Factorizations of Cyclic Groups and Bayonet Codes

Christophe Cordero[*]

[*]Dipartimento di Informatica ed Applicazioni, Università di Salerno,
via Giovanni Paolo II 132, Fisciano, 84084, ITALY.

Nov 20, 2022

Abstract

We study the (variable-length) codes of the form $X \cup \{a^n\}$ where $X \subseteq a^*\omega a^*$ and $|X| = n$. We extend various notions and results from *factorizations of cyclic groups* theory to this type of codes.

In particular, when n is the product of at most three primes or has the form $p^k q$ (with p and q prime), we prove that they are composed of prefix and suffix codes. We provide counterexamples for other n. It implies that the long-standing *triangle conjecture* is true for this type of n. We also prove a conjecture about the size of a potential counterexample to the conjecture.

Introduction

Schützenberger founded and developed the theory of (variable-length) *codes* in the 1960s in order to study encoding problems raised by Shannon's information theory. Since then, the theory has undergone its own development and links with monoids, automata, combinatorics on words and factorizations of cyclic groups have emerged. We refer the reader to the book [BPR10] for an introduction to the theory of codes.

Let $\mathcal{A}$ be an alphabet containing letters a and b. A ***code*** is a subset $X \subseteq \mathcal{A}^*$ such that for all $t, t' \geq 0$ and $x_1, \ldots, x_t, y_1, \ldots, y_{t'} \in X$ the condition

$$x_1\, x_2\, \cdots\, x_t \;=\; y_1\, y_2\, \cdots\, y_{t'}$$

implies $t = t'$ and $x_i = y_i$, for $i = 1, \ldots, t$. For example, the set $\{aabb, abaaa, b, ba\}$ is not a code because

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

A straight forward way to create a code is to build a *prefix set* (respectively *suffix set*), which is a set of words such that none of its words is a prefix (resp. suffix) of another one. For example, the set

$$\{aaa, ab, aab, bba, ba\} \tag{1}$$

[*]ccordero@unisa.it

is prefix but not suffix. According to Proposition 2.1.9 from [BPR10], a prefix (resp. suffix) set different than $\{\varepsilon\}$ is a code, where ε is the empty word. Such codes are called ***prefix codes*** (resp. ***suffix codes***). So the set (1) is a prefix code.

Since any code is included in a ***maximal*** code (code that is not included in another code), most of the theory of codes is dedicated to the study of finite maximal codes.

One of the main conjecture about the characterization of finite maximal codes is the ***factorization conjecture*** from Schützenberger [Sch65]. This conjecture states that for any finite maximal code M, there exists finite sets $P, S \subseteq \mathcal{A}^*$ such that

$$\underline{M} - 1 = \underline{P}\,(\underline{\mathcal{A}} - 1)\,\underline{S}, \tag{2}$$

where given a set $X \subseteq \mathcal{A}^*$, we denote its formal sum

$$\sum_{x \in X} x$$

by $\underline{X}$. The best known result about the conjecture is from Reutenaeur [Reu85]. He proved that for any finite maximal code M, there exists polynomials $\underline{P}, \underline{S} \in \mathbb{Z}\langle\langle\mathcal{A}\rangle\rangle$ (the set of formal power series of $\mathcal{A}^*$ over $\mathbb{Z}$) such that (2).

During some unsuccessful attempts to prove the conjecture, Perrin and Schützenberger proposed an intermediate conjecture called the *triangle conjecture* [PS77b]. It is stated as follows: for any ***bayonet code*** X, i.e. for any code $X \subseteq a^*ba^*$, we have

$$|\{x \text{ such that } x \in X \text{ and } |x| \leq k\}| \leq k, \text{ for all } k \geq 0. \tag{3}$$

However, Shor found a counterexample [Sho85].

Since then, variants of the triangle conjecture have been proposed. In particular the one that we nowadays call, by an abuse of language, the ***triangle conjecture*** which suggests that any bayonet code X either satisfies the inequalities (3) or it is not included in a finite maximal code. This conjecture is implied by the factorization conjecture.

A stronger version of the triangle conjecture proposed by Zhang and Shum [ZS17] states that for all finite maximal codes M, $\omega \in \mathcal{A}^*$, and $k \geq 0$, we have

$$\left|\left\{a^i \omega a^j \text{ such that } a^i \omega a^j \in M^* \text{ and } i + j < k\right\}\right| \leq k.$$

In this paper, our main subject is the (subsets of) codes concerned by the triangle conjectures, which are the codes of the form

$$X \cup \{a^n\},$$

where $X \subseteq a^{\{0,1,\ldots,n-1\}}ba^{\{0,1,\ldots,n-1\}}$ and $|X| = n$, for a given $n \geq 1$. We call them n-***complete bayonet codes*** (cbc). ”Complete” refers to the fact that such a code cannot contain more elements, according to Proposition 2.1 of [DFR85]. We extend various notions and results from *factorizations of cyclic groups* theory to cbc. The framework we develop about cbc generalizes and simplifies the work recently made about the triangle conjectures such as [ZS17, ZS18, DF22] and allows us to improve the best known results.

In particular, when n is the product of at most three primes or has the form $p^k q$ with p and q prime (we call those numbers ***cbc Hajós numbers***), we prove that any code $X \cup \{a^n\}$, where $X \subseteq a^*\omega a^*$, $\omega \in \mathcal{A}^*$, and $|X| = n$, is a composition of prefix and suffix codes. We provide counterexamples in other cases. This implies that the Zhang and Shum conjecture and therefore the triangle conjecture is true for cbc Hajós numbers. Moreover, our Theorem 7.2 proves a conjecture about the size of a potential counterexample to the triangle conjectures and our Theorem 4.7 gives a structural property of codes satisfying the factorization conjecture.

Our paper is organized as follows. In the first section, we mostly introduce and recall some concepts that relate cbc to finite maximal codes. In the second section, we study some operations on cbc that, among others, lead to a criterion that a code must satisfies in order to be included in a finite maximal code. In the third section, we show that each cbc can be associated to a notion that we call *border*. This notion exhibits a link between *factorizations of cyclic groups* and cbc. We deduce from it a characteristic about finite maximal codes. Then we show various operations to build *borders* from others. In the fourth section, similarly to factorization theory, we introduce a *periodic* and a *Hajós* notion for cbc. Then we show that *Hajós cbc* are cbc bordered by a *Krasner factorization* which, in particular, provides a structural property of codes that satisfy the factorization conjecture. In the fifth section, we prove that any cbc of size n, where n is a cbc Hajós numbers, is of Hajós. We provide counterexamples in other cases. In the sixth section, we show that Hajós cbc are composed of prefix and suffix codes and thus are included in some finite maximal codes. We also deduce from it that the triangle conjectures are true for cbc Hajós numbers. In section seven, thanks to the framework on borders, we prove a conjecture about the size of a potential counterexample to the triangle conjecture. Finally, we conclude by exposing our main perspectives.

1 Complete Bayonet Code

It is well known[1] that for any finite maximal code M, there exists a unique integer n such that $a^n \in M$, it is called the ***order*** of the letter a. Most of the known characterizations of finite maximal codes are based on the order of one of its letter. Such as Restivo, Salemi, and Sportelli who have shown [RSS89] the following link between *factorizations* (*of cyclic groups*) and finite maximal codes.

Theorem 1.1. *If M is a finite maximal code such that $b, a^n \in M$ then the ordered pair*

$$\left(\left\{k,\, a^k b^+ \in M\right\}, \left\{k,\, b^+ a^k \in M\right\}\right)$$

is a factorization of size n.

We recall some basics notions about *factorizations*. However, we refer the reader to the books [Sza04, SS09] in order to find proofs of those recalls and for an introduction to the more general theory of factorizations of abelian groups. Given $P, Q \subseteq \mathbb{Z}$, an ordered pair (P, Q) is a ***factorization*** of size n if and only if for all $k \in [n]$ ($[n]$ denotes the set $\{0, 1, \ldots, n-1\}$), there exists a unique $(p, q) \in P \times Q$ such that $k = p + q$ in $\mathbb{Z}_n$ (the cyclic group of size n). In particular, n must be equal to $|P| \times |Q|$. For example, the ordered pair

$$(\{4, 5, 6, 7\}, \{1, 5\}) \tag{4}$$

[1] see, for example, Proposition 2.5.15 of [BPR10].

is a factorization of size 8. A factorization (P, Q) is called ***periodic*** with period $m \neq 0$ (in $\mathbb{Z}_n$), if P or Q is m-periodic in $\mathbb{Z}_n$, i.e. if

$$m + P = P \text{ or } m + Q = Q \text{ in } \mathbb{Z}_n.$$

For example, the factorization (4) is 4-periodic because $4 + \{1, 5\} = \{1, 5\}$ in $\mathbb{Z}_8$.

A factorization (P, Q) is said to be ***normalized*** if $0 \in P$ and $0 \in Q$. If (P, Q) is a (m-periodic) factorization then for any $p \in P$ and $q \in Q$,

$$(P - p, Q - q)$$

is a (m-periodic) normalized factorization.

We recall that given a factorization (P, Q) of size n, if P is periodic then the set made of its periods and 0, i.e.

$$\{m, m + P = P \text{ in } \mathbb{Z}_n\},$$

is a subgroup of $\mathbb{Z}_n$. Moreover, if P is m-periodic then $|Q|$ divides m. A set U is m-periodic in $\mathbb{Z}_n$ if and only if

$$U = \overline{U}^m + m\left[\frac{n}{m}\right] \quad \text{in } \mathbb{Z}_n,$$

where $\overline{U}^m$ denotes the set $\{\overline{u}^m, u \in U\}$ and where $\overline{u}^m$ denotes the remainder of the Euclidean division of u by m.

A factorization (P, Q) of size n is said to be of ***Hajós*** if and only if $n = 1$ or if P (respectively Q) is m-periodic and if

$$\left(\overline{P}^m, Q\right) \quad \left(\text{resp. } \left(P, \overline{Q}^m\right)\right)$$

is again a Hajós factorization of size m. All factorizations of size n where n is the product of at most four primes or a number of the form $p^k q$, where $k \geq 1$ and p, q are primes, are Hajós factorizations. Those numbers are called ***Hajós numbers***. Smallest non-Hajós factorizations are therefore of sizes 72 and 108 [SIa]. See [DB53] for such an example of non-Hajós factorization of size 72.

Thanks to Theorem 1.1, we can prove that the code

$$\left\{a^5, ab, b, baa\right\}, \tag{5}$$

found by Restivo [Res77], cannot be included in a finite maximal code because there is no factorization of the form

$$(\{0, 1\} \subseteq P, \{0, 2\} \subseteq Q),$$

where $|P| \times |Q| = 5$.

In this paper, we expose a deeper link between the theory of codes and factorizations, starting from the following notion introduced by Perrin and Schützenberger in [PS77a].

Definition 1.2. *Given a code M such that $a^n \in M$ and a word $\omega \in \mathcal{A}^*$, we set*

$$C_M(\omega) := \left\{a^{\overline{i}^n} b a^{\overline{j}^n} \text{ such that } a^i \omega a^j \in M^*\right\}. \tag{6}$$

For example, given the finite maximal code

$$E := \left\{b, ab, a^4, a^2ba, a^3b, a^2b^2\right\}, \tag{7}$$

we have

$$C_E(b) = \left\{b, ab, a^2ba, a^3b\right\} \text{ and } C_E(bb) = \left\{b, ab, a^2b, a^3b\right\}.$$

As shown in Proposition 2.2 of [ZS18], sets of type (6) form codes.

Proposition 1.3. *If M is a code containing a^n then for any $\omega \in \mathcal{A}^*$, the set*

$$\{a^n\} \cup C_M(\omega) \tag{8}$$

is a code.

Our statement is slightly different, we produce a straightforward proof.

Proof. Given a word ω and a code M containing a^n, if the set (8) is not a code then there exists

$$a^{i_1}\omega a^{j_1}, \ldots, a^{i_t}\omega a^{j_t}, a^{k_1}\omega a^{\ell_1}, \ldots, a^{k_t}\omega a^{\ell_t} \in M^*$$

such that $\overline{j_1}^n \neq \overline{\ell_1}^n$ and

$$a^{\overline{i_1}^n} ba^{\overline{j_1}^n} \ldots a^{\overline{i_t}^n} ba^{\overline{j_t}^n} \equiv_n a^{\overline{k_1}^n} ba^{\overline{\ell_1}^n} \ldots a^{\overline{k_t}^n} ba^{\overline{\ell_t}^n},$$

where $\equiv_n$ denotes the congruence over $\mathbb{Z}\langle\langle\mathcal{A}\rangle\rangle$ defined by the relation $a^n = \varepsilon$. Thus

$$a^{i_1}\omega a^{j_1} \ldots a^{i_t}\omega a^{j_t} \equiv_n a^{k_1}\omega a^{\ell_1} \ldots a^{k_t}\omega a^{\ell_t}.$$

Which implies that M is not a code since words from the non-empty set

$$(a^n)^* \left(a^{i_1}\omega a^{j_1}\right) (a^n)^* \ldots \left(a^{i_t}\omega a^{j_t}\right) (a^n)^* \cap (a^n)^* \left(a^{k_1}\omega a^{\ell_1}\right) (a^n)^* \ldots \left(a^{k_t}\omega a^{\ell_t}\right) (a^n)^*$$

can be decompose in two different ways. This ends the proof by contradiction. □

Perrin and Schützenberger introduced the notion (6) as a characterization of finite maximal codes.

Theorem 1.4. *If M is a finite code such that $a^n \in M$ then*

$$M \text{ is maximal} \iff \forall \omega \in \mathcal{A}^*, \quad |C_M(\omega)| = n. \tag{9}$$

The left to right implication of (9) is demonstrated as Proposition 12.2.4 in [BPR10] and the converse is true according to Theorem 2.5.13 of [BPR10]. The "finite" hypothesis is necessary because the code (5) of Restivo is contained in some infinite maximal codes and none of which verify (9) (in particular when $\omega = b$).

We now introduce the class of codes studied in this paper and which contains those of type (8).

Definition 1.5. *We call n-**complete bayonet code** (n-**cbc**) a set $X \subseteq a^{[n]}ba^{[n]}$ such that*

$$|X| = n \quad \text{and} \quad \{a^n\} \cup X \text{ is a code.}$$

Thus for any finite maximal code M containing a^n and for any word ω, the set $C_M(\omega)$ is an n-cbc. However, we do not know whether or not to any n-cbc X corresponds a finite maximal code M and a word ω such that $X = C_M(\omega)$. Lam has nevertheless shown [Lam97] that any cbc of the form $a^P ba^Q$, where (P, Q) is a Hajós factorization, is included in a finite maximal code. We improve this result in Theorem 6.2.

One of our main motivation is to study the *strong triangle conjecture* based on *triangle property.*

Definition 1.6. *We say that an n-cbc X satisfies the* ***triangle property*** *if*

$$|\{x \text{ such that } x \in X \text{ and } |x| \leq k\}| \leq k,$$

for all $k \in [n]$. The ***strong triangle conjecture*** *states that every cbc satisfy the triangle property.*

The strong triangle conjecture implies the Zhang and Shum conjecture and therefore the triangle conjecture.

2 Stability

In this section, we introduce and study some operations on cbc and their framework related to finite maximal codes. Firstly, we introduce a composition operation for cbc.

Definition 2.1. *Let X and Y be n-cbc, we set*

$$X \circ_r Y := \left\{a^i ba^\ell \text{ such that } a^i ba^j \in X,\, a^k ba^\ell \in Y, \text{and } \overline{j+k}^n = r\right\},$$

for any $r \in [n]$.

Example 2.2. *For any n-cbc X and $k \in [n]$,*

$$X \circ_k \left\{a^{\overline{k-i}^n} ba^i, i \in [n]\right\} = X.$$

The operations $(\circ_r)_{r \geq 0}$ are associative. Indeed, for any n-cbc X, Y, Z and $r_1, r_2 \in [n]$,

$$(X \circ_{r_1} Y) \circ_{r_2} Z \text{ and } X \circ_{r_1} (Y \circ_{r_2} Z)$$

are equal to

$$\left\{a^i ba^j \text{ such that } a^i ba^{j_1} \in X,\, a^{i_2} ba^{j_2} \in Y,\, a^{i_3} ba^j \in Z,\, \overline{j_1 + i_2}^n = r_1, \text{and } \overline{j_2 + i_3}^n = r_2\right\}.$$

However, the product of two n-cbc does not necessarily results in an n-cbc. For example,

$$\{b, ba\} \circ_0 \{b, ab\} = \{b\}.$$

We introduce the notion of *compatibility* as a framework that enables composition of cbc.

Definition 2.3. *A set $\mathcal{E}$ of n-cbc is said to be* ***compatible*** *if for all $X_1, \dots, X_{k+1} \in \mathcal{E}$ and $r_1, \dots, r_k \in [n]$,*

$$X_1 \circ_{r_1} X_2 \circ_{r_2} X_3 \cdots \circ_{r_k} X_{k+1}$$

is an n-cbc.

The compatibility of a set can be tested thanks to a graph algorithm. Given an integer $n \geq 1$ and a set $\mathcal{E}$ of bayonet codes, we denote by $\mathcal{G}_n(\mathcal{E})$ the directed graph made of the set of vertices $[n]$ and arrows from k_1 to k_2 if and only if there exists $X \in \mathcal{E}$ and two different words $a^{i_1}ba^{j_1}, a^{i_2}ba^{j_2} \in X$ such that

$$k_1 = \overline{i_1 - i_2}^{n} \text{ and } k_2 = \overline{j_2 - j_1}^{n}.$$

Proposition 2.4. *A set $\mathcal{E}$ of n-cbc is compatible if and only if the graph $\mathcal{G}_n(\mathcal{E})$ does* ***not*** *contain a non-empty path from 0 to 0.*

Proof. A set $\mathcal{E}$ of n-cbc is not compatible if and only if there exists $t > 1$, $X_1, \dots, X_t \in \mathcal{E}$, and

$$a^{i_1}ba^{j_1}, a^{k_1}ba^{\ell_1} \in X_1, \dots, a^{i_t}ba^{j_t}, a^{k_t}ba^{\ell_t} \in X_t \tag{10}$$

such that $j_1 \neq \ell_1$ and

$$a^{i_1}ba^{j_1}a^{i_2}ba^{j_2} \dots a^{i_t}ba^{j_t} \equiv_n a^{k_1}ba^{\ell_1}a^{k_2}ba^{\ell_2} \dots a^{k_t}ba^{\ell_t}. \tag{11}$$

Thus if $\mathcal{E}$ is not compatible then $\mathcal{G}_n(\mathcal{E})$ contains the path

$$\boxed{0 = \overline{i_1 - k_1}^{n}} \to \boxed{\overline{\ell_1 - j_1}^{n} = \overline{i_2 - k_2}^{n}} \to \cdots \to \boxed{\overline{\ell_{t-1} - j_{t-1}}^{n} = \overline{i_t - k_t}^{n}} \to \boxed{\overline{\ell_t - j_t}^{n} = 0}.$$

Conversely, for any path from 0 to 0 of length $t > 1$ in the graph $\mathcal{G}_n(\mathcal{E})$, there exists (10) such that the relation (11) is true. □

We can see $\mathcal{G}_n(\mathcal{E})$ as the superposition of graphs $\mathcal{G}_n(\{X\})$, where $X \in \mathcal{E}$. So in the particular case where $\mathcal{E}$ is a singleton, the graph $\mathcal{G}_n(\mathcal{E})$ is equivalent to the graph defined in Proposition 1 of [PS81][2] and equal to the graph $\mathcal{G}_{mod}$ of [Cor19b].

We introduce the *stable* notion as compatible sets closed under composition.

Definition 2.5. *A set $\mathcal{S}$ of n-cbc is* ***stable*** *if for all $X, Y \in S$ and $r \in [n]$,*

$$X \circ_r Y \in \mathcal{S}.$$

A stable set is therefore compatible. Given a set $\mathcal{E}$ of compatible cbc, we denote by $\mathcal{E}^\circ$ the smallest stable set (for inclusion) containing $\mathcal{E}$. We say that $\mathcal{E}^\circ$ is the stable of $\mathcal{E}$. For example, we obtain

$$\{C_E(b), C_E(bb)\}^\circ = \left\{C_E(b), C_E(bb), \left\{ba, aba, a^2b, a^3ba\right\}, \left\{ba, aba, a^2ba, a^3ba\right\}\right\}, \tag{12}$$

where E is the code (7).

We can associate stable sets to any finite maximal code.

[2] In Proposition 1 of [PS81], Perrin and Schützenberger defined a graph on sets of integers. They did not explain the link with theory of codes. However, one can understand it as an algorithm to test whether or not a set of the form $\{a^n\} \cup X$ (where $X \subseteq a^*ba^*$) is a code. Their graph is not equal to $\mathcal{G}_n(\{X\})$ in general but it also contains a non-empty path from 0 to 0 if and only if the considered set is not a code.

Proposition 2.6. *Let M be a finite maximal code, the sets*

$$\mathcal{C}_M := \{C_M(\omega),\, \omega \in \mathcal{A}^*\} \text{ and } \mathcal{C}'_M := \{C_M(\omega),\, \omega \in \mathcal{B}\,(a^*\mathcal{B})^*\}\,,$$

where $\mathcal{B}$ is the alphabet $\mathcal{A} \setminus \{a\}$, are stable.

Proof. Let M be a finite maximal code and n the order of a. According to Proposition 1.3, the set $\mathcal{C}_M$ (respectively $\mathcal{C}'_M$) is a set of n-cbc. Moreover, for all $C_1, C_2 \in \mathcal{C}_M$ (resp. $\mathcal{C}'_M$), there exists $\omega_1, \omega_2 \in \mathcal{A}^*$ (resp. $\mathcal{B}\,(a^*\mathcal{B})^*$) such that $C_1 = C(\omega_1)$ and $C_2 = C(\omega_2)$. For any $r \in [n]$, we have

$$C_1 \circ_r C_2 = C_M(\omega_1 a^{r+tn} \omega_2) \in \mathcal{C}_M \ \text{ (resp. } \mathcal{C}'_M)\,,$$

for $t \geq \frac{2}{n} \max\limits_{m \in M} \{|m|\} - \frac{r}{n}$. □

For example, we obtain that the set $\mathcal{C}'_E$ is equal to the set (12), when E is the set (7).

Proposition 2.6 thus gives a criterion that a code must satisfies in order to be included in a finite maximal code.

Example 2.7. *Suppose that the code*

$$\left\{a^5, ab, aba^2, a^2b^2, ab^2\right\} \tag{13}$$

is included in a finite maximal code M. One can notice that the code (13) *satisfies the necessary conditions implied by Theorem 1.4 and Proposition 1.3. For example, the codes*

$$\left\{ab, aba^2\right\} \subseteq C_M(b) \text{ and } \left\{a^2b, ab\right\} \subseteq C_M(bb) \tag{14}$$

are respectively included in the 5*-cbc*

$$\left\{ab, aba^2, ba^4, ba^3, ba\right\} \text{ and } \left\{a^2b, ab, a^4b, a^3b, b\right\}.$$

However, thanks to an exhaustive computer exploration of the (finite) set of 5*-cbc, we found, using the algorithm from Proposition 2.4, that none of the cbc containing* (14) *are compatible. Thus, according to Proposition 2.6, the code* (13) *is not included in a finite maximal code.*

3 Border

In this section, we first show that each stable set can be associated to a notion that we call *border*. It is a generalization of a notion originally introduced on codes satisfying the factorization conjecture in section 5.3 of [DF99b]. It exhibits a link between factorizations and stable sets. Secondly, we show various operations to build *borders* from others.

3.1 Definition and existence

Definition 3.1. *Given $P, Q \subseteq \mathbb{Z}$, we say that the ordered pair (P, Q) is a* ***border*** *of an n-cbc X if*

$$a^P \, \underline{X} \, a^Q \equiv_n a^{[n]} b a^{[n]} \quad \left(\equiv_n \sum_{i,j \in [n]} a^i b a^j \right).$$

More generally, we say that it is a border of a set of cbc if it borders each of its elements.

Example 3.2. *The ordered pair*

$$(\{2,4\}, \{0,2,4,6\}) \tag{15}$$

and the factorization (4) *are borders of the* 8*-cbc*

$$\left\{b, ba, aba^2, a^3ba^3, a^4b, a^4ba, a^5ba^2, a^7ba^7\right\}. \tag{16}$$

The factorization

$$(\{0\}, \{0,1,2,3\}) \tag{17}$$

is a border of the stable set (12)*.*

Given an n-cbc X, note that (P, Q) borders X if and only if (Q, P) borders its dual

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

and that a factorization (P, Q) borders $\{X\}^\circ$ if and only if

$$a^P \frac{1}{1 - \underline{X}} a^Q \equiv_n \underline{\mathcal{A}^*_{/a^n = \varepsilon}},$$

where $\mathcal{A}^*_{/a^n=\varepsilon}$ is the quotient of $\mathcal{A}^*$ by the relation $a^n = \varepsilon$.

We write $x \in_n X$ if and only if there exists $y \in X$ such that $x \equiv_n y$. For any $Y \subseteq a^*ba^*, n \geq 1$, and $k \in [n]$, we set

$$L^n_k(Y) := \left\{\bar{i}^n, \, a^i b a^k \in_n Y\right\}, \, L(Y) := \left\{\bar{i}^n, \, a^i b a^j \in Y\right\},$$

and

$$R^n_k(Y) := \left\{\bar{j}^n, \, a^k b a^j \in_n Y\right\}, \, R(Y) := \{R^n_k(Y), \, k \in L(Y)\}.$$

For example, $L(X) = \{0,1,3,4,5,7\}$ and $R(X) = \{\{0,1\}, \{2\}, \{3\}, \{7\}\}$ when X is (16). We say that an n-cbc X ***borders*** a set $\mathcal{E}$ if and only if for any $R \in R(X)$, the ordered pair $(R, L(X))$ is a factorization of size n that borders $\mathcal{E}$.

Proposition 3.3. *Any stable set is bordered by one of its elements.*

Proof. Let $\mathcal{S}$ be a stable set of n-cbc. If $Y \in \mathcal{S}$ does not borders $\mathcal{S}$ then there exists $i, j \in [n]$, $k \in L(Y)$, and $X \in \mathcal{S}$ such that

$$a^i b a^j \notin_n a^{R^n_k(Y)} \, X \, a^{L(Y)} \text{ or } a^i \notin_n a^{R^n_k(Y)} a^{L(Y)}.$$

Thus $Y' := Y \circ_i X \circ_j Y$ or $Y' := Y \circ_i Y$ is a cbc belonging to $\mathcal{S}$ such that $|L(Y')| < |L(Y)|$, because $k \in L(Y)$ and $k \notin L(Y')$.

The cardinality of a set being a positive integer, we obtain the expected result by iterating this process at most $|L(X)|$ times starting from any element X of $\mathcal{S}$. □

Thus any stable set admits a bordering factorization and conversely for any factorization, there exists a cbc that it borders. Indeed, a factorization (P, Q) borders the cbc $a^Q ba^P$.

It is possible to build, by compositions of elements of a compatible set, a cbc in a more restrictive form which borders the set.

Theorem 3.4. *Let $\mathcal{E}$ be a compatible set of n-cbc. For all $Z \in \mathcal{E}$, there exists $r_1, \ldots, r_k \in [n]$ and $X_1, \ldots, X_k \in \mathcal{E}$ such that the cbc*

$$X := Z \circ_{r_1} X_1 \circ_{r_2} \cdots \circ_{r_k} X_k$$

borders $\mathcal{E}$ and such that for all $R, R' \in R(X)$,

$$R \cap R' \neq \emptyset \implies R = R'.$$

Proof. Let $\mathcal{E}$ be a compatible set of cbc and $Y \in \mathcal{E}^\circ$ a cbc bordering $\mathcal{E}$. If there exists $r \in R \cap R'$, such that $R \neq R'$ and $R, R' \in R(Y)$ then for any $\ell \in L(Y)$, the cbc

$$Y' := Y \circ_{\overline{r+\ell}^n} Y$$

satisfies the facts that $R(Y')$ is strictly included in $R(Y)$ and that $L(Y') = L(Y)$. Thus $Y' \in \mathcal{E}^\circ$ and Y' also borders $\mathcal{E}$.

The set $R(X)$ of a cbc X cannot be empty, so we obtain the expected result by iterating this process at most $|R(Y)|$ times starting from a cbc Y given by Proposition 3.3. Moreover, according to the proof of Proposition 3.3, such Y can be chosen by starting from any $Z \in \mathcal{E}$. This concludes the proof. □

One of the consequences of Theorem 3.4 is that for any finite maximal code M containing a^n and any word $\omega_1 \in \mathcal{A}^*$, there exists a word $\omega \in \mathcal{A}^*$ such that

$$\underline{C_M\left(\omega_1 \omega\right)} \equiv_n \sum_{k \in [t]} a^{L_k} ba^{R_k},$$

where $R_i \cap R_j = \emptyset$ when $i \neq j$, and such that

$$(L_1 \sqcup \cdots \sqcup L_t, R_k)_{k \in [t]}$$

are factorizations bordering $\mathcal{C}_M$.

3.2 New borders from old ones

Being a border is closed under translations and multiplications.

Proposition 3.5. *If (P, Q) is a border of a cbc X then for all $i, j \in \mathbb{Z}$, d_1 prime to $|P|$, and d_2 prime to $|Q|$, the ordered pairs*

$$(P + i, Q + j) \text{ and } (d_1 P, d_2 Q)$$

are borders of X.

Proof. First, we recall some properties about factorizations. It is well known that for any $j \in \mathbb{Z}$, an ordered pair (P, Q) is a factorization of size n if and only if $(P, Q + j)$ is a factorization of size n, since for all $p_1, p_2 \in P$ and $q_1, q_2 \in Q$, we have

$$\overline{p_1 + (q_1 + j)}^n = \overline{p_2 + (q_2 + j)}^n \iff \overline{p_1 + q_1}^n = \overline{p_2 + q_2}^n.$$

Moreover, according to Proposition 3 of [San00], if (P, Q) is a factorization and d a number prime to $|Q|$ then the ordered pair (P, dQ) is a factorization.

An ordered pair (P, Q) borders an n-cbc X if and only if for any $k \in [n]$, the ordered pair

$$\left(R_k^n\left(a^P X\right), Q\right)$$

is a factorization of size n. Assume that (P, Q) borders X then, according to the previous recalls, for any $k \in [n]$, $j \in \mathbb{Z}$, and d prime to $|Q|$, the ordered pair

$$\left(R_k^n\left(a^P X\right), j + dQ\right)$$

is a factorization. Thus $(P, j + dQ)$ borders X. We obtain the expected result thanks to a symmetrical argument. □

In some cases, Proposition 3.5 enables to explicitly compute a border.

Proposition 3.6. *If an n-cbc X is bordered by (P, Q) such that $p := |P|$ is prime to $q := |Q|$ then the factorization*

$$(q\,[p]\,,\, p\,[q]) \tag{18}$$

borders X.

Proof. Assuming the hypotheses of the Proposition, the number q is prime to p so according to Proposition 3.5, the ordered pair (qP, Q) borders X. The set qP contains p distinct elements, all of which are multiples of q. Thus

$$qP = \{0, q, \ldots, q(p-1)\} = q\,[p]\,.$$

Symmetrically, we obtain that the ordered pair (18) borders X. Moreover, according to Bézout's identity [Béz79], there exists $u, v \in \mathbb{Z}$ such that $up + vq = 1$. Thus for all $k \in [n]$, we have

$$k = \overline{p(ku) + q(kv)}^n \in p\,[q] + q\,[p]\,.$$

Thus the ordered pair (18) is a factorization. □

The composition of cbc from a stable set brings out bordering factorizations.

Theorem 3.7. *Let $\mathcal{S}$ be a stable set of n-cbc and (P, Q) one of its borders. For all $k_1, k_2 \in [n]$ and $X, Y \in \mathcal{S}$, the ordered pairs*

$$\left(P,\, L_{k_2}^n\left(Y a^Q\right)\right),\ \left(R_{k_1}^n\left(a^P X\right),\, L_{k_2}^n\left(Y a^Q\right)\right),\ \textit{and}\ \left(R_{k_1}^n\left(a^P X\right),\, Q\right)$$

are factorizations bordering $\mathcal{S}$.

Proof. Assuming the hypotheses of the Theorem, if the ordered pair

$$\left(R^n_{k_1}\left(a^P X\right),\, L^n_{k_2}\left(Y a^Q\right)\right),\ \text{respectively}\ \left(P,\, L^n_{k_2}\left(Y a^Q\right)\right), \tag{19}$$

is not a factorization then there exists $i \in [n]$ which is not generated by the sum of its two components (modulo n) and thus

$$a^{k_1} b a^{k_2} \notin_n a^P X \circ_i Y a^Q, \text{resp. } a^i b a^{k_2} \notin_n a^P Y a^Q.$$

Thus (P, Q) is not a border of $\mathcal{S}$. Which contradicts the assumptions.

Likewise, if the ordered pair (19) does not borders $\mathcal{S}$ then there exists $Z \in \mathcal{S}$ and $i, j \in [n]$ such that

$$a^i b a^j \notin_n a^{R^n_{k_1}\left(a^P X\right)} Z a^{L^n_{k_2}\left(Y a^Q\right)}, \text{ resp. } a^i b a^j \notin_n a^P Z a^{L^n_{k_2}\left(Y a^Q\right)}.$$

Which implies that

$$a^{k_1} b a^{k_2} \notin_n a^P X \circ_i Z \circ_j Y a^Q, \text{ resp. } a^i b a^{k_2} \notin_n a^P Z \circ_j Y a^Q.$$

Thus (P, Q) does not borders $\mathcal{S}$. Which contradicts the assumptions.

We obtain the last case thanks to a symmetrical argument. □

4 Hajós cbc

In this section, similarly to factorization theory, we introduce a *periodic* and a *Hajós* notion for cbc and compatible sets. Then we show that this *Hajós* notion is equivalent as being bordered by a *Krasner factorization*.

4.1 Periodic cbc

We introduce an operation to build bigger cbc from a smaller one. Given a set

$$X := \left\{a^{i_1} b a^{j_1}, \ldots, a^{i_n} b a^{j_n}\right\} \subseteq a^{[n]} b a^{[n]}$$

and $t \geq 1$, we define the operation

$$H_t(X) := \left\{\bigsqcup_{\ell=1}^{n} \left\{a^{i_\ell + k_{\ell,1} n} b a^{j_\ell}, \ldots, a^{i_\ell + k_{\ell,t} n} b a^{j_\ell + (t-1)n}\right\}, k_{1,1}, \ldots, k_{n,t} \in [t]\right\}.$$

For example, the dual of (16) is equal to

$$\left\{\begin{array}{ll} a^{0+0\times 4} b a^{0} & a^{0+0\times 4} b a^{0+1\times 4} \\ a^{1+0\times 4} b a^{0} & a^{1+0\times 4} b a^{0+1\times 4} \\ a^{2+0\times 4} b a^{1} & a^{2+0\times 4} b a^{1+1\times 4} \\ a^{3+0\times 4} b a^{3} & a^{3+1\times 4} b a^{3+1\times 4} \end{array}\right\} \in H_2\left(\left\{b, ab, a^2 ba, a^3 ba^3\right\}\right). \tag{20}$$

We extend this operation to compatible sets. We write $\mathcal{E}' \in \mathcal{H}_t(\mathcal{E})$, where $t \geq 1$, if and only if

$$Y \in \mathcal{E}' \implies \exists X \in \mathcal{E} \text{ such that } Y \in H_t(X)$$

and

$$X \in \mathcal{E} \implies \exists Y \in \mathcal{E}' \text{ such that } Y \in H_t(X).$$

For example, if $\mathcal{S}$ is the stable set (12) associated to the code (7) then $\delta(\mathcal{S}) \in \mathcal{H}_4(\{\{b\}\})$, where $\delta(\mathcal{S})$ is the set $\{\delta(X), X \in \mathcal{S}\}$.

This operation preserve the fact of being a compatible set.

Proposition 4.1. *Given $t \geq 1$ and $\mathcal{E}' \in \mathcal{H}_t(\mathcal{E})$, the set $\mathcal{E}$ is a compatible set of n-cbc such that $\mathcal{E}^\circ$ is bordered by (P, Q) if and only if $\mathcal{E}'$ is a compatible set of nt-cbc such that $\mathcal{E}'^\circ$ is bordered by $(P + n[t], Q)$.*

Proof. Let $\mathcal{E}$ be a compatible set of n-cbc whose stable is bordered by (P, Q) and $\mathcal{E}' \in \mathcal{H}_t(\mathcal{E})$.

For all $Y_1, \ldots, Y_k \in \mathcal{E}'$, there exists $X_1, \ldots, X_k \in \mathcal{E}$ such that $Y_i \in H_t(X_i)$, when $i \in [1, k]$. Since

$$a^{n[t]}\underline{Y_i} \equiv_{nt} a^{n[t]}\underline{X_i}a^{n[t]}$$

for all $i \in [1, k]$, we have that

$$a^{P+n[t]}\underline{Y_1}\cdots\underline{Y_k}a^Q \equiv_{nt} a^{P+n[t]}\left(\underline{X_1}a^{n[t]}\right)\cdots\left(\underline{X_k}a^{n[t]}\right)a^Q. \tag{21}$$

Moreover, according to the hypothesis,

$$a^P\underline{X_1}\cdots\underline{X_k}a^Q \equiv_n \left(a^{[n]}b\right)^k a^{[n]} \tag{22}$$

and since for all i, j,

$$a^i \equiv_n a^j \iff a^{i+n[t]} \equiv_{nt} a^{j+n[t]}, \tag{23}$$

we have that

$$a^{P+n[t]}\left(\underline{X_1}a^{n[t]}\right)\cdots\left(\underline{X_k}a^{n[t]}\right)a^Q \equiv_{nt} \left(a^{[n]+n[t]}b\right)^k a^{[n]+n[t]} \equiv_{nt} \left(a^{[nt]}b\right)^k a^{[nt]} \tag{24}$$

and thus

$$a^{P+n[t]}\underline{Y_1}\cdots\underline{Y_k}a^Q \equiv_{nt} \left(a^{[nt]}b\right)^k a^{[nt]}. \tag{25}$$

This shows that $\mathcal{E}'$ is a compatible set of nt-cbc whose stable is bordered by $(P + n[t], Q)$.

Conversely, let $\mathcal{E}'$ be a compatible set of nt-cbc whose stable is bordered by $(P + n[t], Q)$ and such that $\mathcal{E}' \in \mathcal{H}_t(\mathcal{E})$. For all $X_1, \ldots, X_k \in \mathcal{E}$, there exists $Y_1, \ldots, Y_k \in \mathcal{E}'$ such that $Y_i \in H_t(X_i)$, when $i \in [1, k]$. We have by hypothesis (25) and (21) thus (24). We apply (23) to (24) in order to get (22).

This concludes the proof. □

We introduce a periodic notion for cbc and compatible sets.

Definition 4.2. *We say that Y is n-**right-periodic** if there exists an n-cbc X and $t > 1$, such that $Y \in H_t(X)$ and we say that Y is n-**periodic** if Y or $\delta(Y)$ is n-**right-periodic**.*

*More generally, we say that a compatible set is n-**right-periodic** if all its elements are n-right-periodic.*

For example, the cbc (16) is 4-periodic since

$$\left\{b, ab, a^2ba, a^3ba^3\right\} \tag{26}$$

is an 4-cbc and (20).

Remark 4.3. *Note that if Y is an n-**right-periodic** nt-cbc then $Y \in H_t\left(\overline{Y}^n\right)$, where*

$$\overline{Y}^n = \left\{a^{\overline{i}^n} b a^{\overline{j}^n},\, a^i b a^j \in Y\right\}.$$

The next proposition links periodicity of factorizations to periodicity of compatible sets.

Proposition 4.4. *Let $\mathcal{E}$ be a compatible set of nt-cbc such that $\mathcal{E}^\circ$ is bordered by $(P + n\,[t]\,, Q)$. If for all $k \in [nt]$ and $Y \in \mathcal{E}$, the sets*

$$R_k^{nt}\left(a^P Y\right) \tag{27}$$

are n-periodic in $\mathbb{Z}_{nt}$ then $\mathcal{E}$ is n-right-periodic.

Proof. For all $Y \in \mathcal{E}$, if the sets (27) are n-periodic then

$$a^{P+n[t]}Y \equiv_{nt} a^{P+n[t]}\overline{Y}^n a^{n[t]} \tag{28}$$

is unambiguous and thus $\left|\overline{Y}^n\right| = n$. Moreover, if $a^{i+k_1 n}ba^j, a^{i+k_2 n}ba^j \in Y$, where $i < n$ and $k_1, k_2 < t$, then for any $p \in P$,

$$a^{p+k_2 n}a^{i+k_1 n}ba^j \equiv_{nt} a^{p+k_1 n}a^{i+k_2 n}ba^j$$

and since (28) is ambiguous it implies that $k_1 = k_2$. Thus if $a^iba^j \in \overline{Y}^n$ then there exists $k_1, \ldots k_t \in [t]$ such that

$$\left\{a^{i+k_1 n}ba^j, \ldots, a^{i+k_t n}ba^{j+(t-1)n}\right\} \subseteq Y.$$

Therefore $Y \in H_t\left(\overline{Y}^n\right)$.

Moreover, according to Proposition 4.1, $\overline{Y}^n$ is an n-cbc. So Y (and thus $\mathcal{E}$) is n-right-periodic. This concludes the proof. □

We define a *Hajós* notion for cbc as composition of periodic cbc. Formally, we denote by H_n the set of ***Hajós cbc*** of size n that we recursively define as follows:

$$H_n := \begin{cases} \{\{b\}\} & \text{if } n = 1, \\ \bigcup\limits_{\substack{n=tm,\, t>1, \\ X \in H_m}} \delta\left(H_t\left(X\right)\right) \cup H_t\left(X\right) & \text{otherwise.} \end{cases}$$

Since $\{b\}$ is an 1-cbc then, according to Proposition 4.1, a Hajós cbc is a cbc. For example, the cbc (16) is a Hajós cbc since (20) and the dual of (26) is equal to

$$\left\{a^{0+0\times 1}ba^0, a^{0+0\times 1}ba^{0+1\times 1}, a^{0+1\times 1}ba^{0+2\times 1}, a^{0+3\times 1}ba^{0+3\times 1}\right\} \in H_4\left(\{b\}\right).$$

We extend the Hajós notion to compatible sets. A compatible set $\mathcal{E}$ is said to be of ***Hajós*** if and only if there exists $t_1, \ldots, t_k > 1$ and some cbc $Y_1, \ldots, Y_{k-1}$ such that for all $Y \in \mathcal{E}$ or for all $Y \in \delta\left(\mathcal{E}\right)$,

$$Y \in H_{t_k}\left(Y_{k-1}\right), \delta\left(Y_{k-1}\right) \in H_{t_{k-1}}\left(Y_{k-2}\right), \ldots, \delta\left(Y_2\right) \in H_{t_2}\left(Y_1\right), \delta\left(Y_1\right) \in H_{t_1}\left(\{b\}\right).$$

Note that, according to Remark 4.3, we necessarily have $Y_i = \overline{Y}^{t_1 \cdots t_i}$, for all $1 \leq i < k$. In particular, $\mathcal{E}$ is of Hajós if and only if $\delta\left(\mathcal{E}\right)$ is of Hajós.

4.2 Krasner border

We first do some recalls about *Krasner factorizations.* An ordered pair (P, Q) is a ***Krasner factorization*** (of size $n := |P| \times |Q|$) if and only if for all $k \in [n]$, there exists $p \in P$ and $q \in Q$ such that

$$k = p + q.$$

For example, the ordered pair (17) is a Krasner factorization of size 4.

Krasner factorizations are completely described in [KR37]. For all $t_1, \ldots, t_k > 1$, the ordered pairs (U, V) and (V, U), where

$$U := \sum_{i\in[1,k],\, 2|i} t_1 \ldots t_{i-1} [t_i] \text{ and } V := \sum_{i\in[1,k],\, 2\nmid i} t_1 \ldots t_{i-1} [t_i], \tag{29}$$

are Krasner factorizations of size $t_1 \cdots t_k$. Conversely, any Krasner factorization can be built that way.

Krasner factorizations naturally appear in the factorization conjecture as shown in [DF99b] and in Proposition 3.6 of [DF22].

Proposition 4.5. *If a finite maximal code M satisfies the factorization conjecture then the set $\mathcal{C}_M$ is bordered by a Krasner factorization.*

Our statement is slightly different, we provide a straightforward proof.

Proof. If a finite maximal code M satisfies the factorization conjecture then there exists $P, S \subseteq \mathcal{A}^*$ such that

$$\underline{P}\,\underline{M}^*\,\underline{S} = \underline{\mathcal{A}}^*. \tag{30}$$

The restriction of (30) to words without letter b, implies that there exists $P_0 \subseteq P$ and $S_0 \subseteq S$ such that (P_0, S_0) is a Krasner factorization of size n, where $a^n \in M$. If (P_0, S_0) does not borders $\mathcal{C}_M$ then there exists $\omega \in \mathcal{A}^*$, $a^{i_1+nk_1}\omega a^{n\ell_1+j_1}, a^{i_2+nk_2}\omega a^{n\ell_2+j_2} \in M^*, p_1, p_2 \in P_0$, and $s_1, s_2 \in S_0$ such that

$$a^{p_1} (a^n)^{k_2} a^{i_1+nk_1}\omega a^{n\ell_1+j_1} (a^n)^{\ell_2} a^{s_1} = a^{p_2} (a^n)^{k_1} a^{i_2+nk_2}\omega a^{n\ell_2+j_2} (a^n)^{\ell_1} a^{s_2}, \tag{31}$$

where $i_1, i_2, j_1, j_2 \in [n]$. Thus the coefficient of (31) in $\underline{P_0}\,\underline{M}^*\underline{S_0}$ is greater or equal to 2. Which contradicts the factorization conjecture. □

According to Theorem 3.2 of [DF99a], a factorization (P, Q) is of Hajós if and only if there exists a Krasner factorization (U, V) such that (U, Q) and (P, V) are factorizations. Our next Theorem shows a equivalent result for compatible sets. We will use the following Lemma according to the proof of Theorem 4.13 of [SS09].

Lemma 4.6. *Let (U, V) be a Krasner factorization of size n. If U is an m-periodic set then for any factorization (P, V) of size n, the set P is m-periodic.*

Theorem 4.7. *A compatible set is of Hajós if and only if its stable is bordered by a Krasner factorization.*

Proof. We prove by recurrence on n that any compatible set of n-cbc whose stable is bordered by a Krasner factorization is of Hajós. First, note that the unique (non-empty) compatible set of 1-cbc is $\{\{b\}\}$ and that it is of Hajós.

Assume now that any compatible set of j-cbc (where $j < n$) whose stable is bordered by a Krasner factorization is of Hajós. Let $\mathcal{E}$ be a compatible set of n-cbc whose stable is bordered by a Krasner factorization (U, V). We can assume that $n = t_1 \cdots t_k$, where $t_i > 1$ (for $i \in [1, k]$), and that (U, V) is equal to (29) (otherwise, we can consider $\delta(\mathcal{E})$ instead of $\mathcal{E}$).

If k is even (respectively odd) then U (resp. V) is $t_1 \cdots t_{k-1}$-periodic and for any $X \in \mathcal{E}$ and $\ell \in [n]$,

$$\left(R_\ell^n\left(a^U X\right), V\right) \quad \left(\text{resp. } \left(U, L_\ell^n\left(X a^V\right)\right)\right)$$

is a factorization. Moreover according to Lemma 4.6, we know that

$$R_\ell^n\left(a^U X\right) \quad \left(\text{resp. } L_\ell^n\left(X a^V\right)\right)$$

is also $t_1 \cdots t_{k-1}$-periodic.

Thus according to Proposition 4.4, $\mathcal{E} \in \mathcal{H}_{t_k}(\mathcal{E}')$ (resp. $\delta(\mathcal{E}) \in \mathcal{H}_{t_k}(\mathcal{E}')$), where $\mathcal{E}'$ is a compatible set of $t_1 \cdots t_{k-1}$-cbc whose stable is bordered by the Krasner factorization (U, V), where k is decremented (i.e. $k \leftarrow k - 1$). Thanks to the recurrence hypothesis, $\mathcal{E}'$ is of Hajós thus $\mathcal{E}$ is also of Hajós.

The converse is a straight forward recurrence. Indeed, $\{\{b\}\}$ is bordered by the Krasner factorization $(\{0\}, \{0\})$ and, according to Proposition 4.1, if $\mathcal{E}$ is a compatible set of n-cbc whose stable is bordered by a Krasner factorization (U, V) then $\mathcal{E}' \in \mathcal{H}_t(\mathcal{E})$ (resp. $\delta(\mathcal{E}') \in \mathcal{H}_t(\delta(\mathcal{E}))$) is bordered by the Krasner factorization $(U + n[t], V)$ (resp. $(U, V + n[t])$). □

According to Theorem 4.7 and its constructive proof, we know that given a stable set $\mathcal{S}$ (such as $\mathcal{C}_M$, when M is a code that satisfies the factorization conjecture) bordered by a Krasner factorization (U, V) (we can suppose that it is equal to (29) and that k is even, the others cases are similar), we have

$$Y \in H_{t_k}(Y_{k-1}), \ \delta(Y_{k-1}) \in H_{t_{k-1}}(Y_{k-2}), \ \ldots, \delta(Y_2) \in H_{t_2}(Y_1), \ \delta(Y_1) \in H_{t_1}(\{b\}),$$

for all $Y \in \mathcal{S}$, where $Y_i = \overline{Y}^{t_1 \cdots t_i}$.

5 Cbc Hajós numbers

In this section, we fully characterize ***cbc Hajós numbers***. They are numbers n such that every compatible sets of n-cbc are of Hajós. This is sum up in Theorem 5.12.

5.1 Hajós cases

It is well known in theory of factorizations of abelian groups that given a factorization (P, Q) such that $|P|$ is a power of a prime then either P or Q is periodic. See for example Theorem 6.1.1 from [SS09]. Inspired by Proposition 3.1 from [Sza15], we prove the following slightly stronger result for the particular case of cyclic groups.

Proposition 5.1. *If (P, Q_1) and (P, Q_2) are factorizations of size n such that $|P|$ is a power of a prime then either P is periodic or Q_1 and Q_2 share a common period.*

In order to prove it, we will use the following lemma stated as Theorem 5.5 in [SS09].

Lemma 5.2. *If (P, Q) is a normalized factorization of size n and $|P| = p^\alpha q^\beta$, where p, q are primes and $\alpha, \beta \geq 0$, then either $\langle P \rangle$ (the subgroup generated by P) is not equal to $\mathbb{Z}_n$ or $\langle Q \rangle \neq \mathbb{Z}_n$.*

Proof of Proposition 5.1. We prove it by a recurrence on n. We can suppose that (P, Q_1) and (P, Q_2) are normalized factorizations of size n and that $|P| = p^\alpha$, where p is prime and $\alpha \geq 0$.

If $|P| = 1$ then $P = \{0\}$ and $Q_1 = Q_2 = [n]$ (in $\mathbb{Z}_n$) and thus they verify the proposition. Symmetrically, if $|Q_1| = |Q_2| = 1$ then $P = [n]$ (in $\mathbb{Z}_n$) and $Q_1 = Q_2 = \{0\}$ and thus the proposition is satisfied.

Suppose that the proposition is true for every factorizations of size $k < n$. According to Lemma 5.2 either $\langle P \rangle \neq \mathbb{Z}_n$ or $\langle Q_1 \rangle \neq \mathbb{Z}_n$ and $\langle Q_2 \rangle \neq \mathbb{Z}_n$. In the first case, there exists a prime $t \,|\, n$ such that $P \subseteq t\mathbb{Z}$. According to Lemma 2.4 from [SS09], for all $q_1 \in Q_1$ and $q_2 \in Q_2$,

$$\left(\frac{1}{t}P, \frac{1}{t}\left((Q_i - q_i) \cap t\mathbb{Z}\right)\right) \qquad \text{(where } i = 1, 2) \tag{32}$$

are normalized factorizations of size $\frac{n}{t}$.

By recurrence hypothesis, either $\frac{1}{t}P$ is periodic in $\mathbb{Z}_{\frac{n}{t}}$ and thus P is periodic in $\mathbb{Z}_n$ or the right sides of (32) share a common period g in $\mathbb{Z}_{\frac{n}{t}}$. For the second case, we have that

$$tg \in \bigcap_{q_j \in Q_i} (Q_i - q_j)\,,$$

for $i = 1, 2$. Thus tg is a common period of Q_1 and Q_2 in $\mathbb{Z}_n$ according to Lemma 2.8 from [SS09].

Last case occurs when $\langle P \rangle = \mathbb{Z}_n$ and thus $\langle Q_1 \rangle \neq \mathbb{Z}_n$. There exists a prime $t \,|\, n$ such that $Q_1 \subseteq t\mathbb{Z}$. If $t \neq p$ then $tP + Q_1 \subseteq t\mathbb{Z} \neq \mathbb{Z}_n$ which contradicts Proposition 3 from [San00]. Thus $t = p$ and $Q_1 \subseteq p\mathbb{Z}$. We also get $Q_2 \subseteq p\mathbb{Z}$ with the same argument.

As similar as before, for all $p_j \in P$,

$$\left(\frac{1}{p}\left((P - p_j) \cap p\mathbb{Z}\right), \frac{1}{p}Q_i\right) \qquad \text{(where } i = 1, 2) \tag{33}$$

are normalized factorizations of size $\frac{n}{p}$. By recurrence hypothesis, either $\frac{1}{p}Q_1$ and $\frac{1}{p}Q_2$ share a commune period in $\mathbb{Z}_{\frac{n}{p}}$, and thus Q_1 and Q_2 share a commune period in $\mathbb{Z}_n$, or the left sides of (33) are periodic in $\mathbb{Z}_{\frac{n}{p}}$.

For the second case, since their cardinalities are powers of p then they share a common period g in $\mathbb{Z}_{\frac{n}{p}}$ (take g as the maximum of their periods, for example). Thus, we have that

$$pg \in \bigcap_{p_j \in P} (P - p_j)\,.$$

So pg is a period of P in $\mathbb{Z}_n$, according to Lemma 2.8 from [SS09]. This concludes the proof. □

We extend Proposition 5.1 to compatible sets.

Theorem 5.3. *If $\mathcal{E}$ is a compatible set of cbc such that its stable is bordered by (P, Q) where $|P|$ is a power of a prime then $\mathcal{E}$ is of Hajós.*

Proof. We prove it by recurrence. Let $\mathcal{E}$ be a compatible set of n-cbc whose stable is bordered by (P, Q). If $|P| = 1$ (resp. $|Q| = 1$) then the Krasner factorization $(\{0\}, [n])$ (resp. $([n], \{0\})$) borders $\mathcal{E}^\circ$ and thus $\mathcal{E}$ is of Hajós according to Theorem 4.7.

Suppose that the proposition is true for every compatible set of i-cbc, where $i < n$. Let

$$\mathcal{L} := \{Q\} \cup \left\{L_k^n\left(Xa^Q\right), k \in [n], X \in \mathcal{E}\right\}$$

and

$$\mathcal{R} := \{P\} \cup \left\{R_k^n\left(a^P X\right), k \in [n], X \in \mathcal{E}\right\}.$$

For any $L \in \mathcal{L}, R \in \mathcal{R}$, the ordered pair (R, L) is a factorization where $|R|$ is a power of a prime thus, according to Proposition 5.1, either elements of $\mathcal{L}$ or elements of $\mathcal{R}$ share a common period. In first case (resp. second), according to Proposition 4.4, there exists a compatible set $\mathcal{E}'$ and $t > 1$ such that $\delta(\mathcal{E}) \in \mathcal{H}_t(\mathcal{E}')$ (resp. $\mathcal{E} \in \mathcal{H}_t(\mathcal{E}')$). Thanks to the recurrence hypothesis, $\mathcal{E}'$ is of Hajós thus $\mathcal{E}$ is also of Hajós according to Proposition 4.1. □

Theorem 5.3 provides two straight forward corollaries that characterize cbc Hajós numbers.

Corollary 5.4. *If n is the product of at most three primes (eventually equal) then it is a cbc Hajós number.*

Proof. Let $\mathcal{E}$ be a compatible set of n-cbc, where n is the product of at most three primes. According to Theorem 3.4, $\mathcal{E}^\circ$ is bordered by a factorization (P, Q). Since $n = |P| \times |Q|$, either $|P|$ or $|Q|$ is equal to 1 or a prime thus $\mathcal{E}$ is of Hajós according to Theorem 5.3. This concludes the proof. □

Corollary 5.5. *Numbers of the form $p^k q$, where $k \geq 0$ and p, q are primes, are cbc Hajós numbers.*

Proof. Let $\mathcal{E}$ be a compatible set of $p^k q$-cbc, where $k \geq 0$ and p, q are primes. According to Theorem 3.4, $\mathcal{E}^\circ$ is bordered by a factorization (P, Q). Since $p^k q = |P| \times |Q|$, either $|P|$ or $|Q|$ is a power of p thus $\mathcal{E}$ is of Hajós according to Theorem 5.3. This concludes the proof. □

Hajós characterization provides some simple enumerative formulas.

Example 5.6. *Given a prime number p, we can enumerate and count p-cbc which are also Hajós cbc of size p, according to Corollary 5.4. We have that*

$$|H_p| = |H_p(\{b\})| + |\delta(H_p(\{b\}))| - |H_p(\{b\}) \cap \delta(H_p(\{b\}))|.$$

We first enumerate the set $H_p(\{b\})$ which is equal to

$$\left\{\left\{a^{k_1}b, a^{k_2}ba, \ldots, a^{k_p}ba^{p-1}\right\}, k_1, \ldots, k_p \in [p]\right\}.$$

Thus $|H_p(\{b\})| = p^p$. Similarly, we have $|\delta(H_p(\{b\}))| = p^p$. Moreover, their meet is equal to

$$\left\{\left\{a^0ba^{\sigma_1-1}, a^1ba^{\sigma_2-1}, \ldots, a^{p-1}ba^{\sigma_p-1}\right\}, \sigma \in \mathfrak{S}_p\right\}, \tag{34}$$

where $\mathfrak{S}_p$ is the group of permutations of size p. Thus the cardinal of (34) is equal to $p!$. Finally, we have the formula

$$|H_p| = 2p^p - p!.$$

5.2 Non-Hajós cases

In this section, we prove that numbers not concerned by Corollaries 5.4 and 5.5 are not cbc Hajós numbers.

Proposition 5.7. *Non-Hajós numbers are non-cbc Hajós numbers.*

Proof. Let n be a non-Hajós number and (P, Q) be a non-Hajós factorization of size n. Suppose that the n-cbc a^Pba^Q is of Hajós then it is bordered by a Krasner factorization (U, V), according to Theorem 4.7. The ordered pairs (U, P) and (Q, V) must be factorizations and thus, according to Theorem 3.2 of [DF99a], (P, Q) must be a Hajós factorization which is a contradiction. Thus n is a non-cbc Hajós number. □

Even if the numbers $p_1^2q_1^2, p_1p_2q_1^2$, and $p_1p_2q_1q_2$ (when p_1, p_2, q_1, q_2 are distinct primes) are of Hajós, we prove in this section that there are not cbc Hajós numbers.

We set for the rest of this section, the ordered pairs (L, R_1) and (L, R_2), where

$$L := p_1p_2[q_1] + q_1q_2[p_1], R_1 := p_1p_2q_1[q_2] + p_1[p_2], R_2 := p_1q_1q_2[p_2] + q_1[q_2],$$

and p_1, p_2, q_1, q_2 are primes such that $p_1p_2 \wedge q_1 = q_1q_2 \wedge p_1 = 1$. For example, if $p_1 = 2, p_2 = 2, q_1 = 3$, and $q_2 = 3$ then

$$\begin{array}{rclcl} L &=& \{0,4,8\} + \{0,9\} &=& \{0,4,8,9,13,17\}, \\ R_1 &=& \{0,12,24\} + \{0,2\} &=& \{0,2,12,14,24,26\}, \\ R_2 &=& \{0,18\} + \{0,3,6\} &=& \{0,3,6,18,21,24\}. \end{array}$$

First, we prove that those ordered pairs are factorizations of size $n := p_1p_2q_1q_2$.

Proposition 5.8. *The ordered pairs (L, R_1) and (L, R_2) are factorizations.*

Proof. The sum $L + R_1$ is equal to

$$p_1[p_2] + p_1p_2[q_1] + p_1p_2q_1[q_2] + q_1q_2[p_1] = p_1[p_2q_1q_2] + q_1q_2[p_1]$$

Since $q_1q_2 \wedge p_1 = 1$ then $q_1q_2[p_1]$ is equal to $[p_1]$ in Z_{p_1}. So $L + R_1$ is equal to

$$p_1[p_2q_1q_2] + [p_1] = [n]$$

in Z_n. Thus (L, R_1) is a factorization.

Similar argument can be applied to (L, R_2). □

Now, we study their periodicity.

Proposition 5.9. *The sets R_1 and R_2 are periodic in Z_n without common period and L is not periodic in Z_n.*

Proof. By definition, R_1 and R_2 are periodic in $\mathbb{Z}_n$ with respectively period $p_1p_2q_1$ and $p_1q_1q_2$. Since $|R_1| = |R_2| = p_2q_2$, if R_1 and R_2 share a common period then either R_1 or R_2 has period p_1q_1. Suppose that p_1q_1 is a period of R_1 then $R_1 = p_1q_1\,[p_2q_2]$ in $\mathbb{Z}_n$, which is impossible since $p_1 = 0 + p_1 \in R_1$ and $p_1 \notin p_1q_1\,[p_2q_2] = R_1$. Similarly, we prove that p_1q_1 is not a period of R_2. Thus R_1 and R_2 are periodic in Z_n without common period.

Suppose that L is periodic in $\mathbb{Z}_n$ with period g. Since $|L| = p_1q_1$, $g \in \{p_2q_2, p_2q_2p_1, p_2q_2q_1\}$. If $g = p_2q_2$ then $L = p_2q_2\,[p_1q_1]$ in $\mathbb{Z}_n$ but $q_1q_2 \in L$ and $q_1q_2 \notin p_2q_2\,[p_1q_1]$ thus $g \neq p_2q_2$. Moreover, since for all $k \in [p_1]$, $p_1 \wedge q_2q_1k = 1$ then there is no L' such that $L = L' + p_2q_2p_1\,[q_1]$ and thus $g \neq p_2q_2p_1$. Similarly, we prove that $g \neq p_2q_2q_1$.

This concludes the proof. □

We build a cbc over theses factorizations. Let Y be a cbc

$$\sum_{\ell \in L} a^{\ell} b a^{D_\ell},$$

where $D_{(l \in L)} \in \{R_1, R_2\}$ and where $\ell_1, \ell_2 \in L$ be such that $D_{\ell_1} = R_1$ and $D_{\ell_2} = R_2$.

Proposition 5.10. *The set Y is a non-Hajós cbc.*

Proof. Suppose that Y is a Hajós cbc then it is bordered by a Krasner factorization (U, V). In particular, (U, L), (R_1, V), and (R_2, V) must be factorizations. According to Theorem 3.2 of [DF99a], (U, L) is of Hajós and since L is not periodic then U is periodic. Moreover, according to Lemma 4.6, the sets U, R_1, and R_2 must share a common period which is contradicted by Proposition 5.9. □

Proposition 5.10 implies that numbers of the form $p_1^2q_1^2, p_1p_2q_1^2$, and $p_1p_2q_1q_2$, where p_1, p_2, q_1, q_2 are distinct primes, are of non-cbc Hajós numbers.

Example 5.11. *According to Proposition 5.10, the 36-cbc*

$$\left\{a^{36}\right\} \cup ba^{\{0,2,12,14,24,26\}} \cup a^{\{4,8,9,13,17\}}ba^{\{0,3,6,18,21,24\}}$$

is not of Hajós. Similarly to Proposition 5.10, we can show that the code

$$\left\{a^{36}\right\} \cup a^{\{0,4,8,9,13,17\}}ba^{\{0,2,12,14,24,26\}} \cup a^{\{0,4,8,9,13,17\}}ca^{\{0,3,6,18,21,24\}}$$

over the alphabet $\{a, b, c\}$ is not of Hajós. If one of them is included in a finite maximal code then it would not be bordered by a Krasner factorization and thus it would provide a counterexample to the factorization conjecture.

Thanks to Corollaries 5.4 and 5.5 and Propositions 5.7 and 5.10, we conclude this section by providing the exhaustive list of cbc Hajós numbers.

Theorem 5.12. *Cbc Hajós numbers are product of at most three primes or numbers of the form p^kq, where $k \geq 0$ and p, q are primes.*

Smallest non-cbc Hajós numbers are therefore $2^23^2 = 36$, $2^23 \times 5 = 60$, and $2^33^2 = 72$. It is referred as sequence A320632 in [SIb].

6 Prefix-suffix codes

We recall that given two codes C_1 and C_2 over the alphabet $\mathcal{A}$, the code C_1 is said to be a ***composition*** of C_2 if and only if C_1 is a code over the alphabet C_2 (i.e. $C_1 \subseteq {C_2}^*$). For example, the code

$$\{aa, ab, abbab, bbaa\} \tag{35}$$

is a composition of the code $\{aa, ab, b\}$ since it is equal to

$$\{aa, ab, (ab)\,(b)\,(ab)\,, (b)\,(b)\,(aa)\}\,.$$

Of course, a code is always a composition of himself and of its alphabet.

We recall that according to Proposition 2.6.1 from [BPR10], if C_2 is a code (over $\mathcal{A}$) and C_1 is a code over C_2 then C_1 is a code over $\mathcal{A}$. A code C_1 is recursively said to be a ***prefix-suffix*** code over C_2 if it is equal to C_2 or if it is a prefix or suffix code over a *prefix-suffix* code over C_2. For example, the code (35) is a prefix code over

$$\{aa, ab, abb, bb\}$$

which is a suffix code over

$$\{aa, ab, b\}$$

which is again a prefix code over $\mathcal{A}$. Thus (35) is a prefix-suffix code (over $\mathcal{A}$). We simply say *prefix-suffix code* when it is a prefix-suffix code over $\mathcal{A}$. Prefix-suffix codes are included in finite maximal codes according to Corollary 1 from [RSS89].

We have the following proposition, inspired by Lemmas 3.3 and 3.4 from [Lam97].

Lemma 6.1. *If C is a code containing a^n then for any $i_1(\omega), \dots, i_t(\omega), j_1(\omega), \dots, j_t(\omega) \geq 0$, where $\omega \in C \setminus \{a^n\}$, the set*

$$\left\{a^{nt}\right\} \cup \bigsqcup_{\omega\in C\setminus a^n} \left\{a^{ni_1(\omega)}\omega a^{ntj_1(\omega)}, a^{ni_2(\omega)}\omega a^{n(1+tj_2(\omega))}, \dots, a^{ni_t(\omega)}\omega a^{n(t-1+tj_t(\omega))}\right\} \tag{36}$$

is a prefix-suffix code over C.

Proof. The set

$$\left\{(a^n)^t\right\} \cup \bigsqcup_{\omega\in C\setminus a^n} \left\{(a^n)^{i_1(\omega)}\,\omega, (a^n)^{i_2(\omega)}\,\omega\,(a^n)\,, \dots, (a^n)^{i_t(\omega)}\,\omega\,(a^n)^{t-1}\right\} \tag{37}$$

is a suffix code over the code C and

$$\left\{a^{nt}\right\} \cup \bigsqcup_{\omega\in C\setminus a^n} \left\{\left(a^{ni_1(\omega)}\omega\right)\left(a^{nt}\right)^{j_1(\omega)}, \left(a^{ni_2(\omega)}\omega a^n\right)\left(a^{nt}\right)^{j_2(\omega)}, \dots, \left(a^{ni_t(\omega)}\omega a^{n(t-1)}\right)\left(a^{nt}\right)^{j_t(\omega)}\right\}$$

is a prefix code over the code (37). Thus the code (36) is a prefix-suffix code over C. □

We deduce from this lemma a theorem about completion.

Theorem 6.2. *Let $\mathcal{E}$ be a Hajós compatible set of n-cbc, where $n > 1$, and $C := \{a, \omega_1, \ldots, \omega_k\}$ a prefix-suffix code. For any $X_1, \ldots, X_k \subseteq a^*ba^*$ such that $\overline{X_1}^n, \ldots, \overline{X_k}^n \in \mathcal{E}$, the set*

$$\{a^n\} \cup \bigsqcup_{i=1}^{k} X_i[b \leftarrow \omega_i], \tag{38}$$

where $X[b \leftarrow \omega]$ is the set of words X whose letters b are replaced by word ω, is a prefix-suffix code and thus it is included in a finite maximal code.

Proof. We prove it by a recurrence on n.

Since $\mathcal{E}$ is of Hajós then there exists a compatible set $\mathcal{E}'$ of m-cbc such that $n = mt, t > 1$, and $\mathcal{E} \in \mathcal{H}_t(\mathcal{E}')$ or $\delta(\mathcal{E}) \in \mathcal{H}_t(\mathcal{E}')$. We can assume that $\mathcal{E} \in \mathcal{H}_t(\mathcal{E}')$, the other case is similar. Therefore, for all $X_1, \ldots, X_k \in \mathcal{E}$, there exists $Y_1, \ldots, Y_k \in \mathcal{E}'$ such that $X_i \in H_t(Y_i)$ for all $i \in [1, k]$.

If $m = 1$ then $X_i \in H_t(\{b\})$, for all $i \in [1, k]$. Moreover, since C is a prefix-suffix code then according to Proposition 6.1, the set (38) is also a prefix-suffix code.

Otherwise (when $m > 1$) we can assume, by recurrence hypothesis, that

$$\{a^m\} \cup \bigsqcup_{i=1}^{k} Y_i[b \leftarrow \omega_i]$$

is a prefix-suffix code and thus according to Proposition 6.1, the set (38) is also a prefix-suffix code. □

Theorem 3.2 from [Lam97] is the particular case of Theorem 6.2 where $C = \{a, b\}$ and $\mathcal{E}$ is made of one cbc of the form $a^P ba^Q$. Note that our alphabet $\mathcal{A}$ does not have to be binary.

Our next corollary is a small step towards the inclusion problem.

Corollary 6.3. *Let n be a cbc Hajós number, $\omega \in \mathcal{A}^* \setminus a^*$, and $X \subseteq a^*\omega a^*$. Considering the set $\{a^n\} \cup X$, the following statements are equivalent:*

1. *it is included in a finite maximal code,*
2. *$C_X(\omega)$ is included in an n-cbc,*
3. *$C_X(\omega)$ is included in an n-Hajós cbc,*
4. *it is a prefix-suffix code.*

Proof. Statement 1 implies Statement 2 according to the recalls made in Section 1 and Statement 2 implies Statement 3 since n is a cbc Hajós number.

Suppose that Statement 3 is true. Let Y be a Hajós cbc that contains $C_X(\omega)$. The set $\{a, \omega\}$ is a code since $\omega \in \mathcal{A}^* \setminus a^*$ and it is prefix-suffix because any code with two elements is prefix-suffix according to Theorem 3 from [RSS89]. Thus according to Theorem 6.2,

$$\{a^n\} \cup X \subseteq \{a^n\} \cup Y[b \leftarrow \omega]$$

is a prefix-suffix code. This proves that Statement 3 implies Statement 4.

We recall that Statement 4 implies Statement 1 according to Corollary 1 from [RSS89]. □

For example, the code

$$\{aaab, aaba, b, ba\} \tag{39}$$

is not prefix-suffix (we do not prove it, we just did a computer check). Thus if it is included in a finite maximal code then it would not be bordered by a Krasner factorization and thus it would provides a counterexample to the factorization conjecture. Such a code would contain a word of the form a^n where n is a non-cbc Hajós number, in particular $n \geq 36$.

Remark 6.4. *There is a converse to Theorem 6.2. Indeed, any prefix-suffix code is included in a prefix-suffix finite maximal code. Such a code, let call it M, satisfies the factorization conjecture, according to Proposition 14.1.2 from [BPR10]. Thus according to Proposition 4.5, C_M is bordered by a Krasner factorization and thus it is of Hajós according to Theorem 4.7.*

Next Theorem provides the best known bound for (the strong version of) the long-standing *triangle conjecture.*

Theorem 6.5. *The strong triangle conjecture is true for the particular cases where n is a cbc Hajós number.*

Proof. If X is an n-cbc where n is a cbc Hajós number then it is prefix-suffix according to Theorem 6.2. Moreover, according to Example 14.6.1 and Proposition 14.6.3 from [BPR10], any prefix-suffix cbc verifies the triangle property. □

According to Theorem 6.5, the strong triangle conjecture (and thus the Zhang and Shum conjecture) is, in particular, true when $n < 36$.

7 Not commutatively prefix bayonet codes

In this section, we prove a conjecture about the size of a potential counterexample to the triangle conjecture.

A list of codes that do not verify the original triangle conjecture[3] is exhibit in [Cor19b, Cor19a], they are called ***not commutatively prefix*** bayonet codes. We recall that if one of those is included in a finite maximal code then the triangle conjecture and the factorization conjecture are false. And a necessary condition for a bayonet code to be included in a finite maximal code is to be included in a cbc.

The following conjecture about the divisibility of n such that an n-cbc contains a given bayonet code is proposed in [Cor19b].

Conjecture 7.1. *For any n-cbc X and d prime to n, the set*

$$\varphi_d(X) := \left\{ a^i b a^{\overline{dj}^n} \text{ such that } a^i b a^j \in X \right\}$$

is an n-cbc.

We prove a stronger version of this conjecture.

[3] the first counterexample was found by Shor, as recalled in the introduction.

Theorem 7.2. *Let $\mathcal{E}$ be a compatible set of n-cbc such that $\mathcal{E}^\circ$ is bordered by (P,Q). For any $X \in \mathcal{E}$, d_1 prime to $|Q|$, and d_2 prime to $|P|$, the set*

$$\{\varphi_{d_1,d_2}(X)\} \cup \mathcal{E},$$

where

$$\varphi_{d_1,d_2}(X) := \left\{ a^{\overline{d_1 i}^n} b a^{\overline{d_2 j}^n} \text{ such that } a^i b a^j \in X \right\},$$

is a compatible set of n-cbc and its stable is bordered by (P,Q).

Proof. We prove by a recurrence on k the following property: for all $X_1, \ldots, X_j \in \mathcal{E} \cup \{\varphi_d(X)\}$ such that

$$|\{X_i \text{ such that } i \in [1,j] \text{ and } X_i = \varphi_d(X)\}| \leq k,$$

we have

$$a^P \underline{X_1} \cdots \underline{X_j} a^Q \equiv_n \left(a^{[n]} b\right)^j a^{[n]}.$$

It is true for $k = 0$ because $\mathcal{E}$ is a compatible set whose stable is bordered by (P,Q). Suppose now that it is true for k. Let $X_1, \ldots, X_j \in \mathcal{E} \cup \{\varphi_d(X)\}$ be such that

$$|\{X_i \text{ such that } i \in [1,j] \text{ and } X_i = \varphi_d(X)\}| = k+1$$

and let ℓ be

$$\min\{i \text{ such that } X_i = \varphi_d(X)\}.$$

By recurrence hypothesis,

$$a^P \underline{X_1} \cdots \underline{X_{\ell-1}}\, \underline{X}\, \underline{X_{\ell+1}} \cdots \underline{X_j} a^Q \equiv_n \left(a^{[n]} b\right)^j a^{[n]}$$

thus for all $i, i_1, \ldots, i_{\ell-1} \in [n]$,

$$\left(R_i^n \left(a^P X_1 \circ_{i_1} \cdots X_{\ell-1} \circ_{i_{\ell-1}} X\right), Q\right)$$

are borders of $\mathcal{E}^\circ$. According to Proposition 3.5, for all $i, i_1, \ldots, i_{\ell-1} \in [n]$ and d prime to $|P|$,

$$\left(dR_i^n \left(a^P X_1 \circ_{i_1} \cdots X_{\ell-1} \circ_{i_{\ell-1}} X\right), Q\right)$$

are also borders of $\mathcal{E}^\circ$. So

$$\left(R_i^n \left(a^P X_1 \circ_{i_1} \cdots X_{\ell-1} \circ_{i_{\ell-1}} \varphi_d(X)\right), Q\right)$$

are borders of $\mathcal{E}^\circ$ and thus

$$a^P \underline{X_1} \cdots \underline{X_j} a^Q \equiv_n \left(a^{[n]} b\right)^j a^{[n]}.$$

Thus the proposition is true for $k+1$. This proves that $\mathcal{E} \cup \{\varphi_d(X)\}$ is a compatible set. We obtain the expected result by duality. □

Theorem 7.2 does imply Conjecture 7.1 because according to Proposition 3.3, for any n-cbc X, there exists an ordered pair (P,Q) which borders $\{X\}^\circ$ and any number prime to $n = |P| \times |Q|$ is also prime to $|P|$ and $|Q|$.

Theorem 7.2 allows us to compute some lower bounds about potential counterexamples to the triangle conjecture.

Example 7.3. *According to [Cor19b], one of the four smallest (for cardinality) not commutatively prefix bayonet codes is*

$$T := \left\{b, ba^2, ba^8, ba^{10}, aba^8, aba^{10}, a^4b, a^4ba^2, a^5b, a^5ba^3, a^5ba^6, a^9b, a^9ba^2\right\}.$$

We already know[4]*, thanks to computer exploration and factorization theory, that if T is included in an n-cbc then $n = 4k$, where $k \geq 8$.*

We note that

$$\left(ba^{2\times 2}\right)(b) = (b)\left(a^4b\right) \text{ and } \left(a^5ba^{3\times 3}\right)(b) = \left(a^5b\right)\left(a^9b\right)$$

thus $\mu_{1,2}(T)$ and $\mu_{1,3}(T)$ are not codes, where

$$\mu_{d_1,d_2}(T) := \left\{a^{d_1 i}ba^{d_2 j} \text{ such that } a^iba^j \in T\right\}.$$

Likewise, we note that $\mu_{2,1}(T)$ and $\mu_{3,1}(T)$ are not codes. Thus according to Theorem 7.2, if T is included in an n-cbc X then any border (P, Q) of $\{X\}^\circ$ is such that $2\times 3 \mid |P|$ and $2\times 3 \mid |Q|$, thus $36 \mid n$.

Similar argument can be applied to others known not commutatively prefix bayonet codes.

Conclusion and perspectives

We conclude this article by exposing our main perspectives. We do not conjecture that the general case of the strong triangle conjecture is true. We believe that techniques developed in order to build non-Hajós factorizations and non-*Rédei* factorizations such as in [San07] could be useful to create counterexamples to the strong triangle conjecture. Since every counterexample of the (Zhang and Shum) triangle conjecture must contain a counterexample to the strong triangle conjecture, we believe that it is an intermediate step in order to find a counterexample to the triangle conjecture (if it exists).

Our second perspective is the converse of Proposition 4.5, we wounder if every finite maximal codes bordered by Krasner factorizations satisfy the factorization conjecture. Thanks to the characterization provided by Theorem 4.7, we are more confident about a positive answer. If it is the case then results about the triangle conjecture from Theorem 6.5 could be extend to the factorization conjecture.

References

[Béz79] Etienne Bézout. *Théorie générale des équations algébriques.* de l'imprimerie de Ph.-D. Pierres, rue S. Jacques, 1779.

[BPR10] Jean Berstel, Dominique Perrin, and Christophe Reutenauer. *Codes and automata*, volume 129. Cambridge University Press, 2010.

[Cor19a] Christophe Cordero. *Explorations combinatoires des structures arborescentes et libres.* PhD thesis, Paris Est, 2019.

[4] see section 3.1 of [Cor19b]

[Cor19b] Christophe Cordero. A note with computer exploration on the triangle conjecture. *International Conference on Language and Automata Theory and Applications*, pages 409–420, 2019.

[DB53] Nicolaas Govert De Bruijn. On the factorization of cyclic groups. *Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen: Series A: Mathematical Sciences*, 61(4):370–377, 1953.

[DF99a] Clelia De Felice. Hajós factorizations of cyclic groups-a simpler proof of a characterization. *Journal of Automata Languages and Combinatorics*, 4:111–116, 1999.

[DF99b] Clelia De Felice. On a property of the factorizing codes. *International Journal of Algebra and Computation*, 9(03n04):325–345, 1999.

[DF22] Clelia De Felice. Finite maximal codes and factorizations of cyclic groups. *https://arxiv.org/abs/2202.09675*, 2022.

[DFR85] Clelia De Felice and Antonio Restivo. Some results on finite maximal codes. *RAIRO. Informatique théorique*, 19(4):383–403, 1985.

[KR37] Marc Krasner and Britt Ranulac. Sur une propriété des polynômes de la division du cercle. *CR Acad. Sci. Paris*, 240:397–399, 1937.

[Lam97] Nguyen Huong Lam. Hajós factorizations and completion of codes. *Theoretical Computer Science*, 182(1):245–256, 1997. URL: `https://www.sciencedirect.com/science/article/pii/S0304397597000327`, `doi:https://doi.org/10.1016/S0304-3975(97)00032-7`.

[PS77a] Dominique Perrin and Marcel-Paul Schützenberger. Codes et sous-monoïdes possédant des mots neutres. *Theoretical Computer Science*, pages 270–281, 1977.

[PS77b] Dominique Perrin and Marcel-Paul Schützenberger. Un problème élémentaire de la théorie de l'information. *Théorie de l'Information*, pages 249–260, 1977.

[PS81] Dominique Perrin and Marcel-Paul Schützenberger. A conjecture on sets of differences of integer pairs. *J. Comb. Theory, Ser. B*, 30(1):91–93, 1981.

[Res77] Antonio Restivo. On codes having no finite completions. *Discrete Mathematics*, 17(3):309–316, 1977.

[Reu85] Christophe Reutenauer. Noncommutative factorization of variable-length codes. *Journal of Pure and Applied Algebra*, 36:167–186, 1985.

[RSS89] Antonio Restivo, Sergio Salemi, and Tecla Sportelli. Completing codes. *RAIRO-Theoretical Informatics and Applications*, 23(2):135–147, 1989.

[San00] Arthur D Sands. Replacement of factors by subgroups in the factorization of abelian groups. *Bulletin of the London Mathematical Society*, 32(3):297–304, 2000.

[San07] Arthur D Sands. A question concerning the factorization of cyclic groups. *International Journal of Algebra and Computation*, 17(08):1573–1575, 2007.

[Sch65] Marcel-Paul Schützenberger. Codes à longueur variable, cours à l'école d'été de l'otan sur les méthodes combinatoires en théorie du codage. *Royan, France*, 1965.

[Sho85] Peter W Shor. A counterexample to the triangle conjecture. *Journal of Combinatorial Theory, Series A*, 38(1):110–112, 1985.

[SIa] Neil J. A. Sloane and The OEIS Foundation Inc. Sequence A102562. *The on-line encyclopedia of integer sequences.* URL: `http://oeis.org/A102562`.

[SIb] Neil J. A. Sloane and The OEIS Foundation Inc. Sequence A320632. *The on-line encyclopedia of integer sequences.* URL: `http://oeis.org/A320632`.

[SS09] Sándor Szabó and Arthur D Sands. *Factoring groups into subsets.* Chapman and Hall/CRC, 2009.

[Sza04] Sándor Szabó. *Topics in factorization of abelian groups.* Springer, 2004.

[Sza15] Sándor Szabó. Cyclic groups with hajos property, an elementary approach. *Journal of Algebra and Its Applications*, 2015.

[ZS17] Liang Zhang and Kar-Ping Shum. Finite maximal codes and triangle conjecture. *Discrete Mathematics*, 340(3):541–549, 2017.

[ZS18] Liang Zhang and Kar-Ping Shum. Finite maximal codes related to triangular conjecture. *researchgate.net*, 2018.