

# Open Problems for Polynomials over Finite Fields and Applications <sup>1</sup>

Daniel Panario  
School of Mathematics and Statistics  
Carleton University  
daniel@math.carleton.ca

ALCOMA, March 2015

---

<sup>1</sup>“Open problems for polynomials over finite fields and applications”, Chap. 5 of “Open Problems in Mathematics and Computational Science”, Springer, 111-126, 2015.

# Schedule of the Talk

We focus only on **univariate polynomials over a finite field**.

- We first comment on the existence and number of several classes of polynomials. Open problems are **theoretical**.
- Then, we center in classes of low-weight (irreducible) polynomials. The conjectures here are **practically** oriented.
- Finally, we comment on a selection of open problems from several areas including factorization, special polynomials (APN functions, permutation), finite dynamical systems, and relations between integer numbers and polynomials.

- 1 Introduction
- 2 Prescribed Coefficients**
- 3 Low Weight Polynomials
- 4 Potpourri of Open Problems
- 5 Conclusions

# Irreducible Polynomials

A polynomial  $f \in \mathbb{F}_q[x]$  is **irreducible** over  $\mathbb{F}_q$  if  $f = gh$  with  $g, h \in \mathbb{F}_q[x]$  implies that  $g$  or  $h$  is in  $\mathbb{F}_q$ .

The **number** of monic irreducible polynomials of degree  $n$  over  $\mathbb{F}_q$  is

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d} = \frac{q^n}{n} + O(q^{n/2}),$$

where  $\mu : \mathbb{N} \rightarrow \mathbb{N}$  is the Mobius function

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

This is known from 150 years, but if we **prescribed some coefficient to some value**, how many irreducibles are there?

# Irreducibles with Prescribed Coefficients: Existence

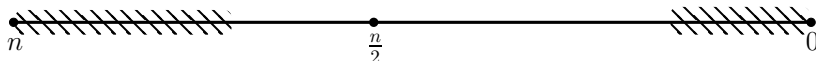
## Existence of irreducibles with prescribed coefficients:


The Hansen-Mullen conjecture (1992) asks for irreducibles over  $\mathbb{F}_q$  with **any** one coefficient **prescribed to a fix value**.

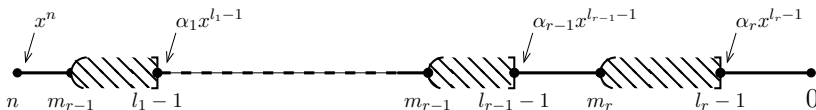
Wan (1997) proved the Hansen-Mullen conjecture using Dirichlet characters and Weil bounds.


There are generalizations for the existence of irreducibles with two coefficients prescribed.

On the other hand, there are also results for up to **half coefficients prescribed** (Hsu 1995) and variants:



 = coefficients prescribed to any value with total size of roughly  $\frac{n}{2} - \log_q n$



 = zero coefficients

However, as we will see later, [experiments show that we could prescribe almost all coefficients](#) and obtain irreducible polynomials!

# Irreducibles with Prescribed Coefficients: Number

The number of irreducibles with prescribed coefficients:

Results so far include: exact results for the number of irreducibles with up to 2 coefficients ( $x^{n-1}$  and  $x^0$ , or  $x^{n-1}$  and  $x^{n-2}$ ) prescribed over any finite field. The techniques are elementary.

Over  $\mathbb{F}_2$  there are also results

- with up to the three most significant coefficients ( $x^{n-1}, x^{n-2}, x^{n-3}$ ) prescribed to any value,
- conjectures for the four most significant coefficients prescribed...
- and nothing else!

# Open Problems

## Open problems:

- (1) prefix some coefficients to some values; prove that there **exist** irreducible polynomials with those coefficients prescribed to those values;
- (2) give **exact (or asymptotic) counting** for irreducibles with prescribed coefficients.

The techniques used so far are from number theory (characters, bounds on character sums) for **existence** results, and from discrete mathematics for the **number** of these polynomials.



# Example of Method of Proof

## Definition

Let  $f \in \mathbb{F}_q[x]$  of positive degree. A **Dirichlet character modulo  $f$**  is a map  $\chi$  from  $\mathbb{F}_q[x]$  to  $\mathbb{C}$  such that for all  $a, b \in \mathbb{F}_q[x]$

$$\chi(a + bf) = \chi(a), \quad \chi(a)\chi(b) = \chi(ab),$$

$$\chi(a) = 0 \quad \text{if and only if } (a, f) \neq 1.$$

The Dirichlet character  $\chi_0$  modulo  $f$  which maps all  $a \in \mathbb{F}_q[x]$  with  $(a, f) = 1$  to 1 is **the trivial** Dirichlet character.

The set of Dirichlet characters modulo  $f$  is a group with product as  $\chi\psi(a) = \chi(a)\psi(a)$  for all  $a \in \mathbb{F}_q[x]$ , identity the trivial Dirichlet character and inverse the conjugate of the Dirichlet character.

## Example of Method of Proof (cont.)

Bounds of certain character sums, often referred to as [Weil bounds](#), are the cornerstones of this area. Let

$$c_n(\chi) = \sum_{d|n} \sum_{P \in \mathbb{I}_d} d\chi(P^{\frac{n}{d}}) \quad \text{and} \quad c'_n(\chi) = \sum_{P \in \mathbb{I}_n} \chi(P).$$

### Proposition

Let  $n$  be a positive integer,  $f \in \mathbb{F}_q[x]$  and  $\chi$  a non-trivial Dirichlet character modulo  $f$ . With  $c_n$  and  $c'_n$  as defined above, we have

$$|c_n(\chi)| \leq (\deg(f) - 1)q^{\frac{n}{2}} \quad \text{and} \quad |c'_n(\chi)| \leq \frac{\deg(f)}{n}q^{\frac{n}{2}}.$$

Furthermore,  $c_n(\chi_0) = q^n$  and  $c'_n(\chi_0) = I_n$ .

The proofs of the above bounds use the Riemann hypothesis for function fields; see for instance Rosen's book (2002).

## Example of Method of Proof (cont.)

Some results follow directly from an asymptotic version of Dirichlet's Theorem for primes in arithmetic progressions in  $\mathbb{F}_q[x]$ .

### Theorem

Let  $f, g \in \mathbb{F}_q[x]$  such that  $(f, g) = 1$  and  $\pi(n; f, g)$  denote the number of polynomials in  $\mathbb{I}_n$  which are congruent to  $g$  modulo  $f$ . Then

$$\left| \pi(n; f, g) - \frac{q^n}{n\Phi(f)} \right| \leq \frac{1}{n}(\deg(f) + 1)q^{\frac{n}{2}}. \quad (1)$$

By setting  $f(x) = x^m$  we obtain the following corollary.

### Corollary

Let  $m, n$  be positive integers and  $\alpha_0, \dots, \alpha_{m-1} \in \mathbb{F}_q$ . If  $m \leq n/2 - \log_q n$ , then *there exists a polynomial in  $\mathbb{I}_n$  with its  $m$  least significant coefficients being  $\alpha_0, \dots, \alpha_{m-1}$ .*

# Primitive Polynomials with Prescribed Coefficients

Results exists for **primitive polynomials**: an irreducible polynomial  $f$  of degree  $n$  is **primitive** if every root of  $f$  is a primitive element.

Hansen-Mullen conjecture for primitive polynomials: primitive polynomials do exist with **any coefficient prescribed** to a value.

This conjecture was proved for  $n \geq 9$  by Cohen (2006), and without restrictions by Cohen and Presern (2007). There are generalizations to few prescribed coefficients but no results for the **number** of primitive polynomials with prescribed coefficients.

**Open problems**: prefix some coefficients to some values; prove that there **exist** (or give the **number** of) primitive polynomials with those coefficients prescribed to those values.

# Primitive Normal Polynomials with Prescribed Coefficients

**Primitive normal polynomials** are polynomials whose roots form a normal basis and are primitive elements. An element  $\alpha$  in  $\mathbb{F}_{q^n}$  is **normal** if  $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$  is a basis of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$ .

The **existence** of primitive normal polynomials was established by Carlitz (1952), for sufficiently large  $q$  and  $n$ , Davenport (1968) for prime fields, and finally for all  $(q, n)$  by Lenstra and Schoof (1987). A proof without the use of a computer was later given Cohen and Huczynska (2003).

Hansen-Mullen (1992) also conjecture that **primitive normal polynomials with one prescribed coefficient** exist for all  $q$  and  $n$ .

Fan and Wang (2009) proved the conjecture for  $n \geq 15$ . There are generalizations for two (norm and trace) and three coefficients.

# Primitive Complete Normal Polynomials

An element  $\alpha$  in  $\mathbb{F}_{q^n}$  is **completely normal** if  $\alpha$  is a normal element of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_{q^d}$ , for every subfield  $\mathbb{F}_{q^d}$  ( $d|n$ ). The minimal polynomial of  $\alpha$  over  $\mathbb{F}_q$  is a **completely normal polynomial**.

Morgan and Mullen (1996) conjecture that for any  $n \geq 2$  and any prime power  $q$  there **exists** a completely normal primitive basis of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$ . This conjecture is still open; major advances have been done by Hachenberger (2001, 2010).

The methods here are **algebraic** and allow derivation of lower bounds, while for primitive normal results hybrid additive and multiplicative characters sums are employed.

- 1 Introduction
- 2 Prescribed Coefficients
- 3 Low Weight Polynomials**
- 4 Potpourri of Open Problems
- 5 Conclusions

# Low Weight Polynomials

A particular important case of **prescribed coefficient** occurs when **most coefficients are set to zero**. The **weight** of a polynomial is the number of nonzero coefficients of a polynomial. Loosely speaking, a polynomial has low weight when “most” coefficients are zero.

This case is relevant in **practice** where we prefer sparse irreducible polynomials, like **trinomials** (polynomials with 3 monomials) or **pentanomials** (polynomials with 5 monomials) over  $\mathbb{F}_2$ , to construct the extension fields. These are for example the recommendations of IEEE and NIST. Among same degree irreducible trinomials or pentanomials we choose following a **lowest lexicographical order**.

However, for example, Scott (2007) shows that the irreducible with the optimal performance for a given implementation does not necessarily follow the lowest lex-order!



# Conjectures

The state of affairs is very poor; these are old conjectures:

- What is the density of  $n$ 's such that there is an irreducible **trinomial** of degree  $n$  over  $\mathbb{F}_2$ ?
- Are there **irreducible pentanomial**s over  $\mathbb{F}_2$  for all  $n$ ?
- Are there **irreducible tetranomial**s over  $\mathbb{F}_q$ ,  $q \geq 3$ , for all  $n$ ?

Experimentally, there are only about 50% of  $n$  with irreducible trinomials of degree  $n$  over  $\mathbb{F}_2$ . But there seems to be a pentanomial for every  $n$ . In Magma **there are tables of trinomials and pentanomials** for the following values of  $q$  and  $n$ :

$q$	$n \leq$	$q$	$n \leq$	$q$	$n \leq$	$q$	$n \leq$
2	120,000	3	50,000	4, 5, 7	2000	$9 \leq q \leq 127$	1000

## Conjectures (cont.)

A **sedimentary polynomial** is a polynomial over  $\mathbb{F}_q$  of the form  $f(x) = x^n + g(x)$  with  $g$  of degree close to  $\log_q n$ .

**Conjecture:** for every positive integer  $n$ , there exists a polynomial  $g$  of degree at most  $\log_q n + 3$  such that  $f(x) = x^n + g(x)$  is irreducible over  $\mathbb{F}_q$ .

These polynomials are used for instance by Coppersmith (1984) to represent elements in  $\mathbb{F}_{2^n}$  in a subexponential algorithm for discrete logarithm computations in finite fields.

# Discriminants

**Definition.** Let  $f(x) = a_0(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \in \mathbb{K}[x]$ , where  $\mathbb{K}$  is a field and  $\alpha_1, \alpha_2, \dots, \alpha_n$  are the roots of  $f$  in its splitting field. The **discriminant** of  $f$  is defined as

$$D(f) = a_0^{2n-2} \prod_{0 \leq i < j \leq n-1} (\alpha_i - \alpha_j)^2.$$

Since  $D(f)$  is a symmetric product of the roots of  $f$ , it can be shown that  $D(f) \in \mathbb{K}$ .

If  $f$  has a repeated root, then  $\alpha_i = \alpha_j$  for some  $i \neq j$  and  $D(f) = 0$ .

**Examples.** If  $n = 2$ , then  $D(ax^2 + bx + c) = b^2 - 4ac$ . If  $n = 3$ ,  $D(ax^3 + bx^2 + cx + d) = b^2c^2 - 4b^3d - 4ac^3 - 27a^2d^2 + 18abcd$ .

# Pellet-Stickelberger Theorem

**Theorem.** Let  $p$  be an odd prime and suppose that  $f$  is a monic polynomial of degree  $n$  with integral coefficients in a  $p$ -adic field  $\mathbb{F}$ . Let  $\bar{f}$  be the result of reducing the coefficients of  $f \pmod{p}$ . Assume further that  $\bar{f}$  has no repeated roots. If  $\bar{f}$  has  $r$  irreducible factors over the residue class field, then  $r \equiv n \pmod{2}$  if and only if  $D(f)$  is a square in  $\mathbb{F}$ .

Swan shows how to apply this idea when the characteristic is 2.

**Corollary.** Let  $g$  be a polynomial of degree  $n$  over  $\mathbb{F}_2$  with  $D(g) \neq 0$  and let  $f$  be a monic polynomial over the 2-adic integers such that  $g$  is the reduction of  $f \pmod{2}$ . Furthermore, let  $r$  be the number of irreducible factors of  $g$  over  $\mathbb{F}_2$ . Then  $r \equiv n \pmod{2}$  if and only if  $D(f) \equiv 1 \pmod{8}$ .

# Swan Theorem

**Theorem.** Let  $n > k > 0$ . Assume precisely one of  $n, k$  is odd. Then if  $r$  is *the number of irreducible factors* of  $f(x) = x^n + x^k + 1 \in \mathbb{F}_2[x]$ , then  $r$  *is even* in the following cases:

- $n$  even,  $k$  odd,  $n \neq 2k$  and  $nk/2 \equiv 0, 1 \pmod{4}$ ;
- $n$  odd,  $k$  even,  $k \nmid 2n$  and  $n \equiv 3, 5 \pmod{8}$ ;
- $n$  odd,  $k$  even,  $k \mid 2n$  and  $n \equiv 1, 7 \pmod{8}$ .

In other cases  $f$  has an odd number of factors.

The case where  $n$  and  $k$  are both odd can be covered by making use of the fact that the reverse of  $f$  has the same number of irreducible factors. If both  $n$  and  $k$  are even the trinomial is a square and has an even number of irreducible factors.

**Corollary.** There is no irreducible trinomial over  $\mathbb{F}_2$  with degree a multiple of 8.

# Reducibility of Fewnomials

Swan (1962) characterizes the parity of the number of irreducible factors of a trinomial over  $\mathbb{F}_2$  relating the discriminant of the trinomial to the parity of the number of factors (Stickelberger): if the number of irreducible factors of a polynomial is even, the trinomial is **reducible**.

**Main problem:** the calculation of the discriminant of the polynomial is hard when the polynomial has even moderate number of terms.

By now, over  $\mathbb{F}_2$ , we know the reducibility of few pentanomials but not if they exist for all degrees. Over  $\mathbb{F}_q$ , we know when binomials are reducible; we also have partial results for trinomials and tetranomials, as well as for some very special type of polynomials.

# Applications of Low Weight Polynomials

## (1) Orthogonal arrays and covering arrays

Consider an LFSR sequence generated by a primitive polynomial  $f$  over a finite field. The set of its subintervals is a linear code whose dual code is formed by all polynomials divisible by  $f$ .

Since the minimum weight of dual codes is directly related to the strength of the corresponding orthogonal arrays, one can produce orthogonal arrays by studying the divisibility of polynomials.

Munemasa (1998) uses trinomials over  $\mathbb{F}_2$  to construct orthogonal arrays of guaranteed strength 2 (and almost strength 3). That result was extended by Dewar et al. (2007) to construct orthogonal arrays of guaranteed strength 3 by considering divisibility of trinomials by pentanomials over  $\mathbb{F}_2$ . Raaphorst, Moura and Stevens (2014) construct covering arrays using LFSRs.

## (2) Divisibility of low weight polynomials

To obtain orthogonal arrays of larger strength  $t$  (equivalently dual codes of minimum weight  $t + 1$ ), we need conditions on when a low weight polynomial divides another (low)  $t$ -weight polynomial. At this moment we only know conditions for trinomials and pentanomials over  $\mathbb{F}_2$ , and some similar cases over  $\mathbb{F}_3$ .

Low weight multiples of a public polynomial compromise the private key for the *TCHo cryptosystem* and its security therefore rests on the difficulty of finding low weight multiples (Aumasson et al., 2007; Hermann and Leander, 2009).

**Open Problem:** study the divisibility of low weight polynomials over finite fields.



### (3) The great trinomial hunt

Brent and Zimmerman, Notices of the AMS, Feb. 2011

**Facts:** (a) Let  $P_r(x) = x^{2^r} - x \in \mathbb{F}_2[x]$ , then  $P_r$  is the product of all irreducible polynomials over  $\mathbb{F}_2$  of degree  $d$  dividing  $r$ .

(b) If  $r$  is an odd prime, then a polynomial  $P \in \mathbb{F}_2[x]$  with degree  $r$  is irreducible if and only if  $x^{2^r} \equiv x \pmod{P}$ .

(c) If  $r$  is a Mersenne exponent (that is,  $2^r - 1$  is prime), then all irreducibles of degree  $r$  are primitive.

(d) Using [repeated squaring](#) we have a simple check for primitivity of polynomials of degree  $r$ , where  $r$  is a Mersenne exponent.

The primitive trinomial over  $\mathbb{F}_2$  with largest known degree is

$$x^{43112609} + x^{3569337} + 1$$

To find such trinomials requires an intense amount of sieving.  
A crucial test is the application of [Stickelberger/Swan's theorem](#).

- 1 Introduction
- 2 Prescribed Coefficients
- 3 Low Weight Polynomials
- 4 Potpourri of Open Problems**
- 5 Conclusions

# Factorization of Polynomials

**The problem:** given a monic univariate polynomial  $f \in \mathbb{F}_q[x]$ , find the complete factorization  $f = f_1^{e_1} \cdots f_r^{e_r}$ , where the  $f_i$ 's are monic distinct irreducible polynomials and  $e_i > 0$ ,  $1 \leq i \leq r$ .

**Standard method:**

- ERF Elimination of repeated factors** replaces a polynomial by a squarefree one which contains all the irreducible factors of the original polynomial with exponents reduced to 1.
- DDF Distinct-degree factorization** splits a squarefree polynomial into a product of polynomials whose irreducible factors have all the same degree.
- EDF Equal-degree factorization** factors a polynomial whose irreducible factors have the same degree.

# Factorization of Polynomials (cont.)

Practical versions use a **probabilistic algorithm** for EDF.

**Open Problem (Theoretical):** find a polynomial time **deterministic** algorithm for factoring polynomials over finite fields.

**Techniques so far:** purely algebraic.

Fast practical versions use **interval partitions** for DDF.

**Open Problem (Practical):** find the **best interval partition** for factoring a random polynomial over a finite field.

**Techniques so far:** analytic combinatorics.

# Permutation Polynomials over Finite Fields

A **permutation polynomial** (PP) over a finite field is a bijection which maps the elements of  $\mathbb{F}_q$  onto itself.

There have been massive amount of work on PPs since the 19th century. Many results have appeared on the last 20 years due to the cryptographic applications of PPs.

However, similar questions as before are still not fully answered:

- find PPs with prescribed coefficients,
- give existence of PPs,
- count PPs, etc.

The **value set** of a polynomial has also been studied but **value sets in subfields** are far less known (only for monomials, linearized polynomials and some Dickson polynomials).

# Coding Theory and Polynomials

Polynomials have been largely used in coding theory (minimal polynomials and BCH codes, linear codes as factors of  $x^n - 1$ , Reed-Solomon codes, weight enumerators, etc).

Recently permutation polynomials have been used in [turbo codes](#) for interleavers. When used as interleavers, the cycle structure of the permutation polynomials is required. For several polynomials only incomplete information on the cycles structure is known.

**Open Problem:** Advance the study of the cycle decomposition of permutation polynomials, and use permutation polynomials in turbo codes.

# Maximum Rank Distance Codes and Polynomials

Linearized polynomials are used in subspace codes and are related to rank-metric codes. Subspace polynomials are a special type of linearized polynomials (squarefree, splitting completely in  $\mathbb{F}_{q^n}$ ) that provide an efficient method of representing subspaces; see Ben-Sasson, Etzion, Gabizon and Raviv preprint.

**Open Problem (Sheekey):** Find all pairs of linearized polynomials  $L, M$  over  $\mathbb{F}_{q^n}$  such that  $N(L(x)) \neq N(M(x))$  for all  $x$ , where  $N$  is the field norm to some field between  $\mathbb{F}_q$  and  $\mathbb{F}_{q^n}$ . In other words, the value sets of  $N(L(x))$  and  $N(M(x))$  are disjoint.

Any such pair would give a new MRD code for all parameters (including a new semifield). The case where  $L$  and  $M$  are monomials is Sheekey's construction presented on Monday.

Sheekey claims that he has some computational examples...

# Relations Between Integers and Polynomials

Similar results for the decomposition of integers into primes can be derived for the decomposition of polynomials over finite fields into irreducibles. For example studies on the

- number of irreducible factors of a polynomial (number of primes of an integer);
- largest/smallest degree irreducible factor (largest/smallest prime);
- irreducibles (primes) in arithmetic progression; and so on.

Techniques so far: analytic combinatorics.



## Relations Between Integers and Polynomials (cont.)

Also some classical number theoretic problems have been translated to polynomials. For example, the [twin primes conjecture](#) has been proved for all finite fields of order bigger than 2.

**Open Problem:** Prove the twin prime polynomial conjecture in  $\mathbb{F}_2$ .

Generalizations (to more than 2 irreducibles, or to irreducible not as close as possible) have not been proved yet.

There have been some results about [additive](#) properties for polynomials related to [Goldbach conjecture](#) and their generalizations (sum of 3 irreducibles); see Effinger et al. (2005).

Several recent results in number theory have not been translated into polynomials over finite fields yet, including studies of divisors, irreducibles in small gaps, digital functions for polynomials; etc.

# Iterations of functions over finite fields

In general, let  $\mathcal{F}_n$  be the set of functions (“mappings”) from the set  $[1..n]$  to itself. With any  $\varphi \in \mathcal{F}_n$  there is associated a **functional graph** on  $n$  nodes, with a directed edge from vertex  $u$  to vertex  $v$  if  $\varphi(u) = v$ . We are interested here in functions over finite fields.

Functional graphs of mappings are sets of connected components; the components are directed cycles of nodes; and each of those nodes is the root of a tree.

The dynamics of iterations of polynomials and rational functions over finite fields have attracted much attention in recent years, in part due to their applications in cryptography and integer factorization methods like **Pollard rho algorithm**.

## Description of Pollard's method

- Iteration function:  $f(x) = x^2 + a$ .
- Rho path of a random element  $x_0$ :

$$x_k = f(x_{k-1}), \text{ for } k \geq 1.$$

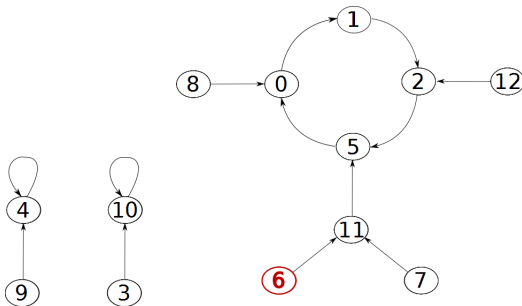


Figure : Rho path of  $x_0 = 6$  under  $f(x) = x^2 + 1 \in \mathbb{F}_{13}[x]$ .



## Description of Pollard's method

- Iteration function:  $f(x) = x^2 + a$ .
- Rho path of a random element  $x_0$ :

$$x_k = f(x_{k-1}), \text{ for } k \geq 1.$$

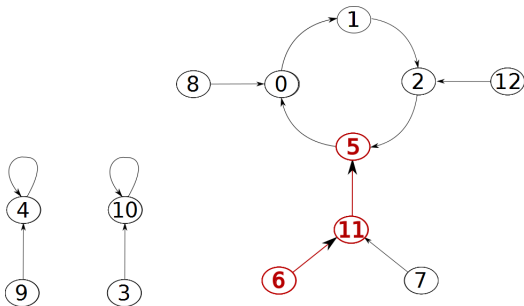


Figure : Rho path of  $x_0 = 6$  under  $f(x) = x^2 + 1 \in \mathbb{F}_{13}[x]$ .

## Description of Pollard's method

- Iteration function:  $f(x) = x^2 + a$ .
- **Rho path** of a random element  $x_0$ :

$$x_k = f(x_{k-1}), \text{ for } k \geq 1.$$

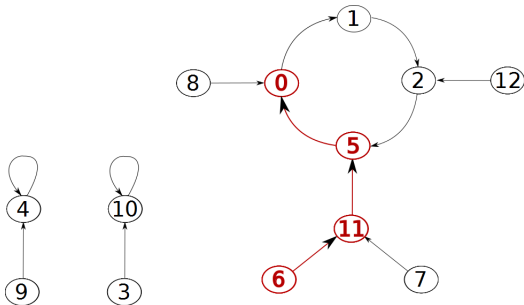


Figure : Rho path of  $x_0 = 6$  under  $f(x) = x^2 + 1 \in \mathbb{F}_{13}[x]$ .

# Description of Pollard's method

- Iteration function:  $f(x) = x^2 + a$ .
- Rho path** of a random element  $x_0$ :

$$x_k = f(x_{k-1}), \text{ for } k \geq 1.$$

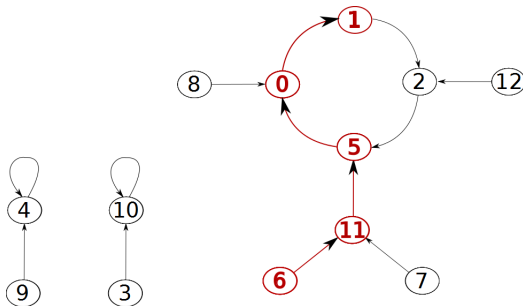


Figure : Rho path of  $x_0 = 6$  under  $f(x) = x^2 + 1 \in \mathbb{F}_{13}[x]$ .

## Description of Pollard's method

- Iteration function:  $f(x) = x^2 + a$ .
- Rho path of a random element  $x_0$ :

$$x_k = f(x_{k-1}), \text{ for } k \geq 1.$$

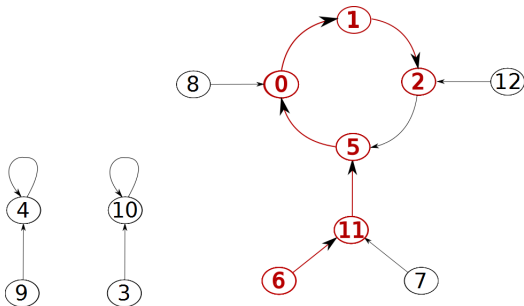


Figure : Rho path of  $x_0 = 6$  under  $f(x) = x^2 + 1 \in \mathbb{F}_{13}[x]$ .



# Description of Pollard's method

- Iteration function:  $f(x) = x^2 + a$ .
- Rho path** of a random element  $x_0$ :

$$x_k = f(x_{k-1}), \text{ for } k \geq 1.$$

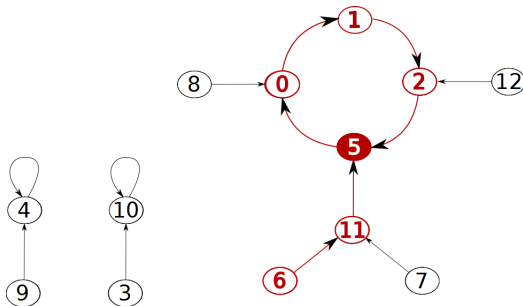


Figure : Rho path of  $x_0 = 6$  under  $f(x) = x^2 + 1 \in \mathbb{F}_{13}[x]$ .

## Description of Pollard's method

- Iteration function:  $f(x) = x^2 + a$ .
- **Rho path** of a random element  $x_0$ :  $x_k = f(x_{k-1})$ , for  $k \geq 1$ .

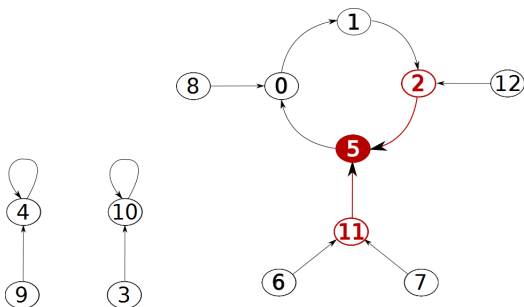


Figure : Rho path of  $x_0 = 6$  under  $f(x) = x^2 + 1 \in \mathbb{F}_{13}[x]$ .

- **Heuristic assumption:** behaviour similar to a random mapping.

# Random mappings and Pollard method

Used in (brief list):

- E. Teske, On random walks for Pollard's Rho Method, Mathematics of Computation, 2001.
- J. Bos, T. Kleinjung, A. K. Lenstra, On the use of the negation map in Pollard rho method, ANTS 2010.
- D.J. Bernstein, T. Lange, Two grumpy giants and a baby, ANTS 2012.

Many parameters defined on mappings; focus on **rho length**.

It is not clear how “close” particular polynomials and rational functions are to random mappings.

# Topics of interest in finite dynamics

Iterations of functions over finite fields have centered on:

- period and preperiod;
- (average) rho length;
- number of connected components;
- length of cycles (largest, smallest, average);
- number of fix points and conditions to be a permutation;
- isomorphic graphs; and so on.

Iterations of some functions have **strong symmetries** that can be mathematically explained.

# Results

- (T.Rogers) Dynamics of  $x \mapsto x^2$ .

T.Rogers. "The graph of the square mapping on the prime fields". Disc.Math 148, 317-324, 1996.

- (A.Peinado et al.) Dynamics of  $x \mapsto x^2 + c$ .

A.Peinado, F.Montoya, J.Muñoz, A.Yuste. "Maximal periods of  $x^2 + c$  in  $\mathbb{F}_q$ ". LNCS 2227, 219-228, 2001.

- (T.Vasiga, J.Shallit) Dynamics of  $x \mapsto x^2 - 2$ .

T.Vasiga, J.Shallit. "On the iteration of certain quadratic maps over  $\text{GF}(p)$ ". Disc.Math 227, 219-240, 2004.

- (S.Ugolini) Dynamics of  $x \mapsto x + x^{-1}$  and  $x \mapsto x^d + x^{-d}$ .

S.Ugolini. "Graphs associated with the map  $x \mapsto x + x^{-1}$  in finite fields of characteristic three and five". Journal of Number Theory 133, 1207-1228, 2013.

# Results (cont.)

- (T.Gassert) [Dynamics of Chebyshev polynomials](#).  
T.Gassert. “Chebyshev action on finite fields”. Disc.Math 315-316, 83-94, 2014.
- (Panario and Qureshi) [Dynamics of Rédei functions](#); submitted.
- (Martins and Panario) [Dynamics of cubic, quartic and “general” polynomials](#); submitted.

Algebraic dynamical systems generated by [several rational functions on many variables](#) over finite fields have also been considered; see Igor Shparlinski’s survey in Section 10.5 of [G.Mullen, D.Panario “Handbook of Finite Fields”. CRC Press, 2013.](#)

# Special Polynomials over Finite Fields

Let  $G_1$  and  $G_2$  be finite Abelian groups of the same cardinality and  $f : G_1 \rightarrow G_2$ . We say that  $f$  is a **perfect non-linear (PN) function** if

$$\Delta_{f,a}(x) = f(x+a) - f(x) = b$$

has exactly one solution for all  $a \neq 0 \in G_1$  and all  $b \in G_2$ .

PN functions provide optimal resistance to linear and differential cryptographic attacks. However, perfect non-linear **permutations** do not exist. Furthermore, PN functions **cannot exist in finite fields of characteristic 2** (the most important for implementations).

They were introduced as **planar functions** by Dembowski-Ostrom (1968); they are also known as **bent functions**.

# APN Functions

An alternate definition for best-possible differential structure:

Let  $G_1$  and  $G_2$  be finite Abelian groups of the same cardinality and  $f : G_1 \rightarrow G_2$ . We say that  $f$  is an **almost perfect non-linear function** if

$$\Delta_{f,a}(x) = f(x + a) - f(x) = b$$

has at most two solutions for all  $a \neq 0 \in G_1$  and all  $b \in G_2$ .

**Example.** The **inverse function**  $f : x \mapsto x^{2^n-2}$  in  $\mathbb{F}_{2^n}$  is **APN** if and only if  $n$  is odd.

**Remark:** This function is used in **AES** but  $n = 8$ !

If  $n$  is even, then  $\Delta_{f,a}$  is close to APN (it is **differential 4-uniform**).



# APN Permutations

In most applications, candidate functions for use in symmetric key cryptosystems must be permutations. Furthermore, for implementation purposes, functions over  $\mathbb{F}_{2^e}$  with  $e$  even are preferred. There are no PN permutations in these fields. Hence, combining these criteria, the most desirable candidate functions are

APN permutations over  $\mathbb{F}_{2^e}$  where  $e$  is even.

**Open Problem:** Find APN permutations over  $\mathbb{F}_{2^e}$ , when  $e$  is even.

Currently, there is **only one** known **APN permutation over  $\mathbb{F}_{2^e}$ , when  $e$  is even**. This function for  $\mathbb{F}_{2^6}$  was given by Dillon (2009).

- 1 Introduction
- 2 Prescribed Coefficients
- 3 Low Weight Polynomials
- 4 Potpourri of Open Problems
- 5 Conclusions**

Want to read more (shameless advertisement coming)?

Want to read more (shameless advertisement coming)?

