# A Note with Computer Exploration on the Triangle Conjecture <br> Christophe Cordero 

## To cite this version:

Christophe Cordero. A Note with Computer Exploration on the Triangle Conjecture. Lecture Notes in Computer Science, 2019, 10.1007/978-3-030-13435-8_30 . hal-03682699

HAL Id: hal-03682699
https://hal.science/hal-03682699
Submitted on 31 May 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# A Note with Computer Exploration on the Triangle Conjecture 

Christophe Cordero ${ }^{1}$<br>Université Paris-Est, LIGM (UMR 8049), CNRS, ENPC, ESIEE Paris, UPEM, F-77454, Marne-la-Vallée, France.


#### Abstract

The triangle conjecture states that codes formed by words of the form $a^{i} b a^{j}$ are either commutatively equivalent to a prefix code or not included in a finite maximal code. Thanks to computer exploration, we exhibit new examples of such non-commutatively prefix codes. In particular, we improve a lower bound in a bounding due to Shor and Hansel. We discuss in the rest of the article the possibility of those codes to be included in a finite maximal code.


Keywords: Codes• Triangle conjecture • Commutative equivalence conjecture.

General notation: Let $A$ be the alphabet $\{a, b\}$. For $n \geq 0$, let $A^{\leq n}$ be the set of words of $A^{*}$ of length at most $n$. For any word $w \in A^{*}$, let $|w|_{x}$ be the number of occurrences of the letter $x \in A$ in $w$. For any integer $n$, let $[n]$ be the set $\{k \in \mathbb{N}: 1 \leq k \leq n\}$ and $[[n]]$ be the set $\{k \in \mathbb{N}: 0 \leq k \leq n-1\}$. For a real number $x \in \mathbb{R}$, let $\lceil x\rceil$ be the least integer greater than or equal to $x$.

## Introduction

Our introduction to the theory of codes follows the book [1]. We call a subset $X \subset A^{*}$ a code if for all $n, m \geq 0$ and $x_{1}, \ldots, x_{n}, y_{1}, \ldots, y_{m} \in X$ the condition

$$
x_{1} x_{2} \cdots x_{n}=y_{1} y_{2} \cdots y_{m}
$$

implies

$$
n=m \text { and } x_{i}=y_{i} \text { for all } i \in[n] .
$$

For example, the set $\{a a b b, a b a a a, b, b a\}$ is not a code since

$$
(b)(a b a a a)(b)(b)=(b a)(b a)(a a b b)
$$

A code is maximal if it is not contained in any other code. A subset $X \subset A^{*}$ is prefix if no element of $X$ is a proper prefix of another element in $X$. A prefix subset not containing the empty word is a code. A code $X$ is commutatively prefix if there exists a prefix code $P$ such that the multisets

$$
\left\{\left(|x|_{a},|x|_{b}\right): x \in X\right\} \text { and }\left\{\left(|p|_{a},|p|_{b}\right): p \in P\right\}
$$

are equal. In other words, it states that one can build a prefix code from $X$ by allowing commutation between the letters. The commutative equivalence conjecture is one of the main open problem in the theory of codes. It states that all finite maximal code are commutatively prefix.

In this work, we study this conjecture for a particular case of codes called bayonet code. A code $X$ is a bayonet code if $X \subset a^{*} b a^{*}$. This particular case of the conjecture is also called the triangle conjecture. It states that a noncommutatively prefix bayonet code is not included in a finite maximal code (see [10] for recent result). It is known that a bayonet code $X$ is commutatively prefix if and only if

$$
\begin{equation*}
\left|X \cap A^{\leq n}\right| \leq n, \text { for all } n \geq 0 \tag{1}
\end{equation*}
$$

In 1984, Shor [9] found the bayonet code

$$
\begin{array}{r}
\left\{b, b a, b a^{7}, b a^{13}, b a^{14}, a^{3} b, a^{3} b a^{2}, a^{3} b a^{4}, a^{3} b a^{6}, a^{8} b, a^{8} b a^{2}, a^{8} b a^{4}, a^{8} b a^{6}\right. \\
\left.a^{11} b, a^{11} b a, a^{11} b a^{2}\right\} \tag{2}
\end{array}
$$

with 16 elements and included in $A^{\leq 15}$, thus it is a non-commutatively prefix code. It is the only known example of finite non-commutatively prefix code. It is still unknown if Shor's code (2) is included in a finite maximal code. If it is the case, then the commutative equivalence conjecture and a stronger conjecture called factorisation conjecture (see [2] for a recent note/summary) would be false.

It is known that for all finite maximal code $X$ and for any letter $x \in A$, there exists $k$ such that $x^{k} \in X$. We call the order of a letter $x$ the smallest integer $k$ such that $x^{k}$ belongs to $X$. It has been showed that if Shor's code (2) is included in a finite maximal code then the order of the letter $a$ is a multiple of 330 .

In the first section, we mainly do some computer explorations of non-commutatively prefix bayonet codes. We exhibit new examples of such codes. In particular, we exhibit the smallest ones and deduce from these a better lower bound in a bounding due to by Shor [9] and Hansel [4]. We discuss in the rest of the article the possibility of those codes to be included in a finite maximal code. In the second section, we use factorisation of cyclic group theory to prove some lower bounds for the orders of the letter $a$. Finally, in the last section, we find the smallest known codes that are non-commutatively prefix and not included in a finite maximal code.

## 1 Non-commutatively prefix bayonet codes

Given a bayonet code $X$, we call its dual the bayonet code

$$
\delta(X):=\left\{a^{i} b a^{j} \mid a^{j} b a^{i} \in X\right\} .
$$

Of course, a bayonet code is commutatively prefix or included in a finite maximal code if and only if its dual is. Thus we consider in this work a bayonet code and its dual to be the same. Even if they cannot be equal in the case we are interested in.

Proposition 1. If a bayonet code $X$ is non-commutatively prefix then $X \neq$ $\delta(X)$.

Proof. Let $X$ be an auto-dual bayonet code (i.e. $X=\delta(X))$ and $n$ be an integer. Let $E_{i}^{n}$ be the set

$$
\left(a^{i} b a^{*} \cup a^{*} b a^{i}\right) \cap A^{\leq n}
$$

for $i \geq 0$. Thus

$$
X \cap A^{\leq n}=\bigsqcup_{0 \leq i \leq\left\lceil\frac{n}{2}\right\rceil}\left(X \cap E_{i}^{n}\right) \text { and }\left|X \cap A^{\leq n}\right|=\sum_{0 \leq i \leq\left\lceil\frac{n}{2}\right\rceil}\left|X \cap E_{i}^{n}\right| .
$$

It is enough to show that $\left|X \cap E_{i}^{n}\right| \leq 2$, for $i \geq 0$. Assume that $\left|X \cap E_{i}^{n}\right|>2$. Then there exists $j_{1} \geq i$ and $j_{1}<j_{2}<n-i$ such that

$$
a^{i} b a^{j_{1}}, a^{i} b a^{j_{2}}, a^{j_{1}} b a^{i}, a^{j_{2}} b a^{i} \in X .
$$

Thus

$$
\left(a^{i} b a^{j_{1}}\right)\left(a^{j_{2}} b a^{i}\right)=\left(a^{i} b a^{j_{2}}\right)\left(a^{j_{1}} b a^{i}\right)
$$

which contradicts the fact that $X$ is a code. Thus $\left|X \cap A^{\leq n}\right| \leq n$ and thanks to (1), we conclude that $X$ is commutatively equivalent to a prefix code. This concludes the proof by contraposition.

Remark 1. Notice that the auto-dual bayonet code $\left\{a^{i} b a^{n-1-i}: 0 \leq i<n\right\}$ reaches the bound (1).

### 1.1 Computer exploration

We run an exhaustive search issuing the following algorithm directly deduced from the definition of a code. Given a set $X \subset a^{*} b a^{*} \cap A^{\leq n}$, we build the oriented graph $\mathcal{G}_{\text {abs }}(X)$ defined by the set of vertices $[[n]]$ and by the edges

$$
|i-k| \longrightarrow|j-\ell|,
$$

for all $a^{i} b a^{j}, a^{k} b a^{\ell} \in X$ with $a^{i} b a^{j} \neq a^{k} b a^{\ell}$.
Example 1. Let $X$ be the set $\left\{a^{4} b a^{3}, a^{2} b a^{5}, a b a^{5}, b, b a^{2}\right\}$, the graph $\mathcal{G}_{\text {abs }}(X)$ is


Thus $X$ is a code (see Proposition 2).
Then we use the following proposition.

Proposition 2. $X$ is a code if and only if $\mathcal{G}_{\text {abs }}(X)$ does not contains a nonempty path from 0 to 0 .

Proof. Given $X \subset a^{*} b a^{*} \cap A^{\leq n}$, there is an edge from $i$ to $j$ in the graph $\mathcal{G}_{\text {abs }}(X)$ if and only if there exist $U, V \in X$ such that

$$
a^{i} U=V a^{j} \text { or } a^{i} U a^{j}=V
$$

By concatenation, there is a path from $i$ to $j$ in the graph if and only if there exist $U, V \in X^{*}$ such that

$$
\begin{equation*}
a^{i} U=V a^{j} \text { or } a^{i} U a^{j}=V \tag{3}
\end{equation*}
$$

Assume that there is a non-empty path from 0 to 0 going through $k \neq 0$. Then by (3) there exist $U_{1}, U_{2}, V_{1}, V_{2} \in X^{*}$ such that

$$
U_{1}=V_{1} a^{k} \text { and } U_{2}=a^{k} V_{2}
$$

Hence $U_{1} V_{2}=V_{1} U_{2}$ with $U_{1}=V_{1} a^{k}$, and thus $X$ is not a code.
Conversely, if $X$ is not a code then there exist $a^{i_{1}} b a^{j_{1}}, \ldots, a^{i_{n}} b a^{j_{n}}$, $a^{k_{1}} b a^{\ell_{1}}, \ldots, a^{k_{n}} b a^{\ell_{n}} \in X$ such that

$$
\left(a^{i_{1}} b a^{j_{1}}\right)\left(a^{i_{2}} b a^{j_{2}}\right) \cdots\left(a^{i_{n}} b a^{j_{n}}\right)=\left(a^{k_{1}} b a^{\ell_{1}}\right)\left(a^{k_{2}} b a^{\ell_{2}}\right) \cdots\left(a^{k_{n}} b a^{\ell_{n}}\right) .
$$

Thus, the graph $\mathcal{G}_{\text {abs }}(X)$ contains the path

$$
0=\left|i_{1}-k_{1}\right| \rightarrow\left|j_{1}-\ell_{1}\right|=\left|i_{2}-k_{2}\right| \rightarrow \cdots \rightarrow\left|j_{n}-\ell_{n}\right|=0 \text {. }
$$

Remark 2. There already exist some algorithm to test in general if a given set is a code [8]. However, we noticed that for an exhaustive search of non-commutatively prefix bayonet code, our backtracking implementation of our algorithm (using mostly bitwise operation) runs faster.

We ran an exhaustive search of codes violating the condition (1), for $n \leq 15$. There is no such code for $n \leq 11, n=13$, and $n=14$. There are 4 codes for $n=12$. We exhibit them below by representing the bayonet word $a^{i} b a^{j}$ by the two digits $x_{i} x_{j}$, where $x_{i}$ is the $i$-th digit in base $17(0, \ldots, 9, \mathrm{~A}, \ldots, \mathrm{G})$.

| ID | Non-commutatively prefix bayonet code |  |  |  |  |  |  |  |  |  |  |  |  |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| $X_{1}$ | 00 | 02 | 08 | $0 A$ | 18 | 1 A | 40 | 42 | 50 | 53 | 56 | 90 | 92 |
| $X_{2}$ | 01 | 03 | 09 | $0 B$ | 18 | 1 A 40 | 42 | 50 | 53 | 56 | 90 | 92 |  |
| $X_{3}$ | 02 | 08 | $0 A$ | 10 | 18 | $1 A$ | 42 | 50 | 53 | 56 | 60 | 92 | A0 |
| $X_{4}$ | 02 | 08 | $0 A$ | 18 | $1 A$ | 20 | 42 | 53 | 56 | 60 | 70 | 92 | B0 |

Up to the knowledge of the author, these are the smallest (in cardinality and maximal word length) known non-commutatively prefix codes. In [9], Shor asked what is the maximal value of the ratio of the cardinality of a bayonet code divided by the length of its longest word. Hansel [4] proved an upper bound and Shor computed the lower bound $\frac{16}{15}$. Thanks to codes $\left(X_{1}-X_{4}\right)$, we improve Shor's lower bound to $\frac{13}{12}$.

There are 38 such codes for $n=15$. They have in common the words

$$
\begin{equation*}
0107 \text { 0D 0E } 828486 \text { B1 B2 } \tag{4}
\end{equation*}
$$

Here follow the 38 codes, where for each code we only write the additional bayonets words.

| ID | Code | ID | Code |
| :---: | :---: | :---: | :---: |
| $Y_{1}$ | 00303234364080 | $Y_{20}$ | 2032343658 A0 D0 |
| $Y_{2}$ | 003032343680 B3 | $Y_{21}$ | 203436 3A 50 A0 |
| $Y_{3}$ | 003034363 A 80 B 0 | $Y_{22}$ | 203436 3A 58 A0 D0 |
| $Y_{4}$ | 00303436 3A 80 B3 | $Y_{23}$ | 3032343660 B0 E0 |
| $Y_{5}$ | 003133353780 B | $Y_{24}$ | 3032343660 B3 |
| $Y_{6}$ | 003133353780 B 3 | $Y_{25}$ | 303436 3A 60 B0 E0 |
| $Y_{7}$ | 00313537 3B 80 B0 | $Y_{26}$ | 303436 3A 60 B3 E0 |
| $Y_{8}$ | 00313537 3B 80 B | $Y_{27}$ | 3133353760 B |
| $Y_{9}$ | $0032343638 \quad 80$ B | $Y_{28}$ | 3133353760 B3 E0 |
| $Y_{10}$ | $0032343638 \quad 80$ B3 | $Y_{29}$ | 313537 3B 60 B0 |
| $Y_{11}$ | 00333537398080 | $Y_{30}$ | 313537 3B 60 B3 |
| $Y_{12}$ | 003335373980 B3 | $Y_{31}$ | 3234363860 B0 E0 |
| $Y_{13}$ | $003436383 \mathrm{~A} 80 \mathrm{B0}$ | $Y_{32}$ | 3234363860 B3 |
| $Y_{14}$ | 00343638 3A 80 B3 | $Y_{33}$ | 3335373960 B0 |
| $Y_{15}$ | 00353739 3B 80 B0 | $Y_{34}$ | 3335373960 B3 |
| $Y_{16}$ | 00353739 3B 80 B3 | $Y_{35}$ | 343638 3A 60 B0 |
| $Y_{17}$ | 103234364090 C 0 | $Y_{36}$ | 343638 3A 60 B3 E0 |
| $Y_{18}$ | 1034363 A 4090 C 0 | $Y_{37}$ | 353739 3B 60 B0 E0 |
| $Y_{19}$ | 2032343650 A0 D0 | $Y_{38}$ | 353739 3B 60 B3 E0 |

Notice that code $\left(Y_{1}\right)$ is Shor's code. We also ran a partial search for $n=16$.

| ID | \|| Non-commutatively prefix bayonet code |
| :---: | :---: |
| $Z_{1}$ | 0001020 B 0 C 3 B 3 C 50515280828486 D0 D1 D2 |
| $Z_{2}$ | 000102 0B 0C 3B 3C 50515281838587 D0 D1 D2 |
| $Z_{3}$ | 000102 0B 0C 3B 3C 50515 A 80828486 D0 D1 D2 |
| $Z_{4}$ | 000102 0B 0C 3B 3C 50515 A 81838587 D0 D1 D2 |
| $Z_{5}$ | 0001 0A 0B 0C 3B 3C 50515280828486 D0 D1 D2 |
| $Z_{6}$ | 0001 0A 0B 0C 3B 3C 50 51 52 81838587 D0 D1 D2 |
| $Z_{7}$ | 0001 0A 0B 0C 3B 3C 50515 A 80828486 D0 D1 D2 |
| $Z_{8}$ | 0001 0A 0B 0C 3B 3C 50515 A 81838587 D0 D1 D2 |
| $Z_{9}$ | 0002 0B 0C 11 3B 3C 50 52 6183858791 D0 D2 E1 |
| $Z_{10}$ | 0002 0B 0C 11 3B 3C 50 5A 6183858791 D0 D2 E1 |
| $Z_{11}$ | 0102030 C 0 D 3 B 3 C 50515280828486 D0 D1 D2 |
| $Z_{12}$ | 0102030 C 0 D 3 B 3 C 50515281838587 D0 D1 D2 |
| $Z_{13}$ | 0102030 C 0 D 3 B 3 C 50515 A 80828486 D0 D1 D2 |
| $Z_{14}$ | 0102030 C 0 D 3 B 3 C 50515 A 81838587 D0 D1 D2 |
| $Z_{15}$ | 0102 0B 0C 0D 3B 3C 50 51 52 80828486 D0 D1 D2 |
| $Z_{16}$ | 0102 0B 0C 0D 3B 3C 50515281838587 D0 D1 D2 |
| $Z_{17}$ | 0102 0B 0C 0D 3B 3C 50515 A 80828486 D0 D1 D2 |
| $Z_{18}$ | 0102 0B 0C 0D 3B 3C 5051 5A 81838587 D0 D1 D2 |
| $Z_{19}$ | 0102 0B 0C 10 3B 3C 51 52 6082848690 D1 D2 E0 |
| $Z_{20}$ | 0102 0B 0C 10 3B 3C 51 5A 6082848690 D1 D2 E0 |
| $Z_{21}$ | 0102 0B 0C 1D 3B 3C 51 52 6082848690 D1 D2 E0 |
| $Z_{22}$ | 0102 0B 0C 20 3B 3C 515270828486 A0 D1 D2 F0 |
| $Z_{23}$ | 0102 0B 0C 20 3B 3C 51 5A 70828486 A0 D1 D2 F0 |
| $Z_{24}$ | 0102 0B 0C 2D 3B 3C 515270828486 A0 D1 D2 F0 |
|  | 1020 0B 0C 2D 3B 3C 51 5A 70828486 A0 D1 D2 F0 |

There is no such code for $n=17$ containing $b$. However, we found the following codes showing that there exist codes violating (1) even when $n$ is prime.

$$
\begin{array}{llllllllllllllllll}
01 & 02 & 03 & 0 \mathrm{C} & 0 \mathrm{D} & 3 \mathrm{C} & 3 \mathrm{D} & 51 & 52 & 5 \mathrm{~B} & 80 & 82 & 84 & 86 & \text { D1 } & \text { D2 } & \text { D3 } & \text { G0 } \\
01 & 02 & 03 & 0 \mathrm{C} & 0 \mathrm{D} & 3 \mathrm{C} & 3 \mathrm{D} & 51 & 52 & 5 \mathrm{~B} & 81 & 83 & 85 & 87 & \text { D1 } & \text { D2 } & \text { D3 } & \text { G0 } \\
01 & 02 & 03 & 0 \mathrm{C} & 0 \mathrm{D} & 3 \mathrm{C} & 3 \mathrm{D} & 51 & 52 & 5 \mathrm{~B} & 82 & 84 & 86 & 88 & \text { D1 } & \text { D2 } & \text { D3 } & \text { G0 } \tag{5c}
\end{array}
$$

Let us recall that if one of these codes is included in a finite maximal code then the triangle conjecture is false. In the next sections, we try to complete each of these codes into a finite maximal one.

## 2 Factorisations of cyclic groups

In this section, we assume that the codes found in the previous section are included in some finite maximal code. Then we use factorisation of cyclic group
theory to prove some lower bounds for the orders of the letter $a$ in those finites codes.

Given $n \geq 1$, the ordered pair $(L, R) \subset[[n]]^{2}$ is a factorisation of $\mathbb{Z} / n \mathbb{Z}$ if for all $k \in[[n]]$ there exists a unique pair $(\ell, r) \in L \times R$ such that $k=\ell+r \bmod n$.
Example 2. The ordered pair $(\{1,3,5\},\{1,2,7,8\})$ is a factorisation of $\mathbb{Z} / 12 \mathbb{Z}$.
In [6], Restivo, Salemi, and Sportelli showed the following link between factorisation and the theory of codes.
Theorem 1. If $X$ is a finite maximal code such that $b, a^{n} \in X$ then $(L, R)$ is a factorisation of $\mathbb{Z} / n \mathbb{Z}$, where

$$
L=\left\{k \bmod n: a^{k} b^{+} \in X\right\} \text { and } R=\left\{k \bmod n: b^{+} a^{k} \in X\right\} .
$$

Such a factorisation is called a factorisation associated to $X$.
In [7], Sands proved the following useful theorem.
Theorem 2. If $(L, R)$ is a factorisation of $\mathbb{Z} / n \mathbb{Z}$ and $p$ is an integer relatively prime to $|L|$ then $(p L, R)$ is a factorisation of $\mathbb{Z} / n \mathbb{Z}$.

We call a Sands factorisation a factorisation $(L, R)$ such that $p, q \in L$ and $1 \in R$ where $p$ and $q$ are relatively prime. We still do not know if there exists a factorisation associated to Shor's code, i.e. if there exists an integer $n$ such that $(L \supseteq\{0,3,8,11\}, R \supseteq\{0,1,7,13,14\})$ is a (Sands) factorisation of $\mathbb{Z} / n \mathbb{Z}$. We now study the factorisations associated to the other codes found in the previous section.

### 2.1 Known factorisations

The reader can check that for $n \geq 2$,

$$
\begin{equation*}
\left(\{0,4,5,9\}, \bigsqcup_{i \in[n n]]}\{8 i, 8 i+2\}\right) \tag{6}
\end{equation*}
$$

is a factorisation of $\mathbb{Z} / 8 n \mathbb{Z}$ associated to the code $\left(X_{1}\right)$. In general, the integer $n$ such that there exists a factorisation of $\mathbb{Z} / n \mathbb{Z}$ associated to the code $\left(X_{1}\right)$ must be a multiple of 4 . Indeed, $(\{0,4,5,9\}, 2\{0,2,8,10\})$ and $(2\{0,4,5,9\},\{0,2,8,10\})$ are not factorisations because $0+2 \times 2=4+0$ and $2 \times 4+0=0+8$. Thus by Theorem 2 we have that $|L|$ and $|R|$ are multiples of 2 , hence $n$ is a multiple of 4 . We did not find any factorisation associated to the code $\left(X_{1}\right)$ where $n$ is a multiple of 4 and not a multiple of 8 .

The reader can check that for $n \geq 2$,

$$
\begin{equation*}
(\{0,8, \cdots, 8(n-1)\},\{0,1,2,3,4,7,13,14\}) \tag{7}
\end{equation*}
$$

is a factorisation of $\mathbb{Z} / 8 n \mathbb{Z}$ associated to the codes $\left(Y_{6}, Y_{8}, Y_{10}, Y_{12}, Y_{14}, Y_{16}\right)$. By a similar argument, we can show that in general a factorisation of $\mathbb{Z} / n \mathbb{Z}$ associated to those codes satisfies the fact that 4 divides $n$.

The others factorisations associated to codes found in the previous section are of Sands type or equivalent to a Sands factorisation.

### 2.2 Sands factorisations

We did not find Sands factorisation but we can compute some constraints about their existence.

Assume that the code $\left(Y_{2}\right)$ is included in a finite maximal code. Let $(L, R)$ be a factorisation associated to this code, thus $L \supseteq\{0,3,8\}$ and $R \supseteq\{0,1,7,13,14\}$. Notice that $(L, 8 R),(L, 3 R)$, and $(L, 5 R)$ are not factorisations since $8+8 \times 0=$ $0+8 \times 1,8+3 \times 0=0+3 \times 1$, and $8+5 \times 0=3+5 \times 1$, so that by Theorem 2 , we have that $|R|$ is a multiple of $2 \times 3 \times 5$. Thus the order of the letter $a$ is of the form $30 \times k$, where $k \geq 3$.

Following a similar argument we compute the following table.

| Codes | Order of the letter $a$ |
| :---: | :---: |
| $Y_{2}, Y_{4}$ | $2 \times 3 \times 5 \times k=30 k$, with $k \geq 3$ |
| $Y_{5}, Y_{7}, Y_{9}, Y_{11}, Y_{13}, Y_{15}$ | $2 \times 3 \times 11 \times k=66 k$, with $k \geq 3$ |
| $Y_{1}, Y_{3}$ | $2 \times 3 \times 5 \times 11 \times k=330 k$, with $k \geq 4$ |
| $Z_{1}, Z_{3}, Z_{5}, Z_{7}$ | $2 \times 3 \times 5 \times 13 \times k=390 k$, with $k \geq 4$ |
| $Z_{2}, Z_{4}, Z_{6}, Z_{8}$ | $2 \times 3 \times 5 \times 13 \times k=390 k$, with $k \geq 3$ |
| $Z_{9}, Z_{10}$ | $2 \times 5 \times 13 \times k=130 k$, with $k \geq 3$ |

Remark 3. It is known [7] that $(L, R)$ is a factorisation if and only if $(L, R-r)$ is a factorisation, where $r \in R$. Thus if $(L \supseteq\{0,5,13\}, R \supseteq\{0,2,11,12\})$ is a factorisation associated to the codes $\left(Z_{9}, Z_{10}\right)$ then $(L, R-11)$ is a Sands factorisation.

The factorisations just take into account the words belonging to $b a^{*} \cup a^{*} b$. In the next section, we look for a more powerful tool.

## 3 Complete modular bayonet code

In this section, we use a theorem by Perrin and Schützenberger to find the smallest known codes that are non-commutatively prefix and not included in a finite maximal code. Then, we propose a new approach of the triangle conjecture thanks to this theorem.

In [5], Perrin and Schützenberger proved the following theorem.
Theorem 3. Let $X$ be a finite maximal code. Let $x \in A$ be a letter and let $n$ be the order of $x$. For all $\omega \in A^{*}$, the set

$$
C_{x}(\omega):=\left\{(i \bmod n, j \bmod n): x^{i} \omega x^{j} \in X^{*}\right\}
$$

has cardinal $n$.
We call a n-modular bayonet code a bayonet code $X$ such that $\left\{a^{n}\right\} \cup X$ is a code and we said that it is complete if $|X|=n$. Thanks to Theorem 3, we know that to be included in a finite maximal code, a bayonet code must be included in a complete $n$-modular bayonet code.

Example 3. We call an $n$-permutation code a set of bayonet words $X \subseteq a^{<n} b a^{<n}$ such that the square binary matrix $\mathcal{M}$ of size $n$ defined by

$$
\mathcal{M}_{i, j}=1 \text { if and only if } a^{i} b a^{j} \in X
$$

is a permutation matrix. An $n$-permutation code is a complete $n$-modular bayonet code.

We now try to find a complete $n$-modular bayonet code containing one of our codes that is non-commutatively equivalent to a prefix code.

### 3.1 Computer exploration

We slightly modify the algorithm given in section 1 to test whether or not a given set is an $n$-modular bayonet code. Given a set $X \in a^{<n} b a^{<n}$, we call $\mathcal{G}_{\bmod }(X)$ the oriented graph defined by the set of vertices $[[n]]$ and by the edges

$$
i-k \bmod n \longrightarrow \ell-j \bmod n
$$

for all $a^{i} b a^{j}, a^{k} b a^{\ell} \in X$, with $a^{i} b a^{j} \neq a^{k} b a^{\ell}$. The set $X$ is an $n$-modular bayonet code if and only if the graph $\mathcal{G}_{\bmod }(X)$ does not contain a non-empty path from 0 to 0 .

In the previous section, we show that the codes $\left(X_{1}, Y_{6}, Y_{8}, Y_{10}, Y_{12}, Y_{14}\right.$, $\left.Y_{16}\right)$ might be included in a finite maximal code where the order of the letter $a$ is of the form $4 \times k$ with $k \geq 4$. By an exhaustive computer search, we found that none of these codes is included in a complete $n$-modular bayonet code, where $n \leq 32$. Thus if $\left(X_{1}\right)$ is included in a finite maximal code then the order of the letter $a$ is of the form $4 \times k$, where $k \geq 10$ (there is no factorisation of $\mathbb{Z} / n \mathbb{Z}$ associated to this code, where $32<n<40)$. If one of the codes $\left(Y_{6}, Y_{8}, Y_{10}\right.$, $\left.Y_{12}, Y_{14}, Y_{16}\right)$ is included in a finite maximal code then the order of the letter $a$ is of the form $4 \times k$, where $k \geq 9$ (there is no factorisation of $\mathbb{Z} / n \mathbb{Z}$ associated to those codes with $32<n<36$ ). In particular, the computer exploration implies the following proposition.

Proposition 3. If $X$ is one of the codes $\left(X_{1}-X_{4}\right)$, then $X \cup\left\{a^{16}\right\}$ is a code that is non-commutatively equivalent to a prefix code and not included in a finite maximal code.

Proof. Let $X$ be one of the codes $\left(X_{1}-X_{4}\right)$. Then $X \cup\left\{a^{16}\right\}$ is a code. Moreover, we checked by an exhaustive search that $X$ is not included in a complete 16modular bayonet code. We conclude the proof thanks to Theorem 3.

Up to the knowledge of the author, the four codes given in Proposition 3 are the smallest (in cardinality and maximal length word) known codes that are not commutatively equivalent to a prefix code and not included in a finite maximal code.

### 3.2 Transformations

In order to have a better understanding of the complete $n$-modular bayonet code, we look at some transformations.

Lemma 1. If $X$ is an n-modular code then for any $r \in[[n]]$, the set

$$
s_{r}(X):=\left\{a^{i} b a^{j}: a^{i} b a^{p}, a^{q} b a^{j} \in X \text { and } p+q=r \bmod n\right\}
$$

is an n-modular code.
Proof. Given an integer $r \in[[n]]$, if $s_{r}(X)$ is not an $n$-modular bayonet code then there exists $a^{i_{1}} b a^{j_{1}}, \ldots, a^{i_{m}} b a^{j_{m}}, a^{k_{1}} b a^{\ell_{1}}, \ldots, a^{k_{m}} b a^{\ell_{m}} \in s_{r}(X)$, with $j_{1} \neq \ell_{1}$ such that

$$
\left\{\begin{aligned}
i_{1} & =k_{1} \\
j_{1}+i_{2} & =\ell_{1}+k_{2} \quad \bmod n \\
& \vdots \\
j_{m-1}+i_{m} & =\ell_{m-1}+k_{m} \bmod n \\
j_{m} & =\quad \ell_{m}
\end{aligned}\right.
$$

By definition of $s_{r}(X)$, there exists $a^{i_{1}} b a^{p_{1}}, a^{q_{1}} b a^{j_{1}}, \ldots, a^{i_{m}} b a^{p_{m}}, a^{q_{m}} b a^{j_{m}} \in X$ and $a^{k_{1}} b a^{p_{1}^{\prime}}, a^{q_{1}^{\prime}} b a^{\ell_{1}}, \ldots, a^{k_{m}} b a^{p_{m}^{\prime}}, a^{q_{m}^{\prime}} b a^{\ell_{m}} \in X$ such that $p_{t}+q_{t}=p_{t}^{\prime}+q_{t}^{\prime}=r$ $\bmod n$, for all $t \in[m]$. Thus

$$
\left\{\begin{array}{rlr}
i_{1} & = & k_{1} \\
p_{1}+q_{1} & = & p_{1}^{\prime}+q_{1}^{\prime} \\
\bmod n \\
j_{1}+i_{2} & = & \ell_{1}+k_{2} \quad \bmod n \\
& \vdots \\
& \\
j_{m-1}+i_{m} & =\ell_{m-1}+k_{m} \bmod n \\
p_{m}+q_{m} & = & p_{m}^{\prime}+q_{m}^{\prime} \bmod n \\
j_{m} & = & \ell_{m}
\end{array}\right.
$$

Thus $X$ is not an $n$-modular code, since it has a double factorisation. We conclude the proof by contraposition.

We use this lemma to prove the following theorem ${ }^{1}$.
Theorem 4. If $X$ is an n-modular code then $|X| \leq n$.
Proof. Assume that $X$ is an $n$-modular code such that $|X|>n$. Thanks to Lemma 1, we know that for any $r \in[[n]]], s_{r}(X)$ is a code thus

$$
\sum_{r \in[[n]]}\left|s_{r}(X)\right|=|X|^{2}
$$

Thus there exists $r_{1} \in[[n]]$ such that $\left|s_{r_{1}}(X)\right| \geq\left\lceil\frac{|X|^{2}}{n}\right\rceil \geq n+1$. By iteration, there exists $r_{2}, \ldots, r_{n^{2}} \in[[n]]$ such that $\left|s_{r_{n} 2}\left(\cdots s_{r_{2}}\left(s_{r_{1}}(X)\right) \cdots\right)\right|>n^{2}$ which contradicts the fact that $X$ belongs to $a^{<n} b a^{<n}$.

[^0]Thanks to this theorem, we now exhibit five transformations of an $n$-modular code that preserve the completeness.

Theorem 5. If $X$ is an n-modular code (respectively complete) then

1. For all $\alpha$ and $\beta$, the set

$$
\tau_{\alpha, \beta}(X):=\left\{a^{i+\alpha \bmod n} b a^{j+\beta} \bmod n: a^{i} b a^{j} \in X\right\}
$$

is an n-modular code (respectively complete).
2. For all $q$ prime to $n$, the set

$$
\rho_{q}(X):=\left\{a^{q i \bmod n} b a^{q j \bmod n}: a^{i} b a^{j} \in X\right\}
$$

is an n-modular code (respectively complete).
3. The set

$$
\iota(X):=\left\{a^{n-1-i} b a^{j}: a^{i} b a^{j} \in X\right\}
$$

is an n-modular code (respectively complete).
4. The dual code $\delta(X)$ is an $n$-modular code (respectively complete).
5. For any $r \in[[n]]$, the set $s_{r}(X)$ is an n-modular code (respectively complete).

Proof. 1. For any $\alpha, \beta \in[[n]]$, the graph $\mathcal{G}_{\bmod }\left(\tau_{\alpha, \beta}(X)\right)$ is equal to the graph $\mathcal{G}_{\bmod }(X)$. Thus $X$ is an $n$-modular code if and only if $\tau_{\alpha, \beta}(X)$ is an $n$-modular code.
2. For any $q$ prime to $n$, the function that associates to $i \in[[n]]$ the integer $q i$ $\bmod n$ is a graph isomorphism from $\mathcal{G}_{\bmod }(X)$ to $\mathcal{G}_{\bmod }\left(\rho_{q}(X)\right)$. Thus $X$ is a code if and only if $\rho_{q}(X)$ is a code.
3. If $\iota(X)$ is not an $n$-modular bayonet code then the graph $\mathcal{G}_{\bmod }(\iota(X))$ contains the paths

$$
0 \rightarrow \boxed{i_{1}} \longrightarrow i_{2} \longrightarrow \cdots \boxed{i_{m}} \longrightarrow 0
$$

and

$$
0 \rightarrow-i_{1} \bmod n \rightarrow-i_{2} \bmod n \rightarrow \cdots-i_{m} \bmod n \rightarrow 0
$$

for $i_{1}, \ldots, i_{m} \in[[n]]$. Thus, the graph $\mathcal{G}_{\bmod }(X)$ contains the path

$$
0 \longrightarrow \boxed{i_{1}} \rightarrow-i_{2} \bmod n \rightarrow i_{3} \rightarrow-i_{4} \bmod n \rightarrow \cdots \longrightarrow 0
$$

which contradicts the fact that $X$ is an $n$-modular code. We conclude the proof by contraposition.
4. The graph $\mathcal{G}_{\text {mod }}(\delta(X))$ is the graph $\mathcal{G}_{\text {mod }}(X)$ with inverted arrows.

5 . If $X$ is an $n$-modular code then, by Lemma $1, s_{r}(X)$ is an $n$-modular code. Let us prove that if $|X|=n$ then for any $r \in[[n]],\left|s_{r}(X)\right|=n$. Assume that $\left|s_{r}(X)\right| \neq n$ for $r \in[[n]]$ then there exists an $r^{\prime} \in[[n]]$ such that $\left|s_{r^{\prime}}(X)\right|>n$ which contradicts Theorem 4.

The author wonders if the following Sands-like statement (a strong version of Theorem 5.2) is true.

Conjecture 1 If $X$ is a complete $n$-modular bayonet code then

$$
\varphi_{q}(X):=\left\{a^{q i \bmod n} b a^{j}: a^{i} b a^{j} \in X\right\}
$$

is a complete n-modular bayonet code, for all $q$ prime to $n$.
If this conjecture is true, then one can compute some lower bound for the order of the letter $a$, using all the bayonet words. Notice that we already proved the case $q=n-1$ of Conjecture 1 in Theorem 5, indeed $\varphi_{q}(X)=\tau_{1,0}(\iota(X))$.

## Conclusion and perspectives

We propose three main perspectives. Firstly, we would like to enumerate the bayonet codes that are non-commutatively equivalent to a prefix code. As we saw in the section 1, the codes we found look closely related to each other. Secondly, we wonder if there exists a code non-commutatively equivalent to a prefix code smaller then the codes $\left(X_{1}-X_{4}\right)$. Such a code would necessarily be a non-bayonet code. Finally, our main perspective is continuing our effort to find whether or not there exists a bayonet non-commutatively prefix code that is included in a complete modular bayonet code.

## Acknowledgements

The author wants to thank Dominique Perrin for introducing him to the commutatively prefix conjecture, also his PhD supervisors Samuele Giraudo and JeanChristophe Novelli.

## References

1. Berstel, J., Perrin, D., Reutenauer, C.: Codes and automata, vol. 129. Cambridge University Press (2010)
2. De Felice, C.: A note on the factorization conjecture. Acta informatica 50(7-8), 381-402 (2013)
3. De Felice, C., Restivo, A.: Some results on finite maximal codes. RAIROTheoretical Informatics and Applications-Informatique Théorique et Applications 19(4), 383-403 (1985)
4. Hansel, G.: Baionnettes et cardinaux. Discrete Mathematics 39(3), 331-335 (1982)
5. Perrin, D., Schützenberger, M.P.: Codes et sous-monoïdes possédant des mots neutres. In: Theoretical Computer Science, pp. 270-281. Springer (1977)
6. Restivo, A., Salemi, S., Sportelli, T.: Completing codes. RAIRO-Theoretical Informatics and Applications 23(2), 135-147 (1989)
7. Sands, A.D.: Replacement of factors by subgroups in the factorization of abelian groups. Bulletin of the London Mathematical Society 32(3), 297-304 (2000)
8. Sardinas, A.A., Patterson, G.W.: A necessary and sufficient condition for unique decomposition of coded messages. Proceedings Of The Institute Of Radio Engineers 41(3), 425-425 (1953)
9. Shor, P.W.: A counterexample to the triangle conjecture. Journal of Combinatorial Theory, Series A 38(1), 110-112 (1985)
10. Zhang, L., Shum, K.P.: Finite maximal codes and triangle conjecture. Discrete Mathematics 340(3), 541-549 (2017)

[^0]:    ${ }^{1}$ Shortly after the publication of this article, the author found that this result is equivalent to Proposition 2.1 in [3] from Restivo and De Felice.

