Polynomials over Finite Fields: Algorithms and Randomness

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

AofA'10, July 2010

Introduction

Let q be a prime power. In this talk, we consider monic univariate polynomials over a finite field $\mathbb{F}_q$.

We review a methodology from analytic combinatorics that allows:

- counting polynomials;
- random polynomials properties in algorithms;
- average-case analysis of algorithms; and
- decomposition of random polynomials in its irreducible factors.

It is well-known that a polynomial of degree n over $\mathbb{F}_q$ is irreducible with probability close to $1/n$.

Can we say something more like we can for the decomposition of integers into primes?

- How many irreducible factors a random polynomial has?
- How often will it be squarefree or k-free?
- What is the expected largest (smallest) degree among its irreducible factors?
- How is the degree distribution among its irreducible factors?
- How often a polynomial is m-smooth (all irreducible factors of degree $\leq m$)?
- How often two polynomials are m-smooth and coprime?
- How is the degree distribution among the irreducible factors of the gcd of several polynomials?
- What is the expected degree of the splitting field of a random polynomial?

and so on.

Algebraic algorithms that deal with polynomials over finite fields can often be analyzed counting polynomials with particular properties. Examples:

- irreducibility tests for polynomials,
- polynomial factorization,
- gcd computations, and
- discrete logarithm problem.

The most important characteristics of these algorithms can be treated systematically by a methodology based on generating functions and asymptotic analysis: analytic combinatorics.

This methodology relates finite fields and their applications to combinatorics and number theory.

However, we also briefly comment on other techniques that have been used in this area:

- Arratia, Barbour and Tavaré probabilistic approach;
- polynomials coming from random matrices (cycle index);
- expected polynomial splitting degree (Erdös-Turán order of a random permutation).

Finally, we provide some open problems from actual research areas in finite fields where univariate polynomials play a central role but no technique from probabilistic and analytic combinatorics have been successfully employed so far.

General framework

Let I_n be the number of monic irreducible polynomials in $\mathbb{F}_q$. The generating functions of monic irreducible polynomials and monic polynomials are

$$I(z) = \sum_{n\geq 1} I_n z^n, \qquad \text{and}$$

$$P(z) = \prod_{k\geq 1} (1 + z^k + z^{2k} + \cdots)^{I_k} = \prod_{k\geq 1} (1 - z^k)^{-I_k}.$$

Since $[z^n]P(z)$ is q^n, we have $P(z) = (1 - qz)^{-1}$, and these relations implicitly determine I_n

$$I_n = \frac{1}{n} \sum_{k|n} \mu(k) q^{n/k}.$$

The proportion of irreducible polynomials of degree n over $\mathbb{F}_q$ is close to $1/n$.

As usual, we consider bivariate generating functions to take care of critical parameters of the problems we are interested in. Asymptotic analysis is then used to extract coefficient information.

Example: number of irreducible factors. Let

$$P(u,z) = \prod_{j\geq 1}(1 + uz^j + u^2 z^{2j} + \cdots)^{I_j} = \prod_{j\geq 1}(1 - uz^j)^{-I_j}$$

where $[u^k z^n]P(u,z)$ is the number of polynomials of degree n with k irreducible factors.

Differentiating two times with respect to the parameter, putting $u = 1$ and asymptotic analysis gives expectation $\log n$ and standard deviation $\sqrt{\log n}$.

Flajolet and Soria (1990) prove that the number of irreducible factors has a Gaussian distribution.

Theorem. Let Ω_n be a random variable counting the number of irreducible factors of a random polynomial of degree n over $\mathbb{F}_q$, where each factor is counted with its order of multiplicity.

1. The mean value of Ω_n is asymptotic to $\log n$ (Berlekamp; Knuth).
2. The variance of Ω_n is asymptotic to $\log n$ (Knopfmacher and Knopfmacher; Flajolet and Soria).
3. For any two real constants $\lambda < \mu$,

$$\Pr\left\{\log n + \lambda\sqrt{\log n} < \Omega_n < \log n + \mu\sqrt{\log n}\right\} \to \frac{1}{\sqrt{2\pi}}\int_\lambda^\mu e^{-t^2/2}dt.$$

4. The distribution of Ω_n admits exponential tails (Flajolet and Soria).
5. A local limit theorem holds (Gao and Richmond).
6. The behaviour of $\Pr\{\Omega_n = m\}$ for all m is known (Cohen; Car; Hwang).

A general factorization algorithm

Folklore Algorithm

- 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.

Distinct-degree factorization (DDF)

Theorem. *For $i \geq 1$, the polynomial $x^{q^i} - x \in \mathbb{F}_q[x]$ is the product of all monic irreducible polynomials in $\mathbb{F}_q[x]$ whose degree divides i.*

```
procedure DDF(a : polynomial); [a squarefree]
  n := deg(a); g := a; h := x;
  for k := 1 to n do
1.      h := h^q mod g;
2.      b[k] := gcd(h-x,g);
3.      g := g/b[k]; [a w/o factors deg<=k]
4.      if b[k] <> 1 then h := h mod g fi;
  od;
  return(b[1].b[2]...b[n]);
end;
```

The computation in step 1 is done by means of the classical *repeated squaring* method. Let $\nu(q)$ be the number of ones in the binary representation of q. The number of products needed to compute h^q mod g by this method is

$$\lambda(q) = \lfloor \log_2 q \rfloor + \nu(q) - 1.$$

Let $\tau_1 n^2$ and $\tau_2 n^2$ be the costs of computing the product and the gcd of two polynomials of degree at most n, respectively (classical arithmetic).

Theorem. (Flajolet, Gourdon and Panario, 2001)
The expected cost of the basic DDF phase satisfies, as $n \to \infty$,

$$\overline{DDF}_n \sim \frac{5}{12} \left(\lambda(q)\tau_1 + \tau_2\right) n^3.$$

Proof (Sketch). The cost of the basic DDF is $\sum_{j=1}^{4} C_j$, where C_j is the cost of line j. Let $\overline{C_j}$ be the expectation of C_j.

Since the mean number of factors of f is $O(\log n)$, $\overline{C_3} + \overline{C_4} = O(n^2 \log n)$.

Let d_k denote the degree of polynomial g when the kth iteration starts; the parameter d_k is also the sum of the degrees of the distinct factors of f with degree $\geq k$. The quantity $C_1 + C_2$ is equal to $(\lambda(q)\tau_1 + \tau_2) \sum_{k \geq 1} d_k^2$.

The bivariate generating function associated with d_k is

$$P_k(z,u) = \prod_{j<k} \left(\frac{1}{1-z^j} \right)^{I_j} \prod_{j \geq k} \left(1 + u^j \frac{z^j}{1-z^j} \right)^{I_j} .$$

The expected value of $C = \sum_{k=1}^{n} d_k^2$ is then given by $\overline{C} = \frac{1}{q^n}[z^n]Q(z)$, where

$$Q(z) = \sum_{k=1}^{n} \left(\frac{\partial^2 P_k(z,u)}{\partial u^2} + \frac{\partial P_k(z,u)}{\partial u} \right)\bigg|_{u=1} .$$

Singularity analysis entails that $[z^n]Q(z) \sim \frac{5}{12} q^n\, n^3$. □

Flajolet and Odlyzko's singularity analysis (1990): If $f(z)$ near its dominant singular at $z = 1/q$ behaves like

$$f(z) = \frac{1}{(1-qz)^{\alpha}} \left(\log \frac{1}{1-qz} \right)^{k} (1 + o(1))$$

then, for $\alpha \neq 0, -1, -2, \ldots$, we have

$$[z^n]f(z) = q^n \frac{n^{\alpha-1}}{\Gamma(\alpha)} (\log n)^{k} (1 + o(1)).$$

Irreducibility tests

Take polynomials at random and test them for irreducibility. The proportion of irreducible polynomials of degree n is close to $1/n$.

We need an irreducibility test!

Theorem. *For $i \geq 1$, the polynomial $x^{q^i} - x \in \mathbb{F}_q[x]$ is the product of all monic irreducible polynomials in $\mathbb{F}_q[x]$ whose degree divides i.*

The algorithm tests the irreducibility of a polynomial by searching for irreducible factors degree by degree.

It stops when the smallest degree irreducible factor is found.

Technical issue: probability that a random polynomial of degree n contains no irreducible factors of degree up to certain value m (the so-called m-rough polynomials).

Panario and Richmond (1998) give the probability that a random polynomial be m-rough, $1 \leq m \leq n$, in terms of the Buchstab function when $m \to \infty$, and singularity analysis when m is fixed; see also Car (1987).

The Buchstab function, $\omega(u)$, is the unique continuous solution of the difference-differential equation

$$\begin{aligned} u\omega(u) &= 1 & 1 \leq u \leq 2, \\ (u\omega(u))' &= \omega(u-1) & u > 2. \end{aligned}$$

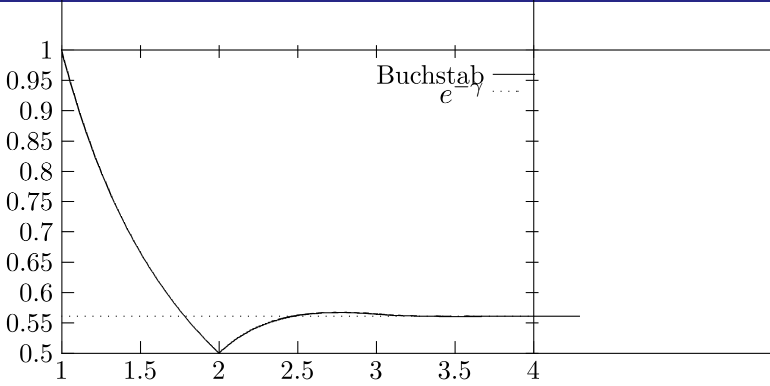

Figure: The relation between the Buchstab function and $e^{-\gamma}$ in the interval $[1, 4]$.

Odlyzko (1984) and then Gourdon (1996) studied m-smooth polynomials and the largest irreducible factors in terms of the Dickman function (that also appears in Quickselect studies).

A simplified picture of a random polynomial:

- it is irreducible with probability tending to 0 as $n \to \infty$;
- it is k-free with probability $1 - 1/q^{k-1}$;
- it has $\log n$ irreducible factors (concentrated);
- it has a factor of degree r with probability $1/r$ (not concent.);
- it has no linear factors with asymptotic probability ranging from 0.25 to $0.3678\ldots$ as q grows;
- it has irreducible factors of distinct degree with asymptotic probability between $0.6656\ldots$ and $e^{-\gamma} = 0.5614\ldots$ as $q \to \infty$;

- it has $c_k n$ expected kth largest degree irreducible factor, where $c_1 = 0.62433\ldots$, $c_2 = 0.20958\ldots$, $c_3 = 0.08831\ldots$ and the remaining irreducible factors have small degree (here c_1 is Dickman-Golomb's constant);
- it has expected first and second smallest degree factors asymptotic to $e^{-\gamma}\log n$ and $e^{-\gamma}\log^2 n/2$ (not concentrated);
- the limiting distribution of $Z_t(\vec{n})$ is a geometric distribution, and the distributions of $Z_d(\vec{n})$ and $Z_r(\vec{n})$ are very close to Poisson distributions when $q \geq 64$;

and so on.

Other results

We briefly comment on other techniques used in this area.

(1) Probabilistic approach.

Arratia, Barbour and Tavaré study the joint degree distribution of the irreducible factors from a probabilistic point of view (see: "Logarithmic Combinatorial Structures: a Probabilistic Approach", 2003).

Let $C_j^{(n)}$, $1 \leq j \leq n$, be the number of irreducible factors of degree j in a polynomial of degree n. They consider the discrete dependent nonnegative integer-valued random process $C^{(n)} = (C_1^{(n)}, \ldots, C_n^{(n)})$ satisfying

$$\sum_j jC_j^{(n)} = n, \quad n = 1, 2, \ldots.$$

The joint distribution satisfies the conditioning relation:

$$\mathcal{L}(C_1^{(n)}, \dots, C_n^{(n)}) = \mathcal{L}(Z_1, \dots, Z_n | \sum_j jZ_j = n),$$

where the random variables $(Z_j, j \geq 1)$ are independent and take nonnegative integer values.

These Z_j random variables also satisfy the following logarithmic condition for some $\theta > 0$:

$$i\mathbb{P}[Z_i = 1] \to \theta, \quad i\mathbb{E}Z_i \to \theta, \qquad \text{as } i \to \infty.$$

This applies to other structures, exactly as Flajolet and Soria (1990) exp-log class.

Open problem: can a similar approach be applied to alg-log structures?

(2) Polynomials from random matrices over finite fields.

Generating functions have been used in the enumeration of groups of random matrices over finite fields (see: Memoirs of the AMS, vol. 830, by Fulman, Neumann and Praeger, 2005).

The decomposition of the characteristic polynomial of a random matrix over finite fields has been considered by Stong (1988).

Hansen and Schmutz (1993) show that, ignoring factors of small degree, the decomposition into irreducibles of the characteristic polynomial of a random matrix over finite fields behaves like the decomposition into irreducibles of a random polynomial over $\mathbb{F}_q$. Hence, previous results on random polynomials can be used.

We have that as $q \to \infty$ random polynomials over $\mathbb{F}_q$ behave like permutations, giving further connections in this asymptotic case.

(3) Other results

Dixon and Panario (2004) study the expected degree of the splitting field of a random polynomial over a finite field. This is closely related to the order of a permutation studied by Goh and Schmutz (1991) and Stong (1998), and to the normal distribution of the logarithm of the order of a permutation studied by Erdös and Turán (1967).

Open problems

We provide some open problems from actual research areas in finite fields where univariate polynomials play a central role but no technique from probabilistic and analytic combinatorics have been successfully employed so far.

(1) Irreducibles with prescribed coefficients

(1.1) Reducibility of fewnomials

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

Consequence of Swan's result: There are no irreducible trinomials over $\mathbb{F}_2$ with degree a multiple of 8.

In practice, we prefer sparse irreducible polynomials, like trinomials or pentanomials over $\mathbb{F}_2$. However, we do not even know the density of n's such that there is an irreducible trinomial of degree n over $\mathbb{F}_2$!.

The technique of proof relates the discriminant of the trinomial to the parity of the number of factors (Stickelberger 1897).
Main problem: the calculation of the discriminant of the polynomial is hard when the polynomial has even moderate number of terms.

By now, over $\mathbb{F}_q$, we know when binomials are reducible, and partial results for trinomials and tetranomials. The reducibility of few pentanomials is also known.

(1.2) Existence of irreducibles with prescribed coefficients

There are results for the existence of irreducibles with prescribed coefficients. The Hansen-Mullen conjecture (1992) asks for irreducibles over $\mathbb{F}_q$ with any coefficient prescribed.

Wan (1997) proved the Hansen-Mullen conjecture. By now there are results for the existence of irreducibles with up to half coefficients prescribed (Hsu 1995) and variants. However, experiments show that we could prescribe almost all coefficients and obtain irreducible polynomials!

Techniques used so far: basic number theory (discriminants, characters, bounds on character sums).

Open problem: prefix some coefficients to some values; prove that there exist irreducible polynomials with those coefficients prescribed to those values.

(1.3) 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}) over any finite field. Over $\mathbb{F}_2$ there are also results with up to 3 most significant coefficients prescribed to any value... nothing else!

Open problem: give exact (asymptotic?) counting for irreducibles with prescribed coefficients.

(2) Relations between integers and polynomials

We showed that classical results from the decomposition of integers into primes can be derived for the decomposition of polynomials over finite fields into irreducibles.

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. There have been some results about additive properties for polynomials related to Goldbach conjecture and their generalizations (sum of 3 irreducibles). See: Effinger, Hicks and Mullen, The Mathematical Intelligencer (2005).

New relations between integers and polynomials?
Several recent results in number theory have not been translated into polynomials, including studies of divisors and shifted divisors, irreducibles in small gaps, digital functions for polynomials (equidistributions of digital sums); etc.

(3) Other areas

(3.1) 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. They can be defined over other rings and fields. For example Nöbauer in the 80's characterized PPs on several variables and over residue class rings.

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

(3.2) Multivariate polynomials over finite fields

We did not treat multivariate polynomials over finite fields at all. There are some results about counting those polynomials (Carlitz, Cohen, etc) or more recently by von zur Gathen, Viola and Ziegler), but no analysis of algorithms yet.

Recent results. Green-Tao uses Gowers norms to derive uniform distribution properties for polynomials in several variables and bounded degree over a fixed finite field of prime order.