{-1}$ .
- $F$  agit à gauche sur  $M$  via  $(f, \chi) \mapsto (f \cdot \chi : t \mapsto \chi(g^{-1}tg))$ .
- $F$  agit à droite sur  $Z$  via la structure de  $X$ -torseur sous  $F$  dont est muni  $Z$ .
- $F$  agit à gauche sur  $\text{Pic}(\bar{Z})$  via l'action précédente : si  $f : \bar{Z} \rightarrow \bar{Z}$  désigne l'action de  $f \in F$  sur  $\bar{Z}$ , et si  $L \in \text{Pic}(\bar{Z})$ , alors  $f \cdot L := f^*L$ .

Montrons alors que pour ces actions naturelles, le morphisme  $\lambda : M \rightarrow \text{Pic}(\bar{Z})$  est  $\bar{F}$ -équivariant.

Soit  $f \in \bar{F}$ , et  $g \in \bar{G}'$  relevant  $f$ . On a alors un diagramme commutatif de morphismes de  $\bar{k}$ -variétés :

$$\begin{array}{ccc} \bar{W} & \xrightarrow{g} & \bar{W} \\ \downarrow \varpi & & \downarrow \varpi \\ \bar{Z} & \xrightarrow{f} & \bar{Z} \end{array}$$

les morphismes horizontaux étant les actions naturelles de  $\bar{G}'$  sur  $\bar{W}$  et de  $\bar{F}$  sur  $\bar{Z}$ . Ce diagramme induit un diagramme commutatif :

$$\begin{array}{ccc}
\overline{W} \times_{\overline{k}} \overline{\mathbb{G}_m} & \xrightarrow{g} & \overline{W} \times_{\overline{k}} \overline{\mathbb{G}_m} \\
\downarrow & & \downarrow \\
\overline{W} & \xrightarrow{g} & \overline{W} \\
\downarrow \varpi & & \downarrow \varpi \\
\overline{Z} & \xrightarrow{f} & \overline{Z}
\end{array}$$

le morphisme  $\overline{W} \times_{\overline{k}} \overline{\mathbb{G}_m} \xrightarrow{g} \overline{W} \times_{\overline{k}} \overline{\mathbb{G}_m}$  étant induit par l'action de  $g$  sur  $\overline{W}$  et l'identité sur  $\overline{\mathbb{G}_m}$ , et les morphismes verticaux  $\overline{W} \times_{\overline{k}} \overline{\mathbb{G}_m} \rightarrow \overline{W}$  étant donnés par la première projection.

Soit alors  $\chi \in M$  un caractère de  $\overline{T}$ . On dispose de deux actions à gauche de  $\overline{T}$  sur la variété  $\overline{W} \times_{\overline{k}} \overline{\mathbb{G}_m}$  : la première est l'action classique, à savoir  $t \cdot_{\chi}(w, \mu) := (w \cdot t^{-1}, \chi(t)\mu)$ , la seconde est l'action «tordue» par  $f$ , à savoir l'action associée au caractère  $f \cdot \chi : t \cdot_{f \cdot \chi}(w, \mu) := (w \cdot t^{-1}, (f \cdot \chi)(t) \cdot \mu)$ , où l'action de  $F$  sur  $M$  est celle définie plus haut :  $(f \cdot \chi)(t) := \chi(g^{-1} \cdot t \cdot g)$ . Si l'on quotiente  $\overline{W} \times_{\overline{k}} \overline{\mathbb{G}_m}$  par la première action de  $\overline{T}$ , on obtient un toreur à droite

$$\overline{W}_{\chi} \xrightarrow{\mathbb{G}_m} \overline{Z}$$

dont la classe  $[\overline{W}_{\chi}]$  dans  $\text{Pic}(\overline{Z})$  est par définition le type du toreur  $\overline{W} \xrightarrow{\overline{T}} \overline{Z}$  évalué en  $\chi$ , i.e.  $\lambda(\chi)$  (voir la définition du type d'un toreur à la page 242 ; voir également [Skorobogatov 2001, lemme 2.3.1(i)]). De même, quand on quotiente  $\overline{W} \times_{\overline{k}} \overline{\mathbb{G}_m}$  par la seconde action de  $\overline{T}$  (tordue par  $f$ ), on obtient un toreur  $\overline{W}_{f \cdot \chi} \xrightarrow{\mathbb{G}_m} \overline{Z}$ , dont la classe est exactement  $\lambda(f \cdot \chi)$ .

Considérons alors le morphisme  $\phi = g : \overline{W} \times_{\overline{k}} \overline{\mathbb{G}_m} \rightarrow \overline{W} \times_{\overline{k}} \overline{\mathbb{G}_m}$  introduit précédemment. On vérifie aisément que

$$\phi(t \cdot_{f \cdot \chi}(w, \mu)) = (g^{-1} \cdot t \cdot g) \cdot_{\chi} \phi(w, \mu) = (f^{-1} \cdot t) \cdot_{\chi} \phi(w, \mu),$$

où les actions de  $\overline{T}$  dans les deux membres de l'égalité sont les deux actions définies plus haut. Cette formule assure que le morphisme  $\phi$  passe au quotient par les actions respectives de  $\overline{T}$  au départ et à l'arrivée. Donc  $\phi$  induit un morphisme

$$\tilde{\phi} : \overline{W}_{f \cdot \chi} \rightarrow \overline{W}_{\chi}$$

et on vérifie que ce morphisme s'inscrit dans le diagramme cartésien suivant :

$$\begin{array}{ccc}
\overline{W}_{f \cdot \chi} & \xrightarrow{\tilde{\phi}} & \overline{W}_{\chi} \\
\downarrow \mathbb{G}_m & & \downarrow \mathbb{G}_m \\
\overline{Z} & \xrightarrow{f} & \overline{Z}
\end{array}$$

qui assure que la classe  $[\overline{W}_{f,\chi}]$  du toseur  $\overline{W}_{f,\chi} \xrightarrow{\mathbb{G}_m} \overline{Z}$  dans le groupe de Picard de  $\overline{Z}$  s'obtient en faisant agir  $f$  sur la classe  $[\overline{W}_\chi]$  du toseur  $\overline{W}_\chi \xrightarrow{\mathbb{G}_m} \overline{Z}$ , c'est-à-dire que l'on a bien la relation  $[\overline{W}_{f,\chi}] = f^*[\overline{W}_\chi]$ , ce qui se réécrit

$$\lambda(f.\chi) = f.\lambda(\chi).$$

Donc  $\lambda$  est  $\overline{F}$ -équivariant.

On conclut la preuve du lemme 7 de la façon suivante : pour tout  $\gamma \in \Gamma_k$ , on note  ${}^{\gamma'}m$  l'action de  $\gamma$  sur  $M^\sigma$  et  $\text{Pic}(\overline{Z}^\sigma)$ , et  ${}^{\gamma}m$  l'action de  $\gamma$  sur  $M$  et  $\text{Pic}(\overline{Z})$ . On a alors  $\lambda({}^{\gamma'}\chi) = \lambda(({}^{\gamma}\chi) \circ \text{int}(\sigma_\gamma^{-1})) = \lambda(\sigma_\gamma.({}^{\gamma}\chi))$  par définition (où  $\text{int}(a) : t \mapsto ata^{-1}$ ). Or par la  $\overline{F}$ -équivariance de  $\lambda$ , on a la relation  $\lambda(\sigma_\gamma.({}^{\gamma}\chi)) = \sigma_\gamma.\lambda({}^{\gamma}\chi)$ , et enfin  $\lambda$  est Galois-équivariant pour l'action non-tordue, c'est-à-dire  $\lambda({}^{\gamma}\chi) = {}^{\gamma}\lambda(\chi)$ , d'où  $\sigma_\gamma.\lambda({}^{\gamma}\chi) = \sigma_\gamma.{}^{\gamma}\lambda(\chi) = {}^{\gamma'}\lambda(\chi)$ . En conclusion, on a bien montré que

$$\lambda({}^{\gamma'}\chi) = {}^{\gamma'}\lambda(\chi),$$

ce qui prouve le lemme 7. □

**Remarque.** Ce lemme est à rapprocher de la preuve de [Harari et Skorobogatov 2005, proposition 2.5].

On déduit de ce  $\Gamma_k$ -morphisme  $\lambda^\sigma$  un nouveau morphisme de  $\Gamma_k$ -modules, noté  $\lambda' : M^\sigma \rightarrow \text{Pic}(\overline{X}')$ , obtenu en composant  $\lambda^\sigma$  avec le morphisme naturel  $\text{Pic}(\overline{Z}^\sigma) \rightarrow \text{Pic}(\overline{X}')$ . Puisque  $\bar{k}[X']^* = \bar{k}^*$  (en effet,  $X'$  est géométriquement intègre par construction, et  $X$  est propre,  $X' \rightarrow X$  est fini, donc  $X'$  est propre), ce morphisme définit un élément  $\partial(\lambda') \in H^2(k, T^\sigma)$  via la suite exacte de la théorie de la descente abélienne (voir par exemple [Colliot-Thélène et Sansuc 1987, théorème 1.5.1] ou [Skorobogatov 2001, corollaire 2.3.9]) :

$$0 \rightarrow H^1(k, T^\sigma) \rightarrow H^1(X', T^\sigma) \xrightarrow{\text{type}} \text{Hom}_k(M^\sigma, \text{Pic}(\overline{X}')) \xrightarrow{\partial} H^2(k, T^\sigma) \quad (1)$$

On va alors identifier cet élément  $\partial(\lambda')$  avec l'élément  $\eta'_\sigma$  dans  $H^2(k, T^\sigma)$ . Remarquons également que la suite exacte

$$0 \rightarrow T \rightarrow G' \rightarrow F \rightarrow 1$$

et l'élément  $[\sigma] \in H^1(k, F)$  définissent un élément  $\Delta(\sigma) \in H^2(k, T^\sigma)$  qui est l'obstruction à relever  $[\sigma]$  en un élément de  $H^1(k, G')$  [Serre 1973, I.5.6].

**Lemme 8.** *Sous les hypothèses de la proposition 5, les trois classes  $\partial(\lambda')$ ,  $\Delta(\sigma)$  et  $\eta'_\sigma$  coïncident (au signe près) dans  $H^2(k, T^\sigma)$ .*

Admettant ce lemme, on conclut la preuve de la proposition 5 de la façon suivante : par le corollaire 6.1.3(1) de [Skorobogatov 2001], les faits que  $X'(\mathbb{A}_k)^{\text{Br}}$  soit non-vide et que  $\bar{k}[X']^* = \bar{k}^*$  assurent l'existence d'un  $X'$ -torseur sous  $T^\sigma$  de type  $\lambda'$  (il suffisait pour cela d'avoir  $X'(\mathbb{A}_k)^{\text{Br}_{\lambda'}} \neq \emptyset$  : voir [Skorobogatov 2001, p. 113])

pour la définition de  $\text{Br}_{\lambda'}$ , ce qui assure que  $\partial(\lambda') = 0$  par la théorie de la descente (voir la suite exacte (1), page 250), et donc que  $\eta'_\sigma = 0$  dans  $H^2(k, T^\sigma)$  par le lemme 8. Pour finir, on utilise la proposition 6.5 de [Borovoi 1993] qui assure que la nullité de  $\eta'_\sigma$  implique que la classe  $\eta_\sigma \in H^2(k, \kappa_\sigma)$  est neutre (puisque  $\eta_\sigma$  est neutre localement partout par le lemme 6). Cela termine la preuve de la proposition 5 (en admettant le lemme 8), puisqu'alors  $U$  est dominé par un espace principal homogène de  $G$ , dont la classe  $[\tau] \in H^1(k, G)$  s'envoie sur  $[\sigma] \in H^1(k, F)$ .  $\square$

*Preuve du lemme 8.* Avant tout, fixons pour tout  $\gamma \in \Gamma_k$  un élément  $a_\gamma \in \bar{G}'$  relevant  $\sigma_\gamma \in \bar{F}$ , de sorte que l'application  $\gamma \mapsto a_\gamma$  soit localement constante.

Identifions d'abord les classes  $\eta'_\sigma$  et  $\Delta(\sigma)$  dans  $H^2(k, T^\sigma)$  :  $\eta_\sigma$  est représenté par un 2-cocycle non-abélien  $(f, g)$ , avec  $f : \Gamma_k \rightarrow \text{SAut}(\bar{H})$  et  $g : \Gamma_k \times \Gamma_k \rightarrow \bar{H}$ . On sait alors qu'un cocycle représentant  $\eta'_\sigma$  est donné par  $z' : \Gamma_k \times \Gamma_k \rightarrow \bar{T}^\sigma$  tel que  $z'_{s,t} = r(g_{s,t})$ , où  $r : H \rightarrow T$  est le morphisme quotient naturel. D'après l'appendice de [Borovoi 1993],  $g_{s,t} = b_s \cdot ({}^s b_t) \cdot b_{st}^{-1}$ , où  $b : \Gamma_k \rightarrow G(\bar{k})$  est une application continue telle que  ${}^s u_0 = u_0 \cdot b_s$  pour tout  $s \in \Gamma_k$ ,  $u_0 \in \bar{U}$  étant par exemple le point de  $U$  correspondant au neutre de  $F$ . Or on a vérifié dans la preuve du second point du lemme 6 qu'alors  $b_s$  s'envoie sur  $\sigma_s$  dans  $\bar{F}$ , ce qui assure que l'image de  $b_s$  dans  $\bar{G}'$  est un relevé de  $\sigma_s$ , que l'on peut donc supposer égal à  $a_s$ . Cela montre que le cocycle  $z'_{s,t}$  est cohomologue au cocycle  $s, t \mapsto a_s \cdot ({}^s a_t) \cdot a_{st}^{-1}$ , qui est un représentant de  $\Delta(\sigma)$  [Serre 1973, I.5.6], ce qui permet bien d'identifier  $\Delta(\sigma)$  et  $\eta'_\sigma$  dans  $H^2(k, T^\sigma)$  (au signe près).

Construisons désormais une nouvelle classe  $\text{Cl}(E) \in H^2(k, T^\sigma)$  coïncidant (au signe près) avec  $\partial(\lambda')$ . On considère pour cela le diagramme suivant, où  $\phi : \bar{Z}^\sigma \rightarrow \bar{Z}$  est l'isomorphisme canonique de schémas :

$$\begin{array}{ccccc}
 \bar{V}' & \xrightarrow{\tilde{\psi}} & \bar{V} & \xrightarrow{\tilde{\phi}} & \bar{W} \\
 \downarrow \bar{T}^\sigma & & \downarrow \bar{T}^\sigma & & \downarrow \bar{T} \\
 \bar{X}' & \xrightarrow{\psi} & \bar{Z}^\sigma & \xrightarrow{\phi} & \bar{Z} \\
 \downarrow \bar{F}' & & \downarrow \bar{F}^\sigma & & \downarrow \bar{F} \\
 \bar{X} & \xrightarrow{=} & \bar{X} & \xrightarrow{=} & \bar{X}
 \end{array} \quad \bar{G}' \quad (2)$$

les deux carrés du haut étant cartésiens (c'est-à-dire  $\bar{V}$  est défini comme le produit fibré de  $\bar{W}$  et  $\bar{Z}^\sigma$  au-dessus de  $\bar{Z}$ , et  $\bar{V}'$  comme le produit fibré de  $\bar{W}$  et  $\bar{X}'$  au-dessus de  $\bar{Z}$ ). Alors  $\tilde{\phi}$  est un isomorphisme de  $\bar{Z}$ -torseurs, et les trois toseurs  $\bar{W} \rightarrow \bar{Z}$ ,  $\bar{V} \rightarrow \bar{Z}^\sigma$  et  $\bar{V}' \rightarrow \bar{X}'$  ont pour types respectifs les morphismes de  $\Gamma_k$ -modules  $\lambda : M \rightarrow \text{Pic}(\bar{Z})$ ,  $\lambda^\sigma : M^\sigma \rightarrow \text{Pic}(\bar{Z}^\sigma)$  et  $\lambda' : M^\sigma \rightarrow \text{Pic}(\bar{X}')$ . Ces morphismes étant  $\Gamma_k$ -équivariants (grâce au lemme 7), on peut définir suivant [Harari et Skorobogatov 2002, définition 3.6] le sous-groupe  $E := \text{SAut}_{T^\sigma}(\bar{V}'/X')$  de  $\text{SAut}(\bar{V}'/X')$  formé

des automorphismes semi-linéaires  $\varphi$  tels que  $\varphi(\bar{v}'.\bar{t}) = \varphi(\bar{v}').(q^{(\varphi)}\bar{t})$  pour tout  $\bar{v}' \in \bar{V}'$  et  $\bar{t} \in \bar{T}$ , où  $q$  est le morphisme  $\text{SAut}(\bar{V}'/X') \rightarrow \Gamma_k$  introduit à la page 240 et l'action de  $q(\varphi)$  sur  $\bar{t}$  est donnée par la  $k$ -forme  $T^\sigma$  de  $\bar{T}$ . Ce groupe  $E$  s'intègre alors dans la suite exacte suivante (où  $q'$  désigne la restriction de  $q$  à  $E$ ) :

$$1 \rightarrow T^\sigma(\bar{k}) \rightarrow E \xrightarrow{q'} \Gamma_k \rightarrow 1$$

et cela permet de définir une classe  $\text{Cl}(E) \in H^2(k, T^\sigma)$  qui est l'obstruction à descendre le tore  $\bar{V}' \rightarrow \bar{X}'$  en un  $X'$ -torseur de type  $\lambda'$  (voir [Harari et Skorobogatov 2002, section 3.3]).

Alors les deux classes  $\partial(\lambda')$  et  $\text{Cl}(E)$  coïncident au signe près dans  $H^2(k, T^\sigma)$  : c'est exactement la proposition 3.7(3) de [Harari et Skorobogatov 2002].

Pour finir la preuve du lemme 8, on va identifier (au signe près)  $\text{Cl}(E)$  et  $\Delta(\sigma)$ . Pour cela, on a besoin du résultat suivant (pour traiter le cas où  $Z$  n'est pas géométriquement intègre) :

**Lemme 9.** *Sous les hypothèses de la proposition 5, on a un diagramme commutatif exact de la forme*

$$\begin{array}{ccccccc} 1 & \longrightarrow & \overline{T^\sigma}(\overline{Z^\sigma}) & \longrightarrow & \text{SAut}_{T^\sigma}(\bar{V}/Z^\sigma) & \xrightarrow{q} & \Gamma_k \longrightarrow 1 \\ & & \downarrow \psi^* & & \downarrow \psi^* & & \downarrow = \\ 1 & \longrightarrow & \overline{T^\sigma}(\bar{X}') = \overline{T^\sigma}(\bar{k}) & \longrightarrow & E = \text{SAut}_{T^\sigma}(\bar{V}'/X') & \xrightarrow{q'} & \Gamma_k \longrightarrow 1 \end{array} \quad (3)$$

Avant de prouver ce résultat, on le suppose connu afin d'achever la démonstration du lemme 8. On définit une section  $\gamma \mapsto \varphi_\gamma$  de  $q : \text{SAut}_{T^\sigma}(\bar{V}/Z^\sigma) \rightarrow \Gamma_k$  de la façon suivante : pour  $\gamma \in \Gamma_k$ , on construit grâce au diagramme (2) un morphisme  $\varphi_\gamma$  défini par :

$$\begin{aligned} \bar{V} &\longrightarrow \bar{V} \\ v &\longmapsto \varphi_\gamma(v) := \tilde{\phi}^{-1}(\gamma \tilde{\phi}(v).a_\gamma^{-1}) \end{aligned}$$

où  $a_\gamma \in \bar{G}'(\bar{k})$  agit sur  $\bar{W}$  grâce à la structure de  $\bar{X}$ -torseur sous  $\bar{G}'$  de  $\bar{W}$ . On vérifie facilement que  $\gamma \mapsto \varphi_\gamma$  définit bien une section (ensembliste) de  $q$ . Avec le diagramme commutatif (3), on en déduit une section  $\varphi' := \psi^* \circ \varphi$  de  $q' : E \rightarrow \Gamma_k$ .

On calcule alors  $\varphi_s.\varphi_t.\varphi_{st}^{-1} \in \overline{T^\sigma}(\overline{Z^\sigma})$ . On trouve facilement (en utilisant que  $\tilde{\phi}$  est  $\overline{T^\sigma}$ -équivariant) que  $\varphi_s.\varphi_t.\varphi_{st}^{-1} = a_{st}.(^s a_t)^{-1}.a_s^{-1}$  dans  $\overline{T^\sigma}(\overline{Z^\sigma})$  (où on envoie  $\overline{T^\sigma}(\bar{k})$  dans  $\overline{T^\sigma}(\overline{Z^\sigma})$  via le morphisme structural  $\overline{Z^\sigma} \rightarrow \text{Spec } \bar{k}$ ). Appliquons maintenant  $\psi^* : \overline{T^\sigma}(\overline{Z^\sigma}) \rightarrow \overline{T^\sigma}(\bar{k})$  : on obtient alors, par commutativité du diagramme (3) et par construction de  $\varphi'$  à partir de  $\varphi$ , l'égalité  $\varphi'_s.\varphi'_t.\varphi'_{st}{}^{-1} = a_{st}.(^s a_t)^{-1}.a_s^{-1}$  dans  $\overline{T^\sigma}(\bar{k})$ .

Or par définition de  $\text{Cl}(E)$ , le 2-cocycle  $s, t \mapsto \varphi'_s.\varphi'_t.\varphi'_{st}{}^{-1}$  est un représentant de  $\text{Cl}(E) \in H^2(k, T^\sigma)$ , et le 2-cocycle  $s, t \mapsto a_s.(^s a_t).a_{st}^{-1}$  est un représentant de la classe  $\Delta(\sigma)$ , donc les classes  $\Delta(\sigma)$  et  $\text{Cl}(E)$  coïncident au signe près dans

$H^2(k, T^\sigma)$ . On a donc montré que  $\Delta(\sigma) = \text{Cl}(E)$  au signe près dans  $H^2(k, T^\sigma)$ , d'où le lemme 8.  $\square$

*Preuve du lemme 9.* Suivant [Harari et Skorobogatov 2002, proposition 3.7(1)], l'exactitude de la seconde ligne est assurée par le fait que le morphisme  $\lambda'$  correspondant est  $\Gamma_k$ -équivariant. L'exactitude de la première ligne est due à l'existence d'une section ensembliste  $\varphi$  de  $q$  (voir paragraphe précédent).

La flèche  $\psi^* : \overline{T^\sigma}(\overline{Z^\sigma}) \rightarrow \overline{T^\sigma}(\overline{X'})$  du lemme 9 est la flèche naturelle induite par  $\psi : X' \rightarrow Z^\sigma$ .

Définissons désormais la flèche  $\psi^* : \text{SAut}_{T^\sigma}(\overline{V}/Z^\sigma) \rightarrow \text{SAut}_{T^\sigma}(\overline{V'}/X')$ . Soit  $\gamma \in \Gamma_k$ , et prenons  $\varphi \in \text{SAut}_{T^\sigma}(\overline{V}/Z^\sigma)$  tel que  $q(\varphi) = \gamma$ . On considère le diagramme suivant de morphismes de schémas, les flèches  $\text{pr}_1$ ,  $\tilde{\psi}$ ,  $\psi$  et  $\text{can}$  étant celles qui apparaissent dans le diagramme (2), et  $\gamma^*$  désignant l'action de Galois de  $\gamma$  sur  $\overline{X'}$  :

$$\begin{array}{ccc} \overline{V'} & \xrightarrow{\varphi \circ \tilde{\psi}} & \overline{V} \\ \gamma^{*-1} \circ \text{pr}_1 \downarrow & & \downarrow \text{can} \\ \overline{X'} & \xrightarrow{\psi} & \overline{Z^\sigma} \end{array}$$

Ce diagramme est commutatif, puisque si  $v' \in \overline{V'}$ , l'image de  $\varphi(\tilde{\psi}(v'))$  dans  $\overline{Z^\sigma}$  coïncide avec  $\gamma^{*-1}(z)$ , où  $z$  est l'image de  $\tilde{\psi}(v')$  dans  $\overline{Z^\sigma}$ . Or le morphisme  $\psi : \overline{X'} \rightarrow \overline{Z^\sigma}$  est  $\Gamma_k$ -équivariant, donc cela assure que le carré précédent commute. Par conséquent, par propriété universelle du produit fibré, cela définit un unique morphisme  $\beta : \overline{V'} \rightarrow \overline{V'}$  faisant commuter le diagramme

$$\begin{array}{ccccc} \overline{V'} & & \xrightarrow{\varphi \circ \tilde{\psi}} & & \overline{V} \\ & \searrow \beta & & \searrow \tilde{\psi} & \\ & \overline{V'} & \xrightarrow{\tilde{\psi}} & \overline{V} & \\ & \downarrow \text{pr}_1 & & \downarrow \text{can} & \\ & \overline{X'} & \xrightarrow{\psi} & \overline{Z^\sigma} & \end{array} \quad (4)$$

$(\gamma^*)^{-1} \circ \text{pr}_1$  (flèche courbe de  $\overline{V'}$  à  $\overline{X'}$ )

Ce diagramme assure que  $\beta$  est un élément de  $\text{SAut}_{T^\sigma}(\overline{V'}/X')$ , tel que  $q(\beta) = \gamma$ .

On a donc construit une application  $\psi^* : \text{SAut}_{T^\sigma}(\overline{V}/Z^\sigma) \rightarrow \text{SAut}_{T^\sigma}(\overline{V'}/X')$  définie par  $\psi^*(\varphi) := \beta$ . C'est un morphisme de groupes par unicité du morphisme  $\beta$  dans le diagramme (4), et ce morphisme est bien compatible avec  $q$  et  $q'$ . Pour finir, on vérifie que l'on a bien un diagramme commutatif

$$\begin{array}{ccccccc} 1 & \longrightarrow & \overline{T^\sigma}(\overline{Z^\sigma}) & \longrightarrow & \text{SAut}_{T^\sigma}(\overline{V}/Z^\sigma) & \xrightarrow{q} & \Gamma_k \longrightarrow 1 \\ & & \downarrow \psi^* & & \downarrow \psi^* & & \downarrow = \\ 1 & \longrightarrow & \overline{T^\sigma}(\overline{X'}) = \overline{T^\sigma}(\bar{k}) & \longrightarrow & E = \text{SAut}_{T^\sigma}(\overline{V'}/X') & \xrightarrow{q'} & \Gamma_k \longrightarrow 1 \end{array}$$

en utilisant le fait que  $\tilde{\psi} : \bar{V}' \rightarrow \bar{V}$  est  $\overline{T^\sigma}$ -équivariant. □

### Remerciements

Je remercie chaleureusement D. Harari pour son soutien et ses nombreux commentaires sur ce texte. Je remercie également J. L. Colliot-Thélène, B. Poonen et A. Skorobogatov pour l'intérêt qu'ils ont porté à ce travail. Enfin, je remercie le rapporteur pour ses nombreuses suggestions pertinentes.

### References

- [Borovoi 1993] M. V. Borovoi, “Abelianization of the second nonabelian Galois cohomology”, *Duke Math. J.* **72**:1 (1993), 217–239. MR 94j:11042 Zbl 0849.12011
- [Colliot-Thélène et Sansuc 1987] J.-L. Colliot-Thélène et J.-J. Sansuc, “La descente sur les variétés rationnelles, II”, *Duke Math. J.* **54**:2 (1987), 375–492. MR 89f:11082 Zbl 0659.14028
- [Flicker et al. 1998] Y. Z. Flicker, C. Scheiderer et R. Sujatha, “Grothendieck’s theorem on non-abelian  $H^2$  and local-global principles”, *J. Amer. Math. Soc.* **11**:3 (1998), 731–750. MR 99a:11129 Zbl 0893.14015
- [Harari 2002] D. Harari, “Groupes algébriques et points rationnels”, *Math. Ann.* **322**:4 (2002), 811–826. MR 2003e:14038 Zbl 1042.14004
- [Harari et Skorobogatov 2002] D. Harari et A. N. Skorobogatov, “Non-abelian cohomology and rational points”, *Compositio Math.* **130**:3 (2002), 241–273. MR 2003b:11056 Zbl 1019.14012
- [Harari et Skorobogatov 2005] D. Harari et A. Skorobogatov, “Non-abelian descent and the arithmetic of Enriques surfaces”, *Int. Math. Res. Not.* **2005**:52 (2005), 3203–3228. MR 2006m:14031 Zbl 1099.14008
- [de Jong 2005] A. J. de Jong, “A result of Gabber”, prépublication, 2005, disponible sur <http://www.math.columbia.edu/~dejong/papers/2-gabber.pdf>.
- [Poonen 2008] B. Poonen, “Insufficiency of the Brauer-Manin obstruction applied to étale covers”, prépublication, 2008, disponible sur <http://math.mit.edu/~poonen/papers/insufficiency.pdf>.
- [Serre 1973] J.-P. Serre, *Cohomologie galoisienne*, 5e éd., Lecture Notes in Mathematics **5**, Springer, Berlin, 1973. MR 53 #8030 Zbl 0259.12011
- [Skorobogatov 1999] A. N. Skorobogatov, “Beyond the Manin obstruction”, *Invent. Math.* **135**:2 (1999), 399–424. MR 2000c:14022 Zbl 0951.14013
- [Skorobogatov 2001] A. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics **144**, Cambridge University Press, Cambridge, 2001. MR 2002d:14032 Zbl 0972.14015
- [Skorobogatov 2008] A. Skorobogatov, “Descent obstruction is equivalent to étale Brauer-Manin obstruction”, prépublication, 2008, disponible sur <http://www.ma.ic.ac.uk/~anskor/EQU.PDF>.
- [Stoll 2007] M. Stoll, “Finite descent obstructions and rational points on curves”, *Algebra Number Theory* **1**:4 (2007), 349–391. MR 2008i:11086

Communicated by Bjorn Poonen

Received 2008-07-11

Revised 2008-10-21

Accepted 2008-11-18

cyril.demarche@math.u-psud.fr *Université Paris-Sud, Laboratoire de Mathématiques  
d'Orsay, 91405 Orsay Cedex, France  
<http://www.math.u-psud.fr/~demarche/>*

## Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

**Originality.** Submission of a manuscript acknowledges that the manuscript is original and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

**Language.** Articles in ANT are usually in English, but articles written in other languages are welcome.

**Required items.** A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

**Format.** Authors are encouraged to use  $\text{\LaTeX}$  but submissions in other varieties of  $\text{\TeX}$ , and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

**References.** Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of Bib $\text{\TeX}$  is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

**Figures.** Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to [graphics@mathscipub.org](mailto:graphics@mathscipub.org) with details about how your graphics were generated.

**White Space.** Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

**Proofs.** Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.



# Algebra & Number Theory

Volume 3    No. 2    2009

---

A jeu de taquin theory for increasing tableaux, with applications to $K$ -theoretic Schubert calculus	121
HUGH THOMAS AND ALEXANDER YONG	
Weak Hopf monoids in braided monoidal categories	149
CRAIG PASTRO AND ROSS STREET	
Chabauty for symmetric powers of curves	209
SAMIR SIKSEK	
Obstruction de descente et obstruction de Brauer–Manin étale	237
CYRIL DEMARCHE	



1937-0652(2009)3:2;1-C