Some results on counting roots of polynomials and the Sylvester resultant.

Michael Monagan and Baris Tuncer, Department of Mathematics, Simon Fraser University.
mmonagan@cecm.sfu.ca and ytuncer@sfu.ca

Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements and let $\mathbb{Z}_n$ denote the ring of integers modulo n. Let $\mathrm{E}[X]$ denote the expected value of a random variable X and let $\mathrm{Var}[X]$ denote the variance of X.

Let f be a polynomial in $\mathbb{F}_q[x]$ of a given degree $d > 0$ and let X be the number of distinct roots of f. Schmidt proves in Ch. 4 of [5] that $\mathrm{E}[X] = 1$ and for $d > 1$, $\mathrm{Var}[X] = 1 - 1/q$. This result has been generalized by A. Knopfmacher and J. Knopfmacher in [2] who count distinct irreducible factors of a given degree of f. The two main results presented in this poster are Theorems 1 and 2.

Motivation

Our motivation comes from the following problems in computer algebra. Let A, B be polynomials in $\mathbb{Z}[x_0, x_1, \ldots, x_n]$ and $G = \gcd(A, B)$. Thus $A = G\widehat{A}$ and $B = G\widehat{B}$ for some polynomials $\widehat{A}$ and $\widehat{B}$ called the cofactors of A and B. Modular GCD algorithms compute G modulo a sequence of primes $p_1, p_2, p_3, \ldots$ and recover the integer coefficients of G using Chinese remaindering. The fastest algorithms for computing G modulo a prime p interpolate G from univariate images. Maple, Magma and Mathematica all currently use Zippel's algorithm (see [6, 1]).

Let $G = \sum_{i=0}^{d} c_i(x_1, \ldots, x_n)x_0^i$. Zippel's algorithm picks a prime p and picks points $\alpha_j \in \mathbb{F}_p^n$, and computes monic univariate images

$$g_j = \gcd(A(x_0, \alpha_j), B(x_0, \alpha_j)) \bmod p,$$

of G, scales them (details omitted), then interpolates $c_i(x_1, \ldots, x_n)$, the coefficients of G, from the coefficients of these scaled images.
But what if $\gcd(\widehat{A}(x_0, \alpha_j), \widehat{B}(x_0, \alpha_j)) \neq 1$ for some j ?
Consider the following example in $\mathbb{Z}[x_0, x_1, x_2]$.

$$\widehat{A} = x_0^2 + x_2,\ \ \widehat{B} = x_0^2 + x_2 + (x_1 - 1) \ \text{ and } \ G = x_0^2 + x_1x_2.$$

Observe that for any prime p, $\gcd(\widehat{A}, \widehat{B}) = 1$ in $\mathbb{F}_p[x_0, x_1, x_2]$ but $\gcd(\widehat{A}(x_0, 1, \beta), \widehat{B}(x_0, 1, \beta)) \neq 1$ for all $\beta \in \mathbb{F}_p$ and therefore we cannot use $\gcd(A(x_0, 1, \beta), B(x_0, 1, \beta))$ to interpolate G.

We say α_j is ***unlucky*** if $\gcd(\widehat{A}(x_0, \alpha_j), \widehat{B}(x_0, \alpha_j)) \neq 1$.
What is the expected number of unlucky evaluation points?
How spread out is the distribution from the mean?

Unlucky evaluation points also arise in our current work in [3] where, given polynomials $a, b, c \in \mathbb{Z}[x_0, x_1, \ldots, x_n]$ with $\gcd(a, b) = 1$ we want to solve the diophantine equation $\sigma a + \tau b = c$ for σ and τ in $\mathbb{Z}[x_0, x_1, \ldots, x_n]$ by interpolating σ and τ modulo a prime p from univariate images.

First Result

Theorem 1. Let $\phi(n) = |\{\, 1 \le i \le n : \gcd(i, n) = 1\}|$ denote Euler's totient function. Let X be a random variable which counts the number of distinct roots of a monic polynomial in $\mathbb{Z}_n[x]$ of degree $m > 0$. Then

(a) $\mathrm{E}[X] = 1$ and
(b) if $m = 1$ then $\mathrm{Var}[X] = 0$, otherwise $\mathrm{Var}[X] = \sum_{d|n, d \neq n} \frac{d}{n}\phi(\frac{n}{d}) = \sum_{d|n} \frac{d-1}{n}\phi(\frac{n}{d})$.
In particular, if $n = p^k$ where p is a prime number and $k \ge 1$, $\mathrm{Var}[X] = k(1 - 1/p)$.

Remark 1. We found this result by direct computation and using the Online Encyclopedia of Integer Sequences (OEIS) see [4]. For polynomials of degree 2,3,4,5 in $\mathbb{Z}_n[x]$ we computed $\mathrm{E}[X]$ and $\mathrm{Var}[X]$ for $n = 2, 3, 4, \ldots, 20$ using Maple and found that $\mathrm{E}[X] = 1$ in all cases. Values for the variance are given in the table below.

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Var[X]	$\frac{1}{2}$	$\frac{2}{3}$	1	$\frac{4}{5}$	$\frac{3}{2}$	$\frac{6}{7}$	$\frac{3}{2}$	$\frac{4}{3}$	$\frac{17}{10}$	$\frac{10}{11}$	$\frac{7}{3}$	$\frac{12}{13}$	$\frac{25}{14}$	2	2
$a(n)$	1	2	4	4	9	6	12	12	17	10	28	12	25	30	32

When we first computed $\mathrm{Var}[X]$ we did not recognize the numbers. Writing $\mathrm{Var}[X] = a(n)/n$ we computed the sequence for $a(n)$ (see the table) and looked it up in the OEIS. We found it is sequence A006579 and that $a(n) = \sum_{k=1}^{n-1} \gcd(n, k)$. The OEIS also has the formula $a(n) = \sum_{d|n}(d-1)\phi(\frac{n}{d})$.

Second Result

Theorem 2. Let $f, g \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ be $f = c_l x_1^l + \sum_{i=0}^{l-1} c_{l-i}(x_2, \ldots, x_n)x_1^i$ and $g = d_m x_1^m + \sum_{i=0}^{m-1} d_{m-i}(x_2, \ldots, x_n)x_1^i$ where $c_l \neq 0$, $d_m \neq 0$, $\deg c_{l-i} \le l - i$, and $\deg d_{m-i} \le m - i$, thus f and g have total degree l and m respectively. Let X be a random variable which counts the number of $\gamma = (\gamma_2, \ldots, \gamma_n) \in \mathbb{F}_q^{n-1}$ such that $\gcd(f(x_1, \gamma_2, \ldots, \gamma_n), g(x_1, \gamma_2, \ldots, \gamma_n)) \neq 1$. If $n > 1$, $l > 0$ and $m > 0$ then

(a) $\mathrm{E}[X] = q^{n-2}$ and
(b) $\mathrm{Var}[X] = q^{n-2}(1 - 1/q)$.

It follows from (a) that if γ is chosen at random from $\mathbb{F}_q^{n-1}$ then

$$\mathrm{Prob}[\gcd(f(x_1, \gamma_2, \ldots, \gamma_n), g(x_1, \gamma_2, \ldots, \gamma_n) \neq 1] = \frac{q^{n-2}}{q^{n-1}} = \frac{1}{q}.$$

Remark 2. We found this result by computation. For quadratic polynomials f, g of the form $f = x^2 + (a_1y + a_2)x + a_3y^2 + a_4y + a_5$ and $g = x^2 + (b_1y + b_2)x + b_3y^2 + b_4y + b_5$ over finite fields of size $q = 2, 3, 4, 5, 8, 9, 11$ we generated all q^{10} pairs and computed $X = |\{\alpha \in \mathbb{F}_q : \gcd(f(x, \alpha), g(x, \alpha)) \neq 1\}|$. We repeated this for cubic polynomials and some higher degree bivariate polynomials for $q = 2, 3$ to verify that $\mathrm{E}[X] = 1$ and $\mathrm{Var}[X] = 1 - 1/q$ holds more generally. For yet higher degree polynomials we used random samples. That $\mathrm{E}[X] = 1$ independent of the degrees of f and g was a surprise to us. We had expected a logarithmic dependence on the degrees of the polynomials f and g.

A comparison with the binomial distribution.

Let Y be a random variable from a binomial distribution $B(n, p)$ with n trials and probability p. So $0 \le Y \le n$, $\mathrm{Prob}[Y = k] = \binom{n}{k}p^k(1 - p)^{n-k}$, $\mathrm{E}[Y] = np$ and $\mathrm{Var}[Y] = np(1 - p)$. Note that if f and g are bivariate then Theorem 2 implies that $\mathrm{E}[X] = 1$ and $\mathrm{Var}[X] = 1 - 1/q$ which is the same as the mean and variance of the binomial distribution $B(n, p)$ with $n = q$ trials and probability $p = 1/q$. In the table below we compare the two distributions for

$f = x^2 + (a_1y + a_2)x + (a_3y^2 + a_4y + a_5)$ and
$g = x^2 + (b_1y + b_2)x + (b_3y^2 + b_4y + b_5)$

in $\mathbb{F}_q[x, y]$ with $q = 7$. Note that there are 7^{10} pairs for f, g. In the table F_k is the number of pairs for which $\gcd(f(x, \alpha), g(x, \alpha)) \neq 1$ for exactly k values for $\alpha \in \mathbb{F}_7$. We computed F_k by computing this gcd for all distinct pairs using Maple. The values for B_k come from $B(7, 1/7)$. They are given by $B_k = 7^{10}\mathrm{Prob}[Y = k]$.

k	0	1	2	3	4	5	6	7
F_k	96606636	110666892	56053746	17287200	1728720	0	0	132055
B_k	96018048	112021056	56010528	15558480	2593080	259308	14406	343

The two zeros F_5 and F_6 can be explained as follows:
Let $R(y)$ be the Sylvester resultant of f and g. We have

$$R(\alpha) = 0 \iff \gcd(f(x, \alpha), g(x, \alpha)) \neq 1 \text{ for } \alpha \in \mathbb{F}_q.$$

For our quadratic polynomials f and g one has $\deg R \le \deg f \deg g = 4$. Hence $R(y)$ can have at most 4 distinct roots unless f and g are not coprime in $\mathbb{F}_7[x, y]$ in which case $R(y) = 0$ and it has 7 roots. Therefore $F_5 = 0$, $F_6 = 0$ and $F_7 = 132055$ is the number pairs f, g which are not coprime in $\mathbb{F}_7[x, y]$.

References

[1] J. de Kleine, M. B. Monagan, A. D. Wittkopf. Algorithms for the Non-monic case of the Sparse Modular GCD Algorithm. *Proc. ISSAC '05*, ACM Press, (2005), 124–131.

[2] Arnold Knopfmacher and John Knopfmacher. Counting irreducible factors of polynomials over finite fields. *Discrete Mathematics* **112** (1993) 103–118.

[3] Michael Monagan and Baris Tuncer. Using Sparse Interpolation in Hensel Lifting. To appear in the Proceedings of CASC 2016, Springer-Verlag LNCS, 2016.

[4] Sequence http://oeis.org/A006579 in *The On-Line Encyclopedia of Integer Sequences*, published electronically at http://oeis.org, 2010.

[5] Wolfgang Schmidt. *Equations over Finite Fields: An Elementary Approach.* Springer-Verlag LNCS **536** (1976) Ch 4 pp. 157–159.

[6] Richard. Zippel. Probabilistic Algorithms for Sparse Polynomials, *Proc. EUROSAM '79*, Springer-Verlag LNCS, **2**, 216–226, 1979.

NSERC CRSNG

Maplesoft
Mathematics • Modeling • Simulation

cecm