Faster Arithmetic over Multiple Algebraic Extensions

Cory Ahn, Michael Monagan (CECM, Simon Fraser University)

Motivation

Let $K = \mathbb{Q}(\alpha_1, \cdots, \alpha_t) \cong \mathbb{Q}[u_1, \cdots, u_t]/\langle m_1, \cdots, m_t\rangle$ be a number field with $t > 1$ extensions.

How should we perform arithmetic over K? (ex. multiply $f, g \in K[x]$)?

Overview of Strategy

1. Find a primitive element $\gamma = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_t\alpha_t$ of $\mathbb{Q}(\alpha_1, \cdots, \alpha_t)$ satisfying $\mathbb{Q}(\alpha_1, \cdots, \alpha_t) \cong \mathbb{Q}(\gamma)$, where $c_1, \cdots, c_t \in \mathbb{Z}$, and the minimal polynomial for γ, $m_\gamma(x) \in \mathbb{Q}[x]$.
2. Express α_i's as elements in $\mathbb{Q}(\gamma)$, $1 \le i \le t$.
3. Perform arithmetic in $\mathbb{Q}(\gamma)$.
4. Convert the result back to $\mathbb{Q}(\alpha_1, \cdots, \alpha_t)$.

In this poster, we only consider the case of $t = 2$. This idea is easily generalized to arbitrarily (finitely) many extensions. Moreover, for efficiency purposes we map the coefficient field $\mathbb{Q}$ to $\mathbb{Z}_p$, for an appropriate primes p and perform arithmetic over $\mathbb{Z}_p$, then convert the solution back to K using rational number reconstruction [3].

Example

Let $K = \mathbb{Q}(\alpha, \beta) \cong \mathbb{Q}[x, y]/\langle m_1, m_2\rangle$ where $m_1(y) = y^2 - 2$ and $m_2(x, y) = x^2 - 3$ are minimal polynomials for α and β respectively. Let $p = 17$ and let

$$r(x) = \text{res}_y(m_2(x - 1 \cdot y, y), m_1(y)) = x^4 + 7x^2 + 1 \in \mathbb{Z}_p[x].$$

Since $r(x)$ is square-free, $\mathbb{Z}_p(\alpha, \beta) \cong \mathbb{Z}_p(\gamma = \beta + 1 \cdot \alpha) \cong \mathbb{Z}_p[x]/\langle r(x)\rangle$ and $r(x) \in \mathbb{Z}_p[x]$ is the minimal polynomial (mod p) for γ. Furthermore, let

$$G := \text{gcd}(m_2(\gamma - 1 \cdot y, y), m_1(y)) = \text{gcd}(\gamma^2 - 3\gamma y + 1, y^2 - 2) = y + 8\gamma^3 + 13\gamma.$$

Thus $\alpha(\gamma) = y - G = -8\gamma^3 + 13\gamma$ and $\beta(\gamma) = \gamma - 1 \cdot \alpha(\gamma) = 8\gamma^3 + 14\gamma$.

Now we can work over one extension $K(\gamma)$ rather than in two extensions $K(\alpha, \beta)$.

Step 1: Finding a Primitive Element using Resultants

In what follows we let K be a field of characteristic 0 and let $m_1(x) \in K[x]$ and $m_2(x) \in K(\alpha)[x]$ be the minimal polynomials for α and β respectively.

Lemma 1. Let $f, g \in K[x, y]$. The **resultant** of f and g with respect to y, denoted by $\text{res}_y(f, g)$, is the polynomial r in $K[x]$ that satisfies

$$r(\alpha) = 0 \iff \text{gcd}(f(\alpha, y), g(\alpha, y)) \neq 1.$$

Definition 2. Let $f \in K[x]\backslash\{0\}$. We say that f is **square-free** iff $\text{res}_x(f, f') \neq 0$.

To find a **primitive element** γ satisfying $K(\alpha, \beta) \cong K(\gamma)$, we utilize Lemma 2:

Lemma 2 [1]. Let the field be $K(\alpha, \beta) = K[x, y]/\langle m_1, m_2\rangle$. If $m_2(x, \alpha) \in K(\alpha)[x]$ is square-free, then there exists $c \in \mathbb{Z}$ such that

$$r(x) := \text{res}_y(m_2(x - c \cdot y), m_1(y)) \in K[x]$$

is square-free. Furthermore, $r(x)$ is the minimal polynomial for a primitive element $\gamma = \beta + c \cdot \alpha$ of $K(\alpha, \beta)$ so that $K(\alpha, \beta) \cong K(\gamma) = K[x]/\langle r(x)\rangle$.

Let us call $c \in \mathbb{Z}$ which produces a non-square-free $\text{res}_y(m_2(x - cy), m_1(y))$ **unlucky**. One can characterize the number of unlucky $c \in \mathbb{Z}$ as follows.

Lemma 3. Let $r(x) = \text{res}_y(m_2(x - c \cdot y), m_1(y)) \in K[x]$ be as in Lemma 2. An element $c \in \mathbb{Z}$ is unlucky iff it is a root of

$$\text{res}_x(r(x), r'(x)) \in K[c].$$

One can express the number of unlucky c's in terms of the degrees of the minimal polynomials as follows.

Lemma 4. Let $d_1 = \deg_y(m_1)$ & $d_2 = \deg_x(m_2)$. The # of unlucky $c \in \mathbb{Z}$ is at most

$$\left[d_1^2 d_2(d_2 - 1)\right]/2.$$

By Lemma 2, to determine the minimal polynomial for a primitive element $\gamma = \beta + c\alpha$ we must compute the resultant of a <u>bivariate</u> $m_2(x - cy)$ and a <u>univariate</u> $m_1(y)$. For this we propose to use **evaluation & interpolation** in x at $\sigma_1, \sigma_2, \ldots \in \mathbb{Z}$.

Evaluation & interpolation reduces the problem of computing a bivariate resultant to that of computing a series of univariate resultants of $m_2(\sigma_i - cy, y)$ and $m_1(y)$ over K. To compute the univariate resultants, we use *polynomial remainder sequences*:

Definition 3. Let R be a ring and $f_1, f_2, \ldots, f_{k+1}$ be polynomials in $R[x]$. Then $\{f_1, f_2, \ldots, f_{k+1}\}$ is a **Polynomial Remainder Sequence (PRS)** if and only if:

- $\deg(f_1) \ge \deg(f_2)$,
- $f_i \neq 0$ for $i = 1, \ldots, k$ and $f_{k+1} = 0$, and
- $f_i = a_i \cdot \text{prem}(f_{i-2}, f_{i-1})$ for $i = 3, \ldots, k+1$ and $a_i \in R$.

There are numerous types of PRS's. We will use the *subresultant PRS* (sPRS) [2]. The last non-zero polynomial of sPRS starting from $f_1(x)$ and $f_2(x)$ equals $\text{res}_x(f_1, f_2)$.

Step 2: Finding $\alpha(\gamma), \beta(\gamma) \in K(\gamma)$

To perform arithmetic in $K(\gamma)$, one must represent α and β as elements in $K(\gamma)$, which we denote by $\alpha(\gamma)$ and $\beta(\gamma)$, respectively. For this we use the following lemma.

Lemma 5 [1]. Let $g(x, y) = m_2(x - c \cdot y, y)$ be square-free and let $\gamma = \beta + c \cdot \alpha$ (note that γ is a root of $g(x, \alpha)$). Then

$$G(\gamma, y) = \text{gcd}(g(\gamma, y), m_1(y)) = y - \alpha(\gamma) \in K(\gamma)[y].$$

Moreover, $\beta(\gamma) = \gamma - c \cdot \alpha(\gamma) \in K(\gamma)$.

Thus to obtain $\alpha(\gamma)$ and $\beta(\gamma)$ one could compute a gcd over $K(\gamma)$. For efficiency, we instead propose to use the sPRS's computed in Step 1 as follows.

1. Obtain $\deg_y(m_1) \cdot \deg_x(m_2)$ next-to-last polynomials appearing in the sPRS starting from $m_2(\beta - cy, y)$ and $m_1(y)$, which are linear in y.
2. Interpolate polynomials in step 1 to get $G(x, y) \in K[y][x]$.
3. Solve $G(x = \gamma, y) = 0$ to obtain $\alpha(\gamma)$.
4. Find $\beta(\gamma)$ using the formula $\gamma - c\alpha(\gamma)$.

Recall that $K = \mathbb{Q}(\alpha, \beta) \cong \mathbb{Q}[x, y]/\langle m_1, m_2\rangle$. One can show that all the above lemmas apply to the *ring* $\Phi_p(K) = \mathbb{Z}_p[x, y]/\langle m_1 \mod p,\ m_2 \mod p\rangle$ as long as p is "appropriately" chosen and no zero divisors are encountered during computation.

Unfortunately, not all elements in $\mathbb{Z}_p$ can be used as evaluation points:

Bad and Unlucky Evaluation points

(1) For the resultant computation, we must not choose any evaluation points that decrease the degree of y in m_2 (called **bad evaluation points**).
(2) For the gcd computation, we must also not choose evaluation points that decrease the degree of y in *any* polynomial in the sPRS (called **unlucky** evaluation points).

We provide two example cases in which unlucky evaluation points are encountered.

Ex 1. The sPRS starting from $m_1(y) = y^3 - 2y^2 - 1$ and $g(x, y) = x^2 - 5xy^2 - x + 4$ over $\mathbb{Z}_{17}[x]$ is:

$$f_1(x, y) = m_1(y) = y^3 - 2y^2 - 1,\quad f_2(x, y) = g(x, y) = x^2 - 5xy^2 - x + 4,$$
$$f_3(x, y) = (5x^3 + 12x^2 + 3x)y + 7x^3 + 2x^2 + 11x,$$
$$f_4(x, y) = x^6 + 11\,x^5 + 6\,x^4 + 8\,x^3 + 7\,x^2 + 6\,x + 13,\quad f_5(x, y) = 0.$$

On the other hand, the sPRS starting from $m_1(y)$ and $g(x = 6, y)$ is:

$$\hat{f}_1(y) = y^3 + 15\,y^2 + 10,\quad \hat{f}_2(y) = 4y^2,\quad \hat{f}_3(y) = 13,\quad \hat{f}_4(y) = 0.$$

The next-to-last polynomial $\hat{f}_2$ is not linear and is not equal to $f_3(x = 6, y)$.

Ex 2. The sPRS starting with $m_1(y) = y^4 + 15 + 11\,y^2$ and $g(x, y) = x^3 + 8\,yx + 15\,y^3$ over $\mathbb{Z}_{17}[x]$ is:

$$f_1(x, y) = m_1(y) = y^4 + 15 + 11\,y^2,\quad f_2(x, y) = g(x, y) = x^3 + 8\,yx + 15\,y^3,$$
$$f_3(x, y) = (10 + 16x)y^2 + 2x^3y + 9,$$
$$f_4(x, y) = (15x^6 + 11 + 2x^3 + 11x^2)y + 13x^5 + 12x^4 + 16x^3,$$
$$f_5(x, y) = x^{12} + 8 + 7\,x^8 + 5\,x^7 + 12\,x^6 + 2\,x^4 + 11\,x^3 + 4\,x^2 + 5\,x,\quad f_6(x, y) = 0.$$

On the other hand, the sPRS starting with $m_1(y)$ and $g(x = 10, y)$ is:

$$\hat{f}_1(y) = m_1(y),\quad \hat{f}_2(y) = 15y^3 + 12y + 14,\quad \hat{f}_3(y) = 11y + 9,\quad \hat{f}_4(y) = 11,\quad \hat{f}_5(y) = 0.$$

The next-to-last polynomial is linear, but corresponds to the degree 2 polynomial, f_3.

Theorem 1. Let $d_1 = \deg_y(m_1)$ and $d_2 = \deg_x(m_2)$.
The number of bad evaluation points in $\mathbb{Z}$ is at most d_2.
The number of unlucky evaluation points in $\mathbb{Z}$ is at most $d_2 d_1(d_1 + 1)/2$.

Theorem 1 implies that the number of unlucky evaluation points is "small".
We do not know *a priori* the number of polynomials in the sPRS of $m_\gamma(y)$ and $g(x, y)$.
Hence to detect an unlucky evaluation point, we proceed as follows.
Let $k = \#$ of polynomials in the sPRS obtained using the first evaluation point.

1. Compute sPRS using the next evaluation point. Let $S = (\#$ polynomials in sPRS$)$.
2. a) If $S < k$, discard current sPRS.
   b) If $S > k$, discard all previous sPRS's. Set k to S.
   c) If $S = k$, keep the sPRS. Go to step 1.

Cost

Theorem 2. Let $d_1 = \deg(m_1)$ and $d_2 = \deg(m_2)$. The overall cost of computing the <u>resultant</u> over $\mathbb{Z}_p$ and the <u>gcd</u> above over $\mathbb{Z}_p[x]/\langle m_\gamma(x) \mod p\rangle$ is

$$\mathcal{O}\left(\left[d_1^3 d_2 + d_1^2 d_2^2)\right] + d_1^4\right) \text{ arithmetic operations in } \mathbb{Z}_p.$$

[Remark: if $d_1 \le d_2$, this cost simplifies to $\mathcal{O}(d_1^2 d_2^2)$.]

In comparison, the costs of computing the resultant and the gcd using the Euclidean algorithm are $\mathcal{O}(d_1^4 d_2^2)$ *each*.

References

[1] Trager, B. *Algebraic Factoring and Rational Function Integration*. Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation, 1976.

[2] Collins, G.E. *The calculation of multivariate polynomial resultants*. J. Assoc. Comput. Mach. 18 (1971), 515-532.

[3] Monagan, M. *Maximal Quotient Rational Reconstruction: An Almost Optimal Algorithm for Rational Reconstruction*. Proceedings of ISSAC '04, ACM Press, p. 243-249, 2004.