The Art of Iterating Rational Functions over Finite Fields

Nigel Boston (University of Wisconsin)
Alina Ostafe (Macquarie University)
Igor Shparlinski (Macquarie University)
Michael Zieve (University of Michigan)

5-10 May, 2013

1 Overview of the Field

The field of complex dynamical systems generated by iteration of polynomials and rational functions is a classical area of mathematics with a rich history and a wide variety of results. Recently, there has been substantial interest in arithmetical dynamical systems (ADS), meaning the iteration of rational functions over fields of number-theoretic interest.

Although isolated results regarding ADS have been proven throughout the twentieth century, it was only in the 1990's that ADS were identified as a field of study. The past two decades have seen an explosion of work in this topic, in which fundamental problems have been solved, new questions and conjectures have been posed, and connections have been forged with a great many different areas of pure and applied mathematics.

Indications of the fast growing significance of ADS also include the 2010 Mathematics Subject Classification, which contains a new section, 37Pxx, devoted to arithmetic and non-archimedean dynamical systems, whose subsections include 37P05 (Polynomial and rational maps), 37P35 (Arithmetic properties of periodic points), and 37P55 (Arithmetic dynamics on general algebraic varieties), all of which are directly related to the proposed workshop.

The significance of and interest in this topic has also been evidenced over the last several years by the large number of international meetings and workshops in this area, which have attracted experts from dynamical systems as well as experts from algebra and number theory. From this list we note in particular the program on Dynamical Systems that was held at ICERM in Spring 2012, which was focused on complex dynamics, p-adic dynamics, global arithmetic dynamics, and moduli spaces associated to dynamical systems. However, despite this recent profusion of scientific activity in related areas, little progress has been made on **Dynamical Systems over Finite Fields** (**DFF**).

The present exciting and challenging mathematical problems in DFF are of an intricate algebraic and number theoretic flavour whose study requires deep mathematical and computational tools. This area of research focuses on the construction of non-classical dynamical systems over finite fields and the study of atypical behaviour which is not present in standard constructions from complex dynamical systems. Such novel constructions and the classification of their anomalous behaviour have led to innovative solutions to problems in cryptography, biological and physical systems.

Many important questions regarding the orbits of DFF remain wide open, including questions on the number of aperiodic points, the size of orbit intersections (in linearly disjoint DFF), cycle lengths, and so on. Furthermore, the problems proposed as the goal of this proposal have barely been touched upon by other meetings. On the other hand,

we believe that there is now enough of a theoretical background and also active interest shown by many distinguished researchers in the area of DFF and related fields to successfully attack many of the long-standing problems.

Besides intrinsic interest, such DFF are of prime interest for applications. They are also more computer-friendly (due, for example, to the limited size of elements in the trajectories) permitting computer simulations and experiments that may lead to the discovery of new effects which may not be visible or even computable in dynamical systems over the real and complex numbers.

Research into DFF has not only a high theoretical value, but also applied significance thanks to the great number of potential applications to many different areas of modern cryptography, coding theory, Monte Carlo simulations, physics, biology, and other areas. It is also a fertile ground for the development of algorithmic and computer-oriented approaches.

2 Recent Developments and Main Themes of the Workshop

The topics of the proposed workshop have been centered on the following closely related and cross-fertilising directions in DFF:

- *Trajectory length and periodic structure*. One of the most fundamental, yet notoriously hard, questions concerns the periodic structure of polynomial iterations. Heuristically, this periodic structure can be predicted based on the *Birthday Paradox*, but very few rigorous results are known in this area (essentially only very weak lower bounds obtained by J. H. Silverman several years ago). This is especially important due to the recently discovered connection (by M. Baake and J. Roberts) between the integrability of dynamical systems and periodic structure of the reductions of polynomial iterations modulo distinct primes.

  A very recent preprint by R. L. Benedetto et al. gives new theoretical insight and also some heuristics and numerics. There is also still an unexplored approach via the image set of polynomials and their iterations. All the aforementioned authors were invited to the workshop.

  Overall, the situation is not well-understood both theoretically and heuristically. Several researchers have conducted extensive series of numerical tests in order to gain better understanding, which in turn may lead to new theoretic advances in linking the global and local behaviour of dynamical systems. It should also be noticed that many numerical experiments have revealed rather surprising and still unexplained phenomena, like "abnormal" smoothness of period length (reported by P. Kurlberg).

- *Functional graphs*. There has been a recent burst in activity in the study of functional graphs generated by algebraic maps over finite fields. This comes from several independent groups of researchers (E. Bach & A. Bridy — S. Konyagin & B. Mans & L. Mathieson & I. E. Shparlinski — S. Liu & M. Zieve), who were not aware of each other's results prior to the workshop. In particular, this direction is motivated by the desire to understand and analyse better Pollard's rho-factorisation algorithm.

- *Representation and algebraic properties of iterates*. The goal is to construct DFF which are generated by multivariate polynomials with prescribed degree growth (e.g., polynomial growth vs. typically expected exponential growth) and admit a concise description of their iterations. In previous work, using just the degree argument has proved to be a very fruitful approach leading to a leap in the quality of results obtained and their applications. For example, this property led to new classes of pseudorandom number generators (PRNGs) with much better distribution properties, opening up a new direction in research.

  It has also been shown that "controlling" algebraic properties of iterates is a fundamental mathematical problem whose solution has multiple implications.

  Little progress has been made in this direction, and the only results known are mainly for univariate polynomials. Some questions which were researched and analysed during the workshop included, but were not limited to: irreducibility of iterations of irreducible polynomials (so-called *stability* of polynomials), the greatest common divisor of polynomial iterates (in particular co-primality), properties of the varieties defined by iterations

of polynomials, exponential and character sums with polynomial iterates, construction of new classes of permutation polynomials using iterations of polynomials, etc. Recently, several new approaches have emerged, attacking these problems from different angles.

One such approach relates the question to Somos sequences. Eric Bedford and Andrew Hone have several results in this direction and the next step would be to put them in a more unified form.

- *Group theoretic aspects*. The group of wild continuous automorphisms of the local field, $\mathbf{F_q}((\mathbf{t}))$, is an object of study both in group theory, as the *Nottingham group*, a source of examples of just-infinite pro-p groups, and in the theory of norm fields in algebraic number theory. By connecting the two independently emerging fields, I. Fesenko simultaneously produced a new family of just-infinite groups and a counter-example to the Coates-Greenberg conjecture. In the direction of dynamics, recent striking advances in finding explicit elements of finite order have been made by T. Chinburg, P. Symonds, and others.

  Moreover, Galois groups of iterates connect dynamics with the relatively new field of iterated monodromy groups. Properties of these groups, such as their size and their proportion of fixed point free elements, answer dynamical questions such as the proportion of primes dividing elements of an iteratively created integer sequence.

- *Applications*. Amongst many other applications, DFF lead to high quality PRNGs. The desirable features of PRNGs depend on the application and there are different quality measures. For example, in cryptography, unpredictability is the most crucial feature. Other common features include the absence of "hidden" linearities, low autocorrelation, and uniform distribution. The use of pseudorandom numbers in a wide range of applications like simulation, cryptography, wireless communication, etc., has made apparent a need for a large variety of generators with "good" behaviour with respect to some particular measures. Other applications include design and analysis of cryptographic hash functions based on iteration of polynomials, sequences over finite fields, quasi-Monte Carlo methods, and integrability, to mention just a few.

3 Open Problems

The following problems were suggested by several participants during the open problem session at this workshop.

Problem 1 (Voloch-Kurlberg)**.** *Let $f : X/\mathbb{Q} \to X/\mathbb{Q}$ and $f_p : X(\mathbb{F}_p) \to X(\mathbb{F}_p)$. We fix $x_0 \in X$ and let C_p be the cycle part of the orbit of f_p starting at x_0. It is expected that $|C_p| \sim p^{d/2}$ as p varies, where $d = \dim X$.*

1. *Is $|C_p|$, $|C_p|^{1/3}$-smooth with at least the same probability that a number of its size is smooth, i.e. does the size of the orbit behave like a random number of its size?*

   Excluding the obvious bad cases such as when the point lies on a periodic subvariety.

2. *Is $|C_p| \equiv 0 \mod 2$ at least 50% of the time?*

3. *$f_t : X \to X$ over $\mathbb{F}_q$, where $t \in \mathbb{F}_q$. Fix a point $x_0(t)$ and iterate. Now given the orbit C_t depending on t, ask the same question: is $|C_t|\ |C_t|^{1/3}$ smooth at least as often as a random number of its size?*

Problem 2 (Maubach)**.** *Let $E = (E_1, E_2, \ldots, E_n)$ where $E_i \in K[x_1, \ldots, x_n]$. E is called a* polynomial automorphism *if there exists $F = (F_1, \ldots, F_n)$ such that*

$$E \circ F = (x_1, \ldots, x_n).$$

Definition. *The equivalence relation: $E \sim E'$ if there exists F, G automorphisms such that*

$$F \circ E \circ G = E'.$$

If the univariate polynomials $p, q \in K[x]$ satisfy $p(x) \not\sim q(x)$, does $(p(x), y_1, \ldots, y_n) \not\sim (q(x), y_1, \ldots, y_n)$ hold? If $\mathrm{char}(K) = 0$, this is true. In $K = \mathbb{F}_2$, given

$$p(x) = x + x^2 + x^8$$
$$q(x) = x + x^4 + x^8$$

not equivalent:

1. *$(p(x), y) \not\sim (q(x), y)$?*
2. *$(p(x), y, z) \not\sim (q(x), y, z)$?*

Problem 3 (Anashin)**.** *Consider the following map $g : x \mapsto \frac{x(x+1)}{2}$ with $x \in \{0, \ldots, 2^n - 1\}$. Calculate $x \mapsto g(x) \mod 2^n$. For all $n \in \mathbb{N}$ this is a permutation.*

1. *Does there exist a polynomial (or rational function) $f(x) \in \mathbb{Z}_2[x]$ such that $x \mapsto f(g(x)) \mod 2^n$ is a single cycle (transitive) permutation for all n?*

Motivation: (Woodcock-Smart 1998, Yurov 1998)

Problem 4 (Ostafe)**.** *In the univariate case, over a field of characteristic zero, it is proved in [5] that the minimum number of terms necessary to express an iterate $f^{(n)}$ of a rational function f tends to infinity with n, provided f is not of an explicitly described special shape:*

We denote by T_d the Chebyshev polynomial of degree d defined by

$$T_d(x + x^{-1}) = x^d + x^{-d}.$$

Theorem 1 (Fuchs-Zannier (2012))**.** *Let $\mathbb{F}$ be a field of characteristic 0 and $f \in \mathbb{F}(X)$ of degree $d \geq 3$. Suppose that f is not conjugate (with respect to the group action given by $PGL_2(\mathbb{F})$ on $\mathbb{F}(X)$) to $\pm X^d$ or to $\pm T_d(X)$. Then, for any integer $n \geq 3$, we cannot express $f^{(n)}$ as a ratio of two polynomials having altogether less than $((n-2)\log d - \log 2016)/\log 5$ terms.*

For univariate polynomials over finite fields no results of this type are known, but it is clear that at least for some special classes of polynomials (e.g. linearised polynomials) or rational functions, such a result does not hold.

Moreover, in the multivariate case one can also show that an analogue of the result [5] does not hold anymore, and this happens over any field, not necessarily over finite fields, as the next example shows (known as the Nagata automorphism).

Let $m = 3$ and

$$F_1 = X_1 - 2X_2(X_1X_3 + X_2^2) - X_3(X_1X_3 + X_2^2)^2$$
$$F_2 = X_2 + X_3(X_1X_3 + X_2^2)$$
$$F_3 = X_3.$$

Then, for any $k \geq 1$,

$$F_1^{(k)} = X_1 - 2kX_2(X_1X_3 + X_2^2) - k^2X_3(X_1X_3 + X_2^2)^2,$$
$$F_2^{(k)} = X_2 + kX_3(X_1X_3 + X_2^2), \quad F_3^{(k)} = X_3.$$

What types of growth for the number of terms exist for iterates of

1. *univariate rational functions over finite fields?*
2. *multivariate polynomials in any characteristic?*

Problem 5 (Ostafe)**.** *Are there families of multivariate Deligne polynomials which are Deligne under iteration?*

Problem 6 (Ostafe)**.** *What is the parity of the number of k-periodic points for a polynomial over finite fields? or of all periodic points?*

Problem 7 (Hone)**.** *Consider a rational map $\phi : \overline{x} \mapsto E(\overline{x})$, $\phi \in \mathrm{End}(K(\overline{x}))$. Let $d_n = \deg \phi^n$ be the degree of the n^{th} iterate. The limit $\mathcal{E} = \lim_{n\to\infty} \frac{\log d_n}{n}$ is called the* entropy *of ϕ. Suppose that $\mathcal{E} = 0$ and d_n is not bounded.*

1. *Does there exist ϕ such that $d_n \not\sim Cn^k$ for some positive integer k (i.e., not polynomial growth). Known: For birational maps of the plane with $K = \mathbb{C}$ it is known that linear or quadratic growth of d_n are the sole possibilities, i.e. $k = 1, 2$ only (Diller and Favre 2001), and very precise information on the constant $C > 0$ has been obtained more recently (Blanc and Déserti 2012).*

2. *Do the two-dimensional results of Diller & Favre require any modification in the case $K = \mathbb{F}_p$?*

Problem 8 (Shparlinski)**.** *Known: given a finite set X and a random permutation f. The average cycle length should be approximately $|X|^{1/2}$, but the number N such that $f^{(N)} = id$ is larger. On average (over all permutations) $N \sim \exp\left(c_0(|X| / \log^2 |X|)^{1/3}\right)$, where $c_0 \approx 3.36$ (Schmutz, 2011).*

1. *Given $x_0 \in \mathbb{F}_q$ and any reasonable map f (polynomial, rational, etc). We expect $|C_p(x_0)| \sim q^{1/2}$. What about N such that*
$$f^{(N)} = id?$$

We may assume that f is a permutation, otherwise $N = \infty$.

Problem 9 (Elkies)**.** *Is there a rationally parametrized quadratic function that has a rational 6-cycle?*
An elliptic curve is known.

4 Presentation Highlights

Noam Elkies

Title: Some computations of dynamics of rational maps of degree 2
Abstract: We describe some computational techniques and results for arithmetic dynamics of algebraic maps $f : \mathbb{P}^1 \to \mathbb{P}^1$. The results include: 0) explicit models for Milnor's curves "Per_n/I" parametrizing cubic polynomial maps with an n-periodic critical point; 1) a degree-2 rational map $f(x) = (14 - 22x)/(28 - 57x + 20x^2)$ for which ∞ has canonical height about 0.0036, probably the minimal positive height (indeed the second-smallest might be $0 = f(\infty)$ with canonical height twice that of ∞); and 2) infinitely many inequivalent degree-2 maps with a 6-periodic rational point, such as $(x - 6)(23x - 25)/(x^2 - 115x - 60)$ with the 6-cycle $(0, -5/2, 3, 1/3, -1, 6)$.

Clements Fuchs

Title: Composite rational functions with few terms
Abstract: When solving Diophantine equations of separated variable type, i.e. equations of the form $f(x) = g(y)$, one needs to understand the possible decompositions of the polynomials f and g. I will start with some examples of problems of this form in order to give an impression of the kind of results one can give and then discuss the Bilu-Tichy criterion which gives a precise general description when such an equation has infinitely many solutions in integers. Afterwards, I shall address the question how to algorithmically describe all polynomials (with given degree, or with a given number of non-zero coefficients) which are composite, together with all their decomposition, in finite terms. The analogous question for rational functions seems to be more complicated. I shall discuss a result (jointly with Umberto Zannier) which can be seen as a first step towards the solution of the same problem for rational functions. The proof of these results use arguments from the theory of algebraic function fields (in particular the theory of S-unit equations over function fields). The talk ends with a number of open problems which we would like to solve in the future.

Andrew Hone

Title: *Cluster algebras and discrete integrable systems*
Abstract: We consider a large family of nonlinear rational recurrence relations which arise from mutations in cluster algebras defined by quivers. We explain how, due to the Laurent property, these nonlinear recurrences are ideal for iteration over finite fields.

The problem of determining which of the recurrences are integrable (in the sense of Liouville's theorem) is related to the notion of algebraic entropy, and via a series of conjectures related to tropical algebra, this leads to a very sharp criterion for the allowed degrees of the terms in the recurrence.

This is joint work with Allan Fordy: see http://arxiv.org/pdf/1207.6072.pdf for more details.

Ben Hutz

Title: *Sage functionality for dynamical systems*
Abstract: When studying dynamical systems it is often useful to be able to compute examples. Why it is possible to do so by hand, it can be quite time consuming. However, none of the major computer algebra systems have good support for dynamical systems. A project to implement such functionality for the open source system SAGE is underway. This talk will introduce SAGE, the current state of functionality for dynamical systems in SAGE, and future goals.

Par Kurlberg

Title: Arithmetic geometry applications of cycle lengths mod p
Abstract: We will investigate the relationship between periods of iterates of rational maps (reduced modulo p) and two questions from arithmetic dynamics, namely dynamical analogues of the Mordell-Lang conjecture (an infinite intersection of an orbit with a subvariety implies strong periodicity properties on the subvariety) and the Brauer-Manin problem (an empty intersection of an orbit with a subvariety follows from the adelic orbit closure having empty intersection with the subvariety.)

Reinhard Laubenbacher

Title: Functions over finite fields arising in systems biology
Abstract: High-dimensional dynamical systems over finite fields are being used to model the dynamics of molecular interaction networks in systems biology. This talk will describe the mathematical challenges that arise from the construction and analysis of such models, as well as some solutions.

Franco Vivaldi

Title: Non-Archimedean phenomena in torus and lattice maps
Abstract: Given a lattice, a fundamental domain, and a parquet matrix, one can constructs two (archimedean) dynamical systems, a torus map and a lattice map. Non-archimedean phenomena are observed in both systems. We discuss specific two-dimensional examples.

5 Scientific Progress Made

We briefly comment on some new results obtained, directions opened and feedback of participants during and after the workshop. We also expect that more results and papers will come out in the future as a result of the lectures, discussions and open problems posed during the workshop.

Noam Elkies posed and answered (positively) a question about the existence of rationally parametrized quadratic functions that have a rational 6-cycle, see Problem 9 above. Indeed, one can find a rational curve in the quotient moduli space $\mathbb{Q}/\langle\sigma\rangle$ that lifts to a rational curve in $\mathbb{Q}$. Explicitly, for each t such that the points

$$\infty,\ \frac{t^3+5t^2+2t+1}{(2t+1)(t^3+t^2+1)},\ 0,\ \frac{(t+2)(t^3-t^2-2t-1)}{2(t-1)(t+1)^2(2t+1)},\ 1,\ \frac{2(t+2)(2t+1)}{(t+1)(t^3+t^2+4t+3)}$$

on $\mathbf{P}^1$ are distinct, there is a rational function of degree 2 that permutes these six points cyclically. But there may be yet further rational curves, because most of the rational points on $\mathbb{Q}$ located by exhaustive search are still not explained by this parametrization, nor by the elliptic curve found earlier.

It is notable that, on the day of Elkies' talk, two workshop participants, Michelle Manes and Michael Zieve, noticed an arXiv preprint that gave much the same results as the last part of this talk. The overlap was not complete in either direction and so this will lead to joint work and a joint paper. We also learned of research by Trevor Hyde, a student of participant Rob Benedetto, finding a quadratic rational map with rational periodic point of order 7. Elkies also answered a question of Michelle Manes on Benford behavior of an elliptic divisibility sequence.

Studying the degree growth of iterations of rational functions is of great interest for the theory of dynamical systems and has been studied in a number of works, see, for example, [8, 18] and references therein. It is also important for applications to PRNGs and also for cryptography to get sequences of provable high linear complexity. Eric Bedford, Domingo Gomez-Perez, Andrew Hone, Alina Ostafe and Igor Shparlisnki had a series of meetings to discuss possible constructions of dynamical systems with slow (quadratic) degree growth. This collaboration is likely to lead to new important results on Somos sequences (degree growth and other properties of such sequences over finite fields) and PRNG's. Andrew Hone also started a project with Noam Elkies on a different (but related) problem.

Arne Winterhof, Andrew Hone and Stefan Maubach also had several discussions on multivariate polynomials with small degree growth which may find applications in cryptography or quasi-Monte Carlo methods. Moreover, discussions between Arne Winterhof, Domingo Gomez and Daniel Panario on analysis and construction of sequences for cryptography and wireless communication provided an excellent starting point for joint research.

Studying the cycle structure of "random" rational functions is a very challenging and hard problem. In this direction, as a result of several discussions between Igor Shparlinski and Eric Schmutz, the latter recently proved that for a fixed positive integer $d > 2$, for degree d polynomials f in $\mathbb{F}_p[x]$, the probability that the number of 2-cycles of f is bigger than 0 is at least $\frac{3}{8} + o(1)$. Based on this result, Igor Shparlinski asked the following: let G_f be the function graph of a polynomial f, and let N_f be the number of connected components of f. What can one say about $M(d, q) = \sum_{\deg f = d} N_f$? The result on 2-cycles of Eric Schmutz seems to imply $M(d, q) \geq f(d)q^{d+1}$, where $f(d) \to \infty$ as $d \to \infty$.

For other participants, the connections between algebraic and computational aspects were particularly fruitful. For example, after the talk by Ben Hutz, Michael Baake realised new possibilities for implementing results on dynamical zeta functions in a computer algebra setting.

John Roberts and Igor Shparlinski have started a joint project on the so-called *saturation index* of lattice equations.

John Roberts and Franco Vivaldi have started a new project on the growth of heights in symplectic maps with divided phase space. The idea is to provide an arithmetical tool (that bears some similarities with the Lyapounov exponent) for the characterisation of the nature of individual orbits (regular vs. irregular), and, more generally, of domains of phase space. The simplest non-trivial setting is that of piecewise affine maps with rational parameters. These maps are only partially understood. They plan to consider the asymptotic growth rate of both global and local (p-adic) heights (here p is a prime that divides the denominator of the parameters). For fixed height, all points in an elliptic island can be shown to have the same exponential growth rate, even though the convergence to this rate is non-uniform. More challenging will be the study of heights on (non-smooth) invariant curves. The existence of such curves has been established only in very special cases, and it is hoped that these methods will shed some light on their existence. Preliminary numerical experiments, performed at BIRS, have been very promising. In particular, the behaviour of heights on some (conjectured) invariant curves was found to differ markedly from that of chaotic orbits.

Vladimir Anashin, Andrew Hone and Franco Vivaldi had very fruitful discussions and have started a new collaboration in the area of p-adic dynamical systems.

Ben Hutz and Adam Towsley developed several ideas for new collaborations both regarding future SAGE functionality and a project about finding points and primes in $\mathbb{C}(t)$ for which a given point has a specified finite orbit portrait modulo p.

Par Kurlberg, Adam Towsley and Felipe Voloch finalised a joint project, as well as outlined some further project directions.

Par Kurlberg and Robert Benedetto discussed some quite promising approaches to the dynamical Mordell–Lang conjecture.

Par Kurlberg and Joachim Rosenthal discussed some very intriguing ideas on integer factoring using dynamical

systems approaches, and Par Kurlberg will visit Joachim Rosenthal in Zurich within the next year to continue with this project.

Rob Benedetto, Nigel Boston, and Rafe Jones had fruitful discussions on factorization of iterates of quadratic polynomials and which ones should have atypical behavior. Rob Benedetto related some observations of Nigel Boston to the Mandelbrot set, which has led to writing of a paper this summer. Nigel Boston showed Rafe Jones a short Frattini subgroup argument to handle a question on iterated monodromy groups that now Richard Pink has produced a preprint on.

Due to the diversity of research directions of the participants, many of them were exposed to new problems and lines of thinking. For example, for Stefan Maubach, whose interests lie in multivariate maps, many of the things he learnt during this workshop about univariate maps are also interesting to be considered for the special types of multivariate maps he is familiar with. An example that he gives is considering directed graphs of polynomial maps over finite fields. He would be interested to see what one gets for certain multivariate endomorphisms - like Keller maps. Can you see from the graph if it has a high(er) probability of being a Keller map? He also confesses: "The conference may have rerouted (part of) my research into a different direction, away from the "geometry" part of affine algebraic geometry, towards more discrete topics, like random number generation, statistical properties of maps, graphs, etc."

6 Outcome of the Meeting

This workshop opened a flood gate for new ideas, problems, and methods as well as concrete results in this area, some of them mentioned above. Bringing together the aforementioned researchers so that they can combine their techniques (and of course, intellectual efforts) will certainly lead to groundbreaking results.

The main outcome of the workshop has been in establishing new collaborations between researchers from different areas (number theory, commutative algebra, dynamical systems, etc.) pursuing similar or related problems from different perspectives and often being unaware of each other achievements. In particular we quote Joachim von zur Gathen:

> *As a senior researcher, I know most scientists (except for newcomers) at most conferences that I attend. This workshop was different. The organizers have put together an interesting group of people working on related problems but from very different directions, many of whom I had not met before. I saw many interesting problems and perspectives. In fact, I will study some of the problems that were posed at the workshop. Several colleagues commented to me along the same lines. Great applause to the organizers for putting together an unusual and highly successful list of participants.*

see `http://www.birs.ca/events/2013/5-day-workshops/13w5141/testimonials` for this and other feedbacks.

For most of the participants, the workshop also brought new contacts and opened new directions of research, collaborations, invitations to research seminars and conferences, etc. For example, this workshop led to invitations of some of the participants of the workshop to the special semester in Linz on applications of algebra and number theory, see `www.ricam.oeaw.ac.at/specsem/specsem2013/`, and also to the "Workshop on Polynomials over Finite Fields: Functional and Algebraic Properties" to be held at CRM, Belaterra (Spain), May 19-23, 2014, see `www.crm.cat/en/Activities/Pages/ActivityFoldersAndPages/Curs%202013-2014/WK%20Polynomials/Workshop-on-Polynomials-over-Finite-Fields.aspx`.

Last, but not least, this workshop was also a good platform for people to come together and plan future research activities, putting together proposals for workshops/conferences and discussing other organizational and editorial aspects of such activities.

References

[1] E. Bach and A. Bridy, 'On the number of distinct functional graphs of affine-linear transformations over finite fields', *Linear Algebra Appl.*, (to appear).

[2] R. Beals, J. Wetherell and M. Zieve, 'Polynomials with a common composite', *Israel J. Math.*, **174** (2009), 93–117.

[3] R. L. Benedetto, D. Ghioca, B. Hutz, P. Kurlberg, T. Scanlon and T. J. Tucker, 'Periods of rational maps modulo primes', *Math. Ann.* **355** (2013), 637–660.

[4] P. Flajolet and A. M. Odlyzko, 'Random mapping statistics', *Lecture Notes in Comput. Sci.*, vol. 434, Springer-Verlag, Berlin, 1990, 329–354.

[5] C. Fuchs and U. Zannier, 'Composite rational functions expressible with few terms', *J. Europ. Math. Soc.*, **14** (2012), 175–208.

[6] D. Ghioca, T. Tucker and M. Zieve, 'Intersections of polynomial orbits, and a dynamical Mordell-Lang conjecture', *Invent. Math.*, **171** (2008), 463–483.

[7] D. Ghioca, T. Tucker, and M. Zieve, 'Linear relations between polynomial orbits', *Duke Math. J.*, (to appear).

[8] B. Hasselblatt and J. Propp, 'Degree growth of monomial maps', *Ergodic Theory and Dynamical Systems*, **27** (2007), 1375–1397.

[9] A. Hone, 'Singularity confinement for maps with the Laurent property', *Phys. Lett. A.*, (to appear).

[10] D. Jogia, J.A.G. Roberts and F. Vivaldi, 'An algebraic geometric approach to integrable maps of the plane', *J. Phys. A: Math. Gen.*, **39** (2006), 1133–1149.

[11] A. MacFie and D. Panario, 'Random mappings with restricted preimages, *Lecture Notes in Comput. Sci.*, vol. 7533, Springer-Verlag, Berlin, 2012, 254–270.

[12] P. Morton, 'Arithmetic properties of periodic points of quadratic maps. II', *Acta Arith.*, **87** (1998), 89–102.

[13] P. Morton and J. H. Silverman, 'Rational periodic points of rational functions', *Internat. Math. Res. Notices*, **2** (1994), 97–110.

[14] J. A. G. Roberts and F. Vivaldi, 'Arithmetical method to detect integrability in maps', *Phys. Rev. Lett.*, **90** (2003), 034102.

[15] J. A. G. Roberts and F. Vivaldi, 'A combinatorial model for reversible rational maps over finite fields', *Nonlinearity*, **22** (2009), 1965–1982.

[16] E. Schmutz, 'Period lengths for iterated functions', *Combinatorics, Probability and Computing*, v.20, (2011), 289–298.

[17] J. H. Silverman, 'Variation of periods modulo p in arithmetic dynamics', *New York J. Math.*, **14** (2008), 601–616.

[18] C.-M. Viallet, 'Algebraic dynamics and algebraic entropy', *Int. J. Geom. Methods Mod. Phys.*, **5** (2008), 1373–1391.