involve

a journal of mathematics

mathematical sciences publishers

involve

pjm.math.berkeley.edu/involve

See inside back cover or http://pjm.math.berkeley.edu/involve for submission instructions and subscription prices.
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 94704-3840, USA.

Involve, at Mathematical Sciences Publisher, 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.

How false is Kempe's proof
of the Four Color Theorem?
Part II

Ellen Gethner, Bopanna Kallichanda, Alexander S. Mentis,
Sarah Braudrick, Sumeet Chawla, Andrew Clune, Rachel Drummond,
Panagiota Evans, William Roche and Nao Takano

(Communicated by Ken Ono)

We continue the investigation of A. B. Kempe's flawed proof of the Four Color
Theorem from a computational and historical point of view. Kempe's "proof"
gives rise to an algorithmic method of coloring plane graphs that sometimes
yields a proper vertex coloring requiring four or fewer colors. We investigate a
recursive version of Kempe's method and a modified version based on the work
of I. Kittell. Then we empirically analyze the performance of the implementa-
tions on a variety of historically motivated benchmark graphs and explore the
usefulness of simple randomization in four-coloring small plane graphs. We end
with a list of open questions and future work.

1. Introduction

The Four Color Theorem for plane graphs states that, given a plane graph Γ, the
vertices of Γ can be properly colored with at most four colors. While the Four
Color Theorem was proven in 1977 through the use of a computer and irreducible
sets [Appel and Haken 1976/77; 1977; Appel et al. 1977; Robertson et al. 1996;
1997], no proof has been found that can be verified by a human without the use
of a computer. Alfred Kempe seemingly came close to accomplishing this in 1879
when he presented a proof of the Four Color Theorem in [Kempe 1879]; however,
his proof contained a flaw, discovered by Heawood [1890] and independently by de
la Vallée Poussin in 1896 [Wilson 2002b]. Although Kempe was unable to repair
the flaw, his innovation of Kempe chains and Kempe chain switches remain useful
to graph theorists, and it is interesting to explore the boundaries of his technique
[Gethner and Springer 2003]. In particular, we focus our attention on the work of

Errera, who was the first person to study the importance of the order in which the vertices are labeled [Errera 1921]. For a comprehensive history of the Four Color Theorem, see [Wilson 2002a; 2002b; Ore 1967; Fritsch and Fritsch 1998; Biggs et al. 1986].

Following [Errera 1921; Hutchinson and Wagon 1998; Gethner and Springer 2003; Wagon 2009], we implemented Kempe's method of proof as a recursive algorithm (Algorithm Kempe) on different vertex labelings for some well known graphs of nine vertices or more. For labelings resulting in the algorithm's inability to properly four-color the graphs, we identify vertices that cause irrevocable Kempe chain failures (the source of the flaw in Kempe's proof), and quantify the graphs' failure rates. In acknowledgement that Algorithm Kempe sometimes correctly four-colors the vertices of a plane graph, we explore some improvements to Algorithm Kempe including random selection among all Kempe chain choices and using random Kempe–Kittell chain switches to overcome irrevocable Kempe chain tangles, following [Kittell 1935; Hutchinson and Wagon 1998; Wagon 2002; 2009; Archuleta and Shapiro 1986; Morgenstern and Shapiro 1991]. While there may be different flaws that also result in failure to four-color a plane graph, our improvements focus solely on circumventing the flaw identified by Heawood and Poussin, since that is the flaw addressed by our implementation of Kittell's approach. Where Kempe–Kittell chain switches allow Algorithm Kempe to continue, we correlate the identified vertex with the number of Kempe–Kittell chain switches required to overcome the tangle.

2. Definitions and algorithm

It is important to understand Kempe's alleged proof and the flaw that led to our investigations. For completeness and ease of reference, the following definitions and algorithm are taken directly from [Gethner and Springer 2003]. In all of the following, R, G, B, Y refer to the four possible colors, and C_i is an element of $\{R, G, B, Y\}$.

Definition 1 (C_1C_2-Kempe chain). Let Γ be a plane graph whose vertices have been properly colored and suppose $v \in V(\Gamma)$ is colored C_1. The C_1C_2-*Kempe chain containing* v is the maximal connected component of Γ that contains v and contains only vertices colored C_1 or C_2.

Importantly, the maximality of the set of colored vertices in a C_1C_2-Kempe chain guarantees that interchanging all occurrences of C_1 and C_2 preserves the proper coloring of Γ.

Definition 2 (C_1C_2-Kempe chain switch). Let K be a C_1C_2-Kempe chain. A C_1C_2-*Kempe chain switch* interchanges all values of C_1 and C_2 in K.
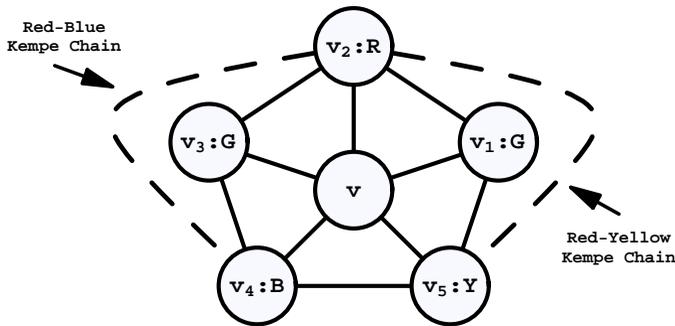
Figure 1. Setup for the faulty case in Kempe's proof.

We need one more notion to illustrate the potential flaw in Kempe's method. To help visualize the setup, see Figure 1.

Definition 3 (Irrevocable Kempe chain tangle). Let Γ be a plane graph, all of whose vertices, with the exception of one vertex v of degree 5, have been properly colored with four colors. Denote the five neighbors of v in cyclic counterclockwise order by v_1, v_2, v_3, v_4, v_5, and assume they are colored G, R, G, B, Y respectively. Moreover, assume that the *RB*-Kempe chain of v_2 contains v_4, and that the *RY*-Kempe chain of v_2 contains v_5.

Denote the *GB*-Kempe chain containing v_1 by K_1 and the *GY*-Kempe chain containing v_3 by K_2. We say that Algorithm Kempe causes an *irrevocable Kempe chain tangle on vertex* v if either

- following a *GB*-Kempe chain switch on K_1 by a *GY*-Kempe chain switch on K_2 causes v_5 to be recolored G, or

- following a *GY*-Kempe chain switch on K_2 by a *GB*-Kempe chain switch on K_1 causes v_4 to be recolored G.

In particular, at least one of the original barriers afforded by either the *RB*-Kempe chain containing v_2 and v_4, or the *RY*-Kempe chain containing v_2 and v_5 has been broken by two successive *GX*-Kempe chain switches, where $X \in \{Y, B\}$. Moreover, the second *GX*-Kempe chain contains two vertices in the neighborhood of v, which reintroduces a vertex colored G as a neighbor of v; thus the procedure has not made G available for vertex v.

We use the adjective *irrevocable* in Definition 3 because under the initial hypotheses, a Kempe chain tangle might occur: that is, one of either the *RB*-Kempe chain or the *RY*-Kempe chain may be "broken" by the two successive *GX*-Kempe chain switches, but the procedure need not force any of the neighbors of v to be recolored with G. In that case, v will be properly colored with G.

With these definitions, we can now describe Algorithm Kempe.

Algorithm Kempe.

INPUT:

- A connected plane graph Γ with n vertices, labeled (in some order) with distinct elements from $\{1, \ldots, n\}$.

- An ordering (C_1, C_2, C_3, C_4) of the set of permissible colors $\Sigma = \{R, G, B, Y\}$.

OUTPUT:

- Either a proper vertex coloring of Γ with colors from Σ, or

- the message "Kempe's algorithm has encountered an irrevocable Kempe chain tangle at vertex v and hence has failed to properly four-color Γ."

Gadget relabel (relabel the vertices):

- Search $\Gamma_0 := \Gamma$ for the first occurrence of a vertex of degree five or less; the existence of such a vertex is guaranteed by Euler's formula. The first occurrence is dictated by the given ordering of the vertices. Call this vertex v_1.

- Recursively label the other $n - 1$ vertices of Γ, choosing for v_{i+1} ($0 \leq i < n$) the first occurrence of a vertex of degree five or less in $\Gamma_i := \Gamma \setminus v_i$.

Gadget greed (color greedily whenever possible):

- Color v_n in Γ_{n-1} with the available color of lowest index from C. In this case, since no colors have been used, v_n will be colored C_1.

- Color v_{n-1} in Γ_{n-2} with the available color of lowest index in C; if v_{n-1} is not adjacent to v_n, then v_{n-1} is colored C_1. On the other hand, if v_{n-1} is adjacent to v_n, color v_{n-1} is colored C_2.

- In general (if possible) color v_i in Γ_{i-1} with the available color of lowest index from C.

Gadget 4 (perform Kempe chain switches on degree four vertices):

- We encounter a vertex v_i of degree four that cannot be greedily colored. That is, suppose degree $v_i = 4$ and the neighbors are colored R, G, B, Y (say) in counterclockwise order, as on the right.
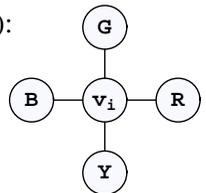
- If there is an RB-Kempe chain containing both the R and B neighbors of v_i, there cannot be a YG-Kempe chain that contains *both* of the Y and G neighbors of v_i. In that case a YG-Kempe chain switch leaves a color available for v_i.

- Otherwise, if there is no RB-Kempe chain containing both the R and B neighbors of v_i, perform an RB-Kempe chain switch to make a color available for v_i.

Gadgets 5_1 and 5_2 (Kempe chain switches on degree-five vertices): Suppose we encounter a vertex v_i of degree five that cannot be greedily colored; a priori, one color is used exactly twice and the other three are used exactly once on the five neighbors of v_i. Without loss of generality, suppose the twice-used color is G. Up to rotation and reflection, only two configurations can occur, illustrated in the two diagrams below.

Gadget 5_1 (degree $v_i = 5$; two G neighbors next to each other):

- In Configuration 1, a gadget much like Gadget 4 will suc-ceed in coloring v_i. Suppose the five neighbors of v_i are colored, in counterclockwise order, by *GGYBR*.

- If there is no *RY*-Kempe chain containing both Y and R neighbors of v_i, then a *RY*-Kempe chain switch will leave a color available for v_i.

- Therefore, assume there is an *RY*-Kempe chain containing both Y and R neighbors of v_i. Thus a *GB*-Kempe chain containing the B neighbor of v_i contains neither of the G neighbors of v_i.

- In that case, a *GB*-Kempe chain switch makes B available for v_i.

- In all cases, v_i can be properly colored.
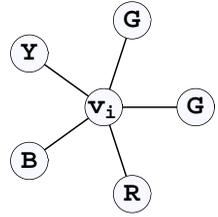
Gadget 5_2 (degree $v_i = 5$; two G neighbors are separated by another neighbor of v_i):

- This is the case in which an irrevocable Kempe chain tan-gle might occur, causing Algorithm Kempe to halt before completing a proper four-coloring of the graph. Suppose the neighbors of v_i are colored in counterclockwise order by $G_a R G_b B Y$ (at this point, it is helpful to distinguish between the two G vertices).

- If there is an *RB*-Kempe chain that does not contain both the R and B neigh-bors of v_i then an *RB*-Kempe chain switch leaves a color available for v_i.

- If there is an *RY*-Kempe chain that does not contain both R and Y neighbors of v_i then an *RY*-Kempe chain switch makes a color available for v_i.

- Otherwise, we must attempt both a $G_a B$-Kempe chain switch followed by a $G_b Y$ Kempe chain switch (or vice versa).

- If no irrevocable Kempe chain tangle occurs, then we successfully color v_i with G and move on to vertex v_{i-1}.

- Otherwise, halt and return an error message that the offending vertex is v_i.
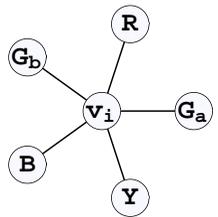
BEGIN

Step 1: Use Gadget relabel to label the vertices of Γ.

Step 2: For $i = n$ down to 1, attempt to color v_i in graph Γ_{i-1} as follows:

 (a) if v_i can be greedily colored in graph Γ_{i-1} by Gadget greed then do so, else

 (b) if degree $v_i = 4$ in Γ_i then color v_i using Gadget 4 else

 (c) if degree $v_i = 5$ in Γ_{i-1} in configuration 1 then color v_i using Gadget 5_1 else

 (d) if degree $v_i = 5$ in Γ_{i-1} in configuration 2 then try to color v_i using Gadget 5_2 employing two Kempe chain switches: try both orders if necessary.

END

Thus, it is obvious that it is possible to color vertices of degree three or less with no more than a fourth color, and it has been shown that it is always possible to color vertices of degree four through the use of Kempe chain switches [Heawood 1890]. Algorithm Kempe only encounters difficulties upon vertices of degree five or more, but it has been shown that Algorithm Kempe will always succeed in properly four-coloring any graph containing eight or fewer vertices (which may contain vertices of degree five or more) [Gethner and Springer 2003]. In light of the fact that Kempe's method of proof works in some, but not all cases, we were interested in identifying patterns of when the algorithm halts without producing a proper four-coloring on our benchmark graphs. In particular, we explore the usefulness of simple randomization when used with Kempe–Kittell chain switches to improve its success on small plane graphs.

3. Results

Identification of vertex failures. We first implemented Algorithm Kempe and explored its success in nine well known, properly four-colored graphs. The first five, shown in Figure 2 (ignore the coloring of vertices for the moment), were introduced in [Heawood 1890], [Fritsch and Fritsch 1998], [Soifer 1997], [Errera 1921] (see also [Hutchinson and Wagon 1998; Wagon 2009]), and Poussin's writings (see [Wilson 2002a]); they are all known counterexamples for Algorithm Kempe with at least one labeling [Gethner and Springer 2003]. The remaining four are the edge graphs of the icosahedron, dodecahedron, octahedron, and cube; since these last three have vertices of degree at most four, Algorithm Kempe must always successfully color them, and they served as benchmarks for our implementations. Further, although the Icosahedron graph is five-regular, we did not expect Kempe's method to fail on any labeling of vertices, and thus that graph served as a benchmark graph as well. See also Open Question 5 in Section 4.

Five groups worked independently to implement Algorithm Kempe and test it on these graphs. For the graphs containing nine vertices or fewer, each group explored Algorithm Kempe's results for all $n!$ labelings. For the graphs containing more than nine vertices, each group independently tested a random subset of at least 9! labelings.

While we expected different failure rates for the graphs with more than nine vertices due to the use of different labeling subsets among the groups, we expected the failure rates for Fritsch, Soifer, and the four benchmark graphs to be the same. Instead, while the benchmark graphs produced no failures, as expected, failure rates did vary for Fritsch and Soifer due to differences in the individual implementations or failure rate calculations. In the case of Group 2, when Gadget 5_2 is required the implementation only tests one of the two possible Kempe chain switch orders, resulting in a higher failure rate. This difference in implementation, however, gives us an idea of how many Kempe chain tangles can be "fixed" by changing the order in which the switches are performed (see Table 1 on the next page).

We initially compared the vertices that caused irrevocable Kempe chain tangles for each implementation on all graphs. Because each group tested all 9! labelings for the two nine-vertex graphs (Fritsch and Soifer), each implementation agreed on the vertices that caused failures for Fritsch and Soifer, as expected. An interesting and unpredicted discovery, however, was that despite the differences in the labeling subsets tested by each group for the graphs containing more than nine vertices, there was considerable consensus among the groups on the vertices that cause failures.

In Figure 2, vertices shown in red are those vertices that all groups found to result in an irrevocable Kempe chain tangle for at least one labeling. Vertices
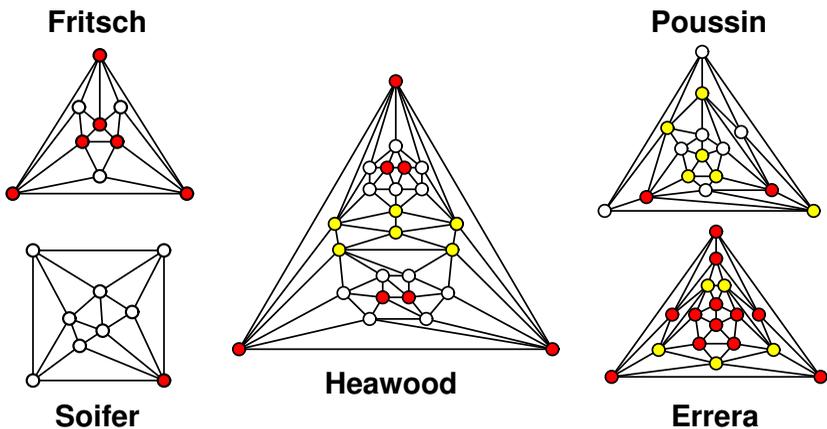
Figure 2. Graph vertex failures.

shown in yellow are those vertices that at least one group, but not all, found to
fail. Vertices shown in white were not found by any groups to cause a failure
on the labelings tested. As one can see, the failure patterns of the vertices are
highly symmetrical for all graphs except the Poussin graph, which itself is a fairly
asymmetrical graph. For the Fritsch and Soifer graphs, since all n! labelings were
tested, we know that the vertices shown in white will never cause Kempe chain
tangles for any labeling. For the remaining graphs, we predict that the vertices
shown in yellow would eventually become red as more labelings are explored. We
cannot predict anything for the vertices shown in white of degree five or more —
they may eventually fail, or they may not. Nevertheless, these results lead us to ask
the question: are there commonalities among these vertices that can be exploited
to improve Algorithm Kempe? We leave this as an open question.

The next step was to add randomization, studied in [Kittell 1935; Hutchinson
and Wagon 1998; Wagon 2002; 2009; Archuleta and Shapiro 1986; Morgenstern
and Shapiro 1991], through the application of Kempe–Kittell chain switches [Kit-
tell 1935] and the use of randomization of the choice of Kempe or Kempe–Kittell
chain switches, rather than heuristics, at various stages of the algorithm. In contrast
to the study of randomization for large graphs in [Archuleta and Shapiro 1986;

Group		F	S	O	C	I	D	P	E	H
1	min	13.947	1.692	0.000	0.000	0.000	0.000	0.610	9.730	7.089
	avg	13.947	1.692	0.000	0.000	0.000	0.000	0.620	9.755	7.124
	max	13.947	1.692	0.000	0.000	0.000	0.000	0.627	9.772	7.153
2	min	14.031	1.783	0.000	0.000	0.000	0.000	0.149	3.350	0.372
	avg	14.083	1.832	0.000	0.000	0.000	0.000	0.153	3.383	0.382
	max	14.131	1.859	0.000	0.000	0.000	0.000	0.156	3.402	0.390
3	min	3.598	0.520	0.000	0.000	0.000	0.000	0.014	8.140	1.089
	avg	3.599	0.523	0.000	0.000	0.000	0.000	0.017	8.168	1.097
	max	3.600	0.525	0.000	0.000	0.000	0.000	0.019	8.186	1.111
4	min	13.687	1.635	0.000	0.000	0.000	0.000	0.165	7.302	0.387
	avg	13.687	1.635	0.000	0.000	0.000	0.000	0.165	7.302	0.387
	max	13.687	1.635	0.000	0.000	0.000	0.000	0.165	7.302	0.387
5	min	13.630	1.620	0.000	0.000	0.000	0.000	0.180	10.680	3.199
	avg	13.635	1.620	0.000	0.000	0.000	0.000	0.186	10.798	3.203
	max	13.637	1.620	0.000	0.000	0.000	0.000	0.190	10.866	3.210

Table 1. Kempe method failure rates by graph. The column heads
stand for Fritsch, Soifer, Octahedron, Cube, Icosahedron, Dodeca-
hedron, Poussin, Errera, Heawood.

Morgenstern and Shapiro 1991], we continue to investigate small, historically significant benchmark graphs.

Randomization implementation. In our recursive implementation of the Kempe method, there are several points at which we must choose one among multiple Kempe chains upon which to perform a switch. In both Gadget 4 and Gadget 5_1, in the case where the vertex cannot be greedily colored, there will be up to four Kempe chains from which to choose; our implementation randomly chooses one that results in a successful coloring. In Gadget 5_2, two Kempe chain switches must be performed, but the order of the switches is not specified in the algorithm. Theorem 4 shows that the order in which the switches are performed can influence the success of the operation. In light of this knowledge, we randomize the choice of which Kempe chain switch to perform first, and perform the alternative order only if the first order fails.

Theorem 4 (Gadget 5_2 is order-dependent). *In Algorithm Kempe, Gadget 5_2 is sometimes noncommutative. That is, the order in which one chooses to execute the Kempe chain switches on K_1 and K_2 may matter; in one order an irrevocable Kempe chain tangle can occur, whereas in the other no Kempe chain tangle occurs.*

Proof. It suffices to exhibit a plane graph Γ and a labeling of the vertices of Γ that cause Algorithm Kempe to execute Gadget 5_2 in the following way: upon that execution, one of the two choices of Kempe chain switch orders causes an irrevocable Kempe chain tangle while the other does not. To this end, we call upon the Fritsch graph, which we denote by F. In Figure 3, the labeling of the vertices in F (the uppermost graph) leads to a successful four-coloring with the exception of vertex 1, whereupon Gadget 5_2 must be invoked. Following the arrows marked A, one choice of Kempe chain switch order has been executed successfully, and vertex 1 is colored G. Following the arrows marked B, the other Kempe chain switch order has been followed, leading to an irrevocable Kempe chain tangle. □

In the case that both orders fail, we encounter the previously defined irrevocable Kempe chain tangle and turn to Kempe–Kittell chain switches in an attempt to solve the impasse. Kempe–Kittell chains present yet another opportunity for randomization of choices. To better understand these choices, we first define the eight Kempe–Kittell chains identified by Kittell [1935].

We use exactly the notation and Kempe chain switches as suggested by Kittell [1935]. The new gadget, called *Gadget Kittell*, is invoked only when Gadget 5_2 is called upon in Algorithm Kempe and fails. For reference, see Figure 1.

Definition 5 (Gadget Kittell). (1) *Chain α*: perform an *RB*-Kempe Chain switch beginning either on v_2 or v_4.

(2) *Chain β*: perform an *RY*-Kempe Chain switch beginning either on v_2 or v_5.
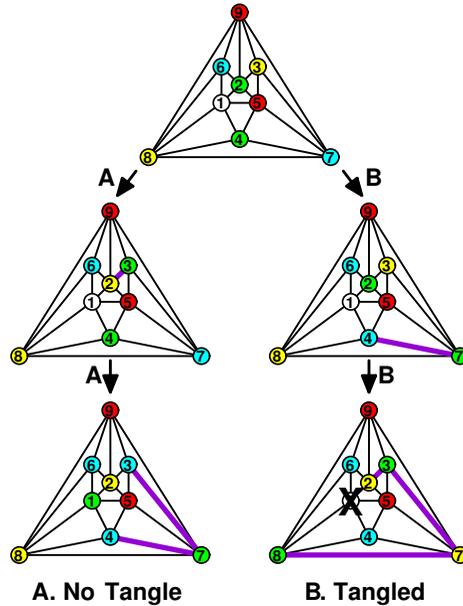
Figure 3. Gadget 5_2 in Algorithm Kempe does not commute. The thick purple lines highlight the current Kempe chain switch.

(3) *Chain γ*: perform a *GY*-Kempe Chain switch beginning either on v_1 or v_5.

(4) *Chain δ*: perform a *GB*-Kempe Chain switch beginning either on v_3 or v_4.

(5) *Chain ϵ*: perform a *BY*-Kempe Chain switch beginning either on v_4 or v_5.

(6) *Chain ζ*: perform a *GB*-Kempe Chain switch beginning either on v_1 or v_4.

(7) *Chain η*: perform a *GY*-Kempe Chain switch beginning either on v_3 or v_5.

(8) *Chain θ*: perform an *RG*-Kempe Chain switch beginning on any of v_2 or v_1.

Upon encountering an irrevocable Kempe chain tangle, we randomly choose one of the eight Kempe–Kittell chains in Gadget Kittell and continue to randomly execute switches from that list until we reach a coloration of the graph that allows us to successfully color the vertex causing the impasse or until a fixed number of Kempe–Kittell chain switches have failed (we chose an upper limit of 100 Kempe–Kittell chain switches).

Thus Algorithm Kempe is modified as follows:

Algorithm Kempe–Kittell.   BEGIN

Step 1: Use Gadget relabel to label the vertices of Γ.

Step 2: For $i = n$ down to 1, attempt to color v_i in graph Γ_{i-1} as follows:

(a) if v_i can be greedily colored in graph Γ_{i-1} by Gadget greed then do so; else

(b) if degree $v_i = 4$ in Γ_i then color v_i using Gadget 4 on a randomly selected viable Kempe chain; else

(c) if degree $v_i = 5$ in Γ_{i-1} in configuration 1 then color v_i using Gadget 5_1 on a randomly selected viable Kempe chain; else

(d) if degree $v_i = 5$ in Γ_{i-1} in configuration 2 then try to color v_i using Gadget 5_2 employing two Kempe chain switches (randomly select an order in which to perform the switches, and try both orders if necessary);

(e) if an irrevocable Kempe chain tangle is reached then select a random Kempe–Kittell chain using Gadget Kittell until v_i successfully colored or 100 attempts have failed.

END

The fixed limit on the number of failures is required because it is unknown if there is always a series of Kempe–Kittell chain switches that will result in successful resolution of the impasse. The set of possible Kempe–Kittell chain switch combinations that can affect the five vertices adjacent to v_i, called the *impasse group*, is known to have a lower bound of 120 [Kittell 1935], but it is impractical to determine and check the upper bound for even a small arbitrary graph. The use of heuristics to guide the search of the impasse group has been studied for large graphs [Morgenstern and Shapiro 1991], but our interest was in determining algorithm performance when executing a purely random sequence of Kempe–Kittell chain switches to color a small graph, as this could provide an easy way to improve the performance of Algorithm Kempe for those cases.

Our randomized recursive implementation of Kempe's method always succeeded in four-coloring the graphs we tested. We ran the algorithm 500 times for each of the nine graphs tested in the original implementation and, additionally, the Kittell graph [1935], shown on the right.
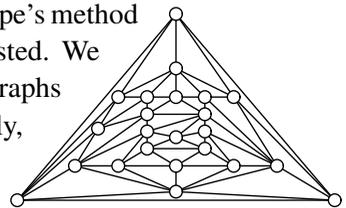
We kept track of the number of times a Kempe–Kittell chain switch was required to solve an impasse (Table 2) and the vertices causing the impasse (see Table 3 on the next two pages).

	F	S	O	C	I	D	P	E	H	K
Kempe–Kittell switches (max)	9	7	0	0	0	0	6	73	6	11

Table 2. Maximum number of Kempe–Kittell chain switches required for any vertex. For the letters on the top row, see Table 1 (plus K = Kittell).

Graph	Node label	Chain switches required			Kittell colored nodes	Kittel use (%)
		min	max	avg		
F	a	3	8	4.52	1088000	0.5996
F	b, f	3	8	4.46	1088000	0.5996
F	c	3	8	4.44	1088000	0.5996
F	d, e, h	0	0	0.00	0	0.0
F	g	3	7	4.49	1088000	0.5996
F	i	3	9	4.50	1088000	0.5996
S	a-b, d-i	0	0	0.00	0	0.0
S	c	3	7	4.45	988089	0.5446
O	a-f	0	0	0.00	0	0.0
C	a-h	0	0	0.00	0	0.0
I	a-l	0	0	0.00	0	0.0
D	a-t	0	0	0.00	0	0.0
P	a, b, g, i-o	0	0	0.00	0	0.0
P	c	1	4	2.26	526486	0.2902
P	d	2	6	2.58	399678	0.2203
P	e	2	5	2.69	323390	0.1782
P	f	2	5	2.82	339534	0.1871
P	h	2	5	2.81	474890	0.2617
E	a	35	73	47.01	4937929	2.7215
E	b	3	8	4.14	463228	0.2553
E	c	3	7	4.11	463000	0.2552
E	d	3	7	4.05	463086	0.2552
E	e	3	7	4.03	464390	0.2559
E	f	2	5	2.83	440437	0.2427
E	g	2	5	2.82	440226	0.2426
E	h	2	5	2.80	440679	0.2429
E	i	3	6	4.05	464517	0.2560
E	j	2	6	2.85	439756	0.2424
E	k	2	5	2.84	440513	0.2428
E	l	3	7	4.07	462705	0.2550
E	m	3	7	4.07	462517	0.2549
E	n	3	7	4.10	463978	0.2557
E	o	35	71	46.29	4938719	2.7220
E	p	3	7	4.07	463436	0.2554
E	q	3	8	4.06	461792	0.2545

Graph	Node label	Chain switches required			Kittell colored nodes	Kittel use (%)
		min	max	avg		
H	a	2	6	3.22	775216	0.4273
H	b	2	6	3.29	1217733	0.6711
H	c	2	5	3.13	847294	0.4670
H	d-f, h-i, q-s, v-y	0	0	0.00	0	0.0
H	g	2	5	2.78	690371	0.3805
H	j	1	1	1.00	6058	0.0033
H	k	1	2	1.56	6037	0.0033
H	l	2	6	3.36	907479	0.5002
H	m	3	8	4.60	1405876	0.7748
H	n	3	7	3.75	828677	0.4567
H	o	2	5	3.15	813156	0.4482
H	p	2	5	3.19	1032339	0.5690
H	t	2	6	3.29	92157	0.0508
H	u	2	6	3.27	91564	0.0505
K	a	2	4	2.79	636989	0.3511
K	b	2	5	2.75	478186	0.2636
K	c,g	0	0	0.00	0	0.0
K	d	2	6	3.33	675394	0.3722
K	e	3	8	4.76	475928	0.2623
K	f	5	9	6.57	792681	0.4369
K	h	2	6	3.25	82375	0.0454
K	i	5	9	6.32	782074	0.4310
K	j	2	5	2.95	457668	0.2522
K	k	4	7	4.92	400408	0.2207
K	l	2	5	2.84	473726	0.2611
K	m	3	6	3.99	386798	0.2132
K	n	5	11	6.48	537869	0.2964
K	o	5	8	5.93	496916	0.2739
K	p	5	9	6.35	691822	0.3812
K	q	0	1	0.98	1676	0.0009
K	r	5	11	6.44	667972	0.3682
K	s	2	6	3.16	660014	0.3638
K	t	2	5	2.83	489486	0.2698
K	u	2	6	3.51	209896	0.1157
K	v	2	5	2.81	551059	0.3037
K	w	0	1	0.98	1966	0.0011

Table 3. Algorithm Kempe–Kittell results (see also top of next page).

In Table 3, the last column gives the percentage of Kittel colored nodes relative to the total number of colored nodes, which is 50 times the numbering of labelings per trial. The latter number, as already explained, was $9! = 362880$ for all graphs except those with less than 9 vertices (O with $6! = 720$ and C with $8! = 40320$).

Our fixed upper limit of 100 for Kempe–Kittell chain switches was more than sufficient since, for most impasses encountered in our tests, eleven or fewer randomly chosen Kempe–Kittell chain switches were sufficient to achieve a successful four-coloring. The exception to this was the Errera graph, which contained two vertices that required over 70 randomly chosen Kempe–Kittell chain switches on the regions marked A and B in Figure 4 to achieve successful four-coloring. These two vertices are the only two vertices in the Errera graph that do not have any neighbors of degree greater than five, and they are the polar regions of Errera's 17-country counterexample when described as a spherical map as shown in [Hutchinson and Wagon 1998, Figure 2; Wagon 2009] and as a fullerene, of molecular formula C_{30}, in our Figure 4.
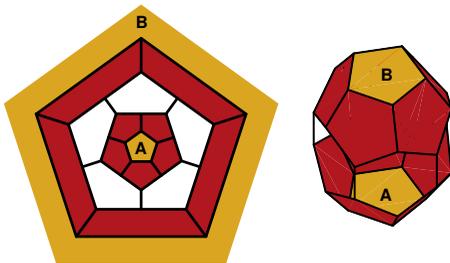
Figure 4. Errera map: planar representation and coordinatized as a fullerene (C_{30}) in $\mathbb{R}^3$.

Comparison of original and randomized implementations. We achieve proper four-coloring of all of our graphs on 100% of our runs through the inclusion of randomly selected Kempe–Kittell chain switches. In addition to this, the percentage of times that Gadget Kittell was required in our algorithm indicates the percentage of irrevocable Kempe chain tangles encountered by our randomized algorithm, which we compare in Table 4 to the failure rates from the original five groups' implementations (see also Table 3).

When we make this comparison to the average failure rate of the original five implementations, we see that our algorithm outperforms the average original algorithm's performance on the two graphs for which all $n!$ labelings were tested (Fritsch and Soifer graphs). In fact, our randomized implementation nearly matches the lowest failure rates observed among the original six implementations: 3.60% and 0.52% for Fritsch and Soifer, respectively (Table 1 and Table 4).

On the Errera and Heawood graphs, randomization results in a higher rate of irrevocable Kempe chain tangles than the average rate of the original algorithm,

Graph	Original algorithm			Randomized algorithm
	Min % Failure	Max % Failure	Avg % Failure	% Failure
Fritsch	3.598	14.131	11.790	3.60
Soifer	0.520	1.859	1.461	0.55
Poussin	0.014	0.627	0.228	1.18
Errera	3.350	10.866	7.881	9.28
Heawood	0.372	7.153	2.439	4.83

Table 4. Comparison of original Algorithm Kempe to randomized version with Kempe–Kittell chains.

but it is still within the range of the minimum and maximum failure rates of the original implementations. On the asymmetrical Poussin graph, our algorithm results in significantly more Kempe chain tangles than the average (Table 4), but this is mitigated by the success of the Kempe–Kittell chain switches in coloring the graph. We exclude the graphs of the platonic solids, as they cause no failures for either algorithm.

4. Conclusions

We evaluated the performance of the version of Algorithm Kempe in [Gethner and Springer 2003] and its performance after the addition of Kempe–Kittell chain switches, which successfully overcame all irrevocable Kempe chain tangles in our benchmark graphs. We have proven that the order in which Kempe chain switches are performed affects the outcome of the algorithm and have shown that the application of randomization to the selection of Kempe and Kempe–Kittell chain switches in this algorithm is a useful method for making the choice of which switch to perform first. In 500 test runs on each of ten benchmark graphs, the use of randomized chain choices resulted in successful four-coloring of the graphs with fewer than 12 random choices for any vertex most of the time. When compared to the original algorithm, there appears to be a performance trade-off in that randomization causes the use of Gadget Kittell in the Poussin graph more often than would have been required by the nonrandomized version. Finally, we discovered that some vertices appear to be more likely to cause irrevocable Kempe chain tangles than others, and we identify those vertices in the hopes of being able to characterize them.

Open questions for future work.

1. Given a plane graph Γ with e edges and n vertices, what is the minimum value of e for which Kempe's method is probably guaranteed to succeed in properly coloring Γ?

2. What percentage of all plane graphs on nine vertices serve as counterexamples to Kempe's method?

3. Do the vertices that cause irrevocable Kempe chain tangles or require high numbers of Kempe–Kittell chain switches share properties which can be exploited to improve Algorithm Kempe–Kittell?

4. Let Γ be a plane graph on n vertices. It follows from [West 2001, Exercise 6.1.9] that, when $n \leq 11$, there is some labeling for which Algorithm Kempe succeeds in properly four-coloring Γ. What is the smallest value of $n > 11$ for which Algorithm Kempe–Kittell is provably guaranteed to succeed?

5. It is not difficult to show that the Icosahedral graph will be properly four-colored by Kempe's algorithm regardless of the labeling of the vertices (and this is confirmed by Table 3). Characterize all plane graphs that will be properly four-colored by Kempe's algorithm under all possible orderings of the vertices. Short of that potentially difficult goal, find interesting families of plane graphs (with at least 11 vertices and whose average vertex degree is at least 5) for which Kempe's algorithm will always succeed.

5. Addendum

Stan Wagon (personal communication, 2008) reports the discovery that the plane graph corresponding to the contiguous 48 United States plus Lake Michigan and the oceanic waters admits a labeling that leads to a Kempe impasse at the great state of Illinois. Details will appear in [Wagon 2009].

References

[Appel and Haken 1976/77] K. Appel and W. Haken, "Every planar map is four colorable", *J. Recreational Math.* **9**:3 (1976/77), 161–169. MR 58 #27598f Zbl 0357.05043

[Appel and Haken 1977] K. Appel and W. Haken, "The solution of the four-color-map problem", *Sci. Amer.* **237**:4 (1977), 108–121, 152. MR 58 #27598e

[Appel et al. 1977] K. Appel, W. Haken, and J. Koch, "Every planar map is four colorable", *Illinois J. Math.* **21**:3 (1977), 429–567 and microfiche supplement. MR 58 #27598b Zbl 0387.05010

[Archuleta and Shapiro 1986] R. A. Archuleta and H. D. Shapiro, "A fast probabilistic algorithm for four-coloring large planar graphs", pp. 595–600 in *Proc. ACM Fall joint computer conference* (Dallas, 1986), IEEE Press, Los Alamitos, CA, 1986.

[Biggs et al. 1986] N. L. Biggs, E. K. Lloyd, and R. J. Wilson, *Graph theory. 1736–1936*, 2nd ed., Oxford University Press, New York, 1986. MR 88e:01035 Zbl 0595.05003

[Errera 1921] A. Errera, *Du colorage des cartes et de quelques questions dánalysis situs*, Ph.D. thesis, Université Livre de Bruxelles, 1921.

[Fritsch and Fritsch 1998] R. Fritsch and G. Fritsch, *The Four-Color Theorem*, Springer, New York, 1998. MR 99i:05079

[Gethner and Springer 2003] E. Gethner and W. M. Springer, II, "How false is Kempe's proof of the four color theorem?", *Congr. Numer.* **164** (2003), 159–175. MR 2005a:05084 Zbl 1050.05049

[Heawood 1890] P. J. Heawood, "Map colour theorem", *Quart. J. Pure Appl. Math.* **24** (1890), 332–338.

[Hutchinson and Wagon 1998] J. Hutchinson and S. Wagon, "Kempe revisited", *Amer. Math. Monthly* **105**:2 (1998), 170–174. MR 1605875 Zbl 0915.05058

[Kempe 1879] A. B. Kempe, "On the geographical problem of the four colours", *Amer. J. Math.* **2**:3 (1879), 193–200. MR 1505218

[Kittell 1935] I. Kittell, "A group of operations on a partially colored map", *Bull. Amer. Math. Soc.* **41**:6 (1935), 407–413. MR 1563103 Zbl 0012.03501

[Morgenstern and Shapiro 1991] C. A. Morgenstern and H. D. Shapiro, "Heuristics for rapidly four-coloring large planar graphs", *Algorithmica* **6**:6 (1991), 869–891. MR 92g:05169

[Ore 1967] O. Ore, *The four-color problem*, Pure and Applied Mathematics **27**, Academic Press, New York, 1967. MR 36 #74 Zbl 0149.21101

[Robertson et al. 1996] N. Robertson, D. P. Sanders, P. Seymour, and R. Thomas, "A new proof of the four-colour theorem", *Electron. Res. Announc. Amer. Math. Soc.* **2**:1 (1996), 17–25. MR 97f:05070 Zbl 0865.05039

[Robertson et al. 1997] N. Robertson, D. Sanders, P. Seymour, and R. Thomas, "The four-colour theorem", *J. Combin. Theory Ser. B* **70**:1 (1997), 2–44. MR 98c:05065 Zbl 0883.05056

[Soifer 1997] A. Soifer, "Map coloring in the victorian age: problems and history", *Mathematics Competitions* **10** (1997), 20–31.

[Wagon 2002] S. Wagon, "A machine resolution of a four-color hoax", pp. 181–193 in *Proc. 14th Canad. Conf. Comput. Geom.*, 2002.

[Wagon 2009] S. Wagon, *Mathematica in Action*, 3rd ed., Springer/TELOS, New York, 2009. To appear.

[West 2001] D. B. West, *Introduction to graph theory*, 2nd ed., Prentice Hall, Upper Saddle River, NJ, 2001. Zbl 0845.05001

[Wilson 2002a] R. Wilson, *Four colors suffice: How the map problem was solved*, Princeton University Press, Princeton, NJ, 2002. MR 2004a:05060

[Wilson 2002b] R. A. Wilson, *Graphs, colourings and the four-colour theorem*, Oxford University Press, Oxford, 2002. MR 2003c:05095 Zbl 1007.05002

ellen.gethner@cudenver.edu   *University of Colorado Denver, Department of Mathematics and Department of Computer Science, Denver, CO 80217, United States*
http://carbon.cudenver.edu/~egethner/

bkallichanda@gmail.com   *eCollege, 4900 S. Monaco Street Suite 200, Denver, CO 80237, United States*
http://www.linkedin.com/pub/bopanna-kallichanda/4/145/b3a

alexander.mentis@us.army.mil   *United States Military Academy, Department of Electrical Engineering and Computer Science, PO Box 67, Fort Montgomery, NY 10922, United States*
http://www.eecs.usma.edu/webs/people/Mentis/

s_braudrick@msn.com   *Lockheed Martin, 12999 W Deer Creek Canyon Rd,*
                             Littleton, CO 80127-5146, United States
                             http://www.linkedin.com/pub/sarah-braudrick/7/22/793

sumeet.chawla@gmail.com   *6885 West 91st Court, Apt #23-301,*
                             Westminster, CO 80021, United States
                             http://ouray.cudenver.edu/~schawla/

andy.clune@gmail.com   *Syntellect, 16610 North Black Canyon Highway Suite 100,*
                             Phoenix, AZ 85053, United States
                             http://www.linkedin.com/pub/andy-clune/4/11/204

rachel.drummond@gmail.com   *OPX Biotechnologies, Inc., 2425 55th Street Suite 100,*
                             Boulder, CO 80301, United States
                             http://www.blogger.com/profile/11006794721285468833

pennye_gr@hotmail.com   *Interactive Intelligence, 7601 Interactive Way,*
                             Indianapolis, IN 46278, United States
                             http://www.linkedin.com/pub/panagiota-evans/12/b01/144

wrroche1@msn.com   *1625 S Iola Street #202, Aurora, CO 80012, United States*
                             http://www.big-baboon.com/

dumnas@comcast.net   *Aurora Loan Services, 10350 Park Meadows Drive,*
                             Littleton, CO 80124, United States
                             http://www.linkedin.com/pub/nao-takano/3/964/24

Dynamical properties of the derivative of the Weierstrass elliptic function

Jeff Goldsmith and Lorelei Koss

(Communicated by Gaven J. Martin)

We discuss properties of the Julia and Fatou sets of the derivative of the Weierstrass elliptic $\wp$ function. We find triangular lattices for which the Julia set is the whole sphere, or which have superattracting fixed or period two points. We study the parameter space of the derivative of the Weierstrass elliptic function on triangular lattices and explain the symmetries of that space.

1. Introduction

The study of complex dynamical systems began in the early 1900s with the work of mathematicians such as Fatou [1919; 1920a; 1920b] and Julia [1918]. These works focused on the iteration of rational functions, although Fatou later published articles on the iteration of entire functions [1926]. Much more recently, Devaney and Keen [1988] published the first paper investigating the dynamics of a transcendental meromorphic function. Since then, it has been well established that transcendental meromorphic functions can exhibit dynamical behavior distinct from that of rational maps [Baker et al. 1991a; 1991b; 1992; Bergweiler 1993; Devaney and Keen 1988; 1989; Erëmenko and Lyubich 1992]. (See also the references in the next paragraph.)

Studies on the dynamical, measure-theoretic, and topological properties of iterated elliptic functions have appeared in [Hawkins 2006; Hawkins and Koss 2002; 2004; 2005; Hawkins and Look 2006; Kotus 2006; Kotus and Urbański 2003; 2004]. Of these, the first five deal with the Weierstrass elliptic $\wp$-function, which satisfies some strong algebraic identities that influence the resulting dynamical behavior. Even within an equivalence class of lattice shape, changing the size or orientation of the lattice can drastically change the dynamics of the Weierstrass elliptic function. Most of the work investigating the dynamics of parametrized families of elliptic functions has involved the study of the Weierstrass function.

In this paper, we investigate the dynamics of the *derivative* of the Weierstrass elliptic function, focusing mainly on triangular lattices. Although the Weierstrass elliptic function and its derivative share some of the same algebraic properties, moving from the order two elliptic function $\wp$ to the order three function $\wp'$ changes many of the dynamical properties. For example, on a triangular lattice Ω, $\wp_\Omega$ has three distinct critical values, but $\wp'_\Omega$ only has two. As the postcritical orbits strongly influence the dynamical properties of an iterated family, $\wp_\Omega$ and $\wp'_\Omega$ exhibit different types of behavior.

Here, we construct lattices for which the Julia set of $\wp'_\Omega$ is the entire sphere, and we also construct lattices for which $\wp'_\Omega$ has a superattracting fixed point or a superattracting period two cycle. We also investigate the symmetries of the parameter space arising from all triangular lattices.

The paper is organized as follows. In Sections 2 and 3 we give background on the dynamics of meromorphic functions and lattices in the plane. In Section 4, we define the function that we study, the derivative of the Weierstrass elliptic function, and discuss the location of the critical points and critical values of this function. In Section 5 we discuss the symmetries of the Fatou and Julia sets that arise from the algebraic properties of these elliptic functions. Section 6 focuses on the postcritical set of $\wp'_\Omega$ when Ω is a triangular lattice. In this section, we construct many triangular lattices Ω for which the postcritical set $\wp'_\Omega$ exhibits especially nice behavior.

In Section 7 we discuss parametrizing the derivative of the Weierstrass elliptic function over all triangular lattices. We find a subset of this parameter space which gives a reduced holomorphic family, and we discuss symmetries of parameter space that arise from other dynamical properties of this family of maps.

2. Background on the dynamics of meromorphic functions

Let $f : \mathbb{C} \to \mathbb{C}_\infty$ be a meromorphic function where $\mathbb{C}_\infty = \mathbb{C} \cup \{\infty\}$ is the Riemann sphere. The *Fatou set* $F(f)$ is the set of points $z \in \mathbb{C}_\infty$ such that $\{f^n : n \in \mathbb{N}\}$ is defined and normal in some neighborhood of z. The *Julia set* is the complement of the Fatou set on the sphere, $J(f) = \mathbb{C}_\infty \setminus F(f)$. Notice that

$$\mathbb{C}_\infty \setminus \overline{\bigcup_{n \geq 0} f^{-n}(\infty)}$$

is the largest open set where all iterates are defined. If f has at least one pole that is not an omitted value, then

$$\overline{\bigcup_{n \geq 0} f^{-n}(\infty)}$$

has more than two elements. Since

$$f\left(\mathbb{C}_\infty \setminus \overline{\bigcup_{n\geq 0} f^{-n}(\infty)}\right) \subset \mathbb{C}_\infty \setminus \overline{\bigcup_{n\geq 0} f^{-n}(\infty)},$$

Montel's theorem implies that

$$J(f) = \overline{\bigcup_{n\geq 0} f^{-n}(\infty)}.$$

Let Crit f denote the set of critical points of f, that is,

$$\text{Crit } f = \{z : f'(z) = 0\}.$$

If z_0 is a critical point then $f(z_0)$ is a *critical value*. The *postcritical set* of f is:

$$P(f) = \overline{\bigcup_{n\geq 0} f^n(\text{Crit } f)}.$$

A point z_0 is *periodic* of period p if there exists a $p \geq 1$ such that $f^p(z_0) = z_0$. We also call the set $\{z_0, f(z_0), \ldots, f^{p-1}(z_0)\}$ a *p-cycle*. The *multiplier* of a point z_0 of period p is the derivative $(f^p)'(z_0)$. A periodic point z_0 is classified as *attracting, repelling,* or *neutral* if $|(f^p)'(z_0)|$ is less than, greater than, or equal to 1, respectively. If $|(f^p)'(z_0)| = 0$ then z_0 is called a *superattracting* periodic point. As in the case of rational maps, the Julia set is the closure of the repelling periodic points [Baker et al. 1991a].

Suppose U is a connected component of the Fatou set. We say that U is *preperiodic* if there exists $n > m \geq 0$ such that $f^n(U) = f^m(U)$, and the minimum of $n - m = p$ for all such n, m is the *period* of the cycle. Although elliptic functions with a finite number of critical values are meromorphic, it turns out that the classification of periodic components of the Fatou set is no more complicated than that of rational maps of the sphere. Periodic components of the Fatou set of these elliptic functions may be attracting domains, parabolic domains, Siegel disks, or Herman rings [Baker et al. 1992; Erëmenko and Lyubich 1992; Hawkins and Koss 2002].

Let

$$C = \{U_0, U_1, \ldots U_{p-1}\}$$

be a periodic cycle of components of $F(f)$. If C is a cycle of immediate attractive basins or parabolic domains, then

$$U_j \cap \text{Crit } f \neq \varnothing \quad \text{for some } 0 \leq j \leq p - 1.$$

If C is a cycle of Siegel disks or Herman rings, then

$$\partial U_j \subset \overline{\bigcup_{n\geq 0} f^n(\text{Crit } f)} \quad \text{for all } 0 \leq j \leq p - 1.$$

In particular, critical points are required for any type of preperiodic Fatou component.

3. Lattices in the plane

Let $\omega_1, \omega_2 \in \mathbb{C} \setminus \{0\}$ be such that $\omega_2/\omega_1 \notin \mathbb{R}$. We define a lattice of points in the complex plane by

$$\Omega = [\omega_1, \omega_2] := \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}.$$

Different sets of vectors can generate the same lattice Ω. If $\Omega = [\omega_1, \omega_2]$, then any other generators η_1, η_2 of Ω are obtained by multiplying the vector (ω_1, ω_2) by the matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$. The values $\omega_3 = \omega_1 + \omega_2$ and $\omega_4 = \frac{1}{2}\omega_3$ will be used later in this paper.

We can view Ω as a group acting on $\mathbb{C}$ by translation, each $\omega \in \Omega$ inducing the transformation of $\mathbb{C}$:

$$T_\omega : z \mapsto z + \omega.$$

Definition 3.1. A closed, connected subset Q of $\mathbb{C}$ is defined to be a *fundamental region* for Ω if

(i) for each $z \in \mathbb{C}$, Q contains at least one point in the same Ω-orbit as z;

(ii) no two points in the interior of Q are in the same Ω-orbit.

If Q is any fundamental region for Ω, then for any $s \in \mathbb{C}$, the set

$$Q + s = \{z + s : z \in Q\}$$

is also a fundamental region. Usually (but not always) we choose Q to be a polygon with a finite number of parallel sides, in which case we call Q a *period parallelogram* for Ω.

Frequently we refer to types of lattices by the shapes of the corresponding period parallelograms. If Ω is a lattice, and $k \neq 0$ is any complex number, then $k\Omega$ is also a lattice defined by taking $k\omega$ for each $\omega \in \Omega$; $k\Omega$ is said to be *similar* to Ω. Similarity is an equivalence relation between lattices, and an equivalence class of lattices is called a *shape*.

Let $\overline{\Omega}$ denote the set of complex numbers $\overline{\omega}$ for all $\omega \in \Omega$. Then $\overline{\Omega}$ is also a lattice. If $\Omega = \overline{\Omega}$, Ω is called a *real lattice*. There are two special lattice shapes: square and triangular. A *square* lattice is a lattice with the property that $i\Omega = \Omega$. A *triangular* lattice is a lattice with the property that $\varepsilon\Omega = \Omega$, where ε is a cube root of unity; such a lattice forms a pattern of equilateral triangles throughout the plane.

A triangular lattice is in the horizontal position if the main axis of the rhombus is parallel to the real axis, and vertical if the main axis is parallel to the imaginary axis.

Among all lattices, those having the most regular period parallelograms are distinguished in many respects. For example, results on how the lattice shape influences the dynamics of the Weierstrass elliptic function can be found in [Hawkins 2006; Hawkins and Koss 2002; 2004; 2005; Hawkins and Look 2006].

4. The derivative of the Weierstrass elliptic function

For any $z \in \mathbb{C}$ and any lattice Ω, the Weierstrass elliptic function is defined by

$$\wp_\Omega(z) = \frac{1}{z^2} + \sum_{\omega \in \Omega \setminus \{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right).$$

Replacing every z by $-z$ in the definition we see that $\wp_\Omega$ is an even function. It is well-known that $\wp_\Omega$ is meromorphic and is periodic with respect to Ω.

The derivative of the Weierstrass elliptic function is given by

$$\wp_\Omega'(z) = -2 \sum_{\omega \in \Omega} \frac{1}{(z - \omega)^3}.$$

It is also an elliptic function and is periodic with respect to Ω. It is clear from the series definition that $\wp_\Omega'$ is an odd function. In addition, $\wp_\Omega'$ is also meromorphic, with poles of order three at lattice points.

The Weierstrass elliptic function and its derivative are related by the differential equation

$$(\wp_\Omega'(z))^2 = 4(\wp_\Omega(z))^3 - g_2 \wp_\Omega(z) - g_3, \tag{1}$$

where

$$g_2(\Omega) = 60 \sum_{\omega \in \Omega \setminus \{0\}} \omega^{-4} \quad \text{and} \quad g_3(\Omega) = 140 \sum_{\omega \in \Omega \setminus \{0\}} \omega^{-6}.$$

The numbers $g_2(\Lambda)$ and $g_3(\Lambda)$ are invariants of the lattice Λ in the following sense: if $g_2(\Lambda) = g_2(\Lambda')$ and $g_3(\Lambda) = g_3(\Lambda')$, then $\Lambda = \Lambda'$. Furthermore, given any g_2 and g_3 such that $g_2^3 - 27 g_3^2 \neq 0$ there exists a lattice Λ having $g_2 = g_2(\Lambda)$ and $g_3 = g_3(\Lambda)$ as its invariants. If Λ is a square lattice then $g_2 = 0$, and if Λ is a triangular lattice, $g_3 = 0$ [Du Val 1973].

It will be useful to have an expression for $\wp_\Omega''$, the second derivative of the Weierstrass elliptic function for a given lattice Ω. Starting with

$$\wp_\Omega'(z) = -2 \sum_\Omega (z - \omega)^{-3},$$

we differentiate term by term to find that

$$\wp_\Omega''(z) = 6 \sum_\Omega (z - \omega)^{-4}.$$

Further, using (1), we have

$$\wp_\Omega''(z) = 6(\wp_\Omega(z))^2 - \frac{g_2(\Omega)}{2}. \tag{2}$$

The Weierstrass elliptic function, its derivatives, and the lattice invariants satisfy the following homogeneity properties.

Proposition 4.1. *For any lattice Ω and for any $m \in \mathbb{C} \setminus \{0\}$,*

$$\wp_{m\Omega}(mz) = m^{-2}\wp_\Omega(z),$$
$$\wp_{m\Omega}'(mz) = m^{-3}\wp_\Omega'(z),$$
$$\wp_{m\Omega}''(mz) = m^{-4}\wp_\Omega''(z),$$
$$g_2(m\Omega) = m^{-4}g_2(\Omega),$$
$$g_3(m\Omega) = m^{-6}g_3(\Omega).$$

Verification of the homogeneity properties can be seen by substitution into the series definitions.

The homogeneity property of $\wp_\Omega'$ influences the behavior of $\wp_\Omega'$ under iteration.

Corollary 4.2. *If Ω is any lattice then*

$$(\wp_\Omega')^n(-z) = -(\wp_\Omega')^n(z).$$

Proof. Since $\Omega = -\Omega$ for any lattice, the result follows from the homogeneity property in Proposition 4.1. □

Critical points and values play an important role in complex dynamics, so it is useful for us to be able to locate these points for $\wp_\Omega$ and $\wp_\Omega'$. From [Du Val 1973], we see that the critical points of $\wp_\Omega$ lie exactly on the half lattice points of Ω; that is, on $\omega_j/2 + \Omega$ for $j \in \{1, 2, 3\}$. We discuss the critical points for $\wp_\Omega'$ in the following proposition.

Proposition 4.3 [Du Val 1973]. *The critical points of $\wp'$ are the points where $\wp^2(z) = g_2/12$. Further, the critical values of $\wp'$ are $\pm\{-g_3 \pm (g_2/3)^{3/2}\}^{1/2}$.*

Proof. We have $\wp''(z) = 6(\wp(z))^2 - g_2/2$ from (2). Solving $\wp''(z) = 0$ gives us that $\wp'$ has critical points in the four congruence classes where $(\wp(z))^2 = g_2/12$.

The critical values of $\wp'$ are found by solving

$$4(\wp(z))^3 - g_2\wp(z) - ((\wp'(z))^2 + g_3) = 0$$

for $\wp'(z)$ as follows. Substitution of $\pm\sqrt{g_2/12}$ for $\wp(z)$ and simplification lead to

$$-\tfrac{1}{3}g_2^{3/2} = \pm\sqrt{3}((\wp'(z))^2 + g_3).$$

Squaring both sides and rearranging terms shows that

$$g_2{}^3 - 27((\wp'(z))^2 + g_3)^2 = 0,$$

and by solving for $\wp'(z)$, we see that the critical values of $\wp'(z)$ are

$$\pm\bigl(-g_3 \pm (g_2/3)^{3/2}\bigr)^{1/2}. \qquad\qquad \square$$

The critical values are distinct unless the lattice is triangular.

Corollary 4.4. *If Ω is triangular then Ω has exactly two equivalence classes of critical points at $\pm(1/3)\omega_3 + \Omega = \pm(1/3)(\omega_1 + \omega_2) + \Omega = \pm(2/3)\omega_4 + \Omega$ and two distinct critical values at $\pm\sqrt{-g_3}$.*

Proof. We note that if Ω is triangular then the critical points coincide in pairs with the zeros of $\wp_\Omega(z)$. These points occur at the points at the center of the equilateral triangles determined by the lattice, $\pm(1/3)\omega_3 + \Omega = \pm(2/3)\omega_4 + \Omega$. Since $g_2(\Omega) = 0$ for triangular lattices there are only two critical values by Proposition 4.3. $\square$

5. Properties of the Julia and Fatou sets of $\wp'_\Omega$

We begin our investigation of the dynamics of $\wp'_\Omega$ for an arbitrary lattice Ω with an examination of the symmetries that arise in the Julia and Fatou sets.

Theorem 5.1. *Let Ω be any lattice.*

(i) $F(\wp'_\Omega) = F(\wp'_\Omega) + \Omega$ and $J(\wp'_\Omega) = J(\wp'_\Omega) + \Omega$.

(ii) $F(\wp'_\Omega) = -1F(\wp'_\Omega)$ and $J(\wp'_\Omega) = -1J(\wp'_\Omega)$.

(iii) $F(\wp'_{\overline{\Omega}}) = \overline{F(\wp'_\Omega)}$ and $J(\wp'_{\overline{\Omega}}) = \overline{J(\wp'_\Omega)}$.

(iv) *If Ω is square, then $F(\wp'_\Omega) = i\,F(\wp'_\Omega)$ and $J(\wp'_\Omega) = i\,J(\wp'_\Omega)$.*

(v) *If Ω is triangular, then $\varepsilon F(\wp'_\Omega) = F(\wp'_\Omega)$ and $\varepsilon J(\wp'_\Omega) = J(\wp'_\Omega)$ where ε is a cube root of unity.*

Proof. The proof of (i) follows immediately from the periodicity of $\wp'_\Omega$ with respect to Ω.

For (ii), let $z \in F(\wp'_\Omega)$. By definition, $(\wp'_\Omega)^n(z)$ exists and is normal for all n. Let U be a neighborhood of z such that $\{(\wp'_\Omega)^n(U)\}$ forms a normal family. Let $V = -U$. By Corollary 4.2, we have that $(\wp'_\Omega)^n(V) = -(\wp'_\Omega)^n(U)$ for all $n \geq 1$ and thus $\{(\wp'_\Omega)^n(V)\}$ forms a normal family. The proof of the converse is identical. So $z \in F(\wp'_\Omega)$ if and only if $-z \in F(\wp'_\Omega)$, and the Fatou set is symmetric with respect to the origin. This of course forces the Julia set to be symmetric with respect to the origin as well.

To prove (iii), define $\phi(z) = \bar{z}$. We see that $\phi \circ \wp'_\Omega = \wp'_{\bar{\Omega}} \circ \phi$ for all lattices Ω, so for a general lattice the map $\wp'_\Omega$ is conjugate to $\wp'_{\bar{\Omega}}$, and the Julia sets are conjugate under ϕ.

For (iv), we know that square lattices satisfy $i\Omega = \Omega$. Using Proposition 4.1, we have

$$(\wp'_\Omega)^n(-iz) = (\wp'_{i\Omega})^n(-iz) = -i(\wp'_\Omega)^n(z).$$

for all $n \geq 0$. Thus the Julia set and the Fatou set of a square lattice must be symmetric with respect to rotation by $\pi/2$.

A similar application of the homogeneity lemma proves (v). If ε is a cube root of one, then so is $\varepsilon^2 = 1/\varepsilon$; thus $\varepsilon^2 \Omega = \Omega$. Then from Proposition 4.1, $\wp'_\Omega(\varepsilon^2 z) = \wp'_{\varepsilon^2 \Omega}(\varepsilon^2 z) = \wp'_\Omega(z)$; by induction, $(\wp'_\Omega)^n(\varepsilon^2 z) = (\wp'_\Omega)^n(z)$.   □

In addition to a basic Julia set pattern repeating on each fundamental region, we also see symmetry within the period parallelogram.

Proposition 5.2. *For the lattice $\Omega = [\omega_1, \omega_2]$, $J(\wp'_\Omega)$ and $F(\wp'_\Omega)$ are symmetric with respect to the half lattice points $\omega_1/2 + \Omega$, $\omega_2/2 + \Omega$, and $(\omega_1 + \omega_2)/2 + \Omega$.*

Proof. This follows easily from Theorem 5.1 (i), (ii). We have $z \in J(\wp'_\Omega)$ if and only if $-z + \Omega \in J(\wp'_\Omega)$, and a half lattice point must lie between z and $-z + \Omega$ for any element of the lattice.   □

6. Postcritical orbits

Recall from Proposition 4.3 that the critical points of $\wp'$ are the points where $\wp^2(u) = g_2/12$. Our next result shows that multiplying the lattice Ω by k changes the location of the critical points from a_Ω to ka_Ω.

Theorem 6.1. *Let Ω be a lattice and suppose a_Ω is a critical point of $\wp'_\Omega$. Then ka_Ω is a critical point of $\wp'_{k\Omega}$.*

Proof. Suppose a_Ω is a critical point for $\wp'_\Omega$; that is, assume that $[\wp_\Omega(a_\Omega)]^2 = g_2(\Omega)/12$. From Proposition 4.1, we have $g_2(k\Omega) = k^{-4} g_2(\Omega)$ and

$$[\wp_{k\Omega}(ka_\Omega)]^2 = \left[\frac{1}{k^2}\wp_\Omega(a_\Omega)\right]^2 = \frac{1}{k^4}[\wp_\Omega(a_\Omega)]^2 = \frac{g_2(\Omega)}{k^4 12} = \frac{g_2(k\Omega)}{12}.$$

Thus if a_Ω is a critical point of $\wp'_\Omega$, then ka_Ω is a critical point of $\wp'_{k\Omega}$.   □

We will use the notation $a_{k\Omega}$ to denote the critical point ka_Ω for $\wp'_{k\Omega}$.

From Corollary 4.4, we know that triangular lattices are distinguished by the fact that they have exactly two critical values. We restrict our attention to triangular lattices throughout the rest of the paper. In particular, the postcritical orbits of $\wp'_\Omega$ are related in an especially nice way when Ω is a triangular lattice.

Proposition 6.2. *If* Ω *is a triangular lattice then* $P(\wp'_\Omega)$ *is contained in two forward invariant sets*: *one set*

$$\alpha = \overline{\bigcup_{n \geq 0} (\wp'_\Omega)^n (a_\Omega)},$$

and the set $e^{i\pi}\alpha$. (*These sets are not necessarily disjoint.*)

Proof. The proof follows from the application of Corollaries 4.2 and 4.4. $\qquad\square$

Let Λ be the lattice generated by $g_2 = 0$, $g_3 = -4$. We call Λ the *standard triangular lattice*, and we reserve the symbol Λ to denote this particular lattice throughout the rest of this paper. Then Λ is a triangular lattice in the horizontal position. Let λ_1, λ_2 be a pair of generators for this lattice such that λ_1 is in the first quadrant and λ_2 is its conjugate in the fourth quadrant. Using Mathematica or the tables in [Milne-Thomson 1950], we can estimate $\lambda_1 \approx 2.1 + 1.2i$ and $\lambda_2 \approx 2.1 - 1.2i$. Define $\lambda_3 = \lambda_1 + \lambda_2$ and $\lambda_4 = (1/2)(\lambda_1 + \lambda_2) = (1/2)\lambda_3$. Note that both λ_3 and λ_4 are real. Recall from Corollary 4.4 that for a general triangular lattice Ω, the critical points are $\pm(2/3)\omega_4$; let $a_\Lambda = (2/3)\lambda_4$ so that a_Λ is a critical point of $\wp'_\Lambda$. For the lattice $k\Lambda$, let $k\lambda_n$ denote the lattice points for $n = 1, 2, 3$, and let $a_{k\Lambda}$ denote the critical point ka_Λ. Theorem 6.1 gives that $a_{k\Lambda} = (2k/3)\lambda_4$. Since any triangular lattice Ω can be written as $\Omega = k\Lambda$ for some k, our discussion will now focus on the lattice Λ.

We begin with a lemma explaining how multiplying the standard triangular lattice Λ by certain values of k changes the critical values of $\wp'_{k\Lambda}$. The lemma will be useful in finding lattices for which the postcritical orbit is especially simple.

Lemma 6.3. *Let* Λ *be the standard triangular lattice,* j *be a nonzero integer, and choose* k *such that* $k^4 = (2/j)(-2/\lambda_3)$. *Then* $\wp'_{k\Lambda}(ka_\Lambda) = (j/2)k\lambda_3$. *That is,* $\wp'_{k\Lambda}$ *maps the critical point* $a_{k\Lambda}$ *to the critical value* $(j/2)k\lambda_3$.

Proof. Note that $\wp'_\Lambda(a_\Lambda) = -\sqrt{-g_3(\Lambda)} = -2$. By Proposition 4.1,

$$\wp'_{k\Lambda}(ka_\Lambda) = \frac{1}{k^3} \wp'_\Lambda(a_\Lambda).$$

Multiplying by k/k gives

$$\frac{k}{k^4}\wp'_\Lambda(a_\Lambda) = \frac{-2k}{\dfrac{2}{j} \times \dfrac{-2}{\lambda_3}} = \frac{j}{2}k\lambda_3,$$

as desired. $\qquad\square$

We can use Lemma 6.3 to find values of k so that $\wp'_{k\Lambda}$ has critical values located at either lattice points or half lattice points.

Lemma 6.4. *Let* Λ *be the standard triangular lattice, and let* j *be an even, nonzero integer. Choose* k *such that* $k^4 = (2/j)(-2/\lambda_3)$. *Then* $\wp'_{k\Lambda}$ *maps the critical point* $a_{k\Lambda}$ *to a lattice point of* $k\Lambda$.

Proof. We know from Lemma 6.3 that $\wp'_{k\Lambda}(ka_\Lambda) = (j/2)k\lambda_3$. Because j is even, $(j/2)k\lambda_3$ is a lattice point of $k\Lambda$. $\qquad\square$

Lemma 6.5. *Let* Λ *be the standard triangular lattice, and let* j *be an odd integer. Choose* k *such that* $k^4 = (2/j)(-2/\lambda_3)$. *Then* $\wp'_{k\Lambda}$ *maps the critical point* $a_{k\Lambda}$ *to a half lattice point of* $k\Lambda$.

Proof. We know from Lemma 6.3 that $\wp'_{k\Lambda}(ka_\Lambda) = (j/2)k\lambda_3$. Because j is odd, $(j/2)k\lambda_3$ is a half lattice point of $k\Lambda$. $\qquad\square$

We can use the previous lemmas to find lattices for which all of the critical points are prepoles and thus lie in the Julia set.

Theorem 6.6. *Let* Λ *be the standard triangular lattice, and choose* k *so that* $k^4 = (2/j)(-2/\lambda_3)$ *for some nonzero integer* j. *Then the Julia set of* $\wp'_{k\Lambda}$ *is* $\mathbb{C}_\infty$.

Proof. Suppose j is odd. By Lemma 6.5, $\wp'_{k\Lambda}(ka_\Lambda)$ lands on a half lattice point of $k\Lambda$. Recall that the critical points of $\wp$ lie at half lattice points; thus

$$\wp'_{k\Lambda}(\wp'_{k\Lambda}(ka_\Lambda)) = 0.$$

Then $a_{k\Lambda}$ is a prepole, and by Corollary 4.2 so is $-a_{k\Lambda}$. Then the postcritical set $\{0, \infty\}$ is a finite subset of $J(\wp'_{k\Lambda})$, and thus $J(\wp'_{k\Lambda}) = \mathbb{C}_\infty$.

Now suppose j is even. By Lemma 6.4, $\wp'_{k\Lambda}(ka_\Lambda)$ lands on a lattice point of $k\Lambda$. But the lattice points of $k\Lambda$ are the poles of $\wp'_{k\Lambda}$, so $\wp'_{k\Lambda}(ka_\Lambda)$ is a pole. Again we have a finite postcritical set contained in $J(\wp'_{k\Lambda})$, and thus $J(\wp'_{k\Lambda}) = \mathbb{C}_\infty$. $\qquad\square$

Next, we focus on finding specific values of k which will map critical points to critical points, which we can use to find examples where the Julia set is not the entire sphere. We begin with a lemma that describes how to map critical points to integer multiples of critical points.

Lemma 6.7. *Let* Λ *be the standard triangular lattice and* m *be a nonzero integer. Choose* k *such that* $k^4 = (-2/ma_\Lambda)$. *Then* $\wp'_{k\Lambda}(a_{k\Lambda}) = ma_{k\Lambda}$.

Proof. By Proposition 4.1, $\wp'_{k\Lambda}(ka_\Lambda) = (1/k^3)\wp'_\Lambda(a_\Lambda)$. Again, we multiply by k/k and have

$$\frac{k}{k^4}\wp'_\Lambda(a_\Lambda) = \frac{-2k}{-2/ma_\Lambda} = mka_\Lambda = ma_{k\Lambda},$$

as desired. $\qquad\square$

The role of the integer m is similar to that of the integer j in Lemma 6.3: different values of m give rise to different consequences.

Lemma 6.8. *Let Λ be the standard triangular lattice, and let m be a nonzero integer of the form $3n$. Choose k such that $k^4 = (-2/ma_\Lambda)$. Then $\wp'_{k\Lambda}(ka_\Lambda)$ lands on a lattice point of $k\Lambda$.*

Proof. From Lemma 6.7, $\wp'_{k\Lambda}(ka_\Lambda) = ma_{k\Lambda}$. Then $ma_{k\Lambda} = 3n(2/3)\lambda_4 = n\lambda_3$. $\square$

Note that this is the same case as in Lemma 6.4.

Next, we show that if m has the form $3n + 1$ then $\wp'_{k\Lambda}$ has two superattracting fixed points.

Lemma 6.9. *Let Λ be the standard triangular lattice, and let m be a nonzero integer of the form $3n + 1$. Choose k such that $k^4 = (-2/ma_\Lambda)$. Then $ma_{k\Lambda}$ and $-ma_{k\Lambda}$ are superattracting fixed points for $\wp'_{k\Lambda}$.*

Proof. We know from Lemma 6.7 that $\wp'_{k\Lambda}(ka_\Lambda) = ma_{k\Lambda}$. Because m has the form $3n + 1$,

$$ma_{k\Lambda} = (3n+1)a_{k\Lambda} = 3n\tfrac{1}{3}k\lambda_3 + \tfrac{2}{3}k\lambda_4 = nk\lambda_3 + \tfrac{2}{3}k\lambda_4 \cong \tfrac{2}{3}k\lambda_4 = a_{k\Lambda}.$$

Hence we see that $ma_{k\Lambda}$ and $a_{k\Lambda}$ are in the same residue class and thus map to the same point. Thus

$$\wp'_{k\Lambda}(ma_{k\Lambda}) = \wp'_{k\Lambda}(a_{k\Lambda}) = ma_{k\Lambda},$$

and we see that $ma_{k\Lambda}$ is a superattracting fixed point of $\wp'_{k\Lambda}$. Since $\wp'_{k\Lambda}$ is odd, $-ma_{k\Lambda}$ is also a superattracting fixed point of $\wp'_{k\Lambda}$ $\square$

On the other hand, if m has the form $3n - 1$ then $\wp'_{k\Lambda}$ has a superattracting two-cycle.

Lemma 6.10. *Let Λ be the standard triangular lattice, and let m be a nonzero integer of the form $3n - 1$. Choose k such that $k^4 = (-2/ma_\Lambda)$. Then $\{ma_{k\Lambda}, -ma_{k\Lambda}\}$ form a superattracting 2-cycle for $\wp'_{k\Lambda}$.*

Proof. We know from Lemma 6.7 that $\wp'_{k\Lambda}(ka_\Lambda) = ma_{k\Lambda}$. Since m has the form $3n - 1$,

$$ma_{k\Lambda} = (3n-1)a_{k\Lambda} = 3n\tfrac{1}{3}k\lambda_3 - \tfrac{2}{3}k\lambda_4 = nk\lambda_3 - \tfrac{2}{3}k\lambda_4 \cong -\tfrac{2}{3}k\lambda_4 = -a_{k\Lambda}.$$

Thus we have that $ma_{k\Lambda}$ and $-a_{k\Lambda}$ are congruent (mod $k\Lambda$). Then, by Proposition 4.1, we see that $\wp'_{k\Lambda}(ma_{k\Lambda}) = \wp'_{k\Lambda}(-a_{k\Lambda}) = -\wp'_{k\Lambda}(a_{k\Lambda}) = -ma_{k\Lambda}$. Similarly, $\wp'_{k\Lambda}(-ma_{k\Lambda}) = ma_{k\Lambda}$, and we have a superattracting 2-cycle. $\square$

The next theorem follows immediately from the previous two lemmas.

Theorem 6.11. *Let Λ be the standard triangular lattice, and choose k so that $k^4 = (-2/ma_\Lambda)$ for some nonzero integer m. Then if m is of the form $3n - 1$ or $3n + 1$ the Fatou set of $\wp'_{k\Lambda}$ is nonempty.*
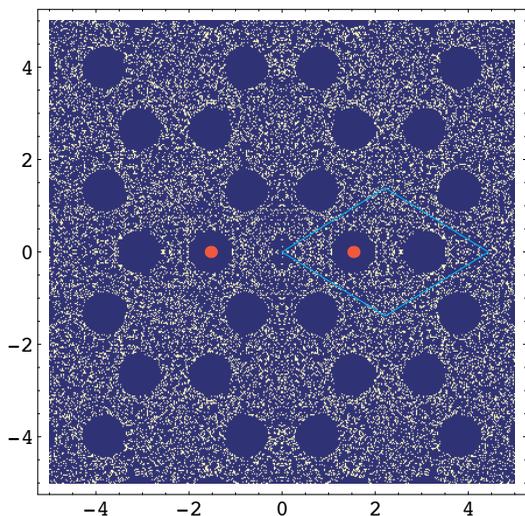
Figure 1. Example with a superattracting 2-cycle.

To illustrate Lemma 6.10, consider Figure 1. In this graph we use Mathematica to draw the Julia and Fatou set of $\wp'_{k\Lambda}$ with k chosen so that $k^4 = (-2/ma_\Lambda)$, where $m = -1$ and Λ is the standard triangular lattice. Thus we have a superattracting 2-cycle $\{a_{k\Lambda}, -a_{k\Lambda}\}$. The Fatou set is colored blue, and the Julia set is yellow. The points of the 2-cycle, at $z \approx \pm 1.532 + 0i$, are shown as red dots, and a period parallelogram is also displayed for reference. For this lattice, we have $g_3(k\Omega) \approx -2.348$.

We note that the sign of k influences the orientation of the lattice. If k^4 is positive, then two of the values of k are real, one positive and one negative, and the other two values are pure imaginary, with one positive and one negative. When k is real, the lattice $k\Lambda$ is triangular in the horizontal orientation, and when k is pure imaginary, the lattice $k\Lambda$ is triangular in the vertical orientation.

If k^4 is negative then the values of k are complex; two lie on the line $y = x$ and two on the line $y = -x$. For such values of k, the lattice $k\Lambda$ is no longer a real lattice. One such example is shown is Figure 2, where we are in the setting of Lemma 6.9, and we have chosen k such that $k^4 = (-2/ma_\Lambda)$ and $m = 1$. In this case, we have two superattracting fixed points. Note for future reference that this lattice has $g_3(k\Omega) \approx -2.348i$.

The method of the last few results has been to start with a lattice Ω and choose a k value so that $k\Omega$ maps a critical point $a_{k\Omega}$ to another critical point, resulting in superattracting fixed points or superattracting two-cycles. The next proposition shows that it is impossible to construct superattracting cycles of length $n > 2$ in this way.
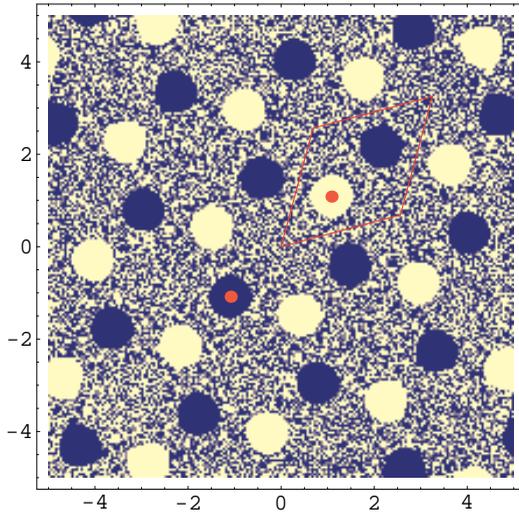
Figure 2. Example with two superattracting fixed points.

Proposition 6.12. *Let Ω be a triangular lattice with critical points t_1 and t_2. Suppose $\wp'_\Omega(t_1) = t_2$. If $t_1 \cong t_2 (\mathrm{mod}\ \Omega)$, t_2 is a superattracting fixed point. If t_1 and t_2 are not congruent, t_2 and $-t_2$ form a superattracting 2-cycle.*

Proof. Case 1: $t_1 \cong t_2 \ (\mathrm{mod}\ \Omega)$. We know that $\wp'_\Omega(t_1) = t_2$. Further, by the congruence of t_1 and t_2, $\wp'_\Omega(t_2) = \wp'_\Omega(t_1) = t_2$. Thus t_2 is a superattracting fixed point.

Case 2: $t_1 \ncong t_2 (\mathrm{mod}\ \Omega)$. Because we are dealing with a triangular lattice, we know that there are only two congruence classes of critical points. From Corollary 4.2, we also know that $\wp'_\Omega(-t_1) = -\wp'_\Omega(t_1)$; thus t_1 and $-t_1$ do not map to the same point, and therefore must be in different congruence classes. Since there are only two congruence classes of critical points, and since both t_2 and $-t_1$ are not congruent to t_1, we see that $t_2 \cong -t_1 (\mathrm{mod}\ \Omega)$.

Again, we know that $\wp'_\Omega(t_1) = t_2$. Further, by the congruence of $-t_1$ and t_2, $\wp'_\Omega(t_2) = \wp'_\Omega(-t_1) = -\wp'_\Omega(t_1) = -t_2$. By Corollary 4.2, we also have $\wp'_\Omega(-t_2) = -\wp'_\Omega(t_2) = t_2$. Thus we have a superattracting 2-cycle. $\qquad\square$

For example, Proposition 6.12 says that we can't have a superattracting three cycle that contains two critical points.

7. Parameter space

Next, we study the parameter space for the elliptic functions $\wp'_\Omega$ for triangular lattices Ω. The theory of holomorphic families was introduced by Mañé et al. [1983], refined by McMullen [2000], generalized to the setting of meromorphic maps with finite singular set by Keen and Kotus [1997], and discussed for the

Weierstrass elliptic function in [Hawkins and Koss 2004] and [Hawkins and Look 2006].

We begin with the definition of parameter space for triangular lattices.

Definition 7.1. Given $g_2 = 0$, we define $g_3 - space$ to be the set of points $g_3 \in \mathbb{C} \setminus \{0\}$ which represent the triangular lattice Γ determined by $g_2 = 0$ and g_3, and therefore the function $\wp_\Gamma$.

Let $\Gamma(0, g_3)$ denote the lattice determined by $g_2 = 0$ and $g_3 \in \mathbb{C} \setminus \{0\}$. Then the map:

$$F : \mathbb{C} \setminus \{0\} \times \mathbb{C} \to \mathbb{C}_\infty$$

given by $F(g_3, z) = \wp'_{\Gamma(0,g_3)}(z)$ is holomorphic in g_3 and meromorphic in z. This defines a holomorphic family of meromorphic functions; we say that the holomorphic family of meromorphic maps parametrized over a complex manifold M is *reduced* if for all triangular lattices $\Gamma \neq \Omega$ in M, $\wp'_\Gamma$ and $\wp'_\Omega$ are not conformally conjugate. In the current setting, g_3-space is not reduced; the next results distinguish the symmetries of parameter space arising from conjugacy from the symmetries that occur for other reasons.

We first describe the possible conformal conjugacies that can occur between two maps $\wp'_\Omega$ and $\wp'_\Gamma$ when Ω and Γ are triangular lattices.

Lemma 7.2. *If $\wp'_\Gamma$ is conformally conjugate to $\wp'_\Omega$ via a Möbius map ϕ, then $\phi(z) = az$ and $\phi(\Gamma) = \Omega$.*

Proof. Assume that $\phi(z) = (az + b)/(cz + d)$ and $\phi \circ \wp'_\Gamma(z) = \wp'_\Omega \circ \phi(z)$ for all $z \in \mathbb{C}$. Then $\phi(\infty) = \infty$ (since neither $\wp'_\Omega$ nor $\wp'_\Gamma$ is defined precisely at that point); that is, ϕ takes $\mathbb{C}$ onto $\mathbb{C}$. This means that $c = 0$ and ϕ is affine. Therefore $\phi(z) = az + b$ with $a \neq 0$; we have $\phi(0) = b \in \Omega$ since it must be a pole of $\wp'_\Omega$.

Since critical points must be mapped to critical points under ϕ, the critical values are mapped to critical values as well. The critical values of $\wp'_\Gamma$ are $c_\Gamma = \sqrt{-g_3(\Gamma)}$ and $-c_\Gamma$, and the critical values of $\wp'_\Lambda$ are $c_\Omega = \sqrt{-g_3(\Omega)}$ and $-c_\Omega$. First, if the critical values are mapped in the order $\phi(c_\Gamma) = c_\Omega$ and $\phi(-c_\Gamma) = -c_\Omega$, then

$$ac_\Gamma + b = c_\Omega \quad \text{and} \quad -ac_\Gamma + b = -c_\Omega;$$

therefore $b = 0$. If the critical values are mapped with the opposite pairing then $b = 0$ as well. Therefore $b = 0$, $\phi(z) = az$, and ϕ induces a group isomorphism between $\mathbb{C}/\Gamma$ and $\mathbb{C}/\Omega$; in particular $a\Gamma = \Omega$. $\square$

Rotating a lattice by $e^{i\pi/2}$ results in conformal conjugacy.

Theorem 7.3. *If Ω is any triangular lattice and $i\Omega = \Gamma$, then $\wp_\Gamma$ and $\wp_\Omega$ are conformally conjugate via the map $\phi(z) = iz$. Further, $g_3(\Gamma) = -g_3(\Omega)$. If $\{z_1, \ldots, z_n\}$ is a cycle of length n with multiplier β under $\wp'_\Omega$ then $\{iz_1, \ldots, iz_n\}$ is a cycle of length n with multiplier β under $\wp'_{i\Omega}$.*

Proof. We need to show that $\phi \circ \wp'_\Omega(z) = \wp'_\Gamma \circ \phi(z)$. From Proposition 4.1,

$$\wp'_\Gamma(iz) = \wp'_{i\Omega}(iz) = i^{-3}\wp'_\Omega(z) = i\wp'_\Omega(z).$$

Also from Proposition 4.1, we have

$$g_3(\Gamma) = g_3(i\Omega) = i^{-6}g_3(\Omega) = -g_3(\Omega).$$

Now assume that $z_1, \ldots, z_n$ is a cycle of length n under $\wp'_\Omega$. From Proposition 4.1, for $1 \le j \le n$ we have

$$\wp'_{i\Omega}(iz_j) = \frac{1}{i^3}\wp'_\Omega(z_j) = i\wp'_\Omega(z_j) = iz_{j+1}.$$

Therefore $\{iz_1, \ldots, iz_n\}$ is a cycle of length n under $\wp'_{i\Omega}$.

Also, from Proposition 4.1, we have

$$\wp''_{i\Omega}(iz) = i^{-4}\wp''_\Omega(z) = \wp''_\Omega(z),$$

so the cycles have the same multiplier. □

Although each $g_3 \in \mathbb{C} \setminus \{0\}$ corresponds to a unique lattice, the conjugacy given in Theorem 7.3 leads to $e^{\pi i}$ rotational symmetry in g_3-space coming from conformal conjugacy of the mappings. Therefore g_3-space is not a reduced space.

Theorem 7.4. *For triangular lattices $\Gamma_1 \ne \Gamma_2$, $\wp'_{\Gamma_1}$ is conformally conjugate to $\wp'_{\Gamma_2}$ if and only if $\Gamma_1 = \pm i\Gamma_2$.*

Proof. ($\Leftarrow$): By Theorem 7.3, if $\Gamma_2 = e^{\pi i/2}\Gamma_1$, then $\wp'_{\Gamma_1}$ is conformally conjugate to $\wp'_{\Gamma_2}$.

($\Rightarrow$): Suppose that $\wp'_{\Gamma_1}$ is conformally conjugate to $\wp'_{\Gamma_2}$. Then the conjugating map is of the form $\phi(z) = az$ by Lemma 7.2, and we write $\Gamma_2 = a\Gamma_1$. It follows from Proposition 4.1 that $g_3(\Gamma_2) = a^{-6}g_3(\Gamma_1)$. The critical values for a triangular lattice always satisfy $c_1 = -c_2 = \sqrt{-g_3}$, by Corollary 4.4. Then $\phi(c_{\Gamma_1}) = ac_{\Gamma_1} = \pm c_{\Gamma_2}$. But

$$ac_{\Gamma_1} = a\sqrt{-g_3(\Gamma_1)} = a\sqrt{-g_3\left(\frac{1}{a}\Gamma_2\right)} = a\sqrt{-a^6 g_3(\Gamma_2)} = a^4 c_{\Gamma_2},$$

and $a^4 = \pm 1$.

If $a^4 = -1$ then $a = e^{m\pi i/4}$ for $m = 1, 3, 5$, or 7. Then $a\wp'_{\Gamma_1}(z) = \wp'_{a\Gamma_1}(az)$. However, from Proposition 4.1,

$$\wp'_{a\Gamma_1}(az) = a^{-3}\wp'_{\Gamma_1}(z),$$

which would imply that $a^4 = 1$, a contradiction.

If $a = \pm 1$ then $\Gamma_2 = \Gamma_1$. The only cases remaining are when $a^2 = -1$, which gives the result. □
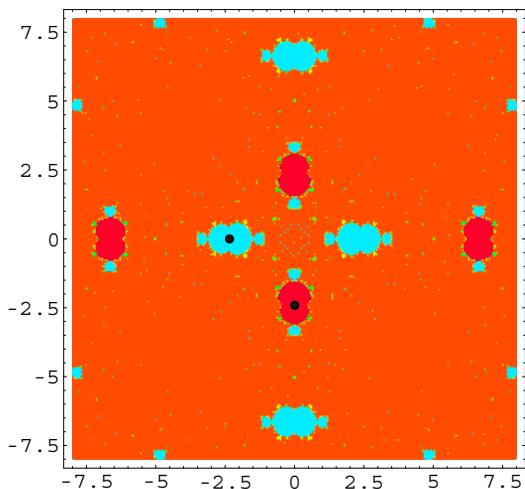
Figure 3. g_3-space showing $g_3 = -2.348$ and $g_3 = -2.348i$.

Corollary 7.5. *For triangular lattices, the sector of g_3-space such that*

$$-\frac{\pi}{2} < \text{Arg } g_3 \leq \frac{\pi}{2}$$

is a reduced holomorphic family of meromorphic maps.

Proof. By Proposition 4.1, $g_3(\Gamma_1) = g_3(i\Gamma_2) = i^{-6}g_3(\Gamma) = -g_3(\Gamma_2)$. $\qquad\square$

In Figure 3 we have drawn a portion of g_3-space centered at the origin using Mathematica. We color each value in the g_3-plane according to the behavior of the stationary point a_Ω for $\wp'_{\Omega(0,g_3)}$. We know that the behavior of the orbits of the critical points a_Ω and $-a_\Omega$ are related by Proposition 6.2, so it suffices to investigate the orbit of a_Ω. Red points are values of g_3 where a_Ω is drawn to a fixed point; blue points are values of g_3 where a_Ω is drawn to a 2-cycle; and green points are values of g_3 where a_Ω is drawn to a 3-cycle. If no cycle was ascertained by Mathematica, then g_3 is colored orange. For reference, we have also labeled the g_3 values in Figure 3 that correspond to the examples shown in Figures 1 and 2.

We observe the $e^{\pi i}$ rotational symmetry in g_3-space predicted by Corollary 7.5. However, we also notice $e^{\pi i/2}$ rotational symmetry of shape, but not color, that does not relate to conformal conjugacy. Our next few results explain this symmetry.

First, we show that for $k = e^{\pi i/4}$, the Fatou set of $\wp'_{k\Omega}$ is the Fatou set of $\wp'_\Omega$ rotated by k.

Theorem 7.6. *Let Ω be any triangular lattice. Then $e^{\pi i/4}F(\wp'_\Omega) = F(\wp'_{e^{\pi i/4}\Omega})$ and $g_3(e^{\pi i/4}\Omega) = i g_3(\Omega)$.*
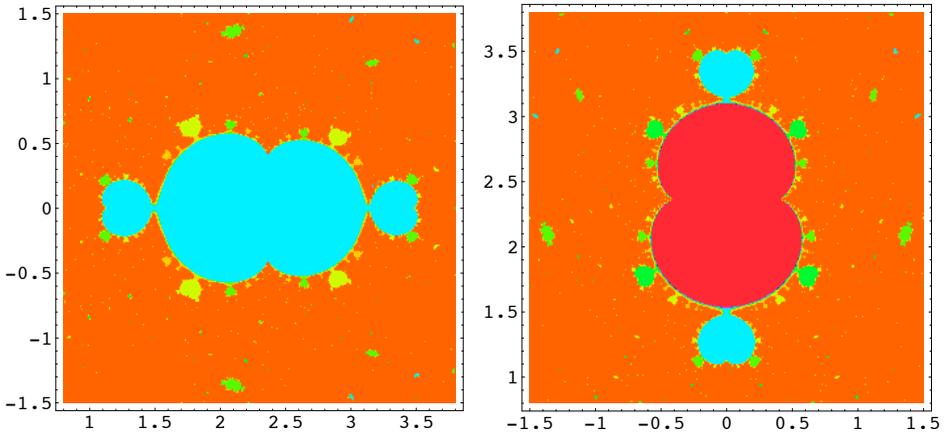
Figure 4. Region of g_3-space near $g_3 = 2.348$ (left); near $g_3 = 2.348i$ (right).

Proof. Using Proposition 4.1, we have

$$\wp'_{e^{\pi i/4}\Omega}(e^{\pi i/4}z) = e^{-3\pi i/4}\wp'_{\Omega}(z) = -e^{\pi i/4}\wp'_{\Omega}(z),$$

and thus

$$(\wp'_{e^{\pi i/4}\Omega})^n(e^{\pi i/4}z) = (-1)^n e^{\pi i/4}(\wp'_{\Omega})^n(z).$$

If U is a neighborhood of z such that $\{(\wp'_{\Omega})^n(U)\}$ forms a normal family, then $V = e^{i\pi/4}U$ is a neighborhood of $e^{i\pi/4}z$ such that $\{(\wp'_{e^{\pi i/4}\Omega})^n(e^{\pi i/4}V)\}$ forms a normal family.

Proposition 4.1 gives that $g_3(e^{\pi i/4}\Omega) = i\,g_3(\Omega)$. $\qquad\qquad\square$

In fact, we can say much more about the behavior of periodic orbits. For example, we see that under rotation by $e^{i\pi/2}$ in g_3-space, red regions become blue, meaning that all 1-cycles become 2-cycles. However, some blue regions rotate to red regions, while other blue regions remain blue under rotation. We show a close-up of this phenomenon in Figure 4. The next three theorems explain what happens to periodic orbits as we rotate by $e^{i\pi/2}$ in g_3-space.

We begin by showing that cycles of odd length n turn into cycles of length $2n$ when the lattice is rotated by $e^{i\pi/4}$.

Theorem 7.7. *If $\{z_j\}_{j=1}^n$ is a cycle of odd length under $\wp'_{\Omega}$ and $k = e^{i\pi/4}$, then*

$$\{(-1)^{j+1}k z_{j\,(\mathrm{mod}\,n)}\}_{j=1}^{2n}$$

is a cycle of length $2n$ under $\wp'_{k\Omega}$. Further, the $2n$-cycle has the same classification as the n-cycle.

Proof. Let $k = e^{\pi i/4}$. Assume that $\{z_j\}_{j=1}^n$ is a cycle of odd length under $\wp'_\Omega$. From [Proposition 4.1](#),

$$\wp'_{k\Omega}(kz_j) = e^{-3i\pi/4}z_j = -kz_{j+1}, \quad \wp'_{k\Omega}(-kz_j) = -e^{-3i\pi/4}z_j = kz_{j+1}.$$

Using these, we see that under $\wp'_{k\Omega}$,

$$kz_1 \to -kz_2 \to \cdots \to kz_n \to -kz_1 \to \cdots \to -kz_n \to kz_1.$$

Since $z_1 \neq z_j$ for $2 \leq j \leq n$, we have $kz_1 \neq kz_j$; we also know that $z_1 \neq -z_1$, and so $kz_1 \neq -kz_1$. However, we still must verify that $kz_1 \neq -kz_j$ for $2 \leq j \leq n$ to ensure that our new cycle under $\wp'_{k\Omega}$ is in fact of length $2n$. Assume not, so that $kz_1 = -kz_j$ for some $2 \leq j \leq n$. Then $z_1 = -z_j$, so that under $\wp'_\Omega$, $z_{j-1} \to -z_1$ and $-z_{j-1} \to -z_j = z_1$. Then our original cycle is

$$\{z_1, z_2, \ldots, z_{j-1}, -z_1, \ldots, -z_{j-1}\}.$$

But the length of this cycle is given by $2(j-1)$, which is even. We therefore have a contradiction, and our new cycle has length $2n$.

To see that the n-cycle and the $2n$-cycle have the same classification, we first examine $\left|[(\wp'_\Omega)^n]'(z_1)\right|$. Using the chain rule, we see that

$$[(\wp'_\Omega)^n]'(z_1) = \prod_{k=0}^{n-1} \wp''_\Omega((\wp'_\Omega)^k(z_1)).$$

Next, we consider $|[(\wp'_{k\Omega})^{2n}]'(kz_1)|$, whose value determines the classification of the $2n$-cycle. We again use the chain rule to see that

$$[(\wp'_{k\Omega})^{2n}]'(kz_1) = \wp''_{k\Omega}((\wp'_{k\Omega})^{2n-1}(kz_1)) \cdot \wp''_{k\Omega}((\wp'_{k\Omega})^{2n-1}(kz_1)) \cdot \cdots \cdot \wp''_{k\Omega}(kz_1).$$

From [Proposition 4.1](#), we see that $(\wp'_{k\Omega})^m(kz_1) = (-1)^m k\wp'_\Omega(z_1)$ for any integer m, and that $\wp''_{k\Omega}((-1)^m kz) = -\wp''_\Omega(z)$. Then

$$\wp''_{k\Omega}((\wp'_{k\Omega})^{2n-1}(kz_1)) \cdot \wp''_{k\Omega}((\wp'_{k\Omega})^{2n-2}(kz_1)) \cdot \cdots \cdot \wp''_{k\Omega}(kz_1)$$
$$= \wp''_{k\Omega}((-1)^{2n-1}k\wp'_\Omega{}^{2n-1}(z_1)) \cdot \wp''_{k\Omega}((-1)^{2n-2}k\wp'_\Omega{}^{2n-2}(z_1)) \cdots \wp''_{k\Omega}(kz_1)$$
$$= -\wp''_\Omega(\wp'_\Omega{}^{2n-1}(z_1)) \cdot -\wp''_\Omega(\wp'_\Omega{}^{2n-2}(z_1)) \cdot \cdots \cdot -\wp''_\Omega(z_1).$$

Finally, we recall that z_1 has period n under $\wp'_\Omega$. Because of this,

$$\wp'_\Omega{}^{2n-s}(z_1) = \wp'_\Omega{}^{n-s}(z_1).$$

Therefore,

$$\left|[(\wp'_{k\Omega})^{2n}]'(kz_1)\right| = \left|[(\wp'_\Omega)^n]'(z_1)\right|^2,$$

and so the $2n$-cycle formed by kz_1 under $\wp'_{k\Omega}$ has the same classification as the n-cycle formed by z_1 under $\wp'_\Omega$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

For example, suppose $\{z_1, z_2, z_3\}$ is a 3-cycle under $\wp'_\Omega$. Theorem 7.7 then says that $\{kz_1, -kz_2, kz_3, -kz_1, kz_2, -kz_3\}$ is a 6-cycle under $\wp'_{k\Omega}$, and that the 6-cycle has the same classification as the 3-cycle.

From Proposition 4.1, $g_3(k\Omega) = ig_3(\Omega)$; thus, we have shown that any region corresponding to a cycle with odd length n will become a region corresponding to a cycle of length $2n$ under rotation by $e^{i\pi/2}$. Specifically, regions corresponding to fixed points will become regions corresponding to 2-cycles. Next we have a similar result involving n-cycles of even length satisfying a certain structure and rotation by $e^{i\pi/2}$.

Theorem 7.8. *If $\{(-1)^{j+1}z_{j(\mathrm{mod}\ n)}\}_{j=1}^{2n}$ with n odd is a cycle under $\wp'_\Omega$ and $k = e^{i\pi/4}$, then $\{kz_j\}_{j=1}^{n}$ and $\{-kz_j\}_{j=1}^{n}$ are cycles of odd length under $\wp'_{k\Omega}$. Further, the classification of the n-cycle under $\wp'_{k\Omega}$ is the same as the classification of the $2n$-cycle under $\wp'_\Omega$.*

Proof. Let $k = e^{i\pi/4}$. Assume that $\{(-1)^{j+1}z_{j(\mathrm{mod}\ n)}\}_{j=1}^{2n}$ with n odd is a cycle under $\wp'_\Omega$. From Proposition 4.1,

$$\wp'_{k\Omega}(kz_j) = e^{-3i\pi/4}\wp'_\Omega(z_j) = -k\wp'_\Omega(z_j) = (-k)(-z_{j+1}) = kz_{j+1}.$$

Thus, under $\wp'_{k\Omega}$,

$$kz_1 \to kz_2 \to \cdots \to kz_n \to kz_1.$$

We know that $z_1 \neq z_j$ for all $2 \leq j \leq n$, so it is also true that $kz_1 \neq kz_j$ for all $2 \leq j \leq n$. Thus $\{kz_j\}_{j=1}^{n}$ is a cycle under $\wp'_{k\Omega}$, as is $\{-kz_j\}_{j=1}^{n}$.

The proof that the n-cycle under $\wp'_{k\Omega}$ has the same classification as the $2n$-cycle under $\wp'_\Omega$ follows from the same reasoning as in the proof of Theorem 7.7. $\qquad\square$

For example, if

$$\{z_1, -z_2, z_3, -z_1, z_2, -z_3\}$$

is a cycle under $\wp'_\Omega$, then

$$\{kz_1, kz_2, kz_3\}$$

is a cycle under $\wp'_{k\Omega}$, and both cycles have the same classification.

Theorems 7.7 and 7.8 are very closely related. If we begin with a g_3 value that corresponds to a lattice with a cycle of odd length n, then $e^{i\pi/2}g_3$ corresponds to a lattice with a cycle of length $2n$; another rotation by $e^{i\pi/2}$ gives a g_3 value whose lattice again has an n cycle. Our theorems have also given us a clear relationship between the cycles generated by the different g_3 values. Also note that we are talking about a specific type of n-cycle in Theorem 7.8. Our next theorem deals with all other cycles of even length.

Theorem 7.9. *Suppose $\{z_j\}_{j=1}^{m}$ is a cycle of even length m under $\wp'_\Omega$ and does not have the form $\{(-1)^{j+1}z_{j(\mathrm{mod}\ n)}\}_{j=1}^{2n}$ with n odd. If $k = e^{i\pi/4}$, then $\{(-1)^{j+1}kz_j\}_{j=1}^{m}$*

is a cycle of length m under $\wp'_{k\Omega}$. Further, the classification of the m-cycle under $\wp'_{k\Omega}$ is the same as the classification of the m-cycle under $\wp'_{\Omega}$.

Proof. Using Proposition 4.1, we know that

$$\wp'_{k\Omega}(kz_j) = -kz_{j+1} \quad \text{and} \quad \wp'_{k\Omega}(-kz_j) = kz_{j+1}.$$

Thus, under $\wp'_{k\Omega}$,

$$kz_1 \to -kz_2 \to \cdots \to kz_{m-1} \to -kz_m \to kz_1.$$

We know that $kz_1 \neq kz_j$, so to ensure that $\{(-1)^{j+1}kz_j\}_{j=1}^m$ is a cycle of length m under $\wp'_{k\Omega}$, we must check that $kz_1 \neq -kz_j$ for j even. Assume not, so that $z_1 = -z_j$ for some even $2 \leq j \leq m$; note that $j - 1$ is odd. Then $\wp'_{\Omega}(z_{j-1}) = -z_1$, and our original cycle has the form $\{z_1, \ldots, z_{j-1}, -z_1, \ldots, -z_{j-1}\}$ and has length $2(j-1)$. If m is not divisible by an odd number, the contradiction is immediate. On the other hand, if m is divisible by an odd number, then our cycle has the form $\{(-1)^{j+1}z_{j\,(\mathrm{mod}\,n)}\}_{j=1}^{2n}$ with n odd, which contradicts our assumption.

To show that $\left|[(\wp'_{\Omega})^m]'(z_1)\right| = \left|[(\wp'_{k\Omega})^m]'(kz_1)\right|$, we use that

$$(\wp'_{k\Omega})^n(kz_1) = (-1)^n k\wp'_{\Omega}(z_1) \quad \text{and} \quad \wp''_{k\Omega}((-1)^n kz) = -\wp''_{\Omega}(z)$$

for any integer n. $\hfill\square$

Theorem 7.9 shows that if we begin with a g_3 value that gives a cycle of even length m that does not have the specific form given in Theorem 7.8, then $e^{i\pi/2}g_3$ again gives us an m-cycle. That is, unless an even cycle has a certain form, it remains the same length when g_3-space is rotated by $e^{i\pi/2}$.

We note the appearance of Mandelbrot-like sets in g_3 parameter space in the sense introduced in [Douady and Hubbard 1985; McMullen 2000] and extended to quadratic-like Weierstrass elliptic functions in [Hawkins and Look 2006]. We do not present any results here; they are a further subject of study by the authors.

References

[Baker et al. 1991a] I. N. Baker, J. Kotus, and L. Yinian, "Iterates of meromorphic functions, I", *Ergodic Theory Dynam. Systems* **11**:2 (1991), 241–248. MR 92m:58113 Zbl 0711.30024

[Baker et al. 1991b] I. N. Baker, J. Kotus, and L. Yinian, "Iterates of meromorphic functions, III: Preperiodic domains", *Ergodic Theory and Dynamical Systems* **11**:04 (1991), 603–618. Zbl 0774.30023

[Baker et al. 1992] I. N. Baker, J. Kotus, and L. Yinian, "Iterates of meromorphic functions, IV: Critically finite functions", *Results Math.* **22**:3-4 (1992), 651–656. MR 94c:58166 Zbl 0774.30024

[Bergweiler 1993] W. Bergweiler, "Iteration of meromorphic functions", *Bull. Amer. Math. Soc. (N.S.)* **29**:2 (1993), 151–188. MR 94c:30033 Zbl 0791.30018

[Devaney and Keen 1988] R. L. Devaney and L. Keen, "Dynamics of tangent", pp. 105–111 in *Dynamical systems* (College Park, MD, 1986–87), Lecture Notes in Math. **1342**, Springer, Berlin, 1988. MR 90e:58093 Zbl 0662.30019

[Devaney and Keen 1989] R. L. Devaney and L. Keen, "Dynamics of meromorphic maps: maps with polynomial Schwarzian derivative", *Ann. Sci. École Norm. Sup.* (4) **22**:1 (1989), 55–79. MR 90e:58071 Zbl 0666.30017

[Douady and Hubbard 1985] A. Douady and J. H. Hubbard, "On the dynamics of polynomial-like mappings", *Ann. Sci. École Norm. Sup.* (4) **18**:2 (1985), 287–343. MR 87f:58083 Zbl 0587.30028

[Du Val 1973] P. Du Val, *Elliptic functions and elliptic curves*, London Math. Soc. Lecture Note Ser. **9**, Cambridge University Press, London, 1973. MR 52 #417 Zbl 0261.33001

[Erëmenko and Lyubich 1992] A. È. Erëmenko and M. Y. Lyubich, "Dynamical properties of some classes of entire functions", *Ann. Inst. Fourier* (*Grenoble*) **42**:4 (1992), 989–1020. MR 93k:30034 Zbl 0735.58031

[Fatou 1919] P. Fatou, "Sur les équations fonctionnelles (premier mémoire)", *Bull. Soc. Math. France* **47** (1919), 161–271. MR 1504787 JFM 47.0921.02

[Fatou 1920a] P. Fatou, "Sur les équations fonctionnelles (deuxième mémoire)", *Bull. Soc. Math. France* **48** (1920), 33–94. MR 1504792 JFM 47.0921.02

[Fatou 1920b] P. Fatou, "Sur les équations fonctionnelles (troisième mémoire)", *Bull. Soc. Math. France* **48** (1920), 208–314. MR 1504797 JFM 47.0921.02

[Fatou 1926] P. Fatou, "Sur l'itération des fonctions transcendantes Entières", *Acta Math.* **47**:4 (1926), 337–370. MR MR1555220

[Hawkins 2006] J. Hawkins, "Smooth Julia sets of elliptic functions for square rhombic lattices", *Topology Proc.* **30**:1 (2006), 265–278. Spring Topology and Dynamical Systems Conference. MR 2007j:37076 Zbl 1132.54021

[Hawkins and Koss 2002] J. Hawkins and L. Koss, "Ergodic properties and Julia sets of Weierstrass elliptic functions", *Monatsh. Math.* **137**:4 (2002), 273–300. MR 2003j:37066 Zbl 1009.37034

[Hawkins and Koss 2004] J. Hawkins and L. Koss, "Parametrized dynamics of the Weierstrass elliptic function", *Conform. Geom. Dyn.* **8** (2004), 1–35. MR 2005b:37089 Zbl 1076.30027

[Hawkins and Koss 2005] J. Hawkins and L. Koss, "Connectivity properties of Julia sets of Weierstrass elliptic functions", *Topology Appl.* **152**:1-2 (2005), 107–137. MR 2007b:37098 Zbl 1074.37029

[Hawkins and Look 2006] J. M. Hawkins and D. M. Look, "Locally Sierpinski Julia sets of Weierstrass elliptic $\wp$ functions", *Internat. J. Bifur. Chaos Appl. Sci. Engrg.* **16**:5 (2006), 1505–1520. MR 2007h:37068

[Julia 1918] G. Julia, "Sur l'itération des fonctions rationelles", *J. Math. Pures Appl.* **4**:7 (1918), 47 – 245.

[Keen and Kotus 1997] L. Keen and J. Kotus, "Dynamics of the family $\lambda \tan z$", *Conform. Geom. Dyn.* **1** (1997), 28–57. MR 98h:58159 Zbl 0884.30019

[Kotus 2006] J. Kotus, "Elliptic functions with critical points eventually mapped onto infinity", *Monatsh. Math.* **149**:2 (2006), 103–117. MR 2007i:37093 Zbl 1104.37033

[Kotus and Urbański 2003] J. Kotus and M. Urbański, "Hausdorff dimension and Hausdorff measures of Julia sets of elliptic functions", *Bull. London Math. Soc.* **35**:2 (2003), 269–275. MR 2003j:37067 Zbl 1023.37027

[Kotus and Urbański 2004] J. Kotus and M. Urbański, "Geometry and ergodic theory of non-recurrent elliptic functions", *J. Anal. Math.* **93** (2004), 35–102. MR 2005j:37065 Zbl 1092.37025

[Mañé et al. 1983] R. Mañé, P. Sad, and D. Sullivan, "On the dynamics of rational maps", *Ann. Sci. École Norm. Sup.* (4) **16**:2 (1983), 193–217. MR 85j:58089 Zbl 0524.58025

[McMullen 2000] C. T. McMullen, "The Mandelbrot set is universal", pp. 1–17 in *The Mandelbrot set, theme and variations*, edited by Tan L., London Math. Soc. Lecture Note Ser. **274**, Cambridge Univ. Press, Cambridge, 2000. MR 2002f:37081 Zbl 1062.37042

[Milne-Thomson 1950] L. M. Milne-Thomson, *Jacobian elliptic function tables*, Dover, New York, 1950. MR 19,464d Zbl 0041.44702

jgoldsmi@jhsph.edu   *Johns Hopkins Department of Biostatistics, 615 N. Wolfe Street E3037, Baltimore, MD 21205, United States*

koss@dickinson.edu   *Department of Mathematics and Computer Science, Dickinson College, P.O. Box 1773, Carlisle, PA 17013, United States*

Maximum minimal rankings of oriented trees

Sarah Novotny, Juan Ortiz and Darren Narayan

(Communicated by Vadim Ponomarenko)

Given a graph G, a k-ranking is a labeling of the vertices using k labels so that every path between two vertices with the same label contains a vertex with a larger label. A k-ranking f is *minimal* if for all $v \in V(G)$ we have $f(v) \leq g(v)$ for all rankings g. We explore this problem for directed graphs. Here every directed path between two vertices with the same label contains a vertex with a larger label. The *rank* number of a digraph D is the smallest k such that D has a minimal k-ranking. The *arank* number of a digraph is the largest k such that D has a minimal k-ranking. We present new results involving rank numbers and arank numbers of directed graphs. In 1999, Kratochvíl and Tuza showed that the rank number of an oriented of a tree is bounded by one greater than the rank number of its longest directed path. We show that the arank analog does not hold. In fact we will show that the arank number of an oriented tree can be made arbitrarily large where the largest directed path has only three vertices.

1. Introduction

A labeling $f : V(G) \rightarrow \{1, 2, \dots, k\}$ is a *k-ranking* of a graph G if, whenever $f(u) = f(v)$, every path joining u and v contains a vertex w such that $f(w) > f(u)$. A k-ranking f is *minimal* if $f(v) \leq g(v)$ for all $v \in V(G)$ and all rankings g. A ranking f has a *drop vertex* x if the labeling defined by $g(v) = f(v)$ when $v \neq x$ and $g(x) < f(x)$ is still a ranking. It was shown in [Jamison 2003; Isaak et al. 2009] that a ranking is minimal if and only if it contains no drop vertices. When the value of k is unimportant, we will refer to a k-ranking simply as a ranking.

Recall that an oriented graph is a directed graph D where for each pair of vertices x, y either (x, y) or (y, x) is an arc in D and D contains no self-loops. We will refer to a path where all of the arcs have the same orientation as a *directed path*. A path where the arcs are alternately oriented (so that each vertex is either a source or a sink) will be referred to as an *antidirected path*. An *undirected path* is simply a path where the edges are not oriented.

We recall that a vertex coloring of a graph is a labeling of the vertices so that no two adjacent vertices receive the same label. Hence a k-ranking is a vertex coloring with an additional condition imposed. Following along the lines of the chromatic number, the *rank number of a graph $\chi_r(G)$* is defined to be the smallest k such that G has a minimal k-ranking. At the other extreme, the *arank number of a digraph $\psi_r(G)$* is defined to be the maximum k such that D has a minimal k-ranking. These rankings are known as *arankings* or *maximum minimal rankings*. We explore rankings and arankings of directed graphs. Here any directed path between two vertices with the same label contains a vertex with a higher label. The rank and arank number of oriented graphs are defined in the same way as they were for undirected graphs.

Early studies involving the rank number for undirected graphs were motivated by its numerous applications including its role in the design of very large scale integration (VLSI) layout and Cholesky factorizations associated with parallel processing [de la Torre et al. 1992; Ghoshal et al. 1999; Sen et al. 1992]. One of the first results involving minimal rankings was by Bodlaender et al. [1998], who determined the rank number of a path of length n to be

$$\chi_r(P_n) = \lfloor \log_2 n \rfloor + 1.$$

A ranking of this form can be obtained by labeling the vertices $\{v_i \mid 1 \le i \le n\}$ with $\alpha + 1$ where 2^α is the highest power of 2 dividing i and this ranking is unique when n is a power of 2. We will refer to this ranking as the *standard ranking of a path*.

Many papers have since appeared on rankings of undirected graphs [Dereniowski 2006; 2004; Dereniowski and Nadolski 2006; Flórez and Narayan 2009; Ghoshal et al. 1999; 1996; Hsieh 2002; Jamison 2003; Kostyuk and Narayan $\ge$ 2009; Kostyuk et al. 2006; Leiserson 1980; Laskar and Pillone 2001; 2000; Novotny et al. 2009]. However only two papers are known to have investigated the ranking of oriented graphs, and to date there have not been any papers on the arank number of an oriented graph. Kratochvíl and Tuza [1999] gave a general bound on the ranking number of oriented trees. They also proved that deciding whether the rank number of an oriented graph is bounded by a constant is NP-complete. Flórez and Narayan [2009] established new results involving the rank number for all orientations of a cycle. In this paper, we build upon known results for oriented graphs and present the first results involving oriented graphs and arank numbers.

Kratochvíl and Tuza [1999] showed that the rank number of an oriented tree is bounded by one plus the rank number of its longest directed path. In Theorem 10 we show that this property does not hold for the arank number. In fact we will show that the arank number of an oriented tree can be made arbitrarily large where the longest directed path has three vertices.

2. Rankings for oriented graphs

In this section we begin by determining the rank and arank numbers for orientations of stars. Later we investigate orientations of a tree.

2.1. *Oriented stars.* The next two theorems give the rank and arank number of an oriented star. We show that for oriented stars on two or more vertices, the rank number is 2 and the arank number is either 2 or 3.

Theorem 1. *Let $DS(n)$ be a digraph that is any orientation of a star. Then*

$$\chi_r(DS(n)) = 2.$$

Proof. A minimal 2-ranking can be formed by labeling the center vertex with a 2 and all other vertices with a 1. □

Theorem 2. *Let $DS^+(n)$ denote a directed out-star, $DS^-(n)$ a directed in-star, and $DS^H(n)$ the directed hybrid star that contains a directed P_3. Then*

(i) $\psi_r(DS^+(n)) = 2$,

(ii) $\psi_r(DS^-(n)) = 2$,

(iii) $\psi_r(DS^H(n)) = 3$.

Proof. We consider the digraphs $DS^+(n)$ and $DS^-(n)$. There are only two possible rankings. First, if the center of the star is labeled 1, each vertex of degree 1 must be labeled 2, leading to the following minimal 2-rankings:
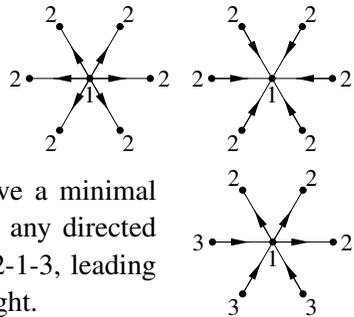
Next we consider $DS^H(n)$. Suppose we have a minimal ranking with the center vertex labeled 1. Then any directed path with labels a-1-b could be relabeled with 2-1-3, leading to a minimal 3-ranking such as the one on the right.

Hence any minimal k-ranking of $DS^H(n)$ must have $k \le 3$. □

2.2. *Oriented paths.* We begin by recalling a theorem of [Bodlaender et al. 1998] that gives the rank number of an undirected path.

Theorem 3. $\chi_r(P_n) = \lfloor \log_2 n \rfloor + 1$.

The directed case the follows immediately.

Corollary 4. *Let $\vec{P}_n$ denote the path on n vertices where all of the arcs have the same direction. Then $\chi_r(\vec{P}_n) = \lfloor \log_2 n \rfloor + 1$.*

Recall that the antidirected path AP_n is a path on vertices $v_1, v_2, \ldots, v_n$ where the arcs alternate in direction.

Theorem 5. *Let AP_n be the antidirected path on n vertices. Then $\chi_r(AP_n) = 2$.*

Proof. Each vertex of an antidirected path is either a source or a sink. Labeling each source with a 1 and each sink with a 2 creates a minimal ranking. $\square$

We restate a known result involving the rank number of an oriented path.

Theorem 6 [Kratochvíl and Tuza 1999]. *Let P_l be the longest directed path contained in the orientation of a path OP_n. Then $\chi_r(OP_n) = \chi_r(P_l)$ or $\chi_r(P_l) + 1$.*

We next consider the arank number of an oriented path. For some oriented paths we may simply join together two ψ_r-rankings on the directed subpaths. Consider the example $\overset{3}{\bullet}\!\!\rightarrow\!\!\overset{1}{\bullet}\!\!\rightarrow\!\!\overset{2}{\bullet}\!\!\leftarrow\!\!\overset{1}{\bullet}$. The first three vertices are labeled according to a ψ_r-ranking of a directed P_3 and the last two vertices are labeled according to a ψ_r-ranking of P_2. Note that there is an overlap on the vertex of the third label. Since none of these labels can be reduced the arank number of this oriented path is at least 3. A 4-ranking would imply that each vertex receives a different label. In either case the label of the end vertex not adjacent to a vertex labeled 1 can be reduced to a 1. Hence the rank number is 3 which equals the arank number of its longest directed path.

Next consider $\overset{1}{\bullet}\!\!\rightarrow\!\!\overset{2}{\bullet}\!\!\leftarrow\!\!\overset{3}{\bullet}\!\!\rightarrow\!\!\overset{1}{\bullet}$. The arank number is at least 3 since no label can be reduced. However the arank number of its longest directed path is 2. It would seem that the difference between the arank number of an oriented path and the arank number of its longest directed path can differ by at most 1. This is in fact the case. Before proving this result we state the following lemma.

Lemma 7. *Let P_n be a path on vertices $v_1, v_2, \ldots, v_n$. Then there exists a ψ_r-ranking f of P_n where $f(v_1) = \psi_r(P_n) + 1$.*

Proof. We first find the largest value less than or equal to m that is either one less than a power of 2, or one less than the average of two consecutive powers of 2. A construction was given in [Kostyuk et al. 2006] showing that ψ_r-rankings can be constructed for paths with these lengths where the endpoints receive the largest two labels. We can construct a ranking for P_n by starting with the endpoint with the largest label and extending the other end of the path, labeling additional vertices so that the new vertex i is labeled $\alpha + 1$ where 2^α is the largest power of 2 that divides i.

By the monotonicity property $\psi_r(P_s) \le \psi_r(P_t)$ whenever $s \le t$ mentioned in [Ghoshal et al. 1996] it follows that this ranking is a ψ_r-ranking. $\square$

We next prove the main result of this section.

Theorem 8. *Let OP_n be an orientation of a path with longest directed path P_l. Then $\psi_r(OP_n) = \psi_r(P_l)$ or $\psi_r(P_l) + 1$.*

Proof. Let OP_n be the union of oppositely directed paths $P_{i_1}, P_{i_2}, \ldots, P_{i_j}$. We will proceed by induction on j. When $j = 1$ the result is immediate. We assume the

result is true for $j - 1$. There are two cases to consider depending on whether or not the P_{i_j} has the largest arank number of all paths in OP_n.

Case (i): $\psi_r(P_{i_j}) \geq \psi_r(P_{i_k})$ for all k, $1 \leq k \leq j$. Then by Lemma 7 the vertices of P_{i_j} can be labeled using a ψ_r-ranking where the largest label is given either to the first or last vertex of this path. We may need to use a larger label for this vertex; however, any larger label for this vertex can be reduced to at most $\psi_r(P_{i_j}) + 1$. We may have to reduce other labels to obtain a minimal ranking, but since these reductions will not increase the largest label we have $\psi_r(OP_n) \leq \psi_r(P_l) + 1$.

Case (ii): $\psi_r(P_{i_j}) < \max_k \psi_r(P_{i_k})$ for all k, $1 \leq k \leq j$. We append a ψ_r-ranking of P_{i_j} as in Case (i). Since the largest label did not increase we again have $\psi_r(OP_n) \leq \psi_r(P_l) + 1$. □

3. Arankings for oriented trees

We recall the following theorem involving the rank number of an oriented tree.

Theorem 9 [Kratochvíl and Tuza 1999]. *Let P_l be the longest directed path contained in the orientation of a tree T_n. Then $\chi_r(T_n) = \chi_r(P_l)$ or $\chi_r(P_l) + 1$.*

Our next theorem shows that the analog does not hold for the arank number of a directed path. In fact we will show that the arank number of an oriented tree can be made arbitrarily large where the longest directed path has only three vertices.

Theorem 10. *For any positive integer t, there exists a directed tree T without a directed P_3 such that $\psi_r(D) = t$.*

Proof. When $t = 1$, D consists of a single vertex with no edges. When $t = 2$, D is a directed K_2.

For the case where $t = 3$, the minimal 3-ranking shows that $\psi_r(D) \geq 3$.

This same digraph can be extended to one with a minimal 4-ranking as follows:
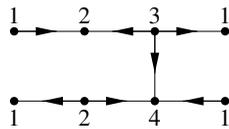
We now give a general extension from the case where $t = j$ to the case where $t = j + 1$.

Suppose $t = j$. We start with the digraph D which contains a vertex v such that $f(v) = j$. Let D' be a copy of the digraph D, with the orientation of all of the arcs in D' reversed. We note that the digraph D' contains a vertex v' such that $f(v') = j$. We then construct the graph D^* from D, D' along with an arc between v and v', where the direction is from the source to the sink. In D^* we let $f(v') = j + 1$, and

label all other vertices as they were in D or D'. The construction gives a minimal $(j+1)$-ranking of D^*. Hence $\psi_r(D^*) \geq j+1$. $\square$

4. Conclusion

At the current time, the rank and arank number are only known for a few families of graphs. Even less is known about these numbers for oriented graphs. We note that Theorem 8 suggests the problem of partitioning oriented paths into two classes. Class 1 contains all oriented paths OP_n where $\psi_r(OP_n) = \psi_r(P_l)$ and Class 2 contains of all paths where $\psi_r(OP_n) = \psi_r(P_l) + 1$.

Acknowledgments

References

[Bodlaender et al. 1998] H. L. Bodlaender, J. S. Deogun, K. Jansen, T. Kloks, D. Kratsch, H. Müller, and Z. Tuza, "Rankings of graphs", *SIAM J. Discrete Math.* **11**:1 (1998), 168–181. MR 99b:68143 Zbl 0907.68137

[Dereniowski 2004] D. Dereniowski, "Rank coloring of graphs", pp. 79–93 in *Graph colorings*, edited by M. Kubale, Contemp. Math. **352**, Amer. Math. Soc., Providence, RI, 2004. MR 2076991

[Dereniowski 2006] D. Dereniowski, *Parallel scheduling by graph ranking*, Ph.D. thesis, PG WETI, Gdańsk, 2006.

[Dereniowski and Nadolski 2006] D. Dereniowski and A. Nadolski, "Vertex rankings of chordal graphs and weighted trees", *Inform. Process. Lett.* **98**:3 (2006), 96–100. MR 2006j:68032

[Flórez and Narayan 2009] R. Flórez and D. A. Narayan, "An optimal ranking characterization of oriented paths and cycles", 2009. Submitted for publication.

[Ghoshal et al. 1996] J. Ghoshal, R. Laskar, and D. Pillone, "Minimal rankings", *Networks* **28**:1 (1996), 45–53. MR 97e:05110 Zbl 0863.05071

[Ghoshal et al. 1999] J. Ghoshal, R. Laskar, and D. Pillone, "Further results on minimal rankings", *Ars Combin.* **52** (1999), 181–198. MR 2000f:05036 Zbl 0977.05048

[Hsieh 2002] S.-y. Hsieh, "On vertex ranking of a starlike graph", *Inform. Process. Lett.* **82**:3 (2002), 131–135. MR 2002k:05085 Zbl 1013.68141

[Isaak et al. 2009] G. Isaak, R. Jamison, and D. A. Narayan, "Greedy rankings and the arank number", *Information Processing Letters* **109**:15 (2009), 825–827.

[Jamison 2003] R. E. Jamison, "Coloring parameters associated with rankings of graphs", *Congr. Numer.* **164** (2003), 111–127. MR 2005d:05129 Zbl 1043.05049

[Kostyuk and Narayan ≥ 2009] V. Kostyuk and D. A. Narayan, "Maximum minimal rankings of cycles", *Ars Combinatoria*. To appear.

[Kostyuk et al. 2006] V. Kostyuk, D. A. Narayan, and V. A. Williams, "Minimal rankings and the arank number of a path", *Discrete Math.* **306**:16 (2006), 1991–1996. MR 2007b:05094 Zbl 1101.05040

[Kratochvíl and Tuza 1999] J. Kratochvíl and Z. Tuza, "Rankings of directed graphs", *SIAM J. Discrete Math.* **12**:3 (1999), 374–384. MR 2000e:05063 Zbl 0932.05032

[Laskar and Pillone 2000] R. Laskar and D. Pillone, "Theoretical and complexity results for minimal rankings", *J. Combin. Inform. System Sci.* **25**:1-4 (2000), 17–33. MR 2001m:05244

[Laskar and Pillone 2001] R. Laskar and D. Pillone, "Extremal results in rankings", *Congr. Numer.* **149** (2001), 33–54. MR 2002m:05173 Zbl 0989.05058

[Leiserson 1980] C. E. Leiserson, "Area efficient graph layouts for VLSI", pp. 270–281 in *Proc. 21st Ann. IEEE Symposium FOCS*, 1980.

[Novotny et al. 2009] S. Novotny, J. Ortiz, and D. A. Narayan, "Minimal k-rankings and the rank number of P_n^2", *Inform. Process. Lett.* **109**:3 (2009), 193–198. MR 2485087

[Sen et al. 1992] A. Sen, H. Deng, and S. Guha, "On a graph partition problem with application to VLSI layout", *Inform. Process. Lett.* **43**:2 (1992), 87–94. MR 1187395 Zbl 0764.68132

[de la Torre et al. 1992] P. de la Torre, R. Greenlaw, and T. Przytycka, "Optimal tree ranking is in NC", *Parallel Processing Letters* **2**:1 (1992), 31–41.

snovotny@math.jhu.edu   *Department of Mathematics, The Johns Hopkins University, Baltimore, MD 21218, United States*

jpo208@lehigh.edu   *Department of Mathematics, Lehigh University, Bethlehem, PA 18015, United States*

dansma@rit.edu   *Rochester Institute of Technology, School of Mathematical Sciences, 85 Lomb Memorial Drive, Rochester, NY 14623-5604, United States*
                             http://people.rit.edu/~dansma/

Applications of full covers in real analysis

Karen Zangara and John Marafino

(Communicated by David Larson)

In this paper we briefly introduce the reader to the concept of full covers and indicate how it can be used to prove theorems in an undergraduate analysis course. The technique exposes the student to the idea of covering an interval $[a, b]$ with a collection of sets and then extracting from this collection a subcollection that *partitions* $[a, b]$. As a consequence, the student is furnished with a unifying thread that ties together and simplifies the proofs of many theorems.

1. Introduction

We were first drawn to the concept of full covers after reading two papers by Botsko [1987; 1989]. We then pursued this idea in [Klaimon 1990] and will now provide full covering arguments for four more theorems: the Lebesgue Number Lemma, the Intermediate Value Theorem for Derivatives, Baire's Theorem, and Ascoli's Theorem.

The following definition and lemma are used in full covering arguments:

Definition. Let $[a, b]$ be a closed, bounded interval. A collection C of closed subintervals of $[a, b]$ is a *full cover* of $[a, b]$ if, for each x in $[a, b]$, there corresponds a number $\delta > 0$ such that every closed subinterval of $[a, b]$ that contains x and has length less than δ belongs to C.

Thomson's Lemma. *If C is a full cover of $[a, b]$, then C contains a partition of $[a, b]$. In other words, there is a partition of $[a, b]$ all of whose subintervals belong to C.*

The proof of the lemma is based upon a bisection argument and is easily accessible to undergraduates. It can be found in [Botsko 1987], [Botsko 1989] and [Thomson 1980]. Thomson's lemma is similar in concept and execution to the version of the Heine–Borel theorem, which states that every open cover of a closed

interval has a finite subcover. So the proof of any theorem that uses the Heine–Borel theorem can be rewritten to use full covers. Our proof of the Lebesgue Number Lemma illustrates this.

The advantage of full covering arguments lies in that the resulting finite subcover of $[a, b]$ is a *partition* of the interval. This extra condition can often be used to streamline and simplify the proofs of certain theorems. For instance, in the proof of the Intermediate Value Theorem for derivatives, we obtain a finite subcover $\{J_k : k = 1, 2, \ldots, m\}$ of $[a, b]$ having the property that a function f defined on $[a, b]$ has a constant sign on each J_k. Since $\{J_k : k = 1, 2, \ldots, m\}$ is a partition of closed subintervals of $[a, b]$, we can order the J_k so that J_k abuts J_{k+1} to the left, J_1 contains a, and J_m contains b. It is then trivial to see that the sign of f on J_1 determines the sign of f on each of the $J_k, k = 2, 3, \ldots, m$, and hence, determines the sign of f on $[a, b]$.

Another instance occurs in Baire's Theorem. In the proof we have a function f defined on $[a, b]$ and a finite subcollection $\{J_k : k = 1, 2, \ldots, m\}$ such that f is bounded above on each J_k by a constant function Φ_k. Since $\{J_k : k = 1, 2, \ldots, m\}$ forms a partition of $[a, b]$, the intervals can easily be ordered as before. Trivially, the interiors of J_k do not intersect, so each interior point of J_k can be associated with only one Φ_k value. By moving from left to right on $[a, b]$, we then indicate a well defined procedure that connects the graphs of each Φ_k and defines a continuous function h_ε on $[a, b]$. Finally, the full covering argument offers a very efficient iterative method for proving Ascoli's Theorem.

We close this section by listing those theorems that have been proved using this technique and that a student would normally encounter in an undergraduate analysis course. We categorize them under four main topics and give a reference for their proof.

Topology:

Heine–Borel Theorem [Botsko 1987, p. 452]. *Any open cover of $[a, b]$ has a finite subcover.*

Bolzano–Weierstrass Theorem [Botsko 1987, p. 452]. *If S is a bounded infinite set of real numbers, then S has an accumulation point.*

Continuity and differentiability:

Theorem [Botsko 1987, p. 451]. *If f is continuous on $[a, b]$, then f is bounded on $[a, b]$.*

Theorem [Klaimon 1990, p. 156]. *If f is a continuous function on $[a, b]$, there exists points M and m on $[a, b]$ such that $f(M) \geq f(x)$ and $f(m) \leq f(x)$ for all x on $[a, b]$.*

Theorem [Botsko 1987, p. 452]. *If f is continuous on $[a, b]$, then f is uniformly continuous on $[a, b]$.*

Intermediate Value Theorem [Botsko 1987, p. 451]. *If f is continuous on $[a, b]$ with $f(a)f(b) < 0$, then there exists x_0 on (a, b) such that $f(x_0) = 0$.*

Remark. The same cover employed to prove this theorem will be used below to prove the Intermediate Value Theorem for derivatives.

Theorem [Botsko 1989, p. 331; Klaimon 1990, p. 158]. *If $f'(x) = 0$ for all x on $[a, b]$, then f is constant on $[a, b]$.*

Theorem [Klaimon 1990, p. 160]. *If $f'(x) > 0 \ (< 0)$ on (a, b), then f is increasing (decreasing) on (a, b).*

Remark. The proofs of these two theorems do not use the Mean Value Theorem as is typically done.

Rolle's Theorem [Klaimon 1990, p. 157]. *If f is continuous on $[a, b]$ and differentiable on (a, b), and $f(a) = f(b)$, there exists a point x_0 on (a, b) such that $f'(x_0) = 0$.*

Integration:

Theorem [Botsko 1989, p. 330]. *If f is continuous on $[a, b]$, then f is Riemann integrable.*

Theorem [Botsko 1989, p. 331]. *If f is bounded on $[a, b]$ and continuous almost everywhere, then f is Riemann integrable on $[a, b]$.*

Remark. By slightly modifying the cover in the first theorem, Botsko is able to prove the stronger second theorem! This also works with other results, as pointed out in [Botsko 1989].

Sequences:

Dini's Theorem [Klaimon 1990, p. 159]. *If $f_n(x)$ is a sequence of continuous functions on $[a, b]$ and $f_n(x) < f_{n+1}(x)$ for all n and for all x in $[a, b]$, and if $f_n(x)$ converges to $f(x)$ where $f(x)$ is continuous on $[a, b]$, then $f_n(x)$ converges uniformly to $f(x)$.*

2. Four theorems proven using full covers

Lebesgue Number Lemma. *Let $\Im$ be an open cover of $[a, b]$. There exists a number $\eta > 0$ such that if B is any subset of $[a, b]$ with diameter $B < \eta$, then there exists a set $A \in \Im$ such that $A \supseteq B$.*

Proof. For each x in $[a, b]$ and $\varepsilon > 0$, set $I_\varepsilon[x] = [x - \varepsilon, x + \varepsilon]$. Let

$$C = \{I_\varepsilon[x] : I_\varepsilon[x] \subset [a, b] \text{ and } I_{2\varepsilon}[x] \text{ is a subset of some } A \in \mathfrak{I}\}.$$

We first show that C is a full cover of $[a, b]$. Let x be an element of $[a, b]$. Since $\mathfrak{I}$ is an open cover of $[a, b]$, there exists an A in $\mathfrak{I}$ that contains x. Because A is open, one can find a $\delta = \delta(x)$ such that $I_{2\delta}[x]$ is a subset of A. Let J be a closed subinterval of $[a, b]$ containing x such that $|J| < \delta$. We can write J as $I_\varepsilon[x']$, where x' is the midpoint of J and $\varepsilon = \delta/2$. Since $I_{2\varepsilon}[x']$ is a subset of A, J is in C and so C is a full cover of $[a, b]$.

By Thomson's Lemma, C contains a partition of $[a, b]$; that is, there exists $a = p_0 < p_1 < \cdots < p_m = b$ such that $[p_{k-1}, p_k] = I_{\varepsilon(k)}[x_k]$ is in C for $k = 1, 2, \ldots, m$. Note that $x_k = (p_k + p_{k-1})/2$ and $\varepsilon(k) = |p_{k-1} - p_k|/2$.

Let $\eta = \min\{\varepsilon(k)\}$ and let B be a subset of $[a, b]$ with diameter $B < \eta$. B intersects $I_{\varepsilon(k)}[x_k]$ for some $k = 1, \ldots, m$ and hence B is a subset of $I_{2\varepsilon(k)}[x_k]$, which is contained in some $A \in \mathfrak{I}$. $\square$

Intermediate Value Theorem for derivatives. *If $f(x)$ is the derivative for some function $g(x)$ on an open interval containing $[a, b]$, and if $f(a)f(b) < 0$, then there exists an x_0 in (a, b) such that $f(x_0) = 0$.*

Proof. Suppose to the contrary that for all x on (a, b), $f(x) \neq 0$. Then $f(x) \neq 0$ on $[a, b]$. Let

$$C = \{I : I \text{ is a closed subinterval of } [a, b] \text{ and } f(x) \text{ has one sign on } I\}.$$

Let x be in $[a, b]$. Assume for definiteness that $f(x) > 0$. We claim that there exists a δ neighborhood about x such that $f(y) > 0$ for all y in this neighborhood. Suppose the claim is false. Then one can find a sequence $\{y_n\}$, where $y_n \to x$ as $n \to \infty$ and $f(y_n) < 0$. Again, for definiteness, suppose $\{y_n\}$ approaches x from the left. Since $f(x) > 0$, there exists a δ_1 such that when $|h| < \delta_1$, $g(x + h) < g(x)$ if $h < 0$. By choosing n large enough, one can find y_n such that $|y_n - x| < \delta_1$ and so $g(y_n) < g(x)$. Since $f(y_n) < 0$, there exists a δ_2 neighborhood about y_n that is contained in the δ_1 neighborhood about x such that if $|h| < \delta_2$ and $h < 0$, then $g(y_n) < g(y_n + h)$. Choose $|h'| < \delta_2$ and $h' < 0$. Then $y_n + h' < y_n < x$ and $g(y_n) < g(y_n + h') < g(x)$. By the Intermediate Value Theorem for Continuous Functions, there exists an x_n in $[y_n, x]$ such that $g(x_n) = g(y_n + h')$. Using Rolle's Theorem on $[y_n + h', x_n]$ one can find an x_0 in $[y_n + h', x_n]$ such that $f(x_0) = 0$. This contradicts our assumption that $f(x) \neq 0$ for all x in $[a, b]$. So there must be a $\delta > 0$ such that $f(y) > 0$ for all y satisfying $|y - x| < \delta$. Let J be a closed interval containing x with $|J| < \delta$. Then J is in C. A similar δ can be found if $f(x) < 0$. Thus C is a full cover of $[a, b]$.

Using Thomson's Lemma, C contains a partition of $[a, b]$; that is, there exist $a = p_0 < p_1 < \cdots < p_m = b$ such that $[p_{k-1}, p_k] = I_k$ is in C for $k = 1, 2, \ldots, m$. Suppose $f(x) > 0$ on I_1. Since the intervals overlap at the endpoints, we have $f(x) > 0$ on I_k for $k = 2, \ldots, m$. But this contradicts our assumption $f(a) f(b) < 0$. The same contradiction results if $f(x) < 0$ on I_1. So our original assumption that $f(x) \neq 0$ on (a, b) is false. Consequently, there exists a point x_0 on (a, b) such that $f(x_0) = 0$. $\square$

Next, we present the proofs of two sequence theorems. For these theorems we will need the following definitions. The function f is upper (lower) semi-continuous at x if $\limsup_{y \to x} f(y) \leq f(x)$ ($\liminf_{y \to x} f(y) \geq f(x)$). If f is upper (lower) semi-continuous for all x on $[a, b]$, then f is upper (lower) semi-continuous on $[a, b]$. The family of functions Ω is equicontinuous on $[a, b]$ if for each x in $[a, b]$ and $\varepsilon > 0$, there exists a $\delta = \delta(x, \varepsilon)$ such that if $|y - x| < \delta$, then $|f(y) - f(x)| < \varepsilon$ for all f in Ω. The family of functions Ω is uniformly bounded on $[a, b]$ provided there exists a constant $M > 0$ such that $|f(x)| < M$ for all $x \in [a, b]$ and for all $f \in \Omega$.

Baire's Theorem. *Let f be upper (lower) semi-continuous on $[a, b]$ and bounded above (below) by M on $[a, b]$. Then there exists a sequence of continuous functions $\{h_n\}$ such that, for all x in $[a, b]$,*

(i) $M \geq h_1(x) \geq \cdots \geq h_n(x) \geq \cdots$ ($M \leq h_1(x) \leq \cdots \leq h_n, (x) \leq \cdots$),

(ii) $\lim_{n \to \infty} h_n(x) = f(x)$.

Proof. Let M be the upper bound of $f(x)$ on $[a, b]$ and let ε be an arbitrarily small positive number.

Define

$$C = \Big\{ J : J \text{ is a closed subinterval of } [a, b], \ |J| < \varepsilon, \text{ and there exists } x \text{ in } J$$
$$\text{such that } f(y) \leq f(x) + \varepsilon \text{ for all } y \text{ in } J \Big\}.$$

Let x be an element in $[a, b]$. Since f is upper semi-continuous at x, there is a $\delta(x) > 0$ such that $|y - x| < \delta(x)$ implies $f(y) \leq f(x) + \varepsilon$. We can further assume that $\delta(x) < \varepsilon$. Now let J be any closed interval of $[a, b]$ containing x with $|J| < \delta(x)$. If we set $\Phi(y) = f(x) + \varepsilon$ for all $y \in J$, then $f(y) < \Phi(y)$ on J. Thus J is in C and C is a full cover of $[a, b]$.

By Thomson's Lemma there exists a partition $\{J_k, k = 1, 2, \ldots m\}$ of $[a, b]$ contained in C. Hence, $|J_k| < \varepsilon$ and on each $J_k, k = 1, 2, \ldots, m$, there is a point x_k such that the constant functions $\Phi_k(x) = f(x_k) + \varepsilon$ defined on J_k satisfy $f(x) \leq \Phi_k(x)$ on J_k.

We first construct a function h_ε that will approximate f in a sense to be clarified below. For each $k, k = 1, 2, \ldots, m$, let Φ_k also denote the constant value of $\Phi_k(x)$

on J_k. If $\Phi_1 > \Phi_2$, then connect the horizontal graph of $\Phi_1(x)$ to that of $\Phi_2(x)$ by the line segment P_1P_2 where P_1 coincides with the end point of the graph of $\Phi_1(x)$ and P_2 lies 1/3 of the distance on the graph of $\Phi_2(x)$. If $\Phi_1 < \Phi_2$, then connect the horizontal graphs by the line segment P_1P_2 where P_1 is 2/3 of the distance on the graph of $\Phi_1(x)$ and P_2 coincides with the initial point of the graph of $\Phi_2(x)$. Doing this for $k = 1, 2, \ldots, m$, we can construct a continuous function $h_\varepsilon(x)$ on $[a, b]$ with the property $f(x) \le h_\varepsilon(x)$ for all x on $[a, b]$. We will say that h_ε approximates f in the following sense. Given any $x \in [a, b]$, $x \in J_k$ for some k and either $(x, h_\varepsilon(x))$ will be on a horizontal step of h_ε or it will be on a line segment connecting two consecutive steps. In either case, it is evident that

$$h_\varepsilon(x) \le \sup_{|y-x|<2\varepsilon} f(y) + \varepsilon,$$

since all J_k are of width at most ε.

We now construct the desired sequence $\{h_n\} \downarrow f$. For each n, let $\varepsilon = 1/n$ and let g_n be a function constructed as h_ε was above. Define $h_1 = \inf(g_1, M)$, $h_2 = \inf(g_2, h_1)$, $h_3 = \inf(g_3, h_2)$, and so on. For each x in $[a, b]$, the sequence $\{h_n(x)\}$ converges, since it is decreasing and bounded below by $f(x)$. Moreover, $\lim_{n\to\infty} h_n(x) \ge f(x)$. Since

$$h_n(x) \le \sup_{|y-x|<2/n} f(y) + 1/n,$$

it follows that $\lim_{n\to\infty} h_n(x) \le \limsup_{y\to x} f(y) \le f(x)$ for all x. Hence $\{h_n\} \downarrow f$, as claimed. $\square$

Ascoli's Theorem. *Let Ω be a family of functions uniformly bounded and equicontinuous at every point of a closed interval $[a, b]$. Then every sequence of functions $\{f_n\}$ in Ω contains a subsequence that converges uniformly on $[a, b]$.*

Proof. Consider a family of functions Ω, equicontinuous and uniformly bounded on $[a, b]$. We first establish this claim:

For any sequence $\{g_n\}_{n=1}^\infty \subseteq \Omega$ and positive number ε, there exists a subsequence $\{g_{n(\varepsilon,k)}\}_{k=1}^\infty$ of $\{g_n\}_{n=1}^\infty$ such that $n(\varepsilon, 1) > 1$ and

$$|g_{n(\varepsilon,k)}(y) - g_{n(\varepsilon,i)}(y)| < \varepsilon \text{ for all } y \in [a, b] \text{ and all } k, i. \tag{1}$$

To see this, fix $\varepsilon > 0$ and let

$C = \big\{ J : J$ is a closed subinterval on $[a, b]$ and for any $\{g_n\} \subseteq \Omega$,

there exists a subsequence $\{g_{n(k)}\}$ of $\{g_n\}$ such that $n(1) > 1$

and $|g_{n(k)}(y) - g_{n(i)}(y)| < \varepsilon$ on J for all $k, i \big\}$.

Let x be an element of $[a, b]$. Since Ω is equicontinuous, there exists a $\delta = \delta(x, \varepsilon)$ such that $|f(x) - f(y)| < \varepsilon/3$ for all f in Ω and y such that $|y - x| < \delta$. Let J be a closed interval containing x such that $|J| < \delta$. We must show J is in C; so we begin with any sequence $\{g_n\}$ from Ω. Since $\{g_n(x)\}$ is bounded, it has a subsequence $\{g_{n(s)}(x)\}$, $s = 1, 2, \ldots$, that converges. Convergent sequences are Cauchy sequences, so we can choose $S > 1$ such that $|g_{n(i)}(x) - g_{n(j)}(x)| < \varepsilon/3$ if $i, j > S$. Consider the collection of functions $g_{n(s)}$, $s > S$, on $[a, b]$. Using the triangle inequality, we have $|g_{n(i)}(y) - g_{n(j)}(y)| < \varepsilon$ for all y in J and $i, j > S$. In addition, $n(S + 1) > 1$. We relabel the sequence by writing $s > S$ as $S + k$, $k = 1, 2, \ldots$ and setting $n(k) = n(S + k)$. The sequence $\{g_{n(k)}\}$ now satisfies the conditions defining C. Thus J is in C and C is a full cover of $[a, b]$. Using Thomson's Lemma, we see that C contains a partition $\{J_h, h = 1, 2, \ldots, m\}$ of $[a, b]$.

Let $\{g_n\}$ be any sequence from Ω. Since J_1 is in C, there exists a subsequence $\{g_{n(1,k)}\}$ of $\{g_n\}$ such that for all y on J_1, $|g_{n(1,k)}(y) - g_{n(1,i)}(y)| < \varepsilon$ for all k, i and $n(1, 1) > 1$. Furthermore, $\{g_{n(1,k)}\}$ is a family of equicontinuous functions uniformly bounded on $[a, b]$. Thus, on J_2 there exists a subsequence $\{g_{n(2,k)}\}$ of $\{g_{n(1,k)}\}$ such that for all y in $J_1 \cup J_2$, $|g_{n(2,k)}(y) - g_{n(2,i)}(y)| < \varepsilon$ for all k, i and $n(2, 1) > n(1, 1)$. By continuing this process on each subinterval J_h, for $h = 3, 4, \ldots, m$, we obtain a subsequence $\{g_{n(m,k)}\}$ of $\{g_n\}$ with the properties that $n(m, 1) > 1$ and $|g_{n(m,k)}(y) - g_{n(m,i)}(y)| < \varepsilon$ for all k, i and all y on $[a, b]$. This sequence, with the change in labeling $n(\varepsilon, k) = n(m, k)$, satisfies (1), so the claim is proved.

We are now ready to conclude the proof of our theorem. Let $\{f_n\}$ be any sequence in Ω. Apply the claim with $\{f_n\}$ and 1 in place of $\{g_n\}$ and ε to obtain a subsequence $\{f_{n(1,k)}\}$ of $\{f_n\}$ such that $n(1, 1) > 1$ and $|f_{n(1,k)}(y) - f_{n(1,i)}(y)| < 1$ for all k, i and all y on $[a, b]$. Apply the claim again with $\{f_{n(1,k)}\}$ and $1/2$ in place of $\{g_n\}$ and ε to obtain a subsequence $\{f_{n(2,k)}\}$ of $\{f_{n(1,k)}\}$ with the properties that $n(2, 1) > n(1, 1)$ and $|f_{n(2,k)}(y) - f_{n(2,i)}(y)| < 1/2$ for all k, i and all y on $[a, b]$. Continuing in this manner, construct for each $p = 2, 3, \ldots$ a subsequence $\{f_{n(p,k)}\}$ of $\{f_{n(p-1,k)}\}$ such that $n(p, 1) > n(p - 1, 1)$ and $|f_{n(p,k)}(y) - f_{n(p,i)}(y)| < 1/p$ for all k, i and all y in $[a, b]$.

Now take the subsequence $\{f_{n(p,1)} : p = 1, 2, \ldots\}$ of $\{f_n\}$. If $q > p$ then $f_{n(q,1)}$ is equal to $f_{(p,k)}$ for some $k = 2, 3, \ldots$. Thus, for all y in $[a, b]$,

$$|f_{n(q,1)}(y) - f_{n(p,1)}(y)| = |f_{n(p,k)}(y) - f_{n(p,1)}(y)| < 1/p. \tag{2}$$

This shows that $\{f_{n(p,1)}(y)\}$ is a Cauchy sequence, hence convergent. Let $f(y)$ denote its limit. By letting $q \to \infty$ in (2) we obtain $|f(y) - f_{n(p,1)}(y)| < 1/p$, which implies $\{f_{n(p,1)} : p = 1, 2, \ldots\}$ converges uniformly to f on $[a, b]$. $\square$

3. Conclusion

Because of their wide applicability, full covering arguments should seriously be considered as part of — or a supplement to — any elementary analysis course. In addition, these arguments prepare the student for the more intricate covering-based proofs of approximate and symmetric derivative theorems [Thomson 1980].

References

[Botsko 1987] M. W. Botsko, "A unified treatment of various theorems in elementary analysis", *Amer. Math. Monthly* **94**:5 (1987), 450–452. MR 1541097

[Botsko 1989] M. W. Botsko, "The use of full covers in real analysis", *Amer. Math. Monthly* **96**:4 (1989), 328–333. MR 90d:26001 Zbl 0721.26003

[Klaimon 1990] K. Klaimon, "More applications of full covering", *Pi Mu Epsilon J.* **9**:3 (Fall 1990), 156–161.

[Thomson 1980] B. S. Thomson, "On full covering properties", *Real Anal. Exchange* **6**:1 (1980), 77–93. MR 82c:26008 Zbl 0459.26004

zangark@gmail.com   *Cheiron, One Greentree Centre, Suite 201,*
                            Marlton, NJ 08053, United States

marafijt@jmu.edu   *Department of Mathematics and Statistics,*
                            305 Roop Hall, MSC 1911, James Madison University,
                            Harrisonburg, VA 22807, United States

Numerical evidence on the uniform distribution of power residues for elliptic curves

Jeffrey Hatley and Amanda Hittson

(Communicated by Nigel Boston)

Elliptic curves are fascinating mathematical objects which occupy the intersection of number theory, algebra, and geometry. An elliptic curve is an algebraic variety upon which an abelian group structure can be imposed. By considering the ring of endomorphisms of an elliptic curve, a property called complex multiplication may be defined, which some elliptic curves possess while others do not. Given an elliptic curve E and a prime p, denote by N_p the number of points on E over the finite field $\mathbb{F}_p$. It has been conjectured that given an elliptic curve E without complex multiplication and any modulus M, the primes for which N_p is a square modulo p are uniformly distributed among the residue classes modulo M. This paper offers numerical evidence in support of this conjecture.

1. Introduction

Let $F(x, y) = y^2 - a_1 xy - a_3 y - x^3 - a_2 x^2 + a_4 x - a_6$ where the $a_i \in \mathbb{C}$. Consider the set of points

$$E = \{(x, y) \in \mathbb{C}^2 : F(x, y) = 0\}.$$

We also wish to associate with the set E a special point $\mathbb{O} \in E$, called the *point at infinity*, an idea which is made rigorous by projective geometry and whose existence is justified below. Provided there are no points (x, y) such that

$$\left.\frac{\partial F}{\partial x}\right|_{(x,y)} = \left.\frac{\partial F}{\partial y}\right|_{(x,y)} = 0,$$

we say that F is *nonsingular*, and when F is nonsingular, we call E an *elliptic curve*. Through some substitutions, the equations defining elliptic curves can be put into the form $F(x, y) = y^2 - x^3 - ax - b$ for some $a, b \in \mathbb{C}$, which is called *Weierstrass normal form*.

If one were to graph the real points $(x, y) \in \mathbb{R}^2$ of E, the graph would form an ordinary-looking plane curve which is symmetric about the x-axis:
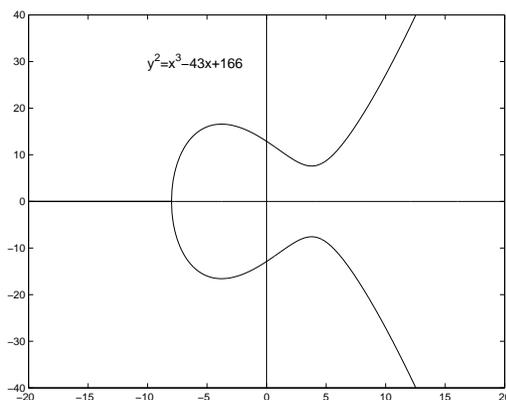
However, elliptic curves are far from ordinary and are the focus of much research due to some remarkable properties they possess. In particular, an addition law can be defined for points on the curve under which the points form an abelian group with identity element $\mathcal{O}$. The addition law can be described in the following geometric way: given two points on the curve, p_1 and p_2, draw the line connecting these two points:
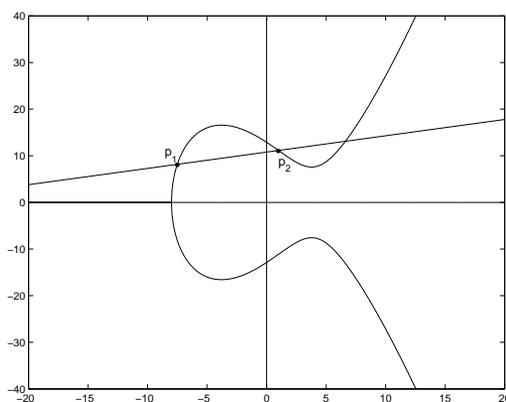
We define $p_3 = p_1 * p_2$ to be the third point of intersection between this line and the curve E. (If $p_1 = p_2$, we take the tangent line to the curve E at that point, which exists since E is nonsingular.)

This third point is guaranteed to exist by the following theorem.

Theorem (Bézout). *Let C and D be two curves in the projective space $\mathbb{CP}_2$ of degrees n and m, respectively, which have no common component (that is, there do not exist curves C_1, D_1, and E of degrees at least 1 such that $C = C_1 \cup E$ and*

$D = D_1 \cup E$). *Then C and D have precisely nm points of intersection counting multiplicities.*

This theorem is about curves in projective space; projective space and its role in the study of elliptic curves is discussed below. For a detailed discussion of projective space, multiplicity, and Bézout's theorem, see [Kirwan 1992].

Bézout's theorem states that two algebraic curves of degrees n and m intersect in exactly nm points (counting multiplicity), provided the curves do not share a common component. Now, the degree of a curve is simply the degree of the homogeneous polynomial defining it. (Homogeneous polynomials are discussed below.) Since E is defined by a polynomial of degree 3, E is of degree 3, and since a line is of degree 1, Bézout's theorem implies that the two curves should intersect in exactly 3 points; hence precisely one such point p_3 is guaranteed to exist. Then $p_1 + p_2$ is defined to be the reflection of p_3 about the x-axis:
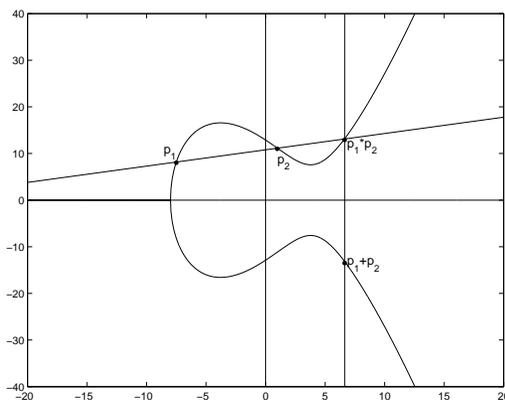
This method of addition is frequently referred to as the *chord and tangent* method. This addition law can be stated succinctly in the following way: three points on E sum to the identity, $\mathbb{O}$, if and only if they are collinear. With this formulation, and the understanding that $\mathbb{O}$ exists "at the top of the y-axis" as discussed below, we see that $p_1 * p_2 = -(p_1 + p_2)$, and the reflection of this point across the y-axis, which we defined to be $p_1 + p_2$, is the third point of E on the line between $p_1 * p_2$ and $\mathbb{O}$.

It is now necessary to consider $\mathbb{O}$, the point at infinity. For our purposes, it suffices to think of $\mathbb{O}$ as the point at which all vertical lines in the $x - y$ plane intersect. Consider the line connecting $p_1 * p_2$ and $p_1 + p_2$. This is a vertical line, and clearly only intersects E twice. However, Bézout's Theorem assures us that there are three points of intersection. In this case, that third point is $\mathbb{O}$.

To make this more rigorous, we consider the homogenized form of the curve E defined by

$$E : F(x, y) = y^2 - x^3 - ax - b.$$

A *homogeneous curve of degree n* defined by an equation in three variables x, y, z is one in which, for every monomial $\alpha x^i y^j z^k$, we have $i+j+k=n$. To homogenize F, we make the substitutions $x = X/Z$ and $y = Y/Z$ and multiply F by Z^3, obtaining the curve

$$\bar{E} : F(X, Y, Z) = Y^2 Z - X^3 - aXZ^2 - bZ^3.$$

Furthermore, we consider the curve in the *complex projective space of degree two*, denoted $\mathbb{CP}_2$, where two 3-tuples $[x, y, z]$ and $[x', y', z']$ in $\mathbb{CP}_2$ are considered equivalent if they differ by a constant multiple; that is, we have the equivalence relation

$$[x, y, z] \sim [x', y', z'] \Longleftrightarrow [x, y, z] = \lambda[x', y', z']$$

for some complex, nonzero constant $\lambda \neq 0$. We do not consider $[0, 0, 0]$ to be an element of $\mathbb{CP}_2$. To summarize, we have

$$\mathbb{CP}_2 = \big\{ [x, y, z] : x, y, z \in \mathbb{C} - \{[0, 0, 0]\} \big\} / \sim .$$

Because of this equivalence, we see that as long as $Z \neq 0$, we may divide by Z and obtain our original curve, since in projective space

$$[X, Y, Z] = \frac{1}{Z}[X, Y, Z] = [x, y, 1],$$

and plugging this point into our homogeneous equation yields

$$E : F(X, Y, 1) = y^2 - x^3 - ax - b.$$

If $Z = 0$, then we have

$$F(X, Y, 0) = X^3.$$

Since points on the curve are those for which $F(X, Y, Z) = 0$, we must have $X = 0$, and Y is free to take any nonzero value, hence we obtain the homogeneous point $[0, Y, 0] = [0, 1, 0]$ corresponding to the line $Z = 0$; this is the point at infinity, $\mathbb{O}$. In projective space, all curves intersect, including parallel lines, which intersect at $\mathbb{O}$. Bézout's theorem, stated above, is actually a statement about projective space, but we extend its implications to $\mathbb{C}^2$ using $\mathbb{O}$.

As an illustration, note that if we have two parallel projective lines, $y = \alpha x + \beta_1 z$ and $y = \alpha x + \beta_2 z$, where $\beta_1 \neq \beta_2$, then to find their intersection, we solve these two equations simultaneously. These lines coincide when $z = 0$, so just as we claimed, these lines intersect at the point at infinity.

To make the addition law rigorous, let us now describe it algebraically. We wish to find the formula for $p_1 + p_2$, the sum any of two points on our curve, E, which is given by the equation $y^2 = x^3 + ax + b$. There are several cases to consider.

CASE 1: Let $p_1 = (x_1, y_1)$ and $p_2 = (x_2, y_2)$, and suppose $p_1 \neq p_2$ and neither point is equal to $\mathbb{O}$. To find $p_1 + p_2$, we must first find $p_1 * p_2 = p_3 = (x_3, y_3)$, the third point of intersection of the line between p_1 and p_2 with E. The line between p_1 and p_2 is given by

$$y = \lambda x + \nu, \quad \text{where } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and } \nu = y_1 - \lambda x_1.$$

Now, we wish to find the points where this line intersects our curve, so we make the following substitution:

$$y^2 = (\lambda x + \nu)^2 = x^3 + ax + b.$$

Subtracting gives us

$$0 = x^3 - \lambda^2 x^2 + (a - 2\lambda)x + (b - \nu^2).$$

The x-coordinates of the three points of intersection of the line and E are given by the roots of this equation. Factoring, we obtain

$$x^3 - \lambda^2 x^2 + (a - 2\lambda)x + (b - \nu^2) = (x - x_1)(x - x_2)(x - x_3),$$

and by identifying coefficients, we know that the sum of the roots is equal to the negative of the coefficient of x^2; that is,

$$x_1 + x_2 + x_3 = \lambda^2 \Rightarrow x_3 = \lambda^2 - x_1 - x_2.$$

By the equation of our line, this allows us to find y_3:

$$y_3 = \lambda x_3 + \nu.$$

Thus, we have $p_3 = (x_3, y_3)$. Now, the definition of our group law tells us that since p_1, p_2, and p_3 are collinear, their sum must be equal to the group identity, which is $\mathbb{O}$. Thus

$$p_1 + p_2 + p_3 = \mathbb{O}.$$

But this implies that $p_3 = -(p_1 + p_2)$. By the definition of the inverse of a group element, we know that

$$(p_1 + p_2) + p_3 = (p_1 + p_2) - (p_1 + p_2) = \mathbb{O}.$$

Using the definition of our group law again, as well as the fact that $\mathbb{O}$ is the identity element, we see that

$$(p_1 + p_2) + p_3 + \mathbb{O} = \mathbb{O},$$

which, geometrically, means that $p_1 + p_2$ is the third point of intersection of E with the line between p_3 and $\mathbb{O}$; but by our definition of $\mathbb{O}$, this is just a vertical

line, and since E is symmetric about the x-axis, we conclude that $p_1 + p_2$ is simply the reflection of p_3 about the x-axis. Thus,

$$p_1 + p_2 = -p_3 = (x_3, -y_3),$$

where x_3 and y_3 are given by

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda x_3 + \nu. \tag{1}$$

CASE 2: Let $p_1 = p_2 = (x_1, y_1) \neq \mathbb{O}$. Then the line "connecting" p_1 and p_2 is simply the line tangent to E at p_1. Since E is given by

$$y^2 = x^3 + ax + b,$$

implicit differentiation yields

$$\frac{\partial y}{\partial x} = \frac{3x^2 - a}{2y}.$$

Then the formulas in (1) hold, by the exact same arguments, with $\lambda = \partial y / \partial x$. Note that λ blows up if $y = 0$; that is, the tangent line is vertical. So if $p = (x, 0)$, then $p + p = 2p = \mathbb{O}$. Thus, the points of order two on E are precisely those with y-coordinate equal to zero.

CASE 3: If $p_1 = \mathbb{O}$, then since $\mathbb{O}$ is the identity element of the group, we have

$$p_1 + p_2 = \mathbb{O} + p_2 = p_2.$$

As an example, consider the curve E defined by

$$E = \{(x, y) \in \mathbb{C}^2 : y^2 = x^3 + 17\}.$$

It is easy to check that the points $p_1 = (2, 5)$ and $p_2 = (-1, 4)$ are on the curve. Applying the addition formulas given above, we see that $\lambda = \frac{1}{3}$, $\nu = \frac{13}{3}$, and $p_1 + p_2 = (-\frac{8}{9}, \frac{109}{27})$, which is also easily verified to be on the curve.

To summarize, under the chord-and-tangent addition law and the inclusion of $\mathbb{O}$, E forms an abelian group with identity element $\mathbb{O}$, where $p_1 + p_2 + p_3 = \mathbb{O}$ if and only if $p_1, p_2, p_3 \in E$ are the three points of intersection of some line with E. A wonderful introduction to elliptic curves can be found in [Silverman and Tate 1992].

Frequently, one prefers to look at the set

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b \text{ with } a, b \in \mathbb{Q}\} \cup \{\mathbb{O}\}$$

of rational points on the curve. Here again, $\mathbb{O}$ is the point at infinity with projective coordinates $\mathbb{O} = [0, 1, 0]$, and under the chord-and-tangent method of addition, the algebraic description of which is given in (1), $E(\mathbb{Q})$ forms an abelian group with identity element $\mathbb{O}$. In fact, this is a subgroup of the original group E, and

interestingly, the Mordell–Weil theorem tells us that it is finitely-generated. More generally, given a field K, one might look at the group

$$E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax + b \text{ with } a, b \in K\} \cup \{\mathbb{O}\}$$

of K-*rational* points on the curve. Once again, $\mathbb{O} = [0, 1, 0]$ is the point at infinity. If $K = \mathbb{F}_p$ is the finite field with p elements, where p is an odd prime, then $E(K)$ is called the *reduction modulo p of E*. An examination of our derivation of the algebraic formulas for the addition law, given in (1), reveals that the formulas hold in any field, provided the field has characteristic other than 2. Under this addition law, $E(K)$ forms an abelian group with identity element $\mathbb{O}$.

Let p be an odd prime. Given an elliptic curve E reduced modulo p, it is common to ask how many points N_p lie on the curve (equivalently, what the order is of the group given by the curve). Clearly this number is finite, since for each of the p possible values of x there are only two possible values of y, plus the point at infinity $\mathbb{O}$; hence there are at most $2p + 1$ points on the curve. A better estimate for N_p might be derived in the following way. An element a of $\mathbb{F}_p$ is said to be a *quadratic residue* if there exists a nonzero $b \in \mathbb{F}_p$ such that $b^2 \equiv a \pmod{p}$. In $\mathbb{F}_p$, there are exactly $(p - 1)/2$ quadratic residues. Finding points (x, y) on E amounts to finding those values of x such that $x^3 + ax + b$ is a quadratic residue modulo p; hence we might expect $x^3 + ax + b$ to be a square modulo p about half of the time. Since each such square yields the two pairs (x, y) and $(x, -y)$, we should expect about $p - 1$ such points. We might also have $x^3 + ax + b = 0$, in which case we get the point $(x, 0)$. Finally, there is the point at infinity. Adding these points up, we get an estimate of $N_p = p + 1$. Of course, this is a heuristic argument, so we should expect an error term. A theorem due to Hasse and Weil bounds this error term:

Theorem (Hasse, Weil). *If E is an elliptic curve defined over the finite field $\mathbb{F}_p$, then the number of points on E with coordinates in $\mathbb{F}_p$ is $p + 1 - a_p$, where the "error term" a_p satisfies $|a_p| \leq 2\sqrt{p}$.*

Returning to our previous example, let us look at the curve

$$\bar{E} = \{(x, y) \in \mathbb{F}_5 : y^2 = x^3 + 2\}.$$

In this case, brute force suffices to show that

$$E = \{(2, 0), (3, 2), (3, 3), (4, 1), (4, 4), \mathbb{O}\},$$

hence $N_p = 6$. Since $p + 1 = 6$, the error term from the Hasse–Weil theorem is in this case $a_p = 0$, and our heuristic argument gave us N_p exactly. This does not happen in general, however.

In this paper, we are particularly interested in the set

$$Q_E = \{\text{odd primes } p \in \mathbb{Z} : N_p \text{ is a quadratic residue modulo } p\}.$$

We have just shown that for the elliptic curve E which we have been considering, $N_5 = 6 \equiv 1 \equiv 1^2 \pmod{5}$, so $5 \in Q_E$. Note that, in general, for two different curves E_1 and E_2 we have $Q_{E_1} \neq Q_{E_2}$.

Recall that an endomorphism of a group G is a homomorphism $\phi : G \to G$. Now, since an elliptic curve $E/\mathbb{C}$ defined over $\mathbb{C}$ forms a group, it is natural to study $\text{End}(E)$, the ring of endomorphisms of E. (To be precise, we actually only look at rational endomorphisms, those which are defined by rational functions with entries in $\mathbb{C}$. These are also called *isogenies*.) For each integer n, the multiplication-by-n map $\phi_n : E \to E$ defined by $\phi_n(x, y) = n(x, y)$ (where $n(x, y)$ represents repeated chord-and-tangent addition) defines an endomorphism of E, hence $\phi_n \in \text{End}(E)$. For most curves, these are the only endomorphisms; however, some curves do have additional endormorphisms, and these curves are said to have *complex multiplication*, or simply CM. Curves for which $\text{End}(E) \cong \mathbb{Z}$ are said to be non-CM.

Returning to our example curve E defined by the polynomial

$$y^2 = x^3 + 17,$$

let $\phi : E \to E$ be the homomorphism defined by

$$\phi(x, y) = \left(\frac{-1 + \sqrt{-3}}{2} x, -y \right).$$

This is not a multiplication-by-n map, and since $\left(\frac{-1+\sqrt{-3}}{2}\right)^3 = 1$ and $(-y)^2 = y$, if $(x, y) \in E$ then also $\phi(x, y) \in E$; hence E has CM.

Conjecture. *Let E be a non-CM curve, fix a modulus M, and let $r_1, \ldots, r_s$ denote the residue classes modulo M such that $\gcd(r_i, M) = 1$ for each i. Now, look at the reduction of E modulo p for each p in the set $P_n = \{3, 5, \ldots, p_n\}$ of the first n odd primes, calculate N_p for each p, and let Q_E be defined as before. Let*

$$R_i = \{p \in Q_E \cap P_n \mid p \equiv r_i \pmod{M}\}.$$

Let $\#R_i$ denote the cardinality of this set. Then the residues of the elements of Q_E modulo M are uniformly distributed among the r_i; that is, for every $1 \leq i, k \leq s$ we have

$$\lim_{n \to \infty} \frac{\#R_i}{\#R_j} = 1.$$

This conjecture, suggested to Martin by Ramakrishna, is based on [Weston 2005], which investigates a similar problem involving the distribution of power residues for $a_p \equiv N_p - 1 \pmod{p}$.

To test this conjecture, we wrote a program using William Stein's project Sage which takes as input an elliptic curve E, a range of moduli M, and a large number B. For each modulus M, the program looks at the reduction of E modulo p for every prime $p < B$ and computes the number of points N_p on the reduced elliptic curve. Finally, it takes those p such that N_p is a quadratic residue modulo p and looks at their residues modulo M. The output data consists of 1) the number of primes congruent to r_i for each residue class r_i relatively prime to M, and 2) the maximum percent deviation of the size of each $\#R_i$ from the expected size (were the N_p distributed uniformly among the r_i).

In this paper, we present data from our program for several curves without CM, arguing that the trends in the data as B increases strongly suggest the truth of the conjecture.

2. The program

2.1. *What the programs do.* To get the data we needed, we wrote a program that takes an elliptic curve and a few other parameters, computes a subset of the prime numbers, called Q_E, and, given a modulus M, computes a count for each residue. The count is the number of elements in Q_E that, when reduced modulo M, have that residue. The program also computes the largest percent difference from the expected value.

More specifically, given an elliptic curve E, a range of prime numbers P, and a range of moduli M, the program computes the set

$$Q_E = \{p \in P \mid N_p \text{ is a quadratic residue modulo } p\}.$$

Then for all $m \in M$, the program computes for each residue r,

$$\#R = \#\{p \in P \mid p \equiv r \ (\mathrm{mod}\, m)\}.$$

This information is written to a file. Then the program computes some statistical information. First, it computes the expected count for each residue. If a residue, r, is not relatively prime to the modulus, m, then $p \in Q_E$ will have $p \equiv r \ (\mathrm{mod}\, m) \Leftrightarrow r \in Q_E$. This means that $\#R = 0, 1$ for all residues, r, that are not relatively prime to m. So we are really only interested in residues relatively prime to the modulus. If the conjecture were true for non-CM elliptic curves, we would expect that

$$\#R_i = \frac{\#Q_E}{\varphi(m)},$$

where $\varphi(m) = \#\{r \in \mathbb{Z} \mid 0 \leq r < m \text{ and } \gcd(r, m) = 1\}$ denotes the Euler-phi function and $r_1, \ldots, r_s$ are the residues relatively prime to m. For each modulus, m, the program computes the percent difference of the actual count, $\#R_i$, from the expected count, $C = (\#Q_E)/\varphi(m)$. So the percent difference for each residue is

$|1 - \#R_i/C| \cdot 100$. The program then picks out the largest percent difference. We are interested in the largest percent difference because it tells us how far off the actual count is from the expected count. Finally, the program writes to a file each modulus and its corresponding largest percent difference.

For example, consider the elliptic curve E defined by

$$F(x, y) = y^2 + xy + y - x^3 - 4x + 6.$$

Then given

$$P = \{p \in \mathbb{Z}^+ \mid p < 10^6, \, p \text{ prime}\},$$
$$M = \{m \in \mathbb{Z} \mid 3 \le m < 301\}, \text{ and}$$
$$Q_E = \{p \in P \mid N_p \text{ is a quadratic residue modulo } p\},$$

the program computed that $\#Q_E = 40593$. Now consider a specific modulus, say $m = 9$. Then the residues relatively prime to m are $r_1 = 1, r_2 = 2, r_3 = 4, r_4 = 5, r_5 = 7, r_6 = 8$, so $\varphi(m) = 6$. Thus the expected count for each residue is

$$C = \frac{\#Q_E}{\varphi(m)} = \frac{40593}{6} = 6765.5.$$

In fact, the program computed that the actual counts are

$$\#R_1 = 6551, \quad \#R_2 = 6876, \quad \#R_3 = 6802,$$
$$\#R_4 = 6850, \quad \#R_5 = 6632, \quad \#R_6 = 6882.$$

So there are 6551 primes p less than one million such that N_p is a quadratic residue modulo p and $p \equiv 1 \pmod 9$. In fact, of these six counts, $\#R_1$ is the farthest off from the expected count $C = 6765.5$. So $\#R_1$ will yield the biggest percent difference, which is

$$\left|1 - \frac{\#R_1}{C}\right| \cdot 100 \approx 3.17.$$

2.2. *Outline of programs and efficiency.* We organized the programs to try to maximize efficiency. The original programs we wrote were slow. Using them, we could not have computed nearly the same amount of data that we did with our newer version. By timing the original programs, we were able to see that the process that took the most time was generating and storing the set Q_E. Since this set was not even an output of our programs, we decided to generate one part of Q_E at a time. It worked like this:

```
while counter < limit:
      compute part of Q_E beginning with counter
      read in previously computed data (if any)
      compute counts for this part of Q_E
```

      save these data
      delete current part of Q_E
compute percentages for all data

Note that counter and limit are simply variables to keep track of which piece of Q_E has been computed.

This while loop lends itself to division into two programs: 1) a program to return a part of the set Q_E and 2) a program to maintain a count of the residue classes in the set Q_E over the various moduli in some set M. After running initial tests on various curves for primes strictly less than one hundred thousand, which ran in under five minutes, and then for primes strictly less than one million, which ran for more than two hours, we realized that the second run of these tests was recomputing data. This led us to modify the second program to look for output files generated by previous runs of the program and start with an updated count and then proceed from there. This also meant that if the program crashed in the middle of running, we wouldn't lose all previous data. Finally, there are several driver programs that run the tests for various elliptic curves, various ranges of moduli and various ranges of prime numbers.

2.3. *How the main programs work.* The main program, called residueCounter, is the second program described in the preceding paragraph. It takes as parameters a starting number and upper bound to specify which range of prime integers to look at, a starting modulus and ending modulus to specify which range of moduli to test, a list of five integers to specify an elliptic curve, and finally a boolean to specify whether or not to look for files containing data that this program can use. The program stores all of the output in a dictionary, called dataDict. The keys of the dictionary are the moduli in the range specified by the parameters. Given a modulus, m, dataDict[m] evaluates to a list of lists. This list is a count for each residue of m.

The program starts by deciding whether or not to look for old files based on the boolean passed as a parameter.

if True:
      find all files generated by previous runs of residueCounter
      pick the most relevant file
      initialize dataDict to include all of the data computed from this file
      exclude the primes already checked by this file
if False:
      initialize a blank dataDict

Note that the most relevant file is the file whose range of moduli match that of the current program and of the files whose ranges match; the one with the highest upper bound has the most data and hence will save the most time.

The program needs to find the set Q_E and update dataDict to include the count from this set. However, as mentioned in the previous section, the program runs too slowly to do this all at once. So, instead it runs a loop that calls a different function, the first one mentioned above, to return a piece of Q_E, update dataDict to get all the counts for this piece, and then repeat this over and over until dataDict has all the data needed.

More precisely, the program has a variable current prime to keep track of what part of Q_E has been retrieved. It then runs the following while loop:

while current prime is strictly less than the upper bound:
    call function
    this function returns a new current prime and a piece of Q_E
    update dataDict for this piece of Q_E
    get rid of that piece of Q_E to clear up memory space
    try to run loop again

The program then calculates the largest percent difference for each modulus, as described in Section 2.1. Finally, it writes this information to two different files, one for the data, one for the statistical information. The file names are keyed to include the elliptic curve, the upper bound, the range of moduli and what kind of file it is.

The function called in the last while loop is the one that actually deals with the elliptic curves. The elliptic curves we are looking at have the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$ for some $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$. This way we can look at the curves reduced modulo p for odd primes p. A standard way to reference a specific curve is by a list of the coefficients $[a_1, a_2, a_3, a_4, a_6]$.

This function takes as parameters an elliptic curve in the form $[a_1, a_2, a_3, a_4, a_6]$, the current prime, how many primes to check and the upper bound. It then calculates the conductor of the elliptic curve. Every elliptic curve has a unique integer associated with it, called the conductor. Essentially, the conductor tells you which primes to avoid; every prime divisor of the conductor has what is known as 'bad reduction', meaning that the reduction of E modulo these primes is singular and therefore not an elliptic curve. Accordingly, this function skips all of these primes. Also, we are only interested in primes p such that N_p is a quadratic residue modulo p. Luckily, there is a quick way to find out if N_p is a quadratic residue. A result due to Euler says that a necessary and sufficient condition for $a \in \mathbb{F}_p$ to be a quadratic residue is:

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

The numbers N_p are calculated in Sage via the command `cardinality` using either the Schoof–Elkies–Atkins algorithm or the baby-step-giant-step algorithm

of Mestre and Shanks. Sage decides which algorithm to use by heuristically deter-
mining which will be more computationally efficient.

That said, here is a sketch of the program:

compute conductor of elliptic curve
initialize blank list to store primes of interest
while (current prime < upper bound) and (counter < how many primes to check):
    if current prime doesn't divide conductor:
        if the coefficients define an elliptic curve:
           if $N_p^{(p-1)/2} \equiv 1 \pmod{p}$:
              add current prime to list
set current prime to the next prime

3. The data

Let us recall the conjecture on which we are working.

Conjecture. *Given a non-CM elliptic curve E, a modulus M, and a list Q_E of
all the primes p for which the number of points N_p on the reduction of E modulo
p are quadratic residues modulo p, the elements of Q_E are uniformly distributed
among the residue classes of M.*

Due to the nature of the conjecture, the data we collect is bound to have some
experimental error, since we can only look at a finite subset of Q_E at a time. When
this subset of Q_E is large with respect to the modulus M, we should expect less
error, and when this subset is small with respect to M, we should expect greater
variance in the distribution of the primes, and hence greater error.

When we ran our program, to obtain our subset of Q_E we took all of the primes
in Q_E below some fixed bound B. We then looked at their distribution among
the residue classes of moduli from 3 to 300. The preceding discussion suggests
that by increasing the size of B, we should expect to see our experimental error
decrease. Consider Figure 1, which shows the data for $F(x, y) = y^2 + y - x^3 + x$, a
curve lacking complex multiplication. The bars in the graph indicate the maximum
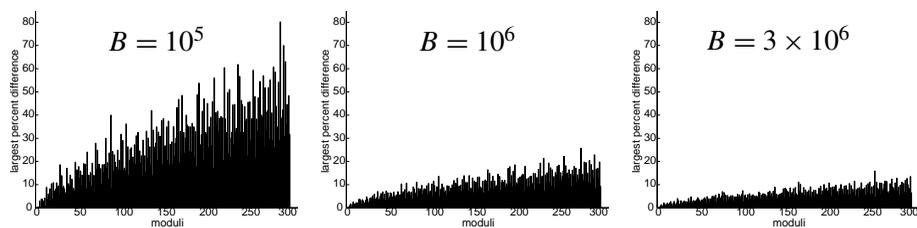
Figure 1. Prime distribution on the non-CM curve $y^2 + y = x^3 - x$
of conductor 37 and rank 1, for different values of the bound B.

percent deviation from the expected (uniform) distribution among the moduli; a higher bar indicates higher deviation. The first important thing to note is that, in all three figures, we can see that the error does indeed increase as the modulus increases. The second thing to note is that as we increase B (and thus the size of our subset of Q_E), the error decreases for every modulus. The three parts of the figure show the error when $B = 10^5$, 10^6, and 3×10^6. As B increases, the graphs "flatten out", indicating a decrease in the error. This suggests that the deviation is simply "experimental error".

We tested our program on several non-CM curves of varying ranks and conductors. The data for some of these curves is presented on this and the next two pages. The data for all of the curves tested strongly suggest that the conjecture is correct. However, we have no proof of it at this time.

All of our data and program code is available upon request.
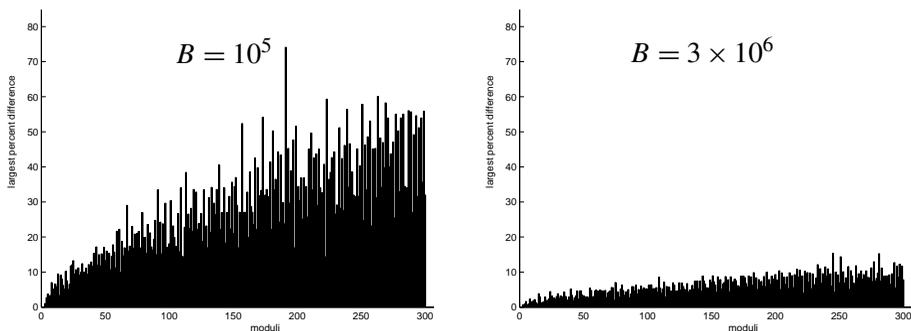


$$y^2 + y = x^3 - x^2 - 10x - 20$$
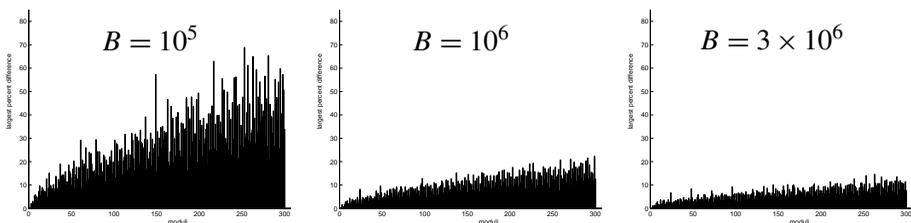
$$y^2 + xy + y = x^3 + 4x - 6$$
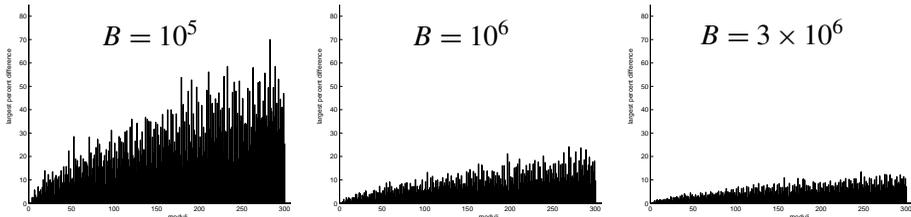

$$y^2 + y = x^3 + x^2 - 2x$$
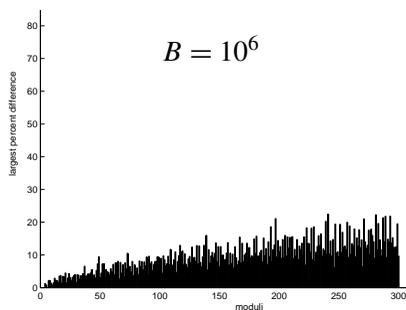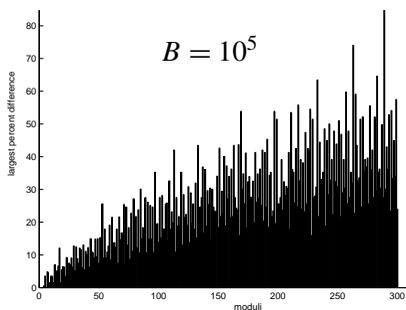
$$y^2 + y = x^3 - 7x + 6$$
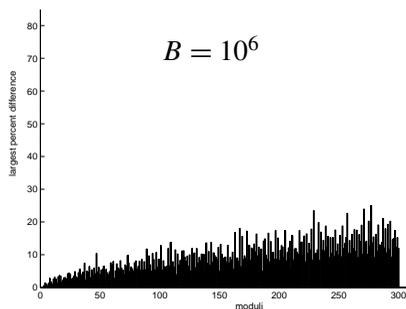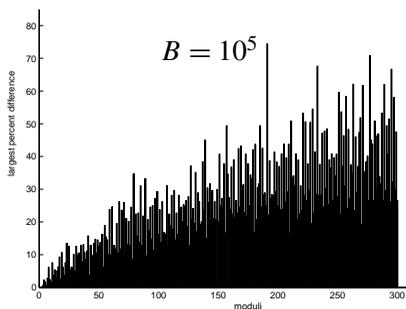
$$y^2 + xy = x^3 - x^2 - 79x + 289$$
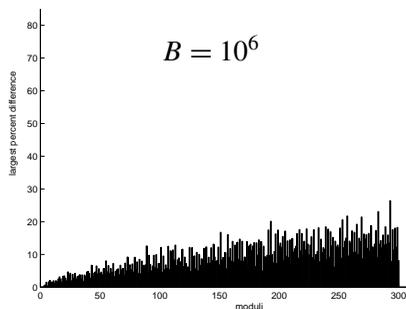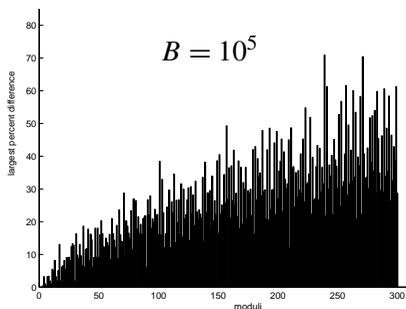
$$y^2 + y = x^3 - 79x + 342$$
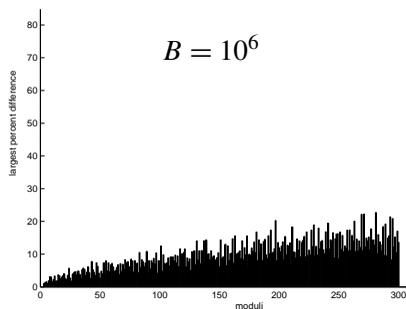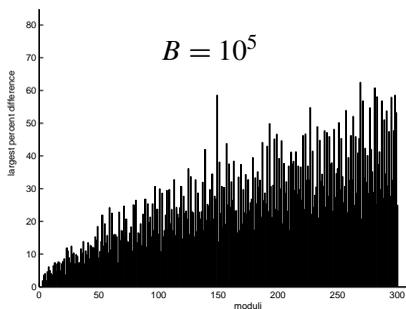
$$y^2 + xy = x^3 + x^2 - 2582x + 48720$$
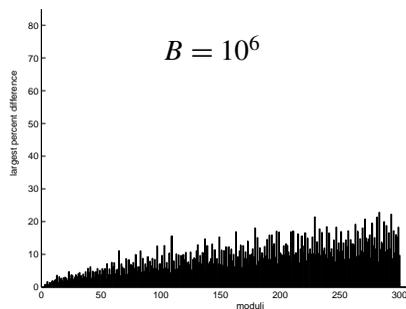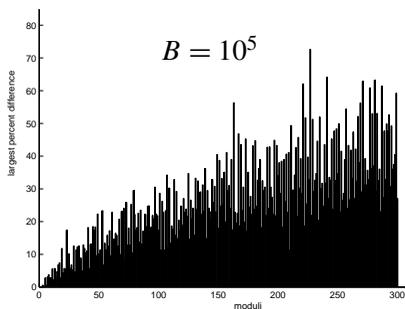
$$y^2 = x^3 - 10012x + 346900$$
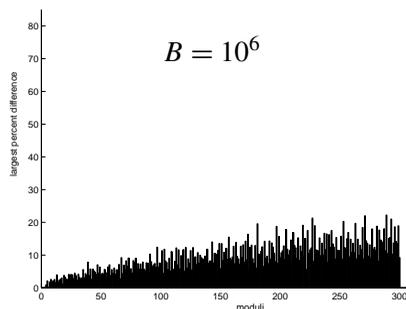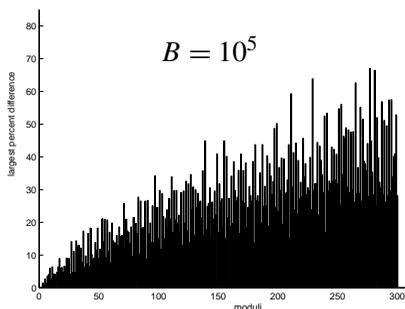
$$y^2 + y = x^3 - 23737x + 960366$$
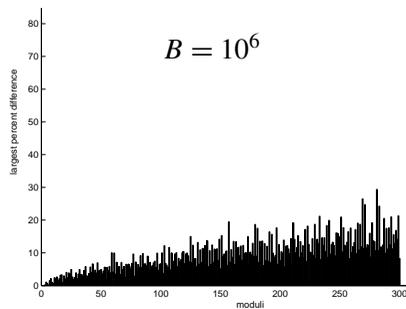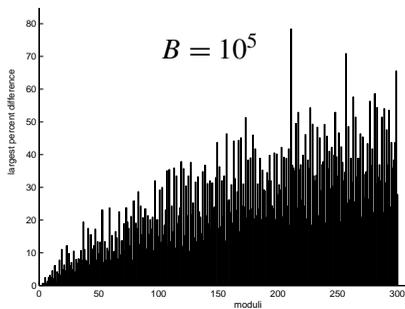
$$y^2 + y = x^3 + x^2 - 3529920x + 2567473020$$

4. Future research ideas

Several related problems might be considered in the future. It would be beneficial
to find an efficient way to run a program like ours for larger primes for further
data collection. The data presented in is paper is for values of B at the limit of
our program's reasonable run time. We plan to modify our program to test the
conjecture regarding a_p rather than N_p; furthermore, Weston [2005] conjectures
that a similar result holds for primes for which the a_p are higher power residues. A

slight modification of our program, or any similar program, would allow for data collection for these cases.

Acknowledgement

References

[Kirwan 1992] F. Kirwan, *Complex algebraic curves*, London Mathematical Society Student Texts **23**, Cambridge University Press, Cambridge, 1992. MR 93j:14025 Zbl 0744.14018

[Silverman and Tate 1992] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer, New York, 1992. MR 93g:11003 Zbl 0752.14034

[Weston 2005] T. Weston, "Power residues of Fourier coefficients of modular forms", *Canad. J. Math.* **57**:5 (2005), 1102–1120. MR 2006e:11058 Zbl 1105.11011

hatley2@tcnj.edu   *Department of Mathematics, University of Massachusetts, Amherst, MA 01003-9305, United States*

ahittson@brynmawr.edu   *Department of Mathematics, University of Wisconsin, 480 Lincoln Drive, Madison, WI 53706-1388, United States*

The genus level of a group

Matthew Arbo, Krystin Benkowski, Ben Coate,
Hans Nordstrom, Chris Peterson and Aaron Wootton

(Communicated by Nigel Boston)

We introduce the notion of the genus level of a group as a tool to help classify finite conformal group actions on compact Riemann surfaces. We classify all groups of genus level 1 and use our results to outline an algorithm to classify actions of p-groups on compact Riemann surfaces. To illustrate our results, we provide a number of detailed examples.

1. Introduction

The group of conformal automorphisms of a compact Riemann surface of genus $\sigma \geq 2$ is always finite. An interesting problem is to determine all groups that can act on a surface X of genus $\sigma \geq 2$ for a fixed σ. For low genus, due to great advances in computer algebra systems, this problem has been completed. Specifically, in [Broughton 1991], all groups that can act on surfaces up to genus 3 were classified. More recently, with the aid of the computer algebra system GAP, the list of all groups that can act on surfaces of genus σ for genera $2 \leq \sigma \leq 48$ were classified in [Breuer 2000] and stored in a database in GAP. Though in principle the algorithms developed to solve this problem could be used to determine automorphism groups of surfaces of higher genus, the computations become much more complicated, and complete classification does not seem reasonable.

A different approach to classifying automorphism groups is to fix some other property than the genus of the surface X. One can, for instance, restrict how a group may act on the surface, or one can restrict the types of groups under consideration that act on X. In many cases, complete classification results are possible. Such results abound in the literature; see for example [Benim 2008; Bujalance et al. 2003; Harvey 1966; Kallel and Sjerve 2001; Wootton 2007b]. One motivation for classifying automorphism groups by imposing further restrictions on the way an

automorphism group can act on a surface is that it may aid in answering other questions about the surface. For example, in certain cases, the classical problem of determining a defining model for a compact Riemann surface X is possible when assumptions are made about the existence of automorphisms on the surface acting in a particular way, as was done in [Fuertes and González-Diez 2007] or [Wootton 2007a]. Another motivational reason for classifying families of surfaces is that it may provide new techniques to the more general problem of classifying all groups that can act on surfaces of genus $\sigma \geq 2$.

Suppose G is a finite group of automorphisms of a compact Riemann surface X of genus $\sigma \geq 0$. We define the *genus level* of G to be the number of distinct genera of the quotient spaces X/H, where H runs over the nontrivial subgroups of G. We will classify all groups of genus level 1. This is an extension of [Kallel and Sjerve 2001], where full results are given for each group G that can act on a surface of genus $\sigma \geq 0$ with the property that every quotient space X/H has genus 0, where H runs over all the nontrivial subgroups of G. We use our results to provide an inductive method to determine all p-groups that act as automorphism groups on surfaces of genus $\sigma \geq 2$ (though it should be noted that with minor modifications, this algorithm would extend to a classification of nonsimple groups).

2. Preliminaries

Suppose that G is a group of conformal automorphisms of a compact Riemann surface X of genus $\sigma \geq 2$ upon which we assume G acts faithfully. We need the following definitions:

Definition 2.1. The *signature* of G is defined to be the tuple of integers

$$(g; m_1, m_2, \ldots, m_r),$$

where the orbit space X/G has genus g and the quotient map $\pi_G : X \to X/G$ is branched over r points $\alpha_1, \ldots, \alpha_r$, where the multiplicity of a point in the fiber $\pi_G^{-1}(\alpha_i)$ is equal to m_i for $1 \leq i \leq r$. We say that the *genus of G* is g and we call the numbers $m_1, \ldots, m_r$ the *periods* of G.

Remark 2.2. We note that for a general holomorphic map $F : X \to Y$, the multiplicities of two different points in the fiber $F^{-1}(\alpha)$ for $\alpha \in Y$ may be different. However, for normal covers, all points in a fiber will have the same multiplicity, and so our definition for the m_i is well defined. For more detail on holomorphic maps, we refer the reader to [Miranda 1995, Chapter 2].

Definition 2.3. We define the *genus level* of G to be the number of distinct genera among those of the nontrivial subgroups of G. If G has genus level n, we define the *genus level vector* to be the n-tuple of increasing integers $(t_1, \ldots, t_n)$, where t_i is the genus of some nontrivial subgroup of G.

Definition 2.4. A vector of elements $(\alpha_1, \ldots, \alpha_t, \beta_1, \ldots, \beta_t, \gamma_1, \ldots, \gamma_r)$ is called a $(t, m_1, \ldots, m_r)$-*generating vector* of G if

(i) $G = \langle \alpha_1, \ldots, \alpha_t, \beta_1, \ldots, \beta_t, \gamma_1, \ldots, \gamma_r \rangle$,

(ii) $O(\gamma_i) = m_i$ for $1 \leq i \leq r$, and

(iii) $\prod_{i=1}^{t} [\alpha_i, \beta_i] \cdot \prod_{j=1}^{r} \gamma_j = e$.

We refer to the elements α_i and β_i as *hyperbolic generators* and the elements γ_i as *elliptical generators*.

The $(t; m_1, m_2, \ldots, m_r)$-generating vectors of a group G provide us with a way to determine when G acts on a surface of genus $\sigma \geq 2$. Specifically, we have the following.

Theorem 2.5. *A group G acts with signature $(t; m_1, \ldots, m_r)$ on a surface X with genus $\sigma \geq 2$ if G has a $(t; m_1, \ldots, m_r)$-generating vector and the Riemann–Hurwitz formula holds*:

$$2\sigma - 2 = |G| \left(2t - 2 + \sum_{i=1}^{r} \left(1 - \frac{1}{m_i} \right) \right).$$

Proof. See [Broughton 1991]. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

If a group G acts on a surface X, so does each of its subgroups. The signatures of the subgroups can be calculated from that of G as follows:

Theorem 2.6 [Singerman 1970]. *Suppose G has signature $(t; m_1, \ldots, m_r)$ and generating vector $(\alpha_1, \beta_1, \ldots, \alpha_t, \beta_t, \gamma_1, \ldots, \gamma_r)$. Suppose $H \leq G$, set $d = |G|/|H|$ and let $\theta \colon G \to S_d$ be the map induced by permutation on the left cosets of H. Then the signature of H is*

$$(s; n_{11}, n_{12}, \ldots, n_{1\rho_1}, n_{21}, \ldots, n_{2\rho_2}, \ldots, n_{r1} \ldots, n_{r\rho_r}), \qquad (1)$$

where

(i) *$\theta(\gamma_j)$ has precisely ρ_j cycles of length $m_j/n_{j_1}, \ldots, m_j/n_{j\rho_j}$, respectively*;

(ii) *s satisfies*

$$2s - 2 + \sum_{i=1}^{r} \sum_{j=1}^{\rho_i} \left(1 - \frac{1}{n_{ij}} \right) = d \left(2t - 2 + \sum_{i=1}^{r} \left(1 - \frac{1}{m_i} \right) \right). \qquad (2)$$

Conversely, if d divides $|G|$ and there exist a map $\theta \colon G \to S_d$ and an integer s such that conditions (i) *and* (ii) *hold, there exists $H \leq G$ of index d and signature* (1).

In the special case that H is a normal subgroup of G, calculation of the signature is much easier.

Theorem 2.7. *Suppose G has signature $(t; m_1, m_2, \ldots, m_k)$ and $H \trianglelefteq G$. Then the signature of H is*

$$\left(s; \underbrace{\frac{m_1}{n_1}, \ldots, \frac{m_1}{n_1}}_{a_1 \text{ times}}, \underbrace{\frac{m_2}{n_2}, \ldots, \frac{m_2}{n_2}}_{a_2 \text{ times}}, \ldots, \underbrace{\frac{m_r}{n_r}, \ldots, \frac{m_r}{n_r}}_{a_r \text{ times}} \right),$$

where $O\left(\rho\left(\gamma_i\right)\right) = n_i$ under $\rho : G \to G/H$, $a_i = |G/H|/n_i$ and s satisfies

$$2s - 2 = \frac{|G|}{|H|} \left(2t - 2 + \sum_{i=1}^{r} \left(1 - \frac{1}{n_i} \right) \right).$$

Remark 2.8. We can use Theorems 2.6 and 2.7 to reconstruct the signature of G given the signature of H and the map $\theta : G \to G/H$; see Theorem 4.3 for example.

The inconsistency of the notation for the order of the elliptic generators of H in Theorems 2.6 and 2.7 is to preserve the form of the summand in the Riemann–Hurwitz formula. To avoid confusion, we shall clearly distinguish between the normal and nonnormal cases.

Remark 2.9. It is an immediate consequence of Theorem 2.6 that $t \leq s$. Note that this also implies, if G has genus vector $(t_1, \ldots, t_r)$, then G must have genus t_1.

All finite groups that can act on surfaces of genus 0 and 1 are well known; see for example [Tyszkowska and Weaver 2008] for genus 1 and [Wootton 2005] for genus 0. Most of the results and definitions we have introduced for groups acting on surfaces of genus $\sigma \geq 2$ hold for genus 0 and 1 too and will be relevant in our work. We summarize below.

Theorem 2.10. (i) *The possible finite groups and corresponding signatures for groups that can act on a surface of genus $\sigma = 1$ are shown in the table on the left. We call these signatures* toroidal signatures.

 (ii) *The possible finite groups and corresponding signatures for groups that can act on a surface of genus $\sigma = 0$ are shown in the table on the right. We call these signatures* spherical signatures.

Group	Signature	Group	Signature
$C_n \times C_m$	$(1; -)$	C_n	$(0; n, n)$
$(C_n \times C_m) \ltimes C_2$	$(0; 2, 2, 2, 2)$	D_n	$(0; 2, 2, n)$
$(C_n \times C_m) \ltimes C_3$	$(0; 3, 3, 3))$	A_4	$(0; 2, 3, 3)$
$(C_n \times C_m) \ltimes C_4$	$(0; 2, 4, 4)$	S_4	$(0; 2, 3, 4)$
$(C_n \times C_m) \ltimes C_6$	$(0; 2, 3, 6)$	A_5	$(0; 2, 3, 5)$

Table 1. Groups of automorphisms of genus 1 surfaces (left) and those of genus 0 surfaces (right).

We finish this section with an explicit example to illustrate the use of these results.

Example 2.11. Consider the group

$$Q_8 = \langle x, y \mid x^4, x^2 y^2, yxy^{-1} = x^{-1} \rangle$$

The vector (x^2, x^2, x, x, y, y) is a $(0; 2, 2, 4, 4, 4, 4)$-generating vector for Q_8. Using the Riemann–Hurwitz formula from Theorem 2.5, it follows that this is a group of automorphisms of a surface of genus

$$\sigma = 1 + |G|(-1) + |G|/2 \sum_{i=1}^{6} (1 - 1/m_i)$$

$$= 1 - 8 + 4 \left(\frac{1}{2} + \frac{1}{2} + \frac{3}{4} + \frac{3}{4} + \frac{3}{4} + \frac{3}{4} \right) = 9.$$

Consider the normal subgroup $N = \langle x \rangle$ and the canonical homomorphism $\rho : G \to G/N$. We have $O(\rho(x^2)) = 1$, $O(\rho(x)) = 1$, and $O(\rho(y)) = 2$. By Theorem 2.6, it follows that H has signature $(s; 2, 2, 2, 2, 2, 2, 4, 4, 4, 4)$, where

$$s = 1 + |G|/|N|(g-1) + |G|/2|N| \sum_{i=1}^{6} (1 - 1/n_i) = 1 - 2 + \left(\frac{1}{2} + \frac{1}{2} \right) = 0.$$

3. Groups of genus level 1

We want to classify all genus level 1 group actions on all compact Riemann surfaces. In [Kallel and Sjerve 2001] all genus level 1 groups with genus level vector (0) are classified for groups acting on surfaces of genus $\sigma \geq 0$. Using Theorem 2.10 we get the following classification for groups acting on genus 1 surfaces with genus level 1.

Theorem 3.1. *Suppose G, a finite group, acts on a surface of genus 1 and has genus vector (1). Then $G \cong C_n \times C_m$, where C_n and C_m are finite cyclic groups.*

It remains to classify all genus level 1 groups acting on a surface of genus $\sigma \geq 2$ with genus vector (t) for $t \geq 1$. We start with the following important result.

Proposition 3.2. *Suppose G has signature $(t; m_1, m_2, \ldots, m_r)$, where $t \geq 1$. Let H be a nontrivial proper subgroup of G that also has genus t. Then $t = 1$ and the elliptical generators $\gamma_i \in H$ for all i.*

Proof. We set $t = s$ in Equation (2) of Theorem 2.6 and rearrange, obtaining

$$2t - 2 + \sum_{i=1}^{r} \sum_{j=1}^{\rho_i} \left(1 - \frac{1}{n_{ij}} \right) = \frac{|G|}{|H|} (2t - 2) + \frac{|G|}{|H|} \sum_{i=1}^{r} \left(1 - \frac{1}{m_i} \right),$$

$$2t - 2 - \frac{|G|}{|H|}\left(2t - 2\right) = \frac{|G|}{|H|}\sum_{i=1}^{r}\left(1 - \frac{1}{m_i}\right) - \sum_{i=1}^{r}\sum_{j=1}^{\rho_i}\left(1 - \frac{1}{n_{ij}}\right),$$

$$2(1 - t)\left(\frac{|G|}{|H|} - 1\right) = \frac{|G|}{|H|}\sum_{i=1}^{r}\left(1 - \frac{1}{m_i}\right) - \sum_{i=1}^{r}\sum_{j=1}^{\rho_i}\left(1 - \frac{1}{n_{ij}}\right).$$

Now, we have $n_{ij} \leq m_i$, since $n_{ij} \mid m_i$, and we know that $\rho_i \leq |G| / |H|$. Furthermore, equality will hold in each case exactly when $\theta\left(\gamma_i\right)$ is the identity permutation, consisting of $|G| / |H|$ 1-cycles. Then

$$2(1 - t)\left(\frac{|G|}{|H|} - 1\right) = \frac{|G|}{|H|}\sum_{i=1}^{r}\left(1 - \frac{1}{m_i}\right) - \sum_{i=1}^{r}\sum_{j=1}^{\rho_i}\left(1 - \frac{1}{n_{ij}}\right)$$

$$\geq \frac{|G|}{|H|}\sum_{i=1}^{r}\left(1 - \frac{1}{m_i}\right) - \sum_{i=1}^{r}\frac{|G|}{|H|}\left(1 - \frac{1}{m_i}\right) = 0.$$

Since $t \geq 1$, the inequality cannot be satisfied unless $t = 1$. Thus each γ_i acts as the identity permutation on the cosets of H, that is, $\gamma_i \in H$ for all i. $\qquad\square$

Remark 3.3. A consequence of this result is that if G has genus $t > 1$, then all proper subgroups have genus strictly greater than t.

This allows us to classify all genus level 1 groups with genus level vector (t) for $t > 1$. Specifically, we have the following.

Corollary 3.4. *Suppose G acts on a surface of genus $\sigma \geq 2$ and has genus level vector (t) for some $t \geq 2$. Then $G \cong C_p$, where C_p is cyclic of prime order p; the possible signatures of G are*

$$(t; \underbrace{p, p, \ldots, p}_{r \text{ times}}),$$

where r is at least 2 for all p and is even when $p = 2$; and finally, the genus σ equals $1 + \frac{1}{4}p(t - 1)(p - 1)$.

An obvious but very useful consequence of this result is the following.

Corollary 3.5. *If G acts with signature $(1; m_1, m_2, \ldots, m_r)$ and all $\gamma_i \in H$ for some subgroup H, then H has genus 1.*

The last case we need to consider is when a group with genus level vector (1) acts on a surface of genus $\sigma \geq 2$.

Theorem 3.6. *Suppose G acts on a surface of genus $\sigma \geq 2$ and has genus level vector (1). Then $G \cong C_{p^n}$ or $G \cong Q_8$.*
When $G \cong C_{p^n}$, the possible signatures are $(1; \overbrace{p, p, \ldots, p}^{r \text{ times}})$, where r is at least 2 for all p and is even when $p = 2$; moreover $\sigma = 1 + \frac{1}{4}p^{2n-1}(t - 1)(p - 1)r$.

In the opposite case the possible signatures are $(1; \underbrace{2, 2, \ldots, 2}_{r \text{ times}})$, *where r is odd;*
moreover $\sigma = 8t + 2r - 7$.

Proof. Suppose the generating vector of G is $(\alpha, \beta, \gamma_1, \ldots, \gamma_r)$. Since every non-trivial subgroup has genus 1, Corollary 3.5 implies that all γ_i lie in each nontrivial subgroup of G. By assumption, $m_i \geq 2$, and $r \geq 1$ since $(1; -)$ does not satisfy the Riemann–Hurwitz formula for a group action on a surface of genus $\sigma \geq 2$. It follows that the intersection of all nontrivial subgroups of G contains each γ_i and hence is nontrivial, and thus G has a unique minimal nontrivial subgroup. The only groups that satisfy this condition are C_{p^n} and Q_{2^n}, by [Robinson 1995, Theorem 5.3.6]. We now proceed by cases.

First consider

$$G = Q_{2^n} = \langle x, y \mid x^{2^{n-1}}, x^{2^{n-2}} y^{-2}, yxy^{-1}x \rangle.$$

Let $H = \langle y^2 \rangle \lhd G$ and let $\theta : G \to G/H$ denote the canonical quotient map. Observe that $G/H \cong D_{2^{n-2}}$, the dihedral group of order 2^{n-1}. By our remarks above, all γ_i lie in H. Now $\alpha \beta \alpha^{-1} \beta^{-1} \gamma_1 \gamma_2 \cdots \gamma_r = e$, so

$$\theta(e_G) = \theta(\alpha \beta \alpha^{-1} \beta^{-1} \gamma_1 \gamma_2 \cdots \gamma_r) = [\theta(\alpha), \theta(\beta)] = e_{G/H}.$$

It follows that $\theta(G)$ must be abelian, since it is generated by $\theta(\alpha)$ and $\theta(\beta)$. The only abelian dihedral group is the Klein 4 group. Hence $G \cong Q_8$.

Now consider

$$G \cong Q_8 = \langle x, y \mid x^4, x^2 y^2, yxy^{-1}x \rangle.$$

Then G has a $(1; \underbrace{2, 2, \ldots, 2}_{r \text{ times}})$-generating vector $(y, x, y^2, y^2, \ldots, y^2)$ for any odd r.
For even r, the generating vector must be of the form

$$(\alpha, \beta, y^2, y^2, \ldots, y^2)$$

for some $\alpha, \beta \in G$. However, when r is even, the product of r copies of y^2 is the identity. It follows that α and β must commute and generate G, and no such generators of Q_8 exist, and hence r cannot be even. To finish, we need to show that every nontrivial subgroup of G has genus 1. First observe that the center $Z(G)$ is the intersection of all nontrivial subgroups. By Remark 2.9, since we are assuming G has genus 1, it suffices to prove that $Z(G)$ has genus 1. But this follows by Corollary 3.5. To determine σ, we simply apply Theorem 2.5.

Finally, consider $G = C_{p^n} = \langle x \mid x^{p^n} \rangle$. Since C_{p^n} is abelian and all γ_i are in the minimal subgroup $\langle x^{p^{n-1}} \rangle = \langle a \rangle$, the order of each γ_i is p. Moreover, the commutator $[\alpha, \beta]$ will be equal to the identity, and hence $\gamma_1 \ldots \gamma_r = e$. It follows that $r \geq 2$. Furthermore, if $p = 2$ then $\gamma_i = a$ for all i. In this case the product $\gamma_1 \ldots \gamma_r = e$ if and only if r is even.

To finish, we need to construct generating vectors. For r even, the vector $(x, x, a, a^{-1}, a, a^{-1}, \ldots, a, a^{-1})$ is a generating vector for G. For r odd, we know $p \neq 2$ and consequently $(x, x, a, a^{-1}, a, a^{-1}, \ldots, a, a^{-1}, a, a, a^{-2})$ is a generating vector for G. To determine σ, we simply apply Theorem 2.5. $\square$

To summarize our results, we need the following definitions.

Definition 3.7. We define a Zassenhaus metacyclic group to be a group with presentation
$$\langle x, y \mid x^m, y^n, yxy^{-1}x^{-r} \rangle$$
, where $r^n \equiv 1 \mod (m)$ and $\gcd((r-1)n, m) = 1$. We denote such a group by $G_{m,n}(r)$.

Definition 3.8. We define a polyhedral group to be a finite subgroup of PSL $(2, \mathbb{C})$. Equivalently, polyhedral groups are the cyclic groups of order n for any n, the dihedral groups of order $2n$ for any n, the alternating groups A_4 and A_5, and the symmetric group S_4.

Combining the results of [Kallel and Sjerve 2001] with Theorems 3.1, 3.6 and Corollary 3.4, we get a complete classification of genus level 1 group actions. We summarize.

Theorem 3.9. *Suppose G is a finite group acting on a compact Riemann surface of genus $\sigma \geq 0$ and G has genus level 1. Then we have the following possibilities*:

(i) *If G has genus level vector (0) then G is either cyclic, generalized quaternion (Q_{2^n}), polyhedral or Zassenhaus metacyclic of the form $G_{p,4}(-1)$ for p an odd prime.*

(ii) *If G has genus level vector (1) and $\sigma = 1$, then $G = C_n \times C_m$, a direct product of two finite cyclic groups.*

(iii) *If G has genus level vector (1) and $\sigma \geq 2$, then $G \cong Q_8$, the quaternion group, or $G \cong C_{p^n}$, a cyclic group of prime power order p^n.*

(iv) *If G has genus level vector (t) for $t \geq 2$, then $G \cong C_p$, a cyclic group of prime order p^n.*

4. Determining p-groups

Suppose G is a nonsimple group of automorphisms acting on a surface X of genus $\sigma \geq 0$ with genus level vector $(t_1, \ldots, t_n)$. If N is a normal subgroup G with genus t_i, then G/N acts on the surface X/N of genus t_i. The genus level vector of the action of G/N on X/N is clearly related to the genus level vector of the action of G of N. The precise relationship is this:

Lemma 4.1. *Suppose G acting on X has genus level vector $(t_1, \ldots, t_k)$ and $N \leq G$ is a nontrivial normal subgroup of G of genus t_i. Then G/N has genus level vector $(m_1, \ldots, m_l)$, where the m_j run over the genera of each subgroup $K \leq G$ with $N \leq K$.*

Proof. Suppose G and N are as given. If $\bar{K} \leq G/N$, let $K > N$ denote its preimage in G given by the correspondence theorem. Then the quotient space $(X/N)/(\bar{K})$ is naturally homeomorphic to the quotient space X/K. In particular, the genus of the quotient space $(X/N)/(\bar{K})$ will be equal to the genus of the quotient space X/K. Conversely, using a similar argument, if $N \leq K$, then the image of K in the quotient group G/N will have the same genus as K. The result follows.   □

Here is a simple consequence of the relationship described in Lemma 4.1.

Corollary 4.2. *Suppose G has genus level vector $(t_1, \ldots, t_k)$ for $k \geq 2$ and $N \leq G$ is a nontrivial normal subgroup of G of genus t_i. Then unless G has genus level vector $(0, 1)$ and $t_i = 1$, the genus level vector of G/N is strictly shorter in length than the genus level vector of G.*

These observations suggest we can construct an inductive algorithm to help determine nonsimple groups of automorphisms of compact Riemann surfaces dependent upon the length of the genus level vector. Specifically, if the genus level of a group G is at least two, then except under the exception provided above in Corollary 4.2, the genus level of a nontrivial quotient group will be strictly smaller than the genus level of a given group. This, coupled with the classification of genus level 1 actions in Section 3, provides an inductive process for classification. Though in principle such an algorithm is possible, the calculations become difficult very quickly, especially the calculation of signatures. Therefore, rather than a general algorithm for all nonsimple groups, we shall construct an algorithm for p-groups. Henceforth assume that G is a p-group for some prime p. Before we construct the algorithm, we shall develop several results specific to p-groups.

Theorem 4.3. *Suppose that G is a p-group of order p^n acting on a surface X of genus σ with genus level vector $V = (t_1, \ldots, t_k)$ and C is a normal cyclic prime subgroup of G with genus t_i, so C has signature*

$$(t_i; \underbrace{p, \ldots, p}_{f \text{ times}}), \quad where \ f = \frac{2\sigma - 2 - 2p(t_i - 1)}{p - 1}.$$

Then the quotient group G/C acts on a surface of genus t_i with genus level vector $(t_1, t_{\beta_1}, \ldots, t_{\beta_s})$, where $\beta_1, \ldots, \beta_s$ run over the genera of each subgroup K with $C \leq K \leq G$. If the signature of G/C is $(t_1; m_1, \ldots, m_r)$, the signature of G is

$$(t_1; a_1 m_1, a_2 m_2, \ldots a_r m_r, \underbrace{p, \ldots, p}_{l \text{ times}}), \quad where \ a_1, \ldots, a_r \in \{1, p\},$$

and where f and l satisfy

$$f = lp^{n-1} + \sum_{i=1}^{r} \frac{(a_i - 1)p^{n-1}}{(p-1)m_i}.$$

Moreover, if $\mathcal{V} = (\alpha_1, \ldots, \alpha_t, \beta_1, \ldots, \beta_t, \gamma_1, \ldots, \gamma_r)$ is a generating vector for G, then $a_i = p$ if and only if $C \leq \langle \gamma_i \rangle$ and $\gamma_{r+i} \in C$ for all $i \geq 1$.

Proof. The specified action of G/C, the genus level vector, and generating vector are consequences of Lemma 4.1 and Theorems 2.5 and 2.7. To determine the signatures, we use a geometric argument similar to that presented in Proposition 3 of [Wootton 2005]. For brevity, let $K = G/C$. Let

$$\pi_C \colon X \to X/C, \quad \pi_K \colon X/C \to (X/C)/K \cong X/G, \quad \pi_G \colon X \to X/G,$$

denote the quotient maps, and if $F \colon Y \to Y/L$ is a holomorphic quotient map between compact Riemann surfaces and $\alpha \in Y/L$, let $M_F(\alpha)$ denote the multiplicity of a point in the fiber of $\pi_F^{-1}(\alpha)$. By the geometric definition of signature, see Definition 2.1, to determine the signature of G, we need to determine the genus of X/G and for each branch point α_i of π_G, the multiplicity of a point in the fiber $\pi_G^{-1}(\alpha_i)$. By assumption, the genus of G, and also K, is t_1. Therefore, we just need to determine the periods of G.

To determine the periods, we first make some simple observations. We have $\pi_G = \pi_K \circ \pi_C$, and for any $\alpha \in X/G$, it is easy to show that $M_{\pi_G}(\alpha) = M_{\pi_K}(\alpha) \cdot M_{\pi_C}(\beta)$, where $\beta \in \pi_K^{-1}(\alpha)$, see [Miranda 1995, page 53]. Also, since π_C is a cyclic prime cover of X/C of order p, all the periods of C will be equal to p. It follows that if $\alpha \in X/G$ is a branch point of π_G, then it will either have order m_i, order p or order $m_i p$ depending upon whether α is a branch point of π_K, the image of a branch point of π_C, or both. Since every branch point of π_K is also a branch point of π_G, it follows that G has signature

$$(t_1; a_1 m_1, a_2 m_2, \ldots a_r m_r, \underbrace{p, \ldots, p}_{l \text{ times}}),$$

where l denotes the number of branch points of π_G that are not branch points of π_K and $a_i \in \{1, p\}$.

To determine the relationship between the periods of G and C, we examine the orbits of branch points of π_C under the action of K. Suppose that β is a branch point of π_C and let $\alpha = \pi_K(\beta)$. The fiber $\pi_K^{-1}(\alpha)$ coincides with the orbit of β under K and hence has size $|K|/|\operatorname{Stab}_K(\beta)|$, where $\operatorname{Stab}_K(\beta)$ denotes the stabilizer of β under the action of K. However, $|\operatorname{Stab}_K(\beta)| = M_{\pi_K}(\alpha)$; see [Miranda 1995, Theorem 3.4]. It follows that if $\operatorname{Stab}_K(\beta)$ is trivial, there are $|K|/|\operatorname{Stab}_K(\beta)| = p^{n-1}$ points in the fiber $\pi_K^{-1}(\alpha)$. If $\operatorname{Stab}_K(\beta)$ is nontrivial, then $\operatorname{Stab}_K(\beta) = m_i$

for some i and we must have $a_i = p$ in the signature of G. In this case we get $|K|/|\operatorname{Stab}_K(\beta)| = p^{n-1}/m_i$. Since $a_j = 1$ for branch points of π_G that are not the image of a branch point of π_C, and the the number of branch points of π_G that are not branch points of π_K is equal to l, we obtain

$$f = lp^{n-1} + \sum_{i=1}^{r} \frac{(a_i - 1)p^{n-1}}{(p-1)m_i}. \qquad \square$$

As indicated by Corollary 4.2, the only barrier preventing us from constructing such an algorithm is the case where G has genus level vector $(0, 1)$. The groups acting on a surface of genus $\sigma = 1$ with genus level vector $(0, 1)$ are given in Theorem 2.10, so we only need to consider groups acting on surfaces of genus $\sigma \geq 2$.

Theorem 4.4. *Suppose G is a group acting on a surface X of genus $\sigma \geq 2$ with genus level vector $(0, 1)$ with the property that if C is any normal cyclic prime subgroup, then C has genus 1 and G/C has genus vector $(0, 1)$. Then one of the following completely describes G:*

(i) *$G = Q_{2^n}$ acts with signature*

$$(0; \underbrace{2, 2, \ldots, 2}_{r \text{ times}}, 4, 4, 4, 4)$$

and X has genus $\sigma = 2^{n-2}(r+2) + 1$;

(ii) *X has genus 3 and we have one of the following cases:*

    (a) *$G = V_4$ acts with signature $(0; 2, 2, 2, 2, 2, 2)$;*

    (b) *$G = C_4 \times C_2$ acts with signature $(0; 2, 2, 4, 4)$;*

    (c) *$G = D_4$ acts with signature $(0; 2, 2, 4, 4)$;*

    (d) *$G = D_4$ acts with signature $(0; 2, 2, 2, 2, 2)$;*

    (e) *$G = C_4 \times C_4$ acts with signature $(0; 4, 4, 4)$;*

    (f) *G of order 16 with presentation $\langle x, y \mid x^2, y^8, xyx^{-1}y^{-5} \rangle$ acts with signature $(0; 2, 8, 8)$;*

    (g) *G of order 16 with presentation*

$$\langle x, y, z \mid x^2, y^2, z^4, [y, z], [x, z], xyx^{-1}z^{-2}y^{-1} \rangle$$

acts with signature $(0; 2, 2, 2, 4)$;

    (h) *G of order 32 with presentation*

$$\langle x, y, z \mid x^2, y^2, z^8, yzy^{-1}z^{-5}, xyx^{-1}z^{-4}y^{-1}, xzx^{-1}z^{-3}y^{-1} \rangle$$

acts with signature $(0; 2, 4, 8)$.

Proof. Fix a normal cyclic prime subgroup $C \trianglelefteq G$ of genus 1. Since C has genus 1, the quotient space will have genus 1 and so by assumption, the group G/C will have genus vector $(0, 1)$ and act on a surface of genus 1. It follows that we can only have $p = 2$ or $p = 3$. Before we determine G explicitly, we make some simple observations about the structure of G to determine all such groups that can act on surfaces of genus $\sigma \leq 3$.

First, we are assuming that both G and the quotient group G/C have genus vector $(0, 1)$. It follows that G has genus 0, there is a subgroup K with genus 1 of order at least p^2 with $C \leq K$, and consequently G must have order at least p^3. We shall examine K. In [Broughton 1991], all groups and signatures that can act on surfaces of genus 2 and 3 are classified. By simply checking these lists, we see that for genus 2 no such K exists, and for genus 3, no such K exists for $p = 3$. To determine all 2-groups acting on genus 3 surfaces with these properties, we simply proceed through the list in [Broughton 1991] to extract all the groups and signatures that satisfy the requirements.

Henceforth, we shall assume that the genus of X is at least 4. We shall show that G has a unique cyclic prime subgroup. Suppose not and let H denote a cyclic prime subgroup different from C. Then the group $L \trianglelefteq \langle C, H \rangle$ is elementary abelian of order p^2. By Theorem 3.6, the genus of L must be 0, so L will have signature

$$(0; \underbrace{p, p, \dots, p}_{r \text{ times}}) \quad \text{for some } r.$$

Let $\mathcal{V}$ denote a corresponding generating vector for L. Now if $K \leq L$ is any nontrivial proper subgroup, by assumption, the genus of K must be 0 or 1. Observe that the genus of $K \leq L$ is completely determined by the number of elements of $\mathcal{V}$ with nontrivial image under the quotient map $\rho \colon L \to L/K$. Specifically, if the genus of K is 0, precisely two generators will have nontrivial image. If the genus of K is 1 and $p = 2$, four will have nontrivial image; if $p = 3$, three will have nontrivial image. We consider the cases $p = 2$ and $p = 3$ separately.

If $p = 2$, then 4 elements of $\mathcal{V}$ will have nontrivial image under $\rho \colon L \to L/C$. It follows that all remaining elements of $\mathcal{V}$ lie in C, and hence will have nontrivial image under $\rho \colon L \to L/K$ for any other nontrivial subgroup $K \leq L$. This can only happen if $r = 6$ and each nontrivial subgroup $K \leq L$ contains two elements of $\mathcal{V}$, or $r = 5$ and two subgroups each contain 2 and the other contains 3. In each of these cases, we apply the Riemann–Hurwitz formula and find that either $\sigma = 2$ or $\sigma = 3$, counter to our assumption that $\sigma \geq 4$.

If $p = 3$, we use a similar argument. Specifically, the only possible signature for L is $(0, 3, 3, 3, 3)$, where a $(0, 3, 3, 3, 3)$-generating vector for L has one element in each nontrivial subgroup K of L. However, it is easy to show that no such generating vector for L exists and hence no such group exists. We shall henceforth assume that G has a unique cyclic prime subgroup.

Since G has a unique cyclic prime subgroup, we can use [Robinson 1995, Theorem 5.3.6] and conclude that either $G = Q_{2^n}$ or $G = C_{p^n}$. We consider each of these cases. Suppose first that $G \cong C_{p^n}$ and let K be the subgroup of maximal order of G that has genus 1. Then the signature of K will be $(1; p, \ldots, p)$. Since G/K will have genus level vector (0) and act on a surface of genus 1, it must either be C_4, or cyclic of prime order 2 or 3. Using the toroidal signatures and Theorem 4.3, we can reconstruct the signature of G for each of these cases. If G/K is cyclic of order 3, then G will have signature $(0; 3, \ldots, 3, 3a, 3b, 3c)$, where a, b and c are either 1 or 3. Since G must be generated by elliptic generators, it follows that G can have order at most 9 contradicting the fact that $|G| \geq p^3$. Likewise, if G/C is cyclic of order 2, then G will have signature $(0; 2, \ldots, 2, 2a, 2b, 2c, 2d)$, where a, b, c and d are either 1 or 2. It follows that G has order at most 4, again a contradiction. Finally, if $G/K = C_4$, then there would exist L with $L > K$ and $G/L = C_2$, which we have already shown cannot happen.

Now suppose that $G \cong Q_{2^n}$ and fix the presentation

$$\langle x, y \mid x^{2^{n-1}}, x^{2^{n-2}} y^{-2}, yxy^{-1}x \rangle$$

for G. The group $L = \langle x \rangle$ is a cyclic subgroup of order 2^{n-1}, where $n \geq 3$. By our previous observations, L must have genus 1. Similar to the last case, using the fact that $G/L = C_2$ and has genus level vector (0), we can reconstruct the signature for G. Specifically, the signature for G will be $(0; 2, 2, \ldots, 2, 2a, 2b, 2c, 2d)$, where $a, b, c,$ and d are either 1 or 2. Any generating vector for G will be of the form $(\gamma_1, \ldots, \gamma_r, \gamma_{r+1}, \gamma_{r+2}, \gamma_{r+3}, \gamma_{r+4})$, where $\gamma_{r+i} \notin L$ for $1 \leq i \leq 4$. However, if any γ_{r+i} has order 2, then by uniqueness of C, it will lie in C and hence L. It follows that each γ_{r+i} has order 4 and so the only possible signature for G is $(0; 2, 2, \ldots, 2, 4, 4, 4, 4)$. We finish by showing that this signature is admissible for every possible value of r.

We know that the product $\gamma_1 \gamma_2 \cdots \gamma_r$ is either e or y^2. We set

$$\gamma_{r+1} = yx, \gamma_{r+2} = y^3 x, \gamma_{r+3} = y.$$

If the product is e, we set $\gamma_{r+4} = y^3$; if it is y^2, we set $\gamma_{r+4} = y$. In either case, the generators multiply to e. Moreover, $x = \gamma_{r+3}\gamma_{r+2}$ and $y = \gamma_{r+3}$ generate Q_{2^n} and thus, for each possible r, we have constructed a generating vector. Application of Theorem 2.7 shows, for this generating vector, all subgroups of L have genus 1 and the Riemann–Hurwitz formula gives the signature for X.   □

Putting our work together, we can now outline the inductive method to determine all p-groups that can act on a compact Riemann surface dependent upon the genus level of the group. We note that all groups are known for genus 0 and 1 surfaces, so we restrict to surfaces of genus $\sigma \geq 2$. Fix an n and assume that we know all

p-group actions for all p-groups with genus level $k \le n - 1$. To determine the possible p-groups actions, with genus level n, we do the following:

(i) If $n = 2$, determine each possible p group G with genus level vector $(0, 1)$ with the property that if C is any normal cyclic prime subgroup, then the group G/C has genus level vector $(0, 1)$. This can be done using Theorem 4.4.

(ii) Else, any such group G of order p^f admits a cyclic subgroup of order p such that G/C is a group of automorphisms of order p^{f-1} acting on a surface with a strictly shorter genus level vector than the genus level vector of G. In particular, by assumption, we know the structure of every possible $K = G/C$. Therefore, to determine G, and its signature, we can do the following:

(a) Determine the solutions of the short exact sequence

$$1 \to C \to G \to K \to 1$$

for each possible K.

(b) For a given G and K from (a), each possible signature $\mathcal{T}$ of G can be determined from K using Theorem 4.3. Specifically, we run over all the possibilities by choosing $a_i = 1$ or p for each i.

(c) For a G and signature $\mathcal{T}$ from (b), we can determine all possible generating vectors and check, for each vector, that G has genus level n. If no valid generating vector exists, then there does not exist an action by G with this signature and with genus level n.

5. Examples

We finish with some explicit examples to illustrate our results.

Example 5.1. It is easy to determine all genus level 1 group actions of a cyclic prime group G of order p on a surface of genus $\sigma \ge 0$. Specifically, the signature for such a group will be

$$(t; \underbrace{p, \ldots, p}_{r \text{ times}}), \quad \text{where } \sigma = 1 + p(t - 1) + \frac{r(p - 1)}{2}.$$

For $\sigma = 0$ or 1, Theorem 2.10 gives all possible signatures. For $\sigma \ge 2$, it is easy to show that a

$$(t; \underbrace{p, \ldots, p}_{r \text{ times}})\text{-generating vector for } G$$

exists for all primes p, provided $r \ne 1$ and when $p = 2$, r is even. The genus on which such a G acts is calculated using the Riemann–Hurwitz formula.

Example 5.2. We can use our results and Example 5.1 to classify all group actions by cyclic groups of order p^2 for any prime p with genus level 2 on surfaces of genus

$\sigma \geq 2$. Let G be such a group. If C is the cyclic prime subgroup of G, Example 5.1 shows the signature of G/C is

$$(t; \underbrace{p, \ldots, p}_{r \text{ times}}) \quad \text{with } r \neq 1$$

and if $p = 2$, then r is even. Using Theorem 4.3, since $C \leq \langle \gamma \rangle$ for any nontrivial $\gamma \in G$, it follows that there are r elements of order p^2 in the signature of G. Therefore, the possible signatures of G are

$$(t, \underbrace{p, \ldots, p}_{r_1 \text{ times}}, \underbrace{p^2, \ldots, p^2}_{r \text{ times}})$$

for certain values of r_1. Using Theorem 2.7, the genus level vector of such an action will be (t, t_1), where $t_1 = 1 + p(t-1) + \frac{1}{2}r(p-1)$. We shall show that such a G exists for every possible r_1 and t. To show this, we need to show that there exists a

$$(t, \underbrace{p, \ldots, p}_{r_1 \text{ times}}, \underbrace{p^2, \ldots, p^2}_{r \text{ times}})\text{-generating vector for } G.$$

This can be done in a similar way to the final argument in Theorem 3.6. The genus on which such a G acts is calculated using the Riemann–Hurwitz formula.

Example 5.3. We can use our results and the Example 5.1 to classify all elementary abelian group actions of order p^2 for any prime p with genus level 2 on surfaces of genus $\sigma \geq 2$. Let G be such a group and let C be a cyclic prime subgroup of G. Using Example 5.1, the signature of G/C is

$$(t; \underbrace{p, \ldots, p}_{r \text{ times}}).$$

According to Theorem 4.3, the fact that all elements of G have order p implies the signature of G is

$$(t, \underbrace{p, \ldots, p}_{r_1 \text{ times}}, \underbrace{p, \ldots, p}_{r \text{ times}})$$

for certain values of r_1. Using Theorem 2.7, the genus level vector of such an action is (t, t_1), where

$$t_1 = 1 + p(t-1) + \frac{r(p-1)}{2}.$$

To determine for which values of t and r_1 such a G exists, we need to construct generating vectors, or show that no such generators exists. We do this on a case-by-case basis. For the remainder of the proof, assume that $G = \langle x, y \rangle$ and let $n = r + r_1$ denote the number of elliptic generators.

First, suppose that $n = 0$. Then $t \geq 2$ since we are assuming $\sigma \geq 2$. A $(t; -)$-generating vector for G is the vector $(x, y, 1, \ldots, 1)$. Using Theorem 2.7, the genus of every possible nontrivial subgroup is t_1. It follows that such a G exists for every possible choice of $t \geq 2$ with $n = 0$.

Now suppose that the number of elliptic generators is $n > 0$ and $t \neq 0, 1$. By assumption, G has genus level 2 and so by Proposition 3.2, every nontrivial subgroup of G must have genus t_1. Consider a generating vector

$$(\alpha_1, \ldots, \alpha_t, \beta_1, \ldots, \beta_t, \gamma_1, \ldots, \gamma_n)$$

for G. By Theorem 2.7, the genus of each nontrivial $C \leq G$ is completely determined by the number of $\gamma_i \in C$. In particular, every nontrivial subgroup $C \leq G$ has the same genus provided each contains the same number of elliptical generators, γ_i. Since there are $p+1$ nontrivial subgroups of G, it follows that the only possible signature for G is

$$(t, \underbrace{p, \ldots, p}_{n \text{ times}}),$$

where $n = r(p + 1)/p$. For any such r, and $t \geq 0$, it is easy to construct a generating vector for G satisfying these properties by generalizing the final argument in Theorem 3.6. For example, if r is even and $x_1, \ldots, x_{p+1}$ is a set of nontrivial elements from distinct subgroups of G, then

$$(\underbrace{1, \ldots, 1}_{2t \text{ times}}, \underbrace{x_1, x_1^{-1}, \ldots, x_1, x_1^{-1}}_{(r/2) \text{ times}}, \ldots, \underbrace{x_{p+1}, x_{p+1}^{-1}, \ldots, x_{p+1}, x_{p+1}^{-1}}_{(r/2) \text{ times}})$$

is a generating vector for G. It follows that such a G exists for every possible choice of $t \geq 2$ provided $n = r(p + 1)/p$, and no such group exists otherwise.

The next case we consider is when $t = 1$. In this case, G could have subgroups with genus 1 as well as with genus t_1. If all the subgroups of G of order p have genus t_1, then it is easy to imitate the proof of the previous case to show that a generating vector for G exists only if $n = r(p + 1)/p$. Therefore, we only need consider the case when at least one of the subgroups of G of order p has genus 1. Let $C \leq G$ be a subgroup with genus 1. By Proposition 3.2, then $\gamma_i \in C$ for all i. It follows that for any other subgroup $K \neq C$, $\gamma_i \notin K$ for all i. Therefore, using Theorem 2.7, the genus of every subgroup $K \neq C$ of order p will be the same. Without loss of generality, suppose that $C = \langle x \rangle$. It is easy to construct a generating vector for G satisfying these properties by generalizing the final argument in Theorem 3.6 and a generating vector always exists unless $p = 2$ and n is odd.

The last case we need to consider is $t = 0$. As above, if every subgroup of order p has genus t_1, then a generating vector for G exists only if $n = r(p+1)/p$. Therefore, we only need consider the case when at least one of the subgroups of G of order

p has genus 0. In [Wootton 2007b], all G containing more than one cyclic prime subgroup with genus 0 were classified and there are only two possibilities for G. In the first case, G has signature $(0; p, p, p)$ and generating vector $(x, y, (xy)^{-1})$ and three genus 0 subgroups - the ones generated by x, y, and xy. Using Theorem 2.7, all other cyclic subgroups of G will have the same genus, and hence G has genus level 2. In the second case, G has signature $(0; p, p, p, p)$ and generating vector (x, y, x^{-1}, y^{-1}) and two genus 0 subgroups - the ones generated by x and y. Using Theorem 2.7, all other cyclic subgroups of G will have the same genus, and hence G has genus level 2. Therefore, the last case we need to consider is when $t = 0$ and G contains a unique cyclic subgroup of genus 0. In this case, if C is the cyclic subgroup with genus 0 and $(\gamma_1, \ldots, \gamma_n)$ is a generating vector for G, then by Theorem 4.3, $\gamma_i \in C$ for all but two values of i, say $n - 1$ and n. As remarked previously, the only way two other subgroups C_1 and C_2 can have the same genus is if they contain the same number of γ_i. This occurs exactly when G contains just two nontrivial, proper subgroups other than C, and each subgroup contains one of γ_{n-1} or γ_n. Such restrictions force $p = 2$. Through our observations, the only possible generating vectors of G are of the form

$$(\underbrace{x, \ldots, x}_{n-2\,\text{times}}, (xy), y).$$

Clearly this defines a generating vector when n is odd and does not for n even, and thus such a G exists only under these circumstances.

Acknowledgement

References

[Benim 2008] R. Benim, "Classification of quasplatonic abelian groups and signatures", *Rose-Hulman Undergraduate Math. J.* **9**:1 (2008).

[Breuer 2000] T. Breuer, *Characters and automorphism groups of compact Riemann surfaces*, London Math. Soc. Lecture Note Ser. **280**, Cambridge University Press, Cambridge, 2000. MR 2002i: 14034 Zbl 0952.30001

[Broughton 1991] S. A. Broughton, "Classifying finite group actions on surfaces of low genus", *J. Pure Appl. Algebra* **69**:3 (1991), 233–270. MR 92b:57021 Zbl 0722.57005

[Bujalance et al. 2003] E. Bujalance, F. J. Cirre, J. M. Gamboa, and G. Gromadzki, "On compact Riemann surfaces with dihedral groups of automorphisms", *Math. Proc. Cambridge Philos. Soc.* **134**:3 (2003), 465–477. MR 2004c:20086 Zbl 1059.30030

[Fuertes and González-Diez 2007] Y. Fuertes and G. González-Diez, "On unramified normal coverings of hyperelliptic curves", *J. Pure Appl. Algebra* **208**:3 (2007), 1063–1070. MR 2007i:14026 Zbl 1123.14019

[Harvey 1966] W. J. Harvey, "Cyclic groups of automorphisms of a compact Riemann surface", *Quart. J. Math. Oxford Ser.* (2) **17** (1966), 86–97. MR 34 #1511 Zbl 0156.08901

[Kallel and Sjerve 2001] S. Kallel and D. Sjerve, "Genus zero actions on Riemann surfaces", *Kyushu J. Math.* **55**:1 (2001), 141–164. MR 2002m:14022 Zbl 0997.30035

[Miranda 1995] R. Miranda, *Algebraic curves and Riemann surfaces*, Graduate Studies in Mathematics **5**, American Mathematical Society, Providence, RI, 1995. MR 96f:14029 Zbl 0820.14022

[Robinson 1995] D. Robinson, *A course in the theory of groups*, Grad. Texts in Math. **80**, Springer, 1995. Zbl 0836.20001

[Singerman 1970] D. Singerman, "Subgroups of Fuschian groups and finite permutation groups", *Bull. London Math. Soc.* **2** (1970), 319–323. MR 43 #7519

[Tyszkowska and Weaver 2008] E. Tyszkowska and A. Weaver, "Exceptional points in the elliptic-hyperelliptic locus", *J. Pure Appl. Algebra* **212**:6 (2008), 1415–1426. MR 2009d:30093 Zbl 1137.14020

[Wootton 2005] A. Wootton, "Non-normal Belyĭ p-gonal surfaces", pp. 95–108 in *Computational aspects of algebraic curves* (Moscow, ID, 2005), edited by T. Shaska, Lecture Notes Ser. Comput. **13**, World Sci. Publ., Hackensack, NJ, 2005. MR 2006g:14054

[Wootton 2007a] A. Wootton, "Defining equations for cyclic prime covers of the Riemann sphere", *Israel J. Math.* **157** (2007), 103–122. MR 2009b:30084 Zbl 1109.30036

[Wootton 2007b] A. Wootton, "The full automorphism group of a cyclic p-gonal surface", *J. Algebra* **312**:1 (2007), 377–396. MR 2008c:14043 Zbl 1117.30034

quicksilver.falcon@gmail.com   *University of Oregon, Department of Mathematics, Fenton Hall, 1222, Eugene, OR 97403, United States* http://uoregon.edu/~arbo

kbenkowski@hotmail.com   *Western Michigan University, Department of Mathematics, 3319 Everett Tower, Kalamazoo, MI 49008, United States*

coateb2@rpi.edu   *Rensselaer Polytechnic Institute, School of Architecture, Greene Building, 110 8th street, Troy, NY 12180, United States*

nordstro@up.edu   *University of Portland, Department of Mathematics, 5000 North Willamette Blvd., Portland, OR 97203, United States* http://faculty.up.edu/nordstro/

cmp02006@mymail.pomona.edu   *Pomona College, Department of Mathematics, 610 North College Avenue, Claremont, CA 91711, United States*

wootton@up.edu   *University of Portland, Department of Mathematics, 5000 North Willamette Blvd., Portland, OR 97203, United States* http://faculty.up.edu/wootton/

A statistical study of extreme nor'easter snowstorms

Christopher Karvetski, Robert B. Lund and Francis Parisi

(Communicated by Sat Gupta)

This short paper studies the statistical characteristics of extreme snowstorms striking the eastern seaboard of the United States — the so-called nor'easters. Poisson regression techniques and extreme value methods are used to estimate return periods of storms of various snow volumes. Return periods of several memorable events are estimated, including the superstorm of 1993, the North American blizzard of 1996, and the blizzard of 1888. While nor'easters are found to occur more frequently in late winter than early winter, no evidence of increasing/decreasing storm frequencies in time or dependencies on the North Atlantic oscillation is found.

1. Introduction

A nor'easter is a large-scale winter storm that impacts the east coast of the United States. A nor'easter can drop copious amounts of snow and may also cause flood and wind damage. Nor'easters occur from late fall through early spring. The superstorm of 1993 (March 12–15), for example, was the largest snowstorm affecting the United States in the last century. This storm deposited over 60 inches of snow in some places, is blamed for 300 fatalities, and caused an estimated six to ten billion dollars of damage.

While nor'easters are sometimes referred to as *winter hurricanes*, literature studying their frequency properties is sparse when compared to that for *summer hurricanes*. The goal here is to quantify the nor'easter snowstorm hazard. The timing of this work coincides with attempts by several insurance risk modeling firms to quantify the hazard.

The total snow volume of each storm will be used as the measure of storm severity. Return periods for various snow volume accumulations will then be estimated. A snow volume return period is how long one waits, on average, until a nor'easter with a preset snow volume or greater strikes. For example, the superstorm of 1993

is also nicknamed the *Storm of the Century*, giving connotations of a 100-year storm. Later, we will see that this storm was more than a 100-year event.

2. The data

The data for this analysis were taken from [Kocin and Uccellinni 2004a; 2004b]. These references contain much information about the individual storms. Nor'easter documentation is scant when compared to that for summer hurricanes (for the latter, see [Blake et al. 2005; Parisi and Lund 2008]). Our data consists of 65 storms occurring during the years 1953–2003 inclusive; the record for this time period is complete. The individual storms are chronologically listed in Table 1; no storms occurred in 1953, 1954, or 1955. As the pre-1953 record is incomplete, we cannot include memorable pre-1953 storms (such as the New England blizzard of 1888), without biasing the overall results.

For each storm in the table, Kocin and Uccellinni 2004a report the areas that accumulated more than four inches, ten inches, twenty inches, and thirty inches, respectively. For each storm, we compute a crude volume estimate via the following rubric. For the superstorm of 1993, an area of 386.0×10^3 squared miles experienced snow accumulations of at least four inches, an area of 283.5×10^3 squared miles saw accumulations of at least ten inches, an area of 142.4×10^3 squared miles had accumulations of at least twenty inches, and an area of 12.9×10^3 squared miles received accumulations of over thirty inches. A volume estimate for the superstorm of 1993 is hence

$$386 \times 4 + 283.5 \times (10 - 4) + 142.4 \times (20 - 10) + 12.9 \times (30 - 20) = 4798,$$

where the units on the volume are 10^3 inches times squared miles. The volumes can be converted to cubic meters upon multiplication by 6.5024×10^7, but we will not do this as the analysis below is invariant of any linear scale change on the volume units. Because of this, volume units will be henceforth suppressed for simplicity.

Whereas our estimated volume underestimates actual values (areas receiving less than 4 inches of snow, for example, are not included in the volume estimates), the estimated volumes are reasonable measures of storm intensity; moreover, all volumes are underestimated in the same way, which makes storm-by-storm comparisons meaningful. The smallest volume was 291.2 and the largest volume was 4798.0. On average, there are about 1.27 storms per season. The number of storms in a single season ranges from zero to five.

We emphasize that this data only contains large-scale nor'easters and not more localized events such as Great Lake effect snowfalls. Alberta Clipper-type storms, whose snowfall volumes tend to be much less than nor'easters, are also not represented in this data.

Date (midstorm)			Sq. miles covered with				NAO	Rough
yr	mo	day	4 in	10 in	20 in	30 in	average	volume
1956	3	16	195.5	92.3	0	0	−1.07	1335.8
1956	3	18	64.9	28.6	2.6	0	−1.07	457.2
1957	12	4	87.2	9.4	0	0	0.073	405.2
1958	2	15	282.6	129.2	20.2	3.4	0.073	2141.6
1958	3	19	146.7	62.1	13.8	3.5	0.073	1132.4
1959	3	12	215.3	121.1	7.7	0	−0.13	1664.8
1960	2	14	353.9	142.1	23.3	0	0.093	2501.2
1960	3	3	590.4	140.8	7.6	0	0.093	3282.4
1960	12	12	302.9	78.5	0.6	0	1.993	1688.6
1961	1	19	144.9	62.3	5.7	0	1.993	1010.4
1961	2	3	369.3	114	19.4	1.4	1.993	2369.2
1961	12	24	105.5	14.8	0	0	0.497	510.8
1962	2	14	101.4	33.8	0.4	0	0.497	612.4
1962	3	6	148.6	70	19.3	0	0.497	1207.4
1963	12	22	374.2	51.3	0	0	−0.763	1804.6
1964	1	12	356.5	129.6	10.3	0	−0.763	2306.6
1964	2	19	169.7	53.4	3.5	0	−0.763	1034.2
1965	1	16	214.5	15.3	0	0	−1.42	949.8
1966	1	22	296.4	145.1	6.6	0	−0.05	2122.2
1966	1	30	371.4	111.7	12.3	1.5	−0.05	2293.8
1966	12	24	292.2	89.8	9.9	0	1.14	1806.6
1967	2	6	246	50.9	0	0	1.14	1289.4
1967	3	21	62.3	7	0	0	1.14	291.2
1969	2	9	107.5	66.4	11.6	0	−2.177	944.4
1969	2	25	101.7	48.4	40.8	24.2	−2.177	1347.2
1969	12	26	250.6	138.7	37.6	0	−0.107	2210.6
1970	12	31	151	46.4	4.4	0	−0.267	926.4
1971	3	4	195.7	101.6	23.3	0	−0.267	1625.4
1971	11	26	163.4	73.4	6.6	0	0.013	1160
1972	2	19	206.3	140.9	13.5	0	0.013	1805.6
1978	1	17	364.4	122.1	0	0	−0.593	2190.2
1978	1	20	295.2	167.7	8.3	0	−0.593	2270
1978	2	6	220.2	132.3	30.7	0.9	−0.593	1990.6
1979	2	18	304	88.2	4.3	0	−1.973	1788.2

Table 1. The nor'easter data (continued on next page).

Date (midstorm)			Sq. miles covered with				NAO	Rough
yr	mo	day	4 in	10 in	20 in	30 in	average	volume
1982	1	14	382.2	133.9	0	0	−0.223	2332.2
1982	4	6	258.3	79.3	2.1	0	−0.223	1530
1983	2	11	157.1	112.6	33.7	0.9	2.07	1650
1984	3	8	120.9	54.6	0	0	1.697	811.2
1984	3	28	124.6	53.3	2.1	0	1.697	839.2
1987	1	1	164.6	76.6	0	0	0.353	1118
1987	1	22	286.9	153.7	2	0	0.353	2089.8
1987	1	25	74.3	38	0	0	0.353	525.2
1987	2	22	61.3	28.3	0.3	0	0.353	418
1988	1	7	488.5	129.7	0	0	−0.13	2732.2
1990	12	26	166	12.7	0	0	0.73	740.2
1992	12	11	118.7	61.6	21.5	0	1.41	1059.4
1993	3	13	386	283.5	142.4	12.9	1.41	4798
1994	1	4	222.3	76.4	10.5	0	1.173	1452.6
1994	2	9	280	57.7	4.4	0	1.173	1510.2
1994	3	3	165.4	109.1	0	0	1.173	1316.2
1995	2	3	200.1	98	0	0	2.897	1388.4
1995	12	20	260.3	85.4	0	0	−2.24	1553.6
1996	1	7	313.8	200.1	90.2	15.1	−2.24	3508.8
1996	2	3	157.3	44.1	0.9	0	−2.24	902.8
1996	2	16	136.7	12.2	0	0	−2.24	620
1997	3	31	76.4	32	13.1	3.1	−0.463	659.6
1996	1	7	313.8	200.1	90.2	15.1	−2.24	3508.8
1996	2	3	157.3	44.1	0.9	0	−2.24	902.8
1996	2	16	136.7	12.2	0	0	−2.24	620
1997	3	31	76.4	32	13.1	3.1	−0.463	659.6
1999	3	14	180.3	58.8	1.4	0	1.55	1088
2000	1	25	205.6	74.2	0.3	0	2.283	1270.6
2000	12	30	103.8	56.5	3.7	0	−0.44	791.2
2001	3	5	161.1	105.1	30.4	1.8	−0.44	1597
2002	12	4	269.7	6.1	0	0	0.17	1115.4
2002	12	25	345.3	91.3	13.8	4.4	0.17	2111
2003	1	3	211.1	77.4	11	0	0.17	1418.8
2003	2	6	88.4	6.1	0	0	0.17	390.2
2003	2	16	303.5	142	51.9	2.7	0.17	2612

Table 1 (continued). The nor'easter data.

3. Arrival properties of nor'easters

To estimate return periods, we need to model the storm arrival times. Following [McDonnell and Holbrook 2004] and [Parisi and Lund 2008], the storm count in season t is modeled as a Poisson random variable with mean λ_t, where

$$\lambda_t = \exp\left(\beta_0 + \alpha t + \beta_1 \text{NAO}_t\right).$$

Here, the parameter α allows for a linear trend in the storm counts (we will assess whether or not this parameter is zero below) and the $\beta_1 \text{NAO}_t$ component allows for possible influences of the North Atlantic oscillation (NAO). The average NAO index over December, January, and February during season t is used for NAO_t. Kocin and Uccellinni [2004a] suggest that the NAO may influence nor'easter storm counts (see [Van den Dool et al. 2006] for generalities about the NAO and North American climate).

Poisson regression techniques were used to fit the above model. The estimated parameters are $\hat{\alpha} = 0.008$ and $\hat{\beta}_1 = -0.0149$. Intervals of 95% confidence for α and β are $[-0.009, 0.025]$ and $[-0.339, 0.041]$. As both of these intervals contain zero, these two parameters are statistically indistinguishable from zero with 95% confidence. All possible subsets of the regression model structure were also fitted and produced insignificant parameters at the 95% level. Thus, we do not find evidence of trends or NAO influences in the storm counts. A Kolmogorov–Smirnov test fails to reject a Poisson distribution for the annual storm counts at the 95% level. In short, the annual nor'easter storm counts pass as statistical white noise with a Poisson marginal distribution with a mean of approximately 1.27 storms per season.

Although the number of storms from season to season appears time-homogeneous, the storms do not arrive uniformly within a season. To investigate this aspect, the kernel intensity estimate in Figure 1 was constructed. This graphic presents a probabilistic description of when storms occur within a season. As the earliest storm in our data record occurred on November 26 (and the latest on April 6), we have chosen to measure a storm's arrival date as the number of days after October 1 that the storm's midpoint took place on (the midpoint, or the average of the storms' beginning and ending dates, is used since some storms last multiple days). Figure 1 displays estimates of the intensity function $\hat{\lambda}(t)$ at time t defined by

$$\hat{\lambda}(t) = \frac{1}{N_{\text{yr}}} \sum_{i=1}^{N_{\text{st}}} h^{-1} K\left(\frac{t - d_i}{h}\right), \quad 0 \le t < 365.$$

Here, $N_{\text{yr}} = 51$ is the number of seasons of data, $N_{\text{st}} = 65$ is the total number of storms, K is the Gaussian kernel function

$$K(x) = \frac{\exp(-x^2/2)}{\sqrt{2\pi}}, \quad -\infty < x < \infty,$$
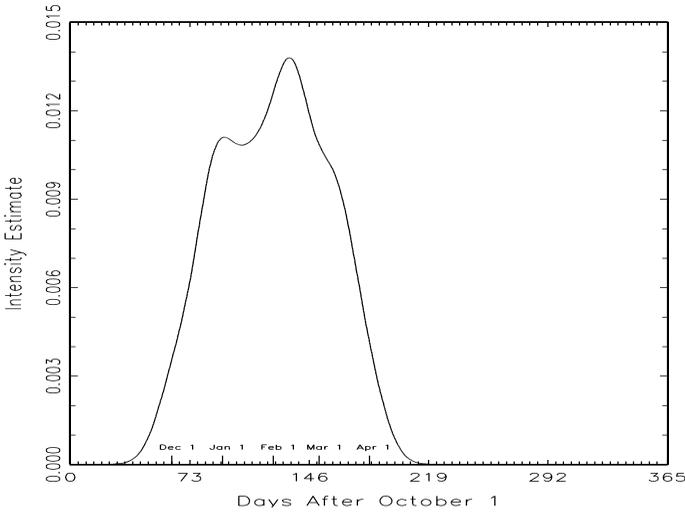
Figure 1. Estimated seasonal intensity function.

$h = 10$ is a bandwidth parameter that controls the amount of smoothing done (see [Sheather and Jones 1991] for discussion about selecting an appropriate h), and d_i is the number of days after October 1 that the midpoint of the ith storm occurs on for $1 \leq i \leq N_{\text{st}}$. The interpretation of $\hat{\lambda}(t)$ is that the probability of a nor'easter occurring in the time interval $(t, t + h]$ is approximately $\hat{\lambda}(t)h$ for small h.

The intensity function in Figure 1 peaks at about 133.8 days after October 1, or around February 11. Hence, nor'easters are slightly more likely to occur after midwinter (which is about January 20) than before midwinter. Though we cannot offer a meteorological explanation for this pattern, we note that summer hurricane arrivals also peak in the later half of their season.

4. Return periods

Our next task lies in estimating the return periods of nor'easters. The return periods derived below apply to the northeastern United States as a whole and not to a specific geographic location. Elaborating, a return period of a twenty inch snowfall for New York City should be estimated from snowfall data taken in New York City proper (whose record is much longer than our 51 years) and not the nor'easter data set in Table 1.

The return period of a volume x storm is simply how long one waits, on the average, until a storm occurs that deposits a snow volume of x or more. We measure all return periods from October 1. For example, one waits an average of 839.5 days after October 1 of any calendar year for a 2.3 year nor'easter to occur.

To estimate return periods, we need to model the snow volumes of the storms. For this, we appeal to the peaks over threshold paradigm (see [Embrechts et al. 1997] for general discussion). Elaborating, there is very general mathematical justification for fitting the Pareto cumulative distribution

$$P(V_i - u \le x | V_i > u) = 1 - \left(1 + \xi \frac{x}{\sigma}\right)_+^{-1/\xi}, \quad x \ge 0, \tag{4.1}$$

to the nor'easter snow volumes $\{V_i\}_{i=1}^{N_{st}}$. The three parameters in the Pareto model are the shape parameter ξ, the scale parameter σ, and the threshold $u > 0$. In Equation (4.1), $x_+ = \max(x, 0)$. The threshold $u = 290$ is selected. This threshold allows all nor'easters in Table 1 to be considered and passes the rudimentary diagnostic checks suggested in [Davison and Smith 1990]. The maximum likelihood parameter estimates of the other Pareto parameters and 95% confidence intervals are $\hat{\xi} = -0.2899$ ($[-0.436, -0.144]$) and $\hat{\sigma} = 1544.931$ ($[1174.10, 2032.90]$). A Kolmogorov–Smirnov goodness of fit test fails to reject the fitted Pareto distribution with a p-value of 0.2175. Due to the support set of the distribution in (4.1), the negative estimate of ξ implies that snow volumes of nor'easters cannot exceed $u - \sigma/\xi$, which is approximately 5619.2 in this case. Finally, we regressed the snow volumes on the average December, January, and February NAO index to ascertain if the NAO influences snow volumes (Section 3 shows that NAO does not influence storm counts). No statistically significant relationship was found.

With the above model, return periods can be estimated via simulation. One season of the process is simulated as follows. First, a nonhomogeneous Poisson process with the intensity function in Figure 1 is simulated. This intensity function integrates to approximately 1.27 over an annual cycle, which is the mean number of storms per season. For each generated storm in this cycle, we then simulate a snow volume from the fitted Pareto model.

For a volume of x, the waiting time of the simulation is the elapsed time, measured from October 1, until the first storm whose snow volume exceeds x is encountered. If no snow volume of x is encountered in this season, then one adds a year to the waiting time and simulates another season. This process is repeated until a snow volume of x or more is encountered.

The above scheme generates one fair draw of a "level x" waiting time. Every time a snow volume of x or more is encountered, the simulation run is over and the next run starts from scratch (October 1). An estimate of the return period is based on empirically averaging many independent waiting times.

Simulating the necessary processes is reasonably easy; see [Ross 2002] for general detail. One aspect, however, does merit some elaboration: how to generate a Poisson process from the intensity function in Figure 1. This is done by Poisson thinning. Specifically, to generate one season of storm arrival times, we generate a

Storm name	Volume	Estimated return period (years)
Blizzard of 1888	1837.0	2.4
February blizzard of 1978	1990.6	2.8
Presidents' Day storm of 2003	2612.0	5.5
North American blizzard of 1996	3508.8	19.0
Superstorm of 1993	4798.0	500.1

Table 2. Estimated return periods for some historical storms.

time-homogeneous Poisson process with arrival rate λ^* satisfying $\hat{\lambda}(t) \leq \lambda^*$ for all $t \in [0, 365]$. If a storm occurs at time t in the time-homogeneous process, we then independently flip a coin with heads probability $\lambda(t)/\lambda^*$. If the coin is heads, the storm is kept; if the coin is tails, we disregard the storm. The "thinned process" of retained storms is indeed a sample from a nonhomogeneous Poisson process with arrival rate $\hat{\lambda}(t)$ at time t (see [Ross 1996, page 80] for a proof).

Figure 2 plots estimated return periods for various volume levels as estimated by the model. For example, a snow volume of 4250 has an estimated return period of 82.4 years. This return period was estimated by averaging one hundred thousand independent waiting time draws; hence, there is little simulation error.

While there is little simulation error in this return period estimate, significant model uncertainties may well be present. One could use asymptotic normality of the Pareto parameter estimators to quantify the Pareto uncertainties in the return period estimates (the uncertainties in the Poisson arrival cycle are somewhat harder
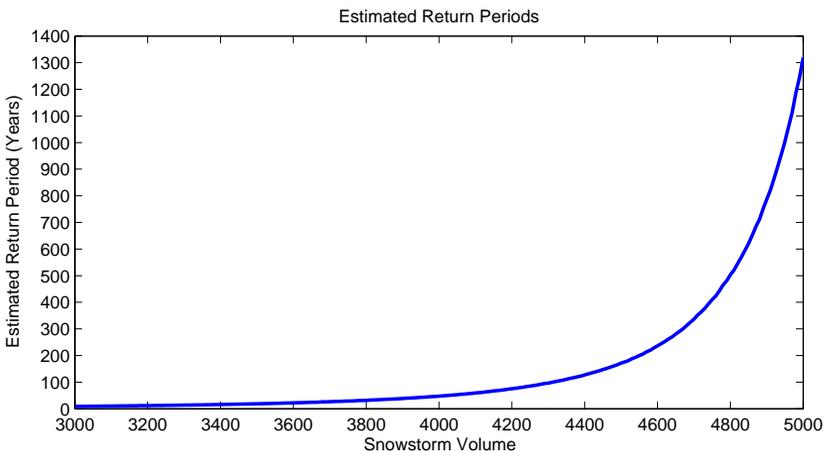
Figure 2. Estimated return periods by snow volume.

to quantify); however, such schemes do not appear to work well in practice (see [Tajvidi 2003] for discussion and possible remedies). While we will not delve into model uncertainties further, Bayesian methods may be promising.

The graphic in Figure 2 shows that a nor'easter with a volume of 3000 occurs about once every nine years on average; a hundred-year volume is about 4300. The return periods increase rapidly for volume levels above 4000. In fact, a volume of 4800 (which is only 2 more than the superstorm of 1993) has a return period of about 500 years. Indeed, it appears that the superstorm of 1993 deserves its "Storm of the Century" nickname.

Table 2 shows estimated return periods of selected historical storms. The blizzard of 1888 has a return period of about 2.4 years, a relatively common event given its historical lore. This estimate is, however, reasonable: while dropping very heavy snow, the storm did not affect a large area. The recent Presidents' Day blizzard of 2003 has a return period of about 5.5 years. The only two storms in our data set with volumes above 3500 are the North American blizzard of 1996 (a volume of 3508.8) and the superstorm of 1993 (a volume of 4798). The return period for the North American blizzard of 1996 is estimated at 19.0 years and the superstorm of 1993's return period is estimated at a whopping 500.1 years. The superstorm of 1993 is clearly an extreme event; indeed, its volume lies close to the statistical boundaries of what is deemed possible. Whereas this return period estimate likely contains considerable error due to model uncertainty, it was indeed an impressive event. In fact, accounts of pre-1953 blizzards do not suggest an event of this magnitude over the last 300 years (the Great Storm of February 1889 and the Great Snow of 1717 seem the closest in magnitude; see [Burt 2004] for descriptions of these storms).

References

[Blake et al. 2005] E. S. Blake, E. N. Rappaport, J. D. Jarrell, and C. W. Landsea, "The deadliest, costliest, and most intense United States tropical cyclones from 1851 to 2004 (and other frequently requested hurricane facts)", NOAA technical memorandum, National Weather Service, Miami, FL, 2005.

[Burt 2004] C. C. Burt, *Extreme weather: guide and record book*, W. W. Norton & Company, New York City, 2004.

[Davison and Smith 1990] A. C. Davison and R. L. Smith, "Models for exceedances over high thresholds (with discussion)", *Journal of the Royal Statistical Society, Series B* **52** (1990), 393–442.

[Van den Dool et al. 2006] H. M. Van den Dool, P. Peng, A. Johansson, M. Chelliah, A. Shabbar, and S. Saha, "Seasonal-to-decadal predictability and prediction of North American climate — the Atlantic influence", *J. Climate* **19** (2006), 6005–6024.

[Embrechts et al. 1997] P. Embrechts, C. Klüppelberg, and T. Mikosch, *Modeling extremal events*, Applications of Mathematics **33**, Springer, Berlin, 1997.

[Kocin and Uccellinni 2004a] P. J. Kocin and L. W. Uccellinni, *Northeast snowstorms, I: overview*, American Meteorological Society, Boston, 2004.

[Kocin and Uccellinni 2004b] P. J. Kocin and L. W. Uccellinni, *Northeast snowstorms, II: the cases*, American Meteorological Society, Boston, 2004.

[McDonnell and Holbrook 2004] K. A. McDonnell and N. Holbrook, "A Poisson regression model of tropical cyclogenesis for the Australian-Southwest Pacific Ocean region", *Weather Forecasting* **19** (2004), 440–455.

[Parisi and Lund 2008] F. Parisi and R. B. Lund, "Return periods of continental U.S. hurricanes", *Journal of Climate* **21** (2008), 403–410.

[Ross 1996] S. M. Ross, *Stochastic processes*, 2nd ed., John Wiley and Sons, New York City, 1996. Zbl 0888.60002

[Ross 2002] S. M. Ross, *Simulation*, 3rd ed., Academic Press, Inc., Orlando, 2002.

[Sheather and Jones 1991] S. J. Sheather and M. C. Jones, "A reliable data-based bandwidth selection method for kernel density estimation", *J. Roy. Statist. Soc. Ser. B* **53**:3 (1991), 683–690. MR 1125725   Zbl 0800.62219

[Tajvidi 2003] N. Tajvidi, "Confidence intervals and accuracy estimation for heavy-tailed generalized Pareto distributions", *Extremes* **6** (2003), 111–123.   Zbl 1063.62037

ckarvetski@gmail.com   Department of Systems and Information Engineering,
                                            The University of Virginia, PO Box 400747,
                                            Charlottesville, VA 22904, United States

lund@clemson.edu   Department of Mathematical Sciences, Clemson University,
                                            Clemson, SC 29634-0975, United States

francis_parisi@standardandpoors.com
                                            Standard & Poor's, Structured Finance Research,
                                            55 Water Street, New York City, NY 10041, United States

Bifurcus semigroups and rings

Donald Adams, Rene Ardila, David Hannasch, Audra Kosh,
Hanah McCarthy, Vadim Ponomarenko and Ryan Rosenbaum

(Communicated by Scott Chapman)

A bifurcus semigroup or ring is defined as possessing the strong property that every nonzero nonunit nonatom may be factored into two atoms. We develop basic properties of such objects as well as their relationships to well-known semigroups and rings.

1. Introduction and basic properties

Factorization theory has traditionally considered unique factorization as "good", and focused attention on semigroups whose factorization is close (in various precise ways) to this ideal. We instead propose to consider semigroups that are by some measures the "worst", those whose factorization is as far as possible from this ideal.

Definition 1.1. We call an atomic semigroup *bifurcus* if every nonunit nonatom can be factored into two atoms. We call a ring *bifurcus* if every nonzero nonunit nonatom can be factored into two atoms. We call a bifurcus semigroup or ring *nontrivial* if it contains at least one (nonzero) nonunit.

We do not require our semigroups to be commutative, cancellative, or possess bounded factorization. We also do not require our rings to possess multiplicative identities. In the sequel, we develop various properties of bifurcus semigroups and rings and give some examples. For a background to factorization theory, see [Geroldinger and Halter-Koch 2006]. For additional undefined terms, see [Baginski et al. 2008; Chapman and Krause 2005].

We begin by presenting some basic properties and calculating standard factorization invariants for bifurcus semigroups.

Theorem 1.1. *Let S be a nontrivial bifurcus semigroup, and let x be a* (*nonzero*) *nonunit nonatom in S. Then*:

(1) *If S is either left or right cancellative, then S contains infinitely many atoms, and the divisor closure $[\![x]\!]$ is not finitely generated.*

(2) *S contains no strong atoms.*

(3) *Let $\mathfrak{L}(x)$ denote the set of factorization lengths of x, and let $L(x) = \sup \mathfrak{L}(x)$. Then $\mathfrak{L}(x)$ is the set of integers in $[2, L(x)]$.*

(4) *The elasticity $\rho(x)$ satisfies $2\rho(x) \in \mathbb{N} \cup \{\infty\}$.*

(5) *The elasticity $\rho(S)$ is ∞.*

(6) *The delta set $\Delta(S)$ equals $\{1\}$.*

(7) *The catenary degree $c(S)$ equals 3.*

(8) *The tame degree $t(S)$ is ∞.*

(9) *The critical length of S is 3.*

Proof.

(1) For each $n \in \mathbb{N}$, we write $x^n = a_n b_n$, where a_i, b_i are atoms. Suppose that S is left cancellative (right cancellative is similar). We will show that $\{a_1, a_2, \ldots\}$ are distinct. Otherwise we have $a_i = a_{i+j}$ for some $i, j \in \mathbb{N}$. We have $a_i b_i x^j = x^i x^j = x^{i+j} = a_{i+j} b_{i+j} = a_i b_{i+j}$. Applying left cancellation yields a factorization of the atom b_{i+j} into nonunits, a contradiction. The second statement holds since $\{a_1, a_2, \ldots\} \subseteq [\![x]\!]$.

(2) Let y be a strong atom. Applying the bifurcus property we have $y^3 = ab$, for atoms a, b. Applying the strong atom property, $a = \epsilon y^\alpha$, $b = \epsilon' y^\beta$, with $\alpha + \beta = 3$ and ϵ, ϵ' units. Without loss of generality $\alpha \geq 2$; but then a is not an atom.

(3) It suffices to prove that if $m \in \mathfrak{L}(x)$ with $m \geq 3$, then $m - 1 \in \mathfrak{L}(x)$. Let $x = b_1 b_2 b_3 \cdots b_m$ be a factorization. By the bifurcus property $b_1 b_2 b_3 = cd$, hence $x = cd b_4 \cdots b_m$, a factorization of length $m - 1$.

(4) Follows directly from the bifurcus property, which gives $\min \mathfrak{L}(x) = 2$.

(5) Consider a^n for any atom a, as $n \to \infty$. $\sup \mathfrak{L}(a^n) \geq n$, but $\inf \mathfrak{L}(a^n) = 2$.

(6) Follows from property (3).

(7) Given any factorization of x, we iteratively apply the construction from (3) to get a sequence of factorizations, each of distance three from each other, ending in two atoms. Given two factorizations, we apply the preceding process twice to get $f_1 \to f_2 \to \cdots \to ab$ and $g_1 \to g_2 \to \cdots \to cd$. Reversing and combining, we have a sequence of factorizations $f_1 \to f_2 \to \cdots \to ab \to cd \to \cdots \to g_2 \to g_1$, each of distance at most three.

(8) Follows from (5) and [Geroldinger and Halter-Koch 2006, Theorem 1.6.6] that gives $\rho(S) \leq t(S)$.

(9) Immediately follows from the observation that $\min \mathfrak{L}(x) = 2$. In fact, the bifurcus property characterizes monoids with critical length 3. □

The bifurcus property excludes many classes of well-studied and familiar semigroups and rings.

Theorem 1.2. *The following are not bifurcus*:

(1) *Block monoids $B(G_0)$, for $G_0 \subseteq G$.*

(2) *Krull monoids.*

(3) *Rings of integers of any algebraic number field.*

(4) *Diophantine monoids.*

(5) *Numerical semigroups.*

Proof.

(1) Let $x \in B(G_0)$ be a nonunit nonatom. We may express x as the multiset $\{x_1^{m_1}, x_2^{m_2}, \dots, x_k^{m_k}\}$ where $k \geq 1$, $x_i \in G_0$, and $m_i \geq 1$ (for all $i \in [1, k]$). Consider the function γ from multisets drawn from $\{x_1, x_2, \dots, x_k\}$ to $\mathbb{N}_0^k$ that gives the multiplicity of each element (e.g. $\gamma(x) = (m_1, m_2, \dots, m_k)$). For all $n \in \mathbb{N}$, the bifurcus property gives a factorization of $x^n = a(n)b(n)$ into two atoms. Without loss we may assume that $\gamma(a(n))_1 \geq \gamma(b(n))_1$. Note that $\gamma(a(n)) + \gamma(b(n)) = \gamma(x^n) = (nm_1, nm_2, \dots, nm_k)$, hence $\gamma(a(n))_1 \in [(nm_1/2), nm_1]$. Consider now the set $S = \{\gamma(a(1)), \gamma(a(2)), \dots\}$, a subset of $\mathbb{N}_0^k$. Because of the condition on the first coordinates of the elements of S, $|S| = \infty$. By a classical theorem attributed to Lothaire (in [Spielman and Bóna 2000]) or Dickson (in [Geroldinger and Halter-Koch 2006]), $\mathbb{N}_0^k$ has no infinite antichain in the usual partial ordering. Hence there must be some i, j with $\gamma(a(i)) \geq \gamma(a(j))$; but then $a(j)|a(i)$ in $B(G_0)$, and hence $a(i)$ is not an atom, contrary to assumption.

(2) Follows from (1) and from [Geroldinger and Halter-Koch 2006, Theorem 2.5.8], which states that all reduced Krull monoids are block monoids.

(3) Follows from [Geroldinger and Halter-Koch 2006, Theorem 1.7.3] together with Theorem 1.1 (5).

(4) Follows from (2) and [Chapman et al. 2002], which shows that Diophantine monoids are Krull.

(5) Follows from [Rosales 2009], which shows that numerical semigroups are cancellative and must have a finite number of atoms. This is violative of Theorem 1.1 (1). □

While it may seem that the bifurcus property is rare, the following result shows that in fact every semigroup can be embedded into a bifurcus semigroup.

Theorem 1.3. *Let R be any semigroup. Let S be any atomic semigroup with no units. Then $T = R \times S \times S$ is bifurcus.*

Proof. Note that T has no units since S does not. Let $x \in T$ be a nonatom. We factor $x = yz$, where $y = (r_y, u_y, v_y)$, $z = (r_z, u_z, v_z)$, and $x = (r_y r_z, u_y u_z, v_y v_z)$. We write $u_y u_z = pu$ and $v_y v_z = vq$, for some atoms $p, q \in S$. Set $y' = (r_y, p, v)$ and $z' = (r_z, u, q)$. These are atoms in T, and $x = y'z'$.   □

2. Examples

We provide several examples of bifurcus rings. These do not have multiplicative units, but (1) and (3) of Example 2.1 do not have zero divisors. The conditions imposed on m, n are all necessary – if n is a prime power, then neither (1) nor (3) is bifurcus; if $m = 1$, then (2) is not bifurcus.

Example 2.1. The following are bifurcus rings:

(1) $n\mathbb{Z}$, for n not a prime power.

(2) $(m\mathbb{Z}) \times (n\mathbb{Z})$ for m, n natural numbers greater than 1.

(3) The subring of $n \times n$ matrices consisting of matrices with all entries identical integers, for n not a prime power.

Proof.

(1) Atoms in our ring are nx where $n \nmid x$. Write $n = pqr$ where p, q are prime and might divide $r \in \mathbb{Z}$. Consider nonatom $z = (nx)(ny) = p^a q^b r^2 s$, where $p, q \nmid s$. Note that $a, b \geq 2$; hence we can factor $z = (pqr(q^{b-2}s))(pqr(p^{a-2}))$. These are atoms since $n \nmid q^{b-2}s$ and $n \nmid p^{a-2}$.

(2) Consider nonatom $z = (ma, nb) \times (mc, nd) = (m, nbd) \times (mac, n)$, a factorization into two atoms.

(3) This ring is isomorphic with $\mathbb{Z}$, with the usual addition but with multiplication given by $x \star y = nxy$. Atoms are those integers that are not multiples of n. Write $n = pqr$ where p, q are prime and might divide $r \in \mathbb{Z}$. Consider nonatom $z = x \star y = nxy = np^a q^b s$ where $p, q \nmid s$. Set $x' = p^a$, $y' = q^b s$. These are atoms and $z = x' \star y'$.   □

Bifurcus semigroups turn out to be common among (noncommutative) matrix semigroups (see [Adams et al. ≥ 2009]). We give just one example.

Example 2.2. Let $n > 1$ and let S denote the semigroup of $n \times n$ rank one matrices with entries from $\mathbb{N}$. Then S is bifurcus.

Proof. Let gcd denote the usual greatest common divisor function, which we will apply to the entries of matrices and vectors. Recall that $a \in S$ may be expressed (nonuniquely) as $a = uv^T$, for u, v column n-vectors. We claim that

$\gcd(a) = \gcd(u)\gcd(v)$. We assume without loss that $\gcd(u) = \gcd(v) = 1$ and prove $\gcd(a) = 1$ by instead considering

$$\frac{a}{\gcd(u)\gcd(v)} = \frac{u}{\gcd(u)}\frac{v^T}{\gcd(v)}.$$

If $p \mid \gcd(a)$, then p divides each entry of the ith columns of a, namely $v_i u$. Since p cannot divide each entry of u, $p \mid v_i$. But this holds for each i, hence p divides each entry of v, a contradiction. Hence $\gcd(a) = 1$, as desired.

Now consider nonatom $a = bc = (u_b v_b^T)(u_c v_c^T) = (v_b^T u_c)(u_b v_c^T)$. Note in passing that since all entries are from $\mathbb{N}$, $\gcd(a) \geq v_b^T u_c \geq n$ for every nonatom a. Set

$$a' = \frac{a}{\gcd(a)} = u'v'^T;$$

by the previous claim $\gcd(u') = \gcd(v') = 1$. Set $x = [\gcd(a) - n + 1, 1, \ldots, 1]^T$, $y = [1, 1, \ldots, 1]^T$. We have $a = \gcd(a)a' = (x^T y)(u'v'^T) = (u'x^T)(yv'^T)$. Because $\gcd(u') = \gcd(v') = \gcd(x) = \gcd(y) = 1$, by the previous claim $\gcd(u'x^T) = \gcd(yv'^T) = 1$, and since $n > 1$ these are both atoms. $\square$

We conclude with some unanswered questions.

Open problems

(1) Does there exist a bifurcus ring with 1? A bifurcus domain?

(2) Can every ring/domain be embedded in a bifurcus ring?

(3) Can a bifurcus semigroup possess finitely many atoms?
    Note that by Theorem 1.1(1), such an example would be neither left nor right cancellative. Further, such an example must be finite (since N atoms yields at most N^2 ordered pairs of atoms), and therefore must not possess bounded factorization.

(4) Can a bifurcus semigroup be inside factorial or Cale?

(5) Can a bifurcus semigroup be locally tame?

Acknowledgment

References

[Adams et al. $\geq$ 2009] D. Adams, R. Ardila, D. Hannasch, A. Kosh, H. McCarthy, V. Ponomarenko, and R. Rosenbaum, "Factorization in matrix semigroups", in preparation.

[Baginski et al. 2008] P. Baginski, S. T. Chapman, and G. J. Schaeffer, "On the delta set of a singular arithmetical congruence monoid", *J. Théor. Nombres Bordeaux* **20**:1 (2008), 45–59. MR 2434157 Zbl 05543190

[Chapman and Krause 2005] S. T. Chapman and U. Krause, "Cale monoids, cale domains, and cale varieties", pp. 142–171 in *Arithmetical properties of commutative rings and monoids*, Lect. Notes Pure Appl. Math. **241**, Chapman & Hall/CRC, Boca Raton, FL, 2005. MR 2006b:13050 Zbl 1100.20040

[Chapman et al. 2002] S. T. Chapman, U. Krause, and E. Oeljeklaus, "On Diophantine monoids and their class groups", *Pacific J. Math.* **207**:1 (2002), 125–147. MR 2004b:20089 Zbl 1060.20050

[Geroldinger and Halter-Koch 2006] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations*, Pure and Applied Mathematics **278**, Chapman & Hall/CRC, Boca Raton, FL, 2006. Algebraic, combinatorial and analytic theory. MR 2006k:20001 Zbl 1113.11002

[Rosales 2009] J. C. Rosales, "Atoms of the set of numerical semigroups with fixed Frobenius number", *Linear Algebra Appl.* **430**:1 (2009), 41–51. MR 2460497 Zbl 05376883

[Spielman and Bóna 2000] D. A. Spielman and M. Bóna, "An infinite antichain of permutations", *Electron. J. Combin.* **7**:article #2 (2000). MR 2000k:05014

djunior82@gmail.com   *San Diego State University, San Diego, CA 92182-7720, United States*

reneardila@hotmail.com   *City College of New York, New York, NY 10031, United States*

davidh@egr.unlv.edu   *University of Nevada at Las Vegas, Las Vegas, NV 89154, United States*

akosh@umail.ucsb.edu   *University of California at Santa Barbara, Santa Barbara, CA 93106, United States*

hanah.j.mccarthy@lawrence.edu   *Lawrence University, Appleton, WI 54912, United States*

vadim@sciences.sdsu.edu   *San Diego State University, Department of Mathematics and Statistics, 5500 Campanile Dr., San Diego, CA 92182-7720, United States*
                                   http://www-rohan.sdsu.edu/~vadim/

rosenbaum.ryan@gmail.com   *San Diego State University, San Diego, CA 92182-7720, United States*

Construction and enumeration of Franklin circles

Rebecca Garcia, Stefanie Meyer, Stacey Sanders and Amanda Seitz

(Communicated by Scott Chapman)

Around 1752, Benjamin Franklin constructed a variant on the popular magic squares and what we call a magic (a, r)-circle. We provide a definition for magic (a, r)-circles, magic a-circles and, more specifically, Franklin magic a-circles. In this paper, we use techniques in computational algebraic combinatorics and enumerative geometry to construct and to count Franklin magic 8-circles. We also provide a description of its minimal Hilbert basis and determine the symmetry operations on Franklin magic 8-circles.

1. Introduction

Benjamin Franklin was a noted American scholar, politician, scientist, inventor, author of various books and scientific articles, publisher of *Poor Richard's Almanac*, and most notably an editor and signer of the Declaration of Independence, who eventually came to enjoy the recreational side of mathematics. Among his most cherished mathematical works are his famous 8×8 and 16×16 magic squares, which are many times more magical than ordinary magic squares. Here is one of Franklin's 8×8 squares, with sum 260:

52	61	4	13	20	29	36	45
14	3	62	51	46	35	30	19
53	60	5	12	21	28	37	44
11	6	59	54	43	38	27	22
55	58	7	10	23	26	39	42
9	8	57	56	41	40	25	24
50	63	2	15	18	31	34	47
16	1	64	49	48	33	32	17

A magic square has three properties: that each row sum, each column sum, and each main diagonal sum is the same "magic" number. A Franklin square, however, has many more properties [Ahmed 2004]:

- Each row sum is the same magic number M.

- Each column sum is M.

- Each *bent* diagonal sum is M.

- Each half-row sum is $M/2$.

- Each half-column sum is $M/2$.

- For 8×8 Franklin squares, each 2×2 block sum is $M/2$.

- For 8×8 Franklin squares, the four corners with the middle four sums to M.

- For 16×16 Franklin squares, each 2×2 block sum is $M/4$, each 4×4 block sum is $M/4$.

These properties can be nicely visualized thus:
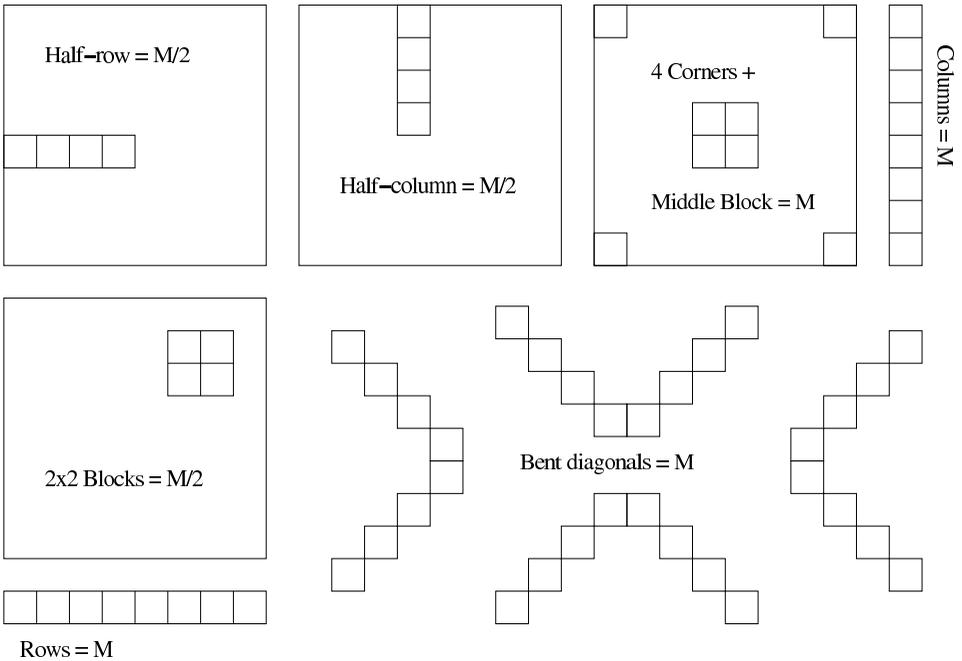
Several magic squares constructed by Franklin were described in a letter written around 1752 to fellow English botanist Peter Collinson [Pasles 2001]. Franklin noted in the same letter that these unusual squares were not his only construction. Franklin provided a similarly complex magic circle in a letter dated 1765 to fellow

English physicist John Canton, describing all of its properties with painstaking detail. In this article, we refer to this magic 8-circle as *the* Franklin magic 8-circle.

There is no standard definition for a magic circle. We will use the following definition, found also in [Nicholas 1955].

Definition 1. A *magic* (a, r)-*circle* is an arrangement of nonnegative integers in a circular grid consisting of a concentric annuli and r radii, with the property that each annular sum is M and each radial sum is M. In the case $a = r$, we shall call it a *magic a-circle*.

Franklin's magic circle, like his magic squares, has additional sophistication. Much like the bent diagonals of Franklin's magic squares, a Franklin magic circle has families of concentric annuli contained within the largest main circle, which however are *eccentric* relative to the basic circular grid. Here is Franklin's original magic 8-circle, with sum $M = 360$; one eccentric annulus is highlighted:
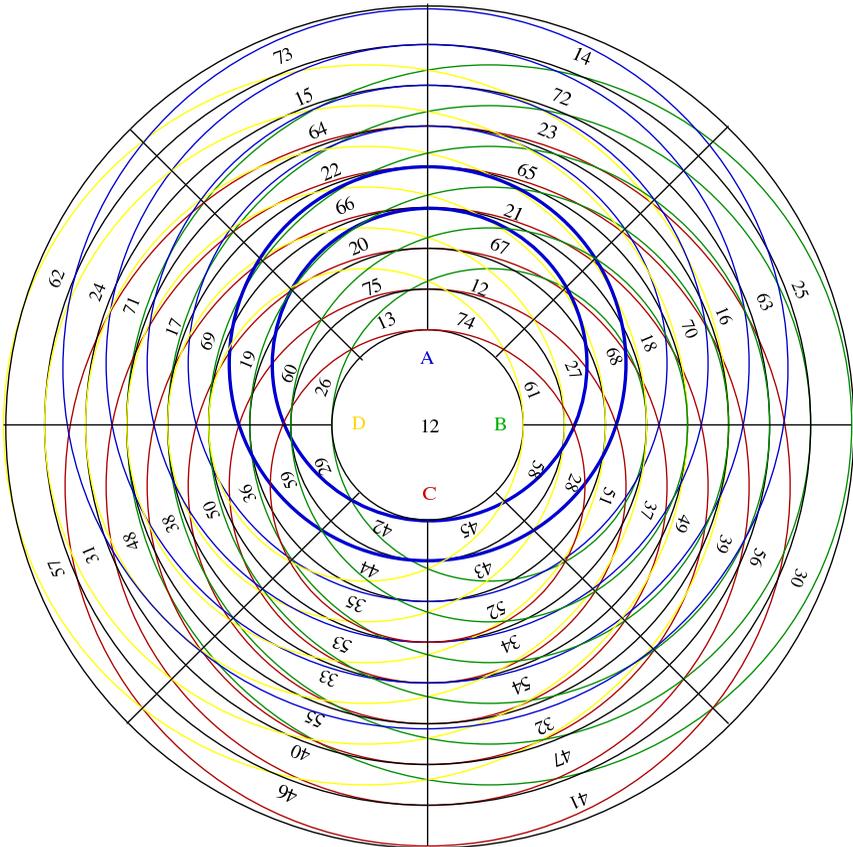
There are four different *excenters* labeled A, B, C, and D, located north, east, south and west of the center. Around each excenter are six concentric circles,

forming five annuli. For example, the innermost annulus centered at A in the previous figure (bounded by the two thick circles) contains, clockwise from the bottom, the entries 42, 59, 19, 66, 21, 68, 28, 45. We call these values x_{17}, x_{28}, x_{31}, x_{42}, x_{43}, x_{34}, x_{25}, x_{16}, according to the cells in which they lie; that is, x_{ij} is the number in the i-th original annulus, counted outward, and in the j-th sector, counted clockwised starting with the lower of the two sectors in the first quadrant. Here is another way to visualize the eccentric circles centered at A:
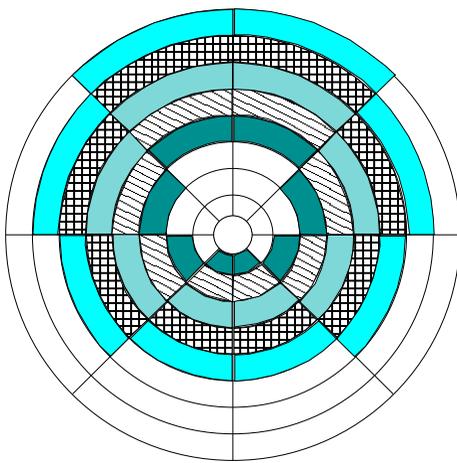
Franklin's original magic circle satisfies the following four properties, which are also depicted graphically on the next page:

(i) Each radial sum plus the central number is the same magic number M.

(ii) Each upper- or lower-half annular sum plus half the central number is $M/2$, and consequently each annular sum plus the central number is M.

(iii) Each 2×2 block sum plus half the central number is $M/2$.

(iv) Each upper- or lower-half annular sum of vertically centered eccentric annuli plus half the central number is $M/2$, and similarly, each left- or right-half annular sum of horizontally centered eccentric annuli plus half the central number is $M/2$. Consequently, each eccentric annular sum plus the central number is M.

Because the central number, appropriately scaled, is added to each of the various types of sums, its role is merely to shift the magic sum. Thus, we will drop the inclusion of the central number in our computations throughout. In this paper, we define a *Franklin magic 8-circle* to be a magic 8-circle with nonnegative integer entries satisfying properties (i)–(iv) above (without a central number). In general, for $n \geq 2$, we define a *Franklin magic 2^n-circle* to be a magic 2^n-circle satisfying (i)–(iv), except that (iii) is modified to read that every 2×2 block sum is $2^{2-n} M$.
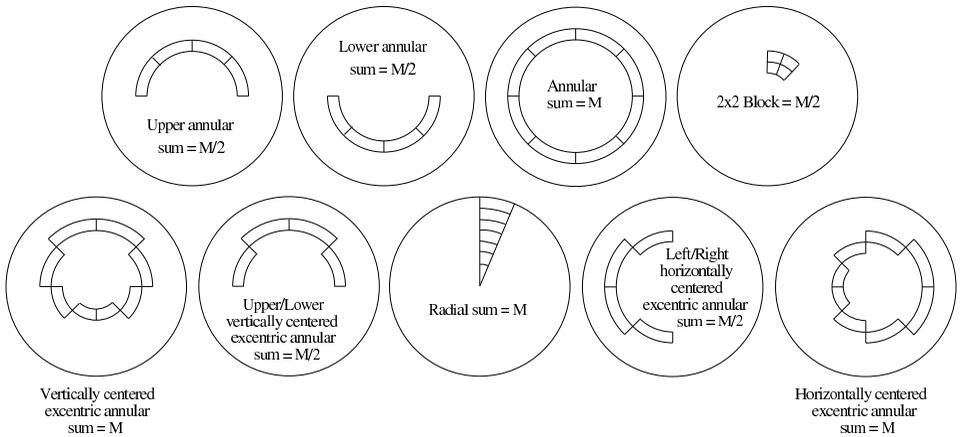
Figure 1. Properties of a Franklin magic circle.

In Section 2, we take a closer look at the tools in computational algebraic combinatorics that allow us to construct all Franklin magic 8-circles. We give a succinct description of the minimal Hilbert basis of the Franklin magic 8-circles, which is a special set of Franklin magic 8-circles that can be used to construct any Franklin magic 8-circle. Furthermore, we give a simple description for producing all possible Franklin magic 4-circles.

In Section 3, we discuss the symmetry operations on the Franklin magic 8-circles and we reveal a *new* Franklin magic 8-circle, that is, a Franklin magic 8-circle which cannot be obtained via symmetry operations on the original Franklin magic 8-circle. Finally, in Section 4, we provide the generating function for Franklin magic 8-circles $FC_8(s)$, a function which determines the number of Franklin magic 8-circles with magic sum s.

2. Background and notation

We now describe the techniques used to derive the building blocks of all Franklin magic 2^n-circles, starting with $n = 3$. To this end, we view a generic Franklin magic 8-circle as a vector in $\mathbb{R}^{8^2}$, with variable entries $x_{11}, \ldots, x_{88}$, where, as before, the entry x_{ij} is in the i-th annulus and the j-th radius.

The four defining properties of the Franklin magic 8-circle can be viewed as linear relations in these variables. For example, the first property states that each radial sum is the (undetermined) magic number M; that is, the sums $\sum_{i=1}^{8} x_{ij}$ must be equal for all j. This gives seven independent linear equations such as

$$x_{11} + x_{21} + x_{31} + x_{41} + x_{51} + x_{61} + x_{71} + x_{81}$$
$$= x_{12} + x_{22} + x_{32} + x_{42} + x_{52} + x_{62} + x_{72} + x_{82}.$$

The half-annular sum property yields sixteen linear equations, while there are fifty-six distinct 2×2 block linear equations coming from the eight radial and seven annular locations in the circular arrangement. There are altogether twenty eccentric annuli coming from the five eccentric annuli centered around each of the four ex-centers, with each eccentric annulus yielding two linear relations for the eccentric half annular sum. Rewriting these equations in matrix form, we have a 119×64 integral matrix M:

$$
M = \begin{pmatrix}
1 & \cdots & 1 & -1 & \cdots & -1 & 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 \\
1 & \cdots & 1 & 0 & \cdots & 0 & -1 & \cdots & -1 & 0 & \cdots & 0 & \cdots & 0 \\
& \vdots & & & \vdots & & & \vdots & & & \vdots & & &
\end{pmatrix}.
$$

We observe that for the Franklin magic 8-circle: (1) any nonnegative integer linear combination of Franklin magic 8-circle is a Franklin magic 8-circle, and (2) the set of all Franklin magic 8-circles is the integral solution set to the 119 integral linear equations mentioned above. This shows that the Franklin magic 8-circles are also the integral points inside the set

$$
C = \{ \boldsymbol{x} = (x_{11}, \ldots, x_{88}) \in \mathbb{R}^{64}_{\geq 0} : M\boldsymbol{x} = 0 \},
$$

which is itself a pointed rational polyhedral cone.

By [Schrijver 1986, Theorem 16.4], there is a unique finite set H of integral points in C, such that every integral point in C is a linear combination of elements in H. This set is known as *the minimal Hilbert basis* of C. Thus with this minimal Hilbert basis, every Franklin magic 8-circle is some linear combination of the elements in H. Using the software 4ti2, we computed the seventy-four elements of the minimal Hilbert basis for the Franklin magic 8-circles.

We observed two distinct subsets of elements in this minimal Hilbert basis. Among the minimal Hilbert basis elements of the first type, we observed that the first radial arrangement determines all others for the following reasons: the second radial arrangement must be the complement of the first, and this alternating pattern repeats for the third through the eighth radial arrangements. We also noted that the first radial arrangement is completely determined by the placement of the four 1s. Since there are eight possible places, that yields precisely $\binom{8}{4} = 70$ Hilbert basis elements of the first type.

To illustrate the construction of a minimal Hilbert basis element of the first type, see Figure 2. Here, the first radial arrangement is in the second quadrant, just above the horizontal diameter. We chose to place the four 1s in annuli 2, 4, 5, and 7. The second radius, clockwise, is then determined by placing a 1 in the complementary annuli: 1, 3, 6, and 8, shown in bold gray type in Figure 2. This pattern alternates in the subsequent radii.
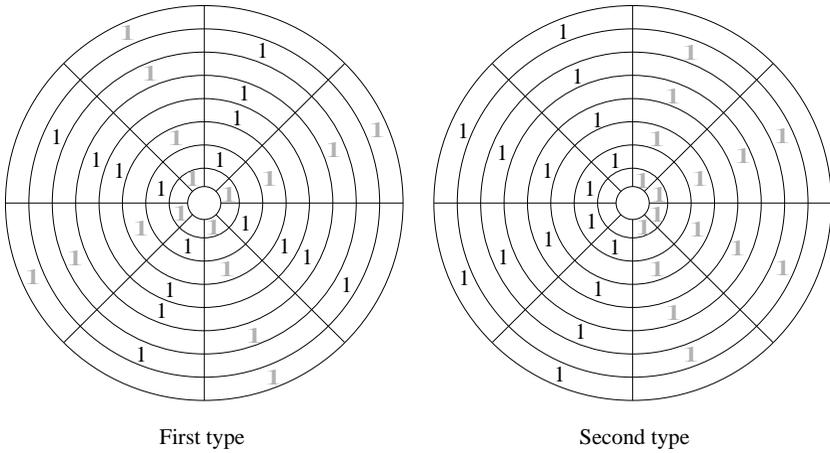
Figure 2. Examples of Hilbert basis elements.

Finally, there are four Hilbert basis elements of the second type. Their description is based on two observations: all radial arrangements consists of alternating 0 and 1, and the two radial arrangements in each of the four quadrants are duplicates, with the upper half consisting of complementary quadrants and likewise for the lower half. This yields precisely four elements. See Figure 2 for an illustration.

With this minimal Hilbert basis, constructing new Franklin magic 8-circles boils down to simple arithmetic. We present another Franklin magic 8-circle in Figure 3.

We computed the integer linear combination that produces the original Franklin magic 8-circle. This combination is shown in Figure 4 and uses eleven minimal
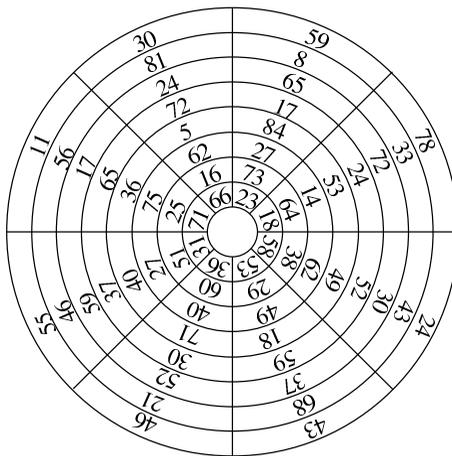
Figure 3. A new Franklin magic 8-circle.
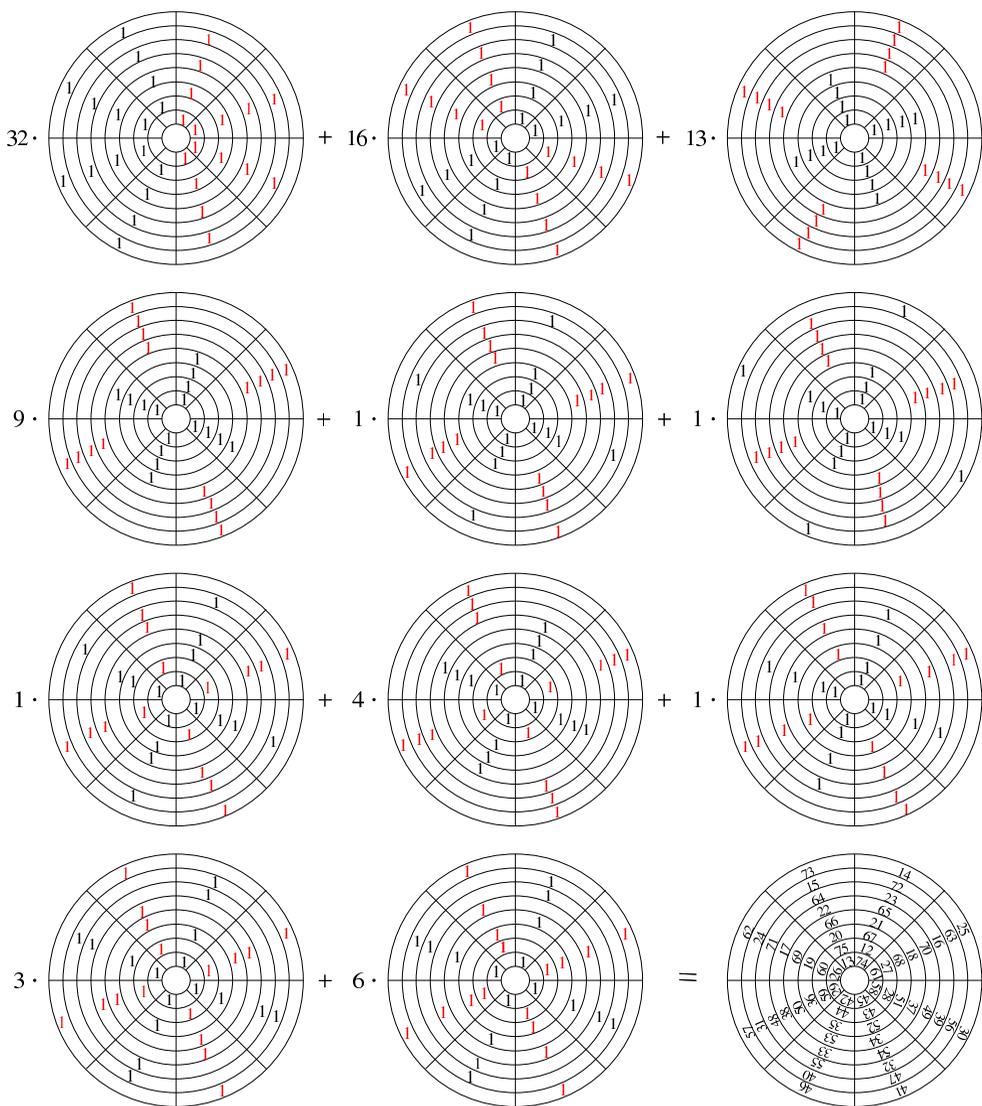
Figure 4. Linear combination of the original Franklin magic 8-circle.

Hilbert basis elements. In terms of the two types of minimal Hilbert basis elements, this linear combination uses two of the second type and nine of the first type.

As for Franklin magic 4-circles, there are precisely six elements in its minimal Hilbert basis. They, too, were computed using 4ti2. Figure 5 shows three elements, with the remaining three obtained by flipping these along the horizontal diameter. The simplicity of its minimal Hilbert basis forces all Franklin magic 4-circles to have repeated entries, whose arrangement is described in Theorem 3.
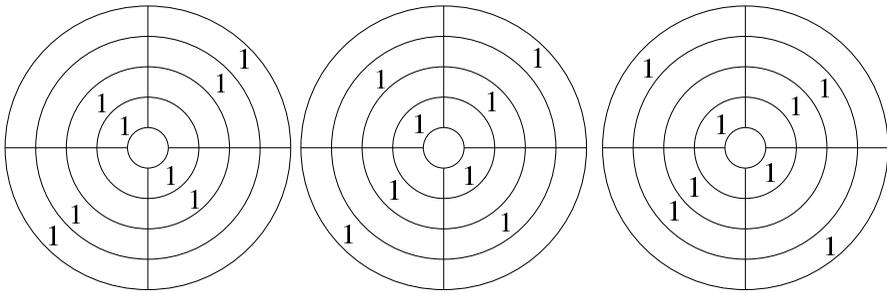
Figure 5. Three elements of the minimal Hilbert basis for Franklin magic 4-circles.

We observe that in this case, the minimal Hilbert basis is only of the first type; that is, the first radial arrangement determines all other radial arrangements. We also noted that the first radial arrangement is completely determined by the placement of the two 1s. Since there are four possible places, then this yields precisely $\binom{4}{2} = 6$ Hilbert basis elements of the first kind. With this observation, we make the following conjecture for the minimal Hilbert basis for Franklin magic 16-circles.

Conjecture 2. *There are $\binom{16}{8} + 16$ elements in the minimal Hilbert basis for Franklin magic 16-circles.*

Theorem 3. *A Franklin magic 4-circle is of the form*
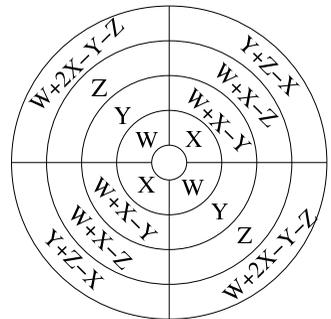
Proof. Consider the matrix whose rows correspond to integer multiples of an element in the minimal Hilbert basis:

$$\begin{pmatrix} 0 & a & 0 & a & a & 0 & a & 0 & 0 & a & 0 & a & a & 0 & a & 0 \\ b & 0 & b & 0 & b & 0 & b & 0 & 0 & b & 0 & b & 0 & b & 0 & b \\ 0 & c & 0 & c & 0 & c & 0 & c & c & 0 & c & 0 & c & 0 & c & 0 \\ d & 0 & d & 0 & 0 & d & 0 & d & d & 0 & d & 0 & 0 & d & 0 & d \\ e & 0 & e & 0 & 0 & e & 0 & e & 0 & e & 0 & e & e & 0 & e & 0 \\ 0 & f & 0 & f & f & 0 & f & 0 & f & 0 & f & 0 & 0 & f & 0 & f \end{pmatrix}$$

Any Franklin magic 4-circle is an integral linear combination of the elements in the minimal Hilbert basis. Thus, any Franklin magic 4-circle corresponds to the sum

of the rows of this matrix:

$$(b{+}d{+}e,\ a{+}c{+}f,\ b{+}d{+}e,\ a{+}c{+}f,\ a{+}b{+}f,\ c{+}d{+}e,\ a{+}b{+}f,\ c{+}d{+}e,$$
$$c{+}d{+}f,\ a{+}b{+}e,\ c{+}d{+}f,\ a{+}b{+}e,\ a{+}c{+}e,\ b{+}d{+}f,\ a{+}c{+}e,\ b{+}d{+}f),$$

where the first four entries represent the first annulus in the Franklin magic 4-circle, the next four entries represent the second annulus, and so forth. Setting $W = b + d + e$, $X = a + c + f$, $Y = a + b + f$ and $Z = c + d + f$, demonstrates that any Franklin magic 4-circle is of the desired form. □

Example 4. Choosing fixed nonnegative integer values for $W = 16$, $X = 24$, $Y = 25$, and $Z = 17$ yields the following Franklin magic 4-circle:
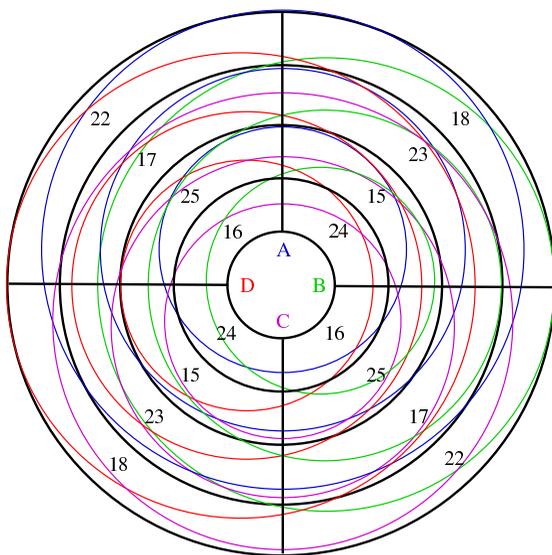
3. Symmetry operations on Franklin magic 8-circles

A *symmetry operation* on the set of Franklin magic 8-circles is defined to be a map σ from the set of all Franklin magic 8-circles to itself, that permutes the entries in a Franklin magic 8-circle. From this definition, one can easily see that there are three obvious such symmetry operations: 180° rotation and reflection along the horizontal and vertical diameters.

There are operations on Franklin magic 8-circles which yield magic 8-circles that do not preserve all defining properties properties (i)–(iv). For example, rotation by 90° is *not* a symmetry operation. This can be readily seen by considering this operation on the first minimal Hilbert basis element in Figure 4 (page 364). Here, the upper half annular sum is 0, while the lower half annular sum is 4. In addition, we also note that the *transpose*, that is, exchanging annuli for radii, is not

a symmetry operation. This can be seen easily from trying to *transpose* an element of the minimal Hilbert basis, such as the multiple of 13 in Figure 4.

We observed that the elements of the minimal Hilbert basis hold the key to finding all symmetry operations on Franklin magic circles, as we see in Theorem 5.

Theorem 5. *Let $\mathscr{F}_8$ denote the set of all Franklin magic 8-circles, and $\mathrm{H}\mathscr{F}_8$ denote the minimal Hilbert basis of the Franklin magic 8-circles. Then $\sigma : \mathscr{F}_8 \longrightarrow \mathscr{F}_8$ is a symmetry operation on $\mathscr{F}_8$ if and only if its restriction $\overline{\sigma} : \mathrm{H}\mathscr{F}_8 \longrightarrow \mathrm{H}\mathscr{F}_8$ is a symmetry operation on $\mathrm{H}\mathscr{F}_8$.*

Proof. ($\Longrightarrow$) By definition. ($\Longleftarrow$) Let $\overline{\sigma} : \mathrm{H}\mathscr{F}_8 \longrightarrow \mathrm{H}\mathscr{F}_8$ be a symmetry operation on $\mathrm{H}\mathscr{F}_8$. Let (x_{ij}) denote a Franklin magic 8-circle. Then, by definition, (x_{ij}) is some integral linear combination of the elements in $\mathrm{H}\mathscr{F}_8$,

$$(x_{ij}) = \sum_{k=1}^{74} n_k (\mathrm{H}[k]_{ij}),$$

where $\mathrm{H}[k]_{ij}$ is the entry in the i-th annulus and j-th radius of the k-th element in $\mathrm{H}\mathscr{F}_8$. By definition, $\overline{\sigma}$ is a permutation on the entries of $(\mathrm{H}[k]_{ij})$. Under $\overline{\sigma}$, the entry in position ij is permuted to a new position $\overline{ij}$, and thus $\overline{\sigma}(\mathrm{H}[k]_{ij}) = (\mathrm{H}[k]_{\overline{ij}})$, which is, by definition of $\overline{\sigma}$, another minimal Hilbert basis element, which we will denote, for the sake of convenience, as $\mathrm{H}[\overline{\sigma}(k)]$. Observe that if $\overline{\sigma}(H[k]) = \overline{\sigma}(H[j])$, then $k = j$, since all the entries move in precisely the same manner.

Given $\overline{\sigma}$, define

$$\sigma : \mathscr{F}_8 \longrightarrow \mathscr{F}_8, \quad (x_{ij}) \mapsto \sum_{k=1}^{74} n_k (\mathrm{H}[\overline{\sigma}(k)]_{ij}). \tag{1}$$

The image of (x_{ij}) under σ in (1) is an integral linear combination of elements in $\mathrm{H}\mathscr{F}_8$ and is therefore a Franklin magic 8-circle. $\qquad\square$

From Theorem 5, we observe that all symmetry operations can be obtained by finding symmetry operations on the minimal Hilbert basis. We used the description of the minimal Hilbert basis given in Section 2 to observe that the operations described in Theorem 6 are in fact symmetry operations on the set of all Franklin 8-circles.

Theorem 6. *Let $\mathscr{F}_8$ denote the set of all Franklin magic 8-circles. The following are symmetry operations on $\mathscr{F}_8$:*

(i) *Rotation by $180°$, and reflections along the horizontal and vertical diameters.*

(ii) *Exchanging two consecutive annuli*

$$x_i, x_{i+1} \quad \text{with} \quad x_{i+2k}, x_{i+2k+1},$$

with $1 \le i \le 5$ and $0 \le k \le 3$ and the restriction that $i + 2k + 1 \le 8$.

Proof. The operations in (i) clearly preserve the four Franklin magic 8-circle properties. For the operations in (ii), recall that there are two types of elements in the minimal Hilbert basis $H\mathscr{F}_8$ of $\mathscr{F}_8$. The first type of elements come from placing 1s in four of the eight possible locations in the first radial arrangement. This pattern is duplicated in the third, fifth and seventh radial arrangements, while the complementary arrangement is duplicated in the second, fourth, sixth and eighth radii. Thus, permuting the annuli among these elements produces another element in $H\mathscr{F}_8$. The second type of elements in $H\mathscr{F}_8$ impose the conditions given in (ii). □

4. Enumeration of Franklin magic 8-circles

In this section, we answer the question *For any positive integer s, how many Franklin magic 8-circles have a magic sum of s?* This is an example of the general question of enumerating integer lattice points contained in polyhedra. For an excellent resource on this general topic, see [Beck and Robins 2007].

As we noted earlier, we view a generic Franklin magic 8-circle as an integer vector $(x_{11}, \ldots, x_{88})$ in $\mathbb{R}^{8^2}$, where the entry x_{ij} is in the i-th annulus and the j-th radius. Also any Franklin magic 8-circle is an integer linear combination of the minimal Hilbert basis described in Section 2. Since each element of the minimal Hilbert basis has magic sum 4, that implies that every Franklin magic 8-circle must have a magic sum divisible by 4.

Alternatively, we can apply commutative algebra, as in [Ahmed et al. 2003; Cox et al. 1998]. Consider the map of polynomial rings

$$\phi : \mathbb{R}[H[1], \ldots, H[74]] \longrightarrow \mathbb{R}[x_{11}, \ldots, x_{88}]$$

defined by mapping the indeterminate $H[k]$ to $\prod_{i,j=1}^{8} x_{ij}^{H[k]_{ij}}$. Integral linear combinations of the elements in $H\mathscr{F}_8$ correspond to products of integral powers of monomials in $\mathbb{R}[H[1], \ldots, H[74]]$. Thus if $\sum_{k=1}^{74} n_k(H[k]_{ij}) = \sum_{k=1}^{74} m_k(H[k]_{ij})$, we have

$$\phi\left(\prod_{k=1}^{74} H[k]^{n_k} - \prod_{k=1}^{74} H[k]^{m_k}\right) = 0.$$

Define the homogeneous ideal $I_{\mathscr{F}_8} = \left\langle \prod_{k=1}^{74} H[k]^{n_k} - \prod_{k=1}^{74} H[k]^{m_k} \right\rangle$, and consider the weighted, graded ring

$$R = \mathbb{R}[H[1], \ldots, H[74]]/I_{\mathscr{F}_8},$$

where the degree of each variable $H[k]$ is 4, for all k. The Hilbert function $H_R(s)$ is defined by

$$H_R(s) = \dim_{\mathbb{R}} \mathbb{R}[H[1], \ldots, H[74]]_s - \dim_{\mathbb{R}} I_{\mathscr{F}_8, s},$$

where $\mathbb{R}[H[1], \dots, H[74]]_s$ is the finite-dimensional vector space over $\mathbb{R}$ of homogeneous polynomials in $\mathbb{R}[H[1], \dots, H[74]]$ of degree s and $I_{\mathscr{F}_8, s}$ is the finite-dimensional vector space over $\mathbb{R}$ of homogeneous polynomials of degree s in $I_{\mathscr{F}_8}$. Applying [Ahmed 2004, Lemma 2.2], since the weight of each variable $H[i]$ in the polynomial ring $\mathbb{R}[H[1], \dots, H[74]]$ is the magic sum of the corresponding magic circle, then the value $H_R(s)$ is the number of distinct Franklin magic 8-circles with magic sum s. Thus, the Hilbert–Poincaré series

$$\mathrm{HP}_R(t) = \sum_{s=1}^{\infty} H_R(s) t^s$$

is also the Ehrhart series of the Franklin magic 8-circles.

To count the number of Franklin magic 8-circles reduces to computing the generating function of the Hilbert–Poincaré series

$$\mathrm{HP}_R(t) = \sum_{s=1}^{\infty} H_R(s) t^s.$$

We used the computer algebra software LattE [De Loera et al. 2003], to find the $\mathrm{HP}_R(t)$ as a rational function, and then used LattE to compute the first sixty-four values of the enumerating function for the Franklin magic 8-circles. Using Mathematica, we found the interpolating polynomial for these values and computationally verified that the function given in Theorem 7 enumerates the Franklin magic 8-circles.

Theorem 7. *Let* $\mathrm{FC}_8(s)$ *denote the number of Franklin magic 8-circles with sum s. The Ehrhart series of the Franklin magic 8-circles has the rational form*

$$\sum_{s=0}^{\infty} \mathrm{FC}_8(s) t^s$$
$$= \frac{t^8 + 64t^7 + 700t^6 + 2352t^5 + 3430t^4 + 2352t^3 + 700t^2 + 64t + 1}{(t^9 - 9t^8 + 36t^7 - 84t^6 + 126t^5 - 126t^4 + 84t^3 - 36t^2 + 9t - 1)(t - 1)}.$$

A partial expansion of this series is

$$\sum_{s=0}^{\infty} \mathrm{FC}_8(s) t^s = 1 + 74t + 1395t^2 + 13092t^3 + 80245t^4 + 367774t^5 + \cdots.$$

The generating function for the Ehrhart series of the Franklin magic 8-circles is

$$\mathrm{FC}_8(s) = \frac{1}{1486356480} (1486356480 + 1980628992s + 1233911808s^2$$
$$+ 448643072s^3 + 103670784s^4 + 16004352s^5$$
$$+ 1677312s^6 + 117888s^7 + 5436s^8 + 151s^9)$$

when 4 divides s; otherwise, $\mathrm{FC}_8(s) = 0$.

Acknowledgments

References

[Ahmed 2004] M. M. Ahmed, "How many squares are there, Mr. Franklin?: constructing and enumerating Franklin squares", *Amer. Math. Monthly* **111**:5 (2004), 394–410. MR 2057391 Zbl 1055.05502

[Ahmed et al. 2003] M. Ahmed, J. De Loera, and R. Hemmecke, "Polyhedral cones of magic cubes and squares", pp. 25–41 in *Discrete and computational geometry*, Algorithms Combin. **25**, Springer, Berlin, 2003. MR 2004m:05016 Zbl 1077.52506

[Beck and Robins 2007] M. Beck and S. Robins, *Computing the continuous discretely*, Undergraduate Texts in Math., Springer, New York, 2007. MR 2007h:11119 Zbl 1114.52013

[Cox et al. 1998] D. Cox, J. Little, and D. O'Shea, *Using algebraic geometry*, Graduate Texts in Mathematics **185**, Springer, New York, 1998. MR 99h:13033 Zbl 0920.13026

[De Loera et al. 2003] J. A. De Loera, D. Haws, R. Hemmecke, P. Huggins, J. Tauzer, and R. Yoshida, *A User's Guide for LattE v1.1*, 2003.

[Nicholas 1955] M. Nicholas, "Magic circles", *Am. Math. Mon.* **62** (1955), 696.

[Pasles 2001] P. C. Pasles, "The lost squares of Dr. Franklin: Ben Franklin's missing squares and the secret of the magic circle", *Amer. Math. Monthly* **108**:6 (2001), 489–511. MR 2002e:01021

[Schrijver 1986] A. Schrijver, *Theory of linear and integer programming*, Wiley-Interscience Ser. in Discrete Math., Wiley, Chichester, 1986. MR 88m:90090 Zbl 0665.90063

rgarcia@shsu.edu   *Sam Houston State University, Department of Mathematics and Statistics, Box 2206, Huntsville, TX 77340, United States*
                                    http://www.shsu.edu/~mth_reg

sem002@shsu.edu   *Sam Houston State University, Department of Mathematics and Statistics, Box 2206, Huntsville, TX 77340, United States*

sls026@shsu.edu   *Sam Houston State University, Department of Mathematics and Statistics, Box 2206, Huntsville, TX 77340, United States*

amanda.seitz@hotmail.com   *Sam Houston State University, Department of Mathematics and Statistics, Box 2206, Huntsville, TX 77340, United States*

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the Involve website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and 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 *Involve* 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 LaTeX but submissions in other varieties of 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 BibTeX 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 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.