2D Gaudry-Schost Algorithm On Equivalence Classes

Vivi

December 1, 2010

A thesis submitted for the degree of Master at The University of Auckland
December 1, 2010

ABSTRACT

In this article, we will talk about the Discrete Logarithm Problems. Especially solving a certain range of Discrete Logarithm Problems by using the Gaudry-Schost algrithm on equivalence classes and the improvment. We mainly do theoritical analysis, it is developed from the Birthday Paradox type analysis. Even the Birthday Paradox Problem is actually a probability theory problem. As the first thing we need to do is to introduce what the Birthday Paradox is and how its theoritical analysis works. Then we give the details of Shank's Baby-Step Giant-Step (BSGS) method, since it is the most famous and basic DLP solving methods in the whole Cryptography. The Gaudry-Schost algorithm is developed from these methods. To introduce the 2-Dimensional case of the Gaudry-Schost Algorithm on Equivalence Classes. We explain the linear case – which is the Gaudry-Schost algorithm for the short interval $0 \leq n \leq N$ precisely in section 4.1.1. Hence, we apply the Gaudry-Schost Algorithm on two types of Equivalence Classes – (1) *Rotation from* 180^o *and* (2) *GLV Method. From our rough calculation, the expected running time on rotation from* 180^o *is* $1.4503\sqrt{N}$ *and the expected running time on GLV Method is* $1.0255\sqrt{N}$*. Eventually, we summary the general optimal formula for the expectation of selection in 2-Dimensional Gaudry-Schost Algorithm on the Equivalence Classes of rotations as our final conclusion.*

AKNOWLEDGEMENTS

I would like to express my gratitude to all those who helped me during the writing of this thesis.

My deepest gratitude goes first and foremost to Dr Steve Galbraith, my supervisor, for his constant encouragement and guidance. He has walked me through all the stages of the writing of this thesis. Without his consistent and illuminating instruction, this thesis could not have reached its present form. Second, I am also greatly indebted to the professors and teachers at the Department of Mathematics, who have instructed and helped me a lot in the past two years. Last my thanks would go to my beloved family for their loving considerations and great confidence in me all through these years. I also owe my sincere gratitude to my friends and my fellow classmates who gave me their help and time in listening to me and helping me work out my problems during the difficult course of the thesis.

Contents

List of Figures

1 Introduction

In 1976, Whitfield Diffie and Martin Hellman published their now famous paper [19] entitled 'New Directions in Cryptography'. In this paper they formulated the concept of a public key encryption system and made several groundbreaking contributions to this new field. A short time earlier, Ralph Merkle had independently isolated one of the fundamental problems and invented a public key construction for an undergraduate project in a computer science class at Berkeley, but this was little understood at the time. Merkle's work "Secure communication over insecure channels" appeared in 1978 [20]. The Diffie-Hellman publication was an extremely important event–it set forth the basic definitions and goals of a new field of mathematics/computer science, a field whose existence was dependent on the then emerging age of the digital computer. Indeed, their paper begins with a call to arms: We stand today on the brink of a revolution in cryptography.

1.1 Diffie-Hellman

The Diffie-Hellman key exchange algorithm solves the following dilemma. Alice and Bob want to share a secret key for use in a symmetric cipher, but their only means of communication is insecure. Every piece of information that they exchange is observed by their adversary Eve. Diffie and Hellman suggest that the difficulty of the discrete logarithm problem (We will introduce in the next subsection) for $\mathbb{F}_p^*$ gives an idea to Alice and Bob . Three steps are needed. First, Alice and Bob agree on a large prime p and a nonzero integer g modulo p. And then post the values of p and g somewhere in publication, for instance, on the web sites. Their adversary Eve also knows about the values of p and g; Second, Alice and Bob pick up integers a and b, respectively, and keep the numbers as a secret to themselves. Then, Bob and Alice use their secret integers to compute

$$A \equiv g^a (\mod p) \text{ (Alice's job)} \quad \text{and} \quad B \equiv g^b (\mod p) \text{ (Bob's job)}$$

Now, Alice and Bob exchange their computed values A and B to each other. Note that Eve still can see these numbers, since they are sent over the insecure communication channel. Finally, Bob and Alice again use their secret integers a and b to compute

$$A' \equiv B^a (\mod p) \text{ (Alice's work)} \quad \text{and} \quad B' \equiv A^b (\mod p) \text{ (Bob's work)}$$

But actually,

$$A' \equiv B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \equiv B' (\mod p)$$

Bob now knows the value of a and Alice knows the value of b.

The Diffie-Hellman key exchange is based on the assumption that the discrete logarithm problem (DLP) is very difficult to solve. After the publication of

Diffie-Hellman's paper [19], two major papers describing public key cryptosystems were introduced: the RSA scheme of Rivest, Shamir and Adleman [21] and the knapsack scheme of Merkle and Hellman [22].

1.2 DLP and Basic Definitions

Before we explain the whole idea of solving Discrete Logarithm Problems in a short interval, some basic definitions are needed to be introduced to the readers. In Cryptography, a cipher is a pair of algorithms that create the encryption and the reversing decryption, so the first key word is *Algorithm*. *Algorithm* is a procedure or formula for solving a problem in finite sequence of steps, starting from an initial point, following the 'rules' ,eventually terminating at a final point. And we don't require each step in the algorithm is deterministic. Our main oberservation the Gaudry-Schost algorithm is a randomized algorithm, incorporate randomness. We give an instance to describe the definition.

Example 1. *Finding the smallest integer in a list of integers. To find the solution of this problem, we should look at every single integer in the list, assuming the first integer we picked up is the smallest, run a programme to check each of the remaining integers if it is smaller than the smallest integer so far, make a record of this new smallest integer, the last recorded smallest integer is the one we are looking for. Therefore the problem gets solved.*

In modern mathematics and computer science, an algorithm means a small procedure of solving a problem. And often we call a computer program an elaborate algorithm. The word algorithm is named after an Persian mathematican, Mohammed ibn-Musa al-Khwarizmi (780-850) [24]. It first published in Arabic language in the $9th$ century and later was translated into Latin in the $12th$ century. It was called Algorithmi de numero Indorum at that time. French introduced the word algorithm, but not its meaning, to Europe in the $17th$ century, following the model of the word logarithm. English adopted the French very soon afterwards, but the word 'Algorithm' took on the its current meaning only in the late $19th$ century. And now is well studied in search algorithms, sorting algorithms, merge algorithms, numerical algorithms, graph algorithms, string algorithms, computational geometric algorithms, combinatorial algorithms, medical algorithms, machine learning, cryptography, data compression algorithms and parsing techniques. To analyse the efficiency of an algorithm, one typically forcuses on the 'speed' of the algorithm, as a function of the size of the input on which it is run. We want the running time of the algorithm as short as possible.

The worst case and the average case of the algorithm are normally observed. The worst case is, just as its name implies, the slowest case of the algorithm. For example, suppose we are searching a list of N integers. Then we guaranteed to complete the task by using N operations, but we wish to solve the task less than N operations, hence it is the worst case of this algorithm. The average case is the number of running time that we expecte on average or we could say the expectation. The average case is usually hard to determine but is our main task

when solving the problem in theoretical analysis. Now we give the definition of the Discrete Logarithm Problem.

Definition 1. *Given a group G with group element $g \in G$. g has order r. The Discrete Logarithm problem (DLP) is: Given h be another group element of G to find n, if it exists such that $h = g^n$.*

In practice, the process of computing g^n could not be counted as a single basic operation. We introduced the 'Big-O' notation to help counting the number of running times.

Definition 2. *Let $f(x)$ and $g(x)$ be the functions of x, where x is a positive integer. $f(x) = O(g(x))$ if $f(x) \leq kg(x)$ for all $x \geq K$ when k and K are positive constants. Then we say 'f is big-O of g'. In particular, we write $f(x) = O(1)$ if $f(x)$ is bounded for all $x \geq K$.*

Proposition 1. *If the limit*

$$\lim_{x \to \infty} \frac{f(x)}{g(x)}$$

exists and is finite, then $f(x) = O(g(x))$.

Example 2. *Let $f(x) = 4x^3 - 12x + 14$ and $g(x) = x^3$, then*

$$\lim_{x \to \infty} \frac{4x^3 - 12x + 14}{x^3} = 4$$

Hence $4x^3 - 12x + 14 = O(x^3)$.

In Cryptography, there is another word that we use frequently, called 'Collision' or 'repeat', 'match'. We usually solve the DLPs by some 'Collision Algorithm'. For instance, Shank's Baby-Step Giant-Step algorithm, we split the steps of walks into two list:Baby list and Giant list. And when the collision happens between the two lists, then the DLP is solved. We'll give more details in Section 3. Note that the Birthday Paradox problem is also a typical collision type problem.

2 Birthday Paradox

Our main task is to present the theoretical analysis of the Gaudry-Schost algorithm, which is based on the Birthday Paradox type analysis. Hence, first of all, we need to know what the Birthday Paradox is and its analysis.

2.1 What is Birthday Paradox

In probability theory, Birthday paradox is well presented by Warren Weaver in his famous book "Lady Luck". [1]

"Suppose there are f people in a room. What is the probability that at least two of them share the same birthday – the same day of the same month? When there are$M = 10$ persons in a room together, this formula shows that the probability is $p = 0.117(11.7\%)$ that at least two of them have the same birthday. For $M = 22$ the formula gives $p = 0.476(47.6\%)$; whereas for $M = 23$ it gives $p = 0.507(50.7\%)$ Most people find this is surprising. But even more surprising is the fact that with $M = 50$ persons, the probability is $p = 0.970$. And with $M = 100$ persons, the odds are better than three million to one that at least two have the same birthday."

The proof of above fact is easy. For the trivial cases, when N = 365 and when N=1, we can easily get the probability that pair of people share a same birthday is 1(ignore the 29th of February and twins)(by the pigeon hole priciple) and 0, repectively. And for the general cases when $1 \leq M \leq 365$, the main idea is to compute the probability $Pr(f)$ that f people all have different birthdays first, then using $1 - Pr(f)$ to get the probability of "at least two people sharing the same birthday". It is easy to get the probability $Pr(f)$. There are 365 possible birthdays, note that the previous $M - 1$ people have taken up $M - 1$ of them. Hence the probability that the M^{th} person has his or her birthday among the remaining $365 - (M - 1)$ days is $\frac{365-(M-1)}{365}$, then compute the probability that every person's birthday is distinct from each other by using the multiplication principle.

$$\prod_{f=1}^{M} \frac{365 - (f - 1)}{365}$$

Therefore, the formula of getting the probabily p is

$$p(f) = 1 - Pr(f) = 1 - 1 \cdot (\frac{365 - 1}{365}) \cdot (\frac{365 - 2}{365}) \cdots (\frac{365 - (M - 1)}{365})$$

by assuming each day of the year equally probable for a birthday. Then we get the above results by subsitituting the values of M in this formla. Observe that when $M = 23$, the probability is approximately 50% and surprisinngly when $M = 57$ the probability goes up to 99%.

2.2 Birthday Paradox in Cryptography

In cryptography, our main observation is the expected running time of getting a collision and we expect to get the collision as fast as possible by using algorithms

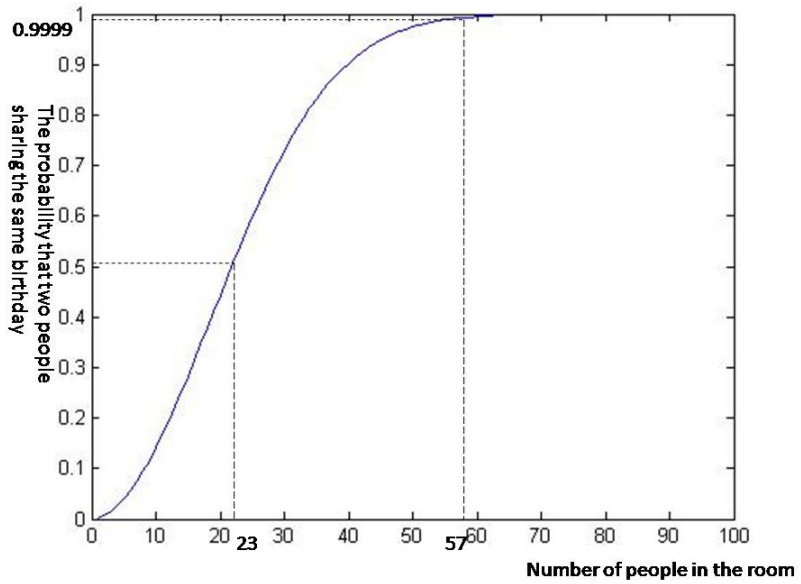

Figure 1: Birthday paradox

or say we are trying to make the expectation as small as possible. The Birthday Paradox Method is borrowed to analyse the expected running times.

Theorem 1. *Let S be a set of N elements. If elements in set S are selected uniformly at random, then the expected number of elements to be taken before some of them are selected twice is less than $\sqrt{\frac{\pi N}{2}} + 2$. The variance is appoximately $0.429N$.*

Here the expected value of a set is defined the same as the mean or average of the set.

Proof. Let X be the uniformly random variable that giving the number of elements selected from set S before some element is selected twice. Assuming the first l elements that we select from the set S are all different to each other, but the next element we select matches one of the previous item. Hence, to compute the expectation of this selection, we have to find out the probability $P(X > l)$

by the definition of the expectation.

$$E(X) = \sum_{i=1}^{\infty} i \cdot P(X = i) \tag{1}$$

$$= \sum_{i=1}^{\infty} P(X = i) \cdot (i - 1 + 1) = \sum_{i=1}^{\infty} Pr(X = i) \cdot \sum_{l=1}^{i} 1 \tag{2}$$

$$= \sum_{i=1}^{\infty} \sum_{l=1}^{i} Pr(X = i) = \sum_{l=1}^{\infty} Pr(X \geq l) = \sum_{l=0}^{\infty} Pr(X > l) \tag{3}$$

The probability $P(X > l)$ is given by the probability $P(N, l)$. Recall the formula of finding $Pr(f)$ is $\prod_{f=1}^{M} \frac{365-(f-1)}{365}$ in the above subsection 2.1, the way of finding the probability $P(N, l)$ is similar to how we find the $Pr(f)$.We now replace 365 possibles by N possibilities and M by l. Hence,

$$P(N, l) = \prod_{k=1}^{l} \frac{N - (k-1)}{N} = \prod_{k=1}^{l} 1 - \frac{k-1}{N}$$

, Now we apply the standard fact $1 - x \leq e^{-x}$ for $x \geq 0$. Therefore,

$$E(X) = \sum_{l=0}^{\infty} Pr(X > l) \tag{4}$$

$$= \sum_{l=0}^{\infty} P(N, l) \tag{5}$$

$$= \sum_{l=0}^{\infty} \prod_{k=1}^{l} 1 - \frac{k-1}{N} \tag{6}$$

$$\leq \sum_{l=0}^{\infty} \prod_{k=1}^{l} e^{-\frac{k-1}{N}} \tag{7}$$

$$= \sum_{l=0}^{\infty} e^{0} \cdot e^{-\frac{1}{N}} \cdot e^{-\frac{2}{N}} \cdot ... \cdot e^{-\frac{l-1}{N}} \tag{8}$$

$$= 1 + \sum_{l=1}^{\infty} e^{-\frac{l(l-1)}{2N}} \tag{9}$$

Since $l > l - 1 \Rightarrow (l-1)l > (l-1)^2 \Rightarrow -(l-1)l < -(l-1)^2$, and function $f(x) = e^{-x}$ is a monotone decreasing function, then

$$E(X) \leq 1 + \sum_{l=1}^{\infty} e^{-\frac{l(l-1)}{2N}} \leq 1 + \sum_{l=1}^{\infty} e^{-\frac{(l-1)^2}{2N}}$$

Since function $f(x) = e^{-x}$ is decreasing and take values $[0, 1]$ for $x > 0$, then as the figure 2 illustrates, we know the difference between sum and integral is at

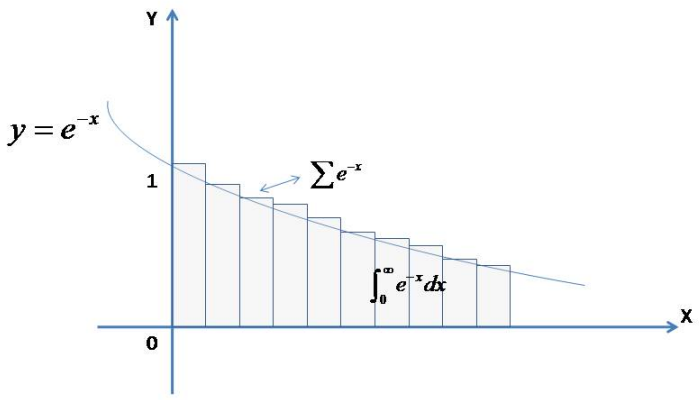

Figure 2: Integral and Summation

most 1. That is

$$\sum_{l=1}^{\infty} e^{\frac{-(l-1)^2}{2N}} \leq 1 + \int_0^{\infty} e^{-\frac{x^2}{2N}} dx$$

Let $u = \frac{x}{\sqrt{2N}}$, then $x = \sqrt{2N} \cdot u$

$$E(x) = 2 + \int_0^{\infty} e^{-x^2/2N} dx = 2 + \int_0^{\infty} e^{-u^2} d\sqrt{2N} \cdot u = 2 + \sqrt{2N} \int_0^{\infty} e^{-u^2} du$$

by using $\int_0^{\infty} e^{-u^2} du = \frac{\sqrt{\pi}}{2}$, we get

$$2 + \sqrt{2N} \int_0^{\infty} e^{-u^2} du = 2 + \sqrt{\frac{\pi N}{2}}$$

Therefore the solution in the theorem applies.

Now, for the proof of the variance $Var(X)$, we will use the formula $Var(X) = E(X^2) - E^2(X)$.

We've aleady seen $E(X) = 2 + \sqrt{\pi N/2}$, thus $E^2(X) = (2 + \sqrt{\pi N/2})^2 = 4 + \pi N/2 + 2\sqrt{2\pi N} \approx \pi N/2 + O(\sqrt{N})$. Now, we concentrate on $E(X^2)$. By the

definition of discrete random variable's expectation, we get

$$E(X^2) = \sum_{l=1}^{\infty} l^2 \cdot Pr(X = l) = \sum_{l=1}^{\infty} l^2 \cdot (Pr(X > l-1) - Pr(X > l)) \tag{10}$$

$$= \sum_{l=0}^{\infty} (l+1)^2 \cdot Pr(X > l) - \sum_{l=0}^{\infty} l^2 \cdot Pr(X > l) \tag{11}$$

$$= \sum_{l=0}^{\infty} (2l+1) \cdot Pr(X > l) = 2\sum_{l=0}^{\infty} l \cdot Pr(X > l) + E(X) \tag{12}$$

Now, the problem becomes what the value of term $\sum_{l=0}^{\infty} l \cdot Pr(X > l)$ is. And from the above argument in this section about $E(X)$. We've proven

$$Pr(X > l) = Pr(N, l) = \prod_{i=0}^{l-1}(1 - \frac{i}{N}) \leq \prod_{i=0}^{l-1} e^{-\frac{i}{N}} \leq e^{-\frac{(l-1)^2}{2N}}$$

Hence

$$\sum_{l=0}^{\infty} l \cdot Pr(X > l) \leq \sum_{l=0}^{\infty} l \cdot e^{-\frac{(l-1)^2}{2N}} = \sum_{l=0}^{\infty} (l+1) \cdot e^{-\frac{l^2}{2N}} = \sum_{l=0}^{\infty} l \cdot e^{-\frac{l^2}{2N}} + \sum_{l=0}^{\infty} e^{-\frac{l^2}{2N}}$$

To get the $E(X^2)$, we have to estimate these two terms $\sum_{l=0}^{\infty} l \cdot e^{-\frac{l^2}{2N}}$ and $\sum_{l=0}^{\infty} e^{-\frac{l^2}{2N}}$, espectively. The second one is easy, we've seen the function $y = e^{-x}$ is monotonical decreasing function, thus $\sum_{l=0}^{\infty} e^{-\frac{l^2}{2N}} \approx 1 + \int_0^{\infty} e^{-\frac{l^2}{2N}} dl$. Make the change of variable $u = l/\sqrt{2N}$ gives $\sqrt{2N}\int_0^{\infty} e^{-u^2} du$, and we know $\sqrt{2N}\int_0^{\infty} e^{-u^2} du \approx \sqrt{\frac{\pi N}{2}}$. Hence, the term

$$\sum_{l=0}^{\infty} e^{-\frac{l^2}{2N}} \approx 1 + \sqrt{\frac{\pi N}{2}}$$

Now,let's deal with the more complicated term $\sum_{l=0}^{\infty} l \cdot e^{-\frac{l^2}{2N}}$. It is difficult because of the factor "l". It makes difficulty to determine the monotonicity of function $z = \sqrt{2N}t \cdot e^{-t^2}$, where $t = l/s\sqrt{2N}$. To do that, we need to analyse the monotonicity of the function $w = 2t^2 + t - 1$. From the figure, we can see

$$0 \leq t < \frac{1}{2} \Rightarrow -1 \leq w < 0 \Rightarrow 0 < -\frac{w}{t} \leq 2 \Rightarrow 0 < 1 + \frac{1}{t} - 2t - 2 \leq 2$$

$$t \geq \frac{1}{2} \Rightarrow w \geq 0 \Rightarrow -\frac{w}{t} \leq 0 \Rightarrow \frac{1}{t} + 1 - 2t - 2 \leq 0$$

By the Taylor expansion series, $e^{2t+1} \approx 1 + 2t + 1 = 2 + 2t$. Thus $e^{2t+1} = e^{-t^2+(t+1)^2} \approx 2 + 2t$. Hence,from 2.2, we have $1 + \frac{1}{t} - e^{t^2 \cdot (t+1)^2} > 0 \Rightarrow (t +$

$1)e^{-(t+1)^2} > te^{-t^2}$ for $0 \leq < \frac{1}{2}$. And from 2.2, we have $(t+1)e^{-(t+1)^2} \leq te^{-t^2}$. That means, the function $z = t \cdot e^{-t^2}$ is monotonically increasing for $0 \leq t < \frac{1}{2}$, then reaches its peak value $\frac{1}{2} \cdot e^{-\frac{1}{4}}$, then becomes monotonically decreasing at $t > \frac{1}{2}$. Note that, when $t = 0, z = 0$ and $t = 1/2, l = \sqrt{2N}/2$. Thus

$$\sum_{l=0}^{\infty} l \cdot e^{-\frac{l^2}{2N}} = 2 \cdot \frac{\sqrt{2N}}{2} \cdot e^{-\frac{1}{4}} + \int_0^{\infty} l \cdot e^{-l^2/2N} dl \tag{13}$$

$$= \sqrt{2N} \cdot e^{-\frac{1}{4}} + \frac{1}{2} \int_0^{\infty} e^{-l^2/2N} dl^2 \tag{14}$$

$$= \sqrt{2N} \cdot e^{-\frac{1}{4}} - \frac{2N}{2} \int_0^{\infty} e^{-l^2/2N} dl^2/2N \tag{15}$$

$$= \sqrt{2N} \cdot e^{-\frac{1}{4}} - N(e^{-l^2/2N}|_0^{\infty}) \tag{16}$$

$$= \sqrt{2N} \cdot e^{-\frac{1}{4}} - N(0-1) \tag{17}$$

$$= \sqrt{2N} \cdot e^{-\frac{1}{4}} + N \tag{18}$$

Therefore, the variance of samples to be taken before some element is taken twice is

$$Var(X) = E(X^2) - E(X)^2 \tag{19}$$

$$= 2\sum_{l=0}^{\infty} l \cdot Pr(X > l) + E(X) - E(X)^2 \tag{20}$$

$$= 2(\sum_{l=0}^{\infty} l \cdot e^{-l^2/2N} + \sum_{l=0}^{\infty} e^{-l^2/2N}) + 2 + \sqrt{\frac{\pi N}{2}} - 4 - \frac{\pi N}{2} - 2\sqrt{2\pi N} \tag{21}$$

$$= 2N - \frac{\pi N}{2} + O(\sqrt{N}) \tag{22}$$

$$\tag{23}$$

Ignore the small terms $O(\sqrt{N})$, the variance of the birthday problem is around $0.429N$. □

3 Baby-Step Giant-Step Algorithm

Baby-Step Giant-Step algorithm (BSGS) due to Shanks [18] is well known on solving the discrete logarithm problems in the intervals. It is an example of collision ,or meet-in-the-middle, algorithm and also a naive way of solving the Discrete Logarithm Problem. And it is useful because the Baby-Step Giant-Step Algorithm can be applied to any group, not just $\mathbb{F}_q^*$, and the proof that it works is no more difficult for arbitrary groups.

In order to keep the consistency, we still continue using the notation of Discrete Logarithm Problems (DLP) definition, which we've given in the Section 1.

Definition 3. *Let G be a cyclic group, generated by the element g of order r, that is $G = \{g^i : i \in [0, r-1]\}$. Let n be a non-negative integer which satisfies $g^n = h$, where $h \in G$. We split integer n into two terms $\lambda m + \mu$, where $m = \left\lceil r^{\frac{1}{2}} \right\rceil$, $0 \leq \lambda, \mu \leq m, \lambda, \mu, m$ are integers. Then*

$$h = g^n = g^{\lambda m + \mu}$$

Hence,

$$h \cdot g^{-\lambda m} = g^{\mu}$$

Here, h,g,m are known. We just need to find the values λ and μ. One creates two sorted lists:

$$BabyList : g^0, g^1, g^2, \cdots, g^{r-1}$$

$$GiantList : h \cdot g^0, h \cdot g^{-m}, h \cdot g^{-2m}, h \cdot -3m, \cdots, h \cdot g^{-(r-1)m}$$

As running this two sorted lists, we get at least one value from Baby list matches one value from the Giant List. Hence, we get the value of n and the DLP is solved. We call this method Baby-Step Giant-Step Algorithm.

For example, we get g^{a_1} from the Baby List, get $h \cdot g^{-b_1 m}$from the Giant List (remember $0 \leq a_1, b_1 \leq r-1$).

$$g^{a_1} = h \cdot g^{-b_1 m} \Rightarrow g^{a_1 + b_1 m} = h \Rightarrow n = a_1 + b_1 m$$

Therefore, the problem has been solved. To explain the Baby-Step Giant-Step algorithm more precisely, we will give an example.

Example 3. *Using Shank's Baby-Step Giant-Step algorithm to solve the discrete logarithm problem*

$$g^n = hinmathbbF_p^* withg = 9782, h = 5739, andp = 17389.$$

The number 9782 *has order* 8694 *in mathbbF*$_1^*$7389. *Set* $m = \lceil \sqrt{8694} \rceil = 94$ *and make* $u = g^{-m} = 9782^{-94} = 396$. *One did a computer work and find that* $g^{88} = 12539, h \cdot g^{-94 \times 10} = 5739 \times 396^{10} = 12539$. *Thus,* $g^{88} = h \cdot g^{-940}$. *Therefore,* $g^{1028} = 5739, n = 1028$, *the discrete logarithm problem is solved.*

Algorithm 1 The Baby-Step Giant-Step algorithm

INPUT: A cyclic group G of order r, having a generator g and an element h.
OUTPUT: A value n satisfying $g^n = h$.

1: $m \leftarrow Ceiling(\sqrt{r})$
2: **for** all j where $0 \leq j < m$ **do**
3: Compute g^j and store (j, g^j) in a ordered table.
4: **end for**
5: Compute g^{-m}.
6: Let $V \leftarrow h$. (Set $V = h$)
7: **for** $i = 0$ to $(m - 1)$ **do**
8: Check to see if V is the second component (g^j) of any pair in the ordered table.
9: **if** **then return** $mi + j$.
10: **else**
11: **return** $V \leftarrow V \cdot g^{-m}$
12: **end if**
13: **end for**

The Baby-Step Giant-Step Algorithm requires about $O(\sqrt{r})$ running times and the space complexity, which is much faster than $O(r)$. But it is the disadvantange of using BSGS, too. Mathematicans discovered other algorithm to reduce the running times and the sample space.

4 Gaudry-Schost algorithm

In this section, we will introduce the Gaudry-Schost algorithm. It is helpful for solving the Discrete Logarithm Problems (DLP) in a short interval. The basic idea of the Gaudry-Schost method is the same as the Pollard's kangaroo method with the van Oorschot and Wiener formulation. The key idea of their formulation is: One uses a herd of $N/2$ tame kangraroos and a herd of $N/2$ wild kangaroos. Then wish to get a collision between the two differnt teams of kangaroos, but not the self collisions. Hence the Discrete Logarithm is solved. Unlike Shank's Baby-step Giant-step method, it doesn't require to store every single point in the pseudorandom walks but the distinguished points. We use the distinguished points idea to the Gaudry-Schost method in order to accelerate the algorithm. It helped us reducing the sample space. One also finds it can further reduce the storage and make the Gaudry-Schost algorthm faster by using the equivalence classes. However, to define the representitives of the equivalence classes and at the meantime also keep the walks being uniformly at random becomes a problem. We try to analysis this problem by using the Galbraith-Rupai algorithm in this section. The main difference between the Gaudry-Schost algorithm and the Pollard's kangaroos is the Gaudry-Schost will restart a new walk while the kangaroos would keep running. And also the theoritical analysis is different. The Gaudry and Scost is built on birthday paradox type analysis and it is heuristic, kagaroos are based on another approach.

The definition of Discrete Logarithm Problem (DLP) in an interval is: Given a cyclic group G and a positive integer N, a group element $g \in G$ with order r, and another group element h such that $h = g^n$ where $0 \leq n \leq N$ (N is less than r). To compute n.

4.1 1-Dimensional Gaudry-Schost Algorithm

4.1.1 Definition in 1-Dimensional

First, we shift the interval from $[0, N]$ to $[-\frac{N}{2}, \frac{N}{2}]$, since the points on interval $[-\frac{N}{2}, \frac{N}{2}]$ are symmetric by the origin 0. To do that without loss of generality, we replace the group element h by $h' \cdot g^{-\frac{N}{2}}$. Therefore,

Definition 4. *Let G be a group with elements $g, h \in G$ such that $h = g^n$ for some $-\frac{N}{2} \leq n \leq \frac{N}{2}$ where N is a positive even number. Run a large number of pseudorandom walks. record each element of the walk, alternatively, 'tame walk' (T) with form g^a*

$$T = \{a| - \frac{N}{2} \leq a \leq \frac{N}{2}\}$$

with a is known and 'wild walk' (W) with form hg^a

$$W = n + T = \{n + a | a \in T\}$$

where n is defined above.

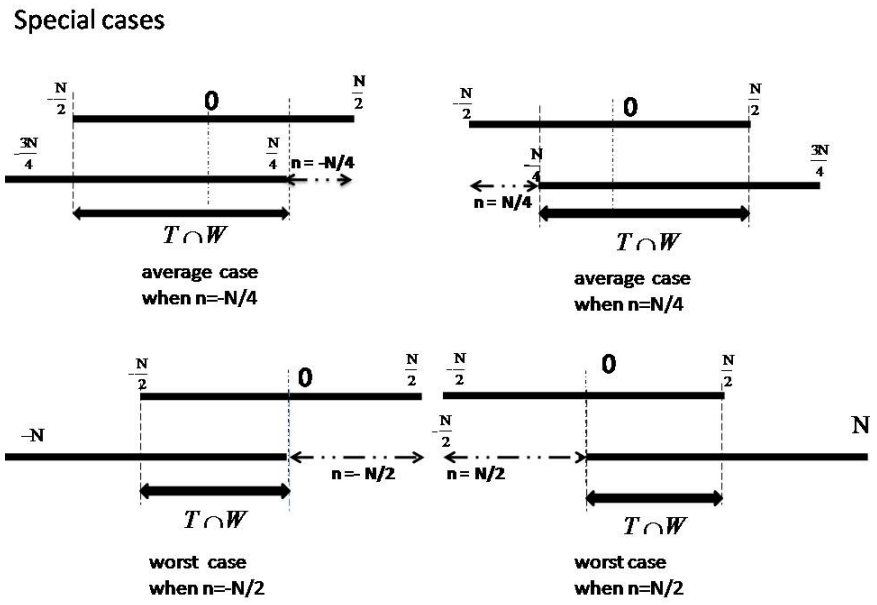

Figure 3: Examples of 'overlap' $T \cap W$ in linear case

Now, walks will keep on running until a distinguished point is hit, then we record the distinguished point, the type of this walk and also, of course, the value of a, restart a new pseudorandom walk, repeat this process until the same distinguished point is visited by two different types of the walks, that means we have $g^{a_1} = hg^{a_2}$,that implies $h = g^{a_1 - a_2}$, hence the DLP is solved.

4.1.2 Theoretical Analysis in 1D

Now, we present a theoretical analysis of the Gaudry-Schost algorithm. Our main result is the expectation of the Discrete Logarithm Problems in a short interval and it has been analysed by Nishmura and Sibuya [6] and Selivanov [8]. It is a birthday paradox type of approach (Pollard's Kangaroos used another different theoretical analysis). And we call it 'Tame Wild Birthday Paradox' (TWBP).

Theorem 2. *Let S be a set of N elements. If elements are samoled uniformly at random with replacement. Record the elements, alternatively, into two lists. Then the expected number of elements that need to be made in total before a coincidence happenned between the lists is $\sqrt{\pi N} + O(1)$*

Proof: See Nishimura and Sibuya[6]

The collision wouldn't appear if the Tame set and the Wild set do not intersect. Hence, we are only interested in $T \cap W$, and often we call it 'overlap'.

First we observe the average case and the worst case. We'll use some charts in 4.1.2 to illustrated those cases. From the definition of Gaudry-Schost algorithm, our n is an integer in the set $\frac{-N}{2} \leq n \leq \frac{N}{2}$. And the positive or the negative sign of n just points out the moving directions of the wild set. For instance, as illustrate in the chart 4.1.2, the elements on the Wild Set move to the 'left' when $n = -\frac{N}{4}$ and move to the 'right' when $n = \frac{N}{4}$, but the intersection $T \cap W$ of both cases are $\frac{3N}{4}$. The worst case is $n = \frac{N}{2}$ and $n = \frac{N}{4}$ is the average case. In other words, $|T \cap W| = \frac{N}{2}$ in the worst case and $|T \cap W| = \frac{3N}{4}$ in the average case.

Define that a collision between the Tame set T and the Wild set W is a $T - W$ collision. Since in the discrete logarithm problems in a short interval, we don't consider the self-collision cases. We expect the number of sellections as small as possible. We apply the theorem 2 in $T \cap W$ to get the expected running time of n.

Theorem 3. *Sampling elements uniformly at random,with replacement and alternately recorded in the Tame set T and the Wild set W. Then the expected number of selections, over all instances, is* $2.08\sqrt{N}$

Proof. By symmetry, we consider $n \in [0, \frac{N}{2}]$ instead of $n \in [-\frac{N}{2}, \frac{N}{2}]$. First, we need to find how many number of elements we expect to choose for tame set and wild set. To do that, we need find the number of elements in $|T \cap W|$, since by theorem 2, the expeced number of selections is roughly $\sqrt{\pi R}$, and the orders of the Tame set and the Wild set are $\frac{R}{2}$ by the definition of Gaudry-Schost algorithm. Then the problem seems to be solved.

As the picture illustrated, let $n = xN$, since $n \in [0, \frac{N}{2}]$, then $x \in [0, \frac{1}{2}]$.Note that the absolute value here means the length of interval, not for counting points on the interval.

$$|T \cap W| = N - n = N - xN = N(1 - x)$$

we expect to select $\sqrt{\pi R} = \sqrt{\pi N(1-x)}$ Hence, half of them came from T. Then the number of samples we expected to pick up from T is

$$\left.\begin{array}{c} \frac{|T|}{|T \cap W|} \cdot \frac{1}{2}\sqrt{\pi N(1-x)} \\ |T \cap W| = N(1-x) \\ a \in [-\frac{N}{2}, \frac{N}{2}] \Rightarrow |T| = N \end{array}\right\} \frac{N}{N(1-x)} \cdot \frac{1}{2}\sqrt{\pi N(1-x)} = \frac{1}{2}\sqrt{\frac{\pi N}{1-x}}$$

The same argument applies to W set. Hence $|W| = N$ as $W = \{n + a | a \in [-\frac{N}{2}, \frac{N}{2}]\}$.

$$\frac{|W|}{|T \cap W|} \cdot \frac{1}{2}\sqrt{\pi N(1-x)} = \frac{N}{N(1-x)} \cdot \sqrt{\pi N(1-x)} = \frac{1}{2}\sqrt{\frac{\pi N}{1-x}}$$

Together, we expected to pick up $\sqrt{\frac{\pi N}{1-x}}$ group elements. Therefore, we average this over all applications is

$$2\int_0^{1/2} \sqrt{\pi N} \cdot \frac{1}{\sqrt{1-x}} dx = 2\sqrt{\pi N} \cdot \int_0^{1/2} (1-x)^{-\frac{1}{2}} dx = 2\sqrt{\pi N} \cdot (2 - \sqrt{2}) \approx 2.08\sqrt{N}$$

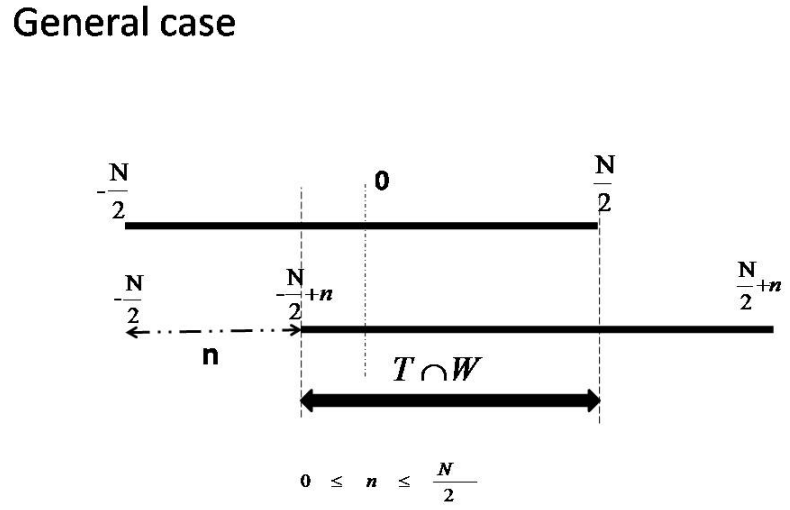

Figure 4: General case of overlap $T \cap W$ in linear case

We multiply by 2 in front because we've restrict the value of x to the interval $[0, 1/2]$ instead of $[-1/2, 1/2]$.

□

4.1.3 Pseudorandom walks and Practical Considerations

The Practical experiments are also considered by Gaudry and Schost. Their goal is to reduce the amount of storage. The algorithm requires $O(\sqrt{N})$ steps, but we don't want to record them all. In order to do that, the distinguished points due to van Oorschot and Wiener point of view are used. We only store the distinguished points instead of every points of pseudorandom walks, that is about $(\theta\sqrt{N})$ group elements, where θ is the probability of a randomly selected an element from a group is a distinguished point. Recall every step is multiplication by g^{a_i} where $a_i \in Z$.Define m is the mean step size of jumps $|a_i|$. We use absolute value here since our main focus is Gaudry-Schost algorithm. It is a 'side-to-side' walk.

Birthday Paradox requires selecting samples uniformly at random, so does Tame-Wild Birthday Paradox. Practical experience shows that we partition the group into n_s parts when n_s is large, then the pseudorandom walks is closed enough to the truely random walks, hence the Tame-Wild Birthday Paradox $(TWBP)$. For the analysis we recall the Cofman, Flajolet, Flatto and Hofri's[9] result.

Lemma 1. *Let $y_0, y_1, \cdots, y_k$ be a symmetric random walk that starts at the origin ($y_0 = 0$) and takes steps uniformly distributed in $[-1, +1]$ then the expected maximum excursion is*

$$E(max|y_i| : 0 \leq i \leq k) = \sqrt{\frac{2k}{3\pi}} + O(1)$$

Here $m = \frac{1}{2}$ by the definition of symmetric random walk. Since θ is the probability that an element in the group is a distinguished point, then the walk is about $\frac{1}{\theta}$ long. Applying the above lemma 1, let $k = \frac{1}{\theta}$, then it takes about $l \cdot \frac{1}{\sqrt{\theta}}$ steps, where $l = \sqrt{\frac{2}{3\pi}}$. And we know the average size of each step is m. Therefore, the average distance of the random walk in total is approximately $\frac{m}{\sqrt{\theta}}$. It natually needs to make the value of $\frac{m}{\sqrt{\theta}}$ large so that it behaves like a truly random walk. Otherwise, the walk would stay around and close to the starting point. But there is also a bad point for making the value of $\frac{m}{\sqrt{\theta}}$ large, that is when the pseudorandom walks oversteps the boundaries. It is not included in our probabilistic analysis and they are 'waste' steps. Hence, to make the pseudorandom walks act exactly like a random walk, we use a small factor $(1 + \epsilon)$ in the heuristic result. And in practice, after the distinguished point is detected and stored in the server, we still need to wait another $1/\theta$ steps until the same distinguished point is hit again. Therefore,

Heuristic 1. *The average expected running time of solving a DLP in an interval of size N by using Gaudry-Schost algorithm is $2.08(1 + \epsilon)\sqrt{N} + 1/\theta$ group operations where ϵ is small.*

We find that the Gaudry-Schost algorithm is not as fast as the van Oorschot and Wiener view of Pollard Kangaroo algorithm, Hence we introduce the Equivalence classes of a group to improve the Gaudry-Schost algorithm over the DLP in an short interval.

4.2 Equivalence Classes

Gallant, Lambert and Vanstone and Wiener and Zuccherato presented that the Pollard's ρ method for some cases can be sped up by defining pseudorandom walks on a set of equivalence classes instead of over the group. For our case – the DLP in a short interval, we define equivalence classes is a set of elements whose discrete logarithm still lie in the interval. Then it requires to think about its unique representitive of the equivalence classes,and the unique representitive of the equivalence classes can be computed efficiently When any group element is given. To explain this idea, we will give an example.

Example 4. *Let G be a cyclic group over a finite field $mathbbF_q$ (q is an odd prime) and $g \in G$ with order r. Define an equivalence relation $x \equiv x^{-1}$, where group element x^{-1} is the inverse element of x in G. That means if $x = g^a h^b$ then $x^{-1} = g^{-a} h^{-b}$. Most often we consider elliptic curves over a finite field as an instance since if we know one point $P = (x_P, y_P) \in mathbbE$, then we*

can immediately get its inverse point $-P = (x_P, -y_P)$ *as elements are pairly symmetrical by the x-axis. Therefore the computation is shorten to its half. Hence define* $\widehat{x} = \max\{x, x^{-1}\}$ *as the representative of our equivalence class.*

There are two things need to be metioned. First, the Side-to-Side walks. Consider the group elements pairly by equivalence classes, such as g, g^{-1}. If g is $[0, \frac{N}{2}]$, then clearly, g^{-1} is in $[-\frac{N}{2}, 0]$. Even for the identity element of the elements who is equal to its inverse. Hence it is a side-to-side walk, we naturally apply the Gaudry-Schost method on it instead of the Standard Pollard Kangaroos. And it is also the reason why we defined the values of a in the interval $[-\frac{N}{2}, \frac{N}{2}]$ instead of the interval $[0, N]$. Second, the equivalence classes may cause some small cycles.

Example 5. *In the above instance, we defined* $x \equiv x^{-1}$ *as the equivalence relation to the pseudorandom walks start with* x_0 *(note that* x_0 *can be any element in the group). Let* $x_i = \widehat{x_i}$ *and* $x_{i+1} = \widehat{x_i}g$*, suppose* $\widehat{x_{i+1}} = x_{i+1}^{-1}$ *and* $S(\widehat{x_{i+1}}) = S(\widehat{x_i})$*, then* $x_{i+2} = \widehat{x_{i+1}}g \equiv {x_{i+1}}^{-1}g = (\widehat{x_i}g)^{-1}g = g^{-1}{\widehat{x_i}}^{-1}g = {\widehat{x_i}}^{-1} \equiv x_i$*. That is a cycle of size 2.*

These sort of cycles would interfere the pseudorandom walk and make walks never reach a distinguished point. But these cycles can be detected by computing and storing a small amount of extra steps. Gallant, Lambert and Vanstone, and Wiener and Zuccherato[4] noticed and introduced a dealing method which is called *Collapsing the cycle*. And Bos Kleinjung and Lenstra showed a theoretical analysis in their paper.[3]

4.3 The Gaudry-Schost Algorithm on Equivalence Classes

Now, we apply the Gaudry-Schost algorithm on equivalence classes to solve the Discrete Logarithm Problems in an interval of size N. Recall that the Discrete Logarithm Problems (DLP) in an interval $[-\frac{N}{2}, \frac{N}{2}]$ is, $G = \langle g \rangle$, group element g has order r. Another group element $h \in G$. We wish to get n such that $h = g^n$. But the Tame set and Wild set are defined slightly different from the Gaudry-Schost algorithm. We make the walks defined on pairs $(P, -P)$.

Definition 5. *Let the notations as above. But*

$$T = \{\{a, -a\} | a \in [-\frac{N}{2}, \frac{N}{2}]\}$$

$$W = \{\{-n - a, n + a\} | a \in [-\frac{N}{2}, \frac{N}{2}]\}$$

where a is known from the pseudorandom walk.

As we described before, the collision should be in the intersection $|T \cap W|$. Otherwise, we can't find any matches. The whole Gaudry-Schost algorithm analysis idea is based on the Birthday Paradox, which requests sampling uniformly at random. Hence,the trick is to determine whether it still works on the equivalence classes.

Example 6. *Let $a = \frac{N}{6}$, $n = \frac{N}{6}$. Let P be the point in the wild set regarding a and n, as the figure illustrate. But the problem is point P is of form $n + a$ or of form $-n - a'$. In fact, both of the forms can express a same point by choosing the different value of as. In our case, when $a' = -(2n + a) = -\frac{N}{2}$, then $n + a = \frac{2N}{6} = \frac{N}{3} = -n - a' = -\frac{N}{6} - (-N) = \frac{2N}{6} = \frac{N}{3}$.*

From the above example, we see there exists two different values of a for a same point P in some part of the interval. In other words, some points are selected ununiformly. We need to identify those parts out from $|T \cap W|$, hence we need a new algorithm.

4.3.1 Galbraith-Ruprai Algorithm

Recal that G is a cyclic group with group elements g and h under relation $h = g^n$ in the interval $[-\frac{N}{2}, \frac{N}{2}]$, in order to find out n, we alternatively record the pseudorandom walks in Tame set and Wild set. But this time, we make the wild set smaller.

Definition 6. *Let $4|N$,*

$$T = \left\{ \{a, -a\} | a \in [-\frac{N}{2}, \frac{N}{2}] \right\}$$

,

$$W = \{\{-n - a, n + a\} | a \in [-\frac{N}{4}, \frac{N}{4}]\}$$

In the Galbraith-Ruprai algorithm, one successfully defined the pseudorandom walk on a set of equivalence classes. This time, when a distinguished point is hit by a walk, we store the representative of the equivalence class, the discrete logarithm and a flag indicating the 'type' of walk. Then as previously, when the same representative is visited by another set, then the DLP is solved. The theoretical analysis of the Gaudry-Schost algorithm is based on the Birthday Paradox (recall 'TWBP'). We expect to sample uniformly at random. But the equivalence class often causes some confusing. In order to dealing with that we redefine a 'fundamental domain' for the Tame sets and the Wild sets. The advantage of doing that is to make the points 'one to one correspondence' and easy to determine the area of intersection $|T \cap W|$ where our 'T-W' collision happens. For the Tame set, let the fundamental domain of Tame is $\widetilde{T} = \{\{a, -a\} | a \in [0, \frac{N}{2}]\}$. Apparently, elements are selected one-to-one correspondence since we only consider values of a here. Now for the Wild set,

Our Wild set is defined as $\widetilde{W} = \{\{-n - a, n + a\} | a \in [-\frac{N}{4}, \frac{N}{4}]\}$. But now we only consider the positive values ,then we fold the negative part to positive (Some part of the interval are overlapping at this time, we call it 'double density'). Hence the fundamental domain of the Wild set $\widetilde{W}$ is a multiset $\widetilde{W} = |n| + a, -(|n| + a) | a \in [0, |n| + \frac{N}{4}] + [0, \frac{N}{4} - |n|]$. As the figure 6 illustrates, when $|n| > \frac{N}{4}$, we are sampling uniformly from the Wild set. But when $|n| \leq \frac{N}{4}$, samples are selected with probability $\frac{4}{N}$ for the 'double density' part

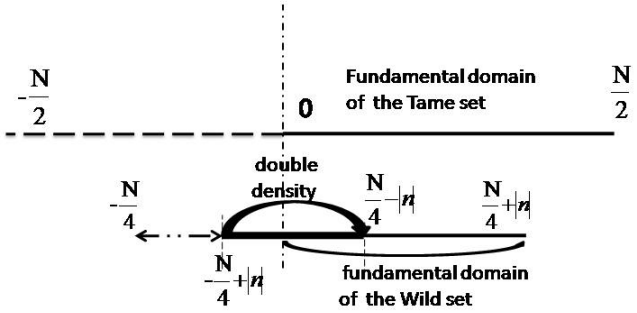

Figure 5: Fundamental domain in the 1D case

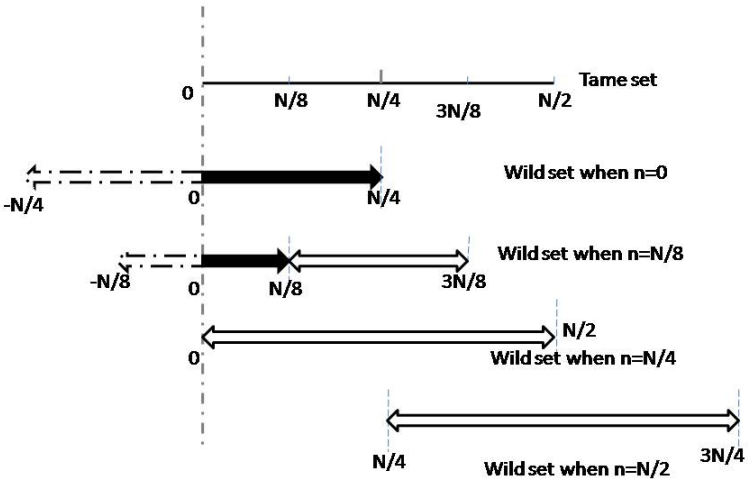

Figure 6: Double density in the 1D case

$a \in [0, \frac{N}{4} - |n|]$, and with probability $\frac{2}{N}$ for the part $a \in [\frac{N}{4} - |n|, \frac{N}{4} + |n|]$. To analyse the expectation of our new algorithm, we need consider its generalisation first.

Theorem 4. *Let $R \in N$ and $0 \leq A \leq \frac{R}{2}$. There are unlimited number of balls (they are exact the same but the colour) and R urns. We pick up the balls and recolour them to red and blue, alternatively, then drop these coloured balls into the urns uniformly at random but with different probabilities. For the red balls, the probability is $1/R$ for all the urns. For the blue balls, (1),the probabilities from urn 1 to urn A is $2/R$. (2), the probabilities from urn $A+1$ to urn $R-A$ is $1/R$. (3), the probabilities from urn $R-A+1$ to urn R is 0.Then the expected number of selection is $\sqrt{\pi R} + O(R^{\frac{1}{4}})$ balls to get at least one red ball and one blue ball in the same urn.*

To explain the idea of this theorem, we use the following claim which is given by Galbraith and Holmes[2].

Lemma 2. *There are unlimited number of balls (only colour different) and R urns. We pick up the balls and recolour them to colour 1 and colour 2, with probabilities $q_c, (c = 1, 2)$, then drop these coloured balls into the urns. And the probability of dropping in the a^{th} urn is $q_{c,a}$ and $q_{c',a}$ for the red balls and the blue balls, respectively. To get at least one red ball and one blue ball in the same urn, we expect to select*

$$\sqrt{\frac{\pi}{2 \cdot A_N}} + O(N^{\frac{1}{4}})$$

balls , where

$$A_N = \sum_{c=1}^{2} q_c \Big(\sum_{c'=1, c \neq c'}^{2} \big(\sum_{a=1}^{R} q_{c,a} \cdot q_{c',a} \big) \Big)$$

.

Applied the result in theorem 4,

$$\begin{aligned} A_R &= \frac{1}{2}\Big(\frac{1}{2}\big(A \cdot \frac{2}{R} \cdot \frac{1}{R} + (R - A - A) \cdot \frac{1}{R} \cdot \frac{1}{R} + (R - R + A) \cdot 0 \cdot \frac{1}{R}\big)\Big) && (24) \\ &\quad + \frac{1}{2}\Big(\frac{1}{2}\big(A \cdot \frac{2}{R} \cdot \frac{1}{R} + (R - A - A) \cdot \frac{1}{R} \cdot \frac{1}{R} + (R - R + A) \cdot 0 \cdot \frac{1}{R}\big)\Big) && (25) \\ &= 2 \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{R} && (26) \\ &= \frac{1}{2R} && (27) \end{aligned}$$

Hence, the expected number of experiments we should make in total before two different colour balls are dropped in a same urn is

$$E = \sqrt{\frac{\pi}{2 \cdot \frac{1}{2R}}} + O(R^{\frac{1}{4}})$$

The expected number of steps that we make before a $T - W$ collision happen is $\sqrt{\pi R} + O(R^{\frac{1}{4}})$. Also note that the probability could help increasing the chance of getting collisions.

Theorem 5. *Sampling uniformly at random with replacement alternately from the Tame set and the Wild set. The expected number of selections that we need to make, over all instance, before a Tame-Wild collision happen is*

$$(\frac{5\sqrt{2}}{4} - 1)\sqrt{\pi N} \approx 1.36\sqrt{N}$$

Proof. Apply theorem 4 in this proof. Ignore the small terms $O(R^{\frac{1}{4}})$. The only problem is $|T \cap W|$(Note that the absolute value here means the length of intersection $T \cap W$). Let $h = g^{xN}, x \in [0, \frac{1}{2}]$, Consider the positive half of x, as using the equivalence class one can determine element $-x$ immediately. For the Tame set, all the values of a are sampled uniformly and the size of tame set is $\frac{N}{2}$. From the discussion of fundermental domain, we consider the wild set in two cases: (i) $0 \leq x < \frac{1}{4}$ (ii)$\frac{1}{4} \leq x \leq \frac{1}{2}$.Case(i), some of the elements in the wild set are not uniformly selected because of the double density part. Now the number of steps we expected to select depends on the tame set, since the tame set is sampled uniformly and the size of the tame set is $\frac{N}{2}$,.Hence, the above theorem 5 can be applied and the expected number of group operations to get a collision is $\sqrt{\pi \cdot \frac{N}{2}}$. Case(ii), first, we need find $|T \cap W|$. From the figure,

$$|T \cap W| = N - \frac{N}{4} - xN = \frac{3N}{4} - xN$$

$$R = |T \cap W| = \frac{3N}{4} - xN$$

We know half of the walks are tame walks and half are wild walks, thus for each set we require selecting

$$\frac{|T|}{|T \cap W|} \cdot \sqrt{\pi |T \cap W|} = \frac{\frac{1}{2}N}{N(\frac{3}{4} - x)} \cdot \sqrt{\pi N(\frac{3}{4} - x)} = \frac{1}{2}\sqrt{\frac{\pi N}{\frac{3}{4} - N}} = \sqrt{\frac{\pi N}{3 - 4x}}$$

Since$|T| = |W| = \frac{N}{2}$. Hence,the expected running time of the algorithm is $2 \cdot \sqrt{\frac{\pi N}{3-4x}}$. Average this over all problem instance as

$$\frac{1}{2}\sqrt{\frac{\pi N}{2}} + 2\int_{\frac{1}{4}}^{\frac{1}{2}} 2 \cdot (3 - 4x)^{-\frac{1}{2}}\sqrt{\pi N}dx = \frac{\sqrt{2}}{4} \cdot \sqrt{\pi N} - \sqrt{\pi N} \cdot (1 - \sqrt{2}) \quad (28)$$

$$= \sqrt{\pi N}(\frac{5}{4}\sqrt{2} - 1) \quad (29)$$

□

We still use the Greek letter ϵ to express the undesirable properties of the pseudorandom walk.

Heuristic 2. *The average expected running time of solving a DLP in an interval of size N by using the impoved Gaudry-Schost algorithm is $1.36(1+\epsilon)\sqrt{N}+1/\theta$ group operations where ϵ is small.*

4.4 Solving 2-Dimensional DLP

There are still a lot of applications relating the Discrete Logarithm Problem in 2-dimensional or even higher dimensional, such as, computing the number of points on genus 2 curves over finite fields [10]; Computing the Gaudry-Schost low-memory algorithm by Gaudry and Schost [11] and by Weng [12]; It also arises ecplicitly in the work of Brands [13] and Cramer, Gennaro and Schoenmakers [14]. It helped understanding the security of the Gallant, Lambert and Vanstone (GLV) method in speeding up elliptic curve arithmetic [5] or helped Koblitz in using Koblitz curves to efficient elliptic curves cryptography [17]. See Galbraith and Scott [15] and Galbraith, Lin and Scott [16] for examples. Hence, the Multi-Dimensional Discrete Logarithm Problem is really worth to be studied. Our main observation in this section is the 2-Dimensional case.

4.4.1 Definitions of 2-Dimensional DLP

First, we update the definition of the Gaudry-Schost type Discrete Logarithm Problem in the 2-Dimensional.

Definition 7. *Let G be a group with elements g_1, g_2, h' and bounds $N_1, N_2 \in Z$, and the relation among them is $h' = g_1^{n_1} g_2^{n_2}$ where $0 \leq n_1 \leq 2N_1$, and $0 \leq n_2 \leq 2N_2$, compute n_1, n_2.*

Convenient for using the equivalence classes to accelrate the algorithm, we shift the domain of x_1, x_2 to $-N_1 \leq x_1 \leq N_1, and - N_2 \leq x_2 \leq N_2$. We can do this since we can redefine the element $h = h' \cdot g_1^{-N_1/2} g_2^{-N_2/2}$, and the benifit of doing that is the new domain is a rectangle centred at origin 0. Like the linear case, in the Gaudry-Schost algorithm, we need to define Tame set and Wild set for the 2-Dimensional case. To do that, we first let the pseudorandom walks be the same as the linear problem, but in a plane.

Definition 8. *Randomly choose a point whose coordinate is (a_0, b_0). Define a function f, such that*

$$(a_1, b_1) = f(a_0, b_0), (a_2, b_2) = f(a_1, b_1), \cdots, (a_{k+1}, b_{k+1}) = f(a_k, b_k)$$

We say these walks are pseudorandom walks in the 2-Dimensinal discrete logarithm problems.

We still alternatively record the walks into two sets calling "Tame" set and "wild" set.

$$T = \{(a, b)| - N_1 \leq a \leq N_1, -N_2 \leq b \leq N_2\}$$

$$W = \{(n_1 + a, n_2 + b)| - N_1 \leq a \leq N_1, -N_2 \leq b \leq N_2\}$$

4.4.2 Theoretical Analysis

In Gaudry-Schost paper, they didn't give details about the running time of the Gaudry-Schost algorithm in 2D case, but we will do it precisely by using

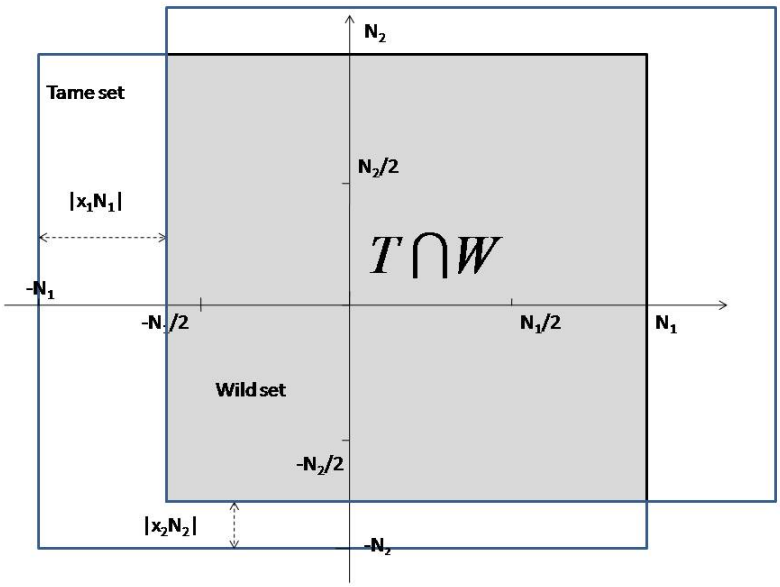

Figure 7: Gaudry-Schost heuristic in the 2D case

the usual assumption. Recall that the $T - W$ type collisions only occur in the intersection $|T \cap W|$, Hence we naturally observe the intersection $|T \cap W|$ in the 2-dimensional problem, and we call $|T \cap W|$ the overlap.

Heuristic 3. *The average expected running time of solving a DLP in 2D case by using the Gaudry-Schost algorithm is* $2.43(1+\epsilon)\sqrt{N} + 1/\theta$ *group operations where* ϵ *is small.*

It is still based on the Birthday Paradox type analysis. And the theorem which Galbraith and Holmes presented in their paper [2] 2 is a very useful tool for our proof. Here, we pick up walks instead of balls and record the walks into two sets tame and wild instead of two colours, thus $q_t = q_w = \frac{1}{2}$, lemma 2 can be used in proving our 2D DLP. Since N is a large integer, then we normally don't count the small term $O(N^{1/4})$. The probabilities of walks in the tame set and the wild set are $p_t = p_w = 1/N$, as the areas of tame and wild are $|T| = |W| = 2N_1 \cdot 2N_2 = N$. Let $n_1 = x_1N_1, n_2 = x_2N_2$, where $0 \leq |x_1|, |x_2| \leq 1$, thus $|T \cap W| = (2N_1 - x_1N_1)(2N_2 - x_2N_2) = N_1N_2(2-x_1)(2-x_2) = \frac{N}{4}(2-x_1)(2-x_2)$. Our

$$A = 2 \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{N} \cdot \frac{1}{N} \cdot \frac{N}{4}(2-x_1)(2-x_2) = \frac{(2-x_1)(2-x_2)}{8N}$$

Therefore,the expected number of running time over all instances (ignore the

small terms) is

$$E = \sqrt{\frac{\pi}{2A}} = \sqrt{\frac{8\pi N}{2}} \int_0^1 \int_0^1 (2-x_1)^{-\frac{1}{2}} (2-x_2)^{-\frac{1}{2}} dx_1 dx_2 \tag{30}$$

$$= 2\sqrt{\pi N} \cdot (-2) \cdot (-2) \cdot (2-x_1)^{\frac{1}{2}} |_0^1 \cdot (2-x_2)^{\frac{1}{2}} |_0^1 \tag{31}$$

$$= 8\sqrt{\pi N} \cdot (1-\sqrt{2})^2 \tag{32}$$

$$= 8\sqrt{\pi N}(1+2-2\sqrt{2}) \tag{33}$$

$$= 2.43\sqrt{N} \tag{34}$$

The small factor $(1+\epsilon)$ is used to make the pseudorandom walk act like a truly random walk. And in practice, it takes extra $1/\theta$ steps to get the distinguished point hitted again. Together, we get our heuristic result $2.43(1+\epsilon)\sqrt{N} + 1/\theta$ for ϵ is small.

4.4.3 Accelerating the algorithm

We've seen the improved Gaudry-Schost algorithm gets accelerated by using the equivalence classes in the 1-Dimensional Discrete Logarithm Problem and the expectation of sampling elements is approximately $1.36\sqrt{N}$ rather than $2.08\sqrt{N}$. Now, we apply the updated 2-D Gaudry-Schost algorithm on equivalence classes to solve the 2-Dimensional DLP. For example, group element h corresponding to (x, y) in the plane, then h^{-1} corresponds to $(-x, -y)$. One can make pseudorandom walks in the half size of the tame set to save the running times, like we did in the linear case. Now to the 2D problem, we need consider the definition of the Tame set and the Wild set. Precisly, let

$$T = \{\{(a,b),(-a,-b)\} : -N_1 \leq a \leq N_1, -N_2 \leq b \leq N_2\}$$

be the set of equivalence classes of points in a box of area $N = 2N_1 \cdot 2N_2$ centred at 0. For the discrete log (n_1, n_2) where $-N_1 \leq n_1 \leq N_1, -N_2 \leq n_2 \leq N_2$, the Wild set is considered as

$$W = \{\{(n_1+a, n_2+b),(-n_1-a,-n_2-b)\} : -\frac{N_1}{2} \leq a \leq \frac{N_1}{2}, -\frac{N_2}{2} \leq b \leq \frac{N_2}{2}\}$$

.To analyse the algorithm again we requires visualising the sets via a 'fundamental domain'. The map $(a, b) \mapsto (-a, -b)$ is rotated by 180^0 a natural fundemental domain is the halfplane $b \geq -\frac{N_2}{N_1}a$ in the plane. Therefore the fundamental domain $\widetilde{T}$ for the Tame set would be

$$\widetilde{T} = \{(a,b) : -N_1 \leq a \leq N_1, -\frac{N_2}{N_1}a \leq b \leq N_2\}$$

To define the fundamental domain of the Wild set $\widetilde{W}$, which is contained in the Tame set, is easy. Note that one just needs to pay attention to when $0 \leq n_1 \leq N_1,$ and $0 \leq n_2 \leq N_2$, like the multi-set case in the linear case, there

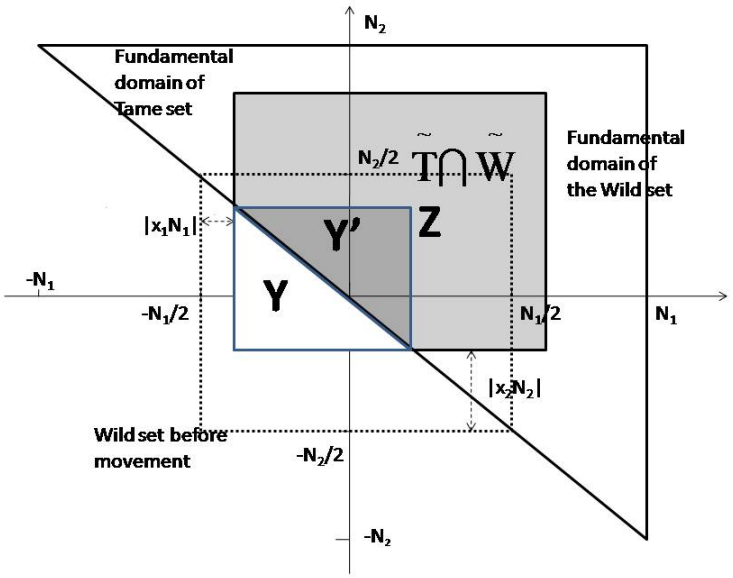

Figure 8: Case 1 of 2D in Rotation 180^o:when $0 \leq |x_1|, |x_2| < \frac{1}{2}$

is some 'double density' area in this situation. But by applying the theorem 2 [2], nomatter what the shape of the overlap is in this case, we can always put it back to its original place, consider the whole region as 'single density' (each point in this region is counted once), then the area of the $\widetilde{W}$ equals to the area of the whole wild set W, which is $N_1 \cdot N_2 = \frac{N}{4}$. When $n_1 \geq N_1/2$ or $n_2 \geq N_2/2$, then the distribution on $\widetilde{w}$ is not inside of the Tame set any more. In these cases, the overlap $|\widetilde{T} \cap \widetilde{W}|$ is varies between $\frac{N}{4}$ and $\frac{N}{8}$.

Theorem 6. *Sampling uniformly at random with replacement alternately from Tame set and Wild set. The expected number of selections that we need to make, over all instance, before a Tame-Wild collision happen in the 2-dimensional discrete logarithm problem is* $(1.4776 + o(1))\sqrt{N}$.

Here the small term $o(1)\sqrt{N}$ goes to 0 as N goes to ∞. But in the proof, we only mention how we get the result $1.4776\sqrt{N}$. And for the following results, we'll do the same in proofs,too.

Proof. Let $n_1 = x_1 N_1, n_2 = x_2 N_2$

i) When $0 \leq |x_1|, |x_2| < \frac{1}{2}$

Samples are selected uniformly at random in the fundamental domain of the Tame set $\widetilde{T}$ (even not in the fundamental domain of the wild set $\widetilde{W}$ sometimes), hence we can apply the theorem 2 to find the expectation of this case. We need find the A_1 in oreder to get the E_1. As the figure 8 illustrated, the overlap $|\widetilde{T} \cap \widetilde{W}|$

is partitioned into two parts: Y' region and Z region (Z region is the region $|\widetilde{T}\cap\widetilde{W}|-Y'$). In particular, the probability of the points in the $Y'+Y$ region is $4/N$ (Since the area of the Wild Set is $4/N$). Now we rotate the points in region Y 180^0 to the region Y', then the number of points in the region Y' is twice the original Y', which we called the 'double density' part of the fundamental domain of the wild set $\widetilde{W}$ in 2-Dimensional case. Hence, the probability of finding a point in $\widetilde{W}$ is $4/N$. Recall the probability of points in the $\widetilde{T}$ region is $2/N$, and the probabilities of the points being recorded in the list $\widetilde{T}$ and list $\widetilde{W}$ are both $1/2$. Hence, $q_1 = q_2 = \frac{1}{2}, q_{1,|\widetilde{T}\cap\widetilde{W}|} = 2/N, q_{2,Y'} = 8/N, q_{2,Z} = 4/N$. Suppose the area of region Y' is γ and the area of region Z is η, thus the ovelap in this case is $|\widetilde{T}\cap\widetilde{W}| = \eta + 2\gamma = \frac{N}{4}$. Hence

$$A_1 = 2\cdot\frac{1}{2}\cdot\frac{1}{2}\cdot(\frac{8}{N}\frac{2}{N}\cdot\gamma + \frac{4}{N}\frac{2}{N}\cdot\eta) \tag{35}$$

$$= 2\cdot\frac{1}{2}\cdot\frac{1}{2}\cdot(\frac{8}{N}\frac{2}{N}\cdot\gamma + \frac{4}{N}\frac{2}{N}\cdot(\frac{N}{4} - 2\gamma)) \tag{36}$$

$$= \frac{4}{N^2}\cdot\frac{N}{4} \tag{37}$$

$$= \frac{1}{N} \tag{38}$$

Then the expectation for this case is

$$E_1 = \sqrt{\frac{\pi}{2\cdot A_1}} + O(N^{\frac{1}{4}}) = \sqrt{\frac{\pi N}{2}} + O(N^{\frac{1}{4}})$$

ii) when $\frac{1}{2} \le |x_1| \le 1, 0 \le |x_2| < \frac{1}{2}$, in this case the fundamental domain of the wild set $\widetilde{W}$ moves to the 'right' along the x-axis. And the expectation at this time relates to the values of $|x_1|$. Since the group elements in the fundamental domains of Tame and Wild are both sampled uniformly at random, the theorem 2 applies. Thus $q_1 = q_2 = \frac{1}{2}, q_{1,|\widetilde{T}\cap\widetilde{W}|} = 2/N, q_{2,|\widetilde{T}\cap\widetilde{W}|} = 4/N$ and note that the little right-angle triangle region of the wild set is not the double density area in the wild's fundamental domain since this little triangle is rotated 180 degree by the diagonal $y = -\frac{N_2}{N_1}x$, hence the region of $|\widetilde{T}\cap\widetilde{W}|$ is still a rectangle, $|\widetilde{T}\cap\widetilde{W}| = \frac{N}{4}(\frac{3}{2} - |x_1|)$ in this case. Then,

$$A_2 = 2\cdot\frac{1}{2}\cdot\frac{1}{2}\cdot(\frac{4}{N}\frac{2}{N}\cdot|\widetilde{T}\cap\widetilde{W}|) \tag{39}$$

$$= 2\cdot\frac{1}{2}\cdot\frac{1}{2}\cdot(\frac{4}{N}\frac{2}{N}\cdot|\widetilde{T}\cap\widetilde{W}|) \tag{40}$$

$$= \frac{4}{N^2}\cdot|\widetilde{T}\cap\widetilde{W}| \tag{41}$$

$$= \frac{4}{N^2}\cdot(\frac{N}{4}(\frac{3}{2} - |x_1|)) \tag{42}$$

$$= \frac{1}{N}(\frac{3}{2} - |x_1|) \tag{43}$$

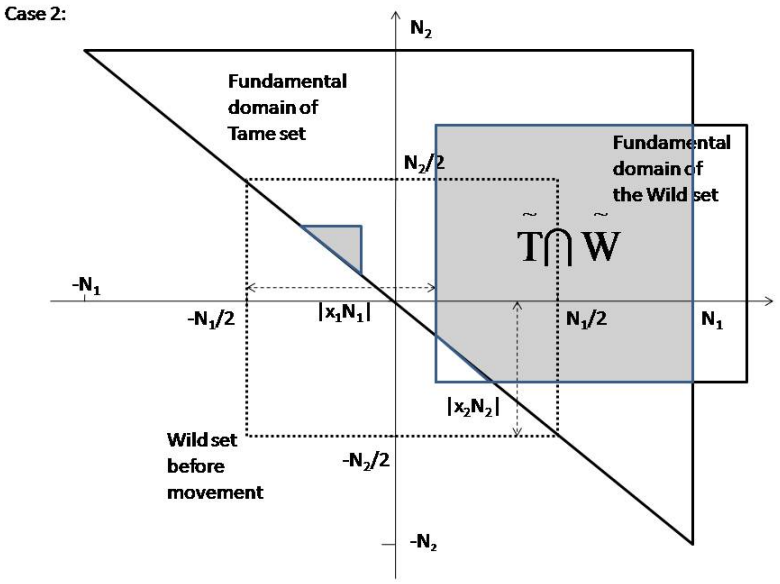

Figure 9: Case 2 of 2D in Rotation 180^o:when $\frac{1}{2} \leq |x_1| \leq 1, 0 \leq |x_2| < \frac{1}{2}$

Then the expectation for this case is

$$E_2 = \sqrt{\frac{\pi}{2 \cdot A_2}} + O(N^{\frac{1}{4}}) \qquad = \frac{\sqrt{2\pi N}}{2} \cdot (\frac{3}{2} - |x_1|)^{-\frac{1}{2}} + O(N^{\frac{1}{4}}) \tag{44}$$

iii) when $0 \leq |x_1| < \frac{1}{2}, \frac{1}{2} \leq |x_2| \leq 1$, this case is similar to the case ii,the only difference is the fundamental domain of the wild set $\widetilde{W}$ moves 'up' along the y-axis. Hence$|\widetilde{T} \cap \widetilde{W}| = \frac{N}{4}(\frac{3}{2} - |x_2|), A_N = \frac{1}{N}(\frac{3}{2} - |x_2|)$. Therefore

$$E_3 = \frac{\sqrt{2\pi N}}{2}(\frac{3}{2} - |x_2|)^{-\frac{1}{2}} + O(N^{\frac{1}{4}})$$

iv) when $\frac{1}{2} \leq |x_1| \leq 1, \frac{1}{2} \leq |x_2| \leq 1$. Now the fundamental domain of the wild set in this case moves not only along the x-axis to the right but also the y-axis to up. The overlap $|\widetilde{T} \cap \widetilde{W}| = \frac{N}{4}(\frac{3}{2} - |x_1|)(\frac{3}{2} - |x_2|), A_4 = \frac{1}{N}(\frac{3}{2} - |x_1|)(\frac{3}{2} - |x_2|)$, hence the expectation of this case is

$$E_4 = \frac{\sqrt{2\pi N}}{2}(\frac{3}{2} - |x_1|)^{-\frac{1}{2}}(\frac{3}{2} - |x_2|)^{-\frac{1}{2}} + O(N^{\frac{1}{4}})$$

Ignore all the small terms. The expected number of elements that we need to

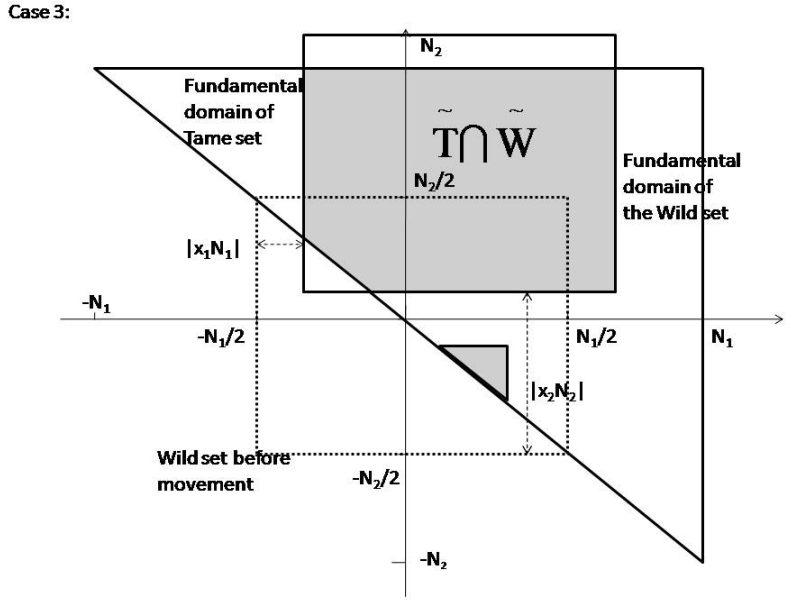

Figure 10: Case 3 of 2D in Rotation 180^o:when $0 \leq |x_1| < \frac{1}{2}, \frac{1}{2} \leq |x_2| \leq 1$

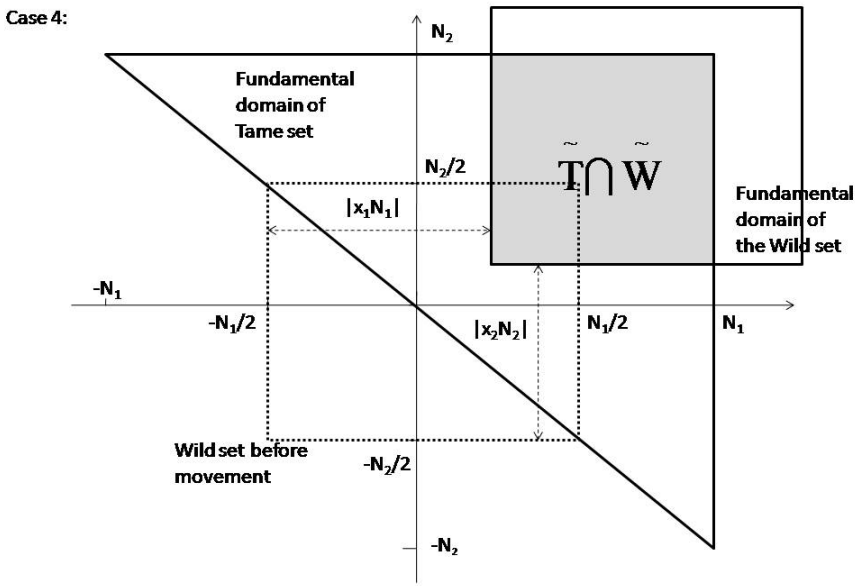

Figure 11: Case 4 of 2D in Rotation 180^o: when $\frac{1}{2} \leq |x_1| \leq 1, \frac{1}{2} \leq |x_2| \leq 1$

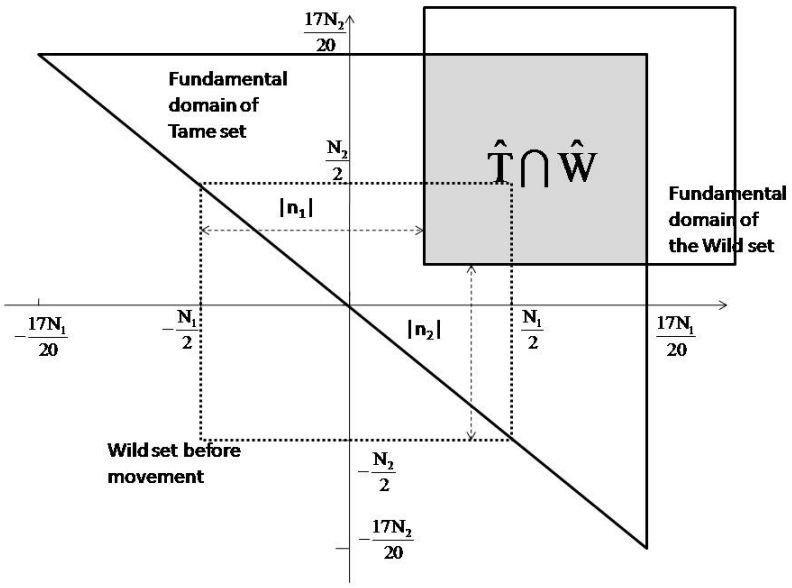

Figure 12: Improved Gaudry-Schost algorithm for 2-Dimensional DLP in Rotation 180^o

select over all instances is

$$E = \frac{1}{4} \cdot \sqrt{\frac{\pi N}{2}} + \frac{1}{2} \int_{\frac{1}{2}}^{1} \frac{\sqrt{2\pi N}}{2} \cdot (\frac{3}{2} - |x_1|)^{-\frac{1}{2}} d|x_1| \tag{45}$$

$$+ \frac{1}{2} \int_{\frac{1}{2}}^{1} \frac{\sqrt{2\pi N}}{2} \cdot (\frac{3}{2} - |x_2|)^{-\frac{1}{2}} d|x_2| \tag{46}$$

$$+ \int_{\frac{1}{2}}^{1} \int_{\frac{1}{2}}^{1} \frac{\sqrt{2\pi N}}{2} (\frac{3}{2} - |x_1|)^{-\frac{1}{2}} (\frac{3}{2} - |x_2|)^{-\frac{1}{2}} d|x_1| d|x_2| \tag{47}$$

$$= \frac{\sqrt{2\pi N}}{8} + (4\sqrt{2} - 5)\sqrt{\pi N} \tag{48}$$

$$\approx 1.4776\sqrt{N} \tag{49}$$

□

4.5 New Algorithm of 2-Dimensional in Rotation 180^0

Our rough calculation requirs the running time of theoretical result is at least $1.4776\sqrt{N}$, which we've given in the section 4.4.3. One can give even better algorithm to reduce the expected running time to around $1.4503\sqrt{N}$. The key observation is that the running time of the Gaudry-Schost algorithm depends on

the size of the overlap $|\widetilde{T} \cap \widetilde{W}|$. We achieve this better result by choosing walks which only cover certain subsets of the fundamental domain of the tame set $\widetilde{T}$ and the wild set $\widetilde{W}$. To avoid the symbol confusion, we'll use $\widehat{T}$ represents the new fundamental domain of Tame set, and $\widehat{W}$ represents the new fundamental domain of the Wild set. Let

$$\widehat{T} = \left\{(a,b) : -\frac{17}{20}N_1 \leq a \leq \frac{17}{20}N_1, -\frac{N_2}{N_1}a \leq b \leq \frac{17}{20}N_2\right\}$$

and

$$\widehat{W} = \left\{\{(n_1+u_1, n_2+u_2), (-n_1-u_1, -n_2-u_2)\} : -\frac{N_1}{2} \leq n_1 \leq \frac{N_1}{2}, -\frac{N_2}{2} \leq n_2 \leq \frac{N_2}{2}\right\}$$

The way of calculation is exactly the same as the calculation in the previous section. Divide the whole problem into four cases and observe the expectation over all the cases then get the final solution.

Theorem 7. *Given the 2-Dimensional Discrete Logarithm Problem as described in Definition 7. Let $\widehat{T}$ and $\widehat{W}$ be the fundamental domain of the Tame set and the Wild set. Then the expected running time of the group operations for the improved Gaudry-Schost algorithm is* $(1.4503 + o(1))\sqrt{N}$.

One can prove it still by using the theorem 2 by S.D.Galbraith and M.Holmes [2]. The rough calculation result is at least $1.4503\sqrt{N}$, we'll prove it without counting the small term $o(1)\sqrt{N}$.

Proof. Let $n_1 = x_1N_1, n_2 = x_2N_2$, and $N = 4N_1N_2, \kappa = \frac{17}{20}$. The ratio of walks being recorded as tame or wild type walk is $1:1$, then the probability of a point being recorded into the tame set or the wild set is $q_t = q_w = \frac{1}{2}$. The area of the fundermental domain of the Tame Set $\widehat{T} = \frac{1}{2} \cdot 4 \cdot \frac{17}{20}^2 \cdot N_1N_2 = \frac{1}{2}\kappa^2 N$, that also means the probabilities of a point being selected from the Tame set is $2/\kappa^2 N$. Clearly, the area of original Wild Set $|W| = \frac{N}{4}$. For the fundamental domain of the Wild Set $\widehat{W}$, we apply the theorem 4. The prove is similar to the prove of theorem 6. case(1) when $0 \leq x_1 < \kappa - \frac{1}{2}$ and $0 \leq x_2 < \kappa - \frac{1}{2}$, As we described in the prove of theorem 6, 'double density' only happens in this case. Play the same trick as above proof–since the 'double density' part is caused by rotation, then we can rotate the overlapped points back to its original place. Then the overlap $|\widetilde{T} \cap \widetilde{W}| = |W| = N/4$, thus

$$A_1 = 2 \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{2}{\kappa^2 N} \cdot \frac{4}{N} \cdot \frac{N}{4} = \frac{1}{N\kappa^2}$$

$\Rightarrow$

$$E_1 = \kappa\sqrt{\frac{\pi N}{2}} + O(N^{\frac{1}{4}})$$

case(2) when $\kappa - \frac{1}{2} \leq x_1 \leq 1$ and $0 \leq x_2 < \kappa - \frac{1}{2}$, then the overlap $|\widetilde{T} \cap \widetilde{W}| = (\kappa N_1 + \frac{1}{2}N_1 - x_1N_1)N_2 = \frac{N}{4}(\kappa + \frac{1}{2} - x_1)$, thus

$$A_1 = 2 \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{2}{\kappa^2 N} \cdot \frac{4}{N} \cdot \frac{N}{4}(\kappa + \frac{1}{2} - x_1) = \frac{1}{N\kappa^2}(\kappa + \frac{1}{2} - x_1)$$

$\Rightarrow$

$$E_2 = \kappa\sqrt{\frac{\pi N}{2}}(\kappa + \frac{1}{2} - x_1)^{\frac{-1}{2}} + O(N^{\frac{1}{4}})$$

case(3) when $0 \le x_1 < \kappa - \frac{1}{2}$ and $\kappa - \frac{1}{2} \le x_2 \le 1$, this case is similar to case (2).

$$E_3 = \kappa\sqrt{\frac{\pi N}{2}}(\kappa + \frac{1}{2} - x_2)^{\frac{-1}{2}} + O(N^{\frac{1}{4}})$$

case(4) when $\kappa - \frac{1}{2} \le x_1 \le 1$ and $\kappa - \frac{1}{2} \le x_2 \le 1$, then the overlap $|\widetilde{T} \cap \widetilde{W}| = (\kappa N_1 + \frac{1}{2}N_1 - x_1N_1)(\kappa N_2 + \frac{1}{2}N_1 - x_2N_2) = \frac{N}{4}(\kappa + \frac{1}{2} - x_1)(\kappa + \frac{1}{2} - x_2)$, thus

$$A_1 = 2 \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{2}{\kappa^2 N} \cdot \frac{4}{N} \cdot \frac{N}{4}(\kappa + \frac{1}{2} - x_1)(\kappa + \frac{1}{2} - x_2) = \frac{1}{N\kappa^2}(\kappa + \frac{1}{2} - x_1)(\kappa + \frac{1}{2} - x_2)$$

$\Rightarrow$

$$E_4 = \kappa\sqrt{\frac{\pi N}{2}}(\kappa + \frac{1}{2} - x_1)^{\frac{-1}{2}}(\kappa + \frac{1}{2} - x_2)^{\frac{-1}{2}} + O(N^{\frac{1}{4}})$$

Therefore, over all instances and ignore all the small terms, we get the Expectation in this improved Gaudry-Schost algorithm is

$$E = (\kappa - \frac{1}{2})^2\kappa\sqrt{\frac{\pi N}{2}} + 2(\kappa - \frac{1}{2})\kappa\sqrt{\frac{\pi N}{2}}\int_{\kappa-\frac{1}{2}}^{1}(\kappa + \frac{1}{2} - x_1)^{-\frac{1}{2}}dx_1 \tag{50}$$

$$+ \kappa\sqrt{\frac{\pi N}{2}}\int_{\kappa-\frac{1}{2}}^{1}\int_{\kappa-\frac{1}{2}}^{1}(\kappa + \frac{1}{2} - x_1)^{-\frac{1}{2}}(\kappa + \frac{1}{2} - x_1)^{-\frac{1}{2}}dx_1dx_2 \tag{51}$$

$$= \kappa\sqrt{\frac{\pi N}{2}}[\kappa - \frac{1}{2} + \int_{\kappa-\frac{1}{2}}^{1}(\kappa + \frac{1}{2} - x_1)^{-\frac{1}{2}}dx_1]^2 \tag{52}$$

$$= \kappa\sqrt{\frac{\pi N}{2}}[\kappa - \frac{1}{2} - 2(\kappa + \frac{1}{2} - x_1)^{\frac{1}{2}}|_{\kappa-\frac{1}{2}}^{1}]^2 \tag{53}$$

$$= \kappa\sqrt{\frac{\pi N}{2}}[\kappa - \frac{1}{2} - 2[(\kappa - \frac{1}{2})^{\frac{1}{2}} - 1]]^2 \tag{54}$$

$$= \kappa\sqrt{\frac{\pi N}{2}}[\kappa + \frac{3}{2} - 2(\kappa - \frac{1}{2})^{\frac{1}{2}}]^2 \tag{55}$$

Finally, one can reaches the solution $1.4503\sqrt{N}$ by subsitute $\kappa = \frac{17}{20}$ into this formula E. Therefore, the proof completes. Together with the small term, our final solution of the New Algorithm is $(1.4503 + o(1))\sqrt{N}$.

□

In general, we get this new solution of the New Algorithm (with Rotation 180^0) by making the Tame Set smaller and the Wild Set bigger, since we expect the overlap $|T \cap W|$ as big as possible (That is the way how we approach to the optimal result). Let

$$T = \{\{(a, b), (-a, -b)\} : -(1-\lambda)N_1 \le a_1 \le (1-\lambda)N_1, -(1-\lambda)N_2 \le b \le (1-\lambda)N_2\}$$

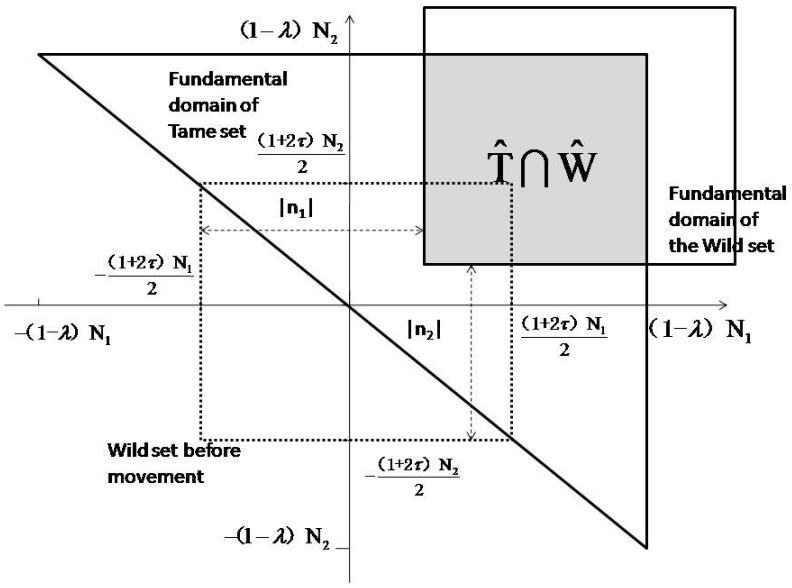

Figure 13: Optimal overlap $|\widehat{T} \cap \widehat{W}|$ of 2D in Rotation 180^o

be the set of equivalence classes of points in a box of area $N = 2(1-\lambda)N_1 \cdot 2(1-\lambda)N_2$ centred at 0. For the discrete log (n_1, n_2) where $-(1-\lambda)N_1 \leq n_1 \leq (1-\lambda)N_1, -(1-\lambda)N_2 \leq n_2 \leq (1-\lambda)N_2$, the Wild set is considered as $W = \{\{(n_1+u_1, n_2+u_2), (-n_1-u_1, -n_2-u_2)\} : -\frac{(1+2\tau)N_1}{2} \leq n_1 \leq \frac{(1+2\tau)N_1}{2}, -\frac{(1+2\tau)N_2}{2} \leq n_2 \leq \frac{(1+2\tau)N_2}{2}\}$Apply the algorithm on the equivalence classes and do the similar calculation with four cases. Finally we get a general formula of the expectation of selection is

$$E = (1-\lambda)\sqrt{\frac{\pi N}{2}}(\frac{5}{2} - \lambda + 3\tau - 2\sqrt{1+2\tau} \cdot \sqrt{\frac{1}{2} - \lambda + \tau})^2$$

Run the following computer programme, we get the optimal value of λ and τ are 0.1467 and 0, respectively. Take $\lambda = 0.1467 \approx 0.1500 = 17/20$, that is how our New Algorithm comes from –why we take $\widehat{T}$ be the set of equivalence classes of points in a box of area $(4(\frac{17}{20})^2 N_1 N_2)$.

```
Optimal parameters e and t

clear all

N1=10;
N2=5;
```

```
N=4*N1*N2;

n=(N-1)/2;
e=[0:1/N:n/N];
maxt=length([0:1/N:0.5-e(1)]);
for i=1:n
    t=[0:1/N:0.5-e(i)];
    for j=1:length(t)
        Y(i,j)=(1-e(i))*sqrt(pi/2)*(2.5-e(i)+3*t(j)-
                2*sqrt(1+2*t(j))*sqrt(0.5-e(i)+t(j)))^2;
    end
    if i>1
        for j=length(t)+1:maxt
            Y(i,j)=NaN;
        end
    end
end


[row col]=find(Y==min(min(Y)));
emin=1/N*(row-1);
tmin=1/N*(col-1);
```

Note that $\kappa = 1 - \lambda$ must be greater than $\frac{1}{2}$. In other words, our the value of λ should be in $[0, \frac{1}{2})$. As figure 14 illustrates, the expectation value goes to infinity when $\lambda = 1/2$. But the strange fact is when we subisitute $\lambda = 1/2$ and $\tau = 0$ into our optimal formula, we get

$$E = (1-\lambda) \cdot \sqrt{\pi/2} \cdot (2.5 - \lambda + 3 \times \tau - 2 \cdot \sqrt{1 + 2 \cdot \tau} \cdot \sqrt{0.5 - \lambda + \tau})^2 = \sqrt{2\pi N}$$

That is because the effect of the small term $O(N^{\frac{1}{4}})$.

5 Gaudry-Schost On The GLV Method

In the Gallant-Lambert-Vanstone (GLV) Method [23], one has an efficiently computable group homomorphism φ and one computes nP for $P \in E(F_q)$ and $n \in N$ as $Q = n_1 P + n_2 \varphi(P)$ where $|n_1|, |n_2| \leq N_1 = c\sqrt{n}$ for some constant. The homomorphism φ satisfies $\varphi^2 = \varphi \cdot \varphi = -1$. Now, we assume that $N_1 = N_2$. Write $N = (2N_1 + 1)(2N_2 + 1)$, since one knows the logarithm of $\varphi(P)$ to the base P it is sufficient to compute n_1 and n_2. Consider the equivalence classes

$$\{Q, -Q, \varphi(Q), -\varphi(Q)\}$$

of size 4. If $Q = n_1 P + n_2 \varphi(P)$ then $-Q = -n_1 P - n_2 \varphi(P)$,$\varphi(Q) = \varphi(n_1 P + n_2 \varphi(P)) = n_1 \varphi(P) + n_2 \varphi^2(P) = -n_2 P + n_1 \varphi(P)$,$-\varphi(Q) = -\varphi(n_1 P + n_2 \varphi(P)) =$

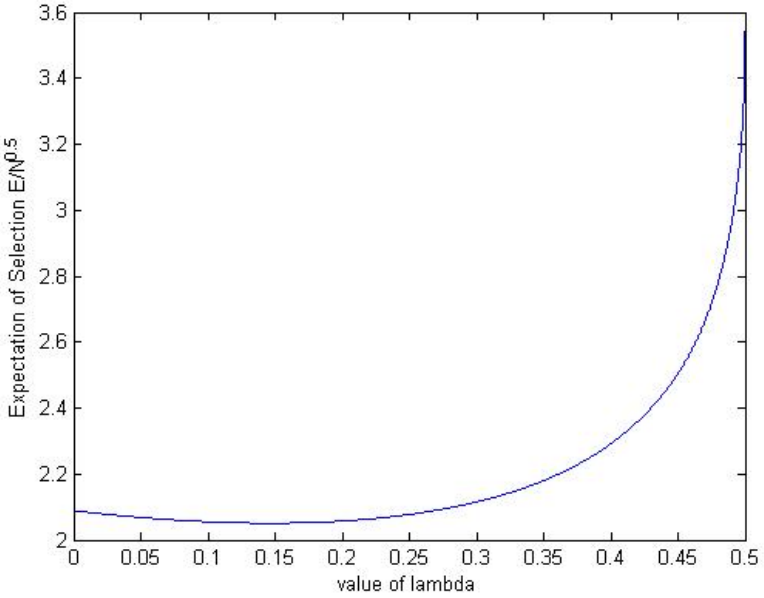

Figure 14: Values of λ: $0 \leq \lambda < \frac{1}{2}$

$-n_1\varphi(P) - n_2\varphi^2(P) = n_2P - n_1\varphi(P)$ these 4 points correspond to the pairs of exponents

$$\{(n_1, n_2), (-n_1, -n_2), (-n_2, n_1), (n_2, -n_1)\}$$

and so action by φ corresponds to rotation by 90 degrees. Hence, we naturally apply the Gaudry-Schost algorithm on these equivalence calsses. Take the Fundamental Domain of the Tame Set

$$\widetilde{T} = \{(a, b) : 0 \leq a \leq N_1, 0 \leq b \leq N_2\}$$

and the Fundamental Domain of the Wild Set $\widetilde{W}$ is a multi-set, see pictures 15, 16,17.

Theorem 8. *Sampling uniformly at random with replacement alternately from Tame set and Wild set. The expected number of selections that we need to make, over all instance, before a Tame-Wild collision happen in the 2-dimensional discrete logarithm problem with GLV Method is* $(1.044 + o(1))\sqrt{N}$.

We prove this theorem similar to the proof of theorem 6. We still ignore the small term $o(1)\sqrt{N}$ first. The ratio of a point being recorded as a Tame type element or a Wild type element is $1 : 1$, hence the probability of a point being recorded as the Tame type or the Wild type is $q_t = q_w = \frac{1}{2}$. Apply this problem on the GLV method. The area of the Fundamental Domain of the

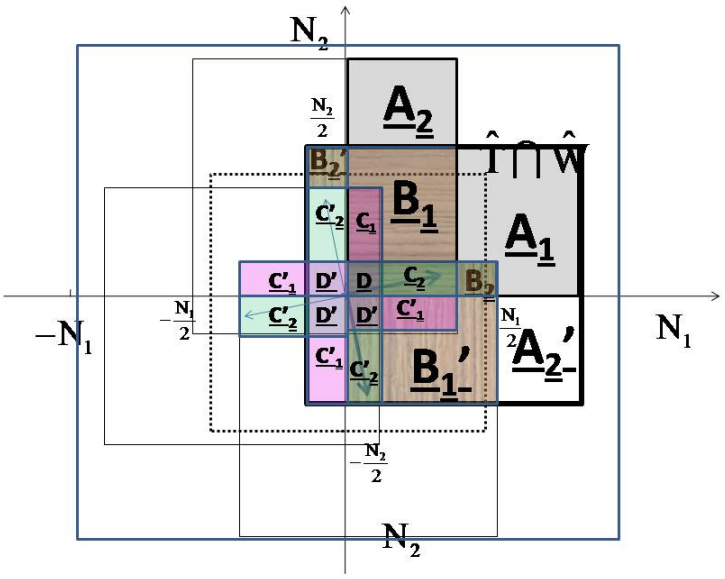

Figure 15: Case 1 of 2D on the GLV Method: $0 \leq ||x_1, |x_2| < \frac{1}{2}$

Tame Set is $|\widetilde{T}| = N_1 \times N_2 = \frac{N}{4}$, thus the probability of collecting a point from the Fundamental Domain of the $|\widetilde{T}|$ is $4/N$. After observe the movement of the centre of $\widetilde{W}$, we still analyse four different cases as the same as the proof in theorem 6 depending on the value of n_1, n_2, and the theorem 4 and Galbraith and Holmes's theorem 2 are still important tool for us. But the trick, this time, is not only 'double density', but also 'triple density' and 'quadruple density' for the Fundamental Domain of the Wild Set $|\widetilde{W}|$. We have to be careful in the proof.

Proof. Let $n_1 = x_1 N_1, n_2 = x_2 N_2$

case 1),When $0 \leq |x_1|, |x_2| < \frac{1}{2}$ Observe that beside 'single density', 'double density', some parts ,what we call 'triple density' and 'quadruple density' (defined the same as 'single density' and 'double density'), exsits. Divided the whole overlap $|\widetilde{T} \cap \widetilde{W}|$ in to four type regions: 'single density' region $\underline{A}$ ($\underline{A}$ is made up by $\underline{A_1}$ and $\underline{A_2}$), 'double density' region $\underline{B}$ ($\underline{B}$ is made up by $\underline{B_1}$ and$\underline{B_2}$), 'triple density' region $\underline{C}$ ($\underline{C}$ is made up by $\underline{C_1}$ and $\underline{C_2}$), 'quadruple density' region $\underline{D}$. Then the probabilities of selecting a point from $\underline{A}$,$\underline{B}$,$\underline{C}$,$\underline{D}$ are $4/N$,$8/N$,$12/N$,$16/N$. We get this figure 15 by the GLV Method, hence we know the areas $\underline{A} = \underline{A'}$,$\underline{B} = \underline{B'}$,$\underline{C} = \underline{C'}$,$\underline{D} = \underline{D'}$, respectively. Looking at the box with solid border in Figure 15, one can see that $\frac{N}{4} = A + 2B + 3C + 4D$.

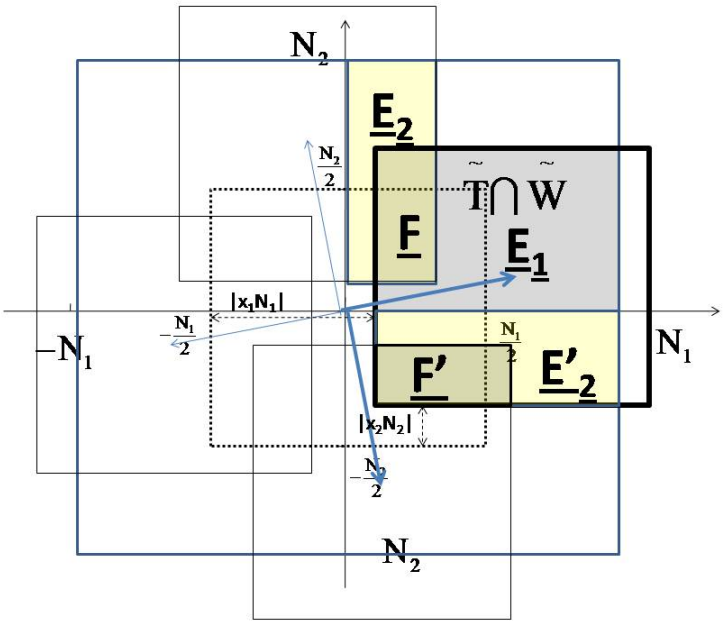

Figure 16: Case 2 of 2D on GLV Method :when $\frac{1}{2} \leq |x_1| \leq 1, 0 \leq |x_2| < \frac{1}{2}$ & Case 3 of 2D on GLV Method :when $0 \leq |x_1| < \frac{1}{2}, \frac{1}{2} \leq |x_2| \leq 1$

Apply the theorem 2,

$$A_1 = 2 \times \frac{1}{2} \times \frac{1}{2} \times \frac{4}{N}[\frac{16}{N} \times \underline{D} + \frac{12}{N} \times \underline{C} + \frac{8}{N} \times \underline{B} + \frac{4}{N} \times \underline{A}] \tag{56}$$

$$= 2 \times \frac{1}{2} \times \frac{1}{2} \times \frac{4}{N} \times \frac{4}{N}[4\underline{D} + 3\underline{C} + 2\underline{B} + \underline{A}] \tag{57}$$

$$= \frac{8}{N^2}[4\underline{D} + 3\underline{C} + 2\underline{B} + \frac{N}{4} - 4\underline{D} - 3\underline{C} - 2\underline{B}] \tag{58}$$

$$= \frac{8}{N^2} \times \frac{N}{4} \tag{59}$$

$$= \frac{2}{N}. \tag{60}$$

Hence,

$$E_1 = \sqrt{\frac{\pi N}{4}} + O(N^{\frac{1}{4}}) = \frac{\sqrt{\pi N}}{2} + O(N^{\frac{1}{4}}).$$

case 2) When $\frac{1}{2} \leq |x_1| \leq 1, 0 \leq |x_2| < \frac{1}{2}$

This case is easier than the case 1). There are only 'Single Density' region $\underline{E}$ ($\underline{E}$ is made up by $\underline{E_1}$ and $\underline{E_2}$) and 'Double Density' region $\underline{F}$ in the overlap $|\widetilde{T} \cap \widetilde{W}|$. And the probabilities of collecting points from the 'Single Density' region and the 'Double Density' region are $4/N$ and $8/N$, respectively. The

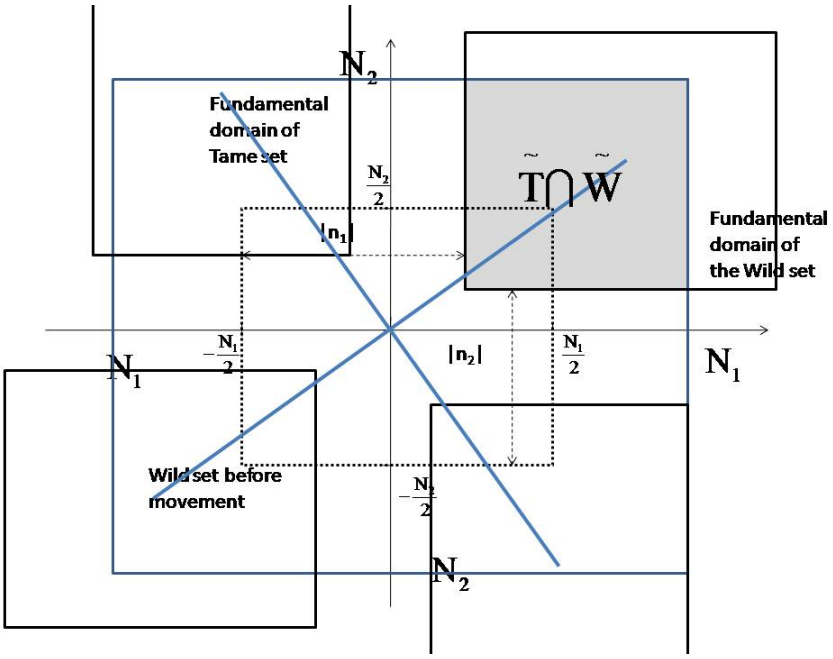

Figure 17: Case 4 of 2D on GLV Method: when $\frac{1}{2} \leq |x_1| \leq 1, \frac{1}{2} \leq |x_2| \leq 1$

same as case 1), the areas of region $\underline{E_2} = \underline{E_2'}$, $\underline{F} = \underline{F'}$ by rotation 90^o.

$$A_2 = 2 \times \frac{1}{2} \times \frac{1}{2} \times \frac{4}{N} \times [\frac{8}{N} \cdot \underline{F} + \frac{4}{N} \cdot \underline{E}] \tag{61}$$

$$= 2 \times \frac{1}{2} \times \frac{1}{2} \times \frac{4}{N} \times [\frac{8}{N} \cdot \underline{F} + \frac{4}{N} \times (\frac{N}{4}(\frac{3}{2} - x_1))] \tag{62}$$

$$= \frac{2}{N}(\frac{3}{2} - x_1) \tag{63}$$

Hence, the expectation

$$E_2 = \sqrt{\frac{\pi}{2 \cdot (\frac{2}{N}(\frac{3}{2} - x_1))}} + O(N^{\frac{1}{4}}) = \frac{\sqrt{\pi N}}{2}(\frac{3}{2} - x_1)^{-\frac{1}{2}} + O(N^{\frac{1}{4}}).$$

case 3) When $0 \leq |x_1| < \frac{1}{2}, \frac{1}{2} \leq |x_2| \leq 1$ Similarly proof as case 2), we get the expectation

$$E_3 = \frac{\sqrt{\pi N}}{2}(\frac{3}{2} - x_2)^{-\frac{1}{2}} + O(N^{\frac{1}{4}}).$$

case 4) When $\frac{1}{2} \leq |x_1| \leq 1, \frac{1}{2} < |x_2| \leq 1$

There is only 'Single Density' in the overlap $|\widetilde{T} \cap \widetilde{W}|$, and the area of the

overlap $|\widetilde{T} \cap \widetilde{W}|$ is $\frac{N}{4}(\frac{3}{2} - x_1)(\frac{3}{2} - x_2)$. Thus

$$A_4 = 2 \times \frac{1}{2} \times \frac{1}{2} \times \frac{4}{N} \times \frac{4}{N} \times \frac{N}{4}(\frac{3}{2} - x_1)(\frac{3}{2} - x_2) \tag{64}$$

$$= \frac{2}{N}(\frac{3}{2} - x_1)(\frac{3}{2} - x_2) \tag{65}$$

Then, the expectation

$$E_4 = \frac{\sqrt{\pi N}}{2}(\frac{3}{2} - x_1)^{-\frac{1}{2}}(\frac{3}{2} - x_2)^{-\frac{1}{2}} + O(N^{\frac{1}{4}})$$

Therefore, ignore the small terms, over all instances, we get

$$E = \frac{\sqrt{\pi N}}{8} + 2 \times \frac{1}{2} \times \frac{\sqrt{\pi N}}{2} \int_{\frac{1}{2}}^{1} (\frac{3}{2} - x_1)^{-\frac{1}{2}} dx_1 + \frac{\sqrt{\pi N}}{2}(\int_{\frac{1}{2}}^{1} (\frac{3}{2} - x_1)^{-\frac{1}{2}} dx_1)^2 \tag{66}$$

$$= \frac{\sqrt{\pi N}}{2}(\frac{1}{2} + \int_{\frac{1}{2}}^{1} (\frac{3}{2} - x_1)^{-\frac{1}{2}} dx_1)^2 \tag{67}$$

$$= \frac{\sqrt{\pi N}}{2}(\frac{1}{2} - 2(\frac{3}{2} - x_1)^{\frac{1}{2}}|_{\frac{1}{2}}^{1})^2 \tag{68}$$

$$= \frac{\sqrt{\pi N}}{2}[\frac{1}{2} - 2(\frac{\sqrt{2}}{2} - 1)]^2 \tag{69}$$

$$= \frac{\sqrt{\pi N}}{2}[\frac{5}{2} - \sqrt{2}]^2 \tag{70}$$

$$\approx 1.044\sqrt{N} \tag{71}$$

Together with the small constant term $o(1)\sqrt{N}$. The expected of sellection is $(1.044 + o(1))\sqrt{N}$. □

5.1 New Algorithm for the GLV Method

We still play a similar game as the subsection 4.5. Let the Fundamental Domain of the Tame Set

$$\widetilde{T} = \{(a, b) : 0 \leq a \leq (1 - \lambda)N_1, 0 \leq b \leq (1 - \lambda)N_2\}$$

and although the Fundamental Domain of the Wild Set $\widetilde{W}$ is differ from each case, we can always do some rotation therefore consider the Wild Set itself. The optimal formula for the GLV Method is

$$E = \frac{(1 - \lambda)\sqrt{\pi N}}{2}[\frac{5}{2} - \lambda + 3\tau - 2\sqrt{1 + 2\tau}(\frac{1}{2} - \lambda + \tau)^{\frac{1}{2}}]^2$$

Run a similar computer programme in subsection 4.5, thus $\lambda = 0.1467$ and $\tau = 0$. Now. we give the optimal solution for the GLV Method.

Theorem 9. *Sampling uniformly at random with replacement alternately from Tame set and Wild set. The expected number of selections that we need to make, over all instance, before a Tame-Wild collision happen in the 2-dimensional discrete logarithm problem on the GLV Method is* $(1.0255 + o(1))\sqrt{N}$.

The proof of this theorem is similar to the proof of theorem 4.5.

6 Conclusion

We give the Optimal Solution for solving the 2-Dimensional Gaudry-Schost Algorithm on the Equivalence Classes – Rotation $\frac{360^o}{2^d}$ (where d is a positive integer). Define the Tame Set in a region with area $\frac{(17/20)^2 N}{2^d}$, and the Wild Set is a box of area $\frac{N}{4}$ centered at origion.

Theorem 10. *Sampling uniformly at random with replacement alternately from Tame set and Wild set. The expected number of selections that we need to make, over all instance, before a Tame-Wild collision happen in the 2-Dimensional Discrete Logarithm Problem on the Equivalence Classes with Rotation* $\frac{360^o}{2^d}$ *is* $(2.0510 \cdot 2^{-\frac{d}{2}} + o(1))\sqrt{N}$, *where d is a positive integer.*

The proof of this theorem is exactly the similar as the theorem 4.5. There are still four cases to be observed. By using the theorem 2 for over all instances (ignore the small terms), we get the expectation is

$$E = \frac{17}{20}\sqrt{\pi N}(2)^{-\frac{d}{2}}[\frac{17}{20} + \frac{3}{2} - 2(\frac{17}{20} - \frac{1}{2})^{\frac{1}{2}}]^2 \tag{72}$$

$$= 0.85 \times \sqrt{\pi N}(2)^{-\frac{d}{2}}[0.85 + 1.5 - 2 \times \sqrt{0.35}]^2 \tag{73}$$

$$= 0.85 \times \sqrt{\pi N}(2)^{-\frac{d}{2}} \times 1.157209 \tag{74}$$

$$= 2.0510 \times 2^{-\frac{d}{2}}\sqrt{N} \tag{75}$$

References

[1] "Lady Luck" By Warren Weaver pp. 132-134

[2] 'A non-uniform birthday problem with applications to discrete logarithms', By Steven D. Galbraith, Mark Holmes *Preprint 2010*

[3] 'On the use of the negation map in the Pollard Rho method', By Joppe W. Bos, Thorsten Kleinjung, Arjen K. Lenstra *In Algorithmic Number Theory (ANTS) 2010, volume 6197 of LNCS, pp. 67-83.*

[4] 'Faster Attacks on Elliptic Curves Cryptosystems', By M.J.Wiener, R.J.Zuccerato *Selected Areas in Cryptography, SAC 98 (LNCS 1556), Springer, 1998, pp. 190-200.*

[5] *'Improving the Parallelized Pollard Lambda Search on Binary Anomalous Curves',* By Robert.P.Gallant, Robert.J.Lambert and Scott.A.Vanstone *Mathematics of Computation* ***69****, 2000 , pp.1699-1705*

[6] *'Probability to meet in the middle',* By K.Nishiramu, M.Sibuya. *Journal of Cryptography* ***2****, 1990, pp.13-22*

[7] *'Using Equivalence Classes to Accelerate Solving the Discrete Logarithm Problem in a Short Interval',* By Steven.D.Galbraith, Ramindar.S.Ruprai *In M. Parker (ed.), Twelfth IMA International Conference on Cryptography and Coding, Cirencester, Springer LNCS 5921, 2009, PP. 368-382*

[8] *'On waiting time in the scheme of random allocation of coloured particles',* By B.I.Selivanov *Discrete Math. Appl.* ***5****(1), 1995, pp. 73-82*

[9] *'The Maximum of a random Walk and its Application to Rectangle Packing',* By E.G.Cheon,P.Flajolet,L.Flatto,M.Hofri *Technical report, INRIA, 1997*

[10] *'An improved baby step gain step algorithm for point counting of hyperelliptic curves over finite fields',* By Matsuo K.Chao, J.Tsujii S *ANTS 2002. LNCS, vol.2369, Springer, Heidelberg, 2002, pp. 461-474.*

[11] *'A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm',* By Gaudry P., Schost E. *ANTS 2004. LNCS, vol.3076, Springer, Heidelberg, 2004, pp. 208-222.*

[12] *'A low-memory algorithm for point conting on picard curves',* By A.Weng. *Designs, Codes and Cryptography 38(3), 2006, pp. 383-393.*

[13] *'An efficient off-line electronic cash system based on the representation problems',*By Brands S. *CWI Technical Report CS-R9323(1993)*

[14] *'A secure and optimally efficient multi-authority election scheme',*By Cramer R., Gennaro R., Schoenmakers B. *Fumy, W.(ed.) EUROCRYPT 1997. LNCS, vol.1233, Springer, Heidelberg, 1997, pp. 103-118.*

[15] *1Exponentiation in pairing-friendly groups using homomorphisms',* By S.D.Galbraith, M.Scott. *Pairing 2008. LNCS, vol.5209, Springer, Heidelberg, 2008, pp. 211-224.*

[16] *'Endomorphisms for faster elliptic cure cryptography on a large class of curves',*By S.D.Galbraith, X.Lin and M.Scott. *EUROCRYPT 2009. LNCS, vol.5479, Springer, Heidelberg, 2009, pp. 518-535.*

[17] *'CM-curves with good cryptographic properties',*By N.Koblitz. *CRYPTO 1991. LNCS vol. 576, Springer,Heidelberg, 1992, pp. 279-287.*

[18] *'Class number, a theory of factorization, and genera',* By D. Shanks. *In Proc. Symp. Pure Math. 20, AMS, Providence, R.I., 1971, pp. 415–440.*

[19] 'New Directions in Cryptography', By W.Diffie, M.Hellman. *IEEE Transactions on information Theory, 22(6) November 1976, pp.644-654.*

[20] 'Secure communications over insecure channels', By R.C.Merkle. *Communications of the ACM, Volume 21 Issue 4, April 1978,pp.294-299,*

[21] 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystems', By R.Rivest, A.Shamir, L.Adleman. *Communications of the ACM 21 (2), pp. 120-126*

[22] 'Hiding information and signatures in trapdoor knapsacks', By R.Merkle, M.Hellman. *Information Theory, IEEE Transactions on, vol.24, no.5, Sep 1978, pp.525-530.*

[23] 'Counting Points on Hyperelliptic Curves over Finite Fields', By P.Gaudry, R.Harley. *In W.Bosma,ed.:Proceeedings of Alforithm Number Theory Symposium - ANTS IV.LNCS, vol.1838, Spring-Verlag, 2000, pp.313-332.*

[24] 'Al-Khwarizmi: the inventor of algebra', By Corona Brezina pp.30-49