DISCRETE EXPONENTIAL EQUATIONS AND NOISY SYSTEMS

TREY LI

ABSTRACT. The history of equations dates back to thousands of years ago, though the equals sign "=" was only invented in 1557. We formalize the processes of *decomposition* and *restoration* in mathematics and physics by defining *discrete exponential equations* and *noisy equation systems* over an abstract structure called a *land*, which is more general than fields, rings, groups, and monoids. Our abstract equations and systems provide general languages for many famous computational problems such as integer factorization, ideal factorization, isogeny factorization, learning parity with noise, learning with errors, learning with rounding, etc. From the abstract equations and systems we deduce a list of new decomposition problems and noisy learning problems. We also give algorithms for discrete exponential equations and systems over algebraic integers. Our motivations are to develop a theory of decomposition and restoration; to unify the scattered studies of decomposition problems and noisy learning problems; and to further permeate the ideas of decomposition and restoration into all possible branches of mathematics. A direct application is a methodology for finding new hardness assumptions for cryptography.

1. INTRODUCTION

Recall that when we were in primary school, we saw equations like $1+1=2$; when we were in middle school, we saw equations like $\sin^2 x+\cos^2 x=1$ and $ax^2+bx+c=0$; when we were in high school and university, we saw equations like $\frac{\partial z}{\partial x}+\frac{\partial z}{\partial y}=a$ (differential equations), $y^2=\int_a^x xyd\,y$ (integral equations), and $Ax=b$ (matrix equations), etc. As our studies went further, we saw more and more different kinds of equations. They are mostly equations over numbers of some number field/ring, and the equals sign "=" (invented by Robert Recorde in 1557 [San57]) denotes exact equality.

In this paper we study equations of the form

$$a_1^{x_1}\cdots a_n^{x_n}\approx a,$$

where "$\approx$" is a generalization of the equals sign "=" to also capture the isomorphism sign "$\cong$", and $a_1,\ldots,a_n,a$ are from an abstract structure called a *land*, which is a monoid without the axiom of associativity. In particular, $a_1,\ldots,a_n,a$ can be numbers, sets, groups, rings, ideals, varieties, modules, lattices, functions, etc. Also, the binary operation "$\cdot$" can be normal multiplication of numbers, intersection or union of sets, direct product (Cartesian product) of groups, direct sum of modules, function composition of isogenies, and even non-associative operations like subtraction and division, etc. We call this kind of equations *discrete exponential equations*.

We further study systems of noisy equations of the form

$$a_1^{x_1}\cdots a_n^{x_n}\cdot e\approx a$$

This is the 8th paper of the series. Previously: [Li22a; Li22b; Li22c; Li22d; Li22e; Li22f; Li22g].
Date: October 8, 2022.
Email: treyquantum@gmail.com

over some land, where $a_1,\ldots,a_n,a$ are given but e is not given. We call this kind of equation systems *noisy equation systems*.

The abstract equations and systems capture some famous algorithmic problems such as integer factorization [Gal12], ideal factorization [HM89], isogeny factorization [CLG09], learning parity with noise (LPN) [BMT78; BFKL94], learning with errors (LWE) [Reg09] learning with rounding (LWR) [BPR12], and the recently proposed multiple modular unique factorization domain subset product with errors problem [Li22d; Li22e; Li22f; Li22g] and multiple modular subset sum with errors problem [Li22d; Li22g]. In fact, the abstract equations and systems reveal the two most common patterns of hard problems in cryptography: decomposition and noisy learning.

Another angle to look at this work is to treat it as a further generalization of the (already quite general) subset product and subset product with errors problems in [Li22a; Li22d] from the area of algebraic number theory to more branches of mathematics such as algebraic geometry, topology, lattice theory, etc.

In the rest of the paper, we discuss the philosophy and motivation of our theory; define the abstract equations and systems; show how the existing problems are captured by the equations and systems; propose new decomposition and noisy learning problems in different mathematical branches; and give basic algorithms for some of them.

2. PHILOSOPHY

It all starts with our consideration about the phenomena of *generation/decomposition* and *distortion/restoration* in mathematics and physics. They reflect two fundamental instincts of human beings: synthesizing/analyzing things and finding causes from effects.

2.1. GENERATION AND DECOMPOSITION.

The concept of generation is everywhere in different branches of mathematics. To see this, just to think about various names like group generators, ring generators, ideal generators, topology generators, basis of vector space, basis of lattice, basis of algebra, etc.

The opposite concept is decomposition, which is about splitting an object into parts. Examples include integer factorization, group decomposition, ideal factorization, variety factorization, isogeny factorization, etc. A special case is irreducible decomposition, which decomposes an object into irreducible parts. For example, integer factorization. We call irreducible decomposition *factorization*.

A decomposition problem can be asked in two different ways. One is only given an object and asks to find all its irreducible components as well as their multiplicities. The other is given an object as well as a range of potential (often reducible) components and asks to find the multiplicities only.

We notice that both cases can be put into a single language, which we call *discrete exponential equations*. This general language provides a systematic methodology to discover new problems.

2.2. DISTORTION AND RESTORATION.

Problems about "finding causes from effects" are called *inverse problems* [Tar05; KS06]. But the effects are usually distorted by noise in the environment before being observed. Hence the difficulty is about how to recover the causes from the distorted effects. Two

typical examples are signal recovery and image recovery, which are given a list of distorted signals or images, recover the original signals or images.

There are at least two differences between our treatment and the traditional study of inverse problems. First is that we mainly care about problems with discrete solutions. Second is that the range of our study is not limited to science/analysis but pure mathematics. We explain the two differences in the following.

Problems from nature are mostly continuous. Hence many inverse problems are defined over real numbers $\mathbb{R}$. For example, the linear inverse problem with Gaussian noise [FNT10, p.24, p.123] is indeed LWE over $\mathbb{R}$ and with solutions in $\mathbb{R}$. Note that solving for continuous solutions to LWE over $\mathbb{R}$ is relatively easy [Tar05; KS06]; but finding discrete solutions to LWE over a finite field $\mathbb{F}_q$ is extremely hard [BLPRS13; APS15]. Hence with the mindset of "hard to solve $\Longrightarrow$ interesting", we mainly study noisy equation systems with discrete solutions.

Also, inverse problems are mostly about the physical world around us. Hence they mostly belong to the branch of analysis, involving metric theory, measure theory, probability theory, functional analysis, etc. However, there is a big whole universe of pure mathematics outside the scope of science and analysis. We therefore try to permeate the phenomenon of noisy distortion into all existing branches of mathematics, and define new noisy learning problems in algebraic number theory, algebraic geometry, topology, lattice theory, abstract algebra, linear algebra, etc.

3. Discrete exponential equations

If we look at decomposition from the perspective of equation solving, a decomposition problem is in fact an equation solving problem that asks to solve an equation of the form

$$a_1^{x_1}\cdots a_n^{x_n}=a$$

for integers $x_1,\dots,x_n\in\mathbb{Z}$, where the multiplication is an abstract binary operation, and $a_i^0:=1$ means that a_i is not a component of a.

Note that there is no need to list all the bases $a_1,\dots,a_n$ out to represent the equation. For example, for integer factorization, we can represent the bases $a_1,\dots,a_n$ by some conditional statement like "prime AND $\le\sqrt{a}$", which is a small representation of size polynomial in the bit length $\lceil\log_2 a\rceil$ of a, even if the number of potential prime factors is exponential.[1]

Also, we do not need to print all entries $x_1,\dots,x_n$ of a solution $(x_1,\dots,x_n)$ after finding it. We can simply print the nonzero entries.[2]

We define this kind of abstract equations below.

3.1. Land.

The first thing is to define the ground structure, i.e., where $a_1,\dots,a_n,a$ live.

At the very least, it should be a set. Again, to have expressions like $a_1^{x_1}\cdots a_n^{x_n}$, there should be a binary operation. Also, to define $a^0:=1$, there should be an identity 1.

These conditions lead to our definition of lands.

Definition 1. A *land* is a set with a binary operation and an identity.

[1] We shall keep in mind that the complexity of an algorithm is measured in the bit length of its input, i.e., the bit length of the problem description.

[2] Note that the number of nonzero entries must be $\le\log_2 a$ because the factors of a are all ≥ 2.

In other words, a land is a semigroup with identity but without requiring associativity; or a monoid without requiring associativity. Typical examples include groups, rings, fields, topologies (with the operation to be set intersection), σ-algebras (with the operation to be set union), etc. A special example is the set of integers with subtraction $(\mathbb{Z}, -)$. It is a land but not a group, a monoid, nor a semigroup because subtraction does not satisfy associativity.

Let L be a land with identity 1. An element $a \in L$ is said to be *invertible* if there is an element $b \in L$ such that $ab = 1$. An invertible element $a \in L$ is called a *unit*. An element $a \in L$ is said to be *irreducible* if it is neither a unit nor the product of two non-units. The land L is called a *unique factorization land* if every non-unit has a unique factorization into non-units, where the uniqueness is up to ordering of the factors and rescaling the non-units by units.

3.2. **Land isomorphism.**

Similar to the structure-preserving maps between other objects such as homomorphisms between groups, linear transformations between vector spaces, continuous functions between topological spaces, and isogenies between varieties, we define homomorphisms between lands.

Definition 2. A *land homomorphism* from a land $(A, *)$ to a land $(B, \cdot)$ is a function $\varphi : A \to B$ such that for all $a \in A$ and $b \in B$ it holds that $\varphi(a * b) = \varphi(a) \cdot \varphi(b)$.

Definition 3. A *land isomorphism* is a bijective land homomorphism.

Example. Let $(\mathbb{Z}, -)$ be the land of integers with subtraction. Let $(2\mathbb{Z}, -)$ be the land of even numbers with subtraction. Then the map $\varphi : (\mathbb{Z}, -) \to (2\mathbb{Z}, -); a \mapsto a - (0 - a)$ is a land homomorphism because $\varphi(a - b) = (a - b) - (0 - (a - b)) = (a - b) - (-(a - b)) = (a - b) - (b - a) = (a - (-a)) - (b - (-b)) = (a - (0 - a)) - (b - (0 - b)) = \varphi(a) - \varphi(b)$. It is also a land isomorphism because integers and even integers are 1-to-1 corresponding and if we define $2a := a - (0 - a)$ then $\varphi : a \mapsto a - (0 - a)$ is actually $\varphi : a \mapsto 2a$, i.e., it maps integers to even integers.

3.3. **Discrete exponential equations.**

Let L be a land. Denote its identity as 1. Let $a \in L$ and $n \in \mathbb{N}$. Define $a^n := \prod_{i=1}^{n} a$ and $a^0 := 1$. Define $\approx$ to mean equality or land isomorphism[3].

Definition 4. A *discrete exponential equation* over a land L is an equation of the form

$$\prod_{i=1}^{n} a_i^{x_i} \approx a,$$

where $a_1, \ldots, a_n, a \in L$. A solution to the equation is an integral vector $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ that satisfies the equation. We call $a_1, \ldots, a_n$ the *bases* and a the *target*.

[3]There is a little conceptual problem here. We suggest that "$\approx$" is different from "$\cong$". One might think that when we write $A \cong B$, it already captures the possibility of $A = B$. However, this makes sense only when the concept of isomorphism is well-defined between A and B. For a counter example, when A and B are two integers, it does not make sense to say that A and B are isomorphic. But it makes sense to write $A \approx B$ because "$\approx$" means "isomorphic to" *or* "equals to", where the first meaning is taken only when the concept of isomorphism exists, regardless whether it captures equality; but the second meaning can be taken even when the concept of isomorphism does not exist.

Let L be a unique factorization land. Let $p_1,\dots,p_m$ be all the irreducible factors of $a_1,\dots,a_n$. We call a matrix $M \in \mathbb{Z}^{m\times n}$ a *characteristic matrix* of the discrete exponential equation if $a_i = \prod_{i=1}^m p_i^{M_{i,j}}$ for all $j \in n$. We call the row rank of M (over any field) the *rank* of the equation (over the same field). Note that there can be different characteristic matrices of a discrete exponential equation depending on the ordering of the irreducible factors. But the rank is an invariant of a discrete exponential equation over a unique factorization land.

3.4. WELL-KNOWN PROBLEMS.

Following are examples of irreducible decomposition.

Integer factorization. The problem is given a positive integer $a \in \mathbb{Z}_{>0}$, find primes $p_1,\dots,p_m$ and positive integers $x_1,\dots,x_m \in \mathbb{Z}_{>0}$ such that $\prod_{i=1}^m p_i^{x_i} = a$.

In the language of discrete exponential equations, it is to solve the equation

$$\prod_{i=1}^w p_i^{x_i} = a$$

for nonnegative integers $x_1,\dots,x_w \in \mathbb{Z}_{\geq 0}$, where $p_1,\dots,p_w$ are all the primes $\leq \sqrt{a}$.

Recall that we do not need to list all the bases $p_1,\dots,p_w$ out to describe the equation (but a rule like "prime AND $\leq \sqrt{a}$"); nor to list all the exponents $x_1,\dots x_w$ out to describe an answer (but the nonzero ones).

Ideal factorization [HM89]. Let $Cl(K)$ be the ideal class group of a number field K. It is an abelian group. Assuming the generalized Riemann hypothesis, $Cl(K)$ is generated by prime ideals of norm $\leq 12(\log|\triangle_K)|)^2$ [Bac90], where $\triangle_K$ is the discriminant of K.

The problem is given an ideal $\mathfrak{a} \in Cl(K)$, find prime ideals $\mathfrak{p}_1,\dots,\mathfrak{p}_m \in Cl(K)$ and nonzero integers $x_1,\dots,x_m \in \mathbb{Z}^\times$ such that $\prod_{i=1}^n \mathfrak{p}_i^{x_i} = \mathfrak{a}$.

In the language of discrete exponential equations, it is to solve the equation

$$\prod_{i=1}^w \mathfrak{p}_i^{x_i} = \mathfrak{a}$$

for integers $x_1,\dots,x_w \in \mathbb{Z}$, where $\mathfrak{p}_1,\dots,\mathfrak{p}_w$ are all prime ideals of norm $\leq 12(\log|\triangle_K)|)^2$.

Isogeny factorization [CLG09]. The problem is given two elliptic curves E_1 and $E_2 := \phi(E_1)$, where ϕ is a separable isogeny, find ϕ. It is essentially asking to find the factorization $\phi = \phi_1 \circ \cdots \circ \phi_m \circ [n]$ of the isogeny ϕ into isogenies ϕ_i of prime degrees, where n is the greatest integer such that the torsion subgroup $E_1[n] \subseteq \ker\phi$, also $\deg(\phi) = n^2 \prod_{i=1}^m \deg(\phi_i)$.

In the language of discrete exponential equations, it is to solve the equation

$$\prod_{i=1}^w \phi_i^{x_i} = \phi$$

for binary integers $x_1,\dots,x_w \in \{0,1\}$, where the product is successive function compositions, and $\phi_1,\dots,\phi_w$ are all the possible intermediate irreducible isogenies between E_1 and E_2 in the isogeny graph.

3.5. NEW PROBLEMS.

Following are decomposition problems that either have not been considered in the literature or have not been thoroughly studied from the computational point of view. Also note

that the bases in each problem are possibly irreducible, but we mostly think of them as reducible.

Integer decomposition. The problem is given $n+1$ positive integers $a_1,\ldots,a_n,a \in \mathbb{Z}_{>0}$, find n nonnegative integers $x_1,\ldots,x_n \in \mathbb{Z}_{\geq 0}$ such that

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

Several mixable variations can be considered: (1) the summation version is to replace multiplication by addition; (2) the modular version is to reduce both sides of the equation modulo some integer N; and (3) a more general version is to replace $\mathbb{Z}$ by the order $\mathcal{O}_K$ of a number field K.

For (3), 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 $\mathcal{O}_K$ might not be a UFD. It follows that the factorization (i.e. irreducible decomposition) problem over $\mathcal{O}_K$ might not have a unique solution.

Polynomial decomposition. Let K be a field and let $m \geq 1$. Let $K[z_1,\ldots,z_m]$ be the m-variate polynomial ring over K. The problem is given $n+1$ polynomials $f_1,\ldots,f_n,f \in K[z_1,\ldots,z_m]$, find n nonnegative integers $x_1,\ldots,x_n \in \mathbb{Z}_{\geq 0}$ such that

$$\prod_{i=1}^{n} f_i^{x_i} = f.$$

Note that if $m = 1$ then the univariate polynomial ring $K[z]$ is a UFD. This is because for any polynomial ring $R[z]$, it is a UFD if the ground ring R is; and that a field R is aways a UFD.

Two mixable variations are: (1) the summation version is to replace polynomial multiplication by polynomial addition; and (2) the modular version is to reduce both sides of the equation modulo a polynomial $g \in K[z_1,\ldots,z_m]$.

Ideal decomposition. Let R be a ring (e.g. the order $\mathcal{O}_K$ of a number field K). The problem is given $n+1$ ideals $I_1,\ldots,I_n,I$ of R, find n nonnegative integers $x_1,\ldots,x_n \in \mathbb{Z}_{\geq 0}$ such that

$$\prod_{i=1}^{n} I_i^{x_i} = I.$$

Two mixable variations are: (1) the summation version is to replace ideal multiplication by ideal addition; and (2) the modular version is to reduce both sides of the equation modulo some ideal J.

Ideal class group decomposition. Let K be a number field and $\mathcal{O}_K$ be its order. Let $\mathcal{F}$ be the group of fractional ideals of $\mathcal{O}_K$. Let $\mathcal{P}$ be the group of principal ideals of $\mathcal{O}_K$. Then $Cl := \mathcal{F}/\mathcal{P}$ is the ideal class group of K.

The problem is given $n+1$ ideals $\mathfrak{a}_1,\ldots,\mathfrak{a}_n,\mathfrak{a} \subset \mathcal{O}_K$, find n nonnegative integers $x_1,\ldots,x_n \in \mathbb{Z}_{\geq 0}$ such that

$$\prod_{i=1}^{n} \mathfrak{a}_i^{x_i} = \mathfrak{a} \pmod{\mathcal{P}}.$$

where we define $\mathfrak{a} = \mathfrak{b} \pmod{\mathcal{P}} := \mathfrak{a}\cdot\mathcal{P} = \mathfrak{b}\cdot\mathcal{P}$ for all $\mathfrak{a},\mathfrak{b} \in \mathcal{F}$.

A more general version is to consider $\mathfrak{a}_1,\ldots,\mathfrak{a}_n,\mathfrak{a} \in \mathcal{F}$ and $x_1,\ldots,x_n \in \mathbb{Z}^\times$. Note that unique factorization holds for both ideals and fractional ideals of $\mathcal{O}_K$.

Variety decomposition. Let K be a field and $\mathbb{A}^m = K^m$ be the m-dimensional affine variety over K.

One way to define the problem is: given $n+1$ varieties (i.e. algebraic sets) $X_1, \ldots, X_n, X \subset \mathbb{A}^m$, find n binary integers $x_1, \ldots, x_n \in \{0,1\}$ such that $\bigcup_{i=1}^n X_i^{x_i} = X$, where we define $X_i^1 := X_i$ and $X_i^0 := \varnothing$. However this problem is trivial when the varieties $X_1, \ldots, X_n$ are of polynomial sizes and the elements are given in the plain. In fact, one could throw away those X_i's that have points not in X and take the union of the rest X_i's; then either the union equals X or the problem has no solutions.

A better problem is: given $n+1$ varieties $X_1, \ldots, X_n, X \subset \mathbb{A}^m$, find a binary vector $(x_1, \ldots, x_n) \in \{0,1\}^n$ of lowest Hamming weight such that

$$\bigcup_{i=1}^n X_i^{x_i} = X,$$

where $X_i^1 := X_i$ and $X_i^0 := \varnothing$.

The intersection version of the problem is to replace $\bigcup$ by $\bigcap$ and replace $X_i^0 := \varnothing$ by $X_i^0 := \mathbb{A}^n$.

If we think about the basic relations $V(I) \cup V(J) = V(IJ)$ and $V(I) \cap V(J) = V(I+J)$ between varieties and ideals, we can see that the union and intersection versions of variety decomposition correspond to the product and summation versions of ideal decomposition respectively.

Topology decomposition. Let τ be a topology on a set S.

The naive problem is: given $n+1$ open sets $A_1, \ldots, A_n, A \in \tau$, find $n+1$ binary integers $x_1, \ldots, x_n \in \{0,1\}$ such that $\bigcap_{i=1}^n A_i^{x_i} = A$, where $A_i^1 := A_i$ and $A_i^0 := S$. This problem is trivial when the open sets $A_1, \ldots, A_n$ are of polynomial sizes and the elements are given in the plain. In that case one can pick out all open sets A_i that contain A; then either their intersection is A or the problem has no solutions.

A better problems is: given $n+1$ open sets $A_1, \ldots, A_n, A \in \tau$, find a binary vector $(x_1, \ldots, x_n) \in \{0,1\}^n$ of lowest Hamming weight such that

$$\bigcap_{i=1}^n A_i^{x_i} = A,$$

where $A_i^1 := A_i$ and $A_i^0 := S$.

The union version is to replace $\bigcap$ by $\bigcup$ and replace $A_i^0 := S$ by $A_i^0 := \varnothing$. In fact, the union (resp. integersection) version of variety decomposition is a special case of the intersection (resp. union) version of topology decomposition with the concrete topology the Zariski topology of varieties.

Module decomposition. The problem is given $n+1$ modules $M_1, \ldots, M_n, M$, find n binary integers $x_1, \ldots, x_n \in \{0,1\}$ such that

$$\bigoplus_{i=1}^n M_i^{x_i} = M,$$

where $\bigoplus$ is direct sum, $M_i^1 := M_i$ and $M_i^0 := \{0\}$ (trivial module).

Vector space decomposition. This is a special case of module decomposition since every vector space is a module over a field. Typical fields include $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and finite fields $\mathbb{F}_q$ for prime powers q.

Ring decomposition. This is also a special case of module decomposition since every ring is an abelian group hence a $\mathbb{Z}$-module. Typical rings include polynomial rings and number rings.

Group decomposition The problem is given $n+1$ groups $G_1,\ldots,G_n,G$, find n nonnegative integers $x_1,\ldots,x_n \in \mathbb{Z}_{\geq 0}$ such that

$$\bigotimes_{i=1}^{n} G_i^{x_i} \cong G,$$

where $\otimes$ is direct product (i.e. Cartesian product), $G_i^1 := G_i$ and $G_i^0 := \{1\}$ (trivial group).

Matrix decomposition. The problem is given $n+1$ square matrices $M_1,\ldots,M_n,M \in \mathbb{Z}^{m\times m}$, find n nonnegative integers $x_1,\ldots,x_n \in \mathbb{Z}_{\geq 0}$ such that

$$\prod_{i=1}^{n} M_i^{x_i} = M,$$

where $M_i^1 := M_i$ and $M_i^0 = 1$ (identity matrix). Note that this problem is a " noncommutative problem" in the sense that operation, namely matrix multiplication is noncommutative.

Lattice vector decomposition. We take Euclidean lattice as an example. Let $\mathbb{R}^m$ be the m-dimensional Euclidean space. A lattice in $\mathbb{R}^m$ is the set $\Lambda(B) = \{Bz : z \in \mathbb{Z}^k\}$, where $B = (b_1,\ldots,b_k) \in \mathbb{R}^{m\times k}$ is a matrix with linear independent columns. We call $\{b_1,\ldots,b_n\}$ the *lattice basis*.

The problem is given $n+1$ lattice vectors $v_1,\ldots,v_n,v \in \Lambda(B)$, find n integers $x_1,\ldots,x_n \in \mathbb{Z}$ such that

$$\sum_{i=1}^{n} x_i v_i = v.$$

Elliptic point decomposition. Let E be an elliptic curve. The problem is given $n+1$ points $P_1,\ldots,P_n,P \in E$, find n nonnegative integers $x_1,\ldots,x_n \in \mathbb{Z}_{\geq 0}$ such that

$$\sum_{i=1}^{n} [x_i]P_i = P,$$

where $[x_i]P_i := P_i + \cdots + P_i$ (x_i times) is scalar multiplication, and $[0]P_i := \infty$ is the point at infinity which is the identity of the elliptic curve group.

Isogeny decomposition. It is given $n+1$ isogenies $\phi_1,\ldots,\phi_n,\phi$, find n binary integers $x_1,\ldots,x_n \in \{0,1\}$ such that

$$\prod_{i=1}^{n} \phi_i^{x_i} = \phi,$$

where the multiplications are function compositions, which are noncommutative.

3.6. **NON-ASSOCIATIVE DECOMPOSITIONS.** Following are some atypical examples where the operations are non-associative.

Subtraction decomposition. The problem is given $n+1$ positive integers $a_1,\ldots,a_n,a \in \mathbb{Z}_{>0}$, find n binary integers $x_1,\ldots,x_n \in \{0,1\}$ such that

$$\ominus_{i=1}^{n} x_i a_i = a,$$

where $\ominus$ denotes successive subtractions executed from left to right or right to left as required, $1a_i := a_i$ and $0a_i := 0$.

A variant is to replace integers by polynomials.

Devision decomposition. The problem is given $n+1$ integers $a_1,\dots,a_n,a$, find integers $x_1,\dots,x_n \in \mathbb{Z}_{\geq 0}$ such that

$$\oslash_{i=1}^{n} a_i^{x_i} = a,$$

where $\oslash$ denotes successive divisions executed from left to right or right to left as required, $a_i^1 := a_i$ and $a_i^0 := 1$.

A variant is to replace integers by polynomials.

4. Noisy equation systems

Now we spread the phenomenon of distortion to all possible branches of mathematics. This philosophical goal coincides with the following technical consideration.

From a purer technical point of view, our goal is to fix the solution $(x_1,\dots,x_n)$ of a discrete exponential equation to make it "well-defined". A natural way is to consider equation systems and hope that more restrictions helps to narrow down the solution space. However, more equations can make solutions easier to find because intuitively more equations means more hints. To avoid trivializing the problem, we insert noises into the equations and this leads to our definitions of noisy equations and noisy equation systems.

4.1. Noisy Equation Systems.

Definition 5. A *noisy discrete exponential equation* (abbr. *noisy equation*) over a land L is an equation of the form

$$\left(\prod_{i=1}^{n} a_i^{x_i}\right) \cdot e \approx a,$$

where $a_1,\dots,a_n \in L$ and $a \in L$ are given, but $e \in L$ is not given. The goal is to find $(x_1,\dots,x_n) \in \mathbb{Z}^n$.

Definition 6. A *noisy discrete exponential equation system* (abbr. *noisy system*) is a system of noisy discrete exponential equations. The goal is to find $(x_1,\dots,x_n) \in \mathbb{Z}^n$ that satisfy all the equations.

Definition 7. A *noisy restoration problem* (abbr. *noisy problem*) with respect to a base distribution $D_1(L)$ and a noise distribution $D_2(L)$ is given oracle access to random noisy discrete exponential equations of the form

$$\left(\prod_{i=1}^{n} a_i^{x_i}\right) \cdot e \approx a$$

with respect to the same vector $(x_1,\dots,x_n) \in \mathbb{Z}^n$, where $a_1,\dots,a_n \leftarrow D_1(L)$ and $a \in L$ are given, but $e \leftarrow D_2(L)$ are not given, find the vector $(x_1,\dots,x_n)$.

4.2. Well-known problems.

Following are well-known noisy problems in coding theory and lattice theory.

Learning parity with noise problem (LPN) [BMT78; BFKL94]. The problem (over uniform distributions) is given oracle access to instances of the form $(a_1,\dots,a_n,a)$ with respect

to the same vector $(x_1,\ldots,x_n)\in\mathbb{Z}_2^n$, where $a_1,\ldots,a_n,e\leftarrow\mathbb{Z}_2$ and

$$a=\left(\sum_{i=1}^{n}a_ix_i\right)+e\pmod 2,$$

find the vector $(x_1,\ldots,x_n)$.

Learning with errors problem (LWE) [Reg09]. Let $\mathbb{R}$ be the additive group of real numbers. Let $\mathbb{Z}_q$ be the additive group of integers modulo a prime q. Let $\mathbb{T}:=\mathbb{R}/\mathbb{Z}$ be the additive group of real numbers modulo one. Let $N(\mathbb{T})$ be a Gaussian distribution over $\mathbb{T}$.

The problem is given oracle access to instances of the form $(a_1,\ldots,a_n,a)$ with respect to the same vector $(x_1,\ldots,x_n)\in\mathbb{Z}_q^n$, where $a_1,\ldots,a_n\leftarrow\mathbb{Z}_q^n$, $e\leftarrow N(\mathbb{T})$, and

$$a=\left(\sum_{i=1}^{n}a_ix_i\right)+e\pmod q,$$

find the vector $(x_1,\ldots,x_n)$.

Learning with rounding problem (LWR) [BPR12]. Following the settings of LWE, let $p<q$ be a prime.

The problem is given oracle access to instances of the form $(a_1,\ldots,a_n,a)$ with respect to the same vector $(x_1,\ldots,x_n)\in\mathbb{Z}_q^n$, where $a_1,\ldots,a_n\leftarrow\mathbb{Z}_q^n$,

$$a=\left\lfloor\sum_{i=1}^{n}a_ix_i\pmod q\right\rceil_p,$$

and $\lfloor\cdot\rceil_p:\mathbb{Z}_q\to\mathbb{Z}_p$ divides $\mathbb{Z}_q$ into p intervals of size roughly q/p each and outputs the index of the interval that the input belongs to, find the vector $(x_1,\ldots,x_n)$. Note that the noise distribution of this problem is given in an implicit way by rounding.

Bounded distance decoding (BDD). Let $\Lambda(B)=\{Bx:x\in\mathbb{Z}^n\}$ be a Euclidean lattice with basis $B=(b_1,\ldots,b_n)\in\mathbb{R}^{k\times n}$.

The γ-bounded distance decoding problem (BDD_γ) is given a lattice basis B and a vector t such that $\mathrm{dist}(B,t)<\gamma\lambda_1(B)$, find the (unique) lattice vector $v\in\Lambda(B)$ that is closest to t.

In the language of noisy equation systems, it is to solve the system

$$\left(\sum_{i=1}^{n}x_ib_i\right)+e=t$$

over $\mathbb{R}$.

Note that there are no distributions being specified. Hence BDD is a worst-case problem. In fact, LWE is an average-case version of BDD.

4.3. New problems.

We define noisy problems in different branches of mathematics. They differ from our previous decomposition examples in the following three ways: (1) they are equation systems rather than single equations; (2) each equation has an invisible noisy term; (3) the binary operation is reduced by an equivalence relation, which we uniformly call *modular* operation.

Note that we do not conjecture that all of the proposed problems are hard.

Integer noisy problem (Integer-NP)[4]**.** Let q be a prime. The problem is given oracle access to equations of the form

$$\left(\prod_{i=1}^{n} a_i^{x_i}\right) \cdot e = a \pmod{q}$$

with respect to the same vector $(x_1,\ldots,x_n) \in \mathbb{Z}_q^n$, where $a_i \leftarrow \mathbb{Z}_q^\times$ and $a \in \mathbb{Z}_q^\times$ are given, but $e \leftarrow \mathbb{Z}_q^\times$ are not given, find the vector $(x_1,\ldots,x_n)$.

Two mixable variations are: (1) the summation version is to replace multiplication by addition[5]; and (2) the binary version asks for binary solutions $(x_1,\ldots,x_n) \in \{0,1\}^n$.

Polynomial noisy problem (Poly-NP). Let $\mathbb{F}_q$ be a finite field with q a prime. Let $R := \mathbb{F}_q[z_1,\ldots,z_m]$ be the m-variate polynomial ring over $\mathbb{F}_q$. Let $I = (h_1,\ldots,h_r)$ be an ideal of R generated by some polynomials $h_1,\ldots,h_r \in R$. A typical case is that $I = (h)$ is a principal ideal generated by a single polynomial $h \in R$.

The problem is given oracle access to equations of the form

$$\left(\prod_{i=1}^{n} f_i^{x_i}\right) \cdot g = f \pmod{I}$$[6]

with respect to the same vector $(x_1,\ldots,x_n) \in \mathbb{Z}^n$, where $f_i \leftarrow R/I$ and $f \in R/I$ are given, but $g \leftarrow R/I$ are not given, find the vector $(x_1,\ldots,x_n)$.

Two mixable variations are: (1) the summation version is to replace multiplication by addition; (2) the binary version asks for binary solutions $(x_1,\ldots,x_n) \in \{0,1\}^n$.

Ideal noisy problem (Ideal-NP). Let $Cl(K)$ be the ideal class group of some number field K. As mentioned previously, $Cl(K)$ is generated by prime ideals of norm $\leq 12(\log|\triangle_K|)^2$ [Bac90], assuming the generalized Riemann hypothesis. Let $P = \{\mathfrak{p}_1,\ldots,\mathfrak{p}_m\}$ be a subset of prime ideals of norm $\leq 12(\log|\triangle_K|)^2$, where m is polynomial in n. Let $S = \{\prod_{i=1}^{m} \mathfrak{p}_i^{e_i} \mid e_i \in \{0,\ldots,d\}\}$ be the set of ideals factored over P with the multiplicities of the factors upper bounded by d.

The problem is given oracle access to equations of the form

$$\left(\prod_{i=1}^{n} \mathfrak{a}_i^{x_i}\right) \cdot \mathfrak{e} = \mathfrak{a} \pmod{\mathcal{P}}$$[7]

with respect to the same vector $(x_1,\ldots,x_n) \in \mathbb{Z}_d^n$, where $\mathfrak{a}_i \leftarrow S$ and $\mathfrak{a} \in Cl(K)$ are given, but $\mathfrak{e} \leftarrow S$ are not given, find the vector $(x_1,\ldots,x_n)$.

Two mixable variations are: (1) the summation version is to replace multiplication by addition; (2) the binary version asks for binary solutions $(x_1,\ldots,x_n) \in \{0,1\}^n$.

Variety noisy problem (Variety-NP). Let K be a field and $\mathbb{A}^m = K^m$ be the m-dimensional affine variety on K. Let $S \subset \mathbb{A}^m$ be a finite variety. Let $W = V(I) \subset \mathbb{A}^m$ be the variety of the ideal $I = (h_1,\ldots,h_r)$ generated by some polynomials $h_1,\ldots,h_r \in K[z_1,\ldots,z_m]$. A typical case is that $I = (h)$ is a principal ideal with $h \in K[z_1,\ldots,z_m]$.

---

[4] This is actually the multiple modular subset product with errors problem (M-MSPE) in [Li22g].

[5] This is actually the multiple modular subset sum with errors problem (M-MSSE) in [Li22g].

[6] The modular operation is defined as: $f = g \pmod{I} := f + I = g + I$.

[7] The modular operation is defined as: $\mathfrak{a} = \mathfrak{b} \pmod{\mathcal{P}} := \mathfrak{a} \cdot \mathcal{P} = \mathfrak{b} \cdot \mathcal{P}$.

The problem is given oracle access to equations of the form

$$\left(\bigcup_{i=1}^{n} X_i^{x_i}\right) \bigcup Y = X \pmod{W}$$[8]

with respect to the same vector $(x_1,\ldots,x_n) \in \{0,1\}^n$, where $X_i \leftarrow S/W$ and $X \in S/W$ are given, but $Y \leftarrow S/W$ are not given, also $X_i^1 := X_i$ and $A_i^0 := \varnothing$, find the vector $(x_1,\ldots,x_n)$.

Topology noisy problem (Topology-NP). Let τ be a topology on a set S. Let $T \subset \tau$ be a finite subset of τ.

The problem is given oracle access to equations of the form

$$\left(\bigcap_{i=1}^{n} A_i^{x_i}\right) \bigcap B = A$$

with respect to the same vector $(x_1,\ldots,x_n) \in \{0,1\}^n$, where $A_1,\ldots,A_n \leftarrow T$ and $A \in \tau$ are given, but $B \leftarrow T$ are not given, also $A_i^1 := A_i$ and $A_i^0 := S$, find the vector $(x_1,\ldots,x_n)$.

Note that subvarieties of $\mathbb{A}^m$ are closed sets of the Zariski topology on the variety $\mathbb{A}^m$. Hence by De Morgan's laws, Variety-NP equations $\bigcup_{i=1}^n X_i^{x_i} \bigcup Y = X$ are in fact Topology-NP equations $\bigcap_{i=1}^n \overline{X}_i^{x_i} \bigcap \overline{Y} = \overline{X}$ with respect to the complements of the subvarieties.

Module noisy problem (Module-NP). We give a concrete example. Let R be the ring of $k \times k$ matrices over $\mathbb{Z}$. Let M be an R-module. Let $S = \{e_1M,\ldots,e_mM\}$ be a set of modules, where e_i is the $n \times n$ matrix with the (i,i)-th entry 1 and all other entries 0. Let $T = \{\bigoplus_{i=1}^n (e_iM)^{c_i} \mid c_i \in \{0,1\}\}$ be the set of "square-free" direct sums of modules in S, where $(e_iM)^1 := e_iM$ and $(e_iM)^0 := 0$.

The problem is given oracle access to equations of the form

$$\left(\bigoplus_{i=1}^{n} A_i^{x_i}\right) \bigoplus B = A$$

with respect to the same vector $(x_1,\ldots,x_n) \in \{0,1\}^n$, where $A_1,\ldots,A_n \leftarrow T$ and $A \in \tau$ are given, but $B \leftarrow T$ are not given, also $A_i^1 := A$ and $A_i^0 := 0$, find the vector $(x_1,\ldots,x_n)$.

Vector space noisy problem (VecSpac-NP). This is a special case of Module-NP. A concrete example is the above Module-NP example with the ring $\mathbb{Z}$ replaced by the field $\mathbb{R}$.

Ring noisy problem (Ring-NP) This is also a special case of Module-NP since every ring is a $\mathbb{Z}$-module.

Group noisy problem (Group-NP). We give a concrete example. Let $p_1,\ldots,p_m$ be m prime numbers. Let S be the set of square-free integers factored over $p_1,\ldots,p_m$.

The problem is given oracle access to equations of the form

$$\left(\bigotimes_{i=1}^{n} (\mathbb{Z}/a_i\mathbb{Z})^{x_i}\right) \bigotimes \mathbb{Z}/e\mathbb{Z} \cong G$$

with respect to the same vector $(x_1,\ldots,x_n) \in \{0,1\}^n$, where the base groups $\mathbb{Z}/a_1\mathbb{Z},\ldots,\mathbb{Z}/a_n\mathbb{Z} \leftarrow S$ and the resulting groups G are given, but the noise groups $\mathbb{Z}/e\mathbb{Z}$ are not given, also $(\mathbb{Z}/a_i\mathbb{Z})^1 := \mathbb{Z}/a_i\mathbb{Z}$ and $(\mathbb{Z}/a_i\mathbb{Z})^0 := \{1\}$, find the vector $(x_1,\ldots,x_n)$.

[8] The modular operation is defined as: $X = Y \pmod{W} := X \cup W = Y \cup W$.

Note that if $\gcd(a,b)=1$ then $\mathbb{Z}/a\mathbb{Z}\oplus\mathbb{Z}/b\mathbb{Z}\cong\mathbb{Z}/ab\mathbb{Z}$. However the integers $a_1,\ldots,a_n$ are probably not coprime. Hence we shall not misunderstand that $G=\mathbb{Z}/(\prod_{i=1}^n a_i^{x_i})\mathbb{Z}$. I.e., this problem is different from Integer-NP over S.

Matrix noisy problem (Matrix-NP). Let q be a prime. The problem is given oracle access to equations of the form

$$\left(\prod_{i=1}^n M_i^{x_i}\right)\cdot N = M \pmod q$$

with respect to the same vector $(x_1,\ldots,x_n)\in\mathbb{Z}_{\geq 0}$, where $M_1,\ldots,M_n\leftarrow\mathbb{Z}_q^{m\times m}$ and $M\in\mathbb{Z}_q^{m\times m}$ are given, but $N\leftarrow\mathbb{Z}_q^{m\times m}$ are not given, also $M_i^1:=M_i$ and $M_i^0=1$ (identity matrix), find the vector $(x_1,\ldots,x_n)$.

The summation version is to solve

$$\left(\sum_{n=1}^n x_i M_i\right)+N=M \pmod q$$

for a vector $(x_1,\ldots,x_n)\in\mathbb{Z}_q$.

Note that the module learning with errors problem (MLWE) [BGV14; LS15] is of a similar form with the matrices of integers M_i,N,M replaced by vectors of polynomials v_i,u,v, and the solution vector $(x_1,\ldots,x_n)$ replaced by a vector of polynomials $(f_1,\ldots,f_n)$.

Lattice vector noisy problem (LatVec-NP). Let $\Lambda(B)=\{Bz : z\in\mathbb{Z}^k\}$ be a Euclidean lattice with basis $B=(b_1,\ldots,b_k)\in\mathbb{R}^{m\times k}$.

The problem is given oracle access to equations of the form

$$\left(\sum_{i=1}^n x_i v_i\right)+u=v$$

with respect to the same vector $(x_1,\ldots,x_n)\in\mathbb{Z}$, where $v_1,\ldots,v_n\leftarrow\Lambda(B)$ and $v\in\Lambda(B)$ are given, but $u\leftarrow\Lambda(B)$ are not given, find the vector $(x_1,\ldots,x_n)$.

Elliptic point noisy problem (ECPoint-NP). Let E be an elliptic curve. The problem is given oracle access to equations of the form

$$\left(\sum_{i=1}^n [x_i]P_i\right)+Q=P$$

with respect to the same vector $(x_1,\ldots,x_n)\in\mathbb{Z}$, where $P_1,\ldots,P_n\leftarrow E$ and $P\in E$ are given, but $Q\leftarrow E$ are not given, find the vector $(x_1,\ldots,x_n)$.

Isogeny noisy problem (Isogeny-NP). Let $E: y^2+a_1xy+a_3=x^3+a_2x^2+a_4x+a_6$ be an elliptic curve over some field K. Let $N=\prod_{j=1}^m p_j^{e_j}$ be a composite integer with $e_j\in\{0,\ldots,d\}$ for some $d\in\mathbb{N}$. Let $M=\{(e_{i,1},\ldots,e_{i,m})\}_{i\in[n]}$ be a prefixed matrix of integers such that $e_j>e_{i,j}$ for $i\in[n]$, $j\in[m]$, and $e_{k,j}>e_{i,j}$ for $k>i$, $k,i\in[n]$, $j\in[m]$. Denote

$$G_i:=\mathbb{Z}/p_1^{e_{i,1}}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_m^{e_{i,m}}\mathbb{Z},$$

for $i\in[n]$. In other words, each row of M defines a subgroup G_i; and all the subgroups form a subgroup tower

$$G_1\subset\cdots\subset G_n.$$

Let S be the set of subgroups of E such that each subgroup is isomorphic to one of the groups $G_1,\ldots,G_n$. Let T be the set of quotient groups E/G for all $G \in S$. Then the curves E/G give an isogeny graph. Let $D_1 = D_2$ be the distribution that samples two curve $A,B \leftarrow T$ uniformly at random, and outputs the isogeny $\phi : A \to B$ between them. Note that the isogeny from any curve in T to any curve in T exists because the isogeny graph is connected and that we also consider dual isogenies.

The problem is given equations of the form

$$\left(\prod_{i=1}^{n} \phi_i^{x_i}\right) \circ \varphi = \phi$$

with respect to the same vector $(x_1,\ldots,x_n) \in \{0,1\}^n$, where $\phi_i \leftarrow D_1$ and ϕ are given, but $\varphi \leftarrow D_2$ are not given, also $\phi_i^1 := \phi_i$ and $\phi_i^0 := 1$ (identity morphism), find the vector $(x_1,\ldots,x_n)$.

4.4. **NON-ASSOCIATIVE NOISY EQUATION SYSTEMS.** Following are two special examples over lands that are not monoids, groups, rings, etc.

Subtraction noisy problem (Subtraction-NP). Let q be a prime. The problem is given oracle access of equations of the form

$$\left(\ominus_{i=1}^{n} x_i a_i\right) - e = a \pmod q$$

with respect to the same vector $(x_1,\ldots,x_n) \in \mathbb{Z}_q$, where $a_1,\ldots,a_n \leftarrow \mathbb{Z}_q$ and $a \in \mathbb{Z}_q$ are given, but $e \leftarrow \mathbb{Z}_q$ are not given, find the vector $(x_1,\ldots,x_n)$.

A variant is to replace integers by polynomials.

Devision noisy problem (Division-NP). Let q be a prime. The problem is given oracle access of equations of the form

$$\left(\oslash_{i=1}^{n} a_i^{x_i}\right)/e = a \pmod q$$

with respect to the same vector $(x_1,\ldots,x_n) \in \mathbb{Z}_q^\times$, where $a_1,\ldots,a_n \leftarrow \mathbb{Z}_q^\times$ and $a \in \mathbb{Z}_q^\times$ are given, but $e \leftarrow \mathbb{Z}_q^\times$ are not given, find the vector $(x_1,\ldots,x_n)$.

A variant is to replace integers by polynomials.

5. ALGORITHMS

We give a basic algorithm for discrete exponential equations over a PID order and with small solutions $(x_1,\ldots,x_n) \in \mathbb{Z}_\ell^n$ for some small prime $\ell \in \mathbb{N}$ (e.g., 2). We also give a basic algorithm for (modular) discrete exponential equation systems over a PID order with small solutions $(x_1,\ldots,x_n) \in \mathbb{Z}_\ell^n$. We then show how to solve more discrete exponential equations over other lands by reducing them to discrete exponential equations over a PID order.

5.1. **ALGORITHM FOR SINGLE EQUATIONS.**

We have given this algorithm in [Li22c]. We describe the idea in the following. Given a discrete exponential equation $\prod_{i=1}^{n} a_i^{x_i} = a$ over some PID order $\mathcal{O}_K$, the algorithm takes the ℓ-th power residue symbols for the equation above k different prime ideals $\mathfrak{q}_1,\ldots,\mathfrak{q}_k$, obtaining k equations of the form

$$\prod_{j=1}^{n} \left(\frac{a_i}{\mathfrak{q}_i}\right)^{x_j} = \left(\frac{a_i}{\mathfrak{q}_i}\right)$$

for $i \in [k]$. These equations yield k linear equations of the form

$$\sum_{j=1}^{n} \alpha_{i,j} x_j = \alpha_i \pmod{\ell},$$

where $\alpha_{i,j}, \alpha_i \in \mathbb{Z}_\ell$. Write them in the matrix form one has

$$Ax = b \pmod{\ell}.$$

The algorithm then brute forces its solutions and find those that also satisfy the target discrete exponential equation.

The algorithm is efficient only when the linear system is of high $\mathbb{Z}_\ell$-rank. This requires the characteristic matrix of the target equations to be of high $\mathbb{Z}_\ell$-rank initially.

Note that this algorithm does not work for modular equations since in that case the modulus $\mathfrak{q}$ is fixed and we do not have the flexibility to reduce a single equation to different modular equations using different prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_k$.

5.2. Algorithm for equation systems.

For non-modular equation systems over a PID order $\mathcal{O}_K$ and with small solution $(x_1, \ldots, x_n) \in \mathbb{Z}_\ell^n$, the algorithm is a trivial extension of the above algorithm for single equations. In fact, we can simply transform each equation into a linear system $Ax = b \pmod{\ell}$ and put all the linear systems together to get a bigger system $A'x = b' \pmod{\ell}$. We expect that the rank of the bigger system is higher than the single systems hence the algorithm has a better chance to be a polynomial time algorithm. In the following we look at modular equation systems.

For modular systems over a PID order $\mathcal{O}_K$ and with small solution $(x_1, \ldots, x_n) \in \mathbb{Z}_\ell^n$, we use a similar idea to the case of singe equations.

Let the system be consist of $k \geq 2$ discrete exponential equations of the form

$$\prod_{j=1}^{n} a_{i,j}^{x_j} = a_i \pmod{\mathfrak{q}_i},$$

where $a_{i,j}, a_i \in \mathcal{O}_K$ for $i \in [k]$, $j \in [n]$, and $\mathfrak{q}_i$ are prime ideals that are possibly the same or different. The goal is to find vector(s) $(x_1, \ldots, x_n) \in \mathbb{Z}_\ell^n$ that satisfy all the k equations, where $\ell \geq 2$ is a prime.

The algorithm takes the ℓ-th power residue symbols for the equations to get k equations of the form

$$\prod_{j=1}^{n} \left(\frac{a_{i,j}}{\mathfrak{q}_i}\right)^{x_j} = \left(\frac{a_i}{\mathfrak{q}_i}\right).$$

Similar to before, the k ℓ-the power residue symbol equations yield a system of linear equation of the form

$$\sum_{j=1}^{n} \alpha_{i,j} x_j = \alpha_i \pmod{\ell}.$$

Write the linear system in the matrix form we have

$$Ax = b \pmod{\ell}.$$

We then brute force its solutions and find those that also satisfy the original modular discrete exponential system.

5.3. ALGORITHM FOR OTHER EQUATIONS.

For discrete exponential equations/systems over other lands, the strategy is to transform them into equations over PID orders, then use the above algorithms to solve them. More specifically, the algorithm involves the following two phases:

> *Phase 1.* transform the target discrete exponential equation(s) into discrete exponential equation(s) $\prod_{i=1}^{n} a_i^{x_i} = a$ over a PID order $\mathcal{O}_K$ (e.g., $\mathbb{Z}$);
> *Phase 2.* use the previous two algorithms to transform the resulting equation(s) of Phase 1 into a linear system over $\mathbb{Z}_\ell$ and solve it for solutions that also satisfy the target discrete exponential equation(s).

Example 1. Ideal decomposition. To transform an ideal decomposition equation $\prod_{i=1}^{n} \mathfrak{a}_i^{x_i} = \mathfrak{a}$ into an integer decomposition equation, we simply take the ideal norms of the bases to get $\prod_{i=1}^{n} N(\mathfrak{a}_i)^{x_i} = N(\mathfrak{a})$. Obviously $\prod_{i=1}^{n} \mathfrak{a}_i^{x_i} = \mathfrak{a} \Longrightarrow \prod_{i=1}^{n} N(\mathfrak{a}_i)^{x_i} = N(\mathfrak{a})$, namely every solution $(x_1, \ldots, x_n) \in \mathbb{Z}_\ell^n$ to the former equation is a solution to the latter equation. We then enter Phase 2 to solve the latter equation. Note that the efficiency of the algorithm depends on the rank of the norm equation $\prod_{i=1}^{n} N(\mathfrak{a}_i)^{x_i} = N(\mathfrak{a})$.

Example 2. Isogeny decomposition. Given an isogeny decomposition equation $\prod_{i=1}^{n} \phi^{x_i} = \phi$, we simply take the degrees of the bases. We have $\prod_{i=1}^{n} \phi^{x_i} = \phi \Longrightarrow \prod_{i=1}^{n} \deg(\phi)^{x_i} = \deg(\phi)$. We then enter Phase 2 to solve it. The efficiency of the algorithm depends on the rank of the degree equation $\prod_{i=1}^{n} \deg(\phi)^{x_i} = \deg(\phi)$.

6. ON CRYPTOGRAPHY

We talk a bit about cryptography. We suggest that simpler and cleaner problems are more reliable (in the sense of hardness) than problems that have more structures or properties that associate with other areas. This is simply because more structures or properties provide more tools for finding fast algorithms.

In particular, purer combinatorial reasons seem more reliable than number theoretical or geometrical reasons for a problem to be hard. For historical examples, think about the break of the integer factorization problem [Sho99], compared with the hardness of XC; also the recent break of the "auxiliary" isogeny factorization problem [CD22; MM22; Rob22][9], compared with the hardness of SP [GJ79, p. 224]. Note that they are all decomposition problems, but XC and SP seem more combinatorial and have less associations with other mathematics.

However it is usually a compromise between simplicity and usefulness. For example. LPN is a simple and clean problem, but the lack of extra properties makes it hard to have many applications. Hence one of the motivations that we permeate the ideas of decomposition and restoration into different areas is to give more fruitful properties to simple problems so that we can use them to do more things. One try we have made is the different variants of Integer-NP in our previous papers [Li22d; Li22e; Li22f; Li22g; Li22a], where we call the

[9]Note that they only solved the isogeny factorization problem given an extra auxiliary point computed by the isogeny; and the isogeny factorization problem has not been literally solved. The algorithms in [CD22; MM22; Rob22] only works when they are provided an auxiliary point computed by the isogeny.

problems subset product with errors problems. They have strong relations[10] with LPN and have extra properties that we can control to do cryptographic constructions.

Another point we want to make is that lands seem to be useful for cryptography. To see this, just to notice that lands do not guarantee commutativity nor associativity. Also, if we take a look at the new problems we proposed, we can see that some of them are "non-commutative problems", namely the operations involved are noncommutative; and some of them are even "nonassociative problems". These kinds of noncommutative or nonassociative problems might imply new opportunities for the research of cryptography.

After all, we emphasize that the new problems proposed in this paper are just a tip of the iceberg. We expect that our theory can inspire more interesting computational problems that are useful in cryptography.

7. Final remarks

To develop a theory for the phenomena/processes of generation/decomposition and distortion/restoration in mathematics and nature, we have defined discrete exponential equations and noisy equation systems over lands; we have given concrete examples in algebraic number theory, algebraic geometry, topology, lattice theory, algebra, etc.; we have given algorithms for discrete exponential equations and systems over PID orders. As an application, our theory provides a methodology to find hard underlying problems for cryptographic constructions.

References

[APS15] Martin R Albrecht, Rachel Player, and Sam Scott. "On the concrete hardness of learning with errors". In: *Journal of Mathematical Cryptology* 9.3 (2015), pp. 169–203.

[Bac90] Eric Bach. "Explicit bounds for primality testing and related problems". In: *Mathematics of Computation* 55.191 (1990), pp. 355–380.

[BFKL94] Avrim Blum, Merrick Furst, Michael Kearns, and Richard J. Lipton. "Cryptographic Primitives Based on Hard Learning Problems". In: *Advances in Cryptology — CRYPTO' 93*. Ed. by Douglas R. Stinson. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 278–291. ISBN: 978-3-540-48329-8.

[BGV14] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. "(Leveled) fully homomorphic encryption without bootstrapping". In: *ACM Transactions on Computation Theory (TOCT)* 6.3 (2014), pp. 1–36.

[BLPRS13] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. "Classical hardness of learning with errors". In: *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*. 2013, pp. 575–584.

[BMT78] E. Berlekamp, R. McEliece, and H. van Tilborg. "On the inherent intractability of certain coding problems (Corresp.)" In: *IEEE Transactions on Information Theory* 24.3 (1978), pp. 384–386. DOI: 10.1109/TIT.1978.1055873.

[10] In fact, by taking Legendre symbols for Integer-NP instances one can reduce uniform Integer-NP (i.e. Integer-NP with uniform base and noise distributions) to uniform LPN (i.e. LPN with uniform coefficient and noise distributions), which means that uniform LPN is at least as hard as uniform Integer-NP.

[BPR12] Abhishek Banerjee, Chris Peikert, and Alon Rosen. “Pseudorandom Functions and Lattices”. In: *Advances in Cryptology – EUROCRYPT 2012*. Ed. by David Pointcheval and Thomas Johansson. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 719–737. ISBN: 978-3-642-29011-4.

[CD22] Wouter Castryck and Thomas Decru. *An efficient key recovery attack on SIDH (preliminary version)*. Cryptology ePrint Archive, Paper 2022/975. https://eprint.iacr.org/2022/975. 2022. URL: https://eprint.iacr.org/2022/975.

[CLG09] Denis X Charles, Kristin E Lauter, and Eyal Z Goren. “Cryptographic hash functions from expander graphs”. In: *Journal of CRYPTOLOGY* 22.1 (2009), pp. 93–113.

[FNT10] Colin Fox, Geoff K Nicholls, and Sze M Tan. “An Introduction To Inverse Problems”. In: *Course notes for ELEC* 404 (2010).

[Gal12] Steven D Galbraith. *Mathematics of public key cryptography*. Cambridge University Press, 2012.

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

[HM89] James Lee Hafner and Kevin S. McCurley. “A rigorous subexponential algorithm for computation of class groups”. In: *Journal of the American Mathematical Society* 2 (1989), pp. 837–850.

[KS06] Jari Kaipio and Erkki Somersalo. *Statistical and computational inverse problems*. Vol. 160. Springer Science & Business Media, 2006.

[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.

[Li22c] Trey Li. “Power Residue Symbol Order Detecting Algorithm for Subset Product over Algebraic Integers”. 3rd paper of the series. 2022, October 3.

[Li22d] Trey Li. “Multiple Modular Unique Factorization Domain Subset Product with Errors”. 4th paper of the series. 2022, October 4.

[Li22e] Trey Li. “Post-Quantum Key Exchange from Subset Product with Errors”. 5th paper of the series. 2022, October 5.

[Li22f] Trey Li. “Post-Quantum Public Key Cryptosystem from Subset Product with Errors”. 6th paper of the series. 2022, October 6.

[Li22g] Trey Li. “Post-Quantum Signature from Subset Product with Errors”. 7th paper of the series. 2022, October 7.

[LS15] Adeline Langlois and Damien Stehlé. “Worst-case to average-case reductions for module lattices”. In: *Designs, Codes and Cryptography* 75.3 (2015), pp. 565–599.

[MM22] Luciano Maino and Chloe Martindale. *An attack on SIDH with arbitrary starting curve*. Cryptology ePrint Archive, Paper 2022/1026. https://eprint.iacr.org/2022/1026. 2022. URL: https://eprint.iacr.org/2022/1026.

[Reg09] Oded Regev. “On lattices, learning with errors, random linear codes, and cryptography”. In: *Journal of the ACM (JACM)* 56.6 (2009), p. 34.

[Rob22] Damien Robert. *Breaking SIDH in polynomial time*. Cryptology ePrint Archive, Paper 2022/1038. https://eprint.iacr.org/2022/1038. 2022. URL: https://eprint.iacr.org/2022/1038.

[San57] Vera Sanford. "Robert Recorde's Whetstone of witte, 1557". In: *The Mathematics Teacher* 50.4 (1957), pp. 258–266.

[Sho99] Peter W Shor. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer". In: *SIAM review* 41.2 (1999), pp. 303–332.

[Tar05] Albert Tarantola. *Inverse problem theory and methods for model parameter estimation*. SIAM, 2005.