A Note with Computer Exploration on the Triangle Conjecture

Christophe Cordero

Université Paris-Est Marne-la-Vallée
Laboratoire d'Informatique Gaspard-Monge

29 mars 2019

Introduction to Coding Theory

Variable-length code:

$$\mathcal{S} \longrightarrow \mathcal{T}$$

Introduction to Coding Theory

Variable-length code:

$$\mathcal{S} \longrightarrow \mathcal{T}$$

Table	
11	a
10001	b
01	c
$\vdots$	

Introduction to Coding Theory

Variable-length code:

$$\mathcal{S} \xrightarrow[\cdots|11|10001|01|01|11]{\hspace{6cm}} \mathcal{T}$$

Table	
11	a
10001	b
01	c
$\vdots$	

Introduction to Coding Theory

Variable-length code:

$$\mathcal{S} \xrightarrow[\cdots|11|10001|01|01|11]{} \mathcal{T}$$

Table	
11	*a*
10001	*b*
01	*c*
⋮	

Difficulty: the frame must be uniquely decomposable!

Code

Definition

A set $X \subset \mathcal{A}^*$ is a **code** if and only if for all $\omega \in X^*$ there exist a unique $n \geq 0$ and a unique sequence $x_1, \ldots, x_n \in X$ such that

$$\omega = x_1 \, x_2 \, \cdots \, x_n.$$

Code

Definition

A set $X \subset \mathcal{A}^*$ is a **code** if and only if for all $\omega \in X^*$ there exist a unique $n \geq 0$ and a unique sequence $x_1, \ldots, x_n \in X$ such that

$$\omega = x_1 \, x_2 \, \cdots \, x_n.$$

Example

The set $\{aabb, abaaa, b, ba\}$ is not a code because

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

Prefix Code

Definition

A set $X \subset \mathcal{A}^*$ is **prefix** if no element of X is a proper prefix of another element in X.

Prefix Code

Definition

A set $X \subset \mathcal{A}^*$ is **prefix** if no element of X is a proper prefix of another element in X.

Example

The set $\{b, ab, a^2b, a^3b, a^4b, \dots\}$ is prefix.

Prefix Code

Definition

A set $X \subset \mathcal{A}^*$ is **prefix** if no element of X is a proper prefix of another element in X.

Example

The set $\{b, ab, a^2b, a^3b, a^4b, \ldots\}$ is a prefix code.

Proposition

A prefix set different than $\{\varepsilon\}$ is a code.

Commutatively Prefix Conjecture

Definition

A set $X \subset \mathcal{A}^*$ 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.

Commutatively Prefix Conjecture

Definition

A set $X \subset \mathcal{A}^*$ 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.

Example

The set

$$\{a, ba, aabb, baabb, ababb\}$$

is commutatively prefix.

Commutatively Prefix Conjecture

Definition

A set $X \subset \mathcal{A}^*$ 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.

Example

The set

$$\{a, ba, aabb, baabb, ababb\}$$

is commutatively prefix, because it is equivalent to the prefix code

$$\{a, ba, bbaa, bbaba, bbbaa\}.$$

Commutatively Prefix Conjecture

Definition

A set $X \subset \mathcal{A}^*$ 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.

Example

The set

$$\{a, ba, aabb, baabb, ababb\}$$

is commutatively prefix, because it is equivalent to the prefix code

$$\{a, ba, bbaa, bbaba, bbbaa\}.$$

Conjecture from Perrin and Schützenberger (1965)

All finite maximal codes are commutatively prefix.

Triangle Conjecture

Definition

A **bayonet** code X is a code such that $X \subset a^* b a^*$.

Triangle Conjecture

Definition

A **bayonet** code X is a code such that $X \subset a^* b a^*$.

Example

The set $\{ab, abaa, aaaab\}$ is a bayonet code.

Triangle Conjecture

Definition

A **bayonet** code X is a code such that $X \subset a^* b a^*$.

Example

The set $\{ab, abaa, aaaab\}$ is a bayonet code.

Triangle conjecture (Perrin and Schützenberger)

A finite bayonet code is either commutatively prefix or it is not included in a finite maximal code.

Non-Commutatively Prefix Bayonet Code

(Well known) Proposition

A bayonet code X is commutatively prefix if and only if

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

Non-Commutatively Prefix Bayonet Code

(Well known) Proposition

A bayonet code X is commutatively prefix if and only if

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

Example

In 1984, Shor found the bayonet code

$$\begin{array}{lllll}
\{ \quad b, & ba, & ba^7, & ba^{13}, & ba^{14}, \\
a^3b, & a^3ba^2, & a^3ba^4, & a^3ba^6, & \\
a^8b, & a^8ba^2, & a^8ba^4, & a^8ba^6, & \\
a^{11}b, & a^{11}ba, & a^{11}ba^2 & \} &
\end{array}$$

with 16 elements and included in $\mathcal{A}^{\leq 15}$. Hence, it is a <u>non-commutatively prefix code</u>.

Non-Commutatively Prefix Bayonet Code

(Well known) Proposition

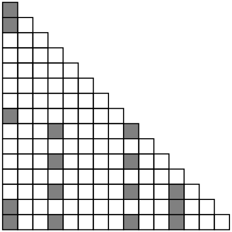
A bayonet code X is commutatively prefix if and only if

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

Example

In 1984, Shor found the bayonet code

$$\left\{ \begin{array}{ccccc} b, & ba, & ba^7, & ba^{13}, & ba^{14}, \\ a^3b, & a^3ba^2, & a^3ba^4, & a^3ba^6, & \\ a^8b, & a^8ba^2, & a^8ba^4, & a^8ba^6, & \\ a^{11}b, & a^{11}ba, & a^{11}ba^2 & & \end{array} \right\} \leftrightarrow$$



with 16 elements and included in $\mathcal{A}^{\leq 15}$. Hence, it is a non-commutatively prefix code.

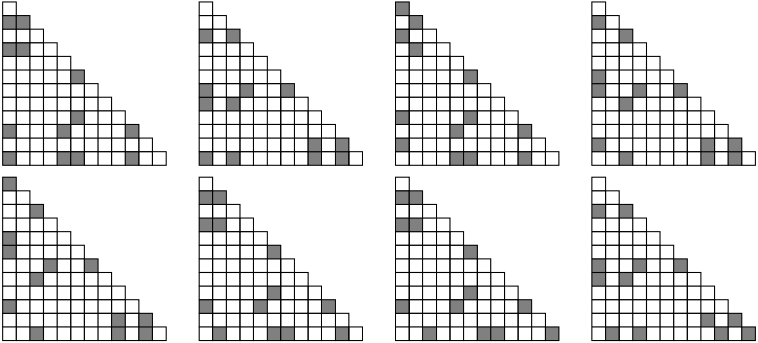
Results of the Computer Exploration

$\underline{n \leq 11}$: 0 code.

Results of the Computer Exploration

$n \leq 11$: 0 code.

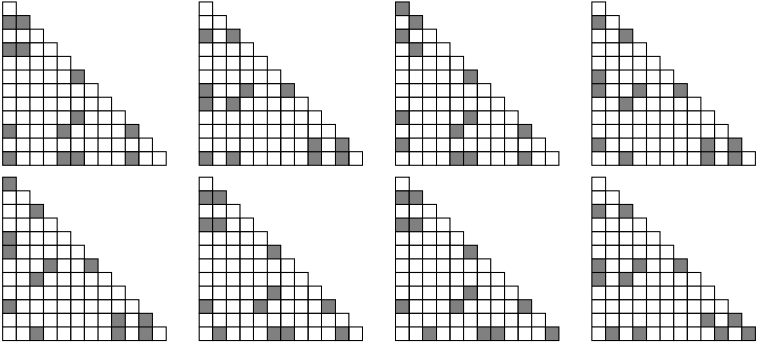
$n = 12$:



Results of the Computer Exploration

$n \leq 11$: 0 code.

$n = 12$:

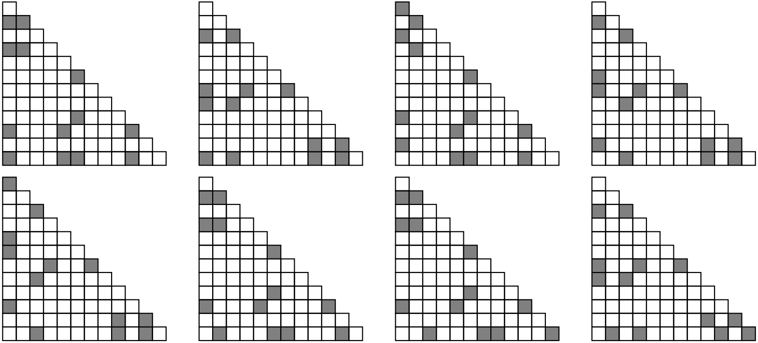


$n = 13, 14$: 0 code.

Results of the Computer Exploration

$n \leq 11$: 0 code.

$n = 12$:



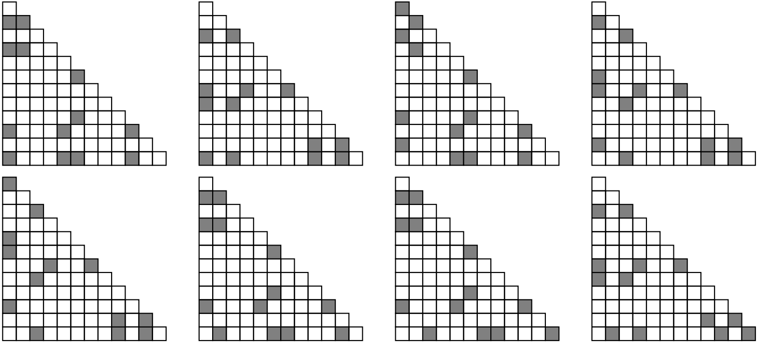
$n = 13, 14$: 0 code.

$n = 15$: 76 codes.

Results of the Computer Exploration

$n \leq 11$: 0 code.

$n = 12$:



$n = 13, 14$: 0 code.

$n = 15$: 76 codes.

$n = 16$: at least 50 codes...

$n = 17$: at least 6 codes...

Shor Inequality

A consequence of our computing

Question from Shor (1984)

What is the maximum value of $\frac{|X|}{n}$ where X is a code belonging to $a^*ba^* \cap \mathcal{A}^{\leq n}$ and n an integer?

Shor Inequality

A consequence of our computing

Question from Shor (1984)

What is the maximum value of $\frac{|X|}{n}$ where X is a code belonging to $a^*ba^* \cap \mathcal{A}^{\leq n}$ and n an integer?

Partial answer from Shor and Hansel

This value in between $\frac{16}{15}$ and $1 + \frac{1}{\sqrt{2}}$.

Shor Inequality

A consequence of our computing

Question from Shor (1984)

What is the maximum value of $\frac{|X|}{n}$ where X is a code belonging to $a^*ba^* \cap \mathcal{A}^{\leq n}$ and n an integer?

Partial answer from Shor, Hansel, and us

This value in between $\frac{13}{12}$ and $1 + \frac{1}{\sqrt{2}}$.

Factorisations of Cyclic Groups

Definition

Given $n \geq 1$, the ordered pair $(L, R) \subset [0, n[^2$ is a **factorisation** of $\mathbb{Z}/n\mathbb{Z}$ if

$$\forall k \in [0, n[, \ \exists!(\ell, r) \in L \times R \text{ such that } k = \ell + r \bmod n.$$

Factorisations of Cyclic Groups

Definition

Given $n \geq 1$, the ordered pair $(L, R) \subset [0, n[^2$ is a **factorisation** of $\mathbb{Z}/n\mathbb{Z}$ if

$$\forall k \in [0, n[,\ \exists!(\ell, r) \in L \times R \text{ such that } k = \ell + r \bmod n.$$

Example

The ordered pair $(\{1, 3, 5\}, \{1, 2, 7, 8\})$ is a factorisation of $\mathbb{Z}/12\mathbb{Z}$.

Factorisations of Cyclic Groups

Definition

Given $n \geq 1$, the ordered pair $(L, R) \subset [0, n[^2$ is a **factorisation** of $\mathbb{Z}/n\mathbb{Z}$ if

$$\forall k \in [0, n[, \ \exists!(\ell, r) \in L \times R \text{ such that } k = \ell + r \bmod n.$$

Example

The ordered pair $(\{1, 3, 5\}, \{1, 2, 7, 8\})$ is a factorisation of $\mathbb{Z}/12\mathbb{Z}$.

2

Factorisations of Cyclic Groups

Definition

Given $n \geq 1$, the ordered pair $(L, R) \subset [0, n[^2$ is a **factorisation** of $\mathbb{Z}/n\mathbb{Z}$ if

$$\forall k \in [0, n[, \; \exists!(\ell, r) \in L \times R \text{ such that } k = \ell + r \bmod n.$$

Example

The ordered pair $(\{1, 3, 5\}, \{1, 2, 7, 8\})$ is a factorisation of $\mathbb{Z}/12\mathbb{Z}$.

$$2, 3$$

Factorisations of Cyclic Groups

Definition

Given $n \geq 1$, the ordered pair $(L, R) \subset [0, n[^2$ is a **factorisation** of $\mathbb{Z}/n\mathbb{Z}$ if

$$\forall k \in [0, n[, \exists!(\ell, r) \in L \times R \text{ such that } k = \ell + r \bmod n.$$

Example

The ordered pair $(\{1, 3, 5\}, \{1, 2, 7, 8\})$ is a factorisation of $\mathbb{Z}/12\mathbb{Z}$.

$$2, 3, 8$$

Factorisations of Cyclic Groups

Definition

Given $n \geq 1$, the ordered pair $(L, R) \subset [0, n[^2$ is a **factorisation** of $\mathbb{Z}/n\mathbb{Z}$ if

$$\forall k \in [0, n[, \ \exists!(\ell, r) \in L \times R \text{ such that } k = \ell + r \bmod n.$$

Example

The ordered pair $(\{1, 3, 5\}, \{1, 2, 7, 8\})$ is a factorisation of $\mathbb{Z}/12\mathbb{Z}$.

$$2, 3, 8, 9$$

Factorisations of Cyclic Groups

Definition

Given $n \geq 1$, the ordered pair $(L, R) \subset [0, n[^2$ is a **factorisation** of $\mathbb{Z}/n\mathbb{Z}$ if

$$\forall k \in [0, n[, \ \exists!(\ell, r) \in L \times R \text{ such that } k = \ell + r \bmod n.$$

Example

The ordered pair $(\{1, 3, 5\}, \{1, 2, 7, 8\})$ is a factorisation of $\mathbb{Z}/12\mathbb{Z}$.

$$2, 3, 8, 9, 4, 5, 10, 11$$

Factorisations of Cyclic Groups

Definition

Given $n \geq 1$, the ordered pair $(L, R) \subset [0, n[^2$ is a **factorisation** of $\mathbb{Z}/n\mathbb{Z}$ if

$$\forall k \in [0, n[,\ \exists!(\ell, r) \in L \times R \text{ such that } k = \ell + r \bmod n.$$

Example

The ordered pair $(\{1, 3, 5\}, \{1, 2, 7, 8\})$ is a factorisation of $\mathbb{Z}/12\mathbb{Z}$.

$$2, 3, 8, 9, 4, 5, 10, 11, 6, 7, 0, 1.$$

Factorisations of Cyclic Groups

Definition

Given $n \geq 1$, the ordered pair $(L, R) \subset [0, n[^2$ is a **factorisation** of $\mathbb{Z}/n\mathbb{Z}$ if

$$\forall k \in [0, n[, \ \exists!(\ell, r) \in L \times R \text{ such that } k = \ell + r \bmod n.$$

Example

The ordered pair $(\{1, 3, 5\}, \{1, 2, 7, 8\})$ is a factorisation of $\mathbb{Z}/12\mathbb{Z}$.

$$2, 3, 8, 9, 4, 5, 10, 11, 6, 7, 0, 1.$$

Link Between Factorisations and Codes

Theorem from Restivo, Salemi, and Sportelli (1989)

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.

Link Between Factorisations and Codes

Theorem from Restivo, Salemi, and Sportelli (1989)

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

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

Such a factorisation is called a **factorisation associated** to X.

Example (Shor's code)

$$\begin{array}{cccccc}
\{ & b, & ba, & ba^7, & ba^{13}, & ba^{14}, \\
 & a^3b, & a^3ba^2, & a^3ba^4, & a^3ba^6, & \\
 & a^8b, & a^8ba^2, & a^8ba^4, & a^8ba^6, & \\
 & a^{11}b, & a^{11}ba, & a^{11}ba^2 & \} &
\end{array}$$

Link Between Factorisations and Codes

Theorem from Restivo, Salemi, and Sportelli (1989)

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.

Example (Shor's code)

$$\begin{array}{llllll} \{ & b, & ba, & ba^7, & ba^{13}, & ba^{14}, \\ & a^3b, & a^3ba^2, & a^3ba^4, & a^3ba^6, & \\ & a^8b, & a^8ba^2, & a^8ba^4, & a^8ba^6, & \\ & a^{11}b, & a^{11}ba, & a^{11}ba^2 & \} & \end{array}$$

Link Between Factorisations and Codes

Theorem from Restivo, Salemi, and Sportelli (1989)

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.

Example (Shor's code)

$$\begin{array}{llllll} \{ & b, & ba, & ba^7, & ba^{13}, & ba^{14}, \\ & a^3b, & a^3ba^2, & a^3ba^4, & a^3ba^6, & \\ & a^8b, & a^8ba^2, & a^8ba^4, & a^8ba^6, & \\ & a^{11}b, & a^{11}ba, & a^{11}ba^2 & \} & \end{array}$$

A factorisation associated to Shor's code is of the form

$$(L \supseteq \{0, 3, 8, 11\}, R \supseteq \{0, 1, 7, 13, 14\})$$

Link Between Factorisations and Codes

Theorem from Restivo, Salemi, and Sportelli (1989)

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.

Example (Shor's code)

$$\begin{array}{lccccc} \{ & b, & ba, & ba^7, & ba^{13}, & ba^{14}, \\ & a^3b, & a^3ba^2, & a^3ba^4, & a^3ba^6, & \\ & a^8b, & a^8ba^2, & a^8ba^4, & a^8ba^6, & \\ & a^{11}b, & a^{11}ba, & a^{11}ba^2 & \} & \end{array}$$

A factorisation associated to Shor's code is of the form

$$(L \supseteq \{0, 3, 8, 11\}, R \supseteq \{0, 1, 7, 13, 14\})$$

We do not know any of these factorisations.

A theorem from Sands

Theorem from Sands (2000)

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 $\mathbb{Z}/n\mathbb{Z}$.

A theorem from Sands

Theorem from Sands (2000)

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 $\mathbb{Z}/n\mathbb{Z}$.

Application

Recall: the factorisation of $\mathbb{Z}/n\mathbb{Z}$ associated to Shor's code is of the form

$$(L \supseteq \{0, 3, 8, 11\}, R \supseteq \{0, 1, 7, 13, 14\}).$$

A theorem from Sands

Theorem from Sands (2000)

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 $\mathbb{Z}/n\mathbb{Z}$.

Application

Recall: the factorisation of $\mathbb{Z}/n\mathbb{Z}$ associated to Shor's code is of the form

$$(L \supseteq \{0, 3, 8, 11\}, R \supseteq \{0, 1, 7, 13, 14\}).$$

Notice that $(L, 3R)$, $(L, 5R)$, $(L, 8R)$, and $(L, 11R)$ are not factorisations.

A theorem from Sands

Theorem from Sands (2000)

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 $\mathbb{Z}/n\mathbb{Z}$.

Application

Recall: the factorisation of $\mathbb{Z}/n\mathbb{Z}$ associated to Shor's code is of the form

$$(L \supseteq \{0, 3, 8, 11\}, R \supseteq \{0, 1, 7, 13, 14\}).$$

Notice that $(L, 3R)$, $(L, 5R)$, $(L, 8R)$, and $(L, 11R)$ are not factorisations. Thus $3|n$, $5|n$, $2|n$, and $11|n$.

A theorem from Sands

Theorem from Sands (2000)

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 $\mathbb{Z}/n\mathbb{Z}$.

Application

Recall: the factorisation of $\mathbb{Z}/n\mathbb{Z}$ associated to Shor's code is of the form

$$(L \supseteq \{0, 3, 8, 11\}, R \supseteq \{0, 1, 7, 13, 14\}).$$

Notice that $(L, 3R)$, $(L, 5R)$, $(L, 8R)$, and $(L, 11R)$ are not factorisations. Thus $3|n$, $5|n$, $2|n$, and $11|n$.
Hence n is a multiple of $2 \times 3 \times 5 \times 11 = 330$.

Results About Factorisations

Recall: we found 54 non-commutatively prefix code containing b.

Number of codes	Order of the letter a
4	$2 \times 3 \times 5 \times k = 30k$, with $k \geq 3$
12	$2 \times 3 \times 11 \times k = 66k$, with $k \geq 3$
4	$2 \times 3 \times 5 \times 11 \times k = 330k$, with $k \geq 4$
8	$2 \times 3 \times 5 \times 13 \times k = 390k$, with $k \geq 4$
8	$2 \times 3 \times 5 \times 13 \times k = 390k$, with $k \geq 3$
4	$2 \times 5 \times 13 \times k = 130k$, with $k \geq 3$

Lower bound

A corollary of a theorem from Perrin and Schützenberger (1977)

To be included in a finite maximal code, a bayonet code must be included in a bayonet code $X \subseteq a^{<n}ba^{<n}$ such that $|X| = n$ and $\{a^n\} \cup X$ is a code, for an integer n.

Lower bound

A corollary of a theorem from Perrin and Schützenberger (1977)

To be included in a finite maximal code, a bayonet code must be included in a bayonet code $X \subseteq a^{<n}ba^{<n}$ such that $|X| = n$ and $\{a^n\} \cup X$ is a code, for an integer n.

Computer exploration

None of the 140 non-commutatively prefix bayonet codes satisfies this condition for $n \leq 32$.

Lower bound

A corollary of a theorem from Perrin and Schützenberger (1977)

To be included in a finite maximal code, a bayonet code must be included in a bayonet code $X \subseteq a^{<n}ba^{<n}$ such that $|X| = n$ and $\{a^n\} \cup X$ is a code, for an integer n.

Computer exploration

None of the 140 non-commutatively prefix bayonet codes satisfies this condition for $n \leq 32$.

THANK YOU!