Workshop on Polynomials over Finite Fields: Functional and Algebraic Properties
19–23 May 2014

OPEN PROBLEMS

Problem 1 (Igor Shparlinski). Obtain a function field analogue of the bound of Bombieri and Pila [1, Theorem 4]:

Let \( R = \mathbb{F}_q[T] \) and let \( F(X,Y) \in R[X,Y] \) be an absolutely irreducible polynomial of degree \( d \) over \( K \). Obtain an upper bound on the number of solutions to the equations \( F(x,y) = 0 \) in polynomials \( x(T), y(T) \in R \) of degree at most \( n \) (as \( n \to \infty \)).

It is reasonable to assume that \( q \) and \( d \) are fixed but \( n \) is a growing parameter. There are several problems on polynomials in finite fields where such a bound can be used, see, for example, [3].

Problem 2 (Igor Shparlinski). Obtain analogues of the results of Ford [6] on the number of polynomials having a divisor of a degree in a given range and then on multiplication table for polynomials.

Let \( n \geq m \geq k \geq 0 \) be integers. Obtain tight bounds on the number of monic polynomials \( f \in \mathbb{F}_q[X] \) having a divisor \( g \in \mathbb{F}_q[X] \) of degree \( m \geq \deg g \geq k \).

Let \( n \geq 1 \) be an integer. Obtain tight bounds on the number of distinct products of the form \( fg \) where \( f, g \in \mathbb{F}_q[X] \) are monic polynomials of degree \( \deg g, \deg f \leq n \).

It is probably reasonable to assume that \( q \) is fixed but \( k, m, n \) are growing parameters. One should expect results of at least the same strength as those of [6] and maybe even stronger as it often happens in the function field case.

Problem 3 (Andreas Bender). The \( 3x + 1 \) conjecture for polynomials

Start with a natural number \( x \in \mathbb{N} \) on the left and a polynomial \( f \in \mathbb{F}_2[t] \) on the right and construct a sequence by iterating the corresponding rule as follows:

\[
\begin{align*}
x & \rightarrow \begin{cases} 
3x + 1 & \text{if } x \text{ is odd,} \\
x/2 & \text{if } x \text{ is even}
\end{cases}, \\
f(t) & \rightarrow \begin{cases} 
(t+1)f(t) + t & \text{if } f(0) \neq 0, \\
f(t)/t & \text{if } f(0) = 0.
\end{cases}
\end{align*}
\]

Conjecture: The sequence reaches the number 1 for any starting value \( x \in \mathbb{N} \) and \( f(t) \in \mathbb{F}_2[t] \).

This conjecture is wide open for \( \mathbb{N} \) ([14, 15]) and not embedded in a well-developed theory.

The conjecture for \( f(t) \in \mathbb{F}_2[t] \) can be proved by a simple induction on the degree [13], which also works for a version for polynomials over an arbitrary field. However, the conjecture fails already for \( \mathbb{F}_3[t] \).

With very few sources available ([3], [4] and [5]) and a lot of freedom to choose the parameters of such dynamical systems, there seems ample opportunity for further investigations.

Problem 4 (Luis Gallardo). Consider the sequence \( g_n \) defined in \( \mathbb{F}_2[x] \) by \( g_0 = 0, g_1 = 1 \) and by

\[ g_{n+1} = g_n + \Delta g_{n-1}, \]

where \( \Delta \) is a fixed non-constant polynomial in \( \mathbb{F}_2[x] \). In a recent work in common with Reinhardt Euler and Florian Luca [4] (see also [2, 5]) we discovered some simple properties of \( g_n \), mainly an explicit formulae to write

\[ g_n = P_n(\Delta) \]

as a polynomial in \( \Delta \) with coefficients in \( \mathbb{F}_2 \), in very special cases for \( n \), as well as a description of the number of nonzero terms of \( P_n(x) \). However we do not know anything about the number of irreducible factors of \( P_n(x) \), nor about the degrees of these factors. Moreover, is it true that all roots of \( P_{2n+1}(x) \) are simple?
Problem 5 (Luis Gallardo). A binary perfect polynomial $A \in \mathbb{F}_2[x]$ is a fixed point of the $\sigma$ function i.e., satisfies
\[ \sigma(A) = A, \]
where $\sigma(A) = \sum_{D|A} D$ is the sum of all divisors of $A$ in $\mathbb{F}_2[x]$, including $A$ and 1. A binary polynomial is even if it has at least one root in $\mathbb{F}_2$, otherwise it is called odd. The even perfect polynomials $(x(x+1))^{2^n-1}$ are trivial perfect. The other even perfect polynomials are sporadic. There are only 11 known sporadic polynomials. Nine of them are characterized by their factorization into a product of primes, namely into a product of irreducible polynomials of $\mathbb{F}_2[x]$. More precisely, these 9 polynomials are the only polynomials $A \in \mathbb{F}_2[x]$ such that
\[ A = x^n(x+1)^h M_1^{h_1} \cdots M_r^{h_r}, \]
where each $h_j+1$ is some power of 2 and the $M_i$ are Mersenne irreducible polynomials, i.e. irreducible polynomials $M$ of the form $M = 1 + x^c(x+1)^d$. We do not know how we can characterize the remaining two known sporadic even perfect polynomials, namely how to characterize:
\[ S_1 = x \ast (x+1)^2 \ast (x^2 + x + 1)^2 \ast (x^4 + x + 1) \]
and
\[ S_2 = S_1(x+1) = (x+1) \ast x^2 \ast (x^2 + x + 1)^2 \ast (x^4 + x + 1). \]
See [8, 9, 10, 11, 12] for results regarding this problem.

Banff Workshop: The Art of Iterating Rational Functions over Finite Fields

The following problems were suggested by several participants during the open problem session at the workshop The Art of Iterating Rational Functions over Finite Fields, 5-10 May 2013, Banff.

Problem 6 (Voloch-Kurlberg). Let $f : X/\mathbb{Q} \to X/\mathbb{Q}$ and $f_p : X(\mathbb{F}_p) \to X(\mathbb{F}_p)$. We fix $x_0 \in X$ and let $C_p$ be the cycle part of the orbit of $f_p$ starting at $x_0$. It is expected that $|C_p| \sim p^{d/2}$ as $p$ varies, where $d = \dim X$.

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

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

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

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

Problem 7 (Maubach). Let $E = (E_1, E_2, \ldots, E_n)$ where $E_i \in K[x_1, \ldots, x_n]$. $E$ is called a polynomial automorphism if there exists $F = (F_1, \ldots, F_n)$ such that
\[ E \circ F = (x_1, \ldots, x_n). \]

Definition 1. The equivalence relation: $E \sim E'$ if there exists $F, G$ automorphisms such that
\[ F \circ E \circ G = E'. \]
If the univariate polynomials \( p, q \in K[x] \) satisfy \( p(x) \not\sim q(x) \), does \( p(x, y_1, \ldots, y_n) \not\sim (q(x, y_1, \ldots, y_n) \) hold?

If \( \text{char}(K) = 0 \), this is true. In \( K = \mathbb{F}_2 \), given
\[
\begin{align*}
p(x) &= x + x^2 + x^8 \\
q(x) &= x + x^4 + x^8
\end{align*}
\]
not equivalent:

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

**Problem 8** (Anashin). Consider the following map \( g : x \mapsto \frac{x(x+1)}{2} \) with \( x \in \{0, \ldots, 2^n - 1\} \). Calculate \( x \mapsto g(x) \mod 2^n \). For all \( n \in \mathbb{N} \) this is a permutation.

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

**Motivation:** (Woodcock-Smart 1998, Yurov 1998)

**Problem 9** (Ostafe). In the univariate case, over a field of characteristic zero, it is proved in [7] that the minimum number of terms necessary to express an iterate \( f^{(n)} \) of a rational function \( f \) tends to infinity with \( n \), provided \( f \) is not of an explicitly described special shape:

We denote by \( T_d \) the Chebyshev polynomial of degree \( d \) defined by
\[
T_d(x + x^{-1}) = x^d + x^{-d}.
\]

**Theorem 1** (Fuchs-Zannier (2012)). Let \( \mathbb{F} \) be a field of characteristic 0 and \( f \in \mathbb{F}(X) \) of degree \( d \geq 3 \). Suppose that \( f \) is not conjugate (with respect to the group action given by \( \text{PGL}_2(\mathbb{F}) \) on \( \mathbb{F}(X) \)) to \( \pm X^d \) or to \( \pm T_d(X) \). Then, for any integer \( n \geq 3 \), we cannot express \( f^{(n)} \) as a ratio of two polynomials having altogether less than \( ((n - 2) \log d - \log 2016)/\log 5 \) terms.

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

Moreover, in the multivariate case one can also show that an analogue of the result [7] does not hold anymore, and this happens over any field, not necessarily over finite fields, as the next example shows (known as the Nagata automorphism).

Let \( m = 3 \) and
\[
\begin{align*}
F_1 &= X_1 - 2X_2(X_1X_3 + X_2^2) - X_3(X_1X_3 + X_2^2)^2 \\
F_2 &= X_2 + X_3(X_1X_3 + X_2^2) \\
F_3 &= X_3.
\end{align*}
\]
Then, for any \( k \geq 1 \),
\[
\begin{align*}
F_1^{(k)} &= X_1 - 2kX_2(X_1X_3 + X_2^2) - k^2X_3(X_1X_3 + X_2^2)^2, \\
F_2^{(k)} &= X_2 + kX_3(X_1X_3 + X_2^2), \\
F_3^{(k)} &= X_3.
\end{align*}
\]

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

1. univariate rational functions over finite fields?
2. multivariate polynomials in any characteristic?
Problem 10 (Ostafe). Are there families of multivariate Deligne polynomials which are Deligne under iteration?

Problem 11 (Hone). Consider a rational map \( \phi : \overline{\mathbb{F}} \to E(\overline{\mathbb{F}}) \), \( \phi \in \text{End}(K(\overline{\mathbb{F}})) \). Let \( d_n = \deg \phi^n \) be the degree of the \( n \)th iterate. The limit \( E = \lim_{n \to \infty} \frac{\log d_n}{n} \) is called the entropy of \( \phi \). Suppose that \( E = 0 \) and \( d_n \) is not bounded.

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

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

Problem 12 (Shparlinski). Known: given a finite set \( X \) and a random permutation \( f \). The average cycle length should be approximately \( |X|^{1/2} \), but the number \( N \) such that \( f^{(N)} = \text{id} \) is larger. On average (over all permutations) \( N \sim \exp \left( c_0 \left| \frac{|X|}{\log^2 |X|} \right|^{1/3} \right) \), where \( c_0 \approx 3.36 \) (Schmutz, 2011).

1. Given \( x_0 \in \mathbb{F}_q \) and any reasonable map \( f \) (polynomial, rational, etc). We expect \( |C_p(x_0)| \sim q^{1/2} \). What about \( N \) such that \( f^{(N)} = \text{id} \)?
   We may assume that \( f \) is a permutation, otherwise \( N = \infty \).

Problem 13 (Elkies). Is there a rationally parametrized quadratic function that has a rational 6-cycle? An elliptic curve is known.

References


