Mathematisches Forschungsinstitut Oberwolfach

Report No. 54/2004

Finite Fields: Theory and Applications

Organised by
Joachim von zur Gathen (Paderborn)
Igor E. Shparlinski (Sydney)
Henning Stichtenoth (Essen)

December 5th – December 11th, 2004

Abstract. Finite fields are the focal point of many interesting geometric, algorithmic and combinatorial problems. The workshop was devoted to progress on these questions, with an eye also on the important applications of finite field techniques in cryptography, error correcting codes, and random number generation.

Mathematics Subject Classification (2000): 11Txx, 14Gxx, 68W30.

Introduction by the Organisers

The workshop *Finite Fields: Theory and Applications* was organized by Joachim von zur Gathen (Bonn), Igor Shparlinski (Sydney), and Henning Stichtenoth (Essen), and ran from 5 to 11 December 2004. Its forty participants, with a wide geographical distribution, enjoyed the hospitality of the Mathematical Research Institute, and its beautiful surroundings. Two previous meetings on the topic had been held in 1997 and 2001. The schedule consisted of three plenary talks each morning, and specialized sessions later in the day, with vast time for discussions and collaborative work. The traditional Wednesday afternoon hike was blessed with wonderful sunny weather and the compulsory Black Forest cake reward at the end.

Very broadly, we can distinguish seven subject areas:

- structure of finite fields,
- field towers,
- points on varieties,
- error-correcting codes,

- computation,
- combinatorics,
- cryptography.

Of course, many of the results presented bridge between two or more of these areas. The abstracts that follow speak for themselves. Avoiding an exhaustive discussion, we now mention one particular talk from each of the seven areas.

The *structure theory* includes questions about polynomials. The well-known Hansen-Mullen conjecture (whose second author was in the audience) was stated in 1992 and asserts that for any finite field $\mathbb{F}_q$, integers n and m with $0 < m < n$ and $a \in \mathbb{F}_q$, there exists a monic primitive polynomial in $\mathbb{F}_q[x]$ of degree n having a as the coefficient of x^m; there are a few well-known exceptional cases where this fails to hold. Cohen presented a proof of this conjecture at degrees $n \geq 9$, assuring the audience that smaller values of n are also under consideration.

Towers of function fields are of great interest because they may yield good algebraic-geometric codes. Beelen introduced a recursive construction of such towers, using a certain type of Fuchsian differential equations. They can be obtained from modular curves, and in some cases can be shown to be asymptotically optimal (in terms of the parameters of the resulting codes).

A conjecture concerning *points on varieties* was stated by Heath-Brown. Namely, he considers a nonsingular nonlinear hypersurface X in $\mathbb{P}^n$ defined over $\mathbb{Q}$, considers the number $N(B)$ of points on X with rational integral coefficients absolutely bounded by B, and conjectures that this number is $O(B^{n-1+\epsilon})$ for any positive ϵ. Browning presented his proof of this conjecture in all cases, with the possible exceptions $d = 3, 4$ and $n = 7, 8$.

In the theory of *error-correcting codes*, finite fields were fundamental from its beginning in the 1940s. Their importance was heightened by the construction of codes from algebraic curves over finite fields. Voloch discussed a different connection: the quadratic residue codes. It is unknown whether subfamilies of them can yield asymptotically good codes. Voloch showed that there exist subfamilies that do not yield good codes. This is based on an expression of the minimal distance by exponential sums, due to Helleseth, and estimates on the smallest prime that splits completely in a number field.

For *computation*, a difficult class of objects are bivariate polynomials presented in a particularly generous format, namely as a sum of terms where the exponents are written in binary (or decimal). Thus we look at polynomials of humongous degrees. Kaltofen presented two results which illuminate the wide range of behavior for questions about such polynomials. Over the rational numbers, he can compute the linear and quadratic factors in polynomial time. Over a large finite field, testing irreducibility is NP-hard (under randomized reductions).

As a question from *combinatorics*, we give the following illustrative example. A sum-free set A in an additive group G is such that $x+y \neq z$ for all $x, y, z \in A$. For instance the additive group $G = \mathbb{Z}_p$ for a prime p and $A = \{n, n+1, \ldots, 2n-1\}$ for $n = \lfloor (p+1)/3 \rfloor$ is a sum-free set. We can also multiply each element of A by a fixed nonzero element of $\mathbb{Z}_p$. When $p \equiv 2 \bmod 3$, no other sum-free subsets of $\mathbb{Z}_p$

exist. Lev shows that assumption $\#A \geq 0.33p$ implies that A is contained in the corresponding interval or a dilation of it.

In *cryptography*, a central question is the conjectured difficulty of computing the discrete logarithm in certain groups. The method of index calculus provides a subexponential algorithm in the unit groups of finite fields. Elliptic curves owe their popularity in cryptography to the absence, so far, of any discrete logarithm computation of comparable efficiency. Semaev presented an approach, rather speculative at this point, aimed at finding such a method; it works with the new notion of summation polynomials which vanish at the x-coordinates of points that sum to 0 on the curve.

Workshop: Finite Fields: Theory and Applications

Table of Contents

Plenary lectures

Special sessions

Abstracts

Plenary lectures

Rédei polynomials and some applications to finite geometry

Simeon Ball
(joint work with Michel Lavrauw)

A polynomial with coefficients from a finite field $GF(q)$ that is the product of linear polynomials is usually referred to as a *Rédei polynomial*. This is due to the appearance of the polynomial

$$R(T,S)=\prod_{(x,y)\in\mathcal{A}}(T-xS+y),$$

where $\mathcal{A}$ is some subset of $GF(q)^2$, in the book of Rédei [5] from the early seventies.

In the affine plane $AG(2,q)$ the point (x,y) is incident with the line $Y=mX+\alpha$ if and only if $\alpha=-mx+y$. Hence α is a root of $R(T,m)$ of multiplicity k if and only if the line $Y=mX+\alpha$ is incident with k points of the set $\mathcal{A}$. This observation allows one to look at a problem of the following type: Given a subset of points of the affine plane that has restricted intersection properties with the lines of the plane, say something about the size of the subset or, clearly better, determine the possibilities for such a subset.

The problem for which Rédei introduced the polynomial $R(T,S)$ was that of classifying those functions over a finite field that determine few directions. Given a set of q points $\mathcal{A}$ in $AG(2,q)$ each line of a set of q parallel lines is either incident with exactly one point of $\mathcal{A}$ or there is a line incident with at least two points of $\mathcal{A}$. In the latter case we say that the direction corresponding to the parallel class of the line is determined by $\mathcal{A}$. The problem of classifying those functions over a finite field that determine few directions is equivalent to classifying those subsets $\mathcal{A}$ that determine few directions. It is also equivalent to classifying those functions f over a finite field such that the map

$$x\mapsto f(x)+cx$$

is a permutation of $GF(q)$ for a large number of $c\in GF(q)$.

Rédei proved the following theorem which is the first example of what is known as a "mod p" result. Throughout, $q=p^h$ and p is prime.

Theorem 1 ([5]). *If $\mathcal{A}$ is a set of q points of $AG(2,q)$ determining less than $(q+3)/2$ directions then any line that is spanned by two points of $\mathcal{A}$ is incident with 0 mod p points of $\mathcal{A}$.*

In [4] and [1] (for characteristic 2 and 3) it was shown that all functions that determine less than $(q+3)/2$ directions are linear over some subfield of $GF(q)$.

In this talk we concentrate on the analogue of this problem in higher dimensional subspaces. The results in the planar case allow us to classify sets of points that determine very few directions. However, using Rédei polynomials in many indeterminates, we can prove a similar theorem to Theorem 1 in higher dimensional spaces, that applies to sets of points that determine quite a lot of directions.

Theorem 2 ([2]). *Let $\mathcal{A}$ be a set of q^{n-1} points of $AG(n,q)$ and let N be the number of directions not determined by $\mathcal{A}$. If $N \geq p^e q$ for some $e \in \{0,1,\ldots,h-1\}$ then every hyperplane meets $\mathcal{A}$ in 0 mod p^{e+1} points.*

There are some immediate corollaries of Theorem 2 that relate to ovoids of the generalised quadrangles $T_2(O)$ or $T_2^*(O)$ and some questions which arise in the case when q is prime. These will be discussed.

References

[1] S. Ball, The number of directions determined by a function over a finite field, *J. Combin. Theory Ser. A*, **104** (2003) 341–350.

[2] S. Ball and M. Lavrauw, How to use Rédei polynomials in higher dimensional spaces, `www-ma4.upc.es/~simeon/catania.pdf`

[3] S. Ball and M. Lavrauw, On functions in two variables over a finite field that do not determine all directions and some consequences for ovoids of generalised quadrangles, `www-ma4.upc.es/~simeon/quadrangledirections.pdf`.

[4] A. Blokhuis, S. Ball, A. E. Brouwer, L. Storme and T. Szőnyi, On the number of slopes of the graph of a function defined over a finite field, *J. Combin. Theory Ser. A*, **86** (1999) 187–196.

[5] L. Rédei, *Lacunary Polynomials over finite fields*, North-Holland, Amsterdam, 1973.

Asymptotically good towers and differential equations

Peter Beelen

(joint work with Irene I. Bouw)

Let p be a prime and $\mathbb{F}_q$ a finite field of characteristic p. We are interested in obtaining a tower of absolutely irreducible algebraic curves defined over $\mathbb{F}_q$, with many rational points:

$$X_0 \leftarrow X_1 \leftarrow X_2 \leftarrow \cdots .$$

We are particularly interested in the case that the curves are defined recursively; i.e.,

$$X_n = \{(x_0, x_1, \ldots, x_n) \in X_0^{n+1} \mid h(x_i) = g(x_{i-1}), 1 \leq i \leq n\}, \tag{1}$$

where $(g,h) : X_0 \rightrightarrows X_{-1}$ is a correspondence and X_{-1} an absolutely irreducible algebraic curve both defined over $\mathbb{F}_q$.

We will now use the theory of Fuchsian differential equations (see e.g. [3, 4]). Let L be a Fuchsian differential equation of order two on X_{-1}. We say that the

correspondence $(g,h) : X_0 \rightrightarrows X_{-1}$ is adapted to L if the pullback differential equations on X_0 under g and h are equivalent. Given such a correspondence adapted to a certain Fuchsian differential equation, we study the tower of curves defined as in equation (1). We show that under some technical conditions, such a tower is asymptotically good. Examples of correspondences adapted to a differential equation can be obtained by using the theory of modular curves. The resulting towers are towers of modular curves (see [1]).

Now suppose we are given a correspondence $(g,h) : X_0 \rightrightarrows X_{-1}$ of degree one adapted to a Fuchsian differential equation L on X_{-1} and a map $f : Y_{-1} \to X_{-1}$. We show that there exist an absolutely irreducible algebraic curve Y_0, a Fuchsian differential equation L_f on Y_{-1} and a correspondence $(\widetilde{g},\widetilde{h}) : Y_0 \rightrightarrows Y_{-1}$ adapted to L_f. This construction enables one to find new asymptotically good towers. In particular we study the correspondence $(g,h) : \mathbb{P}^1 \rightrightarrows \mathbb{P}^1$ with $h(t) = t^2$ and $g(t) = -t(t-1)/(t+1)$. We show that this correspondence can be seen as a pullback from a correspondence mentioned in [2]. In particular we show that the resulting tower of curves is asymptotically optimal over the field $\mathbb{F}_{p^2}$ if $p \equiv \pm 1 \bmod 8$.

References

[1] N.D. Elkies, *Explicit modular towers*, Proceedings of the 35-th annual Allerton conference on communication, control and computing (Urbana, 1997), 1998, 23–32.

[2] A. Garcia and H. Stichtenoth (with an appendix by H. Rück), *On tame towers over finite fields*, J. Reine Angew. Math. **557** (2003), 53–80.

[3] T. Honda, *Algebraic differential equations*, Symposia Mathematica, Vol. XXIV (Sympos. INDAM, Rome, 1979), Academic Press, London, 1981, 169–204.

[4] N.M. Katz, *Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin*, Inst. Hautes Études Sci. Publ. Math. **39** (1970), 175–232.

Rational points on non-singular hypersurfaces

Timothy D. Browning

(joint work with D.R. Heath-Brown)

For any $n \geq 2$ let $X \subset \mathbb{P}^n$ be a non-singular hypersurface of degree d defined over the field $\mathbb{Q}$ of rational numbers. Since the time of Diophantus of Alexandria, mankind has seeked to better understand the set $X(\mathbb{Q}) = X \cap \mathbb{P}^n(\mathbb{Q})$ of $\mathbb{Q}$-rational points on X. One of the most basic questions that can be asked is: how large is $X(\mathbb{Q})$ whenever it is non-empty?

The purpose of this note is to discuss recent attempts to develop an answer to this question in the case that $X(\mathbb{Q})$ is infinite. For this one usually defines the height of a point $x = [x_0, \dots, x_n] \in \mathbb{P}^n(\mathbb{Q})$ to be $H(x) = \max_{0 \leq i \leq n} |x_i|$, provided that $x_0, \dots, x_n \in \mathbb{Z}$ and h.c.f.$(x_0, \dots, x_n) = 1$. The goal is then to study the asymptotic behaviour of the quantity

$$N_X(B) = \#\{x \in X(\mathbb{Q}) : H(x) \leq B\},$$

as $B \to \infty$, and if possible to relate it somehow to the geometry of X. Whenever $d = 1$ or 2 this quantity is well understood, and it is not hard to establish the estimate

$$N_X(B) = c_X B^{n+1-d}\Big(1 + o(1)\Big),$$

for some constant $c_X > 0$. Whenever d is suitably small compared with n, it is also possible to prove the same asymptotic formula via the circle method [2]. For intermediate values of d the problem of describing $N_X(B)$ becomes much harder. For example we know of only a single rational point on the threefold

$$x_0^5 = x_1^5 + x_2^5 + x_3^5 + x_4^5,$$

this being the solution $\mathbf{x} = (144, 27, 84, 110, 133)$ found by Lander and Parkin [9]. In fact this provided the first counter-example to a conjecture of Euler that no kth power can be written as the sum of $k - 1$ kth powers.

It is now time to discuss the motivation behind much of my recent research. This is the following conjecture due to Heath-Brown [8, Conjecture 2].

Conjecture 1. *Suppose that $X \subset \mathbb{P}^n$ is a non-singular hypersurface of degree $d \geq 2$ and let $\varepsilon > 0$. Then we have $N_X(B) = O(B^{n-1+\varepsilon})$.*

Here, and throughout this note, the implied constant may depend at most upon d, n and the choice of ε. Although one might also ask about bounds where the implied constant is allowed to depend arbitrariliy on X, it transpires that uniform estimates are much more useful in applications and in most cases aren't much harder to prove. Conjecture 1 is essentially best possible when $d = 2$ or $n \leq 3$, but is almost certainly not so otherwise. In this setting Conjecture 1 is a weaker version of the following conjecture due to Batyrev and Manin [1].

Conjecture 2. *Let $d \geq 3, n \geq 4$, and suppose that $X \subset \mathbb{P}^n$ is a non-singular hypersurface of degree d. Then there exists $\delta > 0$ such that $N_X(B) = O(B^{n-1-\delta})$.*

In this note I shall focus only upon Conjecture 1, and begin by presenting a table which charts the progress made towards it in recent years. The table presents values of $\theta = \theta_{d,n} \in \mathbb{R}$ for which an upper bound of the form

$$N_X(B) = O(B^{n-1+\theta+\varepsilon}),$$

holds for all non-singular hypersurfaces $X \subset \mathbb{P}^n$ of degree $d \geq 2$. Conjecture 1 is the statement that one can take $\theta = 0$ in every case.

θ	Restrictions?	Who?	How?
$= \frac{1}{2}$	none	Cohen [11]	large sieve
$= \frac{2}{n+1}$	none	Fujiwara [6]	exponential sums
$= \frac{1}{d}$	none	Pila [10]	plane sections
$= 0$	$n \geq 9$	Heath-Brown [7]	exponential sums
$= 0$	$d = 2$ or $n \leq 3$	Heath-Brown [8]	plane sections
$= 0$	$d \geq 4, n = 4$	Browning [3]	plane sections
$= 0$	$d = 3, n = 4$	Browning, Heath-Brown [4]	lattice methods

It remains to provide a brief account of the latest developments in this exciting area. The rest of this note describes ongoing joint work with Heath-Brown. The following result establishes Conjecture 1 provided that the degree of the hypersurface is large enough.

Theorem 1. *Conjecture 1 holds if* $d \geq 5$.

The main idea in the proof of Theorem 1 is a clever induction argument due to Pila [10]. This renders it sufficient to study the distribution of integer points on non-singular affine surfaces of degree at least 5, for which the techniques developed by Heath-Brown [8] are enough. An account of this method can be found in [5], where it is employed to tackle a version of Conjecture 1 that applies to singular hypersurfaces. A fundamental component of the technique involves fixing a suitable prime p, and then analysing the points $x \in X(\mathbb{Q})$ that have height $H(x) \leq B$, and that reduce to a fixed point $\pi \in X(\mathbb{F}_p)$. Two further ingredients in the proof are the geometry of numbers and the well-known estimate $\#X(\mathbb{F}_p) = O(p^{n-1})$ due to Lang and Weil.

Once combined with the results in the table, Theorem 1 therefore implies that in order to establish Conjecture 1 completely it only remains to handle non-singular hypersurfaces $X \subset \mathbb{P}^n$ of degree d for

$$d \in \{3, 4\}, \quad n \in \{5, 6, 7, 8\}.$$

To tackle these eight cases we utilise an earlier result due to myself and Heath-Brown [4, Theorem 4]. This shows that every point counted by $N_X(B)$ must lie on one of a small number of linear subspaces contained in X. Again, the proof of this result rests upon considering the points in $X(\mathbb{Q})$ that have height at most B and reduce to a fixed point $\pi \in X(\mathbb{F}_p)$ for a suitably large prime p. In order to handle the remaining cases one is therefore led to study the Fano variety

$$F_k(X) = \{\Lambda \in \mathbb{G}(k, n) : \Lambda \subset X\}$$

of k-planes contained in X. The geometry of Fano varieties is a topic that has enjoyed significant development recently. The reader is no doubt familiar with the classical example of cubic surfaces: when $d = n = 3$ it has long been know that $F_1(X)$ has dimension 0 and degree 27. By drawing upon such tools from algebraic geometry, and combining this with techniques from analytic number theory and finite fields we have so far succeeded in establishing the following result.

Theorem 2. *Conjecture 1 holds possibly unless* $d \in \{3, 4\}$ *and* $n \in \{7, 8\}$.

As indicated above, this is a topic that is still very much under investigation and we are optimistic that a final resolution of Conjecture 1 is now within reach.

References

[1] V. Batyrev and Y.I. Manin, Sur le nombre des points rationnels de hauteur bornée des variétés algébriques, *Math. Ann.*, 286 (1990), 27–43.

[2] B.J. Birch. Forms in many variables, *Proc. Roy. Soc. Ser. A*, 265 (1961), 245–263.

[3] T.D. Browning, A note on the distribution of rational points on threefolds, *Quart. J. Math.*, 54 (2003), 33–39.

[4] T.D. Browning and D.R. Heath-Brown, Counting rational points on hypersurfaces, *J. Reine Angew. Math.*, to appear.
[5] T.D. Browning, D.R. Heath-Brown and P. Salberger, Counting rational points on algebraic varieties, 2004. Submitted.
[6] M. Fujiwara, Upper bounds for the number of lattice points on hypersurfaces, *Number theory and combinatorics, Japan*, (1984), 89–96.
[7] D.R. Heath-Brown, The density of rational points on non-singular hypersurfaces, *Proc. Indian Acad. Sci.*, 104 (1994), 13–29.
[8] D.R. Heath-Brown, The density of rational points on curves and surfaces, *Annals of Math.*, 155 (2002), 553–595.
[9] L.J. Lander and T.R. Parkin, Counterexample to Euler's conjecture on sums of like powers, *Bull. Amer. Math. Soc.*, 72 (1966) 1079.
[10] J. Pila, Density of integral and rational points on varieties, *Astérisque*, 228 (1995), 183–187.
[11] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, 1989.

Computing Modular Polynomials

Denis Charles
(joint work with Kristin Lauter)

The ℓ^{th} modular polynomial, $\phi_\ell(x, y)$, parameterizes pairs of elliptic curves with an isogeny of degree ℓ between them. Modular polynomials provide the defining equations for modular curves, and are useful in many different aspects of computational number theory and cryptography. For example, computations with modular polynomials have been used to speed elliptic curve point-counting algorithms ([2] Chapter VII).

The standard method for computing modular polynomials consists of computing the Fourier expansion of the modular **j**-function and solving a linear system of equations to obtain the integral coefficients of $\phi_\ell(x, y)$ ([3]). The computer algebra package MAGMA [4] incorporates a database of modular polynomials for ℓ up to 59.

Our idea is to compute the modular polynomial directly modulo a prime p, without first computing the coefficients as integers. Once the modular polynomial has been computed for enough small primes, our approach can also be combined with the Chinese Remainder Theorem (CRT) approach as in [1] to obtain the modular polynomial with integral coefficients or with coefficients modulo a much larger prime using Explicit CRT. Our algorithm does not involve computing Fourier coefficients of modular functions.

The idea of our algorithm is as follows. Mestre's algorithm, the *Méthode des graphes* [5], uses the ℓ^{th} modular polynomial modulo p to navigate around the connected graph of supersingular elliptic curves over $\mathbb{F}_{p^2}$ in order to compute the number of edges (isogenies of degree ℓ) between each node. From the graph, Mestre then obtains the ℓ^{th} Brandt matrix giving the action of the ℓ^{th} Hecke operator on

modular forms of weight 2. The main idea of our algorithm is to do the reverse: we compute the ℓ^{th} modular polynomial modulo p by computing all the isogenies of degree ℓ between supersingular curves modulo p via Vélu's formulae (see [6]). Specifically, for a given **j**-invariant of a supersingular elliptic curve over $\mathbb{F}_{p^2}$, Algorithm 1 computes $\phi_\ell(x, j)$ modulo p by computing the $\ell + 1$ distinct subgroups of order ℓ and computing the **j**-invariants of the $\ell + 1$ corresponding ℓ-isogenous elliptic curves. Algorithm 2 then uses the connectedness of the graph of supersingular elliptic curves over $\mathbb{F}_{p^2}$ to move around the graph, calling Algorithm 1 for different values of j until enough information is obtained to compute $\phi_\ell(x, y)$ modulo p via interpolation.

There are several interesting aspects to Algorithms 1 and 2. Algorithm 1 does not use the factorization of the ℓ-division polynomials to produce the subgroups of order ℓ. Instead we generate independent ℓ-torsion points by picking random points with coordinates in a suitable extension of $\mathbb{F}_p$ and taking a scalar multiple which is the group order divided by ℓ. This turns out to be more efficient than factoring the ℓ^{th} division polynomial for large ℓ. This approach also gives as a corollary a very fast way to compute a random ℓ-isogeny of an elliptic curve over a finite field for large ℓ.

Algorithm 2 computes $\phi_\ell(x, y)$ modulo p by doing only computations with supersingular elliptic curves in characteristic p even though $\phi_\ell(x, y)$ is a general object giving information about isogenies between elliptic curves in characteristic 0 and ordinary elliptic curves in characteristic p. The advantage that we gain by using supersingular elliptic curves is that for all the supersingular elliptic curves, we can show that the full ℓ-torsion is defined over an extension of degree dividing $6(\ell - 1)$ of the base field $\mathbb{F}_{p^2}$, whereas in general the field of definition can be of degree $\ell^2 - 1$.

References

[1] Agashe, A.; Lauter, K.; Venkatesan, R.; *Constructing Elliptic Curves with a known number of points over a prime field*, in Lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Institute Communications Series, **42**, 1-17, 2003.

[2] Blake, I.; Seroussi, G.; Smart, N.; *Elliptic Curves in Cryptography*, Lond. Math. Soc., Lecture Note Series, **265**, Cambridge University Press, 1999.

[3] Elkies, Noam; *Elliptic and modular curves over finite fields and related computational issues*, in Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A.O.L. Atkin (D.A. Buell and J.T. Teitelbaum, eds.), AMS/International Press, 21-76, 1998.

[4] Bosma, W.; Cannon, J.; *Handbook of MAGMA functions,* Sydney, 2003.

[5] Mestre, J.-F.; *La méthode des graphes. Exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields, Nagoya Univ., Nagoya, 217-242, 1986.

[6] Vélu, Jacques; *Isogénies entre courbes elliptiques*, C. R. Acad. Sc. Paris, **273**, 238-241, 1971.

The Hansen-Mullen conjecture for primitive polynomials

Stephen D. Cohen

Let $\mathbb{F}_q$ be the finite field of order q, a power of its (prime) characteristic p. Its multiplicative group is cyclic of order $q-1$: a generator is called a *primitive element* of $\mathbb{F}_q$. More generally, a primitive element γ of the unique extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ of degree n is the root of a (monic) *primitive* polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n (automatically irreducible). All roots of f (conjugates of γ) are primitive elements of $\mathbb{F}_{q^n}$. In 1992, T. Hansen and G. L. Mullen [14] stated a natural conjecture on the existence of a primitive polynomial of degree n over $\mathbb{F}_q$ with an arbitrary coefficient prescribed.

Conjecture 1 (Hansen and Mullen)**.** *Let $a \in \mathbb{F}_q$ and let $n \geq 2$ be a positive integer. Fix an integer m with $0 < m < n$. Then there exists a primitive polynomial $f(x) = x^n + \sum_{j=1}^{n} a_j x^{n-j}$ of degree n over $\mathbb{F}_q$ with $a_m = a$ with (genuine) exceptions when*

$$(q, n, m, a) = (q, 2, 1, 0),\ (4, 3, 1, 0),\ (4, 3, 2, 0) \text{ or } (2, 4, 2, 1).$$

Like many plausible hypotheses in number theory, this conjecture is difficult to establish in full generality. *Asymptotically*, it has shown it to be true [8] for fixed n and sufficiently large q: applicability, however, is conditional when $m = \frac{n}{2}$ or $\frac{n+1}{2}$. At the time of its formulation, the conjecture had been already been established when $m = 1$, [1]. For $n = m - 1$, it follows from [2], [4], [5]. The papers [13] and [7] cover most cases with $m = 2$ and $n \geq 5$. For $m = 3$, the conjecture holds provided $n \geq 7$ by [9], [10], [15] and [6]. Further, it follows from [3] whenever $m \leq \frac{n}{3}$. Finally, for *even* prime powers q and *odd* degrees n it has shown by Fan and Han [11] provided $n \geq 7$.

Inspired by this last item, we now prove the conjecture for all q and m whenever $n \geq 9$. Further work is currently in hand to extend it to *all* values of n.

Theorem 1. *Assume that $n \geq 9$. Then the Hansen-Mullen conjecture holds.*

Take the candidate for a primitive polynomial to be $f(x) = x^n \cdots + a_m x^{n-m} + \cdots + a_n \in \mathbb{F}_q$. When $m > \frac{n}{2}$, provided that a_n is also suitably prescribed, one can replace $f(x)$ by its reciprocal polynomial $a_n^{-1} x^n f(1/x)$ and thereby m by $n - m$ to suppose that $m \leq \frac{n}{2}$. The characteristic difficulty encountered when $p > m$ is overcome by developing the p-adic method introduced by Fan and Han in their papers cited above (and also used in [3]). Because character sum estimates over $\mathbb{F}_{q^n}$ of the shape $O(q^{n/2})$ feature, it is inevitable that values of m close to $\frac{n}{2}$ are particularly delicate (as indicated in the papers already quoted). It is a consequence of the work of Fan and Han (for example in [11]) that the m-th coefficient a_m can be prescribed by fewer than m conditions. It is a key step in the present paper that this can be strengthened to require at most $\frac{m}{2} + 1$ conditions. Because this is generally significantly less than $\frac{n}{2}$, one can progress to the proof. Observe that it is successively *smaller* values of n that are more difficult. Hence in this paper we consider values of $n \geq 9$ and, to avoid overburdening with numerical

details, defer smaller values for consideration in later articles. Indeed, most of the numerical activity is to check that, in almost every instance, some sufficient arithmetical criterion is satisfied. The verification is completed by the (easy) direct construction of around 200 primitive polynomials. A sieving method of the author (used in many previous items) is also prominent.

A similar result (also conjectured in [14]) on the existence of *irreducible* polynomials of any degree n with an arbitrary prescribed coefficient has been established by Daqing Wan [16], completed through the computations of [12]. The methods of this study can be used to provide an alternative proof.

References

[1] S. D. Cohen, *Primitive elements and polynomials with arbitrary trace*, Discr. Math. **83** (1990), 1–7.

[2] S. D. Cohen, *Gauss sums and a sieve for generators of Galois fields*, Publ. Math. Debrecen **56** (2000), 293-312.

[3] S. D. Cohen,*Primitive polynomials over small fields*, Finite Fields and Applications. 7th International Conference, Toulouse (2003), LNCS **2948**, Springer, 2004, 197–214.

[4] S. D. Cohen and S. Huczynska, *Primitive free quartics with specified norm and trace*, Acta Arith. **109** (2003), 359-385.

[5] S. D. Cohen and S. Huczynska, *Primitive free cubics with specified norm and trace*, Trans. Amer. Math. Soc. **355** (2003), 3099-3116.

[6] S. D. Cohen and C. King, *The three fixed coefficient primitive polynomial theorem*, JP J. Algebra Number Theory Appl., **4** (2004), 79–87.

[7] S. D. Cohen and D. Mills, *Primitive polynomials with first and second coefficients prescribed*, Finite Fields Appl. 9 **9** (2003), 334–350.

[8] S-Q. Fan and W-B. Han, p-adic formal series and primitive polynomials over finite fields, Proc. Amer. Math. Soc., **132** (2004), 15–31.

[9] S.-Q. Fan and W.-B. Han, *Character sums over Galois rings and primitive polynomials over finite fields*, Finite Fields Appl., **10** (2004), 36–52.

[10] S.-Q. Fan and W.-B. Han, *Primitive polynomials with three coefficients prescribed*, Finite Fields Appl., to appear.

[11] S-Q. Fan and W-B. Han, *Primitive polynomials over finite fields of characteristic two*, Appl. Algebra Engrg. Comm. Comput. **14** (2004), 381–395.

[12] K. H. Ham and G. L. Mullen, *Distribution of irreducible polynomials of small degrees over finite fields*, Math. Comp. **67** (1998), 337–341.

[13] Han Wenbao, *The coefficients of primitive polynomials over finite fields*, Math. Comp. **65** (1996), 331–340.

[14] T. Hansen and G.L. Mullen, *Primitive polynomials over finite fields*, Math. Comp. **59** (1992), 639–643, S47–S50.

[15] D. Mills, *Existence of primitive polynomials with three coefficients prescribed*, JP J. Algebra Number Theory Appl., **4** (2004), 36–52.

[16] D. Wan *Generators and irreducible polynomials over finite fields*, Math. Comp. **66** (1997), 1195–1212.

Some wild towers over finite fields

Arnaldo Garcia

The objective of the talk was to present some towers of function fields over finite fields, with wild ramification, having a good limit. A *tower* $\mathcal{F}$ over $\mathbb{F}_q$ is an infinite sequence of fields

$$\mathcal{F} = (F_1 \subsetneqq F_2 \subsetneqq F_3 \subsetneqq \ldots \subsetneqq F_n \subsetneqq \ldots)$$

such that:

- Each field F_n is a $\mathbb{F}_q$-function field; i.e.; the finite field $\mathbb{F}_q$ is algebraically closed in F_n.
- Each extension F_{n+1}/F_n is finite and separable.
- The genus $g(F_n) \to \infty$ as $n \to \infty$.

The following limit $\lambda(\mathcal{F}) = \lim_{n\to\infty} \frac{N(F_n)}{g(F_n)}$ exists (see [5]) and it is called the *limit of the tower* $\mathcal{F}$, where $N(F_n)$ denotes the number of $\mathbb{F}_q$-rational places of the function field F_n. It follows from Weil's theorem that $\lambda(\mathcal{F}) \leq 2\sqrt{q}$, and Ihara [7] was the first to realize that the bound above could be improved. The best upper bound known is $\lambda(\mathcal{F}) \leq \sqrt{q} - 1$ and it is due to Drinfeld-Vladut. For $q = \ell^2$ a square, Ihara and independently Tsfasman-Vladut-Zink (see [7] and [8]) showed the existence of towers $\mathcal{F}$ over $\mathbb{F}_q$ attaining the Drinfeld-Vladut bound; i.e., $\lambda(\mathcal{F}) = \ell - 1 = \sqrt{q} - 1$. For applications to Coding Theory and Cryptography one needs that:

- The function fields F_n, and their $\mathbb{F}_q$-rational places, are *explicitly* given by equations, and by their coordinates.
- The genera $g(F_n)$ are *explicitly* given by formulas, for all $n \in \mathbb{N}$.

The tower $\mathcal{F}$ is said to be *tame* if each ramification degree in F_{n+1}/F_n, for all values of $n \in \mathbb{N}$, is relatively prime to the characteristic. Otherwise the tower $\mathcal{F}$ is said to be *wild*. If $\mathcal{E} = (E_1 \subsetneqq E_2 \subsetneqq \ldots)$ and $\mathcal{F} = (F_1 \subsetneqq F_2 \subsetneqq F_3 \subsetneqq \ldots)$ are towers over $\mathbb{F}_q$, we say that $\mathcal{E}$ is a *subtower* of $\mathcal{F}$ (and we then write $\mathcal{E} < \mathcal{F}$) if for every $n \in \mathbb{N}$, there exists $m \in \mathbb{N}$ such that $E_n \subseteq F_m$. If $\mathcal{E} < \mathcal{F}$ then $\lambda(\mathcal{E}) \geq \lambda(\mathcal{F})$ (see [5]).

1. The first explicit tower $\mathcal{F}_0$ and two subtowers $\mathcal{F}_1$ and $\mathcal{F}_2$.

Let $q = \ell^2$ be a square and let $F_1 = \mathbb{F}_q(x_1)$ be the rational function field over $\mathbb{F}_q$.

1.1 The tower $\mathcal{F}_0$.

Let $F_2 = F_1(z_2)$ with $z_2^\ell + z_2 = x_1^{\ell+1}$ and set $x_2 = z_2/x_1$. Let $F_3 = F_2(z_3)$ with $z_3^\ell + z_3 = x_2^{\ell+1}$ and set $x_3 = z_3/x_2$. Let $F_4 = F_3(z_4)$ with $z_4^\ell + z_4 = x_3^{\ell+1}$ and set $x_4 = z_4/x_3$ and so on. In this way we get a explicit tower $\mathcal{F}_0$ over $\mathbb{F}_{\ell^2}$ satisfying $\lambda(\mathcal{F}_0) = \ell - 1 = \sqrt{q} - 1$ (see [4]). Rational places come from $(x_1 - \alpha)$ with $\alpha \in \mathbb{F}_q^*$; i.e., those are the completely splitting places in the tower $\mathcal{F}_0$.

Definition. Let φ and ψ be two rational functions in one variable. We say that a tower $\mathcal{F} = (F_1 \subsetneqq F_2 \subsetneqq F_3 \subsetneqq \ldots)$ is given by the equation $\varphi(Y) = \psi(X)$ if $F_1 = \mathbb{F}_q(x_1)$ and for $n \geq 1$ we have recursively $F_{n+1} = F_n(x_{n+1})$ with $\varphi(x_{n+1}) = \psi(x_n)$.

1.2 The first subtower $\mathcal{F}_1 < \mathcal{F}_0$.

The tower $\mathcal{F}_1$ over $\mathbb{F}_{\ell^2}$ is given recursively by the equation

$$Y^\ell + Y = X^\ell/1 + X^{\ell-1}.$$

For this tower one has also that $\lambda(\mathcal{F}_1) = \ell - 1$, and the completely splitting places are $(x_1 - \alpha)$ with $\alpha^\ell + \alpha \neq 0$ (see [5]).

1.3 The second subtower $\mathcal{F}_2 < \mathcal{F}_1 < \mathcal{F}_0$.

The tower $\mathcal{F}_2$ over $\mathbb{F}_{\ell^2}$ is given recursively by the equation

$$(Y-1)/Y^\ell = (X^\ell - 1)/X.$$

Here again $\lambda(\mathcal{F}_2) = \ell - 1$. The completely splitting places are $(x_1 - \alpha)$ with $\alpha^\ell + \alpha = 1$ (see [1]). For the function fields F_n of the tower $\mathcal{F}_2$ we have the following genus formulas:

$$(\ell - 1) \cdot g(F_n) = \begin{cases} (\ell^{n/2} - 1)^2, \text{ if } n \text{ even.} \\ (\ell^{\frac{n-1}{2}} - 1)(\ell^{\frac{n+1}{2}} - 1), \text{ if } n \text{ odd.} \end{cases}$$

The interpretation of $\mathcal{F}_0, \mathcal{F}_1$ and $\mathcal{F}_2$ in terms of Drinfeld modules was carried out by Elkies (see [3]).

2. Towers over cubic finite fields

For $q = p^3$ with p a prime number, Zink showed the existence of towers $\mathcal{F}$ over $\mathbb{F}_q$ satisfying $\lambda(\mathcal{F}) \geq \frac{2(p^2-1)}{p+2}$.

2.1 The tower $\mathcal{F}_3$ for $p = 2$.

Over the field with 8 elements, consider the tower $\mathcal{F}_3$ given by the equation (see [6])

$$Y^2 + Y = (X^2 + X + 1)/X.$$

It satisfies $\lambda(\mathcal{F}_3) = 3/2 = 2(p^2-1)/(p+2)$ for $p = 2$. Rational places on $\mathcal{F}_3$ come from $(x_1 - \alpha)$ with $\alpha \in \mathbb{F}_8 \setminus F_2$.

2.2 The tower $\mathcal{F}_3$.

The tower $\mathcal{F}_3$ here is a generalization of the one above. Let ℓ be any prime power and $q = \ell^3$. Consider the tower $\mathcal{F}_3$ over $\mathbb{F}_q$ given by (see [2])

$$\frac{1-Y}{Y^\ell} = \frac{X^\ell + X - 1}{X}.$$

Its limit satisfies $\lambda(\mathcal{F}_3) \geq 2(\ell^2-1)/(\ell+2)$, and hence it gives another proof and a generalization of the lower bound from Zink. The completely splitting places are $(x_1 - \alpha)$ with the conditions:

$$\alpha^\ell + \alpha = \beta \quad \text{where} \quad \beta^{\ell+1} = \beta - 1.$$

References

[1] J. Bezerra and A. Garcia, *A tower with non-Galois steps which attains the Drinfeld-Vladut bound*, J. Number Theory **106** (2004), 142-154.

[2] J. Bezerra, A. Garcia, and H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, preprint 2004.

[3] N. Elkies, *Explicit Towers of Drinfeld Modular Curves*, Progress in Math.**202** (2001), 189-198.

[4] A. Garcia and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. Math. **121** (1995), 211-222.

[5] A. Garcia and H. Stichtenoth, *On the asymptotic behaviour of some towers of function fields over finite fields*, J. Number Theory **61** (1996), 248-273.

[6] G. van der Geer and M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, Bull. London Math. Soc. **34** (2002), 291-300.

[7] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Tokio **28** (1981), 721-724.

[8] M. Tsfasman, S. Vladut, and T. Zink, *Modular curves, Shimura curves and Goppa codes, better than the Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21-28.

Factoring Ore Polynomials over Finite Fields and Congruence Function Fields

Mark Giesbrecht

The work of Ore [7, 9] in the early 1930's has had a significant influence on computing with symbolic linear ordinary difference and differential equations in the past decade. Ore polynomials give a unified treatment to (linear) differential and difference equations. Let F be a field, $\sigma : \mathsf{F} \to \mathsf{F}$ an automorphism of F, and $\delta : \mathsf{F} \to \mathsf{F}$ a *σ-derivation*, a map such that $\delta(a+b) = \delta(a) + \delta(b)$, and $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$. Define the ring of *Ore polynomials* $\mathsf{F}[\mathcal{D}; \sigma, \delta]$, as the set of polynomials in $\mathsf{F}[\mathcal{D}]$ with the usual addition and multiplication defined by $\mathcal{D}a = \sigma(a)\mathcal{D} + \delta(a)$.

Prototypical examples of Ore polynomials include the *shift (or difference) polynomials* $\mathsf{F}(t)[\mathcal{D}; \sigma]$, where $\sigma(t) = t+1$ and $\mathcal{D}t = (t+1)\mathcal{D}$, and the *differential polynomials* $\mathsf{F}(t)[\mathcal{D}; \delta]$, where $\mathcal{D}t = t\mathcal{D} + 1$. Ore polynomials over $\mathsf{F}(t)$ have a natural interpretation as differential or difference operators. An important third class of Ore polynomials (from Ore [8, 10]), is the *additive* or *linearized polynomials* over a finite field $\mathbb{F}_q$ of characteristic p. These are of the form $\sum a_i x^{p^i} \in \mathbb{F}_q[x]$, and form a ring under addition and composition. These are isomorphic to $\mathbb{F}_q[\mathcal{D}; \sigma]$ where $\sigma(a) = a^p$ for $a \in \mathbb{F}_q$.

Ore polynomials have many properties analogous to the usual polynomials, and in particular are left (and right) principal ideal domains, providing unique least common left multiple (LCLM) and greatest common right divisor (GCRD), which can be efficiently computed. While factorization is not unique, it is unique up to permutations of the degree sequence of the factors, as is decomposition as an LCLM of mutually co-prime factors (an *LCLM-decomposition*).

In [4], we give efficient algorithms for factoring and LCLM-decomposing Ore polynomials over $\mathbb{F}_q$. Given $f \in \mathsf{R} = \mathbb{F}_q[\mathcal{D};\sigma]$, we can find a complete factorization and LCLM-decomposition in polynomial time. We proceed by decomposing a related associative algebra to f. Define the *idealizer* $\mathcal{I}_f$ as the largest subring of R in which $\mathsf{R}f$ is a two-sided ideal, and the *eigenring* as $\mathcal{E}_f = \mathcal{I}_f/\mathsf{R}f$. This is a finite-dimensional associative algebra over $\mathbb{F}_p$, for which a basis can be computed efficiently. We prove in [4] that $\mathcal{E}_f$ has zero divisors if and only if f factors, and $\mathcal{E}_f$ has orthogonal idempotents v, w with $v + w = 1$ if and only if f is LCLM-decomposable. From such zero-divisors and idempotents, f can be efficiently factored or decomposed.

While algorithms for finding zero divisors in the eigenring are presented in [4], we give more efficient methods for general associative algebras in [2, 3]. If an algebra $\mathbb{A} \subseteq \mathbb{F}_q^{m\times m}$ is given by a basis $\mathfrak{a}_1, \ldots, \mathfrak{a}_\ell \in \mathbb{F}_q^{m\times m}$, then a complete set of primitive pairwise orthogonal idempotents can be found with an expected $O(m^3 \log m + m^2\ell)$ operations in $\mathbb{F}_q$. When $\mathcal{A}$ is semi-simple, a basis for all the simple components and an isomorphism between each simple component and a full matrix algebra is also found.

Giesbrecht & Zhang [5] generalize techniques for factoring and decomposing Ore polynomials over finite fields to function fields over $\mathbb{F}_q$. This is important as a first step towards modular algorithms for factoring differential and difference polynomials over $\overline{\mathbb{Q}}(t)$. All Ore rings $\mathbb{F}_q(t)[\mathcal{D};\sigma,\delta]$ can be reduced to the usual polynomials, the shift polynomials, the differential polynomials, and the dilation polynomials (where $\mathcal{D}t = \xi t\mathcal{D}$, for some $\xi \in \mathbb{F}_{q^2}$). In each of these cases the main observation is that $\mathbb{F}_q(t)$ is a finite extension of the field of constants $\mathsf{K} \subseteq \mathbb{F}_q(t)$ (the subfield of $\mathbb{F}_q(t)$ commuting with $\mathcal{D}$). In particular, for the differential polynomials $K = \mathbb{F}_q(t^p)$, while for shift polynomials over $\mathbb{F}_p$, $\mathsf{K} = \mathbb{F}_p(t^p - t)$. This allows us to express the eigenring as a finite dimensional algebra over K. We prove, analogously to the finite field case, that zero-divisors in the eigenring exist if and only if f factors, and orthogonal idempotents exist if and only if f can be decomposed as an LCLM of co-prime polynomials. To decompose the eigenring, we adapt the algorithm of [6], and note it can be made more efficient by techniques in [2]. The algorithm for factorization and decomposition of $f \in \mathbb{F}_q(t)[\mathcal{D};\sigma,\delta]$ requires time polynomial in $\deg_t f$, $\deg_{\mathcal{D}} f$ and p (and not $\log p$, as one might hope).

The work in [5] coincides with the different but related approach of Cluzeau [1] for factoring differential polynomials over $\mathbb{F}_p(t)$. Based on earlier works of Van der Put [11], this algorithm decomposes the p-curvature, a linear map associated to f.

References

[1] T. Cluzeau. Factorization of differential systems in characteristic p and application. In *Proc. International Symposium on Symbolic and Algebraic Computation*, 2003.

[2] W. Eberly and M. Giesbrecht. Efficient decomposition of associative algebras over finite fields. *Journal of Symbolic Computation*, 29:441–458, 2000.

[3] W. Eberly and M. Giesbrecht. Efficient decomposition of separable algebras. *Journal of Symbolic Computation*, 37, 2004.

[4] M. Giesbrecht. Factoring in skew-polynomial rings over finite fields. *J. of Symbolic Computation*, 24(5), 1998.

[5] M. Giesbrecht and Y. Zhang. Factoring and decomposing ore polynomials over $\mathbb{F}_q(t)$. In *ACM International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 127–134, 2003.

[6] G. Ivanyos, L. Rónyai, and A. Szántó. Decomposition of algebras over $\mathbb{F}_q(x_1, \ldots, x_m)$. *Applicable Algebra in Engineering, Communication and Computing*, 5:71–90, 1994.

[7] O. Ore. Formale Theorie der linearen Differentialgleichungen. *J. reine angew. Math.*, 168:233–252, 1932.

[8] O. Ore. On a special class of polynomials. *Trans. Amer. Math. Soc.*, 35:559–584, 1933.

[9] O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34(22):480–508, 1933.

[10] O. Ore. Contributions to the theory of finite fields. *Trans. Amer. Math. Soc.*, 36:243–274, 1934.

[11] M. van der Put. Differential equations in characteristic p. *Compositio Mathematica*, 97:227–251, 1995.

On the complexity of factoring bivariate supersparse and straight-line polynomials

Erich Kaltofen

(joint work with Pascal Koiran)

We present algorithms that compute the linear and quadratic factors of supersparse (lacunary) bivariate polynomials over the rational numbers in polynomial-time in the input size. In supersparse polynomials the term degrees can have hundreds of digits as binary numbers. Our algorithms are Monte Carlo randomized for quadratic factors and deterministic for linear factors. Our approach relies on the results by H. W. Lenstra, Jr., [4, 5] on computing factors of univariate supersparse polynomials over the rational numbers.

Furthermore, we show that the problem of determining the irreducibility of a supersparse bivariate polynomial over a large finite field of any characteristic is NP-hard via randomized reductions. The latter theorem sharpens our earlier NP-hardness result of irreducibility of bivariate polynomials over large finite fields given by division-free straight-line programs, which I presented in my talk, by techniques from [1, 3], which were brought to my attention by Joachim von zur Gathen and Igor Shparlinksi during the conference. With our approach we can in turn extend the theorem that testing a supersparse univariate polynomial for squarefreeness is NP-hard via randomized reductions [3] to a sufficiently large finite coefficient field of any characteristic.

References

[1] von zur Gathen, Joachim, Karpinski, Marek, and Shparlinski, Igor. Counting curves and their projections. *Computational Complexity*, 6(1):64–99, 1996/1997.

[2] Győry, Kálmán, Iwaniec, Henryk, and Urbanowicz, Jerzy, editors. *Number Theory in Progress*, volume 1 Diophantine Problems and Polynomials, 1999. Stefan Banach Internat. Center, Walter de Gruyter Berlin/New York. ISBN 3-11-015715-2. Proc. Internat. Conf. Number Theory in Honor of the 60th Birthday of Andrzej Schinzel Zakopane, Poland June 30–July 9, 1997.

[3] Karpinski, Marek and Shparlinski, Igor. On the computational hardness of testing square-freeness of sparse polynomials. In *Proc. AAECC-13*, volume 1719 of *Lect. Notes Comput. Sci.*, pages 492–497, Heidelberg, Germany, 1999. Springer Verlag.

[4] Lenstra, Jr., H. W. Finding small degree factors of lacunary polynomials. In [2], pages 267–276.

[5] Lenstra, Jr., H. W. On the factorization of lacunary polynomials. In [2], pages 277–291.

MDS codes, arcs and algebraic curves

Gábor Korchmáros

A linear (q-ary) code of length n, dimension k and minimum distance d is a *maximum distance separable code*, briefly an MDS code, if it attains the Singleton upper bound, that is, $d = n - k$. An MDS code corresponds via its generator matrix to an arc of size n in $PG(k-1,q)$, the k-dimensional projective space over the finite field $\mathbf{F}_q$ with $q = p^h$, p prime. An *arc* in $PG(k-1,q)$ is a set of at least k points no k of which are in a hyperplane. Non–extendable MDS codes correspond to complete arcs, that is, to arcs not contained in a larger arc. For $q \geq k-1$, the $\mathbf{F}_q$-rational points of a normal rational curve of $PG(k-1,q)$ constitute an arc of size $q+1$. It is plausible that such a $(q+1)$-arc is complete, apart from the cases $k = 3$, $q-1$ and q even; but this has been proven so far for q even, $k \geq 4$, $q > 2k-6$, and q odd, $k \geq 3$, $q > 2k-5$, and for large primes q, see [10, 12].

An important objective is to compute $m(k-1,q)$, the maximum length of an MDS code of given dimension k. A straightforward computation shows that if $q < k$ then $m(k-1,q) = k$ in such cases. The *Main Conjecture* for MDS codes, always taking $q > k-1$, is

$$m(k-1,q) = \begin{cases} q+2 & \text{for } k = 3 \text{ and } k = q-1 \text{ both with } q \text{ even,} \\ q+1 & \text{in all other cases.} \end{cases}$$

Munueara [8] proved this conjecture for algebraic-geometric MDS codes arising from curves with genus g for $g = 0, 1$ and, when $q > 83$, for $g = 2$, see also [3, 16]. Computational results for small values of q are given in [2].

From results on arcs obtained by Blokhuis, Bruen, Casse, Glynn, Hirschfeld, Kaneta, Maruta, Segre, Storme, Thas and others between 1955 and 1990, see Chapter 27 in [3] and [1], the Main conjecture holds in small dimensions $k \leq 5$, and also for $q > 2$ even, $q > (2k - \frac{15}{2})^2$, and for q odd, $q > (4k - \frac{55}{4})^2$.

The study of the odd q order case can greatly benefit by results on algebraic curves over $\mathbf{F}_q$ with many $\mathbf{F}_q$-rational points. From now on, q is odd, and $k \geq 5$. In $PG(2,q)$, every arc of size $m(2,q) = q+1$ consists of all $\mathbf{F}_q$-rational points of

an irreducible conic in $PG(2,q)$, see [9]. Let $m'(2,q)$ be the size of the second largest complete arc in $PG(2,q)$. Then every arc of size larger than $m'(2,q)$ is contained in an irreducible conic in $PG(2,q)$. Induction on dimension together with a result of Kaneta and Maruta, see Theorem 27.6.1 in [3], show that the Main conjecture holds for $q > m'(2,q) + k - 5$. By Segre's connection between arcs and curves, there is a projective, absolutely irreducible (possibly singular) algebraic plane curve Γ defined over $\mathbf{F}_q$ of degree $2t$ with $t = q - m'(2,q) + 2$ which contains at least $t(q-t+2)$ points $P \in PG(2,q)$ such that the intersection multiplicity $I(P, \Gamma \cap \ell)$ is 2 for some line ℓ of $PG(2,q)$. From the Hasse-Weil upper bound, $m'(2,q) \le q - \frac{1}{4}\sqrt{q} + \frac{25}{16}$. The Stöhr-Voloch theorem gives an improvement to this estimate: if $q = p$ is prime, then $m'(2,p) \le \frac{44}{45}p + 89$, see [15], and if q is a non-square, then $m'(2,q) \le q - \frac{1}{4}\sqrt{pq} + \frac{29}{16}p + 1$, see [14]. The best known estimate for square q is $q - \sqrt{q} + 1 \le m'(2,q) \le q - \frac{1}{2}\sqrt{q} + \frac{5}{2}$, see [4, 5]. The proof of the latter upper bound depends essentially on the following result. Let Γ be a projective, absolutely irreducible (possibly singular) algebraic plane curve of degree n, defined over $\mathbf{F}_q$ for an odd square $q > 9$. Assume that Γ is classical, but its Veronese embedding is Frobenius non-classical with Frobenius orders $0, 1, 2, 3, \sqrt{q}$. Two types of branch-points $P \in \Gamma$ centred at a point of $PG(2,q)$ are distinguished, according as $j_2(P)$ equals $j_1(P)$ or does not. Here $(j_0(P) = 0, j_1(P), j_2(P))$ is the order sequence of Γ at P. Let

$$M_q = \sum_P j_1(P), \qquad M'_q = \sum_P j_1(P),$$

as P ranges over the branch-points of first and second type, respectively. Assume that $3 \le n \le \sqrt{q} - 3$, and $q > 23^2$ but $q \ne 3^6, 5^5$. The main result in [5] states that $2M_q + M'_q \le n(q - \sqrt{q} + 1)$. Equality holds if and only if Γ is the Fermat curve of equation $x^{(\sqrt{q}+1)/2} + y^{(\sqrt{q}+1)/2} + 1 = 0$, up to projectivity over $\mathbf{F}_q$, which is the only $\mathbf{F}_q$-maximal plane curve of genus $g = \frac{1}{8}(\sqrt{q} - 1)(\sqrt{q} - 3)$, see [6].

References

[1] A. A. Bruen, J. A. Thas, J. and A. Blokhuis, On M.D.S. codes, arcs in PG(n,q) with q even, and a solution of three fundamental problems of B. Segre. *Invent. Math.* **92** (1988), 441–459.

[2] J. M. Chao and H. Kaneta, Classical arcs in PG(r,q) for $23 \le q \le 29$. *Discrete Math.* **226** (2001), 377–385.

[3] H. Chen and S. T. Yau, Contribution to Munuera's problem on the main conjecture of geometric hyperelliptic MDS codes. *IEEE Trans. Inform. Theory* **43** (1997), 1349–1354.

[4] J. W. P. Hirschfeld and G. Korchmáros, On the embedding of an arc into a conic in a finite plane. *Finite Fields Appl.* **2** (1996), 274-292.

[5] J. W. P. Hirschfeld and G. Korchmáros, On the number of rational points on an algebraic curve over a finite field. *Bull. Belg. Math. Soc. Simon Stevin* **5** (1998), 313–340.

[6] A. Cossidente, J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, On plane maximal curves. *Compositio Math.* **121** (2000), 163–181.

[7] J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries*, Oxford University Press, Oxford, 1991.

[8] C. Munuera, On the main conjecture on geometric MDS codes. *IEEE Trans. Inform. Theory* **38** (1992), 1573–1577.

[9] B. Segre, Ovals in a finite projective plane. *Canad. J. Math.* **7**, (1955). 414–416.
[10] G. Seroussi and R. M. Roth, On MDS extensions of generalized Reed-Solomon codes. *IEEE Trans. Inform. Theory* **32** (1986), 349–354.
[11] L. Storme and J. A. Thas, M.D.S. codes and arcs in PG(n, q) with q even: an improvement of the bounds of Bruen, Thas, and Blokhuis. *J. Combin. Theory Ser. A* **62** (1993), 139–154.
[12] L. Storme and J. A. Thas, Generalized Reed-Solomon codes and normal rational curves: an improvement of results by Seroussi and Roth. Advances in finite geometries and designs (Chelwood Gate, 1990), 369–389, Oxford Sci. Publ., Oxford Univ. Press, New York, 1991.
[13] K. O. Stöhr and J. F. Voloch, Weierstrass points and curves over finite fields. *Proc. London Math. Soc.* **52** (1986), 1–19.
[14] J. F. Voloch, On the completeness of certain plane arcs, *European J. Combin.* **8** (1987), 453–456.
[15] J. F. Voloch, Arcs in projective planes over prime fields, *J. Geom.* **38** (1990), 198–200.
[16] J. L. Walker, Judy L. A new approach to the main conjecture on algebraic-geometric MDS codes. *Des. Codes Cryptogr.* **9** (1996), 115–120.

Sum-free sets in finite fields

Vsevolod F. Lev

A subset A of an (additively written) abelian group is called *sum-free* if the equation $x+y=z$ has no solutions in the elements of A; in other words, if $a_1+a_2 \notin A$ for any $a_1, a_2 \in A$. Letting $2A := \{a_1 + a_2 \colon a_1, a_2 \in A\}$ (the *sumset* of A) and $A - A := \{a_1 - a_2 \colon a_1, a_2 \in A\}$ (the *difference set* of A) we can also re-write the definition of a sum-free set as $2A \cap A = \varnothing$ or equivalently, as $(A - A) \cap A = \varnothing$. Thus, sum-free sets are, in a sense, "anti-subgroups".

To our knowledge, sum-free sets were first introduced in 1916 by Schur whose celebrated result, considered now one of the origins of the Ramsey theory, states that the set of positive integers cannot be partitioned into finitely many sum-free subsets. Further research was, to a large extent, motivated by the famous conjecture by Cameron and Erdős, asserting that the number of sum-free subsets of the interval $[1, n]$ is $O(2^{n/2})$; see [2]. This conjecture was recently settled by Green [5] and independently by Sapozhenko [14]. In this connection we mention the papers by Alon [1], Green and Ruzsa [6], and the papers [7, 8, 9, 11, 12], authored or co-authored by the presenter.

Another research direction is spanned by the following question: how large can a sum-free subset of a finite abelian group be? For some groups the answer has been known for over 30 years, see [4, 13, 15, 16]; however, for a number of particularly "tough" groups this question remained open until recent paper by Green and Ruzsa [6]. Much effort has been made also to determine the structure of sum-free subsets of the maximum possible size; for numerous results of this sort and further references see [17].

The additive group of the finite field GF(2^r) has received particular attention due to relations with finite geometries and coding theory. It is easily seen, for instance, that sum-free sets in GF(2^r) are *caps* (no-three-points-on-a-line sets) in the affine geometry AG(r, 2); moreover, *maximal* sum-free sets are *complete* caps. (For convenience, here and below we identify fields GF(p^r) with their additive

groups.) Since $|2A| \geq |A|$ and $|A - A| \geq |A|$, any sum-free subset $A \subset \mathrm{GF}(2^r)$ satisfies $|A| \leq 2^{r-1}$, and this bound is sharp as the non-zero coset of any index-two subgroup of $\mathrm{GF}(2^r)$ is a sum-free set. Conversely, it can be shown that for $r \geq 4$ any sum-free set $A \subset \mathrm{GF}(2^r)$ with $|A| > 5 \cdot 2^{r-4}$ is a subset of the non-zero coset of an index-two subgroup of $\mathrm{GF}(2^r)$. This result was first established by Davydov and Tombak in [3] and since then has been rediscovered several times. Indeed, the main theorem of [3] is much stronger and consists of complete description of those maximal (by inclusion) sum-free sets $A \subset \mathrm{GF}(2^r)$, satisfying $|A| > 2^{r-2} + 1$: specifically, any such set is a union of cosets of a non-zero subgroup of $\mathrm{GF}(2^r)$. The ideology behind this result is that large sum-free sets possess a rigid structure (while small sum-free sets can be sporadic). More precisely, large maximal sum-free sets can be obtained by the "lifting procedure" from sum-free sets in the quotient groups.

For the groups $\mathrm{GF}(p^r)$ with $p \geq 3$ no similar results were known until recently, though the largest possible size of a sum-free subset $A \subset \mathrm{GF}(p^r)$ is known and sum-free subsets of this largest size are classified in most cases; see, for instance, [6] or [17]. However, there were virtually no attempts to go one step further and to determine the structure of sum-free sets of size *close* to the largest possible. In our paper [8] we address the case $p = 3$.

Theorem. *Let $r \geq 3$ and suppose that $A \subset \mathrm{GF}(3^r)$ is sum-free. If $|A| > 5 \cdot 3^{r-3}$, then A is contained in a non-zero coset of an index-three subgroup of* $\mathrm{GF}(3^r)$.

Here the bound $5 \cdot 3^{r-3}$ is sharp: we present in [8] a construction of sum-free sets $A \subset \mathrm{GF}(3^r)$ of size $|A| = 5 \cdot 3^{r-3}$, not contained in a non-zero coset of an index-three subgroup. Parallel to the main result by Davydov and Tombak is the following conjecture, also stated in [8].

Conjecture. *Let $r \geq 3$ and suppose that $A \subset \mathrm{GF}(3^r)$ is a maximal (by inclusion) sum-free set. If $|A| > (3^{r-1} + 1)/2$, then A is a union of cosets of a non-zero subgroup of* $\mathrm{GF}(3^r)$.

Again, the bound $|A| > (3^{r-1} + 1)/2$ is sharp: we give in [8] a construction of maximal sum-free subsets $A \subset \mathrm{GF}(3^r)$ with $|A| = (3^{r-1} + 1)/2$ such that A is *not* a union of cosets of a non-zero subgroup.

Concerning finite fields $\mathrm{GF}(p)$ of prime order p, it is well-known that the largest possible size of a sum-free subset $A \subset \mathrm{GF}(p)$ is $\lfloor (p + 1)/3 \rfloor$, and all sum-free subsets of this size have been classified. Examples of sum-free subsets of size $n = \lfloor (p + 1)/3 \rfloor$ are the interval $[n, 2n - 1] \pmod p$ and its dilations by non-zero elements of $\mathrm{GF}(p)$, and for $p \equiv 2 \pmod 3$ no other sum-free subsets of size n exist. For $p \equiv 1 \pmod p$, however, more examples can be obtained by slight modifications of the interval $[n, 2n-1] \pmod p$ and dilations. Using a combination of character sums technique (see [10]), tools from additive number theory, and combinatorial considerations, in [9] we establish the following structure result.

Theorem. *Let p be a prime and suppose that $A \subset \mathrm{GF}(p)$ is sum-free. If $n := |A| > 0.33p$, then A is contained in the dilation of the interval $[n, p - n] \pmod p$ by a non-zero element of* $\mathrm{GF}(p)$.

Observe that the number of elements of the interval $[n, p-n] \pmod p$ is $p - 2n + 1 = n + (p - 3n + 1)$, which shows that A is, in fact, a very *dense* subset of a dilation of this interval. We notice also that the interval $[n, p-n] \pmod p$ is smallest possible: as it is shown in [9], for any $n \in (p/4, p/3)$ there exist sum-free sets $A \subset \mathrm{GF}(p)$ with $|A| = n$, not contained in a dilation of a proper subinterval of the interval $[n, p-n] \pmod p$. In contrast, the factor 0.33 is certainly not best possible and it would be interesting to replace it by a smaller value. We have an example of a sum-free subset $A \subset \mathrm{GF}(p)$ of size $n := |A| \approx 0.2p$ which is *not* contained in a dilation of the interval $[n, p-n] \pmod p$, and bridging the gap between $0.2p$ and $0.33p$ is a challenging open problem.

References

[1] N. Alon, *Independent sets in regular graphs and sum-free subsets of finite groups*, Israel Journal of Mathematics **73** (2) (1991), 247–256.

[2] P.J. Cameron and P. Erdős, *On the number of sets of integers with various properties*, Number theory (Banff, AB, 1988), 61–79, de Gruyter, Berlin, 1990.

[3] A. Davydov and L. Tombak, *Quasi-perfect linear binary codes with distance* 4 *and complete caps in projective geometry*, Problemy Peredachi Informatzii **25** (4) (1989), 11–23.

[4] P.H. Diananda and H.P. Yap, *Maximal sum-free sets of elements infinite groups*, Proc. Japan Acad. **45** (1969), 1–5.

[5] B. Green, *The Cameron-Erdős conjecture*, Bull. London Math. Soc. **36** (6) (2004), 769-778.

[6] B. Green and I.Z. Ruzsa, *Sum-free sets in abelian groups*, Israel Journal of Mathematics, to appear.

[7] V.F. Lev, *Sharp estimates for the number of sum-free sets*, Journal für die reine und angewandte Mathematik (Crelle's Journal) **555** (2003), 1–25.

[8] V.F. Lev, *Large sum-free sets in ternary spaces*, Journal of Combinatorial Theory, Series A, to appear.

[9] V.F. Lev, *Large sum-free sets in* $\mathbf{Z}/p\mathbf{Z}$, submitted.

[10] V.F. Lev, *Distribution of points on arcs*, INTEGERS, to appear.

[11] V.F. Lev, T. Łuczak, and T. Schoen, *Sum-free sets in abelian groups*, Israel Journal of Mathematics **125** (2001), 347–367.

[12] V.F. Lev and T. Schoen, *Cameron-Erdős modulo a prime*, Finite Fields and their Applications **8** (1) (2002), 108–119.

[13] A.H. Rhemtulla and A.P. Street, *Maximal sum-free sets in finite abelian groups*, Bull. Austral. Math. Soc. **2** (1970), 289–297.

[14] A.A. Sapozhenko, *The Cameron-Erdős conjecture* [Russian] Dokl. Akad. Nauk **393** (6) (2003), 749–752.

[15] H.P. Yap, *Maximal sum-free sets in finite abelian groups. IV*, Nanta Math. **5** (3) (1972), 70–75.

[16] H.P. Yap, *Maximal sum-free sets in finite abelian groups. V*, Bull. Austral. Math. Soc. **13** (3) (1975), 337–342.

[17] J.S. Wallis, A.P. Street, and W.D. Wallis, *Combinatorics: Room squares, sum-free sets, Hadamard matrices*, Lecture Notes in Mathematics **292** (1972), Springer-Verlag.

Ramanujan graphs and Ramanujan hypergraphs

Wen-Ching Winnie Li

The eigenvalues of a k-regular connected undirected graph X lie between $-k$ and k. Denote by $\lambda^+(X)$ (resp. $\lambda^-(X)$) the largest (resp. smallest) eigenvalue which is smaller than k (resp. larger than $-k$). The Alon-Boppana theorem [7] asserts that for any family of k-regular undirected graphs, one has

$$\liminf_{i\to\infty} \lambda^+(X_i) \geq 2\sqrt{k-1}$$

provided that $|X_i| \to \infty$ as $i \to \infty$. The counter assertion

$$\limsup_{i\to\infty} \lambda^-(X_i) \leq -2\sqrt{k-1}$$

is shown in [4] to hold under the assumption that the minimal length of an odd cycle in X_i approaches infinity as $i \to \infty$. Note that the interval $[-2\sqrt{k-1}, 2\sqrt{k-1}]$ is the spectrum of the universal cover of k-regular graphs. Further, in case $k-1 = q$ is a prime power, the infinite $(q+1)$-regular tree may be realized as $PGL_2(F)/PGL_2(O_F)$ for a nonarchimedean local field with q elements in its residue field. Here O_F denotes the ring of integers of F.

A regular graph is called *Ramanujan* if its nontrivial eigenvalues fall in the spectrum of its universal cover. Such a graph has good expanding property and may be used as a good communication network.

An n-hypergraph consists of vertices and hyperedges; topologically it may be regarded as an $(n-1)$-dimensional simplicial complex. There are $n-1$ adjacency operators $A_1, ..., A_{n-1}$ acting on functions on the vertices of a hypergraph. Assume that the operators A_i commute with each other. The Bruhat-Tits building $PGL_n(F)/PGL_n(O_F) =: B_{n,F}$ is a typical example of $(q+1)$-regular n-hypergraph. It serves as a universal cover and we consider only finite quotients of this building.

The first result is the higher dimensional analogue of the Alon-Boppana theorem proved in [5].

Theorem 1. *Let $\{X_j\}$ be a family of $(q+1)$-regular finite n-hypergraphs such that each X_j contains a geodesic ball of radius d_j isomorphic to a ball of the same radius in $B_{n,F}$. Assume that $d_j \to \infty$ as $j \to \infty$. Then for $1 \leq i \leq n-1$ the closure of the eigenvalues of A_i on X_j for all $j \geq 1$ contains the spectrum of A_i on $B_{n,F}$.*

In view of this theorem, we define a $(q+1)$-regular n-hypergraph to be *Ramanujan* if the nontrivial eigenvalues of $A_i, 1 \leq i \leq n-1$, fall in the spectrum of A_i on $B_{n,F}$. The next result is

Theorem 2. *Given $n \geq 2$ and a prime power q, there exists an infinite family of $(q+1)$-regular finite Ramanujan n-hypergraphs.*

The case $n = 2$ was done by Lubotzky-Phillips-Sarnak [7] and independently by Margulis [8] over $\mathbb{Q}$, and by Morgenstern [9] over a rational function field.

Their method may be extended to construct Ramanujan n-hypergraphs by taking left quotients of $B_{n,F}$ by suitable congruence subgroups of $PGL_n(F)$ arising from division algebras H of dimension n^2 defined over a global field of which F is a local completion. The functions on these hypergraphs may be interpreted as automorphic forms on $H^\times$, and the nontrivial eigenvalues of A_i are eigenvalues of the Hecke operators, whose estimates are the content of the Ramanujan conjecture. For general n and over function fields, Lafforgue [2] establishes the conjecture for GL_n, and Laumon-Rapoport-Stuhler [3] prove it for certain automorphic forms on $H^\times$. To use Lafforgue, one needs the Jacquet-Langlands correspondence from automorphic forms on $H^\times$ to those on GL_n over function fields, currently established for prime n. The work in [6] and [10] assumes the validity of the correspondence. An unconditional result is obtained in [5] for general n by appealing to [3].

In his thesis [10] Sarveniazi describes certain n-hypergraphs as Cayley hypergraphs based on $PGL_n(\mathbb{F}_{q^m})$ or $PSL_n(\mathbb{F}_{q^m})$, following a similar argument as in [7]. These hypergraphs are Ramanujan whenever the Jacquet-Langlands correspondence holds. On the other hand, one gets a Ramanujan 3-hypergraph based on three copies of $\mathbb{F}_{q^3}$, whose nontrivial eigenvalues are generalized Kloosterman sums over $\mathbb{F}_q$ in three variables with estimates furnished by Deligne in [1].

References

[1] P. Deligne, *Cohomologie étale (SGA $4\frac{1}{2}$)*, Lecture Notes in Math., vol. **569**, Springer-Verlag, Berlin, 1977.

[2] L. Lafforgue, *Chtoucas de Drinfeld et correspondance de Langlands*, Invent. Math. **147** (2002), 1-241.

[3] G. Laumon, M. Rapoport and U. Stuhler, *$\mathcal{D}$-elliptic sheaves and the Langlands correspondence*, Invent. Math. **113** (1993), 217-338.

[4] W.-C. W. Li, *On negative eigenvalues of regular graphs*, C. R. Acad. Sci. Paris, t. **333**, Série I (2001), 907-912.

[5] W.-C. W. Li, *Ramanujan hypergraphs*, GAFA, Geom. funct. anal. **14** (2004), 380-399.

[6] A. Lubotzky, B. Samuels, and U. Vishne, *Ramanujan complexes of type $\tilde{A}_d$*, Israel J. Math., to appear.

[7] A. Lubotzky, R. Phillips and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), 261-277.

[8] G. Margulis, *Explicit group theoretic constructions of combinatorial schemes and their application to the design of expanders and concentrators*, J. Prob. of Info. Trans. (1988), 39-46.

[9] M. Morgenstern, *Existence and explicit constructions of $q+1$ regular Ramanujan graphs for every prime power q*, J. Comb. Theory, series B, **62** (1994), 44-62.

[10] A. Sarveniazi, *Ramanujan $(n_1, n_2, ..., n_{d-1})$-regular hypergraphs based on Bruhat-Tits buildings of type $\tilde{A}_{d-1}$*, Ph. D. Thesis, U. Göttingen, 2004.

Explicit constructions of algebraic geometric codes

Hiren Maharaj

Over the past decade there has been substantial research devoted to the explicit construction of curves over finite fields with many points. Consequently we now have a super abundance of such constructions with the primary motivation being

the ultimate construction of algebraic geometric codes. However, relatively little work has been done on the *explicit* constructions of such codes. Below we exhibit a new construction of explicit algebraic geometric codes. The construction has the following advantages: for an explicitly given extension of the rational function field, one always obtains explicit bases and therefore an exact formula for the dimension of the code, genus computation is unnecessary for estimating the parameters of the code, the minimum distance of these codes can be bounded below by the usual Goppa lower bound for minimum distance and furthermore good upper bounds on the minimum distance of the codes are given. The codes constructed here are always subcodes of Goppa codes and in many cases they coincide with Goppa codes. Furthermore, the ideas used in the code construction are adapted to give sharp upper bounds for the minimum distance of a large class of Goppa codes.
Let F be an algebraic function field of a single variable and let K denote the full field of constants of F. For our purposes K is a finite field. Suppose that $F' = F(y)$, $[F' : F] = n$ and that K is the full field of constants of F'. Let $G_0, G_1, \ldots, G_{n-1}$ be n divisors of F. Consider the K-vector space

$$\mathcal{L} := \bigoplus_{i=0}^{n-1} \mathcal{L}(G_i) y^i.$$

We wish to find a good approximation of $\mathcal{L}$ as a Riemann-Roch space of F', that is, we desire a divisor G with the property that $\mathcal{L} \subseteq \mathcal{L}(G)$ and such that both spaces have dimensions as close as possible. Put

$$G := \max\left(\mathrm{Con}_{F'/F}(G_i) - i(y), 0 \leq i \leq n-1\right). \tag{1}$$

In [2] it is shown that $\mathcal{L}(G)$ contains $\mathcal{L}$ and that the above choice of G is optimal if F is the rational function field. Moreover, in [2], a simple procedure is given on how to make the best possible choice of the divisors G_i so that the space $\mathcal{L}(G)$ better approximates the space $\mathcal{L}$. Surprisingly, in many examples and for a wide range of parameters, the spaces $\mathcal{L}$ and $\mathcal{L}(G)$ coincide! The above ideas are easily adapted to differential spaces [4, 5].
Next we present the code construction.
Assume that $F := K(x)$ is the rational function field. Put $\mathcal{G} := (G_0, G_1, \ldots, G_{n-1})$ and put $D = P_1 + P_2 + \ldots + P_N$ where $P_1, \ldots, P_N$ are N rational places of F' which do not belong to the support of the divisor G. Define the map $\mathrm{ev} : \mathcal{L}(G) \to K^N$ by $\mathrm{ev}(f) = (f(P_1), f(P_2), \ldots, f(P_N))$.
Let $C_{\mathcal{L}}(D, \mathcal{G}) := \mathrm{ev}(\mathcal{L})$ and for $i = 0, 1, \ldots, n-1$ put $C_i := \mathrm{ev}(\mathcal{L}(G_i)y^i)$ and let d_i be the minimum distance of the subcode C_i. If $\deg G < N$ then $C_{\mathcal{L}}(D, \mathcal{G})$ is an $[N, k, d]$ code where

(a) $k = \sum_{i=0}^{n-1} \max(\deg G_i + 1, 0) \geq n + \sum_{i=0}^{n-1} \deg G_i$.
(b) $N - \deg G \leq d \leq \min(d_i : 0 \leq i \leq n-1)$.

Since F is the rational function field, explicit bases are easily constructed for the spaces $\mathcal{L}(G_i)$ (see Proposition II.3.3 of [7]). One obtains a basis for the space $\mathcal{L}$ as follows: let B_i be a basis for $\mathcal{L}(G_i)$ for $i = 0, 1, \ldots, n-1$; then $\cup_{i=0}^{n-1} B_i y^i$ is a basis for $\mathcal{L}$. One then obtains a basis for the code $C_{\mathcal{L}}(D, \mathcal{G})$ by applying the map ev.

In many instances in practice the numbers $d_0, d_1, \ldots, d_{n-1}$ are easy to compute: suppose that R_1, R_2, ..., R_t are t rational places of F which do not belong to the support of the divisors G_i $(0 \leq i \leq n-1)$ and which split completely in F to give rise to the places $P_1, \ldots, P_N$ so that $N = nt$. If $\deg G < N$ then $C_{\mathcal{L}}(D, \mathcal{G})$ is an $[N, k, d]$ code where

(*a*) $N = nt$.
(*b*) $k = \sum_{i=0}^{n-1} \max(\deg G_i + 1, 0) \geq n + \sum_{i=0}^{n-1} \deg G_i$.
(*c*) $N - \deg G \leq d \leq N - n \max(\deg G_i : 0 \leq i \leq n-1)$.

Perhaps surprisingly, the upper bound in (*c*) turns out to be close to the lower bound in the many cases. The conditions of the above code constructions are easily satisfied in practice and examples are given in [2].

In [3], the above construction is adapted to produce explicit codes from towers of function fields. There are many explicit constructions of recursively defined asymptotically good towers of function fields. The first few levels of these towers provide excellent examples of curves with many points for code construction. Since the code length from towers increase exponentially with the level, only codes from the first few levels are expected to be of current practical interest. The above estimates of the parameters of the codes are not strong enough to determine if they are asymptotically good or bad and this is an open problem.

The presentation of the above codes as direct sums of very simple codes allow for a more indepth study of their properties. For example, in [6] it is shown how this presentation can easily be exploited to yield substantially improved lower bounds on the minimum distance of a large class of Goppa codes.

References

[1] H. Maharaj, "Code construction on fibre products of Kummer covers," *IEEE Trans. Inform. Theory*, vol. 50, No. 9, September 2004.

[2] H. Maharaj, "Explicit constructions of algebraic-geometric codes," to appear in *IEEE Trans. Inform. Theory.*

[3] H. Maharaj, "Explicit constructions of algebraic-geometric codes from towers," to appear in *IEEE Trans. Inform. Theory.*

[4] H. Maharaj, "Explicit Goppa code construction on fibre products of Kummer Covers using differentials," in review.

[5] H. Maharaj, "Explicit constructions of algebraic geometric codes using differentials," in review.

[6] H. Maharaj, "Improved lower bounds of the minimum distance of a class of Goppa codes," in review.

[7] H. Stichtenoth, "Algebraic Function Fields and Codes," Springer Universitext. Berlin, Heidelberg, New York, 1993.

Maps over finite fields: integrability and reversibility

Franco Vivaldi
(joint work with John A. G. Roberts)

In the theory of dynamical systems, integrability (existence of invariants of the motion) and reversibility (existence of conjugacy with inverse map) are important structural properties. We let two-dimensional algebraic mappings act on finite fields, and, based on experimental evidence, conjecture the existence of limit distributions of the length of the orbits for the integrable and reversible cases, as well as for the case in which both properties are absent. Such distributions feature considerable rigidity (independence from the mapping). These phenomena are relevant to the development of criteria for integrability/reversibility for algebraic mappings.

A mapping $L : \mathbb{C}^2 \to \mathbb{C}^2$ is *integrable* if there exists a function $I : \mathbb{C}^2 \to \mathbb{C}$, non-constant and defined almost everywhere in $\mathbb{C}$, such that $I = I \circ L$. We speak of *algebraic integrability* if L, L^{-1} and I are rational functions. The phase space of an integrable system foliates into level sets of the function I, which are invariant under the dynamics; moreover, the motion on each level set is regular (indeed, conjugate to a rotation, for almost all bounded level sets). If L is algebraically integrable and of infinite order, then the level sets of I are algebraic curves of genus at most one [8].

A smooth mapping L is *R-reversible* if there exists an involution G such that

$$L^{-1} = G \circ L \circ G^{-1} \qquad \det(dG) < 0$$

where dG is the Jacobian of G. In the polynomial case there is a well-developed theory, which, in particular, leads to normal forms for reversible maps [2, 1].

A planar mapping L with coefficients in an algebraic number field can be made to act on $\mathbb{F}_q^2$, for a suitable q. (If L is rational rather than polynomial, we shall implicitly assume that the reduced map $\bar{L}$ acts on the projective plane $P_2(\mathbb{F}_q)$.) We look for fields $\mathbb{F}_q$ for which $\bar{L}$ exists together with the relevant reduced quantity i.e., the integral $\bar{I}$, or the reversor $\bar{G}$. Letting $q = p^n$, we keep n fixed and let $p \to \infty$ through a suitable set of prime numbers p. These primes have positive density, from Cebotarev's theorem, and we are interested in the study of the asymptotic (large p) behaviour of the length of the orbits of $\bar{L}$ and their distribution. For simplicity, in what follows we assume $q = p$.

Let $T(z)$ be the length of the orbit of L through the point $z \in \mathbb{F}_p^2$. We define

$$D_p(x) = \frac{1}{p^2} \#\{z : T(z) \le px\} \qquad D(x) = \lim_{p\to\infty} D_p(x). \tag{1}$$

The distribution D_p represents the probability that a point chosen at random in $\mathbb{F}_p^2$ belongs to a cycle of length not exceeding px, and D is its limiting value.

Extensive experimental evidence suggest the following [6, 5, 7]

Conjecture 1. *The limit (1) exists for any bi-rational map L.*

(*i*) *If L is algebraically integrable, then $D(x)$ is a step function with steps at $1/n, n = 1, 2, \ldots$.*
(*ii*) *If L is R-reversible and possesses a single family of reversing symmetries, then $D(x) = 1 - e^{-x}(1 + x)$.*
(*iii*) *If L is neither integrable nor R-reversible, then $D(x) = 0$.*

To obtain a non-trivial limit in case (*iii*) one must scale orbits differently. We define

$$D'_p(x) = \frac{1}{p^2} \#\{z : T(z) \leq p^2 x\} \qquad \langle D' \rangle_p(x) = \frac{1}{\#L_p} \sum_{m \in L_p} D'_m(x).$$

The average $\langle D' \rangle_p$ is computed over the set L_p of all primes not exceeding p at which the map L can be reduced. Averaging is required by the presence of very long cycles (of order p^2), which is a signature of random permutations.

Conjecture 2. *For every non-integrable bi-rational map, which is not R-reversible and has no other symmetry, we have*

$$\lim_{p \to \infty} \langle D' \rangle_p(x) = x.$$

A heuristic justification of conjecture 1(*i*) goes as follows [3]. A bi-rational map of infinite order, which acts on a curve of genus one, can be shown to be conjugate to a translation $x \mapsto x + \omega$ with respect to the group law on the corresponding Weierstrass curve. Upon reduction to a finite field, all the orbits on that curve will have the same length, while the normalized (divided by p) number of points on the curve approaches 1, due to the Hasse-Weil bound. Thus the distribution D, if it exists, must have steps at the reciprocal of the positive integers, and the size of the step at $1/n$ is the probability that ω generates a subgroup of index n in $E/\mathbb{F}_p$, where E is the given curve. The sample space here is the set of curves that foliate $\mathbb{F}_p^2$. Thus the existence of the distribution D rests on the validity of a variant of the elliptic analogue of Artin's conjecture [4].

References

[1] M. Baake and J. A. G. Roberts, *Symmetries and reversing symmetries of polynomial automorphisms of the plane*, Nonlinearity (2005), to appear.
[2] A. Gómez and J. D. Meiss, *Reversors and symmetries for polynomial automorphisms of the complex plane*, Nonlinearity **17** (2004) 975-1000; nlin.CD/0304035 v2.
[3] D. Jogia, J. A. G. Roberts, and F. Vivaldi, *An algebraic-geometric approach to integrable maps of the plane*, in preparation.
[4] M. RamMurty, *Artin's conjecture for primitive roots*, Math. Intelligencer **10** 1988, 59–67.
[5] J. A. G. Roberts, D. Jogia, and F. Vivaldi, *The Hasse-Weil bound and integrability detection in rational maps*, J. Nonl. Math. Phys. **10** (2003), 166–180.
[6] J. A. G. Roberts and F. Vivaldi, *Arithmetical method to detect integrability in maps*, Phys. Rev. Lett. **90** 3 (2003), [034102].
[7] J. A. G. Roberts and F. Vivaldi, *Signature of time-reversal symmetry in polynomial automorphisms over finite fields*, preprint (2004). `http://www.maths.qmul.ac.uk/~fv/research/Symmetry.pdf`.
[8] A. P. Veselov, *Integrable maps*, Russian Math. Surveys **46** (1991) 1–51.

Asymptotics of the minimal distance of quadratic residue codes

José Felipe Voloch

The binary quadratic residue codes are defined as follows. Given a prime $p \equiv \pm 1 \pmod 8$, let ξ be a primitive p-th root of unity in the algebraic closure of $\mathbb{F}_2$, the field of two elements. The hypothesis on p entails that the monic polynomial $a(x)$, say, whose roots are ξ^r, with r running over the non-zero quadratic residues modulo p, is defined over $\mathbb{F}_2$ and the cyclic code of length p whose generator polynomial is $a(x)$ is, by definition, the binary quadratic residue code of length p. Different choices of ξ lead to different choices of $a(x)$ that give different but equivalent codes. Their minimal distance d_p is, in general, not known although the lower bound $d_p \geq \sqrt{p}$ and minor improvements are known, see [1]. It is possible, using the results of Stark [8] and Helleseth's formula for the weight (see [2] and lemma 1 below), to improve slightly this lower bound (See [3]). However, the general behaviour of d_p is not known, in particular, whether there is an asymptotically good subfamily of of quadratic residue codes, i.e., whether $\limsup d_p/p > 0$. We will show that there are asymptotically bad subfamilies of quadratic residue codes, i.e., $\liminf d_p/p = 0$. More precisely,

Theorem 1. *For infinitely many primes p, the minimal distance d_p of the binary quadratic residue code of length p is $O(p/\log\log p)$. If furthermore, the generalised Riemann hypothesis is true, then the bound can be improved to $O(p/\log p)$.*

In the proof of the Theorem we will use the following lemma of Helleseth. For a proof see [2] or [3].

Lemma 1. *If $a(x) = \sum_{i=1}^{r} x^{j_i} \in \mathbb{F}_2[x]/(x^p - 1)$, define $f(t) = \prod_{i=1}^{r}(t - j_i) \in \mathbb{F}_p[t]$, then the weight $w(\mathbf{c})$ of $q(x)a(x)$ is*

$$w(\mathbf{c}) = \frac{1}{2}\left(p + (-1)^{r-1}\left(\sum_{t\in\mathbb{F}_p}\chi(f(t)) - \sum_{i=1}^{r}\chi(f'(j_i))\right)\right)$$

where χ denotes the quadratic character (Legendre symbol) mod p.

Proof of the Theorem: Let ℓ be an odd prime, ζ a primitive complex ℓ-th root of unity and K the extension of the rational number field obtained by adjoining $\zeta, \sqrt{2}$ and $\sqrt{\zeta^k - 1}$ for all $k = 1, \ldots, \ell - 1$. Let p be a prime that splits completely in K, I claim that $d_p \leq (p-1)/2\ell$. Note that $\ell | (p-1)$ since p splits in the ℓ-th cyclotomic field. Let $f(t) = t^{(p-1)/\ell} - 1 \in \mathbb{F}_p[t]$, then $f(t)$ has all its roots in $\mathbb{F}_p$ and yields a codeword $\mathbf{c}$ of C_p as in the lemma. Again, by the assumption on p, $f(t)$ is a square for all $t \in \mathbb{F}_p$, since $t^{(p-1)/\ell}$ is an ℓ-th root of unity for $t \in \mathbb{F}_p^*$ and -1 is a square in $\mathbb{F}_p$. The roots of $f(t)$ form a subgroup G of index ℓ in $\mathbb{F}_p^*$, $f'(t) = (p-1)/\ell t$ in G and it follows easily that $\sum_{t\in G}\chi(f'(t)) = 0$. So $w(\mathbf{c}) = (p-1)/2\ell$ and the claim follows.

To complete the proof of the theorem we vary ℓ as above and, for each ℓ, we take p to be the smallest prime that splits completely in K. We will show that

$\ell \gg \log\log p$ and $\ell \gg \log p$ under the generalised Riemann hypothesis and this will prove the theorem. To bound p in terms of ℓ we use the following estimates (see [5] and [4] respectively). Let d be the discriminant of K. Then $\log p \ll \log d$ and, under the generalised Riemann hypothesis, $p \ll (\log d)^2$. To estimate d note that only p and 2 ramify in K. Now we use Hensel's bound on the different (see [7] remark 1 after Proposition III.13), which yields that the contribution of a ramified prime to the discriminant has exponent at most $n(n+1)$, where n is the absolute degree of K. We conclude that $d \leq (2p)^{n(n+1)}$. Finally, is immediate that $n \leq (p-1)2^p$, which gives the results claimed.

Remark: The quadratic residue codes have been generalized to (no longer cyclic) binary codes of lenght q for a prime power q when 2 is a square modulo q ([6]). The above lemma has a generalization to these codes sketched in [3]. For q a square it was shown in [6] that the square root bound is best possible. From our perspective, their example consists of noticing that $t^{\sqrt{q}}+t$ is a square for all $t \in \mathbb{F}_q$. If q is not a prime or a square then nothing seems to be known.

References

[1] J. MacWilliams and N. Sloane, *The theory of error-correcting codes*, North-Holland, 1977.

[2] T. Helleseth, "Legendre sums and codes related to QR codes," *Discrete Applied Math.*, vol. 35, pp. 107-113, 1992.

[3] T. Helleseth; J. F. Voloch, "Double Circulant Quadratic Residue Codes" *IEEE Transactions on Information Theory*, to appear.

[4] J. C. Lagarias, H. L. Montgomery and A. M. Odlyzko " A bound for the least prime ideal in the Chebotarev density theorem" Invent. Math., vol 54 (1979), 271–296.

[5] J. C. Lagarias, A. M. Odlyzko, "Effective versions of the Chebotarev density theorem" in *Algebraic Number Fields*, A. Frohlich ed., Academic Press 1997, pp 409–464.

[6] van Lint, J.; MacWilliams, F., "Generalized quadratic residue codes" *IEEE Transactions on Information Theory* Vol. 24, 1978 pp. 730- 737

[7] J.-P. Serre, *Local Fields*, Springer, New York, 1979.

[8] H.M. Stark, "On the Riemann hypothesis in hyperelliptic function fields," *Analytic number theory*, Proc. Sympos. Pure Math., Vol. XXIV, pp. 285-302, 1972.

Factors of Dickson Polynomials over Finite Fields

Joseph L. Yucas

(joint work with Robert W. Fitzgerald)

We let $\mathbf{F_q}$ denote the finite field of characteristic p containing q elements. Let n be a positive integer and write $t = \lfloor n/2 \rfloor$. In his 1897 PhD Thesis, Dickson introduced a family of polynomials

$$D_n(x) = \sum_{i=0}^{t} \frac{n}{n-i} \left(\begin{array}{c} n-i \\ i \end{array} \right) x^{n-2i}.$$

These are the unique polynomials satisfying Waring's identity

$$D_n(x + x^{-1}) = x^n + x^{-n}.$$

In recent years these polynomials have received an extensive examination. They have become known as the *Dickson polynomials* (of the first kind).

Chou, and then later simplified by Bhargava and Zieve, gave a factorization of the Dickson polynomials over $\mathbf{F_q}$. We summarize their results as follows:

Theorem: If q is even, then $D_n(x)$ is the product of irreducible polynomials in $\mathbf{F_q}[\mathbf{x}]$ which occur in cliques corresponding to the divisors d of n, $d > 1$. To each such d there corresponds $\phi(d)/(2k_d)$ irreducible factors, each of which has the form

$$\prod_{i=0}^{k_d-1} (x - (\zeta^{q^i} + \zeta^{-q^i}))$$

where ζ is a d^{th} root of unity, ϕ is Euler's totient function and k_d is the least positive integer such that $q^{k_d} \equiv \pm 1 \pmod{d}$.

Theorem If q is odd, then $D_n(x)$ is the product of irreducible polynomials in $\mathbf{F_q}[\mathbf{x}]$ which occur in cliques corresponding to the divisors d of n for which n/d is odd. To each such d there corresponds $\phi(4d)/(2k_d)$ irreducible factors, each of which has the form

$$\prod_{i=0}^{k_d-1} (x - (\zeta^{q^i} + \zeta^{-q^i}))$$

where ζ is a $4d^{th}$ root of unity and k_d is the least positive integer such that $q^{k_d} \equiv \pm 1 \pmod{4}$.

Notice that the factors appearing in the above results are in $\mathbf{F_q}[\mathbf{x}]$, although their description uses elements from outside of $\mathbf{F_q}$. The purpose of this paper is to better understand these factors. In this regard, we show that these factors can be obtained from the factors of certain cyclotomic polynomials. This in turn gives a relationship between self-reciprocal polynomials and these Dickson factors. We also obtain a recursion for these factors. In the final section of this paper we record a few identities that we discovered in this pursuit which appear to be new.

References

[1] G. Andrews, Reciprocal polynomials and quadratic transformations, Utilitas Math.38 (1985), 255-264.

[2] M. Bhargava, M. Zieve, Factoring Dickson polynomials over finite fields, Finite Fields Appl. 5 (1999), 103-111.

[3] L. Carlitz, Some theorems on irreducible reciprocal polynomials over a finite field, J. Reine Angew. Math. 227 (1967), 212-220.

[4] R. Chapman, Completely normal elements in iterated quadratic extensions of finite fields, Finite Fields Appl. 3 (1997), 1-10.

[5] W.S. Chou, The factorization of Dickson polynomials over finite fields, Finite Fields Appl. 3 (1997), 84-96.

[6] S. D. Cohen, The explicit construction of irreducible polynomials over finite fields, Des. Codes Cryptogr. 2 (1992), 169-174.

[7] M. K. Kyuregyan, Recurrent methods for constructing irreducible polynomials over $GF(2^s)$, Finite Fields Appl. 8 (2002), 52-68.

[8] R. Lidl, G. Mullen, G. Turnwell, Dickson Polynomials, Pitman Monographs and Surveys in Pure and Applied Math., Longman, London/Harlow/Essex, 1993.

[9] H. Meyn, On the construction of irreducible self-reciprocal polynomials over finite fields, Appl. Algebra Engrg. Comm. Comput.1 (1990) 43-53.
[10] R. L. Miller, Necklaces, symmetries and self-rreciprocal polynomials, Discrete Math. 22 (1978), 25-33.
[11] A. Scheerhorn, Iterated constructions of normal bases over finite fields, Finite Fields: Theory, Applications and Algorithms (Las Vegas, NV, 1993), 309-325, Contemp. Math. 168, Amer. Math. Soc., Providence, RI (1994).
[12] J. Yucas and G. Mullen, Self-reciprocal polynomials over finite fields, to appear in Designs, Codes and Cryptography.

Special sessions

On the List and Bounded Distance Decodability of Reed-Solomon Codes

Qi Cheng
(joint work with Daqing Wan)

For an error-correcting code and a distance bound, the *list decoding problem* is to compute all the codewords within a given distance to a received message. The *bounded distance decoding* problem is to find one codeword if there is at least one codeword within the given distance, or to output the empty set if there is not. Obviously the bounded distance decoding problem is not as hard as the list decoding problem. For a Reed-Solomon code $[n,k]_q$, a simple counting argument shows that for any integer $0 < g < n$, there exists at least one Hamming ball of radius $n-g$, which contains at least $\binom{n}{g}/q^{g-k}$ many codewords. Let $\hat{g}(n,k,q)$ be the smallest positive integer g such that $\binom{n}{g}/q^{g-k} < 1$. One knows that

$$k \le \hat{g}(n,k,q) \le \sqrt{nk} \le n.$$

For the distance bound up to $n-\sqrt{nk}$, it is well known that both the list and bounded distance decoding can be solved efficiently [1]. For the distance bound between $n-\sqrt{nk}$ and $n-\hat{g}(n,k,q)$, we do not know whether the Reed-Solomon code is list, or bounded distance decodable, nor do we know whether there are polynomially many codewords in all balls of the radius. It is generally believed that the answers to both questions are no. There are public key cryptosystems proposed recently, whose security is based on the assumptions.

In this talk, we prove: (1) List decoding can not be done for radius $n-\hat{g}(n,k,q)$ or larger, otherwise the discrete logarithm over $\mathbb{F}_{q^{\hat{g}(n,k,q)-k}}$ is easy. (2) Let h and g be positive integers satisfying $q \ge \max(g^2, (h-1)^{2+\epsilon})$ and $g \ge (\frac{4}{\epsilon}+2)(h+1)$ for a constant $\epsilon > 0$. We show that the discrete logarithm problem over $\mathbb{F}_{q^h}$ can be efficiently reduced by a randomized algorithm to the bounded distance decoding problem of the Reed-Solomon code $[q, g-h]_q$ with radius $q-g$. These results show that the decoding problems for the Reed-Solomon code are at least as hard

as the discrete logarithm problem over finite fields. The main tools to obtain these results are an interesting connection between the problem of list-decoding of Reed-Solomon code and the problem of discrete logarithm over finite fields, and a generalization of Katz's theorem [2] on representations of elements in an extension finite field by products of distinct linear factors.

References

[1] Venkatesan Guruswami and Madhu Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Transactions on Information Theory*, 45(6):1757–1767, 1999.

[2] Nicholas M. Katz. Factoring polynomials in finite fields: an application of Lang-Weil to a problem in graph theory. *Mathematische Annalen*, 286:625–637, 1990.

On the lattice profile of pseudorandom number sequences

Gerhard Dorfer

(joint work with Wilfried Meidl and Arne Winterhof)

In [1]–[4] we introduced and analyzed a generalized version of Marsaglia's lattice test for segments of sequences over an arbitrary field. The lecture provides an overview on the results achieved there.

Let $(\eta_n)_{n=0}^{\infty}$ be a sequence of elements in some field $\mathbb{K}$. For given $s \geq 1$ and $N \geq 2$ we say that (η_n) passes the s-dimensional N-lattice test if the vectors $\{\underline{\eta}_n - \underline{\eta}_0 \mid 1 \leq n \leq N-s\}$ span $\mathbb{K}^s$, where $\underline{\eta}_i = (\eta_i, \eta_{i+1}, \ldots, \eta_{i+s-1})$. The greatest s such that (η_n) satisfies the s-dimensional N-lattice test is called the *lattice profile* of (η_n) at N and is denoted by $S((\eta_n), N)$.

It turns out that there is a close relationship between $S((\eta_n), N)$ and the Nth *linear complexity* $L((\eta_n), N)$ which is the least order L of a linear recurrence relation over $\mathbb{K}$

$$\eta_{n+L} = \alpha_0\eta_n + \alpha_1\eta_{n+1} + \ldots + \alpha_{L-1}\eta_{n+L-1}, \quad 0 \leq n \leq N-L-1,$$

satisfied by the first N terms of (η_n). More precisely, we proved in [1] that the knowledge of the linear complexity profile yields a value S such that the largest dimension for passing the above lattice test is either S or $S-1$.

In [2] for periodic sequences over finite fields and sufficiently long parts of the period we determined the exact value S or $S-1$. As an application we deduced from recently obtained lower bounds on the linear complexity profile of certain nonlinear pseudorandom number generators new results on their lattice structure.

In [3] it is shown that an explicit formula expressing the lattice profile in terms of the linear complexity profile (and vice versa) can be provided once the interdependency is known in certain points. Moreover, an intrinsic characterization of lattice profiles among all functions on the nonnegative integers is established.

In [4] we determined for finite fields the number of sequences of length n with given lattice profile at n. From this result we derived an exact formula for the expected value and the standard deviation of the lattice profile at n. For the

binary case we characterized the (infinite) sequences with maximal possible lattice profile.

References

[1] G. Dorfer, A. Winterhof, *Lattice structure and linear complexity profile of nonlinear pseudorandom number generators*, Appl. Alg. Engrg. Comm. Comp. **13** (2003), 499-508.

[2] G. Dorfer, A. Winterhof, *Lattice structure and nonlinear pseudorandom number generators in parts of the period*, Monte Carlo and Quasi Monte Carlo Methods 2002 (H. Niederreiter, ed.), 199-211, Springer Verlag, Berlin 2004.

[3] G. Dorfer, *Lattice profile and linear complexity profile of pseudorandom number sequences*, Proc. of 7th Int. Conf. on Finite Fields and Applications (G.L. Mullen, A. Poli, H. Stichtenoth, eds.), Lecture Notes in Computer Science **2948**, pp. 69-78, Springer Verlag, Berlin 2004.

[4] G. Dorfer, W. Meidl, A. Winterhof, *Counting functions and expected values for the lattice profile at n*, Finite Fields Appl. **10** (2004), 636–652.

Searching in Encrypted Data

Jeroen Mathias Doumen
(joint work with Richard Brinkman, Wim Jonker)

The amount of data an average person has, is becoming so huge that in the near future this cannot be stored locally anymore, and an external server will have to be used. When this server is not (entirely) trusted, the data should be encrypted. However, the data should still be accessible as a database - it should be possible to query the data. When using thin clients or low-bandwidth networks it is best to perform most of the work at the server. In [1] we present a method, inspired by secure multi-party computation, to efficiently search in encrypted data. We represent the data as an XML document, and translate XML elements to polynomials which contain information about themselves and their descendants in the XML tree. These polynomials are split (using secret sharing) into two parts: a random polynomial for the client and the difference between the original polynomial and the client polynomial for the server. The client polynomials are generated by a pseudorandom sequence generator, and thus only the seed has to be stored on the client. In a combined effort of both the server and the client a query can be evaluated without traversing the whole tree and without the server learning too much about the data or the query.

References

[1] R. Brinkman, J.M. Doumen and W. Jonker, *Using secret sharing for searching in encrypted data*, Workshop on Secure Data Management in a Connected World (SDM), LNCS **3178** (2004), 18–27.

An Algorithm for computing Isomorphisms of Algebraic Function Fields

Florian Hess

Let $F_{(1)}/k$ and $F_{(2)}/k$ be algebraic function fields of transcendence degree one and genus g over the constant field k. We consider the problem of computing one or all isomorphisms $\phi : F_{(1)} \to F_{(2)}$ which are the identity on k. This also yields $\mathrm{Aut}(F/k)$ for $F = F_{(1)} = F_{(2)}$. Except for being a problem of general interest our hope is that this will prove useful for example for the elimination of isomorphic entries during the computation of tables of curves over finite fields with many rational points.

For $g = 1$ the task is related to finding rational points and for hyperelliptic function fields the task is related to finding a hyperelliptic model. We restrict in the following to $g \geq 2$ and perfect k. We also assume that k is algebraically closed in $F_{(1)}$ and $F_{(2)}$. For such a function field F/k we essentially make use of the following algorithms, which are available in the computer algebra systems Kash [1] and Magma [2].

- Compute in F as a field, a k- and $k(x)$-vector space, for x a separating element.
- Compute with places, divisors and $\mathcal{L}(D) = \{a \in F^\times \mid (a) + D \geq 0\} \cup \{0\}$.
- Compute Weierstrass places.

Theorem 1. *Let P be a place of degree one of F/k such that the first pole order m at P is coprime to $\mathrm{char}(k)$. There exists an affine curve C with function field isomorphic to F and depending only on P of the following form*

$$C : \begin{cases} t_i t_j - \lambda_{i,j,1}(t_1) - \sum_{\nu=2}^{m} \lambda_{i,j,\nu}(t_1) t_\nu \\ \quad \text{with } \lambda_{i,j,\nu} \in k[t] \text{ and } 2 \leq i, j \leq m. \end{cases}$$

Moreover, C can be efficiently computed in such a way that the isomorphism to F is explicitly given in both directions and such that C is uniquely determined up to the transformation $t_1 \mapsto c^m t_1 + b$ and $t_i \mapsto c^{m_i} t_i$ for explicitly known $m, m_i \in \mathbb{Z}$, $2 \leq i \leq m$ and $c, b \in k$, independently of the given representation of F.

The algorithm to compute an isomorphism essentially proceeds as follows. We choose some suitable set $S_{(1)}$ of places of $F_{(1)}$ of degree one, such that $S_{(1)}$ is an isomorphism invariant, and choose $P_{(1)}$ from this set. We compute the respective set $S_{(2)}$ for $F_{(2)}$. If ϕ exists then $P_{(2)} = \phi(P_{(1)})$ will be one of the places in $S_{(2)}$. We compute $C_{(1)}$ for $F_{(1)}$ and $P_{(1)}$, and $C_{(2)}$ for $F_{(2)}$ and every $P_{(2)}$. Comparing $C_{(1)}$, $C_{(2)}$ equationwise and solving for $c, b \in k$ easily yields all ϕ with $P_{(2)} = \phi(P_{(1)})$. Possible choices for $S_{(1)}$ and $S_{(2)}$ are for example the set of places of degree one or the set of Weierstrass places of degree one.

We close with some remarks. If there are no places of degree 1 one can compute the isomorphisms for constant field extensions and then check which isomorphisms are actually defined over k. The number of comparisons of $C_{(1)}$ and $C_{(2)}$ is roughly between $O(g)$ and $O(g^3)$ if Weierstrass places are used, or $O(\max\{q, gq^{1/2}\})$ if all

places of degree one are used. If all first pole orders are divisible by $\mathrm{char}(k)$ then there is a version of Theorem 1 which should hold true in many cases when P is replaced by suitable divisors D. The number of isomorphisms is bounded by $O(g)$ for $\mathrm{char}(k) = 0$ and roughly $O(g^4)$ otherwise. A proof of Theorem 1 can be found in [3].

References

[1] Kant group, KASH, `http://www.math.tu-berlin.de/~kant`, 2004
[2] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp. **24, 3/4** (1997), 235–265
[3] F. Hess, *An Algorithm for computing Isomorphisms of Algebraic Function Fields*, Proceedings of the Sixth Symposium on Algorithmic Number Theory, ANTS-VI, LNCS 3076, Springer Verlag, 2004, 357–371

Random Walks on Elliptic Curves

Tanja Lange
(joint work with Igor E. Shparlinski)

In some recent papers, elliptic curve analogues of Pseudo Random Number Generators (PRNGs) were proposed for elliptic curves over finite fields. Random multiples of a point P of large order are computed in the generalization of the power generator [3] and the Naor-Reingold PRNG [4, 5]. These methods are slower than the use of LFSRs but the problem of constructing the following sequence element is related to the Diffie-Hellman problem on the elliptic curve which is believed to be hard under some conditions.

This study also serves a different purpose: if the sequences would turn out to have a strongly biased distribution then the discrete logarithm problem (the main building block of elliptic curve cryptography) on the curve should be easier or at least the bit security should be lower than assumed.

The main emphasis of this talk is on random walks on binary elliptic Koblitz curves [1, 6]. These curves are defined over $\mathbb{F}_2$ and are then considered as $E/\mathbb{F}_{2^n}$ such that the Frobenius endomorphism σ can be used to speed up the computation of scalar multiples. The standard use of σ in the computation of scalar multiples involves arithmetic in the rationals to compute a Frobenius expansion, which is impractical for small devices like smart cards.

The approach credited to Lenstra avoids this heavy machinery and starts with a random Frobenius expansion which has the same distribution properties as a genuine expansion. Our study in [2] shows that this alternative set-up can be applied essentially without increasing the probability of collisions, i.e. each point in $\langle P \rangle$ is the result of a scalar multiplication approximately the same number of times.

On the one hand this allows to use this fast method to obtain a PRNG on E but more importantly it supports the belief that the points obtained from the alternative approach are reasonably well distributed.

References

[1] N. Koblitz, N., *CM-curves with good cryptographic properties*, Advances in Cryptology – Crypto'91, Lect. Notes Comput. Sci. **576** (1992), 279–287.

[2] T. Lange and I. E. Shparlinski, *Collisions in Fast Generation of Ideal Classes and Points on Hyperelliptic and Elliptic Curves*, to appear in J. AAECC, (2004).

[3] T. Lange and I. E. Shparlinski, *Certain Exponential Sums and Random Walks on Elliptic Curves*, to appear in J. Canad. Math. Soc., (2004).

[4] I. E. Shparlinski, *On the Naor–Reingold pseudo-random number function from elliptic curves*, Appl. Algebra in Engin., Commun. and Computing, **11** (2000), 27–34.

[5] I. E. Shparlinski and J. H. Silverman, *On the linear complexity of the Naor–Reingold pseudo-random function from elliptic curves*, Designs, Codes and Cryptography, **24** (2001), 279–289.

[6] J. Solinas, *Efficient arithmetic on Koblitz curves*, Designs, Codes and Cryptography **19**, (2000), 195–249.

Zeta functions of supersingular curves of genus 2

Enric Nart

(joint work with Daniel Maisner)

Let k be a finite field of characteristic 2. Any supersingular curve of genus 2 defined over k admits a model of the type:

$$C: \quad y^2 + y = ax^5 + bx^3 + cx + d, \quad a \neq 0.$$

Van der Geer and van der Vlugt expressed the number of k-rational points of C in terms of certain linear invariants. They considered the simplectic bilinear form:

$$\langle\, x\, y \,\rangle_{a,b} := \mathrm{Tr}_{k/\mathbb{F}_2}(axy(x^3+y^3) + bxy(x+y)),$$

which depends only on a, b. The radical W of this form has dimension $w \leq 4$ and one can consider two linear forms on W: ℓ (depending on a, b), ℓ_c (depending on a, b, c) such that:

$$\ell_c \neq \ell \Longrightarrow |C(k)| = q+1, \quad \ell_c = \ell \Longrightarrow |C(k)| = q+1 \pm \sqrt{2^w q}.$$

In a joint work with Daniel Maisner, we have obtained an explicit computation of the invariants w, ℓ, ℓ_c in terms of the coefficients a, b, c of the defining equation. Moreover, we show that the linear form ℓ_c determines the number of points of C over the quadratic extension of k, so that we can express the zeta function of C in terms of objects defined over k. We apply this result to exhibit curves with prescribed zeta function, to find formulas for the number of curves, up to k-isomorphism, having the same zeta function and finally, to determine what isogeny classes of abelian surfaces over k contain jacobians.

References

[1] G. van der Geer, M. van der Vlugt, *Reed-Muller codes and supersingular curves. I*, Compositio Math. **84**, (1992), 333-367.

[2] D. Maisner, E. Nart, *Zeta functions of supersingular curves of genus 2*, `http://www.arxiv.org/math.NT/0408383`

Additive Polynomials and Elementary Abelian Extensions

Ferruh Özbudak

Let K be a field of characteristic p and $h(T) \in K[T]$ be a separable and additive polynomial splitting in K.

We explicitly determine an $\mathbb{F}_p$-linear subspace U of K for which we prove the following theorem.

Theorem 1. *For any $f \in K$, we have that $h(T) - f$ is irreducible over K if and only if*

$$T^p - T - u^p f \in K[T] \text{ is irreducible over } K \text{ for each } u \in U \setminus \{0\}.$$

Next we assume that $h(T)$ splits in a perfect field k of characteristic $p > 0$ and $K \supseteq k(x)$ is an algebraic function field with one variable having k as its constant field. We further assume that $h(T) - f$ is irreducible over K for some $f \in K$. Let F denote the algebraic function field $K(y)$, where $h(y) = f$.

Let $g(F)$ and $g(K)$ be the genera of F and K. Let $P \subseteq U$ be a subset with $1 + p + \ldots + p^{n-1}$ elements forming a projective space of dimension $n-1$ over $\mathbb{F}_p$. For each $a \in P$, let $E_a = K(z_a)$ be the algebraic function field with $z_a^p - z_a = a^p f$. Since $[F : K] = p^n$, we have that $[E_a : K] = p$ and we denote the genus of E_a by $g(E_a)$. If k is a finite field, we further denote the L-polynomial of F by $L_F(t)$, the L-polynomial of K by $L_K(t)$ and for each $a \in P$ the L-polynomial of E_a by $L_{E_a}(t)$

Theorem 2. *Under the notation and assumptions as above, we have that*

$$g(F) = \sum_{a \in P} g(E_a) - \frac{p^n - p}{p - 1} g(K)$$

and

$$L_F(t) = \prod_{a \in P} \frac{L_{E_a}(t)}{L_K(t)^{(p^n - p)/(p-1)}}.$$

In [1], only partial results for irreducibility (and genera) of this class of polynomials (algebraic function fields) were obtained. The corresponding complete results for $h(T) = T^{p^n} - T$ were obtained in [2], and our results can be considered as a generalization of it.

References

[1] V. Deolalikar, "Determining irreducibility and ramification groups for an additive extension of the rational function field", J. Number Theory, vol. 97. pp. 269-286, 2002.

[2] A. Garcia and H. Stichtenoth, "Elementary abelian p-extensions of algebraic function fields", Manuscr. Math., vol. 72, pp. 67-79, 1991.

A Generalized Counting and Factoring Technique for Polynomials over Finite Fields

Gary L. Mullen
(joint work with R.C. Mullin and J. Yucas)

We discuss a transform defined on the ring of polynomials over a finite field. This transform provides a single unified method with which to retrieve several results concerning the number of irreducible polynomials over finite fields with various properties.

As illustrations of our method, we are able to retrieve the formula of Carlitz [1] for the number of monic irreducible *translation invariant* ($f(x+a) = f(x)$ for all $a \in F_p$) polynomials of degree m over F_p.

As another special case we retrieve the formula from Carlitz [2] for the number of monic irreducible *self-reciprocal* ($x^k f(1/x) = f(x)$) irreducible polynomials of degree k over F_q.

References

[1] L. Carlitz, Finite sums and interpolation formulas over $GF[p^n, x]$, Duke Math. J. 15(1948), 1001-1012.
[2] L. Carlitz, Some theorems on irreducible reciprocal polynomials over a finite field, J. reine und angew. Math. 227(1967), 212-220.

Degree distribution of the GCD of several univariate polynomials over finite fields

Daniel Panario
(joint work with Zhicheng (Jason) Gao)

We study the degree distribution of the greatest common divisor of two or more random monic univariate polynomials over finite fields. Related results:

- The probability that several polynomials are coprime has been studied by Corteel, Savage, Wilf and Zeilberger [1].
- Drmota and Panario [2] study pairs of coprime polynomials with the condition of being smooth.
- A survey on random polynomials over finite fields is in [4].

Gao and Panario [3] provide estimates for the following random variables:

- Z_r: number of irreducible factors (counting repetitions) in the gcd;
- Z_d: number of distinct irreducible factors in the gcd;
- Z_t: total degree of the gcd.

We show that the limiting distribution of Z_t is geometric, while the distributions of Z_d and Z_r are very close to Poisson distributions when $q \geq 64$.

The proofs are based on two steps: the derivation of probability generating functions for the above random variables, and the application of asymptotic enumeration methods to obtain expectation, variance, moments and limiting distributions of the random variables.

References

[1] S. Corteel, C. Savage, H. Wilf, and D. Zeilberger, *A pentagonal number sieve*, Journal of Combinatorial Theory Series A **82** (1998), 186–192.

[2] M. Drmota and D. Panario, *A rigorous proof of the Waterloo algorithm for the discrete logarithm problem*, Designs, Codes and Cryptography **26** (2002), 229-241.

[3] Z. Gao and D. Panario, *Degree distribution of the greatest common divisor of polynomials over finite fields*, Preprint (2004).

[4] D. Panario, *What do random polynomials over finite fields look like?*, *Proceedings of the Seventh International Conference on Finite Fields: Theory, Applications, and Algorithms*, G.L. Mullen, A. Poli and H. Stichtenoth (eds), Lecture Notes in Computer Science 2948 (2004), 89-108.

Hyperelliptic curves, continued fractions, and Somos sequences

Alfred J. van der Poorten

(joint work with Alf van der Poorten)

Let $D(X)$ be a squarefree monic polynomial of degree $2g+2$ defined over a base field $\mathbb{F}$ and set $D = A^2 + 4R$ where A is the polynomial part of $\sqrt{D}$ and the remainder R has degree at most g. Set $Z = \frac{1}{2}(\sqrt{D}+A)$. Then $\mathcal{C} : Z^2 - AZ - R = 0$ defines a curve of genus g with a double point at ∞ and the definition of Z makes sense over arbitrary base fields, including those of characteristic 2.

I study the continued fraction expansion of $Z_0 = (Z+P_0)/Q_0$ where Q_0 divides the norm of its numerator, the polynomial s P_0 and Q_0 satisfy $\deg P_0 < g$ and $\deg Q_0 \le g$, and are so chosen that the expansion is 'normal' — all the partial quotients are of degree 1. If $\mathbb{F}$ is infinite this situation is generic. The expansion is then a doubly infinite sequence of lines $\ldots, -2, -1, h = 0, 1, 2, \ldots$

$$(Z+P_h)/Q_h = a_h - (\overline{Z}+P_h)/Q_h \quad \text{or, in brief,} \quad Z_h = a_h - \overline{R}_h$$

where all the Z_h *and* R_h are 'reduced'. More, the Q_h define a sequence $M_{h+1} = M + S_h$ of divisors on $\mathrm{Jac}(\mathcal{C})$ where, remarkably, $S_h = hS$ on $\mathrm{Jac}(\mathcal{C})$.

Now, for easy example, take $g = 1$. Then the $P_h := e_h$ are constants and mildly ingenious manipulation of the recursion formulas of the expansion leads to

$$e_{h-1}e_h^2e_{h+1} = v^2\big(e_h + A(w)\big), \quad \text{where } R(w) = 0.$$

In fact, the $-e_h$ turn out to be the abscissas of the points $M+hS$ on a nonsingular cubic model of $\mathcal{C}$ obtained by moving S to the origin by a suitable transformation. One now sees readily that the recursive definition $A_{h-1}A_{h+1} = e_hA^2$ yields

$$A_{h-2}A_{h+2} = v^2A_{h-1}A_{h+1} + v^2A(w)A_h^2$$

and that the 'Somos 4' sequence (A_h) consists entirely of integers (at most up to a finite number of primes building their denominators). In fact, the A_h are divsion polynomials 'translated by M' and evaluated at the point S.

And, oh! Yes. By reduction at primes this story of course encapsulates the infinitely many corresponding stories over each respective finite field.

References

[1] William W. Adams and Michael J. Razar, 'Multiples of points on elliptic curves and continued fractions', *Proc. London Math. Soc.* **41** (1980), 481–498.

[2] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs **104**, American Mathematical Society 2003, 318pp; see Chapter 10.

[3] David Gale, 'The strange and surprising saga of the Somos sequences', *Mathematical Intelligencer* **13**.1 (1991), 40–42; and 'Somos sequence update' , *ibid.* **13**.4 (1991), 49–50. For more see Jim Propp, 'The Somos Sequence Site' , `http://www.math.wisc.edu/~propp/somos.html`.

[4] Alfred J. van der Poorten, 'Periodic continued fractions and elliptic curves', in *High Primes and Misdemeanours*: lectures in honour of the 60th birthday of Hugh Cowie Williams; Alf van der Poorten and Andreas Stein eds., Fields Institute Communications **42**, American Mathematical Society, 2004, 353–365.

[5] Alf _____ , 'Elliptic curves and continued fractions', about to appear in *J. Integer Sequences*; `http://www.arxiv.org/math.NT/0403225`.

[6] Alf _____, 'Somos sequences and continued fractions', `http://www.maths.mq.edu.au/~alf/EllipticSequencesTalk2.pdf` [effectively, this talk].

[7] Alf _____ , 'Curves of genus 2 and continued fractions', soon to appear on the arXiv.

[8] Rachel Shipsey, *Elliptic divisibility sequences*, Phd Thesis, Goldsmiths College, University of London, 2000 (see `http://homepages.gold.ac.uk/rachel/`).

[9] Christine Swart, *Elliptic curves and related sequences*, PhD Thesis, Royal Holloway and Bedford New College, University of London, 2003; 226pp.

[10] Morgan Ward, 'Memoir on elliptic divisibility sequences', *Amer. J. Math.* **70** (1948), 31–74.

[11] Don Zagier, 'Problems posed at the St Andrews Colloquium, 1996, Solutions', 5th day; see `http://www-groups.dcs.st-and.ac.uk/~john/Zagier/Problems.html`.

Abelian varieties over Q with good reduction at all but a single prime

René Schoof

We study abelian varieties over $\mathbf{Q}$ that have good reduction at all but a single prime l. Our results are concerned with abelian varieties that have semi-stable reduction at l.

Theorem 1. *Let l be 2, 3, 5, 7 or 13. Then there do not exist any non-zero abelian varieties over $\mathbf{Q}$ that have good reduction at every prime different from l and have semi-stable reduction at l.*

This result is best possible, because the Jacobian varieties $J_0(l)$ of the modular curves $X_0(l)$ have good reduction at all primes different from l and are semi-stable at l. The genus of $X_0(l)$ is zero if and only if l is 2, 3, 5, 7 or 13.

For $l = 11$, 17 or 19, the genus of $X_0(l)$ is 1 and the Jacobian variety $J_0(l)$ has dimension 1. For these primes we can show the following.

Theorem 2. *Let l be* 11, 17 *or* 19. *Then any abelian variety over* $\mathbf{Q}$ *that has good reduction at all primes different from l and has semi-stable reduction at l is necessarily isogenous over* $\mathbf{Q}$ *to a power of $J_0(l)$.*

The proofs of Theorems 1 and 2 proceed by studying for a suitable small prime $p \neq l$, the p^n-torsion points $A[p^n]$ of abelian varieties A that have good reduction at every prime different from l and that have semi-stable reduction at l. For any pair of distinct primes p and l we introduce a suitable category $\underline{C}$ of finite flat group schemes of p-power order over the ring $\mathbf{Z}[\frac{1}{l}]$. In terms of this category we formulate two simple criteria for Theorem 1 to hold for the prime l. The first involves extensions of the group schemes μ_p by $\mathbf{Z}/p\mathbf{Z}$ over the ring $\mathbf{Z}[\frac{1}{l}]$. The second is concerned with simple objects in the categories $\underline{C}$. We show that both conditions are satisfied for $l = 2, 3, 5, 7, 13$ and $p = 3, 2, 2, 3, 2$ respectively.

For the primes $l = 11$, 17 and 19 things are different. In each case we take $p = 2$ and study the category $\underline{C}$. For the primes $l = 11$ and 19 the first condition of the criterion mentioned above fails. More precisely, for $l = 11$ and 19 the group scheme $J_0(l)[2]$ is an 'exotic' simple group scheme of order 4 over $\mathbf{Z}[\frac{1}{l}]$. However, the second condition still holds. For $l = 17$ it is the other way around. There exists a non-split extension of μ_2 by $\mathbf{Z}/2\mathbf{Z}$ over the ring $\mathbf{Z}[\frac{1}{17}]$. The group scheme $J_0(17)[2]$ is an example.

For the primes $l = 11, 17, 19$ we show that any abelian variety A that has good reduction at every prime different from l and semi-stable reduction at l, has the property that the group schemes of 2^n-torsion points $A[2^n]$ can be filtered with closed subgroups in such a way that the successive subquotients are isomorphic to $J_0(l)[2]$. The key points is then the fact that the only non-trivial extension of $J_0(l)[2]$ by itself is the group scheme $J_0(l)[4]$.

References

[1] Abraškin, V.A.: Galois moduli of period p group schemes over a ring of Witt vectors, *Izv. Ak. Nauk CCCP*, Ser. Matem. **51**, (1987). English translation in *Math. USSR Izvestiya* **31** (1988) 1–46.

[2] Fontaine, J.-M.: Il n'y a pas de variété abélienne sur $\mathbf{Z}$, *Invent. Math.* **81**, (1985) 515–538.

[3] Schoof, R.: Abelian varieties over $\mathbf{Q}$ with bad reduction in all but one prime, to appear.

Summation polynomials and the discrete logarithm problem on elliptic curves

Igor Semaev

Let E be the elliptic curve defined over the prime finite field $\mathbb{F}_p$ by the equation $Y^2 = X^3 + AX + B$. The discrete logarithm problem here is: given P, $Q \in E(\mathbb{F}_p)$, find an integer number n such that $Q = nP$ in $E(\mathbb{F}_p)$, if such an n exists. The elliptic curve discrete logarithm problem, introduced independently by Miller and Koblitz, is of great significance in cryptology. The aim of this talk is to present a construction of the index calculus type algorithm for the problem. The

construction depends on an auxiliary algorithm the existence of which is generally an open problem.

For any natural $n \geq 2$ we introduce the polynomial $f_n = f_n(X_1, X_2, \ldots, X_n)$ related to the arithmetic operation on E. We call this polynomial the *summation polynomial* and define it by the following property. Let $x_1, x_2, \ldots, x_n$ be any elements from $\overline{\mathbb{F}_p}$, the algebraic closure of $\mathbb{F}_p$. Then $f_n(x_1, x_2, \ldots, x_n) = 0$ if and only if there exist $y_1, y_2, \ldots, y_n \in \overline{\mathbb{F}_p}$ such that points (x_i, y_i) are on E and $(x_1, y_1) + (x_2, y_2) + \ldots (x_n, y_n) = P_\infty$ in the group $E(\overline{\mathbb{F}_p})$.

Theorem 1. *The summation polynomial satisfies* $f_2 = X_1 - X_2$,

$$f_3 = (X_1 - X_2)^2 X_3^2 - 2\left((X_1 + X_2)(X_1X_2 + A) + 2B\right) X_3 + \left((X_1X_2 - A)^2 - 4B(X_1 + X_2)\right),$$

$$\text{and} \quad f_n = \operatorname{Res}_X\left(f_{n-k}(X_1, \ldots, X_{n-k-1}, X), f_{k+2}(X_{n-k}, \ldots, X_n, X)\right)$$

for any $n \geq 4$ *and* $n - 3 \geq k \geq 1$. *It is symmetric and of degree* 2^{n-2} *in each variable for any* $n \geq 3$. *We have*

$$f_n(x_1, x_2, \ldots, x_n) = f_{n-1}^2(x_1, x_2, \ldots, x_{n-1}) X_n^{2^{n-2}} + \ldots.$$

Let d_n *be the total degree of the polynomial* f_n, *then* $(n-1)2^{n-2} \leq d_n \leq n2^{n-2}$.

We fix any natural number $n \geq 2$ and a small $\delta > 0$. For a random residue x modulo p we consider the equation

$$f_{n+1}(x_1, \ldots, x_n, x) \equiv 0 (\operatorname{mod} p) \tag{1}$$

in variables $x_1, x_2, \ldots, x_n$. Very probably (1) has a solution in integer numbers x_i^0 bounded by $p^{1/n+\delta}$. Imagine we have an auxiliary algorithm able to find such a solution. Under this assumption we formulate the algorithm for computing the discrete logarithm of Q to the base P. If the algorithm, finding a bounded solution to (1), works in $t_{p,n}$ operations, then the complexity of the discrete logarithm problem in $E(\mathbb{F}_p)$ is essentially

$$t_{p,n} p^{1/n+\delta} + p^{2/n+2\delta}$$

operations. When $t_{p,n}$ is small enough, this amount may be reduced by a trick due to Harley and Thériault, see [4]. When $n \geq 5$, even for some exponential $t_{p,n}$, this amount may be less than $O(p^{1/2})$ provided by Pollard's methods.

The first variant of the present paper [3] was posted on the Cryptology ePrint Archive web-site. Later the method got a development by Gaudry [2], who applied the ideas introduced in [3] to elliptic curves E over finite fields $\mathbb{F}_{q^n}$ for small n. Gaudry showed that to get a useful relation one solves a system of n nonlinear equations of total degree 2^{n-1} in n variables over $\mathbb{F}_q$, which comes from the $n+1$-th summation polynomial. For fixed n and $q \to \infty$ the system may be effectively solved using the Gröbner basis computation. In so doing he got a method able, at least asymptotically, to beat Pollard's bound regardless of the curve. Afterwards the method got a further development by Diem [1], who gave a variant of the method with subexponential behavior for some pairs q, n.

References

[1] C. Diem, *On the discrete logarithm problem in elliptic curves over non-prime finite fields*, preprint, 2 Aug 2004.

[2] P. Gaudry, *Index calculus for abelian varieties and the elliptic curve discrete logarithm problem*, Cryptology ePrint Archive, report 2004/073, 4 Mar 2004.

[3] I. Semaev, *Summation polynomials and the discrete logarithm problem on elliptic curves*, Cryptology ePrint Archive, report 2004/031, 5 Feb 2004.

[4] N. Thériault, *Index calculus attack for hyperelliptic curves of small genus(Asiacrypt 2003)*, LNCS **2894** (2003), Springer, Berlin, 75–92.

Some Artin-Schreier towers are easy

Henning Stichtenoth

(joint work with Arnaldo Garcia)

An Artin-Schreier tower over the finite field $\mathbb{F}_q$ is a sequence of function fields $\mathcal{F} = (F_0 \subset F_1 \subset F_2 \subset ...)$ such that all extensions F_{n+1}/F_n are Artin-Schreier extensions of function fields F_n over $\mathbb{F}_q$.

One knows two explicitly given Artin-Schreier towers whose limit $\lambda(\mathcal{F}) = \lim_{n\to\infty} N(F_n)/g(F_n)$ achieves the Drinfeld-Vladut bound $\sqrt{q}-1$, resp. the Zink bound $2(p^2-1)/(p+2)$ for $q = p^3$ with a prime number p. Here $N(F)$ and $g(F)$ denote the number of rational places and the genus of the function field F, respectively. These examples, due to Garcia - Stichtenoth [1] and van der Geer - van der Vlugt [2], are defined recursively by the equations

$$y^l + y = \frac{x^l}{x^{l-1}+1} \quad \text{over the field } \mathbb{F}_q \text{ with } q = l^2$$

and

$$y^2 + y = x + 1 + \frac{1}{x} \quad \text{over the field with 8 elements.}$$

The determination of the genus of the fields F_n in [1] and [2] requires long and technical calculations. We give here a much simpler proof for the asymptotic behaviour of the genus in these two towers. This proof is based on a simple lemma about the different exponent in the composite of two cyclic extensions of function fields of degree p.

References

[1] A. Garcia and H. Stichtenoth, *On the asymptotic behaviour of some towers of function fields over finite fields*, J. Number Theory **61** (1996), 248-273.

[2] G. van der Geer and M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, Bull. London Math. Soc. **34** (2002), 291-300.

On the Nonlinear Congruential Pseudorandom Number Generators of Higher Orders

Alev Topuzoğlu
(joint work with Arne Winterhof)

We study nonlinear generators of higher orders defined by recurrence relations of order $m \geq 2$;

$$u_{n+1} = f(u_n, u_{n-1}, \ldots, u_{n-m+1}), \ n = m-1, m, \ldots \tag{1}$$

Here initial values $u_0, \ldots, u_{m-1}$ are in $\mathbb{F}_p$ with prime p and $f \in \mathbb{F}_p(X_1, \ldots, X_m)$. These generators are of particular interest as the period length of generated sequences can go up to p^m. Firstly we give a lower bound for the linear complexity profile of the sequence (1) where we take $f \in \mathbb{F}_p[X_1, \ldots, X_m]$, belonging to the class $\mathcal{LI}$ (see [1]).

Theorem 1. *Let (u_n) be defined as in (1) with $f \in \mathcal{LI}$. Suppose (u_n) is purely periodic with least period t, and the total degree of f is d. Then the linear complexity profile $L((u_n), N)$ of (u_n) satisfies*

$$L((u_n), N) \geq \min\left\{ \left\lceil \log_d \left(\frac{N - \lfloor \log_d(N/p^{m-1}) \rfloor - m + 1}{p^{m-1}} \right) \right\rceil, \left\lceil \log_d \left(\frac{t}{p^{m-1}} \right) \right\rceil \right\}.$$

Theorem 1 can be improved under some additional conditions;

Theorem 2. *Let $f \in \mathbb{F}_p[X_1, \ldots, X_m]$ with total degree d and dominating term $X_1^{d_1} X_2^{d_2} \cdots X_m^{d_m}$, where $d_1 \geq 2$. Suppose (u_n) is defined as in (1) and has least period p^m. Then the linear complexity profile $L((u_n), N)$ of (u_n) satisfies*

$$L((u_n), N) \geq \min\left(\left\lceil \frac{p}{d} \right\rceil p^{m-1} + 1, N + 1 - p^m \right), \quad N \geq 1.$$

We also consider a rational function $f \in \mathbb{F}_p(X_1, \ldots, X_m)$ which yields the inversive congruential pseudorandom number generator of higher orders. We give a lower bound for the linear complexity profile of the generated sequence in case it has least period p^m (see [1]).

Distribution of inversive congruential pseudorandom numbers of higher orders is of great interest. We present a bound on the discrepancy in parts of the period when the sequence has largest possible period p^m (see [2]).

Our work generalizes some previous results obtained for the case $m = 1$.

References

[1] A. Topuzoğlu, A. Winterhof, *On the linear complexity profile of nonlinear congruential pseudorandom number generators of higher orders*, Preprint (2004).
[2] A. Topuzoğlu, A. Winterhof, *On the distribution of inversive congruential pseudorandom numbers of higher orders with largest possible period*, In preparation.

On the point orders of elliptic curves

Serge Vlăduţ

The orders of points on elliptic curves over finite fields are interesting both for applications in crypography and theoretically. In recent papers [2], [3] (cf. also [1]) this question got a satisfactory answer for orders rather close the the possible maximum, but not attaining it. It is shown there that a randomly chosen point over randomly chosen elliptic curve over a finite field, with overwhelming probability generates a cyclic subgroup of size rather close to the maximum. In our talk we are interested in the probability that the order attains this maximum, i.e. that the elliptic curve is cyclic and the point generates its group.

Let E be a (randomly chosen) elliptic curve over a (fixed) finite field $\mathbf{F}_q$, and let G be a (randomly chosen) point in $E(\mathbf{F}_q)$. We note $N = N(E)$ the order of the group $E(\mathbf{F}_q)$, $ord(G)$ being the order of G. Let $P(q)$ be the probability that G generates $E(\mathbf{F}_q)$, i.e. $P(q) := \Pr(ord(G) = N)$.

We consider the two (most important in cryptography) cases:

(1) $q = 2^l$ with prime l;
(2) $q = p$ is prime.

We get using the methods of [4]:

(1) $\lim_{l\to\infty} P(2^l) = 1/2$;
(2) $1/3 \le \liminf_{p\to\infty} P(p) \le \limsup_{p\to\infty} P(p) \le 6/\pi^2$.

References

[1] W. Duke, *Almost all reductions of an elliptic curve have a large exponent*, C. R. Math. Acad. Sci. Paris **337** (2003), 689–692.
[2] F. Luca, J. McKee, I. Shparlinski, *Small exponent point groups on elliptic curves*, Preprint, 2003.
[3] I. Shparlinski, *Order of points on elliptic curves*, Preprint, 2003.
[4] S. Vlăduţ, *Cyclicity statistics for elliptic curves over finite fields*, Finite Fields Appl. **5** (1999), 13–25.

Linear complexity of Sidelnikov sequences

Arne Winterhof
(joint work with Moubariz Garaev, Florian Luca, Wilfried Meidl, and Igor Shparlinski)

Let q be a power of an odd prime p and α a primitive element of the finite field $\mathbb{F}_q$. Let η denote the *quadratic character* of $\mathbb{F}_q$. Then the *Sidelnikov sequence* is the $(q-1)$-periodic binary sequence (s_n) defined by

$$s_n = \begin{cases} 1 & \text{if } \eta(\alpha^n + 1) = -1, \\ 0 & \text{otherwise,} \end{cases} \qquad n = 0, 1, \ldots. \tag{1}$$

The *linear complexity* $L(a_n)$ of a sequence (a_n) over a field $\mathbb{F}$ is the smallest positive integer L such that there are constants $c_1, \ldots, c_L \in \mathbb{F}$ satisfying

$$a_n \equiv c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_L a_{n-L} \quad \text{for all } n \geq L.$$

The linear complexity provides information on the predictability and thus unsuitability for cryptography. Hence, a low linear complexity has turned out to be an undesirable feature of keystreams.

We determine the exact value of the *linear complexity over* $\mathbb{F}_2$ of the sequence (1) in many cases (see [3, 4]). The proofs are based on number theoretic results: bounds on *character sums* and formulas for *cyclotomic numbers*.

Several results on the *linear complexity* L *over* $\mathbb{F}_p$ of Sidelnikov sequences have recently been obtained (see [2] and references therein). More precisely, in [2] it has been shown that

$$L = q - 1 - M,$$

where M is the number of solutions to the congruence

$$2^{-2n}\binom{2n}{n} \equiv (-1)^{(q-1)/2} \pmod{p}, \qquad n = 0, \ldots, \frac{q-3}{2}.$$

We estimate M (see [1]). In particular, these estimates are based on bounds of character sums of the form

$$S(\chi, N) = \sum_{n=0}^{N-1} \chi\left(2^{-2n}\binom{2n}{n}\right), \qquad 1 \leq N \leq (p+1)/2,$$

where χ is a nontrivial multiplicative character of $\mathbb{F}_p$.

References

[1] M. Garaev, F. Luca, I. Shparlinski, and A. Winterhof, *On the Linear Complexity over $\mathbb{F}_p$ of Sidelnikov Sequences*, Preprint 2004.

[2] T. Helleseth, M. Maas, J.E. Mathiassen, and T. Segers, *Linear complexity over $\mathbb{F}_p$ of Sidelnikov sequences*, IEEE Trans. Inform. Theory **50** (2004), 2468–2472.

[3] G.M. Kyureghyan, A. Pott, *On the linear complexity of the Sidelnikov-Lempel-Cohn-Eastman sequences*, Designs, Codes, and Cryptography **29** (2003), 149–164.

[4] W. Meidl, A. Winterhof, *Some Notes on the Linear Complexity of Sidelnikov-Lempel-Cohn-Eastman Sequences*, Preprint 2004.

An algorithm for solving $\sum_{i=1}^{n} a_i x_i^n = b$ over finite fields

Christiaan E. van de Woestijne

(This work is part of my Ph.D. project with Hendrik W. Lenstra, Jr.)

It is a remarkable fact that all known algorithms for solving polynomial equations over finite fields (such as taking square and higher roots, factorisation of polynomials, and derived algorithms for finding zeros of multivariate polynomials) are either probabilistic or inefficient. Even if we assume the Generalised Riemann

Hypothesis (GRH), root taking becomes deterministic, but this is not known for factorisation of polynomials.

In this talk, I present a tower of three new algorithms which are both efficient (taking polynomial time in terms of their input size) and deterministic. This is achieved because these algorithms solve problems that are just somewhat easier than the ones mentioned above (for example, the more variables a polynomial has, the easier it is to find a zero). The problems solved are the following:

(1) Given $\mathbb{F}$ and n, find $\alpha \in \mathbb{F}$ such that $\mathbb{F} = \mathbb{F}_p(\alpha^n)$.
(2) Given $\mathbb{F}$ and n, and a nonzero $b \in \mathbb{F}$, find $x_1, \ldots, x_n \in \mathbb{F}$ such that $b = \sum_{i=1}^n x_i^n$ (if possible).
(3) Given $\mathbb{F}$ and n, and nonzero elements $a_1, \ldots, a_n$ and $b \in \mathbb{F}$, find elements $x_1, \ldots, x_n \in \mathbb{F}$ such that $b = \sum_{i=1}^n a_i x_i^n$ (if possible).

Here n is a given positive integer, while $\mathbb{F}$ denotes a finite field of characteristic p.

Algorithm 1 is based on (what could be called) a multiplicative version of the primitive element theorem. Algorithms 2 and 3 employ a generalisation of the Tonelli-Shanks algorithm, derived (but beyond recognition) from an idea of in [1]. Algorithm 3 is an algorithmic version of an idea of Dem′yanov (see [2] and [3, Théorème 4.1]) and Kneser [4, Theorem XI.4.4]; this idea provides a constructive proof of the case of the Chevalley-Warning theorem that corresponds to the title equation.

Furthermore, Algorithm 2 calls Algorithm 1, and Algorithm 3 calls both preceding ones.

Details of these results will appear in my Ph.D. thesis (defense mid 2005). A preliminary version [5] can be obtained from my home page.

References

[1] Richard T. Bumby. Sums of four squares. In *Number theory (New York, 1991–1995)*, pages 1–8. Springer, New York, 1996.
[2] V. B. Dem′yanov. On representation of a zero of forms of the form $\sum_{i=1}^m a_i x_i^n$. *Dokl. Akad. Nauk SSSR (N.S.)*, 105:203–205, 1955.
[3] Jean-René Joly. Équations et variétés algébriques sur un corps fini. *Enseignement Math. (2)*, 19:1–117, 1973.
[4] T. Y. Lam. *The algebraic theory of quadratic forms*. W. A. Benjamin, Inc., Reading, Mass., 1973. Mathematics Lecture Note Series.
[5] C. E. van de Woestijne. Deterministic equation solving over finite fields. Preprint (2004). Available from `http://www.math.leidenuniv.nl/~cvdwoest`.

A class of Artin-Schreier towers with finite genus

Siman Yang
(joint work with San Ling and Henning Stichtenoth)

This report is on a joint work [5] with San Ling and Henning Stichtenoth. The aim of this work is to exhibit a new class of Artin-Schreier towers of function fields with finite genus, defined over any finite field.

In recent years several asymptotically good function fields towers of Artin-Schreier type have been found [2, 4]. Later they were classified in [1] as Type I Artin-Schreier towers. It is still an open problem if there exist good towers of Type II or Type III. Here we exhibit the first Artin-Schreier tower of Type III with finite genus, which is recursively defined by

$$y^q + by = \frac{1}{x^q + cx} \quad \text{with} \quad bc(b-c)^{2q-2} = 1,$$

over any finite field $K = \mathbb{F}_{p^r}$, where b, c are constants in K, and q is a power of prime p. The genus of this tower is proven to be at most q^2.

The authors studied the ramification behaviour in a broader class of towers recursively defined by $y^p + by = 1/(x^p + cx)$, where b and c are nonzero distinct constants in K, by performing pole order reduction in order to apply Artin-Schreier theory to determine the different exponent in every extension of the tower. The different exponent of any ramified place in any extension step of such tower is proven to be $2q - 2$. This result has been generalized to a general theorem in [3].

We also show the ramification locus of the tower is finite. Let γ be a fixed root of $x^{q-1} + c = 0$ and define $\delta = (b-c)\gamma$, the ramification locus of the tower is found to be $\{P_\infty\} \cup \{P_\alpha \mid \alpha^q + b\alpha = t\delta \text{ for some } t \in \mathbb{F}_q\}$.

Finite ramification locus of the tower and small different exponents of the ramified places ensure finite genus of the tower.

References

[1] P. Beelen, A. Garcia, H. Stichtenoth, *On towers of function fields of Artin-Schreier type*, Bull. Braz. Math. Soc. **35** (2004), 151-164.

[2] A. Garcia, H. Stichtenoth, *On the asymptotic behaviour of some towers of function fields over finite fields*, J. Number Theory **61** (1996), 248-273.

[3] A. Garcia, H. Stichtenoth, *Some Artin-Schreier towers are easy*, Preprint (2004).

[4] G. van der Geer, M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, Bull. London Math. Soc. **34** (2002), 291-300.

[5] S. Ling, H. Stichtenoth, S. Yang, *A class of Artin-Schreier towers with finite genus*, Preprint (2004).

Reporter: Christiaan E. van de Woestijne

Participants

Henning E. Andersen
henning@math.aau.dk
Dept. of Mathematical Sciences
University of Aalborg
Fredrik Bajers Vej 7G
DK-9220 Aalborg East

Dr. Simeon Ball
simeon@mat.upc.es
Dep. de Matematica Aplicada IV
Universitat Politec. de Catalunya
Jordi Girona 1-3
Modul C3, Campus Nord
E-08034 Barcelona

Alp Bassa
alp.bassa@uni-duisburg-essen.de
FB 6 - Mathematik
Universität Duisburg-Essen
Standort Essen
D–45117 Essen

Dr. Peter Beelen
p.beelen@mat.dtu.dk
Department of Mathematics
Technical University of Denmark
Bldg. 303
DK-2800 Lyngby

Dr. Tim D. Browning
browning@maths.ox.ac.uk
Mathematical Institute
Oxford University
24 - 29, St. Giles
GB-Oxford OX1 3LB

Denis Charles
cdx@cs.wisc.edu
Computer Sciences Department
University of Wisconsin-Madison
1210 West Dayton St.
Madison, WI 53706-1685 – USA

Prof. Dr. Qi Cheng
qcheng@bachman.cs.ou.edu
qcheng@cs.ou.edu
School of Computer Science
University of Oklahoma
Norman OK 73019 – USA

Prof. Stephen D. Cohen
sdc@maths.gla.ac.uk
Department of Mathematics
University of Glasgow
University Gardens
GB-Glasgow, G12 8QW

Prof. Dr. Pinaki Das
pxd14@psu.edu
das@math.psu.edu
Department of Mathematics
Penn State-Altoona
3000 Ivyside Drive
Altoona, PA 16601 – USA

Prof. Dr. Hans Dobbertin
Hans.Dobbertin@rub.de
hans.dobbertin@ruhr-uni-bochum.de
Lehrstuhl Informationssicherheit
NA 5/72
Ruhr-Univeristät Bochum
Universitätsstr. 150
D–44780 Bochum

Prof. Dr. Gerhard Dorfer
g.dorfer@tuwien.ac.at
Institut für Diskrete Mathematik
und Geometrie
Technische Universität Wien
Wiedner Hauptstr. 8-10/104
A-1040 Wien

Dr. Jeroen Doumen
doumen@cs.utwente.nl
Department of Computer Science
University of Twente
P. O. Box 217
NL-7500 AE Enschede

Prof. Dr. Arnaldo Garcia
garcia@impa.br
Instituto Nacional de Matematica
Pura e Aplicada; IMPA
Estrada Dona Castorina 110
Rio de Janeiro, RJ - CEP: 22460-320
BRASIL

Prof. Dr. Joachim von zur Gathen
gathen@uni-paderborn.de
gathen@upb.de
Fakultät für Elektrotechnik,
Informatik und Mathematik
Universität Paderborn
D–33095 Paderborn

Prof. Dr. Gerard van der Geer
geer@science.uva.nl
Korteweg-de Vries Instituut
Faculteit WINS
Universiteit van Amsterdam
Plantage Muidergracht 24
NL-1018 TV Amsterdam

Dr. Mark Giesbrecht
mwg@uwaterloo.ca
School of Computer Science
University of Waterloo
Waterloo ONT N2L 3G1 – Canada

Prof. Dr. Wenbao Han
wb.han@netease.com
Department of Applied Mathematics
College of Information Engineering
Information Engineering University
Zhengzhou 450002 – P.R. of China

Prof. Dr. Florian Heß
hess@math.tu-berlin.de
Fakultät II -Institut f. Mathematik
Technische Universität Berlin
Sekr. MA 8-1
Straße des 17. Juni 136
D–10623 Berlin

Prof. Dr. Erich Kaltofen
kaltofen@math.ncsu.edu
Department of Mathematics
North Carolina State University
Campus Box 8205
Raleigh, NC 27695-8205 – USA

Prof. Dr. Gabor Korchmaros
korchmaros@unibas.it
Dipartimento di Matematica
Universita degli Studi
della Basilicata
Contrada Macchia Romana
I-85100 Potenza

Dr. Tanja Lange
lange@exp-math.uni-essen.de
Lange@itsc.ruhr-uni-bochum.de
Institute for Information Security
and Cryptology
Ruhr-Universität Bochum
Universitätsstr. 150
D–44780 Bochum

Prof. Dr. Vsevolod F. Lev
seva@math.haifa.ac.il
Department of Mathematics
University of Haifa at Oranim
36006 Tivon – ISRAEL

Prof. Dr. Winnie Li
wli@math.psu.edu
Department of Mathematics
Pennsylvania State University
University Park, PA 16802 – USA

Prof. Dr. Hiren Maharaj
hmahara@clemson.edu
Dept. of Mathematical Sciences
Clemson University
Martin Hall
Clemson, SC 29634-0975 – USA

Prof. Dr. Gary L. Mullen
mullen@math.psu.edu
Department of Mathematics
Pennsylvania State University
University Park, PA 16802 – USA

Prof. Dr. Enric Nart
nart@mat.uab.es
Departament de Matematiques
Universitat Autonoma de Barcelona
Campus Universitari
E-08193 Bellaterra, Barcelona

Prof. Dr. Ferruh Ozbudak
ozbudak@math.metu.edu.tr
Department of Mathematics
Middle East Technical University
06531 Ankara – Turkey

Prof. Dr. Daniel Panario
School of Mathematics & Statistics
Carleton University
1125 Colonel By Drive
Ottawa, Ont. K1S 5B6 – Canada

Prof. Dr. Alfred J. van der Poorten
alf@math.mq.edu.au
1 Bimbil Place
Killara 2071 – Australia

Prof. Dr. John A.G. Roberts
jagr@maths.unsw.edu.au
Jag.Roberts@unsw.edu.au
School of Mathematics
The University of New South Wales
Sydney NSW 2052 – Australia

Prof. Dr. Hans-Georg Rück
rueck@mathematik.uni-kassel.de
FB 17 - Mathematik/Informatik -
Universität Kassel
D–34109 Kassel

Prof. Dr. Rene Schoof
schoof@science.uva.nl
schoof@mat.uniroma2.it
Dipartimento di Matematica
Universita degli Studi di Roma II
Tor Vergata
Via della Ricerca Scientifica
I-00133 Roma

Prof. Dr. Igor Semaev
igor@ii.uib.no
Department of Informatics
University of Bergen
Hoyteknologisenteret
N-5020 Bergen

Prof. Dr. Igor E. Shparlinski
igor@comp.mq.edu.au
igor@mpce.mq.edu.au
Department of Computing
Macquarie University
Sydney NSW 2109 – Australia

Prof. Dr. Henning Stichtenoth
stichtenoth@uni-essen.de
mat310@uni-essen.de
henning@sabanciuniv.edu
FB 6 - Mathematik
Universität Duisburg-Essen
Standort Essen
D–45117 Essen

Dr. Arne Storjohann
astorjoh@uwaterloo.ca
School of Computer Science
University of Waterloo
Waterloo ONT N2L 3G1 – Canada

Prof. Dr. Alev Topuzoglu
alev@sabanciuniv.edu
Sabanci Universitesi
Orhanli
Tuzla
34956 Istanbul – Turkey

Prof. Dr. Franco Vivaldi
F.Vivaldi@qmul.ac.uk
Department of Mathematics
Queen Mary University of London
Mile End Road
GB-London E1 4NS

Prof. Dr. Serge Vladut
vladut@iml.univ-mrs.fr
IML
CNRS
Case 907 - Luminy
F-13288 Marseille Cedex 9

Prof. Dr. Jose Felipe Voloch
voloch@math.utexas.edu
Department of Mathematics
University of Texas at Austin
1 University Station C1200
Austin, TX 78712-1082 – USA

Prof. Dr. Arne Winterhof
arne.winterhof@oeaw.ac.at
Johann Radon Institute
Austrian Academy of Science
Altenberger Straße 69
A-4040 Linz

Christiaan van de Woestijne
cvdwoest@math.leidenuniv.nl
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Siman Yang
scip0242@nus.edu.sg
Department of Mathematics
National University of Singapore
2 Science Drive
Singapore 117543 – Singapore

Prof. Dr. Joe L. Yucas
jyucas@math.siu.edu
Department of Mathematics
Southern Illinois University
Carbondale, IL 62901-4408 – USA

Dr. Michael Zieve
zieve@idaccr.org
Center for Communications Research
IDA
805 Bunn Drive
Princeton NJ 08540 – USA