POWER RESIDUE SYMBOL ORDER DETECTING ALGORITHM FOR SUBSET PRODUCT OVER ALGEBRAIC INTEGERS

TREY LI

ABSTRACT. We give a probabilistic polynomial time algorithm for high $\mathbb{F}_\ell$-rank subset product problem over the order $\mathcal{O}_K$ of any algebraic field K with $\mathcal{O}_K$ a principal ideal domain and the ℓ-th power residue symbol in $\mathcal{O}_K$ polynomial time computable, for some rational prime ℓ.

1. INTRODUCTION

In [Li22a] we proposed the unique factorization domain subset product problem (USP), and showed that it is generally NP-hard for all unique factorization domains (UFD) with efficient multiplication. A special case of the problem is the classical subset product problem (SP) over $\mathbb{Z}$ [GJ79]. Later in [Li22b] we proposed the *Jacobi symbol parity checking algorithm* to solve high $\mathbb{F}_2$-rank SP in probabilistic polynomial time. Now we extend the algorithm to deal with USP. We show that high $\mathbb{F}_\ell$-rank USP over any UFD number order $\mathcal{O}_K$ with efficient power residue symbol computation can be solved in probabilistic polynomial time, where ℓ is some rational prime such as 2.

2. USP OVER $\mathcal{O}_K$

Let $K = \mathbb{Q}[X]/(f(X))$ be a number field with its order $\mathcal{O}_K$ a principal ideal domain (PID). Note that every number ring is a Dedekind domain; and a Dedekind domain is a UFD if and only if it is a PID. Hence an order is a UFD if and only if it is a PID. Therefore $\mathcal{O}_K$ is a UFD. Typical examples include rational integers $\mathbb{Z}$, Gaussian integers $\mathbb{Z}[i]$, and the integers $\mathbb{Z}[e^{\frac{2\pi i}{n}}]$ with $1 \le n \le 22$, etc.

Since $\mathcal{O}_K$ is a UFD, we can talk about USP over $\mathcal{O}_K$. USP over $\mathcal{O}_K$, denoted USP/$\mathcal{O}_K$, is given $n+1$ elements $a_1, \dots, a_n, X \in \mathcal{O}_K$, find a binary vector $(x_1, \dots, x_n) \in \{0,1\}^n$ such that

$$\prod_{i=1}^{n} a_i^{x_i} = X.$$

Note that SP is the special USP/$\mathcal{O}_K$ with $K = \mathbb{Q}$ and $\mathcal{O}_K = \mathbb{Z}$.

Let $p_1, \dots, p_m$ be the distinct prime factors of $a_1, \dots, a_n$. A matrix $A \in \mathbb{Z}^{m \times n}$ is called a *characteristic matrix* of the USP/$\mathcal{O}_K$ instance $(a_1, \dots, a_n, X)$ if

$$a_i = \prod_{j=1}^{m} p_j^{A_{j,i}}$$

for all $i \in n$. We call the row rank of A (over any field) the *rank* of the USP/$\mathcal{O}_K$ instance (over the same field).

This is the 3rd paper of the series. Previously: [Li22a; Li22b].

Date: October 3, 2022.

Email: treyquantum@gmail.com

Note that a USP/$\mathcal{O}_K$ instance can have different characteristic matrices for different orderings of the primes $p_1,\ldots,p_m$. But the rank (over a specified field) is an invariant of a USP/$\mathcal{O}_K$ instance.

3. Algorithm

Step 1. Choose $k \geq m$ random ideals $\mathfrak{s}_1,\ldots,\mathfrak{s}_k$ of $\mathcal{O}_K$ and a rational prime $\ell \geq 2$ such that the ℓ-th power residue symbols $\left(\frac{\cdot}{(p_i)}\right)_\ell$ are well-defined[1] for all prime factors $p_1,\ldots,p_m$ of $a_1,\ldots,a_n$.[2]

Step 2. Take the ℓ-th power residue symbols for the equation

$$\prod_{i=1}^{n} a_i^{x_i} = X$$

above $\mathfrak{s}_1,\ldots,\mathfrak{s}_k$ respectively to get a system of k equations of the form

$$\prod_{i=1}^{n} \left(\frac{a_i}{\mathfrak{s}_j}\right)_\ell^{x_i} = \left(\frac{X}{\mathfrak{s}_j}\right)_\ell,$$

for $j \in [k]$.

Step 3. Extract from the above system a matrix equation

$$Bx \equiv b \pmod{\ell}$$

over $\mathbb{Z}_\ell$, where $B \in \{0,\ldots,\ell-1\}^{k\times n}$ and $b \in \{0,\ldots,\ell-1\}^k$ with

$$B_{j,i} = \operatorname{ord}\left(\left(\frac{a_i}{\mathfrak{s}_j}\right)_\ell\right),\ b_j = \operatorname{ord}\left(\left(\frac{X}{\mathfrak{s}_j}\right)_\ell\right)$$

the orders of the ℓ-th power residue symbols, which are elements of the group of ℓ-th roots of unity $\mu_\ell = \{1,\zeta,\ldots,\zeta^{\ell-1}\}$ generated by the ℓ-th primitive root of unity ζ.

We call B the characteristic matrix of the ℓ-th residue symbol matrix

$$\left\{\left(\frac{a_i}{\mathfrak{s}_j}\right)_\ell\right\}_{j\in[k],i\in[n]}$$

and b the characteristic vector of the ℓ-th power residue symbol vector

$$\left(\left(\frac{X}{\mathfrak{s}_j}\right)_\ell\right)_{j\in[k],i\in[n]}$$

.

Step 4. Search from the solutions of $Bx \equiv b \pmod{\ell}$ for one that satisfies $\prod_{i=1}^{n} a_i^{x_i} = X$.

[1]By well-define we mean that $N((p_i)) \equiv 1 \pmod{\ell}$ so that by the analogue of Fermat's theorem $a^{N((p_i))-1} \equiv 1 \pmod{(p_i)}$ for any $a \in \mathcal{O}_K - (p_i)$, the number $a^{\frac{N((p_i))-1}{\ell}}$ is "well-defined", namely $a^{\frac{N((p_i))-1}{\ell}} \equiv \zeta^k \pmod{(p_i)}$ for a *unique* ℓ-th root of unity ζ^k, where ζ is a primitive ℓ-th root of unity and $k \in \{0,\ldots,\ell-1\}$, also $N((p_i))$ is the norm of the principal ideal (p_i) generated by the prime element p_i,

[2]Here we do not assume that the prime factors $p_1,\ldots,p_m$ of $a_1,\ldots,a_n$ are given. But it is fair to assume that such an ℓ is given or known because $\ell = 2$ is always a valid choice.

4. MAXIMIZING RANK(B)

We want to maximize the rank of B in order to minimize the solution set of

$$Bx \equiv b \pmod{\ell}$$

and reduce the searching complexity of Step 4.

Note that B decomposes as

$$B = PA,$$

where $P \in \{0,\dots,\ell-1\}^{k\times m}$ is the characteristic matrix of the ℓ-th residue symbol matrix

$$\left\{\left(\frac{p_i}{\mathfrak{s}_j}\right)_\ell\right\}_{j\in[k],i\in[m]}$$

with respect to the prime factors $p_1,\dots,p_m$ of $a_1,\dots,a_n$, and $A = \{A_{j,i}\}_{m\times n}$ is the characteristic matrix of the USP/$\mathcal{O}_K$ with respect to the prime sequence $(p_1,\dots,p_m)$. Hence

$$\mathrm{rank}_{\mathbb{F}_\ell}(B) = \mathrm{rank}_{\mathbb{F}_\ell}(PA) \le \mathrm{rank}_{\mathbb{F}_\ell}(A) \le \min\{m,n\}.$$

In order to maximize $\mathrm{rank}_{\mathbb{F}_\ell}(B)$, we want to maximize $\mathrm{rank}_{\mathbb{F}_\ell}(P)$ to m. We show by the following lemma that for any $\ell \ge 2$ such that the ℓ-th power residue symbols $\left(\frac{\cdot}{(p_i)}\right)_\ell$ are well-defined, i.e., $N((p_i)) \equiv 1 \pmod{\ell}$ for all $i \in [m]$, there exist m ideals $\mathfrak{s}_1,\dots,\mathfrak{s}_m$ such that the characteristic matrix $P \in \{0,\dots,\ell-1\}^{m\times m}$ of the ℓ-th power residue symbol matrix $\{(p_i/s_j)_\ell\}_{j\in[m],i\in[m]}$ is of full $\mathbb{F}_\ell$-rank. In particular, the following lemma is about finding one $\mathfrak{s}_i$ to achieve one row $P_{i,*}$ which can be any vector in $\{0,\dots,\ell-1\}^m$.

LEMMA 1. Let $p_1,\dots,p_m \in \mathcal{O}_K$ be distinct primes and let $\ell \ge 2$ be a positive integer such that the norms $N((p_i)) \equiv 1 \pmod{\ell}$ for all $i \in [m]$. Then for any vector $v \in \mu_\ell^m$, there exists an ideal $\mathfrak{s} \subset \mathcal{O}_K$ such that the vector of the ℓ-th power residue symbols $((p_1/\mathfrak{s})_\ell,\dots,(p_m/\mathfrak{s})_\ell) = v$.

Proof. We want to find $\mathfrak{s}$ such that

$$\left(\frac{p_i}{\mathfrak{s}}\right)_\ell = v_i$$

for all $i \in [m]$. By assumption, $\mathcal{O}_K$ is a principal ideal domain. Let $\mathfrak{s} = (s)$. Our goal is to find $s \in \mathcal{O}_K$.

At the very least, for the ℓ-th power residue symbol above (s) to be well-defined, we require that the norm

$$N((s)) \equiv 1 \pmod{\ell},$$

for which it is sufficient to require that

$$s \equiv 1 \pmod{(\ell)}. \tag{1}$$

Now we show how to satisfy v. Let (p_i) be the principal ideal generated by p_i, for $i = 1,\dots,m$. They are prime ideals since in any integral domain, an element is prime if and only if the principal ideal generated by it is a prime ideal.

Let

$$\eta := \prod_{\mathfrak{p}\mid m\infty}\left(\frac{p_i,s}{\mathfrak{p}}\right)$$

be the Hilbert symbol. By the power reciprocity law,

$$\left(\frac{p_i}{(s)}\right)_\ell = \left(\frac{s}{(p_i)}\right)_\ell \cdot \eta.$$

Hence our goal is to find s such that

$$\left(\frac{s}{(p_i)}\right)_\ell = \eta \cdot v_i,$$

i.e.,

$$s^{\frac{N((p_i))-1}{\ell}} \equiv \eta \cdot v_i \pmod{(p_i)}, \tag{2}$$

for all $i \in [m]$.

By the generalized Chinese remainder theorem (CRT), there is a unique solution $s \in \mathcal{O}_K/((\ell)\prod_{i=1}^{m}(p_m))$ to the $m+1$ equations given by (1) and (2). □

5. Theorem

We state the theorem in terms of average-case USP with uniform characteristic matrix. The conclusion about best-case USP with high rank characteristic matrix, as stated in Abstract and Introduction, is implied.

Theorem 1. Let $m, n \in \mathbb{N}$ with $m \geq n$. Let $\mathcal{O}_K$ be the order of a number field K such that $\mathcal{O}_K$ is a PID. Let $p_1, \ldots, p_m$ be m random prime elements of $\mathcal{O}_K$. Let ℓ be a rational prime such that the ℓ-th power residue symbols $\left(\frac{\cdot}{(p_i)}\right)_\ell$ are well-defined for all the ideals $(p_1), \ldots, (p_m)$. Let d be a multiple of ℓ. Assume polynomial time algorithms to compute ℓ-th power residue symbols in $\mathcal{O}_K$. There exists a probabilistic polynomial time algorithm that solves USP/$\mathcal{O}_K$ with uniform characteristic matrix $A \in \mathbb{Z}_d^{m\times n}$ (with respect to the prime elements $p_1, \ldots, p_m$) with probability $\gtrapprox \prod_{i=m-n+1}^{m}(1 - 1/\ell^i)$.

Proof. Consider the algorithm given in Section 3 (with potential improvement of using different ℓ's parallelly). By the randomness of $p_1, \ldots, p_m$ (and possibly different ℓ's), we expect that by polynomially many random elements $s_1, \ldots, s_k$, the $\mathbb{F}_\ell$-rank of $P \in \{0, \ldots, \ell-1\}^{k\times m}$ achieves m with overwhelming probability. I.e., $\text{rank}_{\mathbb{F}_\ell}(B) = \text{rank}_{\mathbb{F}_\ell}(A)$ with overwhelming probability.

Again, the probability [BKW97; Coo00] that a uniform matrix in $\mathbb{F}_\ell^{m\times n}$ with $m \geq n$ is of full $\mathbb{F}_\ell$-rank is

$$p = \prod_{i=m-n+1}^{m}(1 - \frac{1}{\ell^i}).$$

Now $A \in \mathbb{Z}_d^{m\times n}$ and d is a multiple of ℓ. Hence $A \pmod{\ell}$ is uniform over $\mathbb{F}_\ell$ and that it is of full $\mathbb{F}_\ell$-rank with probability p.

If A is really full rank, we solve for the unique x and check if it gives a solution to the SP. Else if A is not full rank but close to full rank, we can still check all solutions of $Bx \equiv b \pmod{\ell}$ and see if there is one that satisfies the SP. Hence the probability of solving SP is $\geq p$ assuming $\text{rank}_{\mathbb{F}_\ell}(B) = \text{rank}_{\mathbb{F}_\ell}(A)$.

Combining the overwhelming probability of $\text{rank}_{\mathbb{F}_\ell}(B) = \text{rank}_{\mathbb{F}_\ell}(A)$, we have the claimed probability of $\gtrapprox p$. □

The following corollary is more intuitive.

Corollary 1. Let $m, n, d \in \mathbb{N}$ with $m \geq 2n$, and $d \geq 2$ even. Assume polynomial time algorithms to compute power residue symbols in $\mathcal{O}_K$. There exists a probabilistic polynomial time algorithm that solves average-case USP/$\mathcal{O}_K$ with uniform characteristic matrix $A \in {}^{m\times n}_{d}$ with overwhelming probability.

Proof. Note that $\ell = 2$ is always a "good" rational prime such that the ℓ-th power residue symbols $\left(\frac{\cdot}{(q)}\right)_\ell$ are well-defined (i.e. $N((q)) = 1 \pmod 2$) for all prime elements $q \in \mathcal{O}_K$. Hence we can always take $\ell = 2$.

Also note that d is even, which is a multiple of $\ell = 2$. Hence the argument about the full $\mathbb{F}_\ell$-rank probability p in the proof of Theorem 1 is completely inherited.

Now simply plug $\ell = 2$ and $m \geq 2n$ in p and we have that $\mathrm{rank}_{\mathbb{F}_\ell}(A) = n$ with probability

$$p = \prod_{i=m-n+1}^{m} \left(1 - \frac{1}{\ell^i}\right) = \prod_{i=m-n+1}^{m} \left(1 - \frac{1}{2^i}\right) \geq \prod_{i=n+1}^{2n} \left(1 - \frac{1}{2^i}\right) > \left(1 - \frac{1}{2^n}\right)^n,$$

which is overwhelming in n. □

References

[BKW97] Johannes Blömer, Richard Karp, and Emo Welzl. "The rank of sparse random matrices over finite fields". In: *Random Structures & Algorithms* 10.4 (1997), pp. 407–419.

[Coo00] Colin Cooper. "On the distribution of rank of a random matrix over a finite field". In: *Random Structures & Algorithms* 17.3-4 (2000), pp. 197–212.

[GJ79] Michael R Garey and David S Johnson. *Computers and intractability*. Vol. 174. freeman San Francisco, 1979.

[Li22a] Trey Li. "Subset Product with Errors over Unique Factorization Domains and Ideal Class Groups of Dedekind Domains". 1st paper of the series. 2022, October 1.

[Li22b] Trey Li. "Jacobi Symbol Parity Checking Algorithm for Subset Product". 2nd paper of the series. 2022, October 2.