On Calculating the Cardinality of the Value Set of a Polynomial

(and some related problems)

Joshua Erin Hill

Department of Mathematics, University of California, Irvine

Dissertation Defense

2014-Oct-10 (rev. 1.01)

http://untruth.org/s/p12.html

Today's Theme

Unremitting Propaganda for Combinatorics

(Apologies to Michael Spivak)

Section 1

Introduction

Outline

The Problem

- Let $f : X \to Y$ be a map between finite sets.
- Denote the value set $V_f = \{f(\gamma) : \gamma \in X\}$.
- We are interested in the cardinality of V_f, which we denote $|V_f|$.
- Without constraints or structure, it isn't reasonable to expect any non-trivial algorithm.

Algebraic, Single Variable Case

- Let $f \in \mathbb{F}_q[x]$, of degree $d > 0$, where $q = p^a$.
- Denote the value set $V_f = \{f(\gamma) : \gamma \in \mathbb{F}_q\}$.
- This is the case that has been most studied.

Algebraic Varieties Defined Over Finite Fields

- X is an affine variety over $\bar{\mathbb{F}}_q$ defined by the simultaneous vanishing of the polynomials $(\alpha_1, \cdots, \alpha_\ell) = \alpha \in \left(\mathbb{F}_q[x_1, \cdots, x_r]\right)^\ell$.
- Y is an affine subvariety of $\mathbb{A}^s_{\bar{\mathbb{F}}_q}$.
- $(f_1, \cdots, f_s) = f \in \left(\mathbb{F}_q[x_1, \ldots, x_r]\right)^s$, a morphism between X and Y.
- Denote the value set $V_f\left(\mathbb{F}_{q^k}\right) = \left\{f(\gamma) : \gamma \in X\left(\mathbb{F}_{q^k}\right)\right\} \subset Y\left(\mathbb{F}_{q^k}\right)$, and $V_f = V_f\left(\mathbb{F}_q\right)$.
- Note that the $\ell = 0$ case gives an important special case (and this along with $r = 1$ gives the prior case).
- By $f|_{q^k}$, we mean the function $f|_{X(\mathbb{F}_{q^k})} : X\left(\mathbb{F}_{q^k}\right) \to Y\left(\mathbb{F}_{q^k}\right)$.

Outline

Cardinality of Value Sets

$$\left\lceil \frac{q}{d} \right\rceil \leq |V_f| \leq q$$

- These bounds are sharp!
- If $|V_f| = \left\lceil \frac{q}{d} \right\rceil$, then f is a polynomial with a minimal value set.
- If $|V_f| = q$, then f is a permutation polynomial.

Notation: Big-O and Soft-O

- We have two eventually positive real valued functions $A, B : \mathbb{N}^k \to \mathbb{R}^+$. Take $\mathbf{x}$ as an n-tuple, with $\mathbf{x} = (x_1, \ldots, x_n)$
- We'll write $|\mathbf{x}|_{\min} = \min_i x_i$.

Definition

1. $A(\mathbf{x}) = O(B(\mathbf{x}))$ if there exists a positive real constant C and an integer N so that if $|\mathbf{x}|_{\min} > N$ then $A(\mathbf{x}) \leq CB(\mathbf{x})$.
2. $A(\mathbf{x}) = \tilde{O}(B(\mathbf{x}))$ if there exists a positive real constant C' so that $A(\mathbf{x}) = O(B(\mathbf{x}) \log^{C'}(B(\mathbf{x}) + 3))$

Algorithms for Arbitrary Polynomials

One can view the problem of finding $|V_f|$ as being a generalization of the problem of determining if a polynomial, f, is a permutation polynomial. There are a few algorithms for this, but the best is:

- Kayal provided a deterministic-polynomial-time test running in $(d \log q)^{O(1)}$. [Kayal, 2005]

Naïve Algorithms

How to calculate $|V_f|$?

- Evaluate f at each point in $\mathbb{F}_q$. Cost: $\tilde{O}(qd)$ bit operations.
- For each $a \in \mathbb{F}_q$, $a \in V_f \Leftrightarrow \deg \gcd(f(x) - a, X^q - X) > 0$. Cost: $\tilde{O}(qd)$ bit operations.

Section 2

Point Counting and Weil Zeta Functions

The Weil Zeta Function on Varieties

Consider the simultaneous zeros of a set of polynomials $f_1, \ldots, f_r \in \mathbb{F}_q[x_1, \ldots, x_n]$ over $\bar{\mathbb{F}}_q$; call this variety X.

- Let $X(\mathbb{F}_{q^k})$ denote the $\mathbb{F}_{q^k}$-rational points of X.

Definition

The Weil zeta function of the variety X is defined to be

$$Z_X = Z_X(T) = \exp\left(\sum_{k=1}^{\infty} \frac{\left|X(F_{q^k})\right|}{k} T^k\right)$$

Curiouser and Curiouser

- Weil conjectured that the zeta function is rational.
- This conjecture was first proven by Dwork in 1960 using p-adic methods, and then by Grothendieck in 1964 using ℓ-adic cohomological methods.
- Approaches to building up Z_X generally start by calculating $\left|X(\mathbb{F}_{q^k})\right|$ up to a suitably large k (the maximal degree of the numerator or denominator).

Outline

Harvey's Point Counting Algorithm

Corollary

Let a, n, and m be positive integers, p be a prime, $q = p^a$, $\lambda = \max(a, \lceil (n+1)/2 \rceil)$, $f_1, \cdots, f_m \in \mathbb{F}_q[x_1, \cdots, x_n]$ be polynomials of positive degree, where each f_i has total degree d_i, and $d_+ = \sum_i d_i$. There is a deterministic algorithm that calculates the number of simultaneous solutions of $f_1(x_1, \cdots, x_n) = \cdots = f_m(x_1, \cdots, x_n) = 0$ residing in $\mathbb{F}_q^n$ in

$$\tilde{O}\left(2^{n+m}(n + 2d_+\lambda + 2\lambda)^{4n}\lambda^3 a^2 p^{1/2}\right) \text{ bit operations.}$$

Harvey's Point Counting Algorithm: Specification

Time complexity:

$$\tilde{O}\left((n+2d\lambda)^{4n}\lambda^3 a^2 p^{1/2}\right) \text{ bit operations.}$$

- We start by extracting a point counting algorithm from Harvey's zeta function calculation algorithm.
- Counts projective points cut out of an affine torus by a single degree d homogeneous polynomial, ${}^h f \in \mathbb{F}_q[x_0, x_1, \cdots, x_n]$.
- Only works if $p \nmid d$.

Harvey's Point Counting Algorithm: Affine Points

Time complexity:

$$\tilde{O}\left(2^n (n+2d\lambda)^{4n}\lambda^3 a^2 p^{1/2}\right) \text{ bit operations.}$$

- Let ${}^h f(x_0, \cdots, x_n) = x_0^d f(x_1/x_0, \cdots, x_n/x_0)$.
- Points where $x_0 \neq 0$ correspond to affine points (think: $x_0 = 1$).
- Characterize the points by which variables are 0: denote the set of variable indices that are 0 as $S \subset \{0, 1, \cdots, n\}$.
- The polynomial ${}^h f$ with some variables set to 0 is still degree d (or identically 0), and cuts out a variety from the affine torus in projective space. The $\mathbb{F}_q$-rational points of this variety are denoted $X^{\text{proj}}\left(\mathbb{F}_q\right)^S$.
- The various selections of S induce a partition of the full set of points.

$$\left|X(\mathbb{F}_q)\right| = \sum_{S\subset\{1,\cdots,n\}} \left|X^{\text{proj}}\left(\mathbb{F}_q\right)^S\right|.$$

Harvey's Point Counting Algorithm: Divisibility Fix

Time complexity:

$$\tilde{O}\left(2^n(n+2(d+1)\lambda)^{4n}\lambda^3 a^2 p^{1/2}\right) \text{ bit operations.}$$

- If $p \mid d$, then count the points on ${x_0}^h f$, which has the same number of points in the affine torus.

Harvey's Point Counting Algorithm: Easy as P.I.E.

Time complexity:

$$\tilde{O}\left(2^{n+m}(n+2(d_{+}+1)\lambda)^{4n}\lambda^{3}a^{2}p^{1/2}\right) \text{ bit operations.}$$

Denote:

- the variety defined by the simultaneous zeros of polynomials $f_1, \cdots, f_m$ over $\bar{\mathbb{F}}_q$ as X,
- the polynomial $f_I(x) = \prod_{i \in I} f_i(x)$, for some index set $I \subset \{1, \cdots, m\}$,
- and the variety defined by the zeros of $f_I = \prod_{i \in I} f_i$ over $\bar{\mathbb{F}}_q$ as X_I.

The Principal of Inclusion/Exclusion then gives us

$$\left|X\left(\mathbb{F}_q\right)\right| = \sum_{\emptyset \neq I \subset \{1,\cdots,m\}} (-1)^{|I|-1}\left|X_I\left(\mathbb{F}_q\right)\right|.$$

Outline

Harvey's Weil Zeta Algorithm

Corollary

Let a, n, and m be positive integers, p be a prime, $q = p^a$, $\lambda = \max(a, \lceil (n+1)/2 \rceil)$, X be a variety over $\bar{\mathbb{F}}_q$ defined by the simultaneous vanishing set of the polynomials $f_1, \cdots, f_m \in \mathbb{F}_q[x_1, \cdots, x_n]$ with positive total degrees d_i. Denote $d_+ = \sum_i d_i$. There is a deterministic algorithm that calculates the zeta function of X in

$$\tilde{O}\left(2^{8n^2+17n+m} n^{4n+4} (d_+ + 2)^{4n^2+7n} a^{4n+4} p^{1/2}\right) \text{ bit operations.}$$

Harvey's Weil Zeta Algorithm

Time complexity:

$$\tilde{O}\left(2^{8n^2+16n} n^{4n+4} (d+1)^{4n^2+7n} a^{4n+4} p^{1/2}\right) \text{ bit operations.}$$

- Computes the Weil zeta function of the projective variety cut out of an affine torus by a single degree d homogeneous polynomial, ${}^h f \in \mathbb{F}_q[x_0, x_1, \cdots, x_n]$.
- Only works if $p \nmid d$.

Harvey's Weil Zeta Algorithm: Affine Variety

Time complexity:

$$\tilde{O}\left(2^{8n^2+17n} n^{4n+4} (d+1)^{4n^2+7n} a^{4n+4} p^{1/2}\right) \text{ bit operations.}$$

- We follow the same as in the point counting algorithm.
- Homogenize f:

$$^{h}f(x_0, \cdots, x_n) = x_0^d f(x_1/x_0, \cdots, x_n/x_0).$$

- The polynomial ^{h}f with variables in S set to zero is still degree d (or identically 0), and cuts out a projective variety whose weil zeta function is denoted $Z^S_{X^{\text{proj}}}(T)$.
- The analogous addition in every finite extension, which translates to multiplying the zeta functions.

$$Z_X(T) = \prod_{S \subset \{1, \cdots, n\}} Z^S_{X^{\text{proj}}}(T).$$

Harvey's Weil Zeta Algorithm: Divisibility Fix

Time complexity:

$$\tilde{O}\left(2^{8n^2+17n} n^{4n+4} (d+2)^{4n^2+7n} a^{4n+4} p^{1/2}\right) \text{ bit operations.}$$

- If $p \mid d$, then examine ${x_0}^h f$; the number of $\mathbb{F}_{q^k}$-rational points on the variety cut by this polynomial from the affine torus in projective space is the same in every finite extension.

Harvey's Weil Zeta Algorithm: More P.I.E. Please!

Time complexity:

$$\tilde{O}\left(2^{8n^2+17n+m} n^{4n+4} (d_+ + 2)^{4n^2+7n} a^{4n+4} p^{1/2}\right) \text{ bit operations.}$$

For all positive integer k, the Principal of Inclusion/Exclusion then gives us

$$\left|X\left(\mathbb{F}_{q^k}\right)\right| = \sum_{\emptyset \neq I \subset \{1,\cdots,m\}} (-1)^{|I|-1} \left|X_I\left(\mathbb{F}_{q^k}\right)\right|.$$

- Addition of points corresponds to multiplication of zeta functions, and subtraction to division of zeta functions, so

$$Z_X(T) = \prod_{\emptyset \neq I \subset \{1,\cdots,m\}} Z_{X_I}(T)^{(-1)^{|I|-1}}.$$

Outline

Amortized Cost Calculation of Weil Zeta Functions

Corollary

Let n, m, and N be positive integers, $f_1, \cdots, f_m \in \mathbb{Z}[x_1, \cdots, x_n]$ be polynomials with positive total degrees d_i and maximal coefficients $\|f_i\|$, with $\|f\| = \prod_i \|f_i\|$. For a prime p let X_p denote the affine variety defined over $\bar{\mathbb{F}}_p$ defined by the simultaneous vanishing set of all the p-reductions of the f_i. Denote $d_+ = \sum_i d_i$. There is a deterministic algorithm to calculate the zeta function for X_p for all $p < N$ in

$$\tilde{O}\left(2^{8n^2+17n+m+1} n^{4n+6} (d_+ + 2)^{4n^2+7n} N \log \|f\|\right) \textit{ bit operations.}$$

This proceeds from Harvey's original algorithm in exactly the same way as with the single zeta function computation algorithm.

Outline

Here and Back Again?

Recall:

$$Z_X(T) = \exp\left(\sum_{r\geq 1} \frac{\left|X\left(\mathbb{F}_{q^r}\right)\right|}{r} T^r\right)$$
$$= \frac{g(T)}{h(T)},$$

where $g, h \in 1 + T\mathbb{Z}[T]$. Taking the logarithmic derivative of this expression yields

$$\sum_{r\geq 1} \left|X\left(\mathbb{F}_{q^r}\right)\right| T^{r-1} = \frac{g'(T)}{g(T)} - \frac{h'(T)}{h(T)}.$$

Reading is Hard!

Proposition

If $g \in 1 + T\mathbb{Z}[T]$, then the first R terms of the formal power series $g'(T)/g(T)$ can be deterministically calculated in $\tilde{O}(R^2 \log \|g\|)$ bit operations, where $\|g\|$ denotes the maximum of the absolute values of the coefficients of g.

Proceeds via standard formal power series tools:

- Kronecker substitution for multiplication of polynomials.
- Sieveking-Kung for calculating (truncated) the formal power series inverse.

Section 3

Further Combinatorial Antics

The Fiber Product

$$\begin{tikzcd} X \times_Y X \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] & X \arrow[d, "f"] \\ X \arrow[r, "f"'] & Y \end{tikzcd}$$

In other words (in the category of sets):

$$X \times_Y X = \{(x_1, x_2) \in X \times X : f(x_1) = f(x_2)\}\,.$$

Similarly, define

$$X^{\times_Y k} = \underbrace{X \times_Y \cdots \times_Y X}_{k \text{ terms}} = \left\{(x_1, \cdots, x_k) \in X^k : f(x_1) = \cdots = f(x_k)\right\}.$$

$|V_f|$ and the Fiber Product

Theorem

If X and Y are finite sets, and $f : X \to Y$ is a map such that any given fiber has at most d elements, then the cardinality of the image set of f is

$$|V_f| = \sum_{i=1}^{d} (-1)^{i-1} N_i \sigma_i \left(1, \frac{1}{2}, \cdots, \frac{1}{d}\right),$$

where $N_k = \left|X^{\times_Y k}\right|$ and σ_i denotes the ith elementary symmetric polynomial on d elements.

Proof Outline I

- $V_{f,i} = \left\{x \in V_f : \left|f^{-1}(x)\right| = i\right\}$ with $1 \leq i \leq d$ forms a partition of V_f.
- Let $m_i = \left|V_{f,i}\right|$. Thus $m_1 + \cdots + m_d = |V_f|$. Introduce a new value $\xi = -|V_f|$. We then have:

$$m_1 + \cdots + m_d + \xi = 0$$

- Define the space $\tilde{N}_k = X^{\times_Y k}$. Then $N_k = \left|\tilde{N}_k\right|$.
- By a counting argument,

$$m_1 + 2^k m_2 + \cdots + d^k m_d = N_k$$

Proof Outline II

Arrange this into a system of equations:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & \cdots & d & 0 \\ 1 & 2^2 & \cdots & d^2 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 1 & 2^d & \cdots & d^d & 0 \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ m_3 \\ \vdots \\ \xi \end{pmatrix} = \begin{pmatrix} 0 \\ N_1 \\ N_2 \\ \vdots \\ N_d \end{pmatrix}$$

Solve for ξ using Cramer's rule.
Warning: determinant magic!

Variations on a Theme of Matrices

You can just as reasonably solve for m_j through the same process:

Theorem

If X and Y are finite sets, and $f : X \to Y$ is a map such that any given fiber has at most d elements, then for any positive integer $j \leq d$, the number of points in the co-domain whose fiber has exactly j elements is

$$m_j = \binom{d}{j}\frac{1}{j}\sum_{i=1}^{d}(-1)^{i+j}N_i\sigma_{i-1}\left(1, \frac{1}{2}, \cdots, \frac{1}{j-1}, \frac{1}{j+1}, \cdots, \frac{1}{d}\right),$$

where $N_k = \left|X^{\times_Y k}\right|$ and σ_i denotes the ith elementary symmetric polynomial on $d-1$ elements.

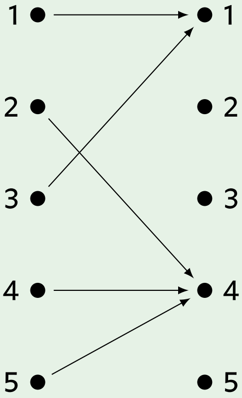
Warning: (similar) determinant magic!

The Fiber Signature

- Note that by calculating $(m_1, \cdots, m_d)$ you know a profound amount about the map.
- We refer to this value as the fiber signature.
- Trivially, if we have the fiber signature, we can calculate the size of the value set.

An Example Map

Example



Example (Value Set Cardinality)

Example

j	m_j	N_j	$\sigma_j\left(1, \frac{1}{2}, \frac{1}{3}\right)$
1	0	5	$11/6$
2	1	13	1
3	1	35	$1/6$

$$|V_f| = 5 \cdot \frac{11}{6} - 13 \cdot 1 + 35 \cdot \frac{1}{6} = 2.$$

Example (Fiber Signature)

Example

j	N_j	$\sigma_{j-1}\left(\frac{1}{2},\frac{1}{3}\right)$	$\sigma_{j-1}\left(1,\frac{1}{3}\right)$	$\sigma_{j-1}\left(1,\frac{1}{2}\right)$
1	5	1	1	1
2	13	5/6	4/3	3/2
3	35	1/6	1/3	1/2

$$m_1 = \binom{3}{1} \cdot \frac{1}{1} \cdot \left(5 \cdot 1 - 13 \cdot \frac{5}{6} + 35 \cdot \frac{1}{6}\right) = 0$$

$$m_2 = \binom{3}{2} \cdot \frac{1}{2} \cdot \left(-5 \cdot 1 + 13 \cdot \frac{4}{3} - 35 \cdot \frac{1}{3}\right) = 1$$

$$m_3 = \binom{3}{3} \cdot \frac{1}{3} \cdot \left(5 \cdot 1 - 13 \cdot \frac{3}{2} + 35 \cdot \frac{1}{2}\right) = 1.$$

Section 4

Counting the Value Set of Morphisms in Affine Varieties

One Dimensional Case

Corollary

Let a be a positive integer, p be a prime, $q = p^a$, and $f(x) \in \mathbb{F}_q[x]$ be a polynomial with positive degree d. There is a deterministic algorithm that calculates the cardinality of the value set, $|V_f|$ in $\mathbb{F}_q$, and more generally the fiber signature of f, with computational complexity

$$\tilde{O}\left(2^{6d-1}\lambda^{4d+3}d^{8d+1}a^2p^{1/2}\right) \text{ bit operations,}$$

where $\lambda = \max\left(a, \lceil (d+1)/2 \rceil\right)$.

Proof Outline

- Surely there are no more than d elements in any given pre-image.
- The spaces we are looking at are thus of the form:

$$\tilde{N}_k = \left\{(x_1, \cdots, x_k) \in \mathbb{F}_q^k : f(x_1) = \cdots = f(x_k)\right\}$$
$$= \left\{ (x_1, \cdots, x_k) \in \mathbb{F}_q^k \,\middle|\, \begin{array}{ll} f(x_1) - f(x_2) & = 0 \\ f(x_1) - f(x_3) & = 0 \\ \vdots & \\ f(x_1) - f(x_k) & = 0 \end{array} \right\}$$

- For N_k, apply the point counting algorithm to the polynomials for g_1 to g_{k-1}, where

$$g_i(x_1, \cdots, x_k) = f(x_1) - f(x_{i+1}) .$$

- Calculate N_1 to N_d and the relevant elementary symmetric polynomials.
- PROFIT!

General Case

Theorem

If there is a positive integer $\mathcal{D}$ so that $\left|(f|_q)^{-1}(y)\right| \leq \mathcal{D}$ for all $y \in V_f$, then there is a deterministic algorithm to calculate the cardinality of the value set of $f|_q$, and more generally the fiber signature of f, with computational complexity

$$\tilde{O}\left(2^{\mathcal{D}(\ell+s+r)-s}\mathcal{D}(\mathcal{D}r + 2d_+\lambda + 2\lambda)^{4\mathcal{D}r}\lambda^3 a^2 p^{1/2}\right) \text{ bit operations,}$$

where $\lambda = \max\left(a, \lceil(\mathcal{D}r+1)/2\rceil\right)$ *and* $d_+ = \sum_{i=1}^{\mathcal{D}\ell+(\mathcal{D}-1)s} d_i$.

(My Apologies for) The General Case

- By hypothesis, there are no more than $\mathcal{D}$ elements in any given pre-image.
- The spaces we are looking at are thus of the form:

$$\tilde{N}_k(\mathbb{F}_q) = \left\{\left(x^{(1)}, \cdots, x^{(k)}\right) \in X(\mathbb{F}_q)^k : f\left(x^{(1)}\right) = \cdots = f\left(x^{(k)}\right)\right\}$$

$$= \left\{ \left(x^{(1)}, \cdots, x^{(k)}\right) \in \left(\mathbb{F}_q^r\right)^k \;\middle|\; \begin{array}{cc} \alpha(x^{(1)}) & = 0 \\ \vdots & \\ \alpha(x^{(k)}) & = 0 \\ f\left(x^{(1)}\right) - f\left(x^{(2)}\right) & = 0 \\ \vdots & \\ f\left(x^{(1)}\right) - f\left(x^{(k)}\right) & = 0 \end{array} \right\}$$

- This is a total of $k\ell + (k-1)s$ polynomials, each in kr variables.
- Calculate N_1 to $N_{\mathcal{D}}$, and scale by the relevant elementary symmetric polynomials.

A Lemma From Algebraic Geometry

Lemma

If $f : X \to Y$ is a finite dominant morphism and $\mathcal{O}(X)$ is generated by t elements or fewer as an $\mathcal{O}(Y)$-module (via the induced $\bar{\mathbb{F}}_q$-algebra homomorphism $f^\star$), then $\left|f^{-1}(y)\right| \leq t$ for all $y \in Y$. If X is irreducible, then the fibers of f have cardinality at most the degree of f.

Additional Corollaries I

Corollary

If X is irreducible and f is a finite dominant morphism from X to Y of fixed degree d, then there is a deterministic algorithm to calculate the cardinality of the value set of $f|_q$, and more generally the fiber signature of $f|_q$, with computational complexity described in the prior theorem, with $\mathcal{D} = d$.

Corollary

If f is a finite dominant morphism, and $\mathcal{O}(X)$ is generated by a set of t elements from $\mathcal{O}(Y)$ (via the induced $\bar{\mathbb{F}}_q$-algebra homomorphism $f^\star$), then there is a deterministic algorithm to calculate the cardinality of the value set of $f|_q$, and more generally the fiber signature of $f|_q$, with computational complexity described in the prior theorem, with $\mathcal{D} = t$.

Additional Corollaries II

Corollary

If f is a finite dominant morphism from $\mathbb{A}^r_{\bar{\mathbb{F}}_q}$ to $\mathbb{A}^r_{\bar{\mathbb{F}}_q}$ of fixed degree d, then there is a deterministic algorithm to calculate the cardinality of the value set of $f|_q$, and more generally the fiber signature of $f|_q$, with computational complexity

$$\tilde{O}\left(2^{2dr-r}d(dr+2d_+\lambda+2\lambda)^{4dr}\lambda^3a^2p^{1/2}\right) \text{ bit operations,}$$

where $\lambda = \max\left(a, \lceil (dr+1)/2 \rceil\right)$ *and* $d_+ = \sum_{i=1}^{(d-1)r} d_i$.

Section 5

Amortized Algorithms

Amortized Across Many Characteristics

Theorem

Let r, s, N and R be positive integers. Let f be an s-tuple of polynomials $f(x) = (f_1(x), \cdots, f_s(x))$, where $f_i(x) = \mathbb{Z}[x_1, \cdots, x_r]$, where the total degree of f_i is d_i.

If there is a positive integer $\mathcal{D}$ so that $\left|\left(f|_{p^R}\right)^{-1}(y)\right| \leq \mathcal{D}$ for all $y \in \mathbb{F}_{p^R}^s$ and for all primes $p < N$, then there is a deterministic algorithm to calculate the cardinality of the value set of $f|_{p^w}$, and more generally the fiber signature of $f|_{p^w}$, for all $w \leq R$ and all primes $p < N$, with computational complexity

$$\tilde{O}\left(2^{\mathcal{D}(8\mathcal{D}r^2+17r+s)-s+1}\mathcal{D}^{4\mathcal{D}r+8}r^{4\mathcal{D}r+6}((\mathcal{D}-1)d_+ + 2)^{\mathcal{D}r(4\mathcal{D}r+7)}N\log\|f\| + N\mathcal{D}^2R^2r2^{(\mathcal{D}-1)s}\left(4(\mathcal{D}-1)d_+ + 5\right)^{\mathcal{D}r}\right) \text{ bit operations,}$$

where $d_+ = \sum_{i=1}^s d_i$ and $\|f\| = \prod_{j=1}^s \|f_j\|$.

Proof Outline

- Use the amortized cost zeta function calculation algorithm to find all zeta functions for $\tilde{N}_{k,p}$.
- Extract the number of $\mathbb{F}_{p^w}$-rational points for each of these varieties for all $w \leq R$.
- Apply the combinatorial results used previously.
- Larger scale profit
- (but at what cost?)

Doubly Amortized: Single Variable Case

Corollary

Let N and R be positive integers and f be a polynomial $f(x) \in \mathbb{Z}[x]$ of positive degree d. There is a deterministic algorithm to calculate the cardinality of the value set of $f|_{p^w}$, and more generally the fiber signature for $f|_{p^w}$, for all positive integers $w \leq R$ and for all primes $p \leq N$ with computational complexity

$$\tilde{O}\left(2^{d(8d+18)} d^{8d^2+18d+8} N \log \|f\| + NR^2 2^{3d-1} d^{2d+2}\right) \text{ bit operations.}$$

Fixed Single Variable Polynomial Case

$$\pi(N) \sim \frac{N}{\log N}.$$

- Divide by the number of expected values $\pi(N)R$.

Cor.	Complexity (bit operations)
Single Value	$\tilde{O}\left(R^2 N^{1/2}\right)$
Amortized	$\tilde{O}\left(R^{-1} N^{1/2} + R \log N\right)$
Doubly Amortized	$\tilde{O}(R \log N)$

Section 6

Conclusion

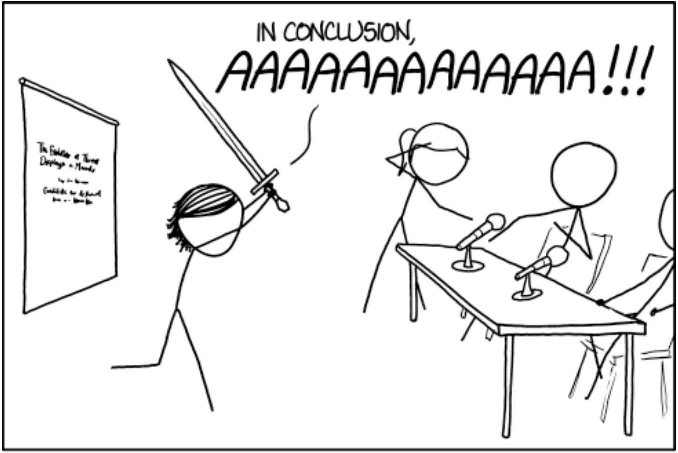
Conclusion

- Adapted and analyzed point counting and zeta function calculation algorithms.
- Combinatorial results linking the iterated fiber product and the cardinality of the value set (and fiber signature).
- Calculation of the cardinality of the value set (and fiber signature) for certain types of finite morphisms between affine varieties over finite fields.
- Two types of "amortized cost" algorithms, whose cost per result is excellent.

Future Work

- Additional applications of the fiber signature.
- Adapt Harvey's approach to the function field case.
- Refine dependence of asymptotic finding on the function degree.

Thanks!



THE BEST THESIS DEFENSE IS A GOOD THESIS OFFENSE.

Randall Munroe, `xkcd.com`

UNIVERSITY *of* CALIFORNIA · IRVINE

Colophon

- The principal font is Evert Bloemsma's 2004 humanist san-serif font Legato. This font is designed to be exquisitely readable, and is a significant departure from the highly geometric forms that dominate most san-serif fonts. Legato was Evert Bloemsma's final font prior to his untimely death at the age of 46.
- Mathematical symbols are from the MathTime Professional II (MTPro2) fonts, a font package released in 2006 by the great mathematical expositor Michael Spivak.
- The URLs are typeset in Luc(as) de Groot's 2005 Consolas, a monospace font with excellent readability.
- Diagrams were produced in TikZ.