Paper presentation: Fast polynomial factorization, modular composition, and multipoint evaluation of multivariate polynomials in small characteristic

by Christopher Umans

Bijayan Ray

May 23, 2024

Paper presentation

Fast polynomial factorization, modular composition, and multipoint evaluation of multivariate polynomials in small characteristic by Christopher Umans [Uma07].

Contents

Main problems

Definition 1.1 (Multivariate multipoint evaluation [Uma07])

Given $f(x_0, \cdots x_{m-1})$ *in* $\mathbb{F}_q[x_0, \cdots x_{m-1}]$ *with individual degrees at most* $d-1$ *and evaluation points* $\alpha_0, \cdots \alpha_{d^m-1} \in \mathbb{F}_q^m$, *output* $f(\alpha_i)$ *for* $i = 0, \cdots d^m - 1$.

Definition 1.2 (Modular composition)

Given $f(x_0, \cdots, x_{m-1})$ *in* $\mathbb{F}_q[x_0, \cdots, x_{m-1}]$ *with individual degrees at most* $d-1$, *and polynomials* $g_0(x), \cdots, g_{m-1}(x)$ *and* $h(x)$ *all in* $\mathbb{F}_q[x]$ *and with degree at most* $d^m - 1$, *output* $f(g_0(x), \cdots, g_{m-1}(x)) mod\ h(x)$.

Main result

1. Randomized algorithms for factoring degree n univariate polynomials over $\mathbb{F}_q$ that use $O(n^{1.5+o(1)} + n^{1+o(1)} \log q)$ field operations given the characteristic is at most $n^{o(1)}$.
2. For $\log q < n$ this turns out to be asymptotically faster than the best previously known algorithms by von zur Gathen[VZGG13] and Shoup and Kaltofen & Shoup [KS95].
3. For $\log q \geq n$ it matches the asymptotic running time of the best known algorithms.
4. It has been achieved by showing that modular composition and multipoint evaluation of multivariate polynomials are algorithmically equivalent.

Main idea of the new algorithm

- It uses the idea of modular composition in small characteristics, not relying on the conventional methods using fast matrix multiplication algorithms.
- It uses an asymptotically optimal number of operations solving the modular composition problem over $\mathbb{F}_q$ in $O(n^{1+o(1)})$ operation assuming the characteristic being at most $n^{o(1)}$.
- This leads to polynomial factorization in $O(n^{1.5+o(1)} + n^{1+o(1)} \log q)$ time.
- The main operations in these algorithms are just the standard fast univariate polynomial arithmetic operations, and multipoint evaluation and interpolation of univariate polynomials.

Equivalence using reduction I

Theorem 4.1

Given $f(x_0, \cdots x_{m-1}) \in \mathbb{F}_q[x_0, \cdots x_{m-1}]$ *with individual degrees* $\leq d-1$ *and polynomials* $g_0(x), \cdots g_{m-1}(x)$ *and* $h(x)$ *all* $\in \mathbb{F}_q[x]$ *and with degree* $\leq d^m - 1$, *there is for every* $d_0 < d$ *an algorithm that outputs* $f(g_0(x), \cdots g_{m-1}(x)) \mod h(x)$ *in* $\tilde{O}_{d^m}((d^m + T(d_0, \lceil \log_{d_0} d \rceil m))d_0)$ *field operations where* $T(d_0, m_0)$ *is the number field operations to solve the multivariate multipoint evaluation with parameters* d_0, m_0.

Corollary 4.1

Fix parameters d, m, *for every* $\epsilon \geq 0$ *if multivariate multipoint evaluation with parameter* $d_0 = d^\epsilon$ *and* $m_0 = m/\epsilon$ *can be solved in* $\tilde{O}_{d_0^{m_0}}((d_0^{m_0})^\alpha)$ *operations for some constant* $\alpha > 1$ *then the modular composition problem with parameters* d, m *can be solved in* $\tilde{O}_{d^m}((d^m)^{\alpha+\epsilon})$ *operations.*

Equivalence using reduction II

Theorem 4.2

Given $f(x_0, \cdots x_{m-1}) \in \mathbb{F}_q[x_0, \cdots x_{m-1}]$ *with individual degrees* $\leq d-1$ *and evaluation points* $\alpha_0, \cdots \alpha_{d^m-1} \in \mathbb{F}_q^m$ *there is an algorithm that outputs* $f(\alpha_i)$ *for* $i = 0, 1 \cdots d^m - 1$ *in* $\tilde{O}_{d^m}(d^m + T(d, m))$ *field operations where* $T(d, m)$ *is the number field operations to solve the modular composition problem with parameters* d, m.

Corollary 4.2

Fix parameters d, m *then if modular composition with parameters* d *and* m *can be solved in* $\tilde{O}_{d^m}((d^m)^\alpha)$ *operations for some constant* $\alpha > 1$ *then multivariate multipoint evaluation with parameters* d, m *can be solved in* $\tilde{O}_{d^m}((d^m)^\alpha)$ *operations.*

New algorithm for multipoint evaluation I

Construction of extension ring:

- Fix parameters d and m and a field $\mathbb{F}_q$ with characteristic p and $h = p^c$ is the smallest integer power of p that is larger than $m^2 d$.
- Construct ring $R = \mathbb{F}_q[W]/P(W)$, $P(W)$ being the degree c polynomial with coefficients in $\mathbb{F}_p$ that is irreducible over $\mathbb{F}_q$
- Notice that $\mathbb{F}_q[W]/P(W) \subset R$, $\mathbb{F}_q \subseteq R$ and that these embeddings are easy to compute.
- Choose η to be a primitive element of the field $\mathbb{F}_q[W]/P(W)$ and note that this has multiplicative order $h - 1$.
- Given the m-variate polynomial f over R we are to find it at many points in $\mathbb{F}_q^m \subseteq R^m$.
- We lift the evaluation points to elements of an extension ring S and evaluate a related univariate polynomial f^* at those points, and then project back to an element of R.

New algorithm for multipoint evaluation II

- We choose the ring S to be the extension ring $R[Z]/E(Z)$ where $E(Z) := Z^{h-1} - \eta$. Refer to the figure 1.

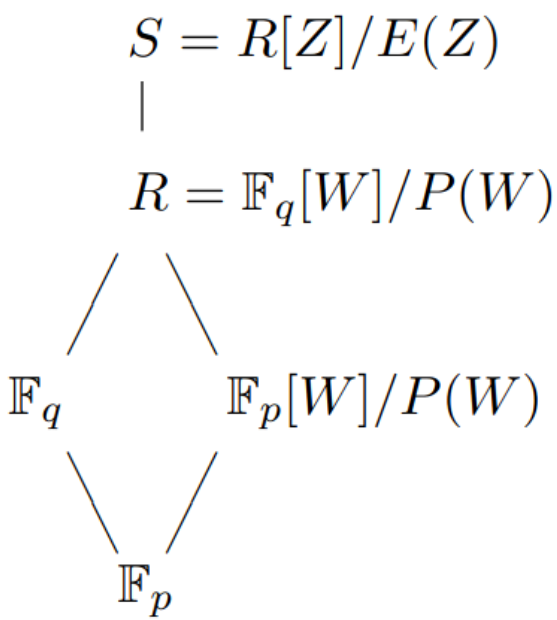

Figure: Extension ring

New algorithm for multipoint evaluation III

Lemma 5.1

$f(x_{0,\cdots x_{m-1}}) \in \mathbb{F}_q[x_0, \cdots x_{m-1}]$ with individual degrees $d-1$ and suppose $\mathbb{F}_q$ has characteristic p. Define h, R, E, S, ϕ, π as per the above construction and define the univariate polynomial $f^* \in S[Y]$ as

$$f^*(Y) := f(y,\ y^h, \cdots, y^{h^{m-1}})$$

For every $\alpha \in \mathbb{F}_q^m \subseteq R^m$ then $\pi(f^*\phi(\alpha)) = f(\alpha)$ holds where $\phi : R \to S$ and $\pi : S \to R$ is the projection map.

Proof: We outline a sketch of its proof here:

New algorithm for multipoint evaluation IV

- Fix $\phi(\alpha)$ an element of $R[Z]/E(Z)$ and take $g_\alpha \in R[\mathbb{Z}]$ be its (degree $m-1$) canonical representative, and denote by $\sigma^i(g_\alpha)$ the polynomial obtained by applying σ^i to the coefficients of g_α which implies:

$$\begin{aligned}(g_\alpha(Z))^{h^i} &= \sigma(\gamma_\alpha)(Z^{h^i}) \\ &= \sigma(\gamma_\alpha)(Z^{h^i-1}Z) \\ &= \sigma(\gamma_\alpha)(\eta^{(h^i-1)/(h-1)}Z)(\mod E(Z)) \\ &= \sigma(\gamma_\alpha)(\eta^i Z) \\ &\quad (\text{ since } \eta \text{ has order } h-1 \text{ thus stays fixed under } \sigma)\end{aligned} \tag{1}$$

- Denote $g_\alpha^{(i)}(Z) := (g_\alpha(Z))^{h^i} \mod E(Z)$. Note that $\deg(g_\alpha^{(i)}) = \deg(g_\alpha)$.

New algorithm for multipoint evaluation V

- From equation above we get:

$$g_\alpha^{(i)} = \sigma(g_\alpha)(\eta^i) = \sigma^i(g_\alpha(\sigma^{-i}\eta)) = \sigma^i g(\sigma^{-i}\alpha_i) = \alpha_i \tag{2}$$

  because η is fixed under σ.

- When we evaluate the polynomial f^* at the element of S whose canonical representative is g_α we get the element of S whose canonical representative is

$$f(g_\alpha^{(0)}(z), \cdots, g_\alpha^{(m-1)}(z))$$

  whose evaluation at 1 gives

$$f(g_\alpha^{(0)}(1), \cdots, g_\alpha^{(m-1)}(1))$$

  using equation 2, hence proved.

New algorithm for multipoint evaluation VI

Theorem 5.1

$f(x_0, \cdots x_{m-1}) \in \mathbb{F}_q[x_0, \cdots x_{m-1}]$ with individual degrees $\leq d-1$ and evaluation points $\alpha_0, \cdots \alpha_{d^m-1} \in \mathbb{F}_q^m$ there is an algorithm that outputs $f(\alpha_i)$ for $i = 0, \cdots d^m - 1$ in $\tilde{O}_{d^m}(d^m(m^2p)^m poly(d, p))$ many field operations.

Proof: Set $N = d^m$ and perform:

1. Choose $h = p^c$ to be the smallest power of p that is at least $m^2 d$ and find a degree c irreducible polynomial $P(W)$ over $\mathbb{F}_q$ and a primitive element η of $\mathbb{F}_q[W]/P(W)$. Define the ring $R = \mathbb{F}_q[W]/P(W)$ and the ring $S = R[Z]/E(Z)$ where $E(Z) = Z^{h-1} - \eta$
2. for $i = 0, 1, \cdots N-1$, compute the canonical representative of $\phi(\alpha_i)$: the degree $m-1$ polynomial $g_{\alpha_i}(Z) \in R[Z]$.
3. Produce the univariate polynomial $f^*(y) = f(y, y^h, \cdots y^{h^{m-1}})$ over S.

New algorithm for multipoint evaluation VII

4. Find f^* at the points $g_{\alpha_i}(Z)$ and for each evaluation apply π to recover $f(\alpha_i)$.

Analysis

- Step 1 requires constructing the field $\mathbb{F}_h$ and finding a primitive element which can be done by brute force in $poly(h)$ time.
- Each polynomial g_{α_i} computed in step 2 requires the operations:
  - Computing $\sigma^{-j}(\alpha_i)_j$ for $j = 0, 1 \cdots m-1$. Since a single field operation gives us $(\alpha_i)_j^{-1}$ and then using repeated squaring we can apply σ^j using at most $O(\log(h^m))$ $\mathbb{F}_q$ operations which overall takes $O(Nm^2 \log h)$ operations.
  - Perform N polynomial interpolations in R, each costing $O(M(m) \log m)$ operations in R or $O(M(m) \log mM(c))$ operations in $\mathbb{F}_q$.
  - For every two interpolation points η^i, η^j the difference $\eta^i - \eta^j$ is a unit in R which implies that the total cost of step 2 = $O(N(m^2 \log j + M(m) \log m)M(c))$ $\mathbb{F}_q$ operations.

New algorithm for multipoint evaluation VIII

- Step 3 is near-linear time evaluation of the univariate polynomial at a specific point.
- Step 4 is a univariate multiple evaluation problem, in the sense that, we have N elements of S and a univariate polynomial f^* over S of degree at most dmh^m which takes $O(M(dmh^m)\log(dmh^m)M(h)M(c))$ $\mathbb{F}_q$-operations but since $h \leq dm^2p$ and $poly(m)$ factors are polylogarithmic in the main size d^m, the claimed bound of the theorem follows.

New algorithm for multipoint evaluation IX

Corollary 5.1

The modular composition problem 1.2 with parameters $d, 1$ can be solved in $O(d^{1+o(1)})$ operations, provided the characteristic $p = d^{o(1)}$.

Proof: If we are able to choosem for any $\epsilon > 0$, the paramter $d_0 \leq d_\epsilon$ so that $m_0 := (\log d)/(\log d_0)$ that satisfies: $m_0 \leq d^\epsilon$ and $p^{m_0} \leq d^\epsilon$ then we can apply the theorem 5.1 for sufficiently large d (since $p \leq d^{o(1)}$) these demands are met by choosing $d_0 = \max\left\{(\log d)^{2/\epsilon}, p^{1/\epsilon}\right\}$.

Some applications

- The running time for polynomial factorization using Kaltofen & Shoup [KS95] in small characteristic has been improved using the modular composition.
- Running time of the testing irreducibility in [Rab80] is improved using this result yielding the asymptotically fastest irreducibility test in this setting.
- Kaltofen & Shoup's [KS95] algorithm to the problem of basis selection uses modular composition as well.
- Using the transposition principle the modular projection problem is solved using the modular composition problem in small characteristics and this leads to faster algorithms for computing minimal polynomials in these fields with small characteristics.

Future research in this direction

1. Given a monic squarefree polynomial $f \in \mathbb{F}_q[X]$ of degree n, a positive integer m and the polynomial $x^q \mod f(x)$, compute the polynomial

$$s_1(x)^{a_1} \cdots s_m(x)^{a_m} \mod f(x) = \prod_{i=1}^{m} (x^{q^i} - x)^{a_i} \mod f(x)$$

   for any positive integers a_i in $O(n^{1+o(1)})m^{o(1)}$ operations.
2. Improvement over the Brent & Kung [BK78] and Huang & Pan [HP98] algorithms for modular composition.
3. Extend this algorithm for fields to make it work in commutative rings of small characteristics.
4. If the strategy of dealing with multivariate polynomials by lifting to an extension ring and working with a related univariate polynomial can be extended to attack other problems as well.

References I

[BK78] Richard P Brent and Hsiang T Kung. "Fast algorithms for manipulating formal power series". In: *Journal of the ACM (JACM)* 25.4 (1978), pp. 581–595.

[HP98] Xiaohan Huang and Victor Y Pan. "Fast rectangular matrix multiplication and applications". In: *Journal of complexity* 14.2 (1998), pp. 257–299.

[KS95] Erich Kaltofen and Victor Shoup. "Subquadratic-time factoring of polynomials over finite fields". In: *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing*. 1995, pp. 398–406.

[Rab80] Michael O Rabin. "Probabilistic algorithms in finite fields". In: *SIAM Journal on computing* 9.2 (1980), pp. 273–280.

[Uma07] Christopher Umans. *Fast polynomial factorization, modular composition, and multipoint evaluation of multivariate polynomials in small characteristic*. 2007.

References II

[VZGG13] Joachim Von Zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge university press, 2013.

Thank you!