Computing sparse multiples of polynomials

Mark Giesbrecht Daniel S. Roche Hrushikesh Tilak

Symbolic Computation Group
School of Computer Science
UNIVERSITY OF WATERLOO

ISAAC 2010
Jeju, Republic of Korea
15 December 2010

Problem Statement

Sparsest Multiple Computation

Input Univariate polynomial f in $\mathbb{Q}[x]$ or $\mathbb{F}_q[x]$

Output A sparsest multiple of f of least degree.
(That is, a multiple of f with fewest nonzero terms)

Example (in $\mathbb{Q}[x]$)

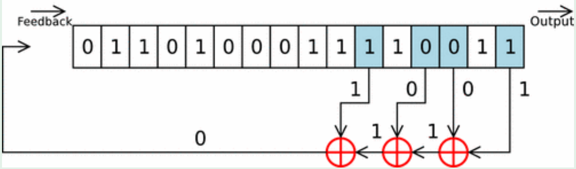
Input: $f = x^4 - 3x^3 + x^2 + 6x + 4$

Sparsest multiple: $h = x^{12} + 259x^6 + 64$

Not computed: $h/f = x^8 + 3x^7 + 8x^6 + 15x^5 + 15x^4 + \cdots \in \mathbb{Q}[x]$

Motivations: Cryptography

LFSR-based stream ciphers



- Sparse multiples of feedback polynomial lead to fast attacks.

TCHo

- Crytosystem proposed by (Aumasson et al, 2007)
- Computing sparse multiples in $\mathbb{F}_2[x]$ is their hard problem
- They explicitly assume average-case exponential lower bound

Motivations: Efficient Arithmetic

First noticed by Brent & Zimmerman (2003)

- Arithmetic in prime power fields $\mathbb{F}_{p^k}$ is usually done in $\mathbb{F}_p/\langle\Gamma\rangle$ for irreducible $\Gamma \in \mathbb{F}_p[x]$.
- Some field sizes admit no very-sparse irreducibles
- **Idea**: Work modulo a sparse multiple with low degree.
- Lots of searching has been done over $\mathbb{F}_2[x]$

Motivations: Computer Aided Geometric Design

source: CAEbridge, LLC

Motivations: Computer Aided Geometric Design

- Geometric surfaces are represented either
  - **Parametrically**: vector of parametric rational functions, or
  - **Implicitly**: solution set of multivariate polynomial
- Coverting from parametric to implicit is called implicitization.
- Can be thought of as finding a polynomial with given roots.
- Sparse implicitizatons make certain computations easier.

Motivations: Coding Theory

The problem can be formulated in linear algebra terms:

$$\begin{array}{ccccc} M_f & \times & v_g & = & v_h \\ \begin{bmatrix} f_0 & & & \\ f_1 & f_0 & & \\ \vdots & f_1 & \ddots & \\ f_d & \vdots & \ddots & f_0 \\ & f_d & \ddots & f_1 \\ & & \ddots & \vdots \\ & & & f_d \end{bmatrix} & & \begin{bmatrix} g_0 \\ g_1 \\ \\ \vdots \\ \\ g_{n-d} \end{bmatrix} & = & \begin{bmatrix} h_0 \\ h_1 \\ \\ \vdots \\ \\ h_n \end{bmatrix} \end{array}$$

Motivations: Coding Theory

The problem can be formulated in linear algebra terms:

$$\begin{array}{ccccc} M_f & \times & v_g & = & v_h \\ \begin{bmatrix} f_0 & & & \\ f_1 & f_0 & & \\ \vdots & f_1 & \ddots & \\ f_d & \vdots & \ddots & f_0 \\ & f_d & \ddots & f_1 \\ & & \ddots & \vdots \\ & & & f_d \end{bmatrix} & & \begin{bmatrix} g_0 \\ g_1 \\ \\ \vdots \\ \\ g_{n-d} \end{bmatrix} & = & \begin{bmatrix} h_0 \\ h_1 \\ \\ \vdots \\ \\ h_n \end{bmatrix} \end{array}$$

- Finding sparse vectors in a lattice is **NP**-hard.
- Similar to maximum likelihood decoding of cyclic codes.

Summary of Results

	Over $\mathbb{F}_q[x]$	Over $\mathbb{Q}[x]$
Binomial multiples	Equivalent to order finding	In **P**
t-sparse multiples, t constant	Harder than order finding	(mostly) in **P**
t-sparse multiples, t variable	???	???

Order Finding

Definition (Order)

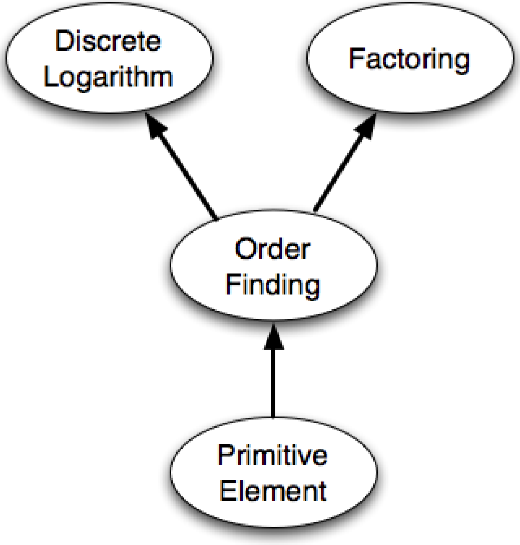
Given $\alpha \in \mathbb{F}_q[x]$, the multiplicative order of α is the least integer k such that $\alpha^k = 1$.

Connection to binomial multiples

If $f(\alpha) = 0$, and $f \mid (x^n - 1)$, then $\alpha^n = 1$.

- To show hardness, given $\alpha \in \mathbb{F}_{q^e}$, we take $f = (x-1) \cdot \mathrm{minpoly}(\alpha)$ in $\mathbb{F}_q[x]$ and find a binomial multiple of f.
- To show easiness, given $f \in \mathbb{F}_q[x]$ with $\deg f = d$, we find orders of all distinct roots $\alpha \in \mathbb{F}_{q^d}$ of f

Complexity of Order Finding



t-sparse Multiples Harder than Order Finding

Consider $\alpha \in \mathbb{F}_{q^e}$.
We use an oracle for t-sparse multiples to find the order of α.

- Find $g_i = \mathrm{minpoly}(\alpha^i) \in \mathbb{F}_q[x]$ for $i = 0, 1, \ldots, t-1$
- Let $f \in \mathbb{F}_q[x]$ be product of distinct g_i's.
- **Theorem**: f has a t-sparse multiple with degree $\leq n$
  iff $\mathrm{order}(\alpha) \leq n$.

  (In fact, the t-sparse multiple will be a binomial multiple.)

Sparse multiples in $\mathbb{Q}[x]$ connect to factorization

Related Problems

sparse multiple of a low-degree polynomial	$\Leftrightarrow$	low-degree factor of a sparse polynomial

- The latter problem has received much attention, both from mathematicians and computer scientists.

- It is convenient to associate with a squarefree input $f \in \mathbb{Q}[x]$ the roots $\theta_1, \theta_2, \ldots \in \bar{\mathbb{Q}}$ of its irreducible factors. Then f divides some $h \in \mathbb{Q}[x]$ iff $h(\theta_i) = 0$ for each i.

Binomial multiples in $\mathbb{Q}[x]$

Theorem (Risman (1976))

An irreducible $f \in \mathbb{Q}[x]$ with any binomial multiple has some binomial multiple of degree n, where $n = s \cdot t$ for some $s | \deg f$ and $\phi(t) | \deg f$.

- Leads to a polynomial *upper bound* on degree of least-degree binomial multiple
- Can then find binomial multiples of irreducibles by search
- For reducible f, correlating the binomial multiples of each factor just involves lcms and some more checks.
- We can generate examples of least-degree sparsest multiples with exponential degree and $\log$ height.

t-sparse Multiples in $\mathbb{Q}[x]$

Key Tool: Lenstra (1999)

If $h \in \mathbb{Q}[x]$ written $h_1 + x^k h_2$ has a big gap: $k \gg h_2$,
then any low-degree non-cyclotomic factor of h
is a factor of both h_1 and h_2

For instance, consider the polynomial h given by:

$$\underbrace{2x^{105} + 3x^{104} - 2x^{103} - x^{102} + x^{101} - 3x^{100}}_{h_2} \underbrace{\qquad\qquad\qquad\qquad}_{\text{(the gap)}} \underbrace{-2x^4 + x^3 + 4x^2 - 3x}_{h_1}$$

$f = 2x^2 + x - 3$ divides h, so $f | h_1$ and $f | h_2$.

- Lenstra used this for lacunary factorization

Gap theorem for sparsest multiples

Turning the gap theorem around, we get:

Theorem

The least-degree t-sparse multiple with height at most c of a non-cyclotomic polynomial $f \in \mathbb{Q}[x]$ has degree bounded by

$$(t + \log c + \deg f)^{O(1)}$$

With such a degree bound, the problem reduces to finding the least-height t-sparse rational vector in a lattice.

This is polynomial-time when t is constant using (Ajtai, Kumar, and Sivakumar 2001).

Handling cyclotomics: Example

$$f = x^{10} - 5x^9 + 10x^8 - 8x^7 + 7x^6 - 4x^5 + 4x^4 + x^3 + x^2 - 2x + 4$$

Step 1: Extract cyclotomic factors

$$f = \underbrace{(x^2 - x + 1)}_{\Phi_6} \cdot \underbrace{(x^4 - x^3 + x^2 - x + 1)}_{\Phi_{10}} \cdot \underbrace{(x^4 - 3x^3 + x^2 + 6x + 4)}_{\substack{f_D \\ \text{(cyclotomic-free)}}}$$

Handling cyclotomics: Example

$$f = x^{10} - 5x^9 + 10x^8 - 8x^7 + 7x^6 - 4x^5 + 4x^4 + x^3 + x^2 - 2x + 4$$

Step 2: Calculate degree bound

Target sparsity: ≤ 10, target height: ≤ 1000

Actual degree bound: $\deg h \leq 11\,195\,728$
(asymptotically polynomial, practically quite large!)

For this example, we'll cheat and say $\deg h \leq 20$

Handling cyclotomics: Example

$$f = x^{10} - 5x^9 + 10x^8 - 8x^7 + 7x^6 - 4x^5 + 4x^4 + x^3 + x^2 - 2x + 4$$

Step 3: Find low-degree sparsest multiples

Sparsest multiple of f with degree ≤ 20:

$$h_A = x^{11} - 3x^{10} + 12x^8 - 9x^7 + 10x^6 - 4x^5 + 9x^4 + 3x^3 + 8$$

Sparsest multiple of f_D (cyclotomic-free part):

$$h_B = x^{12} + 259x^6 + 64$$

Handling cyclotomics: Example

$$f = x^{10} - 5x^9 + 10x^8 - 8x^7 + 7x^6 - 4x^5 + 4x^4 + x^3 + x^2 - 2x + 4$$

Step 4: Sparsest multiple of cyclotomic part

Recall $f = \Phi_6 \cdot \Phi_{10} \cdot f_D$.
Cyclotomic part is $f_C = \Phi_6 \cdot \Phi_{10}$

Sparsest multiple of f_C:

$$h_C = \left(x^{\mathrm{lcm}(6,10)} - 1\right) = \left(x^{30} - 1\right)$$

Handling cyclotomics: Example

$$f = x^{10} - 5x^9 + 10x^8 - 8x^7 + 7x^6 - 4x^5 + 4x^4 + x^3 + x^2 - 2x + 4$$

Step 5: Compare candidates

Two candidates for sparsest multiple of f:

- $h_A = x^{11} - 3x^{10} + 12x^8 - 9x^7 + 10x^6 - 4x^5 + 9x^4 + 3x^3 + 8$
- $h_B \cdot h_C = x^{42} + 259x^{36} + 64x^{30} - x^{12} - 259x^6 - 64$

Conclusion: A sparsest multiple of f is

$$h = x^{42} + 259x^{36} + 64x^{30} - x^{12} - 259x^6 - 64$$

Open Problems

- Proving **NP**-hardness for the general case (t variable) over rationals or finite fields
- Improving the t-sparse algorithm over $\mathbb{Q}[x]$:
  - More practical degree bounds
  - Eliminate need for a priori height bound
  - De-randomize
  - Handle missing case:
    non-cyclotomic and repeated cyclotomic factors
- Extending to multivariate polynomials