UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques
i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Group distortion in Cryptography

Autor: Nicolas Werner

Director: Dr. Carlos D'Andrea

Realitzat a: Departament de
Matemàtiques i Informàtica

Barcelona, 19 de juny de 2021

Contents

Foreword

Acknowledgements

I would like to express my gratitude to my advisor, Carlos D'Andrea, for guiding me throughout the past few months and solving my doubts. Sharing with him the exploration of this field of mathematics has been a great pleasure for me. And I would also like to thank my close family, as they make possible for me to live in this city and pursue my studies.

Abstract

In this work, we present a symmetric-key cryptographic protocol based on exponential distortion in arithmetic groups. As an example, we also provide a functional platform for the protocol.

2020 Mathematics Subject Classification: 11F06, 11T71

Introduction

Non-commutative group-based cryptography has been a very active field of research for the past decade. Different protocols based on algorithmic problems, such as the Word Choice problem, the Conjugacy Search problem or the Membership problem, have been proposed. One of these proposals has come, quite recently, from Delaram Kahrobaei and Keivan Mallahi-Karai. In *Some applications of arithmetic groups in cryptography* they present a cryptographic protocol based on the solvability of the Geodesic Length problem and exponential subgroup distortion in arithmetic groups. The goal of the present work is to provide a detailed explanation of some of their ideas.

To fully understand the proposal of Kahrobaei and Mallahi-Karai, we have had to answer some collateral questions: What are arithmetic groups? How do we put metrics on a group? What is exponential distortion? What are the properties of the Zariski topology? Furthermore, concepts from all my previous Algebra and Analysis courses have come into play: eigenvectors, group action, cosets, graphs, metrics, series convergence...

As to the structure of this work, it starts with the presentation of the protocol. We first give a basic version of it, and then a more secure one. After this, in Chapter 2, we provide some fundamental tools: we present arithmetic groups, we put a metric on groups by means of the Cayley Graph and we define exponential distortion. Then, with all this in hand, we are able to state what properties must the groups and subgroups involved have in order to make the protocol effective. We dedicate Chapter 3 to a particular pair group-subgroup. We prove it satisfies all the required properties to be a platform for the protocol. Finally, in Chapter 4, we study the security of the protocol against a known-plaintext attack.

Chapter 1

The protocol

In this chapter we present the cryptographic protocol. The goal is to send secretely a positive integer through a public channel. As always, Alice will send the message, Bob will receive it and Eve will be the eavesdropper. We will first provide a simple version of the protocol, and then a more secure version of it. Then, in the next chapter, we will give the properties that the groups and subgroups involved must have in order to make the protocol effective.

In order to present the protocol, we need to assume that there is a well defined length function over any group. We will provide this definiton in the following chapter, by means of the so called Cayley Graph. For now, for any element in a group, its length will be the minimum number of elements we need from a fixed generating set to express it. We will see that the length of an element strongly depends on the group/subgroup we choose to define it, as well as on the fixed generating set. For G a group and $g \in G$, we note the length of g as $l_G(g)$.

1.1 Basic scheme

Set a finitely generated group G with a fixed set of generators $\{g_1, \dots, g_s\}$ as the public channel. That is, $g_1, \dots, g_s$ are visible to Alice, Bob and Eve. And let Alice and Bob secretely share a finitely generated subgroup H in terms of another fixed set of generators $\{h_1, \dots, h_r\}$. We will keep this notation throughout this chapter. The generators of H are the private key of this protocol, which is as follows:

I. Alice wants to send secretely a positive integer n to Bob. To do so, she picks an element $h \in H$ with $l_H(h) = n$. Then she writes h in terms of m elements in $\{g_1, \dots, g_s\}$, and

sends h to Bob. Under some conditions we will have $m \ll n$.

II. Bob rewrites h in terms of $h_1, \ldots, h_r$ with a minimal expression and finds n.

Remarks.

- H is not known to anyone except Alice and Bob and the fact that $m \ll n$ hides very well the information: many possible lengths in H lead to very few possible lengths in G. Thus, when the eavesdropper Eve intercepts an element of G, she gets an element that, to her eyes, could mean many possible integers. However, Eve might intercept enough elements in H to generate it. At this point Eve would only have to deal with the non-uniqueness of the generating set of H.
- If G and H are sets of matrices with integer entries, Alice can send h as a single matrix through the public channel and let Eve compute its length in G, because Bob is only interested in the length of h in H. The same holds for any group G whose elements can be easily represented as single factors.

1.2 Secure version

Again, we set $G =< g_1, \ldots, g_s >$ as the public channel, and $H =< h_1, \ldots, h_r >$ as the private key that Alice and Bob secretly share. Now Alice will not only send the word she is interested in, she will also send some random words in $G \backslash H$ in order to make H less visible:

I. Alice picks an element $h \in H$ with $l_H(h) = n$. Then she writes h in terms of m elements in $\{g_1, \ldots, g_s\}$ and she randomly generates some $a_1, \ldots, a_t \in G \backslash H$. Then she sends Bob all these elements together.

II. Bob seeks the element in $\{a_1, \ldots, a_t, h\}$ that belongs to H and gets h. Then he rewrites h in terms of $h_1, \ldots, h_r$ with a minimal expression and finds n.

The reader might have noticed that in the protocol we present there are computational problems involved: it could be hard to find an element in H that has the desired length and, conversely, it could also be hard to find a minimal expression for $h \in H$ in terms of the generator set of H. Furthermore, Bob needs to be able to distinguish the element that belongs to H from the others that are sent. We will not work on these computational aspects in general. However, we will provide a particular operational platform for the protocol (see Chapter 3).

Chapter 2

Fundamentals

2.1 Arithmetic groups.

Throughout this work, we will turn to the so called arithmetic groups since they provide a good platform for the protocol. Roughly speaking, to build an arithmetic group, we consider a linear algebraic group defined over $\mathbb{Q}$ and we take those elements with integer entries. In the following, we provide a more precise construction, as well as some properties and examples.

Unless otherwise stated, V will denote an n-dimensional vector space over $\mathbb{C}$ endowed with a $\mathbb{Q}$-structure, ie, V contains an n-dimensional vector space defined over $\mathbb{Q}$. We call it $V_{\mathbb{Q}}$. Roughly speaking, given a vector space V over $\mathbb{C}$, $V_{\mathbb{Q}}$ are all linear combinations with rational coeficients of some basis in it. For our purposes, we will normally set $V = \mathbb{C}^n$ and $V_{\mathbb{Q}} = \mathbb{Q}^n$.

Now let A be a subring of $\mathbb{C}$. $\mathrm{GL}_n(A)$ will denote the group of matrices with determinant equal to a unit in A. $\mathrm{SL}_n(A)$ will denote the special linear group, that is, the subgroup of elements in $\mathrm{GL}_n(A)$ with determinant equal to 1.

For A a subring of $\mathbb{C}$ and G a subgroup of $\mathrm{GL}_n(\mathbb{C})$, we will refer to $G \cap \mathrm{GL}_n(A)$ as G_A. Notice that these are the matrices in G with all entries in A.

Definition 1. *Let G be a subgroup of $GL_n(\mathbb{C})$, and K a subfield of $\mathbb{C}$. We will say that G is algebraic over K if there is a finite set of polynomial equations over K in the matrix coefficients that define G. We also say that G is a K-subgroup of $GL_n(\mathbb{C})$.*

Example 1. $\mathrm{SL}_n(\mathbb{C})$ is algebraic, since it is defined in $\mathrm{GL}_n(\mathbb{C})$ by the polinomial equation $det(M) = 1$. The orthogonal group of matrices $O_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) : MM^T = M^TM = Id\}$

is also algebraic.

Definition 2. *We call lattice to any additive group isomorphic to $\mathbb{Z}^n$, $n \in \mathbb{N}$.*

Any lattice in $\mathbb{C}^n$ can be constructed as all linear combinations with integer coefficients of a finite subset of $\mathbb{C}^n$. In our case, we will be picking lattices in $\mathbb{Q}^n \subseteq \mathbb{C}^n$.

Definition 3. *Let L be a lattice in $V_{\mathbb{Q}}$ and G an algebraic subgroup of $GL_n(\mathbb{C})$ over $\mathbb{Q} \subseteq \mathbb{C}$. We define the group of L-units of G as $G_{Lu} = \{g \in G : g(L) = L\}$.*

One can think of the L-units we have just described as the elements that both satisfy the polynomial equations of the subgroup G and let the lattice L invariant. Notice that the condition $g(L) = L$ defines a subgroup, that is, L-units form a subgroup of G.

Definition 4. *Two subgroups A and B of a group Γ, are said to be commensurable if $A \cap B$ has finite index both in A and B.*

Example 2.

- $2\mathbb{Z}$ and $3\mathbb{Z}$ are commensurable because their intersection is $6\mathbb{Z}$, which has index 3 in $2\mathbb{Z}$ and has index 2 in $3\mathbb{Z}$.
- $\mathrm{GL}_n(\mathbb{C})$ and $\mathrm{SL}_n(\mathbb{C})$ are commensurable because their intersection is $\mathrm{SL}_n(\mathbb{C})$, with index 2 in $\mathrm{GL}_n(\mathbb{C})$ and index 1 in itself. Recall that there are only two equivalence classes in this case, that are defined by the sign of the determinant.

Lemma 1. *For G a group, the intersection of two finite index subgroups has finite index. More precisely, the quotient over the intersection of two finite index subgroups, H and K, is formed by all possible intersections between left cosets in G/H and left cosets in G/K.*

Proof. Given H and K, they both lead to a finite set of left-cosets:

$$G/H = \{\bar{h}_1, \dots \bar{h}_n\}; \quad G/K = \{\bar{k}_1, \dots, \bar{k}_m\} \quad \text{where } h_1, \dots, h_n \in H \text{ and } k_1, \dots, k_m \in K.$$

For $x \in G$ and $\bar{y} \in G/H \cap K$ we have that $y \in \bar{h}_i$ and $y \in \bar{k}_j$ for some $i \in \{1, \dots, n\}, j \in \{1, \dots, m\}$. And $x \in \bar{y} \Leftrightarrow yx^{-1} \in H \cap K \Leftrightarrow yx^{-1} \in H$ and $yx^{-1} \in K \Leftrightarrow x \in \bar{h}_i$ and $x \in \bar{k}_j$.

This proves that the left-cosets in $G/H \cap K$ are all possible intersections of left-cosets in G/H and G/K. Therefore, $G/H \cap K$ is indeed finite. □

Lemma 2. *Let H_1, H_2 be two subgroups of G such that $H_1 \subseteq H_2$. If H_1 has finite index, so has H_2.*

Proof. For convenience of the proof, for $g \in G$, we will denote its left coset in ${}^{G}/_{H_1}$ and ${}^{G}/_{H_2}$ as gH_1 and gH_2, respectively. We consider the following map:

$$f : {}^{G}/_{H_1} \longrightarrow {}^{G}/_{H_2}$$
$$gH_1 \longmapsto f(gH_1) = gH_2$$

Firstly, we see it is well defined. For $g, s \in G$, assume that $gH_1 = sH_1$, that is, $g^{-1}s \in H_1$. We want to prove that $gH_2 = sH_2$. This holds if, and only if, $g^{-1}s \in H_2$, which is true because $g^{-1}s \in H_1 \subseteq H_2$. Hence, it is indeed well defined. Furthermore, any $gH_2 \in {}^{G}/_{H_2}$ has preimage gH_1, thus, f is surjective. Therefore, as ${}^{G}/_{H_1}$ is finite, so is ${}^{G}/_{H_2}$. □

Proposition 1. *Commensurability is an equivalence relation.*

Proof. The relation is clearly reflexive and symmetric. We prove it is transitive. Assume A commensurable to B and B commensurable to C. We know from Lemma 1 the intersection of two finite index subgroups has finite index, hence,

$$\text{as we know that } \begin{cases} [B : A \cap B] \text{ is finite} \\ [B : B \cap C] \text{ is finite} \end{cases} \Rightarrow [B : A \cap B \cap C] \text{ is finite}$$

$$\Rightarrow \text{ From Lemma 2, we get } \begin{cases} [A \cap B : A \cap B \cap C] \text{ is finite (I)} \\ [B \cap C : A \cap B \cap C] \text{ is finite (II)} \end{cases}$$

And we know that $[A : A \cap B]$ is finite, hence, from (I) we see that $[A : A \cap B][A \cap B : A \cap B \cap C] = [A : A \cap B \cap C]$ is finite. Thus, from Lemma 2, $[A : A \cap C]$ is finite.

We also know that $[C : B \cap C]$ is finite, hence, from (II) we see that $[C : B \cap C][B \cap C : A \cap B \cap C] = [C : A \cap B \cap C]$ is finite. Finally, again from Lemma 2, $[C : A \cap C]$ is finite. □

Definition 5. *Let G be a $\mathbb{Q}$-subgroup of $GL_n(\mathbb{C})$. Now consider $G_{\mathbb{Q}} = G \cap GL_n(\mathbb{Q})$. A subgroup H of $G_{\mathbb{Q}}$ is said to be arithmetic if there exists a lattice L in $V_{\mathbb{Q}}$ such that H is commensurable to G_{Lu}.*

In other words, an arithmetic group can be built as follows:

- Pick a $\mathbb{Q}$-subgroup of $\mathrm{GL}_n(\mathbb{C})$, call it G. One can think of G as the "universe" where we will be working.
- Now consider only those elements in G with rational entries, $G_{\mathbb{Q}}$.
- Pick a subgroup H in $G_{\mathbb{Q}}$.
- Pick a lattice in $V_{\mathbb{Q}}$ whose L-units in G form a subgroup commensurable to H. Roughly speaking, for H to be arithmetic, it needs to have many of the elements that let a certain lattice invariant.

Remark. As commensurability is an equivalence relation, any subgroup B of an arithmetic group A who has finite index in it, is arithmetic as well.

Example 3. Let's see that $\mathrm{GL}_n(\mathbb{Z})$ is an arithmetic group.

We first notice that all matrices have determinant equal to a unit in $\mathbb{Z}$, ie, ± 1. Hence, all inverses will still be in $\mathrm{GL}_n(\mathbb{Z})$. One can now easily see that $\mathrm{GL}_n(\mathbb{Z})$ is indeed a group (a subgroup of $\mathrm{GL}_n(\mathbb{C})$). Moreover, since $\mathrm{GL}_n(\mathbb{C})$ is trivially algebraic[1], it is also a subgroup of an algebraic group. And we notice that $\mathrm{GL}_n(\mathbb{Z})$ has rational entries. So we have $\mathrm{GL}_n(\mathbb{Z}) \subseteq \mathrm{GL}_n(\mathbb{C})_{\mathbb{Q}}$, as desired.

Now consider the lattice $L = \mathbb{Z}^n \subseteq \mathbb{Q}^n$. It is clearly invariant under any matrix in $\mathrm{GL}_n(\mathbb{Z})$. That is, $\mathrm{GL}_n(\mathbb{Z}) \subseteq G_{Lu}$. Furthermore, if a certain matrix in G_{Lu} had a non-integer entry at row i, column j, then the image of the column vector $(0, \ldots, 0, 1_j, 0, \ldots, 0)^T$, which is exactly the column j of the matrix, would not belong to $\mathbb{Z}^n$. Hence, $\mathrm{GL}_n(\mathbb{Z}) = G_{Lu}$.

Finally, as $\mathrm{GL}_n(\mathbb{Z})$ is commensurable to itself, it is indeed arithmetic. Furthermore, as $\mathrm{SL}_n(\mathbb{Z})$ has index 2 in $\mathrm{GL}_n(\mathbb{Z})$, it is arithmetic as well.

Example 4. Let $\mathcal{H}$ be the subgroup of $\mathrm{SL}_n(\mathbb{Z})$ consisting of all the matrices with ones on the diagonal, an $(n-1)$-dimensional column vector on the last column and zeros everywhere else.

[1] To see this, pick the empty set of polinomial relations.

This is, those with the following form:

$$h = \begin{pmatrix} 1 & 0 & 0 & \dots & h_1 \\ 0 & 1 & 0 & \dots & h_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & h_{n-1} \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

Later in this work, we will see that these particular matrices provide a good cryptographic platform for our protocol. One can easily check that this is indeed a group. Furthermore, the defining equations of $\mathcal{H}$ are linear equations:

$$x_{ii} - 1 = 0 \quad \text{for } 1 \leq i \leq n$$
$$x_{ij} = 0 \quad \text{for } i \neq j \text{ and } j \leq n-1$$

Thus, $\mathcal{H}$ is algebraic in the sense that it is a subgroup of a $\mathbb{Q}$-subgroup in $\mathrm{GL}_n(\mathbb{C})$, which is given by the same equations extended to $\mathbb{C}$. We call it $\bar{\mathcal{H}}$. To sum up, we have the following subgroup inclusions:

$$\mathrm{GL}_n(\mathbb{C}) \supseteq \mathrm{SL}_n(\mathbb{C}) \supseteq \bar{\mathcal{H}} \supseteq \bar{\mathcal{H}} \cap \mathrm{SL}_n(\mathbb{Z}) = \mathcal{H}$$

Pick $L = \mathbb{Z}^n$. Now, for the elements in G_{Lu} (recall that $G_{Lu} \subseteq \bar{\mathcal{H}}$), we need the image of $(0, \dots, 0, 1)^t$ to belong to $\mathbb{Z}^n$. That is, we need the last column of the matrices in G_{Lu} to have integer entries. Thus, $G_{Lu} \subseteq \mathcal{H}$. Since $\mathbb{Z}^n$ is invariant under $\mathcal{H}$, the reverse inclusion also holds. So we get $G_{Lu} = \mathcal{H}$. Hence, $\mathcal{H}$ is arithmetic.

Remark. Notice that the lattice $< (1, 0, \dots, 0)^t, (0, 1, \dots, 0)^t, \dots, (0, \dots, 1, 0)^t >$ is invariant under any matrix in $\bar{\mathcal{H}}$, because it's only afected by the first $n-1$ columns of the matrices. However, $\bar{\mathcal{H}}$ is not commensurable to $\mathcal{H}$, since $[\bar{\mathcal{H}} : \mathcal{H}]$ is not finite, which follows from the fact that $[\mathbb{C}^{n-1} : \mathbb{Z}^{n-1}]$ is not finite. So, as we have just seen, we need to somehow extend this lattice in order to get a smaller group of L-units.

2.2 Metric in a group, the Cayley Graph

Definition 6. *Let G be a group. By a G-set we mean a given set X with a function $G \times X \to X$, $(g, x) \mapsto gx$, such that $1x = x \quad \forall x \in X$, and $g(g'x) = (gg')x \quad \forall g, g' \in G, x \in X$. We say also that G acts on X, and that there is a G-action on X.*

We say that X' is a G-subset of X if it is stable under the G-action, that is $gX' \subseteq X'$ $\forall g \in G$.

We recall that giving a G-action is equivalent to specifying a group homomorphism from G to $Sym\ X$, the group of permutations of X.

Definition 7. *A function $\alpha : X_1 \to X_2$ between G-sets is said to be a G-map if $\alpha(gx) = g\alpha(x)$ $\forall g \in G, x \in X_1$. We also say that X_1, X_2 are G-isomorphic, and denote it $X_1 \approx X_1$, if there exists a bijective G-map from one the other.*

Definition 8. *By a G-graph (X, V, E, μ, τ) we mean a nonempty G-set X with a specified nonempty G-subset V, its complement $E = X - V$, and two G-maps $\mu, \tau : E \to V$, which we call the incidence functions. In this case we simply say that X is a G-graph.*

We call the elements in V "vertices", and the elements in E, "edges".

Notice that the fact that V is G-stable implies that its complement E is also G-stable, because if E had an element e such that, for some $g \in G$, $ge \in V$, then we would have $g^{-1}ge \in E$, which contradicts the fact that V is G-stable.

For us, functions $\mu, \tau : E \to V$ codify, for every edge of a graph, the two vertices it joins. Furthermore, as they are G-maps, it turns out that $\forall g \in G, e \in E$, $g\mu(e) = \mu(ge)$ and $g\tau(e) = \tau(ge)$. That is, when $g \in G$ acts on two adjacent vertices[2] the result is again two adjacent vertices (see figure 2.1).

Definition 9. *Let G be a group and let S be a set of generators of G. The Cayley graph of G with respect to S, denoted $X(G, S)$, is the graph with vertex set G, edge set $G \times S$, and incidence functions $\mu(g, s) = g$, $\tau(g, s) = gs$ $\forall (g, s) \in G \times S$.*

Remark. For our particular interest, in this definition we have defined S as a generator set. However, the definition could be done with S being any subset of G.

[2]That is, two vertices who are the images of the same edge for τ, μ.

One can construct the Cayley Graph of a group in this way. We know that, given a group G, we can present it in terms of a set of generators and a set of relations, that is, $G =< S \mid R >$. Now we pick the identity element as the starting vertex. For every element $\alpha \in S^{\pm 1} = S \cup \{s^{-1} : s \in S\}$, we put one edge starting at 1 and ending at $\alpha 1 = \alpha$. Now from every new vertex we repeat the process: at every new vertex $g \in G$, for every $\alpha \in S^{\pm 1}$, we put an edge starting at g and ending at αg, without redrawing the edge we are coming from. When the set of generators is finite -and not too large-, one can draw these graphs (see figure 2.2).

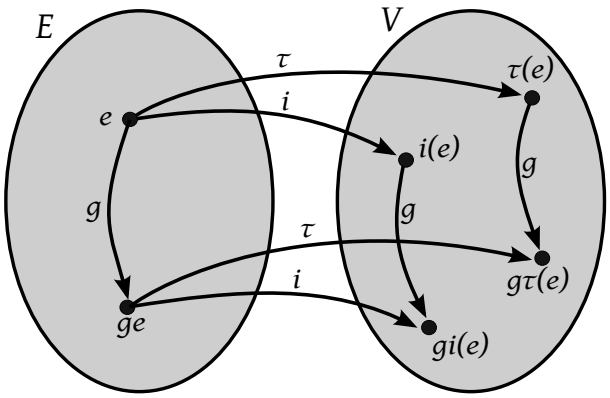

Figure 2.1: $g \in G$ sends two adjacent vertices to two other adjacent vertices.

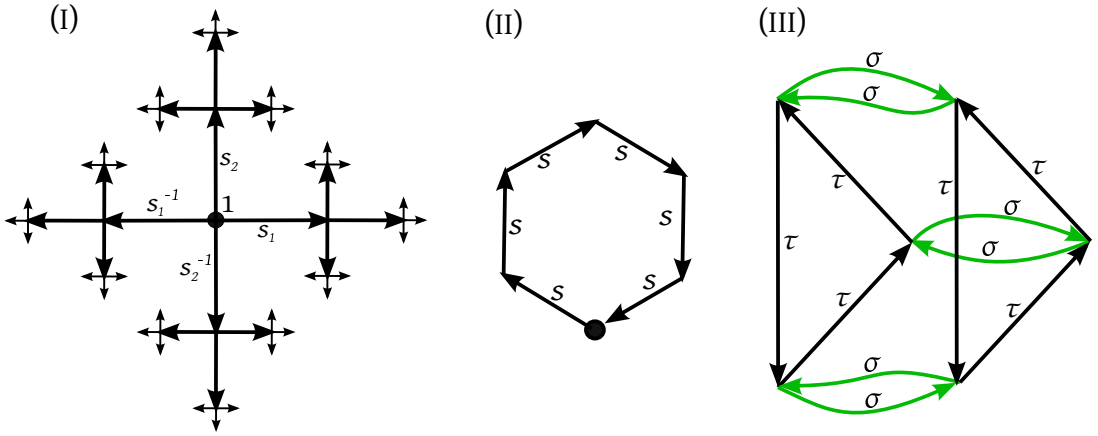

Figure 2.2: (I) represents the Cayley Graph for $< s_1, s_2 \mid \emptyset >$, (II) is the one for $< s \mid s^6 >$ and (III) is the one for the dihedral group $D_{2\cdot 3} = < \sigma, \tau \mid \sigma^2, \tau^3, \tau\sigma\tau\sigma >$.

Definition 10. *Given a group $G =< S \mid R >$ and its Cayley Graph $X(G, S)$, we assign to every edge in X weight 1. We define the distance between every $a, b \in G$ as the minimum length for a path joining a and b in the Cayley's graph, we will denote it $d(a, b)$. We will also denote $d(g, Q)$ the distance between $g \in G$ and a nonempty subset $Q \subseteq G$. We say that a path between two elements $a, b \in G$ is a geodesic when it's length is equal to $d(a, b)$. And we define the length of an element $g \in G$ as $d_G(1, g)$, which we will denote $l_G(g)$.*

Notice that any element in $g \in G =< S \mid R >$, can be reached coming from 1 in $X(G, S)$,

because g can be written as a finite sequence of elements of $S^{\pm 1}$. And this sequence is a path in $X(G,S)$. Therefore, every two elements $a, b \in G$ are connected by the path that goes from a to 1 and then from 1 to b. The length of this path is an upper bound for $d(a,b)$, hence there always exists a geodesic from a to b.

Note also that the distances will depend, not only on the group or subgroup we work with, but also on the particular generating set. Thus, when we write $d_G(a,b)$ or $l_G(c)$, where $a, b, c \in G$, we need to have previously fixed a generator set. Through this work, we will often refer to distances and lengths without mentioning it. In this case, we will assume it is already fixed. However, when needed, we will refer to distances and lengths as $d_S(a,b)$ and $l_S(c)$ respectively, where $a, b, c \in G$ and S is the generating set.

Proposition 2. *For any two finite generating sets S, S' of G such that $S \subseteq S'$,*

$$l_{S'}(g) \leq l_S(g)$$

Proof. Let $g \in G$. When moving from 1 to g, the elements in $S' \backslash S$ add possible shortcuts to a geodesic in $X(G,S)$. □

Proposition 3. *For any two finite generating sets S, S' of G, there is a constant $C \geq 1$ such that, for any $g \in G$ one has*

$$l_{S'}(g) \leq C \; l_S(g)$$

Proof. Let $g \in G$ and write it as a minimal word in S, with length $l_S(g)$. We put each letter of this word as a word in S', each one with length ≥ 1. And we set C as the maximum of all these lengths, so we have $C \geq 1$. This gives an expression for g in terms of S' with no more than $C \; l_S(g)$ letters. Thus, $l_{S'}(g) \leq C \; l_S(g)$. □

Proposition 4. *Let $G =< S \mid R >$ be a group and let $X(G,S)$ be its Cayley Graph. For every $g \in G$, it holds that $l_G(g) = l_G(g^{-1})$.*

Proof. For $g \in G$, pick a minimal path $g = a_1 a_2 \dots a_n$ in the Cayley Graph, its inverse can be written as $g^{-1} = a_n^{-1} \dots a_2^{-1} a_1^{-1}$, which is a path of the same length. Therefore $l_G(g) \geq l_G(g^{-1})$. Repeating the argument exchanging g and g^{-1}, we get that $l_G(g) \leq l_G(g^{-1})$. □

Now consider a finitely generated group G and let H be a finitely generated subgroup in it. We denote with S_G and S_H a pair of fixed generators for G and H, respectively. We have that every $h \in H$ is a vertex in $X(G, S_G)$. Furthermore, every generator in S_H can be expressed as a sequence of generators in S_G. Hence, one can overdraw $X(H, S_H)$ on $X(G, S_G)$ by labelling the vertices that belong to H and taking as single edges all paths between two elements of H (see Figure 2.3).

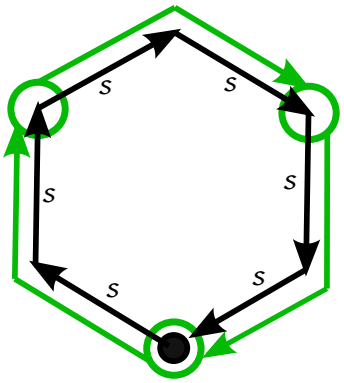

Figure 2.3: In black, $< s \mid s^6 >$ and, in green, $< s^2 \mid s^6 >$.

Proposition 5. *Let $\bar{\mathcal{H}}$ be as in Example 4. Then the following group isomorphisms hold: $(\bar{\mathcal{H}}, \cdot) \simeq (\mathbb{C}^{n-1}, +)$ and $(\mathcal{H}, \cdot) \simeq (\mathbb{Z}^{n-1}, +)$. Hence, $\bar{\mathcal{H}}$ and $\mathcal{H}$ are abelian.*

Proof. For $h, s \in \bar{\mathcal{H}}$ we compute its product:

$$hs = \begin{pmatrix} 1 & 0 & \dots & h_1 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 1 & h_{n-1} \\ 0 & \dots & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & \dots & s_1 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 1 & s_{n-1} \\ 0 & \dots & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \dots & h_1 + s_1 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 1 & h_{n-1} + s_{n-1} \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

The same computation holds when $h, s \in \mathcal{H}$. □

To ease the notation, for a matrix $A \in \mathrm{SL}_{n-1}(\mathbb{Z})$ and a vector $v \in \mathbb{Z}^{n-1}$, we put:

$$M(A, v) = \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}$$

So we can write $\mathcal{H} = \{M(Id, v) : v \in \mathbb{Z}^{n-1}\}$.

Corollary 1. *Let $\{e_1, \dots, e_{n-1}\}$ be the canonical basis of $\mathbb{Z}^{n-1}$. The metric in the Cayley graph of $\mathcal{H}$ with respect to the generator set $\{M(Id, e_i) : 1 \leq i \leq n-1\}$ is the following:*

$$\forall v, w \in \mathbb{Z}^{n-1} \quad d(M(Id, v), M(Id, w)) = \sum_{i=1}^{n-1} |v_i - w_i| \ ,$$

where v_i and w_i denote the components of v and w in the canonical basis, respectively. It follows that

$$\forall v \in \mathbb{Z}^{n-1} \quad l(\ M(Id, v)\ ) = \sum_{i=1}^{n-1} |v_i|$$

Proof. From the proof of the preceding proposition, we see that $e_i \mapsto M(Id, e_i)\ \forall i \in \{1, \dots, n-1\}$ defines an isomorphism from $(\mathbb{Z}^{n-1}, +)$ to $(\mathcal{H}, \cdot)$. By picking $e_1, \dots, e_{n-1}$ as the generators for the Cayley graph of $\mathbb{Z}^{n-1}$ and its images as the generators for the Cayley graph of $\mathcal{H}$, we get the following metrics in the respective groups:

$$\forall v, w \in \mathbb{Z}^{n-1} \quad d(v, w) = d(M(Id, v), M(Id, w)) = \sum_{i=1}^{n-1} |v_i - w_i|$$

□

2.3 Distortion

Definition 11. *Let H be a subgroup of a finitely generated group G and let S_H and S_G be two fixed generating sets for H and G, respectively. We say that H is exponentially distorted in G if there is a positive constant C such that, for each element $h \in H$, we have*

$$l_G(h) \leq C\ log(1 + l_H(h))$$

The interest of this definition is that, if H is an exponentially distorted subgroup of G, the number of generators we need to express an element in terms of the generators of H is exponentially bigger than the number we need in G. Figure (2.4) might help to understand graphically this fenomenon. From Proposition 3 we also have that exponential distortion does not depend on the generator sets we choose for G and H. Indeed, let H and G be exponentially distorted, with respective generator sets S_H and S_G. And let T_H and T_G be two other generator sets for H and G. For $h = 1$ the claim is clear. Now suppose $h \neq 1$. We know that there are two constants $C_1, C_2 \geq 1$ such that

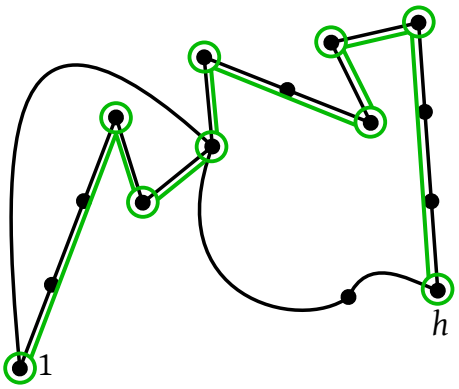

Figure 2.4: Distortion for $h \in H$. In black, we represent some of the edges of a group G. In green, we overdraw a geodesic from 1 to h of some subgroup H. In this case, h has length ≤ 3 in G, and it has length 8 in H.

$$l_{T_G}(h) \leq C_1\ l_{S_G}(h) \quad \text{and} \quad l_{S_H}(h) \leq C_1\ l_{T_H}(h)$$

So we have

$$\begin{aligned} l_{T_G}(h) \leq\ C_1\ l_{S_G}(h)\ \leq\ C_1 C\ log(1 + l_{S_H}(h))\ \leq\ C_1 C\ log(1 + C_2 l_{T_H}(h)) \\ \leq C_1 C\ log\left(C_2[1 + l_{T_H}(h)]\right)\ =\ C_1 C\ log(1 + l_{T_H}(h)) + C_1 C\ log(C_2) \\ \leq C'\ log(1 + l_{T_H}(h)) \quad \text{for some } C' > 0, \text{ as desired.} \end{aligned}$$

Definition 12. *Let A be a ring. An element $a \in A$ is said to be unipotent if there exists an $n \in \mathbb{N}$ such that $(a-1)^n = 0$. And we say that $a \in A$ is virtually unipotent if there exists an $m \in \mathbb{N}$ such that a^m is unipotent, that is, $(a^m - 1)^n = 0$ for some $n \in \mathbb{N}$.*

Remark. If a matrix M is unipotent, its only eigenvalue is 1, because $(M - Id)^n = 0$ for some n, so the minimal polynomial of M must divide $(x-1)^n$.

Definition 13. *For G a group, an element $g \in G$ is called a U-element if the cyclic group $H =< g >$ is infinite and exponentially distorted in G. In other words, $g \in G$ is a U-element if it has infinite order and*

$$l_G(g^n) \leq C\ log(1 + |n|)$$

holds for all $n \in \mathbb{Z}$ and some $C > 0$.

Example 5. Let B denote the Baumslag-Solitar group $B(1,2)$, that is, the group presented as $< t, a \mid tat^{-1} = a^2 >$. We will prove $H =< a >$ is exponentially distorted in B.

We first need to see that $a^{2^k} = t^k a t^{-k} \ \ \forall k \geq 1$. When $k = 1$, it holds by definition. Now assume the equality holds for $k-1$, $k > 1$. We prove it for k:

$$\begin{aligned} a^{2^{k-1}} = t^{k-1} a t^{-(k-1)} \quad \Rightarrow \quad a^{2^{k-1}} a^{2^{k-1}} = t^{k-1} a t^{-(k-1)} t^{k-1} a t^{-(k-1)} \\ \Rightarrow \quad a^{2^k} = t^{k-1} a^2 t^{-(k-1)} = t^{k-1} t a t^{-1} t^{-(k-1)} = t^k a t^{-k}, \text{ as desired.} \end{aligned}$$

We also need to prove that $l_B(a^n) \leq l_B(a^{2^k})$ when $|n| \leq 2^k$. We take $n \geq 0$ and make the proof for both a^n and a^{-n}. We can write n as a sum of powers of 2, that is, $n = \sum_{i=1}^{N} 2^{m_i}$, where we have ordered the powers in an increasing manner. And we will have that $m_N \leq k$ and

$N \leq k$. We also know that $l_B(a^n) = l_B(a^{-n})$, so we can write:

$$l_B(a^{-n}) = l_B(a^n) = l_B\left(a^{2^{m_1}} a^{2^{m_2}} \ \dots \ a^{2^{m_N}}\right) =$$
$$l_B(t^{m_1} a t^{-m_1} t^{m_2} a t^{-m_2} \ \dots \ t^{m_N} a t^{-m_N}) =$$
$$l_B(t^{m_1} a t^{m_2-m_1} a t^{m_3-m_2} \ \dots \ t^{m_N-m_{N-1}} a t^{-m_N}) \leq$$
$$N + m_1 + (m_2 - m_1) + \cdots + (m_N - m_{N-1}) + m_N =$$
$$N + m_N \leq k + k = 2k <$$
$$2k + 1 = l_B(t^k a t^{-k}) = l_B(a^{2^k}), \text{ as desired.}$$

Now consider $h \in H$, $h \neq 1$. That is, $h = a^n$ for some $n \in \mathbb{Z} \{0\}$. And let k be the minimum positive integer such that $|n| \leq 2^k$. On one hand, we have that

$$l_B(h) = l_B(a^n) \leq l_B(a^{2^k}) = l_B(t^{-k} a t^k) = 2k + 1 \quad \text{(I)}$$

On the other hand, by definition of k, we have

$$2^{k-1} \leq \ |n| \ = l_H(a^n) = l_H(h) \quad \text{(II)}$$

From (I) and (II) we get that, for some constants $M, C > 0$,

$$\begin{aligned} l_B(h) \leq \ 2k+1 \ &\leq \ Mk \ = \ M \ (k - 1 + 1) \\ &= \ M \ (log_2(2^{k-1}) + 1) \ \leq \ M \ (log_2|n| + 1) \\ &= \ M \ (log_2[l_H(h)] + 1) \ \leq \ C \ log_2(l_H(h)) \\ &\leq \ C \ log_2(l_H(h) + 1), \ \text{ as desired.} \end{aligned}$$

Notice we have also proved that a is a U-element in B. This group can be realized as a linear group since the following two matrices satisfy the relation $tat^{-1} = a^2$.

$$t = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Proposition 6. *Let $G =< g_1, \dots, g_r >$ be a finitely generated group and $H =< h_1, \dots, h_m >$ a finitely generated abelian subgroup in it. If every element of H is a U-element, H is exponentially distorted.*

Proof. Assume every element of $H =< h_1, \dots, h_m >$ is a U-element. Pick $h \in H$ and write it in terms of the generators of H with minimum length:

$$h = \prod_{k=1}^{N} h_{i_k}^{p_k}, \quad p_k \geq 1 \ \forall k$$

Because H is abelian, $N \leq m$. By assumption, we can write every $h_{i_k}^{p_k}$ in terms of $g_1, \ldots, g_r$ with a length bounded from above by $C_k\ log(1+|p_k|)$ for some positive constant C_k. We define C as the largest of these constants and we define p as de maximum in $\{|p_k| : 1 \leq k \leq N\}$. Then,

$$l_G(h) \leq \sum_{k=1}^{N} C\ log(1+|p_k|) \leq \sum_{k=1}^{N} C\ log(1+|p|) = NC\ log(1+|p|)$$
$$\leq mC\ log(1+|p|) \leq mC\ log\left(1+\sum_{k=1}^{N}|p_k|\right) = mC\ log\left(1+l_H(h)\right)$$

□

2.4 Properties needed for G and H.

The construction of a cryptosystem based on our protocol relies on the existence of pairs (G, H), consisting of a finitely generated group G and a finitely generated subgroup H of G with the following properties:

(i) The geodesic length problem (GLP) and the membership problem (MP) for H are solvable in polynomial time. These problems are defined as follows:

- GLP: given $h \in H$, find $l_H(h)$.
- MP: given $g \in G$ find out if $g \in H$ or $g \notin H$.

(ii) There exists a constant $C_1 > 0$ such that, for every $h \in H$, one can compute in polynomial time a path from the identity to h whose length $m(h)$ is bounded from above by $C_1 l_G(h)$.

This gives Eve the possibility to write and intercepted $h \in H$ in terms of $g_1, \ldots, g_s$ in polynomial time and also doing it with a length $m(h) \in O(l_G(h))$. This last property will fully take sense with the next requirement.

(iii) H is exponentially distorted in G. By definition, for some $C_2 > 0$, we have

$$l_G(h) \leq C_2\ log(1+l_H(h))$$

Combining this condition with $m(h) \leq C_1 l_G(h)$, we get $m(h) \leq C_1 C_2\ log(1+l_H(h))$. That is, Eve might be computing lengths exponentially shorter than the lengths Alice is sending. This phenomenon hides very well the information, because a 'short' element, with length $m(h)$ in G, can be the translation of many 'long' elements.

(iv) The index of the normalizer $N_G(H)$ in G is infinite[3]. We will prove that this property is equivalent to having an infinite number of diferent conjugates of H. We will also prove that the conjugation of the subgroup preserves all the properties above. Hence, the conjugation of H will supply infinite possible private keys for the protocol. This makes more difficult for Eve to find the private key, since she doesn't have a finite set of possibilities.

We prove the results we have just mentioned:

Lemma 3 (Orbit-Stabilizer Theorem)**.** *For a G-action $*$ on a set X and for $s \in X$, we denote $Orb(s) = \{g * s : g \in G\}$, the orbit of s, and $Stab(s) = \{g \in G : g * s = s\}$, the stabilizer of s. Then it holds that $|Orb(s)| = [G : Stab(s)]$.*

Proof. Consider

$$\varphi : G \longrightarrow Orb(s)$$
$$g \longmapsto g * s$$

Because of the definitions of orbit and group action, it is surjective. Now pick $g, q \in G$.

$$\varphi(g) = \varphi(q) \quad \Rightarrow \quad g * s = g * q \quad \Rightarrow \quad s = (g^{-1}q) * s \quad \Rightarrow$$
$$g^{-1}q \in Stab(s), \text{ which is a subgroup.} \quad \Rightarrow \quad g \equiv q \pmod{Stab(s)}$$

Thus, we have the following bijection:

$$\tilde{\phi} : {}^{G}/_{Stab(s)} \longrightarrow Orb(s)$$
$$[g] \longmapsto g * s$$

□

Proposition 7. *For S a subset of G, the number of distinct subsets of G which are conjugates of S is equal to $[G : N_G(S)]$, where $N_G(S)$ is the normalizer of S.*

Proof. Denote $\mathcal{P}(G)$ the power set of G and consider the conjugation aplication:

$$g* : \mathcal{P}(G) \longrightarrow \mathcal{P}(G)$$
$$S \longmapsto gSg^{-1}$$

[3]We recall that the normalizer of H is the set of all elements in G that commute with H.

This defines a G-action on $\mathcal{P}(G)$, because $e * S = S$ and $g * (q * S) = (g * q) * S$ for all $g, q \in G$. And notice that $Stab(S) = N_G(S)$. Then, by the Orbit-Stabilizer theorem, we have that $|Orb(S)| = [G : Stab(S)] = [G : N_G(S)]$. □

Proposition 8. *If properties* **(i), (ii), (iii)** *hold for a subgroup H of G, they hold for any conjugate gHg^{-1}, $g \in G$.*

Proof. For some $g \in G \backslash H$, let $W = gHg^{-1}$ be a conjugate of H in G. Assume all properties hold for H. We notice that if $H =< h_1, \ldots, h_n >$ then $W =< gh_1g^{-1}, \ldots, gh_ng^{-1} >$. Hence with this two respective generator sets, any word in H has the same length as its conjugate in W. Furthermore, because of cancelation of g^{-1} with g, any word in W will be the concatenation of g, some generators of H and finally g^{-1}. Now we give a proof for each property:

(i) Let $w \in G$. We have that $w \in W$ if, and only if, $g^{-1}wg \in H$. Thus, the MP can be solved by computing $h = g^{-1}hg$ -which can be done in polynomial time- and solving for h and H -by assumption, again in polynomial time-.

Now let $w \in W$ and let S be a generator set of W. We can solve the GLP in polynomial by solving the problem for $g^{-1}wg \in H$ with the conjugate generator set $g^{-1}Sg$, because we know that if we choose this generator set for H, the lengths of the elements are preserved under the conjugation $W \mapsto g^{-1}Wg = H$.

(ii) Again, let $w \in W = gHg^{-1}$. We can first compute $h = g^{-1}wg \in H$, which can be done in polynomial time. Now, by assumption, we can put h in terms of the generators, $g_1, \ldots, g_s$, of G in polynomial time and also doing it with a resulting length $m(h) \leq C\ l_G(h)$. Finally, again in polynomial time, we can make its conjugate and get w in terms of $g_1, \ldots, g_s, g$. That is, we get w in terms of $g_1, \ldots, g_s$, because g is expressed in terms of the generator set. As these are finite steps that are all done in polynomial time, the whole process can also be done in polynomial time. Moreover, the difference in letters between $m(h)$ and the length $m(w)$ we get for w is, at most, two times $l_G(g)$, which is a constant. The same holds for the difference between $l_G(h)$ and $l_G(w)$. So there is indeed a positive constant C' such that the resulting length satisfies $m(w) \leq C' l_G(w)$.

(iii) By assumption, for any $h \in H$, $l_G(h) \leq C\ log(1 + l_H(h))$ for some positive constant C.

We also have that

$$\begin{cases} l_G(ghg^{-1}) = l_G(h) + k, \text{ where } |k| \leq 2\ l_G(g) \\ l_W(ghg^{-1}) = l_H(h), \text{ with the appropriate pair of generator sets.} \end{cases}$$

Hence, $l_G(ghg^{-1}) = l_G(h) + k \leq C\ log(1 + l_H(h)) + k = C\ log(1 + l_W(ghg^{-1})) + k$. So there is indeed a positive constant C' such that $l_G(ghg^{-1}) \leq C'\ log(1 + l_W(ghg^{-1}))$. And we know exponential distortion doesn't depend on the particular generator set.

□

Chapter 3

An example of interest

Let $\mathcal{H}$ be the subgroup of $\mathrm{SL}_n(\mathbb{Z})$ introduced in Example 4, from Chapter 2. After giving some results that are needed, we will see that properties **(i), (ii), (iii)** from Section 2.4 hold for $\mathcal{H}$. Hence, the pair $(\mathrm{SL}_n(\mathbb{Z}), \mathcal{H})$ will be a suitable platform for the protocol.

Once again, we will use the following notation. For a matrix $A \in \mathrm{SL}_{n-1}(\mathbb{Z})$ and a vector $v \in \mathbb{Z}^{n-1}$:

$$M(A, v) = \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}$$

With this notation, $\mathcal{H} = \{M(Id, v) : v \in \mathbb{Z}^{n-1}\}$. And we recall from Proposition 5 and Corollary 1, that $(\mathcal{H}, \cdot) \simeq (\mathbb{Z}^{n-1}, +)$ and that by picking the canonical basis in $(\mathbb{Z}^{n-1}, +)$ we get the following metric in the Cayley graph of $\mathcal{H}$, which we will be using throughout this chapter:

$$\forall v, w \in \mathbb{Z}^{n-1} \quad d_{\mathcal{H}}(M(Id, v), M(Id, w)) = \sum_{i=1}^{n-1} |v_i - w_i|$$

Lemma 4. *Let G be a finitely generated group and let H be a finitely generated subgroup of G. Assume there is a nonempty subset $S \subseteq H$ such that, for some positive constant C, it holds that $\forall h \in H \ d_H(h, S) \leq C$. Then there is a positive constant M such that $\forall h \in H \ d_G(h, S) \leq M$.*

Proof. Let $h \in H$. And let $h_1 \dots h_m$ be a minimal path from h to the set S, where every h_i belongs to the generator set of H and there are possible repetitions. By assumption we have that $m \leq C$.

Every generator of H is a finite concatenation of generators of G and, as the generators of H are finite, there is one with maximum length in G. We call this length L. It follows that the

length in G of the path $h_1 \dots h_m$ is upper bounded by mL. We have:

$$d_G(h, S) \leq mL \leq CL \text{ , so we can set } M = CL.$$

□

Lemma 5. *Let $\beta, \lambda \in \mathbb{R}$ be such that $\beta > 0$ and $1 < \lambda < 2$. There is an $m \in \mathbb{N}$ and a positive constant $C \in \mathbb{R}$ such that $m \leq C\ log(1+\beta)$ and*

$$|\beta - \sum_{i=0}^{m} \varepsilon_i \lambda^i| \leq 1, \quad \text{where } \varepsilon_i \in \{0, 1\}\ \forall i.$$

That is, we can approach β at distance ≤ 1 by additioning no more than $C\ log(1+\beta)$ powers of λ.

Proof. If $\beta \leq 1$ we get $|\beta - 1| \leq 1$ and $m = 0$, so the claim holds. Now we assume $\beta > 1$. And we set n_1 as the maximum natural such that $\lambda^{n_1} \leq \beta$. If we get that $\beta - \lambda^{n_1} \leq 1$, we end the process. If not, we set n_2 as the maximum natural such that $\lambda^{n_1} + \lambda^{n_2} \leq \beta$. Again, if we get that $\beta - (\lambda^{n_1} + \lambda^{n_2}) \leq 1$, we end the process. If not, we set n_3 as the maximum natural such that $\lambda^{n_1} + \lambda^{n_2} + \lambda^{n_3} \leq \beta$, and so on.

Assume we have added k powers of λ and that we see that we still can't end process. So we add another power $\lambda^{n_{k+1}}$, with the maximum natural n_{k+1} such that

$$\sum_{i=1}^{k} \lambda^{n_i} + \lambda^{n_{k+1}} \leq \beta \quad \Leftrightarrow \quad \lambda^{n_k} + \lambda^{n_{k+1}} \leq \ \beta - \sum_{i=1}^{k-1} \lambda^{n_i} \ =: \alpha$$

And by construction we also have that n_k is the maximum natural such that

$$\lambda^{n_k} \leq \beta - \sum_{i=1}^{k-1} \lambda^{n_i} = \alpha$$

We want to prove that $n_k > n_{k+1}$. To do so, we assume that $n_k \leq n_{k+1}$. It follows that

$$\lambda^{n_k} + \lambda^{n_{k+1}} \geq \lambda^{n_k} + \lambda^{n_k} = 2\lambda^{n_k} > \lambda^{n_k+1} > \alpha, \quad \text{which leads to a contradiction.}$$

With this in hand we see that the process ends with, at most, $n_1 + 1$ additioned powers of λ. And we know that

$$\lambda^{n_1} \leq \beta \ \Rightarrow \ \lambda^{n_1} \leq \beta + 1 \ \Rightarrow \ n_1 \leq \frac{1}{log\ \lambda} log(1+\beta)$$

Now we set $m = n_1$ and $C = \frac{1}{log\ \lambda}$ and the claim holds. □

Lemma 6. *Let $||\cdot||$ be standard norm and let*

$$w_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad w_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{and } A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} .$$

There are two positive constants C, M such that for every $v \in \mathbb{Z}^2$ there is an $m \in \mathbb{N}$ such that $1 \leq m \leq C\ log(1+||v||)$ and v is at a distance -the standard norm distance- bounded by M from the set

$$S_m := \left\{ \sum_{k=-m}^{-1} \beta_k A^k w_2 + \sum_{k=0}^{m} \beta_k A^k w_1 : (\beta_{-m}, \ldots, \beta_m) \in \{-1, 0, 1\}^{2m+1} \right\}$$

Proof. The matrix A has eigenvalues

$$\lambda_+ = \frac{1+\sqrt{5}}{2} \qquad \lambda_- = \frac{1-\sqrt{5}}{2}$$

$$\text{And by defining } \alpha := \lambda_+ \text{ we also have } \quad -\alpha^{-1} = \lambda_-$$

It will be crucial the fact that $|\lambda_+| > 1$ and $|\lambda_-| < 1$. We have the following equalities:

$$(A - \alpha Id) \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = \begin{pmatrix} 1-\alpha & 1 \\ 1 & -\alpha \end{pmatrix} \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha - \alpha^2 + 1 \\ \alpha - \alpha \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$(A + \alpha^{-1} Id) \begin{pmatrix} -\alpha^{-1} \\ 1 \end{pmatrix} = \begin{pmatrix} 1+\alpha^{-1} & 1 \\ 1 & \alpha^{-1} \end{pmatrix} \begin{pmatrix} -\alpha^{-1} \\ 1 \end{pmatrix} = \begin{pmatrix} -\alpha^{-1} - \alpha^{-2} + 1 \\ -\alpha^{-1} + \alpha^{-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

So the eigenvectors are

$$v_+ = \begin{pmatrix} \alpha \\ 1 \end{pmatrix} \text{ for } \lambda_+ \quad \text{and} \quad v_- = \begin{pmatrix} -\alpha^{-1} \\ 1 \end{pmatrix} \text{ for } \lambda_-$$

Notice they are ortogonal and that we can express the canonical basis $\{w_1, w_2\}$ as follows:

$$w_1 = \frac{1}{\sqrt{5}} \left(\alpha^{-1} v_+ + \alpha v_- \right) \qquad w_2 = \frac{1}{\sqrt{5}} \left(v_+ - v_- \right)$$

For every natural k, we have that

$$A^k w_1 = \frac{1}{\sqrt{5}} \left(\alpha^{-1} \lambda_+^k v_+ + \alpha \lambda_-^k v_- \right) = \frac{1}{\sqrt{5}} \left(\lambda_+^{k-1} v_+ - \lambda_-^{k-1} v_- \right)$$

$$A^{-k} w_2 = \frac{1}{\sqrt{5}} \left(\lambda_+^{-k} v_+ - \lambda_-^{-k} v_- \right)$$

Now let $v \in \mathbb{Z}^2 \backslash \{0\}$. There are $a, b \in \mathbb{R}$ such that

$$v = \frac{a}{\sqrt{5}} v_+ + \frac{b}{\sqrt{5}} v_- \ , \quad \text{and we have } \ |a| + |b| > 0.$$

Since $1 < \lambda_+, -\lambda_-^{-1} < 2$, from Lemma 5 we have that there are sums of powers of λ_+ and λ_-^{-1}, respectively, such that:

$$\left|\sum_{k=0}^{m_a} \varepsilon_k \lambda_+^k - a\right| \leq 1, \text{ where } m_a \leq C_1\ log(1+|a|),\ C_1 > 0, \text{ and } \varepsilon_k \in \{0,1\} \ \veebar\ \varepsilon_k \in \{0,-1\}.$$

$$\left|\sum_{k=0}^{m_b} \delta_k (-\lambda_-)^{-k} - b\right| \leq 1, \text{ where } m_b \leq C_2\ log(1+|b|),\ C_2 > 0, \text{ and } \delta_k \in \{0,1\} \ \veebar\ \delta_k \in \{0,-1\}.$$

If we define

$$t := \frac{1}{\sqrt{5}}\left(\sum_{k=0}^{m_a} \varepsilon_k \lambda_+^k\right) v_+ + \frac{1}{\sqrt{5}}\left(\sum_{k=0}^{m_b} \delta_k (-\lambda_-)^{-k}\right) v_-$$

It follows that

$$||t - v|| \leq \frac{1}{\sqrt{5}}\sqrt{||v_+||^2 + ||v_-||^2} = \frac{\sqrt{5}}{\sqrt{5}} = 1 \quad \text{(I)}$$

Now we will prove that t is at bounded distance from S_m. To do so, we need to show the following:

- $\displaystyle\sum_{k=1}^{+\infty} ||\varepsilon_k \left(A^k w_1 - \frac{\lambda_+^{k-1}}{\sqrt{5}} v_+\right)|| = \sum_{k=0}^{+\infty} \varepsilon_k || \frac{-1}{\sqrt{5}} \lambda_-^{k-1} v_-|| = \frac{||v_-||}{\sqrt{5}} \sum_{k=0}^{+\infty} \varepsilon_k |\lambda_-|^{k-1}$
- $\displaystyle\sum_{k=0}^{+\infty} ||\delta_k \left(A^{-k} w_2 + \frac{\lambda_-^{-k}}{\sqrt{5}} v_-\right)|| = \sum_{k=0}^{+\infty} \delta_k || \frac{1}{\sqrt{5}} \lambda_+^{-k} v_+|| = \frac{||v_+||}{\sqrt{5}} \sum_{k=0}^{+\infty} \delta_k |\lambda_+^{-1}|^k$

Since $|\lambda_-|,\ |\lambda_+^{-1}| < 1$, the series converge. So it follows that

$$\sum_{k=1}^{+\infty} \varepsilon_k \left(A^k w_1 - \frac{\lambda_+^{k-1}}{\sqrt{5}} v_+\right) \quad \text{and} \quad \sum_{k=0}^{+\infty} \delta_k \left(A^{-k} w_2 + \frac{\lambda_-^{-k}}{\sqrt{5}} v_-\right) \quad \text{are convergent.}$$

And, hence, there is an upper bound N such that for every $l, r \in \mathbb{N}$

$$\left|\left|\sum_{k=1}^{l} \varepsilon_k \left(A^k w_1 - \frac{\lambda_+^{k-1}}{\sqrt{5}} v_+\right)\right|\right| \leq N \quad \text{and} \quad \left|\left|\sum_{k=0}^{r} \delta_k \left(A^{-k} w_2 + \frac{(-1)^k (-\lambda)^{-k}}{\sqrt{5}} v_-\right)\right|\right| \leq N$$

Where we have put $\lambda_-^{-k} = (-1)^k (-\lambda_-)^{-k}$. This can also be written as

$$\left|\left|\sum_{k=1}^{l} \varepsilon_k A^k w_1 - \frac{1}{\sqrt{5}}\left(\sum_{k=0}^{l-1} \varepsilon_k \lambda_+^k\right) v_+\right|\right| \leq N \quad \text{and}$$

$$\left|\left|\sum_{k=0}^{r} (-1)^{k+1} \delta_k A^{-k} w_2 - \frac{1}{\sqrt{5}}\left(\sum_{k=0}^{r} \delta_k (-\lambda_-)^{-k}\right) v_-\right|\right| \leq N$$

With this in hand, we set $l - 1 = m_a$ and $r = m_b$. And we define

$$s := \sum_{k=1}^{m_a} \varepsilon_k A^k w_1 + \sum_{k=0}^{m_b} (-1)^{k+1} \delta_k A^{-k} w_2\ .$$

For $m = \max\{m_a, m_b\}$, it is clear that $s \in S_m$. And we get that $||s - t|| \leq 2N$. From (I), it follows that

$$||s - v|| \leq ||s - t|| + ||t - v|| \leq 2N + 1$$

To finish this proof we need to show that there is some $C > 0$ such that $m \leq C\ log(1 + ||v||)$. In the following, all the C_i are positive constants and we use that $||v_+||, ||v_-|| > 1$ and $|a| + |b| > 0$.

$$\begin{aligned}
m &\leq m_a + m_b \leq C_1\ log(1 + |a|) + C_2\ log(1 + |b|) \leq C_3\ [log(1 + |a|) + log(1 + |b|)] \\
&\leq 2C_3\ log(1 + |a| + |b|) = 2C_3\ \left[log\left(\frac{1}{\sqrt{5}} + \frac{|a| + |b|}{\sqrt{5}}\right) + log(\sqrt{5})\right] \\
&\leq C_4\left[log\left(1 + \frac{|a| + |b|}{\sqrt{5}}\right) + log(\sqrt{5})\right] \leq C_5\ log\left(1 + \frac{|a| + |b|}{\sqrt{5}}\right) \\
&= C_5\ log\left(\frac{1}{2} + \frac{1}{2}\frac{|a| + |b|}{\sqrt{5}}\right) + C_5\ log\,(2) \\
&\leq C_5\ log\left(\frac{1}{2} + \sqrt{\left(\frac{|a|}{\sqrt{5}}\right)^2 + \left(\frac{|b|}{\sqrt{5}}\right)^2}\right) + C_5\ log\,(2) \\
&\leq C\ log\left(\frac{1}{2} + \sqrt{\left(\frac{|a|}{\sqrt{5}}\right)^2 + \left(\frac{|b|}{\sqrt{5}}\right)^2}\right) \\
&\leq C\ log\left(1 + \sqrt{\left(\frac{|a|}{\sqrt{5}}\right)^2 + \left(\frac{|b|}{\sqrt{5}}\right)^2}\right) \\
&\leq C\ log\left(1 + \sqrt{\left(\frac{|a|}{\sqrt{5}}||v_+||\right)^2 + \left(\frac{|b|}{\sqrt{5}}||v_-||\right)^2}\right) \\
&= C\ log(1 + ||v||),
\end{aligned}$$

□

Corollary 2. *For $n \geq 3$, we define A_i as a matrix equal to the identity except for a 2×2 block on the diagonal, which is A (see Lemma 6) and it is placed with its $(1,1)$ component on the (i,i) component of A_i. That is,*

$$A_i = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & A & \dots & 0 \\ \vdots & \dots & 0 & \ddots & \vdots \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix}$$

We set $e_1, \dots, e_{n-1}$ as the canonical basis of $\mathbb{Z}^{n-1}$. Then, there are two positive constants C, M such that for every $v \in \mathbb{Z}^{n-1}$ there is an $m \in \mathbb{N}$ such that $1 \leq m \leq C\ log(1 + ||v||)$, and v is

at a distance -the standard norm distance- bounded by M from the set $S_{m,n}$, defined as follows:

$$S_{m,n} = \left\{ \sum_{i \in I_o} \left(\sum_{k=-m}^{-1} \beta_{i,k} A_i^k e_{i+1} + \sum_{k=0}^{m} \beta_{i,k} A_i^k e_i \right) : \right.$$
$$\left. I_o = \{1, 3, \ldots, n-2\}, (\beta_{i,-m}, \ldots, \beta_{i,m}) \in \{-1, 0, 1\}^{2m+1} \right\} \textit{ if } n \textit{ is odd}$$

$$S_{m,n} = \left\{ \sum_{i \in I_e} \left(\sum_{k=-m}^{-1} \beta_{i,k} A_i^k e_{i+1} + \sum_{k=0}^{m} \beta_{i,k} A_i^k e_i \right) : \right.$$
$$\left. I_e = \{1, 3, \ldots, n-3\} \cup \{n-2\}, (\beta_{i,-m}, \ldots, \beta_{i,m}) \in \{-1, 0, 1\}^{2m+1} \right\} \textit{ if } n \textit{ is even}$$

Proof. Every matrix A_i acts on e_i and e_{i+1} in the same way that A acts on w_1 and w_2 in Lemma 6. Hence, from this lemma we get that there are two positive constants C, P such that for every vector $v_i \in < e_i, e_{i+1} >$ there is an $m \in \mathbb{N}$ such that $1 \leq m \leq C\ log(1 + ||v_i||)$ and v_i is at a distance -the standard norm distance- bounded by P from the set

$$S_{m,n}^{(i)} := \left\{ \sum_{k=-m}^{-1} \beta_{i,k} A_i^k e_{i+1} + \sum_{k=0}^{m} \beta_{i,k} A_i^k e_i : (\beta_{i,-m}, \ldots, \beta_{i,m}) \in \{-1, 0, 1\}^{2m+1} \right\}$$

Now let $v \in \mathbb{Z}^{n-1}$. The first two components[1] are at a distance bounded by P from some $s_1 \in S_{m,n}^{(1)}$, the following two are at a distance bounded by P from some $s_3 \in S_{m,n}^{(3)}$, and so on. When n is even (that is, when $n-1$ is odd), we can approach the last remaining component with some $s_{n-2} \in S_{m,n}^{(n-2)}$, which is again at a distance bounded by P. Now we set $s \in \mathbb{Z}^{n-1}$ as the sum of all the vectors s_i we have found. It follows that $s \in S_{m,n}$ and also that $||v - s|| \leq nP$. Finally, we set $M = nP$. □

Lemma 7. *For a matrix $B \in SL_{n-1}(\mathbb{Z})$ and a vector $v \in \mathbb{Z}^{n-1}$,*

$$M(B, 0) M(Id, v) M(B, 0)^{-1} = M(Id, Bv)$$

This can easily be seen by direct computation.

Proposition 9. *For every vector $v \in \mathbb{Z}^{n-1}$, the length of the element $M(Id, v)$ in $SL_n(\mathbb{Z})$ is for some positive constant C, which only depends on n, bounded by $C\ log(1 + ||v||)$. Moreover there exists a constant M, such that a path of length $M\ log(1 + ||v||)$ from the identity element to $M(Id, v)$ can be constructed in polynomial time in $||v||$.*

[1] By two consecutive components, i and $i+1$, we mean the vector $(0, \ldots, v_i, v_{i+1}, \ldots, 0)^T$.

Proof. Firstly, we will prove the bound $l_S(M(Id,v)) \leq C\ log(1+||v||)$, where the subindex S refers to $\mathrm{SL}_n(\mathbb{Z})$ for the case $n=3$. We define S_m as in Lemma 6.

Let $v \in \mathbb{Z}^2$. From Lemma 6 and the isomorphism $\mathbb{Z}^{n-1} \simeq \mathcal{H}$ it follows that there are constants $M, Q > 0$, that only depend on n, such that

$$\begin{aligned} d_{\mathcal{H}}(M(Id,v), M(Id,s)) \leq M \quad & \text{for some} \quad s \in S_m \\ & \text{and with} \quad 1 \leq m \leq Q log(1+||v||) \end{aligned}$$

Now from Lemma 4 we see that we can take this distance in the Cayley graph of $\mathrm{SL}_3(\mathbb{Z})$ just by replacing M with some other bound $P > 0$. That is, there are $P, Q > 0$ such that for every $v \in \mathbb{Z}^2$ there is a natural m such that $1 \leq m \leq Q\ log(1+||v||)$ and there exists $s \in S_m$ with

$$d_S\left(M(Id,v), M(Id,s)\right) \leq P\ .$$

With this in hand, the claim will follow from setting the bound $l_S(M(Id,s)) \leq R\, log(1+||v||)$ for some $R > 0$. From the definition of S_m in Lemma 6, there are $\beta_{-m} \ldots \beta_m$ such that

$$\begin{aligned} M(Id,s) &= M\left(Id, \sum_{k=-m}^{-1} \beta_k A^k w_2 + \sum_{k=0}^{m} \beta_k A^k w_1\right) \\ &= \prod_{k=-m}^{-1} M(Id, \beta_k A^k w_2) \prod_{k=0}^{m} M(Id, \beta_k A^k w_1) \qquad \text{(I)} \end{aligned}$$

For every factor, and using Lemma 7, we have that for $i \in \{1,2\}$

$$\begin{aligned} M(Id, \beta_k A^k w_i) &= M(Id, A^k w_i)^{\beta_k} = \left(M(A,0)^k M(Id,w_i) M(A,0)^{-k}\right)^{\beta_k} \\ &= M(A,0)^k M(Id,w_i)^{\beta_k} M(A,0)^{-k} = M(A,0)^k M(Id, \beta_k w_i) M(A,0)^{-k} \end{aligned}$$

Now we compute one factor by the following:

$$\begin{aligned} & M(A,0)^k M(Id,\beta_k w_i) M(A,0)^{-k}\ M(A,0)^{k+1} M(Id, \beta_{k+1} w_{i'}) M(A,0)^{-k-1} \\ &= \ M(A,0)^k M(Id,\beta_k w_i) M(A,0) M(Id, \beta_{k+1} w_{i'}) M(A,0)^{-k-1} \end{aligned}$$

This cancellation shows that the product above leads to

$$M(Id,s) = M(A,0)^{-m} \left(\prod_{k=-m}^{-1} \left[M(Id,\beta_k w_1) M(A,0)\right] \prod_{k=0}^{m} \left[M(Id,\beta_k w_2) M(A,0)\right] \right) M(A,0)^{m-1}$$

We are looking for a path in $\mathrm{SL}_3(\mathbb{Z})$, but we can't assume that every matrix in this product has determinant 1. However, taking the matrices between brackets as a single factor, we see that

there are $4m$ factors. And one can check that, if m is even, they can be regrouped as $2m$ factors of constant length in $\mathrm{SL}_3(\mathbb{Z})$ with determinant 1 and that, if m is odd, the same can be done with $2m+1$ factors. Hence, in both cases there is a constant $K > 0$ such that

$$l_S(M(Id, s)) \leq Km \leq KQ\ log(1 + ||v||)$$

Now we set $R := KQ$ and we get the desired bound.

From this reasoning we will see the claim in the case $n > 3$. We pick $v \in \mathbb{Z}^{n-1}$. And we follow the same arguments replacing S_m by $S_{m,n}$, defined in Corollary 2. Now expression (I) will turn into the following:

$$\begin{aligned} M(Id, s) &= M\left(Id, \sum_{i\in I}\left(\sum_{k=-m}^{-1} \beta_{i,k}A_i^k e_{i+1} + \sum_{k=0}^{m} \beta_{i,k}A_i^k e_i\right)\right) \\ &= \prod_{i\in I}\left(\prod_{k=-m}^{-1} M(Id, \beta_{i,k}A_i^k e_{i+1}) \prod_{k=0}^{m} M(Id, \beta_{i,k}A_i^k e_i)\right) \ , \quad \text{(II)} \\ &\text{where } \begin{cases} I = I_e = \{1, 3, \ldots, n-3\} \cup \{n-2\} \text{ if } n \text{ is even,} \\ I = I_o = \{1, 3, \ldots, n-2\} \text{ if } n \text{ is odd.} \end{cases} \end{aligned}$$

So we have $\#I = \frac{n}{2}$ if n is even, and $\#I = \frac{n-1}{2}$ if n is odd. And using Lemma 7, we will get that, for some $K > 0$,

$$l_S\left(\prod_{k=-m}^{-1} M(Id, \beta_{i,k}A_i^k e_{i+1}) \prod_{k=0}^{m} M(Id, \beta_{i,k}A_i^k e_i)\right) \leq Km \quad \forall i \in I$$

And it follows that

$$l_S(M(Id, s)) \leq \frac{n}{2}Km \leq \frac{n}{2}K\ log(1 + ||v||)$$

So we set $R := \frac{n}{2}K$.

Finally, we want to see that there exists a constant M, such that a path of length $M\ log\,(1 + ||v||)$ from the identity element to $M(Id, v)$ can be constructed in polynomial time in $||v||$. The following algorithm proves the claim:

- Given $M(Id, v)$, we reach an $s \in S_m$ at bounded distance from v, where $m \leq C\ log(1+||v||)$. We know from Lemma 6 that this can be done by additioning powers of λ_+ and $-\lambda_-$ on

the respective x, y axes until we get to a vector which is at bounded distance from the desired $s \in S_m$. And the number of these powers is, at most, $m \leq C\ log(1 + ||v||)$. So the process is done in time $t_1 \in O\left(log(1 + ||v||)\right)$. We assume that, at each step, the coefficient $\beta_{i,k} \in \{-1, 0, 1\}$ of each power is stored.

We have seen through this prove that these coeficients provide an explicit factorization of $M(Id, s)$ in $\mathrm{SL}_n(\mathbb{Z})$, which has a length upper bounded by $R\ log(1 + ||v||)$.

- Now, as $M(Id, s)$ is at bounded distance from $M(Id, v)$ in the Cayley graph of $\mathcal{H}$, we can build a path from $M(Id, s)$ to $M(Id, v)$ in constant time $t_2 \in O(1)$.

  To sum up, the desired path can be built in time $t = t_1 + t_2 \in O\left(log(1 + ||v||)\right)$, which is better than polynomial time.

□

Now we can finally start to prove that properties **(i), (ii), (iii)** hold for $\mathcal{H}$:

(i) *The membership problem is solvable in polynomial time.*

We recall that the defining equations of $\mathcal{H}$ are:

$$x_{ii} - 1 = 0 \quad \text{for } 1 \leq i \leq n$$

$$x_{ij} = 0 \quad \text{for } i \neq j \text{ and } j \leq n - 1$$

Hence, $n^2 - n - 1$, is the number of conditions to check and therefore the membership problem is solvable in polynomial time. From Proposition 8 we know that this still holds for conjugates. By following the same reasoning in its proof, one can easily check the property for this particular case.

(ii) *There exists a constant $C > 0$ such that, for every $h \in \mathcal{H}$, one can compute in polynomial time a path from the identity to h whose length $m(h)$ is bounded from above by $Cl_S(h)$.*

This follows directly from Proposition 9.

(iii) *$\mathcal{H}$ is exponentially distorted.*

Again from Proposition 9, we get the following inequalities, proving exponential distortion:

$$l_S\left(M(Id, v)\right) \leq C\ log(1 + ||v||) = C\ log\left(1 + \left|\left|\sum_{i=1}^{n-1} m_i e_i\right|\right|\right) \leq$$

$$C\ log\left(1 + \sum_{i=1}^{n-1} m_i\right) = C\ log\left(1 + l_{\mathcal{H}}\left(M(Id, v)\right)\right)$$

This can also be seen through the following result, which is proved in a more general case in [1].

Theorem 1 (Lubotzky, Mozes and Raghunathan)**.** *For $n \geq 3$, an element $g \in SL_n(\mathbb{Z})$ is a U-element if and only if g is virtually unipotent, that is, there exists $k \geq 1$ such that g^k is unipotent.*

With this in hand and the fact that $(M(Id, v) - Id)^n = 0$, we already see that every $h \in \mathcal{H}$ is a U-element. And because $\mathcal{H}$ is abelian, from Proposition 6 it follows that $\mathcal{H}$ is exponentially distorted.

(iv) *The normalizer of $\mathcal{H}$ has infinite index in $SL_n(\mathbb{Z})$.*

To see this we give the following result:

Proposition 10. *The normalizer of $\mathcal{H}$, $N_S(\mathcal{H})$, consists of matrices of the form*

$$\begin{pmatrix} B_{\,n-1\times n-1} & x_{\,n-1\times 1} \\ 0_{\,1\times n-1} & \varepsilon \end{pmatrix}$$

where $B \in GL_{n-1}(\mathbb{Z})$, $\varepsilon = \pm 1$ and $det\ B = \varepsilon$, and it has infinite index in $SL_n(\mathbb{Z})$.

Proof. We pick an arbitrary matrix $A \in \mathrm{SL}_n(\mathbb{Z})$ and we partition it in blocks as follows:

$$A = \begin{pmatrix} B & x \\ y^t & \varepsilon \end{pmatrix}$$

where $B \in \mathrm{GL}_{n-1}(\mathbb{Z})$, $x, y \in \mathbb{Z}^{n-1}$ and $\varepsilon \in \mathbb{Z}$.

Now assume A belongs to the normalizer of $\mathcal{H}$, which holds if, and only if, it commutes with $\mathcal{H}$. That is, for every $v \in \mathbb{Z}^{n-1}$, there is some $v' \in \mathbb{Z}^{n-1}$ such that:

$$\begin{pmatrix} B & x \\ y^t & \varepsilon \end{pmatrix} \begin{pmatrix} Id & v \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} Id & v' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} B & x \\ y^t & \varepsilon \end{pmatrix}$$

Comparing the entries (n, n) of both sides of the equality, we get that $y^t v + \varepsilon = \varepsilon$ for every $v \in \mathbb{Z}^{n-1}$, which implies $y = 0$. From here, as $A \in \mathrm{SL}_n(\mathbb{Z})$, it follows that $\varepsilon\ det\ B = 1$. Since $det\ B \in \mathbb{Z}$, it must be that $\varepsilon = det\ B = \pm 1$. We have proved that if any matrix is in the normalizer, it must satisfy the conditions above. We now need to check that any

matrix of this form belongs to the normalizer. So we pick one if its kind, and for some $v, v' \in \mathbb{Z}^{n-1}$ we compute:

$$\begin{pmatrix} B & x \\ 0 & \varepsilon \end{pmatrix} \begin{pmatrix} Id & v \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} B & Bv + x \\ 0 & \varepsilon \end{pmatrix}$$
$$\begin{pmatrix} Id & v' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} B & x \\ 0 & \varepsilon \end{pmatrix} = \begin{pmatrix} B & x + \varepsilon v' \\ 0 & \varepsilon \end{pmatrix}$$

And now it is clear that for any $v \in \mathbb{Z}^{n-1}$ there will be some $v' \in \mathbb{Z}^{n-1}$ such that the equality between the two expressions holds, which proves the claim.

Now we need to see that the index of this subgroup in $\mathrm{SL}_n(\mathbb{Z})$ is infinite. We pick an arbitrary matrix, again divided in blocks, and we apply to its left side a matrix of the normalizer:

$$\begin{pmatrix} B & x \\ 0 & \varepsilon \end{pmatrix} \in N(\mathcal{H}), \quad \begin{pmatrix} P & v \\ w^t & m \end{pmatrix} \in \mathrm{SL}_n(\mathbb{Z}) \Rightarrow$$
$$\begin{pmatrix} B & x \\ 0 & \varepsilon \end{pmatrix} \begin{pmatrix} P & v \\ w^t & m \end{pmatrix} = \begin{pmatrix} BP & Bv + mx \\ \varepsilon w^t & \varepsilon m \end{pmatrix}$$

This shows that given a matrix in $\mathrm{SL}_n(\mathbb{Z})$, any other matrix in its left-coset must have the same last row multiplied by $\varepsilon = \pm 1$. Hence, for every diferent last row of positive integers there is, at least, one diferent left-coset in $\mathrm{SL}_n(\mathbb{Z})$. It follows that there are infinite left-cosets. □

The protocol, implemented with the pair $(\mathrm{SL}_n(\mathbb{Z}), \mathcal{H})$, would operate as follows. Assume that Alice and Bob have secretly shared a generator set for a conjugate subgroup $g\mathcal{H}g^{-1}$. Also assume that this generator set is gSg^{-1}, where $S = \{M(Ide_i) : 1 \leq i \leq n-1\}$.

- Alice wants to send n to Bob. So she picks a matrix $M(Id, v)$ such that $l_{\mathcal{H}}(M(Id, v)) = \sum_{i=1}^{n-1} |v_i| = n$, she computes $w = gM(Id, v)g^{-1}$, she randomly generates some $a_1, \ldots, a_t \in \mathrm{SL}_n(\mathbb{Z}) \backslash g\mathcal{H}g^{-1}$ and she sends to Bob $\{w, a_1, \ldots, a_t\}$. Notice that the generation of the elements $a_1, \ldots, a_t$ can be done by generating elements in $\mathrm{SL}_n(\mathbb{Z}) \backslash \mathcal{H}$ an then computing the conjugates.

- Bob computes $g^{-1}wg, g^{-1}a_1g, \ldots, g^{-1}a_tg$ and finds which of these elements belongs to $\mathcal{H}$, that is, he finds $g^{-1}wg = M(Id, v) \in \mathcal{H}$. Finally, to recover n, he only needs to sum up the absolute values of the components of v.

Chapter 4

KPA security

In this chapter we take $\mathrm{GL}_n(\mathbb{C})$ as the cryptographic platform and we give a result that shows that in this case the protocol is secure against a known-plaintext attack. That is, we assume that Eve has intercepted several messages, of which she knows both the ciphertext and the plaintext, and we show how difficult it is for her to recover the encryption key. For us, the ciphertext is a matrix in $\mathrm{GL}_n(\mathbb{C})$, the plaintext is the length it has with a fixed generator set, and the key is the generator set. Proposition 13 proves that Eve has an infinity of possible generator sets that could match with the information she has. But, before we state it, we give some tools that will be needed for the proof:

Definition 14. *Let K be a field and $P \subseteq K[x_1, \ldots, x_m]$ a set of polynomials. The affine variety defined by P is the set*

$$\mathcal{V}(P) := \{p \in K^n : f(p) = 0 \quad \forall f \in P\}$$

We call affine variety to any set of this form. When a variety is a subset of another, we also say it is a subvariety.

It is known that affine varieties are closed under finite unions and infinite intersections[1]. This allows to define the so called Zariski topology in K^n, for which the closed sets are all affine varieties in K^n. Note that $\mathcal{V}(\{0\}) = K^n$ and that $\mathcal{V}(\{1\}) = \emptyset$.

Definition 15. *We say that an affine variety X is irreducible if for any pair of closed subvarieties $Y, Z \subseteq X$ such that $X = Y \cup Z$, either $Y = X$ or $Z = X$.*

[1] See reference [9] for more details.

Definition 16. *The dimension of an irreducible affine variety X is k if it admits a finite-to-one dominant map to the projective space $\mathbb{P}^k$. We will denote it as $dim(X)$.*

Proposition 11 ([9])**.** *Any affine variety X may be uniquely expressed as a finite union of irreducible subvarieties X_i with $X_i \nsubseteq X_j$ if $i \neq j$.*

Proposition 12 ([10])**.** *Let X be an irreducible variety of dimension n and let Y be a subvariety in X. Then $dim(Y) \leq dim(X)$ and the equality holds if, and only if, $X = Y$.*

Proposition 13. *Let Γ be a finitely generated subgroup of $GL_n(\mathbb{C})$. Given $\tau_1, \ldots, \tau_n \in \Gamma$ and positive integers $k_1, \ldots, k_n$, suppose that there exists a generating set S for Γ such that $l_S(\tau_i) = k_i$ for all $i \in \{1, \ldots, n\}$. Then there are infinitely many generating set sets S_j for Γ such that:*

(i) $l_{S_j}(\tau_i) = k_i$ *for all* $i \in \{1, \ldots, n\}$ *and for all* $j \in \mathbb{N}$

(ii) The associated metrics to the generating sets S_j are pairwise different.

Proof. We first prove that there are infinitely many generating sets satisfying condition *(i)*. For every $i \in \{1, \ldots, n\}$ we define the sets

$$A_i := \left\{h \in \mathrm{GL}_n(\mathbb{C}) : \ l_{S\cup\{h\}}(\tau_i) < k_i\right\}$$
$$A := \bigcup_{i=1}^{n} A_i$$

So for every $h \in A$, the generating set $S \cup \{h\}$ leads to $l_{S\cup\{h\}}(\tau_i) < k_i$ for some $i \in \{1, \ldots, n\}$, that is, it breaks condition *(i)*. We take its complementary:

$$A^c = \bigcap_{i=1}^{n} A_i^c \ = \ \bigcap_{i=1}^{n} \left\{h \in \mathrm{GL}_n(\mathbb{C}) : \ l_{S\cup\{h\}}(\tau_i) \geq k_i\right\} \quad \text{where} \ \ l_{S\cup\{h\}}(\tau_i) \leq l_S(\tau_i) = k_i,$$

$$\text{so we get} \quad A^c = \bigcap_{i=1}^{n} \left\{h \in \mathrm{GL}_n(\mathbb{C}) : \ l_{S\cup\{h\}}(\tau_i) = k_i\right\}$$

That is, for every $h \in A^c$ the generating set $S \cup \{h\}$ leads to the same lengths for the matrices $\tau_1, \ldots, \tau_n$. So we are interested in proving that Γ has an infinity of elements in A^c, that is, $\Gamma - A$ is infinite.

Let $S = \{s_1, \ldots, s_r\}$ and let $F(x_1, \ldots, x_r, y)$ be the free group generated by the variables $x_1, \ldots, x_r, y$. We denote the length of a word $w \in F(x_1, \ldots, x_r, y)$ as $|w|$. We can express the sets A_i as follows:

$$\text{We define} \ \ A(i, w) := \{h \in \mathrm{GL}_n(\mathbb{C}) : w(s_1, \ldots, s_r, h) = \tau_i\}$$
$$\text{and we have} \ \ A_i = \bigcup_{|w|<k_i} A(i, w).$$

Note that this is a finite union and that the equations $w(s_1, \ldots, s_r, h) = \tau_i$ are polynomial equations in the entries h_{ij} of h, so every $A(i, w)$ is the zero set of a finite set of polynomial equations, that is $A(i, w)$ is a Zariski-closed set. Thus, A_i is also Zariski-closed, and so is $A = \cup_{i=1}^{n} A_i$. Also note that the identity matrix is not a solution of any of the defining equations of A, because, if it was, the equality $w(s_1, \ldots, s_r, Id) = \tau_i$ would give an expression for τ_i in S shorter than k_i. So we have that $Id \notin A(i, w)$ for every $i \in \{1, \ldots, n\}$ and for every $w \in F(x_1, \ldots, x_r, y)$, $|w| < k_i$. So $Id \notin A$.

From Proposition 11, we can express the Zariski-closure of Γ as a finite union of irreducible varieties such that any one is a subvariety of another:

$$\bar{\Gamma} = G_1 \cup \cdots \cup G_r$$

Since Γ is infinite, some G_i is also infinite. We pick $h \in G_i$. It must be that $h^{-1}G_i = G_j$ for some j, because h defines an automorphism of $\mathrm{GL}_n(\mathbb{C})$. It follows that G_j is also infinite and that $Id \in G_j$. WLOG, we assume that $G_j = G_1$.

It suffices to prove that $G_1 - A$ is infinite, because it will follow that $\bar{\Gamma} - A$ is infinite. And this implies that $\Gamma - A$ is infinite, as desired. To prove this last implication, assume that $\Gamma - A = \Gamma \cap A^c$ is finite and consider the induced Zariski topology in A^c. It follows that the Zariski closure of $\Gamma \cap A^c$ in A^c is finite, that is, $\bar{\Gamma} \cap A^c = \bar{\Gamma} - A$ would be finite.

In order to prove that $G_1 - A$ is infinite, we write G_1 as a disjoint union:

$$G_1 = (G_1 - A) \cup (G_1 \cap A)$$

And we have that $G_1 \cap A$ is an affine subvariety in G_1, with G_1 irreducible and infinite. And $Id \in G_1$, but $Id \notin A$. From Proposition 12, it follows that $dim(G_1 \cap A) < dim(G_1)$. So $G_1 - A$ is infinite, as desired.

Now we use this to build an infinite sequence of generating sets that both satisfy *(i)* and *(ii)*. We start with S. We pick $h_1 \in (\Gamma - A) \backslash S$ and we define $S_1 := S \cup \{h_1\}$. By definition S_1 preserves the lengths of $\tau_1, \ldots, \tau_n$. And it also leads to a diferent metric, because, by construction, $l_S(h_1) > 1$ and $l_{S_1}(h_1) = 1$.

Assume we have extended S until some $S_j = S \cup \{h_1, \ldots, h_j\}$, which preserves the desired lengths, and that the generating sets $S, S_1, \ldots, S_j$ lead to pairwise different metrics. Now we build A in the same way, but using S_j instead of S. So we can pick $h_{j+1} \in (\Gamma - A) \backslash S_j$ and set $S_{j+1} := S_j \cup \{h_{j+1}\}$. Because $h_{j+1} \notin S_k$, $k \in \{1, \ldots, j\}$, we have that $l_{S_k}(h_{j+1}) > 1$ for $k \in \{1, \ldots, j\}$ and $l_{S_{j+1}}(h_{j+1}) = 1$, so the metric for S_{j+1} is different from all the preceding. $\square$

Conclusions

We have seen that distortion in arithmetic groups can indeed be useful to build a symetric-key protocol. And we have shown that there exists a particular platform, namely $\mathcal{H}$, where the protocol would be operational. However, we still don't know what other platforms could work. In this direction we mention the work of Riley, *Navigating in the Cayley Graphs of* $SL_N(\mathbb{Z})$ *and* $SL_N(\mathbb{F}_p)$ ([7]), in which we find some results that may be useful to build other exponentially distorted subgroups of $\mathrm{SL}_n(\mathbb{Z})$ and for which the Geodesic Length problem is solvable in polynomial time.

As for the key exchange, we still don't know how Alice and Bob could safely share the key of this protocol (the generating set of the subgroup) through a public channel, while it is well known that there are other cryptosystems, such as elliptic curves cryptosystems or the RSA algorithm, where this can be safely done.

Bibliography

[1] Kahrobaei, D. & Mallahi-Karai, K. *Some aplications of arithmetic groups in cryptography*, The Gruyter, (2019), https://doi.org/10.1515/gcc-2019-2002

[2] Trappe, W. & Washington, L. C. *Introduction to Cryptography with Coding Theory*, Pearson Education, Inc., (2006).

[3] Borel, A. *Introduction aux groupes arithmétiques*, Paris: Hermann, Actualités scientifiques et industrielles, **1341**, (1969), 49-50.

[4] Dicks, W. & Dunwoody, M.J. *Groups acting on graphs*, Cambridge: Cambridge University Press, (1989), 3-5.

[5] Chahal, J.S. *Arithmetic subgroups of the symplectic group*, Osaka: Osaka J. Math **14** (1977), 487-488.

[6] Chatterji, I. & Kahrobaei, D. & Lu, N.Y. *Cryptosystems using subgroup distortion*, Theoretical and Applied Informatics, Vol 29 (2017), no. 1-2, 14-24.

[7] Riley, T.R. *Navigating in the Cayley Graphs of $SL_N(\mathbb{Z})$ and $SL_N(\mathbb{F}_p)$*, Geometriae Dedicata (2005) 113: 215-229, Springer 2005.

[8] Lang, S. *Algebra*, California: Addison-Wesley Publishing Company, Inc., (1984), 20-23.

[9] Harris J. *Algebraic Geometry - A First Course*, 1992 Springer-Verlag New York, Inc. (1992), 17-18, 51-53, 133-135.

[10] Wallach, N.R. *Some Algebraic Geometry*, Department of Mathematics, University of California, San Diego, http://math.ucsd.edu/ nwallach/lectures-ch-1-math207.pdf