A Note with Computer Exploration on the Triangle Conjecture

Christophe Cordero[1]

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^iba^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 $\{aabb, abaaa, b, ba\}$ is not a code since

$$(b)(abaaa)(b)(b) = (ba)(ba)(aabb).$$

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

$$\{(|x|_a, |x|_b) : x \in X\} \text{ and } \{(|p|_a, |p|_b) : p \in P\}$$

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 $X \subset a^*ba^*$. This particular case of the conjecture is also called the *triangle conjecture*. It states that a non-commutatively 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

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

In 1984, Shor [9] found the bayonet code

$$\{b, ba, ba^7, ba^{13}, ba^{14}, a^3b, a^3ba^2, a^3ba^4, a^3ba^6, a^8b, a^8ba^2, a^8ba^4, a^8ba^6, a^{11}b, a^{11}ba, a^{11}ba^2\} \tag{2}$$

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

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

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

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

It is enough to show that $|X \cap E_i^n| \leq 2$, for $i \geq 0$. Assume that $|X \cap E_i^n| > 2$. 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 $\{a^i b a^{n-1-i} : 0 \leq i < n\}$ reaches the bound (1).

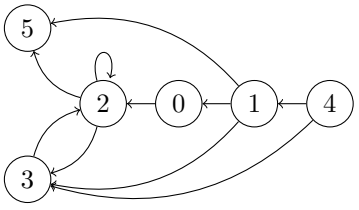
1.1 Computer exploration

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

$$\boxed{|i-k|} \longrightarrow \boxed{|j-\ell|},$$

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 $\mathcal{G}_{abs}(X)$ does not contains a non-empty path from 0 to 0.*

Proof. Given $X \subset a^*ba^* \cap A^{\leq n}$, 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

$$a^iU = Va^j \text{ or } a^iUa^j = V.$$

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

$$a^iU = Va^j \text{ or } a^iUa^j = V. \tag{3}$$

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

$$U_1 = V_1a^k \text{ and } U_2 = a^kV_2.$$

Hence $U_1V_2 = V_1U_2$ with $U_1 = V_1a^k$, and thus X is not a code.

Conversely, if X is not a code then there exist $a^{i_1}ba^{j_1}, \ldots, a^{i_n}ba^{j_n}$, $a^{k_1}ba^{\ell_1}, \ldots, a^{k_n}ba^{\ell_n} \in X$ such that

$$\left(a^{i_1}ba^{j_1}\right)\left(a^{i_2}ba^{j_2}\right)\cdots\left(a^{i_n}ba^{j_n}\right) = \left(a^{k_1}ba^{\ell_1}\right)\left(a^{k_2}ba^{\ell_2}\right)\cdots\left(a^{k_n}ba^{\ell_n}\right).$$

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

$$\boxed{0 = |i_1 - k_1|} \to \boxed{|j_1 - \ell_1| = |i_2 - k_2|} \to \cdots \to \boxed{|j_n - \ell_n| = 0}.$$

□

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^iba^j by the two digits x_ix_j, where x_i is the i-th digit in base 17 $(0, \ldots, 9, \text{A}, \ldots, \text{G})$.

ID	Non-commutatively prefix bayonet code
X_1	00 02 08 0A 18 1A 40 42 50 53 56 90 92
X_2	01 03 09 0B 18 1A 40 42 50 53 56 90 92
X_3	02 08 0A 10 18 1A 42 50 53 56 60 92 A0
X_4	02 08 0A 18 1A 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 (X_1-X_4), we improve Shor's lower bound to $\frac{13}{12}$.

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

$$01\ \ 07\ \ 0D\ \ 0E\ \ 82\ \ 84\ \ 86\ \ B1\ \ B2 \tag{4}$$

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

ID	Code	ID	Code
Y_1	00 30 32 34 36 80 B0	Y_{20}	20 32 34 36 58 A0 D0
Y_2	00 30 32 34 36 80 B3	Y_{21}	20 34 36 3A 50 A0 D0
Y_3	00 30 34 36 3A 80 B0	Y_{22}	20 34 36 3A 58 A0 D0
Y_4	00 30 34 36 3A 80 B3	Y_{23}	30 32 34 36 60 B0 E0
Y_5	00 31 33 35 37 80 B0	Y_{24}	30 32 34 36 60 B3 E0
Y_6	00 31 33 35 37 80 B3	Y_{25}	30 34 36 3A 60 B0 E0
Y_7	00 31 35 37 3B 80 B0	Y_{26}	30 34 36 3A 60 B3 E0
Y_8	00 31 35 37 3B 80 B3	Y_{27}	31 33 35 37 60 B0 E0
Y_9	00 32 34 36 38 80 B0	Y_{28}	31 33 35 37 60 B3 E0
Y_{10}	00 32 34 36 38 80 B3	Y_{29}	31 35 37 3B 60 B0 E0
Y_{11}	00 33 35 37 39 80 B0	Y_{30}	31 35 37 3B 60 B3 E0
Y_{12}	00 33 35 37 39 80 B3	Y_{31}	32 34 36 38 60 B0 E0
Y_{13}	00 34 36 38 3A 80 B0	Y_{32}	32 34 36 38 60 B3 E0
Y_{14}	00 34 36 38 3A 80 B3	Y_{33}	33 35 37 39 60 B0 E0
Y_{15}	00 35 37 39 3B 80 B0	Y_{34}	33 35 37 39 60 B3 E0
Y_{16}	00 35 37 39 3B 80 B3	Y_{35}	34 36 38 3A 60 B0 E0
Y_{17}	10 32 34 36 40 90 C0	Y_{36}	34 36 38 3A 60 B3 E0
Y_{18}	10 34 36 3A 40 90 C0	Y_{37}	35 37 39 3B 60 B0 E0
Y_{19}	20 32 34 36 50 A0 D0	Y_{38}	35 37 39 3B 60 B3 E0

Notice that code (Y_1) is Shor's code. We also ran a partial search for $n = 16$.

ID	Non-commutatively prefix bayonet code
Z_1	00 01 02 0B 0C 3B 3C 50 51 52 80 82 84 86 D0 D1 D2
Z_2	00 01 02 0B 0C 3B 3C 50 51 52 81 83 85 87 D0 D1 D2
Z_3	00 01 02 0B 0C 3B 3C 50 51 5A 80 82 84 86 D0 D1 D2
Z_4	00 01 02 0B 0C 3B 3C 50 51 5A 81 83 85 87 D0 D1 D2
Z_5	00 01 0A 0B 0C 3B 3C 50 51 52 80 82 84 86 D0 D1 D2
Z_6	00 01 0A 0B 0C 3B 3C 50 51 52 81 83 85 87 D0 D1 D2
Z_7	00 01 0A 0B 0C 3B 3C 50 51 5A 80 82 84 86 D0 D1 D2
Z_8	00 01 0A 0B 0C 3B 3C 50 51 5A 81 83 85 87 D0 D1 D2
Z_9	00 02 0B 0C 11 3B 3C 50 52 61 83 85 87 91 D0 D2 E1
Z_{10}	00 02 0B 0C 11 3B 3C 50 5A 61 83 85 87 91 D0 D2 E1
Z_{11}	01 02 03 0C 0D 3B 3C 50 51 52 80 82 84 86 D0 D1 D2
Z_{12}	01 02 03 0C 0D 3B 3C 50 51 52 81 83 85 87 D0 D1 D2
Z_{13}	01 02 03 0C 0D 3B 3C 50 51 5A 80 82 84 86 D0 D1 D2
Z_{14}	01 02 03 0C 0D 3B 3C 50 51 5A 81 83 85 87 D0 D1 D2
Z_{15}	01 02 0B 0C 0D 3B 3C 50 51 52 80 82 84 86 D0 D1 D2
Z_{16}	01 02 0B 0C 0D 3B 3C 50 51 52 81 83 85 87 D0 D1 D2
Z_{17}	01 02 0B 0C 0D 3B 3C 50 51 5A 80 82 84 86 D0 D1 D2
Z_{18}	01 02 0B 0C 0D 3B 3C 50 51 5A 81 83 85 87 D0 D1 D2
Z_{19}	01 02 0B 0C 10 3B 3C 51 52 60 82 84 86 90 D1 D2 E0
Z_{20}	01 02 0B 0C 10 3B 3C 51 5A 60 82 84 86 90 D1 D2 E0
Z_{21}	01 02 0B 0C 1D 3B 3C 51 52 60 82 84 86 90 D1 D2 E0
Z_{22}	01 02 0B 0C 20 3B 3C 51 52 70 82 84 86 A0 D1 D2 F0
Z_{23}	01 02 0B 0C 20 3B 3C 51 5A 70 82 84 86 A0 D1 D2 F0
Z_{24}	01 02 0B 0C 2D 3B 3C 51 52 70 82 84 86 A0 D1 D2 F0
Z_{25}	01 02 0B 0C 2D 3B 3C 51 5A 70 82 84 86 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.

$$01\ 02\ 03\ 0C\ 0D\ 3C\ 3D\ 51\ 52\ 5B\ 80\ 82\ 84\ 86\ D1\ D2\ D3\ G0 \tag{5a}$$

$$01\ 02\ 03\ 0C\ 0D\ 3C\ 3D\ 51\ 52\ 5B\ 81\ 83\ 85\ 87\ D1\ D2\ D3\ G0 \tag{5b}$$

$$01\ 02\ 03\ 0C\ 0D\ 3C\ 3D\ 51\ 52\ 5B\ 82\ 84\ 86\ 88\ D1\ D2\ D3\ G0 \tag{5c}$$

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 (pL, 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 $n \geq 2$,

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

is a factorisation of $\mathbb{Z}/8n\mathbb{Z}$ associated to the code (X_1). In general, the integer n such that there exists a factorisation of $\mathbb{Z}/n\mathbb{Z}$ associated to the code (X_1) 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 (X_1) where n is a multiple of 4 and not a multiple of 8.

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

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

is a factorisation of $\mathbb{Z}/8n\mathbb{Z}$ associated to the codes (Y_6, Y_8, Y_{10}, Y_{12}, Y_{14}, Y_{16}). 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 (Y_2) 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 $(L, 8R)$, $(L, 3R)$, and $(L, 5R)$ 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	$2\times 3\times 5\times k = 30k$, with $k \geq 3$
Y_5, Y_7, Y_9, Y_{11}, Y_{13}, Y_{15}	$2\times 3\times 11\times k = 66k$, with $k \geq 3$
Y_1, Y_3	$2\times 3\times 5\times 11\times k = 330k$, with $k \geq 4$
Z_1, Z_3, Z_5, Z_7	$2\times 3\times 5\times 13\times k = 390k$, with $k \geq 4$
Z_2, Z_4, Z_6, Z_8	$2\times 3\times 5\times 13\times k = 390k$, with $k \geq 3$
Z_9, Z_{10}	$2\times 5\times 13\times k = 130k$, 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 $(Z_9,\ Z_{10})$ then $(L, R-11)$ is a Sands factorisation.

The factorisations just take into account the words belonging to $ba^* \cup a^*b$. 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 $\{a^n\} \cup X$ 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 $X \subseteq a^{<n}ba^{<n}$ such that the square binary matrix $\mathcal{M}$ of size n defined by

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

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 $X \in a^{<n}ba^{<n}$, we call $\mathcal{G}_{\text{mod}}(X)$ the oriented graph defined by the set of vertices $[[n]]$ and by the edges

$$\boxed{i-k \bmod n} \longrightarrow \boxed{\ell - j \bmod n},$$

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

In the previous section, we show that the codes (X_1, Y_6, Y_8, Y_{10}, Y_{12}, Y_{14}, Y_{16}) 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 (X_1) 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 (Y_6, Y_8, Y_{10}, Y_{12}, Y_{14}, Y_{16}) 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 (X_1- X_4), then $X \cup \{a^{16}\}$ 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 (X_1- X_4). Then $X \cup \{a^{16}\}$ is a code. Moreover, we checked by an exhaustive search that X is not included in a complete 16-modular 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*

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

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 $a^{i_1}ba^{j_1}, \ldots, a^{i_m}ba^{j_m}, a^{k_1}ba^{\ell_1}, \ldots, a^{k_m}ba^{\ell_m} \in s_r(X)$, with $j_1 \neq \ell_1$ such that

$$\begin{cases} i_1 = k_1 \\ j_1 + i_2 = \ell_1 + k_2 \mod n \\ \vdots \\ j_{m-1} + i_m = \ell_{m-1} + k_m \mod n \\ j_m = \ell_m \end{cases}$$

By definition of $s_r(X)$, there exists $a^{i_1}ba^{p_1}, a^{q_1}ba^{j_1}, \ldots, a^{i_m}ba^{p_m}, a^{q_m}ba^{j_m} \in X$ and $a^{k_1}ba^{p'_1}, a^{q'_1}ba^{\ell_1}, \ldots, a^{k_m}ba^{p'_m}, a^{q'_m}ba^{\ell_m} \in X$ such that $p_t + q_t = p'_t + q'_t = r \mod n$, for all $t \in [m]$. Thus

$$\begin{cases} i_1 = k_1 \\ p_1 + q_1 = p'_1 + q'_1 \mod n \\ j_1 + i_2 = \ell_1 + k_2 \mod n \\ \vdots \\ j_{m-1} + i_m = \ell_{m-1} + k_m \mod n \\ p_m + q_m = p'_m + q'_m \mod n \\ j_m = \ell_m \end{cases}$$

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

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

Thus there exists $r_1 \in [[n]]$ such that $|s_{r_1}(X)| \geq \left\lceil \frac{|X|^2}{n} \right\rceil \geq n+1$. 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 $a^{<n}ba^{<n}$. □

[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.

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 α and β, 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*
$$\rho_q(X) := \left\{a^{qi \bmod n} b a^{qj \bmod n} : a^i b a^j \in X\right\}$$
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 α, $\beta \in [[n]]$, the graph $\mathcal{G}_{\mathrm{mod}}(\tau_{\alpha,\beta}(X))$ is equal to the graph $\mathcal{G}_{\mathrm{mod}}(X)$. 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 $qi \bmod n$ is a graph isomorphism from $\mathcal{G}_{\mathrm{mod}}(X)$ to $\mathcal{G}_{\mathrm{mod}}(\rho_q(X))$. 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 $\mathcal{G}_{\mathrm{mod}}(\iota(X))$ contains the paths
$$\boxed{0} \longrightarrow \boxed{i_1} \longrightarrow \boxed{i_2} \longrightarrow \cdots \boxed{i_m} \longrightarrow \boxed{0}$$
and
$$\boxed{0} \longrightarrow \boxed{-i_1 \bmod n} \longrightarrow \boxed{-i_2 \bmod n} \longrightarrow \cdots \boxed{-i_m \bmod n} \longrightarrow \boxed{0},$$
for $i_1, \ldots, i_m \in [[n]]$. Thus, the graph $\mathcal{G}_{\mathrm{mod}}(X)$ contains the path
$$\boxed{0} \longrightarrow \boxed{i_1} \longrightarrow \boxed{-i_2 \bmod n} \longrightarrow \boxed{i_3} \longrightarrow \boxed{-i_4 \bmod n} \longrightarrow \cdots \longrightarrow \boxed{0}$$
which contradicts the fact that X is an n-modular code. We conclude the proof by contraposition.

4. The graph $\mathcal{G}_{\mathrm{mod}}(\delta(X))$ is the graph $\mathcal{G}_{\mathrm{mod}}(X)$ 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 $r \in [[n]]$, $|s_r(X)| = n$. Assume that $|s_r(X)| \neq n$ for $r \in [[n]]$ then there exists an $r' \in [[n]]$ such that $|s_{r'}(X)| > n$ 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*

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

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 (X_1-X_4). 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 Jean-Christophe 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. RAIRO-Theoretical 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)