J. Korea Soc. Math. Educ. Ser. B: Pure Appl. Math.
Volume 15, Number 3 (August 2008), Pages 229–243

ISSN 1226-0657

REPRESENTATION ALGORITHMS IN SOME FREE GROUPS

SU-JEONG CHOI

ABSTRACT. This paper is intended to clarify and verify two representation algorithms computing representations of elements of free groups generated by two linear fractional transformations. Moreover in practice some parts of the two algorithms are modified for computational efficiency. In particular the justification of the algorithms has been rigorously done by showing how both algorithms work correctly and efficiently according to inputs with some properties of the two linear fractional transformations.

1. INTRODUCTION

Grigoriev and Ponomarenko in 2004 presented two representation algorithms which are used in the decryption scheme of a homomorphic public key cryptosystem [1]. The two representation algorithms compute representations of elements of free groups generated by two linear fractional transformations. However the details related to the algorithms were shortened. So due to their importance in a mathematical viewpoint, through this paper the two representation algorithms are much more clarified and rigorously verified. Further some parts of the two representation algorithms are modified for computational efficiency and termination of the algorithms. Particularly this note focuses on the justification of both algorithms to show how they operate correctly and efficiently according to inputs with some properties of the two linear fractional transformations. It leads to analysis and improvement of both algorithms and especially in connection with combinatorial group theory, the two representation algorithms can play an important role in computing representations of elements of some specific free groups in practice.

2. REPRESENTATION ALGORITHM IN A FREE GROUP Γ_n

Let $n \in \mathbb{N}$ with $n \geq 2$ and Γ_n a group generated by two linear fractional trans-

Received by the editors September 28, 2007.
2000 *Mathematics Subject Classification.* Primary 20C20, 20F05.
Key words and phrases. representation, algorithm, linear fractional transformation, free group.

formations $A_n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ and $B_n = \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix}$. Then Γ_n is a free group [2, pp.168] and put $X_n = \{A_n, B_n\}$. Every element of Γ_n can be represented as a reduced word in ${X_n}^{\pm}$ and it is called the X_n-representation. For a given $M \in \Gamma_n$, the X_n-representation of M is one of the following forms

$$\begin{gathered} {A_n}^{u_1}{B_n}^{u_2}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m} \\ {B_n}^{u_1}{A_n}^{u_2}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m} \\ {A_n}^{u_1}{B_n}^{u_2}\cdots{A_n}^{u_{m-1}}{B_n}^{u_m} \\ {B_n}^{u_1}{A_n}^{u_2}\cdots{A_n}^{u_{m-1}}{B_n}^{u_m} \end{gathered}$$

where u_i is a nonzero integer for $m \in \mathbb{N}$ and $i = 1, 2, \cdots, m$.

If a matrix M is input to the X_n-representation algorithm [1], then it outputs a reduced word in ${X_n}^{\pm}$ as the X_n-representation of M. It is the first stage in the decryption process of the cryptosystem. After the X_n-representation of M is obtained from the X_n-representation algorithm, the second stage of the decryption scheme can go forward. Suppose that n is unknown. Then computation of the X_n-representation in Γ_n becomes one of hard problems involved with the membership problem for Γ_n that security of the cryptosystem replies on. So in the decryption scheme of the cryptosystem, it is assumed that the natural number n with $n \geq 2$ is already set up in the X_n-representation algorithm for computing the X_n-representation of an element of Γ_n.

Let D be a unit open disk in the complex plane $\mathbb{C}$ with the center 0, $D = \{z \in \mathbb{C} \mid |z| < 1\}$ and $D^c = \mathbb{C} - \bar{D} = \{z \in \mathbb{C} \mid |z| > 1\}$ a complement of the closure of D. (z, z') denotes a pair of complex numbers with $|z| < 1$ and $|z'| > 1$. The fact that there is at most one integer u such that $(z \in D^c \wedge {A_n}^u(z) \in D) \vee (z \in D \wedge {B_n}^u(z) \in D^c)$ for $z \in D \cup D^c$ is observed and it induces the following explicit formulae to compute the exponent u of ${A_n}^u$ and ${B_n}^u$. Moreover related with the termination of the algorithm, more concrete cases such as ${B_n}^u(z) = \infty$, $|{B_n}^u(z)| = 1$ and ${A_n}^u(z) = 0$ are considered because it could run infinitely or crash.

Theorem 2.1. *If there exists a nonzero integer u such that $|{A_n}^u(z)| < 1$ for $z \in \mathbb{R}$ and $|z| > 1$, then $u = \lceil -\frac{1+z}{n} \rceil = \lfloor \frac{1-z}{n} \rfloor$.*

Proof. Assume that there is a nonzero integer u such that $|{A_n}^u(z)| = |nu + z| < 1$ for $z \in D^c \cap \mathbb{R}$, namely, $-\frac{1+z}{n} < u < \frac{1-z}{n}$. Since the distance between $-\frac{1+z}{n}$ and $\frac{1-z}{n}$ is $\frac{2}{n}(\leq 1)$, there is at most one integer between them. If one of $-\frac{1+z}{n}$ and $\frac{1-z}{n}$ is an integer, then there is no integer between $-\frac{1+z}{n}$ and $\frac{1-z}{n}$, and this is in contradiction with the assumption. Thus neither $-\frac{1+z}{n}$ nor $\frac{1-z}{n}$ is an integer and so $u = \lceil -\frac{1+z}{n} \rceil = \lfloor \frac{1-z}{n} \rfloor$. □

Theorem 2.2. *If there exists a nonzero integer u such that $|B_n{}^u(z)| > 1$ for $z \in \mathbb{R}$ and $|z| < 1$, then $u = \lceil -\frac{1}{nz} - \frac{1}{n} \rceil = \lfloor -\frac{1}{nz} + \frac{1}{n} \rfloor$.*

Proof. Suppose that there is a nonzero integer u such that $|B_n{}^u(z)| = |\frac{z}{nuz+1}| > 1$ for $z \in D \cap \mathbb{R}$. Then the case of $z = 0$ is clearly excluded as $|B_n{}^u(0)| = 0$. If $z > 0$, then $-\frac{1}{nz} - \frac{1}{n} < u < -\frac{1}{nz} + \frac{1}{n}$. If $z < 0$, then $-\frac{1}{nz} - \frac{1}{n} < u < -\frac{1}{nz} + \frac{1}{n}$. As the distance between $-\frac{1}{nz} - \frac{1}{n}$ and $-\frac{1}{nz} + \frac{1}{n}$ is $\frac{2}{n}(\leq 1)$, there exists at most one integer between $-\frac{1}{nz} - \frac{1}{n}$ and $-\frac{1}{nz} + \frac{1}{n}$. If one of $-\frac{1}{nz} - \frac{1}{n}$ and $-\frac{1}{nz} + \frac{1}{n}$ is an integer, then there is no integer between $-\frac{1}{nz} - \frac{1}{n}$ and $-\frac{1}{nz} + \frac{1}{n}$ and it contradicts the assumption. Hence neither $-\frac{1}{nz} - \frac{1}{n}$ nor $-\frac{1}{nz} + \frac{1}{n}$ is an integer and so $u = \lceil -\frac{1}{nz} - \frac{1}{n} \rceil = \lfloor -\frac{1}{nz} + \frac{1}{n} \rfloor$. □

Modified X_n-representation algorithm. Let $M \in \Gamma_n$ and I the identity matrix. 1_{X_n} denotes the empty word and ϵ does the error message.

```
Step 0
$L \leftarrow M$
$w \leftarrow 1_{X_n}$.
Step 1 (1) $L(z) = 0$, $|L(z)| = 1$, $L(z) = \infty \Rightarrow$ output $\epsilon$.
(2) $|L(z)| > 1 \Rightarrow v \leftarrow \lfloor \frac{1-L(z)}{n} \rfloor$ and $C \leftarrow A_n{}^v$.
(3) $|L(z)| < 1 \Rightarrow v \leftarrow \lfloor -\frac{1}{nL(z)} + \frac{1}{n} \rfloor$ and $C \leftarrow B_n{}^v$.
Step 2
$C = I \Rightarrow$ output $\epsilon$.  Otherwise $L \leftarrow CL$ and $w \leftarrow wC^{-1}$.
Step 3
$L = I \Rightarrow$ output $w$.  Otherwise return Step 1.
```

If the algorithm outputs the X_n-representation of M for $z = \frac{1}{2}$, then it is not necessary to run the algorithm for $z = 2$. If the algorithm outputs ϵ for $z = \frac{1}{2}$ as an error message, then it has to operate for $z = 2$ to obtain the X_n-representation of M. Hence the algorithm outputs either the X_n-representation of M or the error message ϵ, and then it terminates. In the three cases of (1) of Step 1, the algorithm can not work properly and so those of cases end up with the error message ϵ. By Theorem 2.1 and Theorem 2.2 explicit formulae which find exponents of the two linear fractional transformations are added in (2) and (3) of Step 1. The statement of Step 2 that if $C = I$, then it outputs ϵ is also added related to the termination of the algorithm.

From now the algorithm will be justified according to inputs and previously some characteristics of ${A_n}^u$ and ${B_n}^u$ with a nonzero integer u are shown.

Lemma 2.3. *${A_n}^u(z) \in D^c$ for $z \in D$.*

Proof. Let $z = a + bi \in D$. Then ${A_n}^u(z) = (a + nu) + bi$ with $-1 < a < 1$. For $u \geq 1$, $a+nu > -1+nu \geq 1$ and so $a+nu \in D^c$. For $u \leq -1$, $a+nu < 1+nu \leq -1$ and then $a + nu \in D^c$. Hence in either case ${A_n}^u(z) \in D^c$ for $z \in D$. □

Lemma 2.4. *${B_n}^u(z) \in D$ for $z \in D^c$.*

Proof. Let $z = a + bi \in D^c$ and consider ${B_n}^u(z) = \frac{1}{nu+\frac{1}{z}}$. Then $\frac{1}{z} \in D$ and by Lemma 2.3 ${A_n}^u(\frac{1}{z}) = \frac{1}{z} + nu \in D^c$. Hence ${B_n}^u(z) = \frac{1}{nu+\frac{1}{z}} \in D$. □

The following is immediately obtained by Lemma 2.3 and Lemma 2.4.

Theorem 2.5. (1) *${A_n}^{u_1}{B_n}^{u_2}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m} \in D^c$ for $z \in D$.*

(2) *${B_n}^{u_1}{A_n}^{u_2}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m} \in D$ for $z \in D$.*

(3) *${A_n}^{u_1}{B_n}^{u_2}\cdots{A_n}^{u_{m-1}}{B_n}^{u_m} \in D^c$ for $z \in D^c$.*

(4) *${B_n}^{u_1}{A_n}^{u_2}\cdots{A_n}^{u_{m-1}}{B_n}^{u_m} \in D$ for $z \in D^c$.*

Theorem 2.6. *If a matrix $M = {A_n}^{u_1}{B_n}^{u_2}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m}$ with odd $m \geq 3$ is input to the algorithm for $z = \frac{1}{2}$, then it outputs ${A_n}^{u_1}{B_n}^{u_2}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m}$ as the X_n-representation of M.*

Proof. For a matrix $M = {A_n}^{u_1}{B_n}^{u_2}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m} \in \Gamma_n$ (odd $m \geq 3$), in Step 1 of the first iteration, by Theorem 2.5 (1),

$$\left|L\left(\frac{1}{2}\right)\right| = \left|{A_n}^{u_1}{B_n}^{u_2}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m}\left(\frac{1}{2}\right)\right| = |{A_n}^{u_1}(\beta_1)| = |nu_1 + \beta_1| > 1,$$

where $\beta_1 = {B_n}^{u_2}\cdots{B_n}^{u_{m-1}}\ {A_n}^{u_m}(\frac{1}{2})$. By Theorem 2.5 (2), $|\beta_1| < 1$ and so $0 < \frac{1-\beta_1}{n} < \frac{2}{n} \leq 1$. Thus $v = \lfloor\frac{1-L(\frac{1}{2})}{n}\rfloor = -u_1$ and $C = {A_n}^v = {A_n}^{-u_1}$. In Step 2 $L = CL = {B_n}^{u_2}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m} \neq I$ and $w = wC^{-1} = {A_n}^{u_1}$. So return Step 1.

Assume that for $1 < j < m$, in Step 2 of the $j-1$th iteration, $L = CL = {B_n}^{u_j}{A_n}^{u_{j+1}}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m}$ and $w = {A_n}^{u_1}{B_n}^{u_2}\cdots{A_n}^{u_{j-1}}$ with even j or $L = {A_n}^{u_j}{B_n}^{u_{j+1}}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m}$ and $w = {A_n}^{u_1}{B_n}^{u_2}\cdots{B_n}^{u_{j-1}}$ with odd j.

(Case 1) For even j, in Step 1 of the jth iteration, $L(\frac{1}{2}) = {B_n}^{u_j}(\alpha_j) = \frac{1}{nu_j+\frac{1}{\alpha_j}}$ where $\alpha_j = {A_n}^{u_{j+1}}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m}(\frac{1}{2})$ and by Theorem 2.5 (2), $|L(\frac{1}{2})| = |{B_n}^{u_j}(\alpha_j)| < 1$. By Theorem 2.5 (1), $|\alpha_j| > 1$ and so $0 < \frac{1}{n}(1-\frac{1}{\alpha_j}) < \frac{2}{n} \leq 1$. Thus $v = \lfloor\frac{-1}{nL(\frac{1}{2})}+\frac{1}{n}\rfloor = -u_j$ and $C = {B_n}^v = {B_n}^{-u_j}$. In Step 2 $L = CL = {A_n}^{u_{j+1}}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m} \neq I$ and $w = wC^{-1} = {A_n}^{u_1}{B_n}^{u_2}\cdots{A_n}^{u_{j-1}}{B_n}^{u_j}$. So return Step 1.

(Case 2) For odd j, in Step 1 of the jth iteration, by Theorem 2.5 (1),

$$\left|L\left(\frac{1}{2}\right)\right| = \left|A_n{}^{u_j}B_n{}^{u_{j+1}}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m}\left(\frac{1}{2}\right)\right| = |A_n{}^{u_j}(\beta_j)| = |nu_j + \beta_j| > 1$$

where $\beta_j = B_n{}^{u_{j+1}}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m}(\frac{1}{2})$. By Theorem 2.5 (2), $|\beta_j| < 1$ and so

$$0 < \frac{1-\beta_j}{n} < \frac{2}{n} \leq 1.$$

Thus $v = \lfloor\frac{1-L(\frac{1}{2})}{n}\rfloor = -u_j$ and $C = A_n{}^v = A_n{}^{-u_j}$. In Step 2 $L = CL = B_n{}^{u_{j+1}}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m} \neq I$ and $w = wC^{-1} = A_n{}^{u_1}B_n{}^{u_2}\cdots B_n{}^{u_{j-1}}A_n{}^{u_j}$. So return Step 1.

If $j = m$, then in Step 1 of the mth iteration, $L = A_n{}^{u_m}$ and by Lemma 2.3

$$\left|L\left(\frac{1}{2}\right)\right| = \left|A_n{}^{u_m}\left(\frac{1}{2}\right)\right| = \left|nu_m + \frac{1}{2}\right| > 1, v = \lfloor\frac{1-L(\frac{1}{2})}{n}\rfloor = -u_m$$

and $C = A_n{}^v = A_n{}^{-u_m}$. In Step 2 $L = CL = A_n{}^{-u_m}A_n{}^{u_m} = I$ and $w = wC^{-1} = A_n{}^{u_1}B_n{}^{u_2}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m}$. Therefore it outputs $A_n{}^{u_1}B_n{}^{u_2}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m}$ as the X_n-representation of M and it terminates. □

Theorem 2.7. *If a matrix $M = A_n{}^{u_1}B_n{}^{u_2}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m}$ with odd $m \geq 3$ is input to the algorithm for $z = 2$, then it outputs ϵ.*

Proof. For a matrix $M = A_n{}^{u_1}B_n{}^{u_2}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m} \in \Gamma_n$ (odd $m \geq 3$), in Step 1 of the first iteration,

$$L(2) = A_n{}^{u_1}B_n{}^{u_2}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m}(2) = A_n{}^{u_1}(\beta_1) = nu_1 + \beta_1,$$

where $\beta_1 = B_n{}^{u_2}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m}(2)$.

(i) If $n = 2$ and $u_m = -1$, then $A_n{}^{u_m}(2) = nu_m + 2 = 0$, $B_n{}^{u_{m-1}}(0) = 0$ and $A_n{}^{u_{m-2}}(0) = nu_{m-2} \in D^c$. By Theorem 2.5 (1), $|L(2)| = |A_n{}^{u_1}B_n{}^{u_2}\cdots A_n{}^{u_{m-2}}(0)| > 1$ and by Theorem 2.5 (2), $|\beta_1| = |B_n{}^{u_2}\cdots A_n{}^{u_{m-2}}(0)| < 1$.

(ii) If $n = 3$ and $u_m = -1$, then $A_n{}^{u_m}(2) = nu_m + 2 = -1$ and $B_n{}^{u_{m-1}}(-1) = \frac{-1}{-nu_{m-1}+1} \in D$. Put $\gamma = B_n{}^{u_{m-1}}A_n{}^{u_m}(2)$ and then $|\gamma| < 1$. By Theorem 2.5 (1), $|L(2)| = |A_n{}^{u_1}B_n{}^{u_2}\cdots A_n{}^{u_{m-2}}(\gamma)| > 1$ and by Theorem 2.5 (2), $|\beta_1| = |B_n{}^{u_2}\cdots A_n{}^{u_{m-2}}(\gamma)| < 1$.

(iii) If neither $n = 2$ and $u_m = -1$ nor $n = 3$ and $u_m = -1$, then $A_n{}^{u_m}(2) = nu_m + 2 \in D^c$. By Theorem 2.5 (3), $|L(2)| = |A_n{}^{u_1}B_n{}^{u_2}\cdots B_n{}^{u_{m-1}}(nu_m + 2)| > 1$ and by Theorem 2.5 (4), $|\beta_1| = |B_n{}^{u_2}A_n{}^{u_3}\cdots B_n{}^{u_{m-1}}(nu_m + 2)| < 1$.

In all cases (i), (ii) and (iii), $|L(2)| > 1$ and $|\beta_1| < 1$, so that $0 < \frac{1-\beta_1}{n} < \frac{2}{n} \leq 1$, $v = \lfloor\frac{1-L(2)}{n}\rfloor = -u_1$ and $C = A_n{}^v = A_n{}^{-u_1}$. In Step 2 of the first iteration, $L = CL = B_n{}^{u_2}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m} \neq I$ and $w = wC^{-1} = A_n{}^{u_1}$. So return Step 1.

Suppose that in Step 2 of the $j-1$th iteration, for $1 < j < m-1$, $L = {B_n}^{u_j}{A_n}^{u_{j+1}} \cdots {B_n}^{u_{m-1}}{A_n}^{u_m}$ and $w = {A_n}^{u_1}{B_n}^{u_2} \cdots {A_n}^{u_{j-1}}$ with even j or $L = {A_n}^{u_j}{B_n}^{u_{j+1}} \cdots {B_n}^{u_{m-1}}{A_n}^{u_m}$ and $w = {A_n}^{u_1}{B_n}^{u_2} \cdots {B_n}^{u_{j-1}}$ with odd j.

(Case 1) For even j, in Step 1 of the jth iteration, $L(2) = {B_n}^{u_j}(\alpha_j) = \frac{\alpha_j}{\alpha_j n u_j + 1}$ where $\alpha_j = {A_n}^{u_{j+1}}{B_n}^{u_{j+2}} \cdots {B_n}^{u_{m-1}}{A_n}^{u_m}(2)$.

(i) If $n = 2$ and $u_m = -1$, then ${A_n}^{u_m}(2) = nu_m + 2 = 0$, ${B_n}^{u_{m-1}}(0) = 0$ and ${A_n}^{u_{m-2}}(0) = nu_{m-2} \in D^c$. By Theorem 2.5 (2), $|L(2)| = |{B_n}^{u_j}{A_n}^{u_{j+1}} \cdots {A_n}^{u_{m-2}}(0)| < 1$ and by Theorem 2.5 (1), $|\alpha_j| = |{A_n}^{u_{j+1}}{B_n}^{u_{j+2}} \cdots {A_n}^{u_{m-2}}(0)| > 1$.

(ii) If $n = 3$ and $u_m = -1$, then ${A_n}^{u_m}(2) = nu_m + 2 = -1$ and ${B_n}^{u_{m-1}}(-1) = \frac{-1}{-nu_{m-1}+1} \in D$. Put $\gamma = {B_n}^{u_{m-1}}{A_n}^{u_m}(2)$ and then $|\gamma| < 1$. By Theorem 2.5 (2), $|L(2)| = |{B_n}^{u_j}{A_n}^{u_{j+1}} \cdots {A_n}^{u_{m-2}}(\gamma)| < 1$ and by Theorem 2.5 (1), $|\alpha_j| = |{A_n}^{u_{j+1}}{B_n}^{u_{j+2}} \cdots {A_n}^{u_{m-2}}(\gamma)| > 1$.

(iii) If neither $n = 2$ and $u_m = -1$ nor $n = 3$ and $u_m = -1$, then ${A_n}^{u_m}(2) = nu_m + 2 \in D^c$. By Theorem 2.5 (4), $|L(2)| = |{B_n}^{u_j}{A_n}^{u_{j+1}} \cdots {B_n}^{u_{m-1}}(nu_m + 2)| < 1$ and by Theorem 2.5 (3), $|\alpha_j| = |{A_n}^{u_{j+1}} \cdots {B_n}^{u_{m-1}}(nu_m + 2)| > 1$.

In all cases (i), (ii) and (iii), $-1 < \frac{1}{\alpha_j} < 1$ and $0 < \frac{1}{n}(1 - \frac{1}{\alpha_j}) < \frac{2}{n} \leq 1$, so that $v = \lfloor \frac{-1}{nL(2)} + \frac{1}{n} \rfloor = -u_j$ and $C = {B_n}^v = {B_n}^{-u_j}$. In Step 2 of the jth iteration, $L = CL = {A_n}^{u_{j+1}} \cdots {B_n}^{u_{m-1}}{A_n}^{u_m} \neq I$ and $w = wC^{-1} = {A_n}^{u_1}{B_n}^{u_2} \cdots {A_n}^{u_{j-1}}{B_n}^{u_j}$. So return Step 1.

(Case 2) For odd j, in Step 1 of the jth iteration, $L(2) = {A_n}^{u_j}(\beta_j) = nu_j + \beta_j$ where $\beta_j = {B_n}^{u_{j+1}} \cdots {B_n}^{u_{m-1}}{A_n}^{u_m}(2)$.

(i) If $n = 2$ and $u_m = -1$, then ${A_n}^{u_m}(2) = nu_m + 2 = 0$, ${B_n}^{u_{m-1}}(0) = 0$ and ${A_n}^{u_{m-2}}(0) = nu_{m-2} \in D^c$. By Theorem 2.5 (1), $|L(2)| = |{A_n}^{u_j}{B_n}^{u_{j+1}} \cdots {B_n}^{u_{m-3}} {A_n}^{u_{m-2}}(0)| > 1$ and by Theorem 2.5 (2), $|\beta_j| = |{B_n}^{u_{j+1}} \cdots {A_n}^{u_{m-2}}(0)| < 1$.

(ii) If $n = 3$ and $u_m = -1$, then ${A_n}^{u_m}(2) = nu_m + 2 = -1$, ${B_n}^{u_{m-1}}(-1) = \frac{-1}{-nu_{m-1}+1} \in D$. Put $\gamma = {B_n}^{u_{m-1}}{A_n}^{u_m}(2)$ and then $|\gamma| < 1$. By Theorem 2.5 (1), $|L(2)| = |{A_n}^{u_1}{B_n}^{u_2} \cdots {A_n}^{u_{m-2}}(\gamma)| > 1$ and by Theorem 2.5 (2), $|\beta_j| = |{B_n}^{u_{j+1}} \cdots {A_n}^{u_{m-2}}(\gamma)| < 1$.

(iii) If neither $n = 2$ and $u_m = -1$ nor $n = 3$ and $u_m = -1$, then ${A_n}^{u_m}(2) = nu_m + 2 \in D^c$. By Theorem 2.5 (3), $|L(2)| = |{A_n}^{u_j}{B_n}^{u_{j+1}} \cdots {B_n}^{u_{m-1}}(nu_m + 2)| > 1$ and by Theorem 2.5 (4), $|\beta_j| = |{B_n}^{u_{j+1}} \cdots {B_n}^{u_{m-1}}(nu_m + 2)| < 1$.

In all cases (i), (ii) and (iii), $|L(2)| > 1$ and $|\beta_j| < 1$. Since $-1 < \beta_j < 1$ and $0 < \frac{1-\beta_j}{n} < \frac{2}{n} \leq 1$, $v = \lfloor \frac{1-L(2)}{n} \rfloor = -u_j$ and $C = {A_n}^{-u_j}$. In Step 2 of the jth iteration,

$L = CL = B_n{}^{u_{j+1}} \cdots B_n{}^{u_{m-1}} A_n{}^{u_m} \neq I$ and $w = wC^{-1} = A_n{}^{u_1} B_n{}^{u_2} \cdots B_n{}^{u_{j-1}} A_n{}^{u_j}$. So return Step 1.

If $j = m-1$, then in Step 1 of the $m-1$th iteration, let $L = B_n{}^{u_{m-1}} A_n{}^{u_m}$.

(i) If $n = 2$ and $u_m = -1$, then $A_n{}^{u_m}(2) = nu_m + 2 = 0$, $B_n{}^{u_{m-1}}(0) = 0$ and $L(2) = B_n{}^{u_{m-1}} A_n{}^{u_m}(2) = 0$. Hence it outputs ϵ and then terminates.

(ii) If $n = 3$ and $u_m = -1$, then

$$A_n{}^{u_m}(2) = nu_m + 2 = -1,\ B_n{}^{u_{m-1}}(-1) = \frac{-1}{-nu_{m-1}+1} \in D$$

and $|L(2)| = |B_n{}^{u_{m-1}} A_n{}^{u_m}(2)| < 1$. Hence $v = \lfloor \frac{-1}{nL(2)} + \frac{1}{n} \rfloor = -u_{m-1}$ and $C = B_n{}^v = B_n{}^{-u_{m-1}}$. In Step 2 of the $m-1$th iteration, $L = CL = A_n{}^{u_m} \neq I$ and $w = wC^{-1} = A_n{}^{u_1} B_n{}^{u_2} \cdots A_n{}^{u_{m-2}} B_n{}^{u_{m-1}}$. So return Step 1.

(iii) If neither $n = 2$ and $u_m = -1$ nor $n = 3$ and $u_m = -1$, then

$$A_n{}^{u_m}(2) = nu_m + 2 \in D^c$$

and by Lemma 2.4 $B_n{}^{u_{m-1}}(nu_m + 2) \in D$. Thus

$$|L(2)| = |B_n{}^{u_{m-1}} A_n{}^{u_m}(2)| < 1$$

and so

$$0 < \frac{1}{n}\left(1 - \frac{1}{nu_m + 2}\right) < \frac{2}{n} \leq 1.$$

Hence $v = \lfloor \frac{-1}{nL(2)} + \frac{1}{n} \rfloor = -u_{m-1}$ and $C = B_n{}^v = B_n{}^{-u_{m-1}}$. In Step 2 of the $m-1$th iteration, $L = CL = A_n{}^{u_m} \neq I$ and $w = A_n{}^{u_1} B_n{}^{u_2} \cdots A_n{}^{u_{m-2}} A_n{}^{u_{m-1}}$. So return Step 1.

If $j = m$, then in Step 1 of the $j = m$th iteration, $L = A_n{}^{u_m}$ and $L(2) = A_n{}^{u_m}(2) = nu_m + 2$.

(i) If $n = 2$ and $u_m = -1$, then in the $m-1$th iteration, the algorithm outputs ϵ and it terminates. So this case is not included.

(ii) If $n = 3$ and $u_m = -1$, then as $|L(2)| = 1$, it outputs ϵ and terminates.

(iii) Otherwise $|L(2)| = |A_n{}^{u_m}(2)| = |nu_m + 2| > 1$, so that $v = \lfloor \frac{1-L(2)}{n} \rfloor = -u_m - 1$ and $C = A_n{}^v = A_n{}^{-u_m-1}$. In Step 2 of the mth iteration, $L = CL = A_n{}^{-1} \neq I$ and $w = wC^{-1} = A_n{}^{u_1} B_n{}^{u_2} \cdots B_n{}^{u_{m-1}} A_n{}^{u_m+1}$. So return Step 1.

If $j = m+1$, then in Step 1 of the $m+1$th iteration, $L(2) = A_n{}^{-1}(2) = -n+2$.

(i) If $n = 2$, then then as $|L(2)| = 0$, it outputs ϵ and terminates.

(ii) If $n = 3$, then then as $|L(2)| = 1$, it outputs ϵ and terminates.

(iii) If $n \geq 4$, then $|L(2)| > 1$ and so $v = \lfloor \frac{1-L(2)}{n} \rfloor = 0$. In Step 2 of the $m+1$th iteration, $C = A_n{}^v = I$. So it outputs ϵ and terminates. □

For the sake of avoiding tiresome similarity in proofs of correctness of the algorithm, the rest of cases in which the algorithm operates are just stated as follows.

Theorem 2.8. (1) *If a matrix $M = {B_n}^{u_1}{A_n}^{u_2}\cdots {B_n}^{u_{m-1}}{A_n}^{u_m}$ with even $m \geq 2$ is input to the algorithm for $z = \frac{1}{2}$, then it outputs ${B_n}^{u_1}{A_n}^{u_2}\cdots {B_n}^{u_{m-1}}{A_n}^{u_m}$ as the X_n-representation of M.*
(2) *If a matrix $M = {B_n}^{u_1}{A_n}^{u_2}\cdots {B_n}^{u_{m-1}}{A_n}^{u_m}$ with even $m \geq 2$ is input to the algorithm for $z = 2$, then it outputs ϵ.*
(3) *If a matrix $M = {A_n}^{u_1}{B_n}^{u_2}\cdots {A_n}^{u_{m-1}}{B_n}^{u_m}$ with even $m \geq 2$ is input to the algorithm for $z = \frac{1}{2}$, then it outputs ϵ.*
(4) *If a matrix $M = {A_n}^{u_1}{B_n}^{u_2}\cdots {A_n}^{u_{m-1}}{B_n}^{u_m}$ with even $m \geq 2$ is input to the algorithm for $z = 2$, then it outputs ${A_n}^{u_1}{B_n}^{u_2}\cdots {A_n}^{u_{m-1}}{B_n}^{u_m}$ as the X_n-representation of M.*
(5) *If a matrix $M = {B_n}^{u_1}{A_n}^{u_2}\cdots {A_n}^{u_{m-1}}{B_n}^{u_m}$ with odd $m \geq 3$ is input to the algorithm for $z = \frac{1}{2}$, then it outputs ϵ.*
(6) *If a matrix $M = {B_n}^{u_1}{A_n}^{u_2}\cdots {A_n}^{u_{m-1}}{B_n}^{u_m}$ with odd $m \geq 3$ is input to the algorithm for $z = 2$, then it outputs ${B_n}^{u_1}{A_n}^{u_2}\cdots {A_n}^{u_{m-1}}{B_n}^{u_m}$ as the X_n-representation of M.*

3. REPRESENTATION ALGORITHM IN A FREE GROUP $G(n, S)$

Let S be a finite set of randomly chosen integers $s_1, s_2, \cdots, s_t$ and define each word by ${A_n}^{-s_i}B_n{A_n}^{s_i}$ with $s_i \in S$. Put $X(n,S) = \{{A_n}^{-s_i}B_n{A_n}^{s_i} \mid s_i \in S\}$ and let $G(n,S)$ be a group generated by $X(n,S)$. First it will be proved that $X(n,S)$ is a free basis of $G(n,S)$ and every element of $G(n,S)$ can be represented by elements of $X(n,S)^{\pm}$ and it is called the $X(n,S)$-representation. Let F be a free group with a generating set X and $U = \{u_i \mid i \in \mathbb{N}\}$ a subset of a free group F. Elementary Nielsen transformation on a set $U = \{u_i \mid i \in \mathbb{N}\}$ is introduced by [2]

- replace some u_i by ${u_i}^{-1}$
- replace some u_i by u_iu_j where $j \neq i$.
- delete some u_i where $u_i = 1$

where 1 denotes the empty word. A product of such elementary transformations is called Nielsen transformation. If all triples $v_1, v_2, v_3 \in U^{\pm}$ satisfy the following conditions [2]

- $v_1 \neq 1$
- $v_1v_2 \neq 1$ implies $|v_1v_2| \geq |v_1|, |v_2|$.

- $v_1v_2 \neq 1$ and $v_2v_3 \neq 1$ implies $|v_1v_2v_3| > |v_1| - |v_2| + |v_3|$,

then U is called Nielsen reduced. The Nielsen reduced set plays an important role as it is a free generating set for the subgroup that it generates. Now it will be shown that $X(n, S)$ satisfies the three conditions to be Nielsen reduced.

Theorem 3.1. *$X(n, S)$ is Nielsen reduced where $n \geq 2$ and $S \subset \mathbb{Z}$ with $|S| = t$.*

Proof. Let $v_1 = {A_n}^{-s}{B_n}^{\alpha}{A_n}^{s}$, $v_2 = {A_n}^{-t}{B_n}^{\beta}{A_n}^{t}$ and

$$v_3 = {A_n}^{-u}{B_n}^{\gamma}{A_n}^{u} \in X(n, S)^{\pm}$$

where α, β, $\gamma \in \{1, -1\}$ and s, t, $u \in S$.
1. For $v_1 = {A_n}^{-s}{B_n}^{\alpha}{A_n}^{s}$, if $s = 0$, then $v_1 = {B_n}^{\alpha} \neq 1$ and if $s \neq 0$, then

$$|v_1| = |{A_n}^{-s}{B_n}^{\alpha}{A_n}^{s}| = 2|s| + 1 \neq 0$$

and so $v_1 \neq 1$.
2. For $v_1 = {A_n}^{-s}{B_n}^{\alpha}{A_n}^{s}$ and

$$v_2 = {A_n}^{-t}{B_n}^{\beta}{A_n}^{t},\ v_1v_2 = {A_n}^{-s}{B_n}^{\alpha}{A_n}^{s-t}{B_n}^{\beta}{A_n}^{t}.$$

(i) If $s = t$ and $\alpha = \beta$, then $|v_1v_2| = |{A_n}^{-s}{B_n}^{\alpha+\beta}{A_n}^{t}| = 2|s| + 2$ and thus $v_1v_2 \neq 1$. As $|v_1| = 2|s| + 1$ and

$$|v_2| = 2|t| + 1,\ |v_1v_2| \geq |v_1|, |v_2|.$$

(ii) If $s = t$ and $\alpha \neq \beta$, then $v_1v_2 = {A_n}^{-s}{B_n}^{\alpha}{A_n}^{s-t}{B_n}^{\beta}{A_n}^{t} = I$ and so $v_1v_2 = 1$. Hence, this case is excluded.
(iii) If $s \neq t$ and $\alpha = \pm\beta$, then $v_1v_2 = {A_n}^{-s}{B_n}^{\alpha}{A_n}^{s-t}{B_n}^{\beta}{A_n}^{t}$, by the triangle inequality

$$|v_1v_2| = |s| + |t| + |s - t| + 2 \geq 2|s| + 2$$

and

$$|v_1v_2| = |t| + |s| + |t - s| + 2 \geq 2|t| + 2.$$

As $|v_1| = 2|s| + 1$ and $|v_2| = 2|t| + 1$, $|v_1v_2| \geq |v_1|, |v_2|$.
3. For $v_1 = {A_n}^{-s}{B_n}^{\alpha}{A_n}^{s}$, $v_2 = {A_n}^{-t}{B_n}^{\beta}{A_n}^{t}$ and

$$v_3 = {A_n}^{-u}{B_n}^{\gamma}{A_n}^{u},\ v_1v_2v_3 = {A_n}^{-s}{B_n}^{\alpha}{A_n}^{s-t}{B_n}^{\beta}{A_n}^{t-u}{B_n}^{\gamma}{A_n}^{u}.$$

(i) If $s = t$, $\alpha = \beta$, $t = u$ and $\beta = \gamma$, then

$$|v_1v_2v_3| = |{A_n}^{-s}{B_n}^{\alpha+\beta+\gamma}{A_n}^{u}| = 2|s| + 3$$

and $|v_1| - |v_2| + |v_3| = 2|s| + 1$. Hence

$$|v_1v_2v_3| > |v_1| - |v_2| + |v_3|.$$

(ii) If $s = t$, $\alpha = \beta$, $t \neq u$ and $\beta = \pm\gamma$, then by the triangle inequality

$$\begin{aligned}|v_1v_2v_3| &= |{A_n}^{-s}{B_n}^{\alpha+\beta}{A_n}^{t-u}{B_n}^{\gamma}{A_n}^{u}| \\ &= |s| + 2 + |t-u| + 1 + |u| \\ &= |s| + 2 + |s-u| + 1 + |u| \\ &= |s| + 2 + |u-s| + 1 + |u| \geq 2|u| + 3\end{aligned}$$

and

$$|v_1| - |v_2| + |v_3| = 2|s| + 1 - 2|t| - 1 + 2|u| + 1 = 2|u| + 1.$$

Thus

$$|v_1v_2v_3| > |v_1| - |v_2| + |v_3|.$$

(iii) If $s \neq t$, $\alpha = \pm\beta$, $t = u$ and $\beta = \gamma$, then by the triangle inequality

$$\begin{aligned}|v_1v_2v_3| &= |{A_n}^{-s}{B_n}^{\alpha}{A_n}^{s-t}{B_n}^{\beta+\gamma}{A_n}^{u}| \\ &= |s| + 1 + |s-t| + 2 + |u| \\ &= |s| + 1 + |s-u| + 2 + |u| \\ &\geq 2|s| + 3\end{aligned}$$

and

$$|v_1| - |v_2| + |v_3| = 2|s| + 1 - 2|t| - 1 + 2|u| + 1 = 2|s| + 1.$$

Hence

$$|v_1v_2v_3| > |v_1| - |v_2| + |v_3|.$$

(iv) If $s \neq t$, $\alpha = \pm\beta$, $t \neq u$ and $\beta = \pm\gamma$, then

$$\begin{aligned}|v_1v_2v_3| &= |{A_n}^{-s}{B_n}^{\alpha}{A_n}^{s-t}{B_n}^{\beta}{A_n}^{t-u}{B_n}^{\gamma}{A_n}^{u}| \\ &= |s| + 1 + |s-t| + 1 + |t-u| + 1 + |u| \\ &= |s| + |s-t| + |t-u| + |u| + 3 \\ &\geq 2|s| - 2|t| + 2|u| + 3\end{aligned}$$

and

$$|v_1| - |v_2| + |v_3| = 2|s| - 2|t| + 2|u| + 1.$$

Thus

$$|v_1v_2v_3| > |v_1| - |v_2| + |v_3|.$$

□

Theorem 3.2 ([2]). *If F is a free group with a basis X and a subset Y of F is Nielsen reduced and $w = y_1 \cdots y_m$, $(m \geq 0)$, $y_i \in Y^{\pm}$ and all $y_i y_{i+1} \neq 1$, then $|w| \geq m$.*

Theorem 3.3 ([2]). *Let X be a subset of a group G such that $X \cap X^{-1} \neq \emptyset$. Then X is a basis for a free subgroup of G if and only if no product $w = x_1 \cdots x_n$ is trivial, where $n \geq 1$, $M_i \in X^{\pm}$, and all $x_i x_{i+1} \neq 1$.*

Theorem 3.4. *$X(n, S)$ is a free basis of $G(n, S)$ where $n \geq 2$ and $S \subset \mathbb{Z}$ with $|S| = t$.*

Proof. By Theorem 3.1 $X(n, S)$ is Nielsen reduced and the set Y in Theorem 3.2 is replaced by $X(n, S)$. So it satisfies $|w| \geq m$ where $w = w_1 w_2 \cdots w_m$ with $m \geq 0$, $w_i \in X(n, S)^{\pm}$ and all $w_i w_{i+1} \neq 1$ and by Theorem 3.3 $X(n, S)$ is a free basis of $G(n, S)$. □

Since the free group $G(n, S)$ is a subgroup of Γ_n, every element of $G(n, S)$ also has the X_n-representation. As it is mentioned, in the decryption scheme of the cryptosystem, the $X(n, S)$-representation algorithm is required after the X_n-representation of an element of $G(n, S)$ is taken from the X_n-representation algorithm.

Assume that given $M \in G(n, S)$,

$$A_n{}^{u_1} B_n{}^{u_2} A_n{}^{u_3} B_n{}^{u_4} \cdots A_n{}^{u_{m-2}} B_n{}^{u_{m-1}} A_n{}^{u_m}$$

is the X_n-representation of M with odd $m \geq 3$ and it is input to the $X(n, S)$-representation algorithm. Then it outputs

$$A_n{}^{-s_{a_1}} B_n{}^{u_2} A_n{}^{s_{a_1}} A_n{}^{-s_{a_2}} B_n{}^{u_4} A_n{}^{-s_{a_2}} \cdots A_n{}^{s_{a_{\frac{m-3}{2}}}} A_n{}^{-s_{a_{\frac{m-1}{2}}}} B_n{}^{u_{m-1}} A_n{}^{s_{a_{\frac{m-1}{2}}}}$$

as the $X(n, S)$-representation of M where for $i = 1, \cdots \frac{m-1}{2}$,

$a_i \in \{1, \cdots, t\}$, $s_{a_i} \in S$, $-u_1 = s_{a_1}$, $u_{2i-1} = s_{a_{i-1}} - s_{a_i}$ $(i \geq 2)$, $s_{a_{i-1}} \neq s_{a_i}$ $(i \geq 2)$ and $u_m = s_{a_{\frac{m-1}{2}}}$. Hence the X_n-representation of M can also be written as

$$A_n{}^{u_1} B_n{}^{u_2} A_n{}^{-u_1} A_n{}^{u_1+u_3} B_n{}^{u_4} \cdots A_n{}^{\sum_{i=1}^{\frac{m-1}{2}} u_{2i-1}} B_n{}^{u_{m-1}} A_n{}^{-\sum_{i=1}^{\frac{m-1}{2}} u_{2i-1}} A_n{}^{\sum_{i=1}^{\frac{m+1}{2}} u_{2i-1}}$$

where the exponent of the last term A_n is

$$u_m = -(u_1 + u_3 + u_5 + u_7 + \cdots + u_{2i-1} + \cdots + u_{m-2}).$$

Compare the exponents of the X_n-representation of M with those of the $X(n. S)$-representation of M and then it finds an explicit formula

$$s_{a_i} = -(u_1 + u_3 + u_5 + \cdots + u_{2i-1})$$

to compute elements of S. So the original algorithm will be changed by adding the formula for computational efficiency in reality. Let us consider likely inputs of the $X(n, S)$-representation algorithm [1] and those of types can be replaced by the right forms in the following.

(i) ${B_n}^{v_1}{A_n}^{v_2}\cdots{B_n}^{v_{p-1}}{A_n}^{v_p}$ (even p) $\Rightarrow$ ${A_n}^{u_1}{B_n}^{u_2}{A_n}^{u_3}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m}$ $(u_1 = 0,$ $m = p+1,\ i = 2, 3, \cdots, m,\ u_i = v_{i-1})$

(ii) ${A_n}^{v_1}{B_n}^{v_2}\cdots{A_n}^{v_{p-1}}{B_n}^{v_p}$ (even p) $\Rightarrow$ ${A_n}^{u_1}{B_n}^{u_2}{A_n}^{u_3}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m}$ $(i = 1, 2,$ $\cdots, p,\ u_i = v_i,\ m = p+1,\ u_m = 0)$

(iii) ${B_n}^{v_1}{A_n}^{v_2}\cdots{A_n}^{v_{p-1}}{B_n}^{v_p}$ (odd p) $\Rightarrow$ ${A_n}^{u_1}{B_n}^{u_2}\cdots{B_n}^{u_{m-1}}{A_n}^{m}$ $(u_1 = 0,\ i = 2,$ $\cdots, p+2,\ u_i = v_{i-1},\ m = p+2,\ u_m = 0)$

The modified algorithm takes only one form of the X_n-representations, namely, ${A_n}^{u_1}{B_n}^{u_2}{A_n}^{u_3}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m}$ as the input unlike the original algorithm. Motivation of such a change comes from the constant form of elements of $X(n, S)$, i.e., ${A_n}^{-s}B_n{A_n}^{s}$ with $s \in S$. Additionally the modified algorithm stops with either the $X(n, S)$-representation or the error message ϵ. Next the modified algorithm will be shown and its verification will be followed.

Modified $X(n, S)$-representation algorithm.

```
Step 0
$i \leftarrow 1$.
$w \leftarrow {A_n}^{u_1}{B_n}^{u_2}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m}$
$w = 1_{X_n} \Rightarrow$ output $1_{X(n,S)}$.
Step 1
$e_i \leftarrow -(u_1 + u_3 + u_5 + \cdots + u_{2i-1})$
$e_i \notin S \Rightarrow$ output $\epsilon$.
$e_i \in S \Rightarrow C_i \leftarrow {A_n}^{-e_i}{B_n}^{u_{2i}}{A_n}^{e_i}$.
Step 2
$w \leftarrow {C_i}^{-1}w$
$w = 1_{X_n} \Rightarrow$ output $C_1C_2\cdots C_i$.
Otherwise,
$i \leftarrow i + 1$
$i = \frac{m+1}{2} \Rightarrow$ output $\epsilon$ and return Step 1.
```

Theorem 3.5. *Given $M \in \Gamma_n$, let ${A_n}^{u_1}{B_n}^{u_2}\cdots{B_n}^{u_{m-1}}{A_n}^{u_m}$ be the X_n-representation of M as the input of the algorithm with nonzero integers $u_2, u_3, \cdots, u_{m-1}$. Then it outputs*

$$A_n{}^{u_1}B_n{}^{u_2}A_n{}^{-u_1}A_n{}^{u_1+u_3}B_n{}^{u_4}A_n{}^{-(u_1+u_3)}\cdots A_n{}^{u_1+u_3+u_5+\cdots+u_{m-2}}B_n{}^{u_{m-1}}$$
$$\cdot A_n{}^{-(u_1+u_3+u_5+\cdots+u_{m-2})}$$

as the $X(n,S)$-representation of M. Otherwise, it outputs ϵ.

Proof. If the X_n-representation $A_n{}^{u_1}B_n{}^{u_2}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m}$ of M is input to the algorithm with each nonzero integer u_i ($i = 2,3,\cdots,m-1$), then in Step 0 of the first iteration $i = 1$,

$$w = A_n{}^{u_1}B_n{}^{u_2}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m}.$$

In Step 1 of the first iteration, $e_1 = -u_1$. If $e_1 \notin S$, then it outputs ϵ and terminates. If $e_1 = -u_1 \in S$, then

$$C_1 = A_n{}^{-e_1}B_n{}^{u_2}A_n{}^{e_1} = A_n{}^{u_1}B_n{}^{-u_2}A_n{}^{-u_1}.$$

In Step 2 of the first iteration,

$$\begin{aligned} w = C_1{}^{-1}w &= A_n{}^{u_1}B_n{}^{-u_2}A_n{}^{-u_1}A_n{}^{u_1}B_n{}^{u_2}A_n{}^{u_3}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m} \\ &= A_n{}^{u_1+u_3}B_n{}^{u_4}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m} \end{aligned}$$

As $w \neq 1_{X_n}$, $i = 2$ and return Step 1.

Assume that for $1 \leq j-1 \leq \frac{m-5}{2}$, in Step 2 of the $i = j-1$th iteration,

$$w = A_n{}^{(u_1+u_3+u_5+\cdots+u_{2j-3}+u_{2j-1})}B_n{}^{u_{2j}}A_n{}^{u_{2j+1}}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m}.$$

In Step 1 of the jth iteration,

$$e_j = -(u_1+u_3+u_5+\cdots+u_{2j-1}).$$

If $e_j = -(u_1+u_3+u_5+\cdots+u_{2j-1}) \notin S$, then it outputs ϵ and terminates. If $e_j = -(u_1+u_3+u_5+\cdots+u_{2j-1}) \in S$, then in Step 2 of the jth iteration,

$$\begin{aligned} w &= C_j{}^{-1}w \\ &= A_n{}^{u_1+u_3+u_5+\cdots+u_{2j-1}}B_n{}^{-u_{2j}}A_n{}^{-(u_1+u_3+u_5+\cdots+u_{2j-1})} \\ &\quad A_n{}^{u_1+u_3+u_5+\cdots+u_{2j-3}+u_{2j-1}}B_n{}^{u_{2j}}A_n{}^{u_{2j+1}}B_n{}^{u_{2j+2}}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m} \\ &= A_n{}^{u_1+u_3+u_5+\cdots+u_{2j-1}+u_{2j+1}}B_n{}^{u_{2j+2}}A_n{}^{u_{2j+3}}\cdots B_n{}^{u_{m-1}}A_n{}^{u_m} \end{aligned}$$

As $w \neq 1_{X_n}$, $i = j+1$ and return Step 1.

For $j+1 = \frac{m-1}{2}$, in Step 1 of the $j+1$th iteration,

$$e_{\frac{m-1}{2}} = -(u_1+u_3+u_5+\cdots+u_{m-2}).$$

If $e_{\frac{m-1}{2}} \notin S$, then it outputs ϵ and terminates.

If $e_{\frac{m-1}{2}} \in S$, then

$$\begin{aligned} C_{\frac{m-1}{2}} &= {A_n}^{-e_{\frac{m-1}{2}}} {B_n}^{u_{m-1}} {A_n}^{e_{\frac{m-1}{2}}} \\ &= {A_n}^{u_1+u_3+u_5+\cdots+u_{m-2}} {B_n}^{u_{m-1}} {A_n}^{-(u_1+u_3+u_5+\cdots+u_{m-2})}. \end{aligned}$$

In Step 2 of the $j+1 = \frac{m-1}{2}$th iteration,

$$\begin{aligned} w &= {C_{\frac{m-1}{2}}}^{-1} w \\ &= {A_n}^{u_1+u_3+u_5+\cdots+u_{m-2}} {B_n}^{-u_{m-1}} {A_n}^{-(u_1+u_3+u_5+\cdots+u_{m-2})} w \\ &= {A_n}^{u_1+u_3+u_5+\cdots+u_{m-2}} {B_n}^{-u_{m-1}} {A_n}^{-(u_1+u_3+u_5+\cdots+u_{m-2})} \\ &\quad \cdot {A_n}^{u_1+u_3+u_5+\cdots+u_{m-2}} {B_n}^{u_{m-1}} {A_n}^{u_m} \\ &= {A_n}^{u_1+u_3+u_5+\cdots+u_{m-2}+u_m} \end{aligned}$$

If $u_m = -(u_1+u_3+u_5+\cdots+u_{m-2})$, then $w = 1_{X_n}$ and it outputs

$$\begin{aligned} & C_1 C_2 C_3 \cdots C_{\frac{m-3}{2}} C_{\frac{m-1}{2}} \\ &= {A_n}^{u_1} {B_n}^{u_2} {A_n}^{-u_1} {A_n}^{u_1+u_3} {B_n}^{u_4} {A_n}^{-(u_1+u_3)} \cdots \\ &\quad \cdot {A_n}^{u_1+u_3+u_5+\cdots+u_{m-2}} {B_n}^{u_{m-1}} {A_n}^{-(u_1+u_3+u_5+\cdots+u_{m-2})} \end{aligned}$$

as the $X(n, S)$-representation of M.
If $u_m \neq -(u_1+u_3+u_5+\cdots+u_{m-2})$, then

$$w = {A_n}^{u_1+u_3+u_5+\cdots+u_{m-2}+u_m} \neq 1_{X_n}$$

and $i = \frac{m+1}{2}$. Therefore it outputs ϵ and then terminates. □

4. Conclusion

Through this paper two representation algorithms used in the decryption of the homomorphic public key cryptosystem have been surveyed. Both algorithms are strictly justified by showing how each step of the algorithms operates according to inputs and also modified for computational efficiency and termination of the algorithms. This work takes more cases not appearing in the original algorithms into account to clarify both algorithms and it leads to more efficient decryption scheme. Especially for understanding the algorithms those theoretical background is described clearly in the process. Note that in practice programming both modified algorithms and its demonstration with experiments are omitted in this note.

References

1. D. Grigoriev & I. Ponomarenko: Homomorphic Public Key Cryptosystems over Groups and Rings. *Complexity of computations and proofs, Quaderni di mathematica* **13** (2004), 305–325.
2. R.C. Lyndon & P.E. Schupp: *Combinatorial Group Theory.* Springer-Verlag, 1977.

Center for Information Security and Technologies, Korea University, Seoul 136-701, Korea
Email address: purity100@hotmail.com