Loopless Algorithms to Generate Maximum Length Gray Cycles wrt. k-Character Substitution

Jean Néraud

Loopless Algorithms to Generate Maximum Length Gray Cycles wrt. k-Character Substitution

Jean Néraud
Univ Rouen Normandie, LITIS UR 4108, F-76000 Rouen, France

Abstract

Given a binary word relation τ onto A^* and a finite language $X \subseteq A^*$, a τ-Gray cycle over X consists in a permutation $\left(w_{[i]}\right)_{0 \leq i \leq |X|-1}$ of X such that each word $w_{[i]}$ is an image under τ of the previous word $w_{[i-1]}$. We define the complexity measure $\lambda_{A,\tau}(n)$, equal to the largest cardinality of a language X having words of length at most n, and st. some τ-Gray cycle over X exists. The present paper is concerned with $\tau = \sigma_k$, the so-called k-character substitution, st. $(u, v) \in \sigma_k$ holds if, and only if, the Hamming distance of u and v is k. We present loopless (resp., constant amortized time) algorithms for computing specific maximum length σ_k-Gray cycles.

1 Introduction

In the framework of combinatorial algorithms, one of the most well-documented issues concerns the development of methods for generating, once and for all, each object of a specific class. [23]. Many topics are concerned by such a problem: suffice it to mention sequence counting [1], signal encoding [25], and data compression [30].

In the whole paper we fix some alphabet, say A, and we assume that $|A|$, the cardinality of A, is not less than 2. The so-called *binary Gray codes* first appeared in [13]: given a binary alphabet A and some positive integer n, such objects referred to sequences with maximum length of pairwise different n-tuples of characters (that is, words in A^n), provided that any pair of consecutive items differ by exactly one character. Shortly after, a similar study was drawn in the framework of non-binary alphabets [11]. Regarding other famous combinatorial classes of objects, the term of *combinatorial Gray code*, for its part, appeared in [16]: actually, the difference between successive items, although being fixed, need not to be small [33]. Generating all permutations of a given n-element set constitutes a noticeable example [2, 10, 38, 41]. The so-called bubble languages [5, 32] are also involved, as well as cross-bifix-free sets [4], Debruijn sequences [12], Dyck words [36], Fibonacci words [3], Lyndon words [39], Motzkin words

[37], necklaces [31, 39], set partitions [19], subsets of fixed size [9, 15]: the list is far from exhaustive. For some surveys we suggest the reader report to [26, 33, 40, 42]. From an algorithmic point of view, the ultimate feature is to develop methods for producing each new object with constant, or at least constant amortized time delay, that is *loopless* or *constant amortized time* algorithms are desired [10, 24, 35, 38, 41].

The Combinatorial Gray sequences are often required to be *cyclic* [7], in the sense that the initial term itself can be retrieved as successor of the last one. Such a condition justifies the terminology of *Gray cycle* [20, Sect. 7.2.1.1]. In order to develop a formal framework, we note that each of the sequences we have mentioned above is concerned with a binary word relation $\tau \subseteq A^* \times A^*$ (A^* stands for the free monoid generated by A). For its part, the combinatorial class of objects can be modeled by some finite language $X \subseteq A^*$. Given a sequence of words we denote in square brackets the corresponding indices: this will allow us to clearly distinguish the difference with w_i, the character in *position* i in a given word w. In addition, we set $\tau(w) = \{w' : (w, w') \in \tau\}$. We define a *Gray cycle over* X *wrt.* τ (for short: τ*-Gray cycle over* X) as every finite sequence of words $\left(w_{[i]}\right)_{i\in[0,|X|-1]}$ satisfying each of the three following conditions:

(G1) For every word $x \in X$, some $i \in [0, |X| - 1]$ exists st. we have $x = w_{[i]}$;

(G2) For every $i \in [1, |X| - 1]$, we have $w_{[i]} \in \tau\left(w_{[i-1]}\right)$; in addition, the cond. $w_{[0]} \in \tau\left(w_{[|X|-1]}\right)$ holds;

(G3) For every pair $i, j \in [0, |X| - 1]$, $i \neq j$ implies $w_{[i]} \neq w_{[j]}$.

With this definition, in the Gray cycle the terms may have a variable length. For instance, given the alphabet $A = \{0, 1\}$, take for τ the binary word relation Λ_1 which, with every word w, associates all the strings located within a *Levenshtein distance* of 1 from w (see e.g. [28]). Actually the sequence $(0, 00, 01, 11, 10, 1)$ is a Λ_1-Gray cycle over $X = A \cup A^2$.

In addition to the topics we mentioned above, two other fields involved by those Gray cycles should be mentioned. Firstly, regarding graph theory, a τ-Gray cycle over X exists iff. there is some Hamiltonian circuit in the graph of the relation τ (see [33] and for some surveys on such a notion [14, 21, 34, 22]). Secondly, the existence of a τ-Gray cycle over X implies $\tau(X) \subseteq X$ (with $\tau(X) = \{\tau(w) : w \in X\}$): as defined in [28], X is τ*-closed*. Actually, closed sets constitute a special subfamily in the famous *dependence systems* [18]. However, the fact that X is τ*-closed* does not guarantees that some τ-Gray cycle may exist over X. A typical example is provided by $\tau = id_{A^*}$, the identity over A^*. Indeed, although every finite set $X \subseteq A^*$ is τ-closed, non-empty τ-Gray cycle can only exist over X if $|X| = 1$.

In the present paper, we consider the family of all sequences that can be a τ-Gray cycle over some subset X of $A^{\leq n}$ (with $A^{\leq n} = \{w \in A^* : |w| \leq n\}$). This is a natural question to focus on those sequences of maximum length: clearly, they

correspond to subsets X of maximum cardinality. We denote by $\lambda_{A,\tau}(n)$ that maximum length. This actually means introducing some complexity measure for the binary word relation τ [27]. We focus on the case where τ is σ_k, the so-called *k-character substitution*. With every word with length at least k, say w, this relation associates all the words w', with $|w'| = |w|$, and st. the character w'_i differs from w_i in exactly k values of $i \in [1, |w|]$: in other words, the Hamming distance of w and w' is k.

Some words on the word binary relation σ_k: firstly, as commented in [17, 28], this relation has noticeable inference in the famous framework of *error detection*. Secondly, the cond. $w' \in \sigma_k(w)$ implies $|w'| = |w|$, therefore if there is some σ_k-Gray cycle over a language X, then all the words in X have a common length: by definition X is a *uniform* set. From this point of view, the classical Gray codes that allow to generate all n-tuples over A, correspond to σ_1-Gray cycles over A^n. Actually, in the case where A is a binary alphabet, some maximum length σ_2-Gray cycles have also been constructed (we have $\lambda_{A,\sigma_2}(n) = 2^{n-1}$) [20, Exercice 8, p. 77]. However, in the most general case, although an exhaustive description of σ_k-closed variable-length codes has been provided in [28], the question of generating some σ_k-Gray cycle of maximum length has remained open. The present paper present algorithmic constructions to generate those sequences of maximum length. More precisely, we establish the following result:

Theorem *Given a finite alphabet A, $k \geq 1$, and $n \geq k$, there is a loopless algorithm that allows to generate some maximum length σ_k-Gray cycle. In addition the following equation holds:*

$$\lambda_{A,\sigma_k}(n) = \begin{cases} |A^n| & |A| \geq 3, n \geq k \\ 2 & |A| = 2, n = k \\ |A|^n & |A| = 2, n \geq k+1, k \text{ is odd} \\ |A|^{n-1} & |A| = 2, n \geq k+1, k \text{ is even.} \end{cases}$$

Beforehand, the computation of such maximum length σ_k-Gray cycles is done thanks to induction-based equations. In addition, in each case we present an iteration-based method for computing those sequences: it directly allows to compute the term of index i by starting from the term of index $i-1$.

We now shortly describe the contents of the paper:

– Section 2, is devoted to the preliminaries. We fix some complementary definitions and notations; in addition, we recall the two famous examples of the *binary* (resp., *$|A|$-ary*) *reflected Gray code*.

– In Sect. 2, we focus on the case where the alphabet A possesses at least 3 letters. Starting with the *$|A|$-ary* reflected Gray code, by establishing some induction formula we prove that, given a pair of positive integers n, k, there is a peculiar Gray cycle, namely $h^{n,k} = \left(h^{n,k}_{[i]}\right)_{0 \leq i \leq |A|^n - 1}$: its length is $|A|^n$.

– An iteration-based method for computing the preceding cycle is developed in Sect. 3.

– In Sect. 4, in the case where A is a binary alphabet, with k being an odd integer, we also compute a maximum length σ_k-Gray cycle. Once more this is done by establishing some inductive method: practically it relies on two peculiar k-Gray cycles.

– A corresponding iteration-based method of computation is developed in Sect. 5.

– At last, in Sect. 6, in the case where A is a binary alphabet, with k being an even positive integer, we also compute a maximum length Gray cycles : this leads to complete the proof of the theorem we mentioned above.

In addition, it is common in the literature to define a k-Gray code as the sequence where two consecutive items have distance at most k [26]. In the case of the Hamming distance, this notion corresponds to the so-called Σ_k-Gray cycles, where the relation Σ_k st. $(w, w') \in \Sigma_k$ iff. the Hamming distance of w and w' is not greater than k. We discuss where our results intersect with such a topic. Some further development is also raised.

2 Preliminaries

Several definitions and notation have already been fixed. In the whole paper, A stands for a finite alphabet, with $|A| \geq 2$. Given a word $w \in A^*$, we denote by $|w|$ its length; in addition, for every $a \in A$, we denote by $|w|_a$ the number of occurrences of the character a in w. Given a pair of words $w, w' \in A^*$, w' is a *prefix* (resp., *suffix*) of w if some word $u \in A^*$ exists st. $w = w'u$ (resp. $w = uw'$). Given a word $w \in A^*$, $m \in [0, |w|]$, we denote by $A^{-m}w$ the unique suffix of w with length $|w| - m$.

Historically Gray cycles have been developed in order to generate integers in $|A|$-ary numeration system. From this point of view, regarding the position of the characters in the word w, it is convenient to set $w = w_n \cdots w_1$, with $w_i \in A$, for every $i \in [1, n]$ (we say that w_i is the character with *position* i in the word w). In other words, in the $|A|$-ary numeration system the word $w = w_n \cdots w_1$ is the representation of the integer $w_n|A|^{n-1} + w_{n-1}|A|^{n-2} + \cdots + w_1$.

The reflected binary Gray cycle
Let $A = \{0, 1\}$ and $n \geq 1$. The most famous example of σ_1-Gray cycle over A^n is certainly the so-called *reflected binary Gray code* (see e.g. [20, pp. 5-6] or [26, Sect. 3.1]): in the present paper we denote it by $g^{n,1}$. It can be computed in different ways:

– Firstly, the sequence can be defined recursively by the following rule:

$$g^{0,1} = (\varepsilon); \quad g^{n+1,1} = \left(\left(0g^{n,1}\right), \left(1\left(g^{n,1}\right)^R\right)\right) \tag{1}$$

In this notation the comma stands for the sequence concatenation. Moreover, given a finite sequence, say $x = (x_1, \cdots x_n)$ and a word $w \in A^*$, we set $x^R = (x_n, \cdots, x_1)$ and $wx = (wx_1, \cdots, wx_n)$. Actually Eq. (1) leads to construct the

whole sequence $g^{n+1,1}$ by applying a series of one character concatenations on the left over the words of $g^{n,1}$.

– Secondly, in the literature there is a famous constant amortized-time iterative algorithm (in the paper we denote it by Algorithm (a)) that allows to compute $g^{n,1}$. The method starts by setting $g^{n,1}_{[0]} = 0^n$. After that, for every $i \in [1, |A|^n - 1]$, the word $g^{n,1}_{[i]}$ is computed from right to left by starting from $g^{n,1}_{[i-1]}$. Actually a unique integer $j \in [1, n]$ exists st. in both words $g^{n,1}_{[i]}$ and $g^{n,1}_{[i-1]}$, the corresponding characters in position j differ: with the preceding convention over character positions, j is chosen in order to satisfy the following condition:

$$j \text{ is the } \textit{minimum} \text{ position in } g^{n,1}_{[i]} \text{ st. } g^{n,1}_{[i]} \notin \{g^{n,1}_{[0]}, \cdots, g^{n,1}_{[i-1]}\}. \tag{2}$$

Example 2.1. *Below are column representations of the sequences $g^{2,1}$ and $g^{3,1}$:*

$$\begin{array}{cc} \overbrace{\begin{array}{c} 00 \\ 01 \\ 11 \\ 10 \end{array}}^{g^{2,1}} & \overbrace{\begin{array}{c} 000 \\ 001 \\ 011 \\ 010 \\ 110 \\ 111 \\ 101 \\ 100 \end{array}}^{g^{3,1}} \end{array}$$

By construction, for every $n \geq 1$, each of the following identities holds:

$$g^{n,1}_{[0]} = 0^n, \quad g^{n,1}_{[1]} = 0^{n-1}1, \quad g^{n,1}_{[2^n-2]} = 10^{n-2}1, \quad g^{n,1}_{[2^n-1]} = 10^{n-1}. \tag{3}$$

The $|A|$-ary reflected Gray cycle

The preceding constructions can be extended in order to obtain the so-called *$|A|$-ary reflected Gray code* over A^n, that we denote by $h^{n,1}$. More precisely we set $A = \{0, \cdots, p-1\}$ and we denote by θ the cyclic permutation defined by $0 \to 1, \ldots, p-2 \to p-1, p-1 \to 0$.

– Firstly, $h^{n,1}$ can be defined recursively by the following rule [26, Sect. 3.19]:

$$h^{0,1} = (\varepsilon); \quad h^{n+1,1} = \left(0h^{n,1}, 1\left(h^{n,1}\right)^R, 2h^{n,1}, 3\left(h^{n,1}\right)^R, \cdots, (p-1)\Gamma\right) \tag{4}$$

$$\text{with } \Gamma = \begin{cases} h^{n,1} & \text{if } p \text{ is odd} \\ \left(h^{n,1}\right)^R & \text{otherwise.} \end{cases}$$

– Secondly, the sequence $h^{n,1}$ can be generated by applying a constant amortized-time algorithm [8, 11], that we denote by Algorithm (b). The method starts by setting $h^{n,1}_{[0]} = 0^n$. For every $i \in [1, |A|^n - 1]$, starting from $h^{n,1}_{[i-1]}$ the

word $h^{n,1}_{[i]}$ is computed from right to left. More precisely, there are $j \in [1, p^{n_0}-1]$, $c, d \in A$, where c and d are the characters respectively in position j in $h^{n,1}_{[i-1]}$ and $h^{n,1}_{[i]}$, st. both the each of following conditions holds:

$$j \text{ is the } \textit{minimum} \text{ position in } h^{n,1}_{[i]} \text{ st. } h^{n,1}_{[i]} \notin \{h^{n,1}_{[0]}, \cdots, h^{n,1}_{[i-1]}\}, \tag{5}$$

$$d = \begin{cases} \theta(c) \text{ if } i \div p^j \text{ is even} \\ \theta^{-1}(c) \text{ otherwise.} \end{cases} \tag{6}$$

Example 2.2. *For $A = \{0, 1, 2\}$ the sequence $h^{3,1}$ is the concatenation in this order of the three following subsequences:*

$$\overbrace{}^{h^{3,1}}$$

000	122	200
001	121	201
002	120	202
012	110	212
011	111	211
010	112	210
020	102	220
021	101	221
022	100	222

3 The case where we have $|A| \geq 3$

Let $n \geq k \geq 1$, $p \geq 3$, and $A = \{0, 1, \cdots, p-1\}$. In what follows, we indicate the construction of a peculiar σ_k-Gray cycle over A^n, namely $h^{n,k}$. This is done by applying some induction over $k \geq 1$: in view of that, we set $n_0 = n - k + 1$.

– The starting point corresponds to $h^{n_0,1}$, the p-ary reflected Gray code over A^{n_0} as reminded in Section 2.

– For the induction stage, by starting with a σ_{k-1}-Gray cycle over A^{n-1}, namely $h^{n-1,k-1}$, we compute the corresponding sequence $h^{n,k}$ as indicated in the following:
Let $i \in [0, p^n - 1]$, and let $q \in [0, p-1]$, $r \in [0, p^{n-1} - 1]$ be the unique pair of non-negative integers st. $i = qp^{n-1} + r$. We set:

$$h^{n,k}_{[i]} = h^{n,k}_{[qp^{n-1}+r]} = \theta^{q+r}(0) h^{n-1,k-1}_{[r]}. \tag{7}$$

As shown in Example 3.1, by construction the resulting sequence $h^{n,k}$ is the concatenation in this order of p subsequences namely $C_0, \ldots, C_{p-1}$, with $C_q = \left(h^{n,k}_{[qp^{n-1}+r]}\right)_{0 \leq r \leq p^{n-1}-1}$, for each $q \in [0, p-1]$. Since θ is one-to-one, given a pair of different integers $q, q' \in [0, p-1]$, for every $r \in [0, p^{n-1}-1]$, in each of the subsequences C_q, $C_{q'}$, the words $h^{n,k}_{[qp^{n-1}+r]}$ and $h^{n,k}_{[q'p^{n-1}+r]}$ only differ in their initial characters, which respectively are $\theta^{q+r}(0)$ and $\theta^{q'+r}(0)$. In addition, since $h^{n-1,k-1}$ is a σ_{k-1}-Gray cycle over A^{n-1}, we have $\left|h^{n,k}\right| = p\left|h^{n-1,k-1}\right| = p^n$.

Example 3.1. Let $A = \{0, 1, 2\}$, $n = 3$, $k = 2$, thus $p = 3$, $n_0 = 2$. By starting with $h^{n-1,k-1} = h^{2,1}$, we construct the sequence $h^{n,k}$ as the concatenation of C_0, C_1, and C_2:

$h^{n-1,k-1}$	$h^{n,k}$		
00	000	100	200
01	101	201	001
02	202	002	102
12	012	112	212
11	111	211	011
10	210	010	110
20	020	120	220
21	121	221	021
22	222	022	122

Proposition 3.2. *The sequence $h^{n,k}$ is a σ_k-Gray cycle over A^n.*

Proof. We argue by induction over $k \geq 1$. Regarding the base case, as indicated above $h^{n_0,1}$ is the $|A|$-ary reflected Gray sequence. In view of the induction stage, we assume that the finite sequence $h^{n-1,k-1}$ is a σ_{k-1}-Gray cycle over A^{n-1}, for some $k \geq 2$.

(i) We start by proving that $h^{n,k}$ satisfies Condition (G2). This will be done through the three following steps:

(i.i) Firstly, we prove that, for each $q \in [0, p-1]$, in the subsequence C_q two consecutive terms are necessarily in correspondence under σ_k. Given $r \in [0, p^{n-1} - 1]$, by definition, we have $\theta^{r+q}(0) \in \sigma_1\left(\theta^{r+q-1}(0)\right)$. Since $h^{n-1,k-1}$ satisfies Condition (G2), we have $h^{n-1,k-1}_{[r]} \in \sigma_{k-1}\left(h^{n-1,k-1}_{[r-1]}\right)$. We obtain $\theta^{q+r}(0)h^{n-1,k-1}_{[r]} \in \sigma_k\left(\theta^{q+r-1}(0)h^{n-1,k-1}_{[r-1]}\right)$, thus according to Eq. (7): $h^{n,k}_{[qp^{n-1}+r]} \in \sigma_k\left(h^{n,k}_{[qp^{n-1}+r-1]}\right)$.

(i.ii) Secondly, we prove that, for each $q \in [1, p-1]$, the last term of C_{q-1} and the initial term of C_q are also connected under σ_k. At first take $r = 0$ in Eq. (7): it follows from $\theta^{p^{n-1}} = id_A$ that we have $h^{n,k}_{[qp^{n-1}]} = \theta^q(0)h^{n-1,k-1}_{[0]} = \theta^{p^{n-1}+q}(0)h^{n-1,k-1}_{[0]}$. Now take $r = p^{n-1} - 1$ in Eq. (7) , moreover substitute $q - 1 \in [0, p-2]$ to $q \in [1, p-1]$: we obtain $h^{n,k}_{[qp^{n-1}-1]} = \theta^{q+p^{n-1}-2}(0)h^{n-1,k-1}_{[p^{n-1}-1]}$. It follows from $p = |A| \geq 3$ that $\theta(0) \neq \theta^{-2}(0)$: since θ is one-to-one this implies $\theta^{q+p^{n-1}}(0) \neq \theta^{q+p^{n-1}-2}(0)$, thus $\theta^{q+p^{n-1}}(0) \in \sigma_1\left(\theta^{q+p^{n-1}-2}(0)\right)$. Since by induction we have $h^{n-1,k-1}_{[0]} = \sigma_{k-1}\left(h^{n-1,k-1}_{[p^{n-1}-1]}\right)$, we obtain $h^{n,k}_{[qp^{n-1}]} \in \sigma_k\left(\theta^{q+p^{n-1}-2}(0)h^{n-1,k-1}_{[qp^{n-1}-1]}\right)$ that is, $h^{n,k}_{[qp^{n-1}]} \in \sigma_k\left(h^{n,k}_{[qp^{n-1}-1]}\right)$.

(i.iii) At last, we prove that the first term of C_0 is connected under σ_k with the last term of C_{p-1}. In Eq. (7), take $q = 0$ and $r = 0$: we obtain

$h^{n,k}_{[0]} = 0h^{n-1,k-1}_{[0]}$. Similarly, by setting $q = p-1$ and $r = p^{n-1}-1$, we obtain $h^{n,k}_{[(p-1)p^{n-1}+p^{n-1}-1]} = \theta^{p^{n-1}+p-2}(0)h^{n-1,k-1}_{[p^{n-1}-1]}$, thus $h^{n,k}_{[p^n-1]} = \theta^{-2}(0)h^{n-1,k-1}_{[p^{n-1}-1]}$. Since $h^{n-1,k-1}$ is a σ_{k-1}-Gray cycle over A^{n-1}, we have $h^{n-1,k-1}_{[0]} \in \sigma_{k-1}\left(h^{n-1,k-1}_{[p^{n-1}-1]}\right)$. In addition, it follows from $p \geq 3$, that $\theta^{-2}(0) \neq 0$, thus $0 \in \sigma_1\left(\theta^{-2}(0)\right)$. We obtain $h^{n,k}_{[0]} \in \sigma_k\left(\theta^{-2}(0)h^{n-1,k-1}_{[p^{n-1}-1]}\right)$, thus $h^{n,k}_{[0]} \in \sigma_k\left(h^{n,k}_{[p^n-1]}\right)$ that is, the required property.

(ii) Now, we prove that $h^{n,k}$ satisfies Cond. (G2) that is, in its terms are pairwise different. Let $i, i' \in [0, p^n-1]$ st. $h^{n,k}_{[i]} = h^{n,k}_{[i']}$ and consider the unique 4-tuple of integers $q, q' \in [0, p-1]$, $r, r' \in [0, p^{n-1}-1]$ st. $i = qp^{n-1}+r$ and $i' = q'p^{n-1}+r'$. According to Eq. (7) we have $\theta^{q+r}(0)h^{n-1,k-1}_{[r]} = \theta^{q'+r'}(0)h^{n-1,k-1}_{[r']}$: since we have $\theta^{q+r}(0), \theta^{q'+r'}(0) \in A$, this implies $\theta^{q+r}(0) = \theta^{q'+r'}(0)$, whence we have $h^{n-1,k-1}_{[r]} = h^{n-1,k-1}_{[r']}$. Since $h^{n-1,k-1}$ satisfies Cond. (G3), the second equation implies $r = r'$, whence the first one implies $\theta^q(0) = \theta^{q'}(0)$, thus $q = q' \bmod p$. Since we have $q, q' \in [0, p-1]$ we obtain $q = q'$, thus $i = i'$.

(iii) At last, since the terms of $h^{n,k}$ are pairwise different, we have: $\left|\bigcup_{0\leq i\leq p^n-1}\{h^{n,k}_{[i]}\}\right| = p^n$, thus: $\bigcup_{0\leq i\leq p^n-1}\{h^{n,k}_{[i]}\} = A^n$: this completes the proof. □

4 An alternative approach for computing the sequence $h^{n,k}$

According to Eq. (7), given an integer pair n, k, the sequence $h^{n,k}$ can be computed by starting with $h^{n-1,k-1}$. Clearly, in view of the full computation of $h^{n,k}$, that type of approach leads to a recursive algorithm. In the present section we will provide some alternative method: actually we will prove that, for each $i \in [0, p^n-1]$, the word $h^{n,k}_{[i]}$ can be directly computed by starting with $h^{n,k}_{[i-1]}$. Beforehand we introduce some complementary definitions and notations:

- Given an integer pair $a, b \in \mathbb{N}$, with $a \leq b$, and a finite word sequence $x = \left(x_{[i]}\right)_{a\leq i\leq b}$, for convenience we set $x = x_{[a\cdot\cdot b]}$.

- With the preceding notation, given a positive integer c, we say that the sequence x is *c-periodic* if either we have $|x| = b-a+1 \leq c$, or the equation $x_{[i+c]} = x_{[i]}$ holds for every $i \in [a, b-c]$. In particular, wrt. finite sequence concatenation, $x = y^q$ with $q > 0$ implies x being $|y|$-periodic.

- Given a non-negative integer m with $m \leq \max\{|x_i| : i \in [a, b]\}$, we set $A^{-m}x = \left(A^{-m}x_{[i]}\right)_{a\leq i\leq b}$.

- At last, given a positive integer m, and given $w \in A^*$, with $|w| \geq m$, it is convenient to denote by $\mathrm{P}_m(w)$ the unique prefix of w that belongs to A^m: this notation can be extended in a straightforward way to any sequence of words in A^mA^*.

4.1 A property involving periodicity

Recall that we set $n_0 = n - k + 1$. With this notation the following prop. holds:

Lemma 4.1. *For every $j \in [n_0, n]$ the sequence $A^{j-n}h^{n,k}$ is p^j-periodic. More precisely $A^{j-n}h^{n,k}$ is a concatenation power of $h^{j,k-n+j}_{[0..p^j-1]}$.*

Proof. We apply a top-down induction-based argument over $j \in [n_0, n]$.

– The base case corresponds to $j = n$. With this condition we have $A^{j-n}h^{n,k} = h^{n,k} = h^{j,k-n+j}_{[0..p^j-1]}$, thus trivially the prop. holds.

– For the induction stage, we assume that $A^{j-n}h^{n,k}$ is a concatenation power of the sequence $h^{j,k-n+j}_{[0..p^j-1]}$. With this condition, the sequence $A^{j-n-1}h^{n,k} = A^{-1}\left(A^{j-n}h^{n,k}\right)$ is a concatenation power of $A^{-1}h^{j,k-n+j}_{[0..p^j-1]}$. Let i be an arbitrary integer in $[0, p^j - 1]$ and let $q \in [0, p-1]$, $r \in [0, p^{j-1} - 1]$ be the unique integer pair st. $i = qp^{j-1} + r$. By substituting j to n and $k - n + j$ to k in Eq. (7), we obtain $A^{-1}h^{j,k-n+j}_{[qp^{j-1}+r]} = h^{j-1,k-n+j-1}_{[r]}$. As a consequence, we have $A^{-1}h^{j,k-n+j}_{[qp^{j-1}..(q+1)p^{j-1}-1]} = h^{j-1,k-n+j-1}_{[0..p^{j-1}-1]}$ therefore, wrt. sequence concatenation, we obtain $\prod_{0 \le q \le p-1} A^{-1}h^{j,k-n+j}_{[qp^{j-1}..(q+1)p^{j-1}-1]} = \left(h^{j-1,k-n+j-1}_{[0..p^{j-1}-1]}\right)^p$, thus $A^{-1}h^{j,k-n+j}_{[0..p^j-1]} = \left(h^{j-1,k-n+j-1}_{[0..p^{j-1}-1]}\right)^p$. Consequently, the sequence $A^{j-n-1}h^{n,k}$, which is a concatenation power of $A^{-1}h^{j,k-n+j}_{[0..p^j-1]}$, is a concatenation power of $h^{j-1,k-n+j-1}_{[0..p^{j-1}-1]}$. □

4.2 Some map of the combinatorial structure of $h^{n,k}$

For every $i \in [0, p^n - 1]$ Eq. (7) leads to compute $h^{n,k}_{[i]}$ by applying a series of one-character left-concatenations. On the other hand, with the convention over the character positions in words the following equation holds:

$$h^{n,k}_{[i]} = \left(h^{n,k}_{[i]}\right)_n \left(h^{n,k}_{[i]}\right)_{n-1} \cdots \left(h^{n,k}_{[i]}\right)_1, \quad \text{with} \quad \left(h^{n,k}_{[i]}\right)_j \in A \quad (j \in [1, n]). \tag{8}$$

Our aim is to prove that the word $h^{n,k}_{[i]}$ can be directly computed starting from $h^{n,k}_{[i-1]}$. In order to do this, we are going to highlight a combinatorial structure common to all words $h^{j,k-n+j}_{[i]}$ $(j \in [n_0, n], i \in [0, p^j - 1])$. In what follows, we fix the integers n and k. According to Eq. (8), we set:

$$H^{[j]}_{[i]} = \begin{cases} \left(h^{n,k}_{[i]}\right)_j \in A \ \text{ if } \ j \in [n_0 + 1, n] \\ h^{n_0,1}_{[i]} = \left(h^{n,k}_{[i]}\right)_{n_0} \cdots \left(h^{n,k}_{[i]}\right)_1 \in A^{n_0} \ \text{ if } \ j = n_0. \end{cases} \tag{9}$$

Let H be the matrix with components $H^{[j]}_{[i]}$. The row index is $i \in [1, p^n - 1]$, the column index being $j \in [n_0 + 1, n]$. We emphasize on the fact that the row

of index i is:

$$\left(H_{[i]}^{[n]}, H_{[i]}^{[n-1]}, \cdots, H_{[i]}^{[j+1]}, H_{[i]}^{[j]}, \cdots, H_{[i]}^{[n_0+1]}, H_{[i]}^{[n_0]}\right) =$$

$$\left(\left(h_{[i]}^{n,k}\right)_n, \left(h_{[i]}^{n,k}\right)_{n-1}, \cdots, \left(h_{[i]}^{n,k}\right)_{n_0+1}, \left(h_{[i]}^{n,k}\right)_{n_0} \cdots \left(h_{[i]}^{n,k}\right)_1\right). \tag{10}$$

Although at first glance the preceding notation may seem cumbersome, there are several reasons why we have adopted it:

– Firstly, the notation is naturally connected to the computation process generated Eq. (7). In particular, it is coherent with the right to left computation of $h^{n_0,1}$ using Algorithm (b) [20, p.6].

– Secondly, with reference to the origins of Gray code topic, the word $h_{[i]}^{n,k} = H_{[i]}^{[n]} \cdots H_{[i]}^{[n_0]}$ (or, equivalently, the polynomial in (10)) is actually the representation in base $p = |A|$ of some non-negative integer.

– Last and not least, regarding our experience concerning the present study, in adopting some alternative non-reversal representation, the results that we state below, and their proofs, would become much more difficult to read. In particular Eq. (7), would be applied to more heavy indices, moreover the period of the columns in H could not take an expression as simple as p^j (see Lemma 4.2).

We introduce an additional notation: given $i \in [0, p^n - 1]$ and $j \in [n_0, n]$, we denote by $r(i,j)$ the unique integer in $[0, p^j - 1]$ st. $i = r(i,j) \bmod p^j$. In particular, it follows from $i \in [0, p^n - 1]$ that $r(i,n) = i$. As a consequence of Lemma 4.1, we obtain the following statement:

Lemma 4.2. *With the preceding notation, each of the following props. holds:*

(i) *For each $j \in [n_0, n]$ the sequence of words $H_{[0\cdot\cdot p^n-1]}^{[j]}$ is p^j-periodic.*

(ii) *For each $j \in [n_0 + 1, n]$, we have $H_{[i]}^{[j]} = \mathrm{P}_1\left(h_{[r(i,j)]}^{j,k-n+j}\right)$.*

Proof. (i) Firstly assume $j \in [n_0 + 1, n]$. According to Eq. (9), in the matrix H the component $H_{[i]}^{[j]} = \left(h_{[i]}^{n,k}\right)_j \in A$ is the initial character of the word $\left([H_{[i]}^{[n]} H_{[i]}^{[n-1]} \cdots H_{[i]}^{[j+1]}\right)^{-1} h_{[i]}^{n,k}$, thus with the notation introduced above: $H_{[i]}^{[j]} = \mathrm{P}_1\left(A^{j-n} h_{[i]}^{n,k}\right)$. According to Lemma 4.1 the sequence $A^{j-n} h^{n,k}$ is p^j-periodic, therefore $H_{[0\cdot\cdot p^n-1]}^{[j]}$ itself is p^j-periodic.
Now, we assume $j = n_0$. Once more according to Eq. (9), we have:

$$H_{[i]}^{[n_0]} = h_{[i]}^{n_0,1} = \left(H_{[i]}^{[n]} H_{[i]}^{[n-1]} \cdots H_{[i]}^{[n_0+1]}\right)^{-1} h_{[i]}^{n,k} \in A^{n-n_0} h_{[i]}^{n,k}.$$

Once more according to Lemma 4.1, the sequence $H_{[0\cdot\cdot p^n-1]}^{[n_0]}$ is p^j-periodic. Consequently, for each $j \in [n_0, n]$ the sequence of words $H_{[0\cdot\cdot p^n-1]}^{[j]}$ is p^j-periodic.

(ii) Let $j \in [n_0 + 1, n_0]$. According to Lemma 4.1, the sequence $A^{j-n} h^{n,k}$ is a concatenation power of $h_{[0\cdot\cdot p^j-1]}^{j,k-n+j}$, hence we have $A^{j-n} h_{[i]}^{n,k} = h_{[r(i,j)]}^{j,k-n-j}$ that is, by construction: $H_{[i]}^{[j]} = \mathrm{P}_1\left(A^{j-n} h_{[i]}^{n,k}\right) = \mathrm{P}_1\left(h_{[r(i,j)]}^{j,k-n-j}\right)$. □

In addition the following prop. holds:

Lemma 4.3. *The condition* $r(i,j) = 0 \bmod p^{j-1}$ *is equivalent to* $i = 0 \bmod p^{j-1}$.

Proof. The cond. $i = r(i,j) \bmod p^j$ implies $i = r(i,j) \bmod p^{j-1}$. Consequently, $r(i,j) = 0 \bmod p^{j-1}$ implies $i = 0 \bmod p^{j-1}$. Conversely, assume $i = mp^{j-1}$, with $m \in \mathbb{N}$. From the fact that $i = r(i,j) + m'p^j$, with $m' \in \mathbb{N}$, we obtain $r(i,j) = (m - m'p)p^{j-1}$, thus $r(i,j) = 0 \bmod p^{j-1}$. □

4.3 An algorithmic interpretation

On the basis of the above, an iteration-based method for computing the word $h_{[i]}^{n,k}$ can be drawn.

– We start by setting $H_{[0]}^{[n_0]} = h_{[0]}^{n_0,1} = 0^{n_0}$.

– Next, for $i \in [0, p^{n_0} - 1]$, according to Formula (9), the component $H_{[i]}^{[n_0]}$ is actually $h_{[i]}^{n_0,1}$, which can be generated starting from $h_{[i-1]}^{n_0,1}$ by construction.

– In addition, for every $i \in [0, p^n - 1]$, according to Lemma 4.2, we have $H_{[i]}^{[n_0]} = h_{[r(i,n_0)]}^{n_0,1}$. In other words, wrt. sequence concatenation, the column of index n_0 in the matrix H is obtained by applying the following equation:

$$H^{[n_0]} = \left(h^{n_0,1}\right)^{p^{n-n_0}}. \tag{11}$$

In what follows we introduce a permutation, namely ω:

ω operates onto the set $\left\{H_{[0]}^{[n_0]}, H_{[1]}^{[n_0]}, \cdots, H_{[p^{n_0}-1]}^{[n_0]}\right\}$ as indicated in the following

$$\omega\left(H_{[i]}^{[n_0]}\right) = \begin{cases} H_{[i+1]}^{[n_0]} & \text{if} \quad i \in [0, p^{n_0} - 2] \\ H_{[0]}^{[n_0]} & \text{if} \quad i = p^{n_0-1}. \end{cases} \tag{12}$$

Accordingly, for every $i \in [1, p^{n_0} - 1]$ we have $H_{[i]}^{[n_0]} = h_{[i]}^{n_0,1}$. Note that, thanks to Algorithm (b) (see the preliminaries), $h_{[i]}^{n_0,1}$ can be generated from $h_{[i-1]}^{n_0,1}$ that is, $H_{[i]}^{[n_0]}$ can be generated from $H_{[i-1]}^{[n_0]}$. The following result is at the basis of an iterative algorithm for computing the whole matrix H (recall that θ stands for the cyclic permutation $(0, \cdots, p-1)$):

Proposition 4.4. *Given* $i \in [1, p^n - 1]$*, each of the following equations hold:*

(i) $H_{[i]}^{[n_0]} = \omega\left(H_{[i-1]}^{[n_0]}\right)$.

(ii) *For every* $j \in [n_0 + 1, n]$*:*

$$H_{[i]}^{[j]} = \begin{cases} \theta^2\left(H_{[i-1]}^{[j]}\right) & \text{if} \quad i = 0 \bmod p^{j-1} \\ \\ \theta\left(H_{[i-1]}^{[j]}\right) & \text{otherwise.} \end{cases}$$

Proof. (i) Firstly, assume $i \neq 0 \bmod p^{n_0}$. This condition implies $r(i,n_0) \in [1, p^{n_0}-1]$, hence we have $r(i-1,n_0) = r(i,n_0)-1 \in [0, p^{n_0}-1]$. According to the definition of ω, this implies $H^{[n_0]}_{[r(i,n_0)]} = \omega\left(H^{[n_0]}_{[r(i-1,n_0)]}\right)$. According to the prop. (i) of Lemma 4.2, we obtain $H^{n_0,1}_{[i]} = H^{[n_0]}_{[r(i,n_0)]} = \omega\left(H^{[n_0]}_{[r(i-1,n_0)]}\right) = \omega\left(H^{[n_0]}_{[i-1]}\right)$. Now, we assume $i = 0 \bmod p^{n_0}$. Once more according to the prop. (i) of Lemma 4.2 we have $H^{[n_0]}_{[i]} = H^{[n_0]}_{[0]}$ and $H^{[n_0]}_{[i-1]} = H^{[n_0]}_{[p^{n_0}-1]}$ (recall that, according to the condition of the present proposition we have $i \geq 1$). By the definition of ω (see (12), we have $H^{[n_0]}_{[0]} = \omega\left(H^{[n_0]}_{[p^{n_0}-1]}\right)$, thus $H^{[n_0]}_{[i]} = H^{[n_0]}_{[i-1]}$. This completes the proof of the prop. (i) of our proposition.

(ii) Let $j \in [n_0+1, n]$, and let q, s be the unique integer pair st. $r(i,j) = qp^{j-1} + s$, with $0 \leq s \leq p^{j-1}-1$. By substituting $r(i,j)$ to i, j to n, and $k-n+j$ to k in Eq. (7) ,we obtain $h^{j,k-n+j}_{[r(i,j)]} = \theta^{q+s}(0) h^{j-1,k-n+j-1}_{[s]}$, whence $\theta^{q+s}(0)$ is the initial character of $h^{j,k-n+j}_{[r(i,j)]}$. According to the prop. (ii) of Lemma 4.2, we obtain $H^{[j]}_{[i]} = \theta^{q+s}(0)$. Now we examine the component $H^{[j]}_{[i-1]}$. Actually, according to the value of s exactly one of the two following conds. occurs:

<u>*Cond. $s = 0$*</u>
By definition this cond. is equivalent to $r(i,j) = qp^{j-1}$. It follows from $i \geq 1$ that $r(i-1,j) = r(i,j) - 1 = qp^{j-1} - 1 = (q-1)p^{j-1} + (p^{j-1}-1)$. Note that we have $p^{j-1}-1 \in [0, p^{j-1}-1]$: by substituting $r(i-1,j)$ to i, j to n, and $k-n+j$ to k in Eq. (7), we obtain $h^{j,k+j-n}_{[r(i-1,j)]} = h^{j,k+j-n}_{[(q-1)p^{j-1}+(p^{j-1}-1)]} = \theta^{(q-1)+(p^{j-1}-1)}(0) h^{j-1,k+j-n-1}_{[p^{j-1}-1]}$, whence $\theta^{q+p^{j-1}-2}(0) = \theta^{q-2}(0)$ is the initial character of $h^{j,k-n+j}_{[r(i-1,j)]}$. According to the prop. (ii) of Lemma 4.2, we have $H^{[j]}_{[i-1]} = \theta^{q-2}(0)$. As indicated above, we have $H^{[j]}_{[i]} = \theta^{q+s}(0)$: we obtain $H^{[j]}_{[i]} = \theta^q(0) = \theta^2\left(\theta^{q-2}(0)\right) = \theta^2\left(H^{[j]}_{[i-1]}\right)$.

<u>*Cond. $s > 0$*</u>
With this cond. we have $r(i-1,j) = qp^{j-1} + (s-1)$, with $0 \leq s-1 \leq p^{j-1}-1$. Once more by substituting in Eq. (7) $r(i-1,j)$ to i, j to n, and $k-n+j$ to k, we obtain $h^{j,k-n+j}_{r[(i-1,j)]} = \theta^{q+s-1}(0) h^{j-1,k-n+j-1}_{[s-1]}$, whence $\theta^{q+s-1}(0)$ is the initial character of $h^{j,k-n+j}_{[r(i-1,j)]}$. According to the prop. (ii) of Lemma 4.2, this implies $H^{[j]}_{[i-1]} = \theta^{q+s-1}(0)$ that is, $H^{[j]}_{[i]} = \theta^{q+s}(0) = \theta\left(\theta^{q+s-1}(0)\right) = \theta\left(H^{[j]}_{[i-1]}\right)$. □

In view of Proposition 4.4, an iterative algorithm to the sequence $h^{n,k}$, namely Algorithm 1, can be drawn. This algorithm computes row by row each component of the matrix H. Such a computation actually makes use of a unique generic row, namely:

$$\mathcal{H} = \left(\mathcal{H}^{[n]}, \mathcal{H}^{[n-1]}, \cdots, \mathcal{H}^{[j]}, \mathcal{H}^{[j-1]}, \cdots, \mathcal{H}^{[n_0+1]}, \mathcal{H}^{[n_0]}\right).$$

From this point of view, each time the counter i is incremented, the generic row $\mathcal{H}$ is updated to $\left(H^{[n]}_{[i]}, H^{[n-1]}_{[i]}, \cdots, H^{[j]}_{[i]}, H^{[j-1]}_{[i]}, \cdots, H^{[n+0]}_{[i]}, H^{[n_0]}_{[i]}\right)$. Recall

that, according to Eq. (11) the following equalities hold:

$$H_{[0]}^{[n_0]} = h_{[0]}^{n_0,1} = 0^{n_0}, \quad H_{[0\cdot\cdot p^{n_0}-1]}^{[n_0]} = h^{n_0,1}, \qquad H_{[0\cdot\cdot p^n-1]}^{[n_0]} = \left(h^{n_0,1}\right)^{p^{n-n_0}} \tag{13}$$

Algorithm 1

1: $n_0 \leftarrow n-k+1$; $max \leftarrow p^n-1$
2: $i \leftarrow 0$; $\mathcal{H}^{[n_0]} \leftarrow h_{[0]}^{n_0,1}$; $h_{[i]}^{n,k} \leftarrow \mathcal{H}^{[n_0]}$
3: **for** $n_0+1 \le j \le n$ **do** $\mathcal{H}^{[j]} \leftarrow 0$; $h_{[i]}^{[n,k]} \leftarrow h_{[i]}^{[n,k]}\mathcal{H}^{[j]}$
4: **end for**
5: **while** $i \le max$ **do**
6: $\quad\mathcal{H}^{[n_0]} \leftarrow \omega\left(\mathcal{H}^{[n_0]}\right)$; $h_{[i]}^{n,k} \leftarrow \mathcal{H}^{[n_0]}$
7: $\quad j \leftarrow n_0+1$; $p' \leftarrow p^{n_0}$
8: $\quad$**while** $j \le n$ **do**
9: $\quad\quad$**if** $i = 0 \bmod p'$ **then**
10: $\quad\quad\quad\mathcal{H}^{[j]} \leftarrow \theta^2\left(\mathcal{H}^{[j]}\right)$
11: $\quad\quad$**else**
12: $\quad\quad\quad\mathcal{H}^{[j]} \leftarrow \theta\left(\mathcal{H}^{[j]}\right)$
13: $\quad\quad$**end if**
14: $\quad\quad h_{[i]}^{n,k} \leftarrow \mathcal{H}^{[j]}h_{[i]}^{n,k}$; $j \leftarrow j+1$; $p' \leftarrow p'p$
15: $\quad$**end while**
16: $\quad i \leftarrow i+1$
17: **end while**

A few comments on Algorithm 1
– The component $\mathcal{H}^{[n_0]}$ is initialized to $H_{[0]}^{[n_0]} = h_{[0]}^{n_0,1}$. This is done by applying the process described in lines 2–4.
– Each time the counter i is incremented, in the stage described in lines 6–16 Algorithm 1 computes from right to left the row $\left(H_{[i]}^{[n]}, \cdots, H_{[i]}^{[n_0+1]}, H_{[i]}^{[n_0]}\right)$. The term $h_{[i]}^{n,k}$ itself is computed as the concatenation $H_{[i]}^{[n]} \cdots H_{[i]}^{[n_0+1]} \cdot H_{[i]}^{[n_0]}$. This is done by updating the generic row $\mathcal{H}$: its components are computed by applying the formula from Proposition 4.4. In addition, at line 14, after incrementation of the variable j, p^{j-1} is memorized in the variable p', which took the initial value p^{n_0} (line 7).
– The algorithm stops when the counter i reaches the value max+1= p^n (see l. 6).

Questions related to complexity
By construction, applying Algorithm 1 for computing the whole sequence $h^{n,k}$ that is, computing all the rows of the matrix H, requires at most np^n insertions. In what follows, our goal is to improve such a bound.

Beforehand we note that, in any case, the alphabet A and the permutation θ should be computed in some preprocessing stage.

– On the one hand, for each incrementation of the counter i, updating the generic sequence $\mathcal{H} = \left(\mathcal{H}^{[n]}, \cdots \mathcal{H}^{[n_0+1]}\right)$ is done by applying the stage in lines 8–15: there is a positive integer, say ℓ, st. applying that stage requires at most $\ell(n - n_0) \leq \ell k$ insertions. When the counter i reaches the value max, $\mathcal{H}$ has been updated p^n times, whence the total amount of corresponding operations is at most $p^n \ell k$.

– On the other hand, in order to update the component $\mathcal{H}^{[n_0]}$, in l. 6. we need to apply the permutation ω. From this point of view, there are actually two strategies of implementation:

(a) In the first approach, for each value of i, in order to compute the finite sequence $h^{n_0,1} = \left(H^{[n_0]}_{[i]}\right)_{0 \leq i \leq p^{n_0-1}}$ we apply the step (5) from Algorithm (b), as mentioned in the preliminaries. Actually, the right-most character flips each time, the second one flips every p time, and so on: classically, that method requires an amount of $p^{n_0} + p^{n_0-1} + \cdots + p \leq p^{n_0}$ one-character substitutions. For computing the whole column $H^{[n_0]} = \left(H^{[n_0]}_{[i]}\right)_{0 \leq i \leq p^{n-1}}$, the total cost of the preceding operations is bounded by $p^{n-n_0} \cdot p^{n_0} = p^n$. Consequently, computing the whole sequence $h^{n,k}$ requires a total amount of operations bounded by $p^n \ell k + p^n = p^n(\ell k + 1)$. Note that in the computation of each term of $h^{n_0,1}$ the amount of substitutions actually depends of the value of the counter i that is, the process cannot be loopless. However, the amortized cost per operation is $p^{-n} p^n (\ell k + 1) = \ell k + 1$ that is, $O(1)$. In other words, with this strategy Algorithm 1 runs in constant amortized-time wrt. n, with space linear in $n - n_0 + n_0 = n$.

(b) The second approach consists in implementing in a preprocessing phase the sequence $h^{n_0,1}$ and the permutation ω: such an implementation requires space $O(n_0 p^{n_0})$ and, as indicated above, a total amount of $O(p^{n_0})$ substitutions. After that, in the processing phase, updating $\mathcal{H}^{n_0}$ will be performed by applying the result of lemma 4.2: this leads to a constant number of requests to $h^{n_0,1}$ and ω (see l. 6). In other words, updating the whole sequence $\mathcal{H}$ requires constant time that is, with such a strategy implementation, Algorithm 1 is loopless and requires space linear in $n_0 p^{n_0} + n$.

5 The case where A is a binary alphabet, with k odd

Let $A = \{0, 1\}$ and $n \geq k$. With this condition, the cyclic permutation θ, which was introduced in Section 2, is defined by $\theta(0) = 1$ and $\theta(1) = 0$. Classically, this permutation can be extended into a one-to-one monoid homomorphism onto A^*: in view of this, we set $\theta(\varepsilon) = \varepsilon$ and, for any non-empty n-tuple of characters $a_1, \cdots, a_n \in A$, $\theta(a_1 \cdots a_n) = \theta(a_1) \cdots \theta(a_n)$. Trivially, in the case where we have $n = k$, if a non-empty σ_k-Gray code exists over $X \subseteq A^n$, then we have $X = \{x, \theta(x)\}$, for some $x \in A^n$. In the sequel we assume $n \geq k + 1$; with this condition we will construct a pair of peculiar σ_k-Gray cycles over A^n, namely $\gamma^{n,k}$ and $\rho^{n,k}$. This will be done by induction over k', the unique non-negative

integer st. $k = 2k' + 1$. Beforehand, we set $n_0 = n - 2k' = n - k + 1$: necessarily we have $n_0 \geq 2$.

– For the base case, $\gamma^{n_0,1}$ and $\rho^{n_0,1}$ are computed by applying some reversal (resp., shift) over the sequence $g^{n_0,1}$, which was introduced in the cond. (5) grom Section 2. We set :

$$\gamma^{n_0,1}_{[0]} = g^{n_0,1}_{[0]} \text{ and } \gamma^{n_0,1}_{[i]} = g^{n_0,1}_{[2^{n_0}-i]} \ (1 \leq i \leq 2^{n_0} - 1). \tag{14}$$

$$\rho^{n_0,1}_{[0]} = g^{n_0,1}_{[2^{n_0}-1]} \text{ and } \rho^{n_0,1}_{[i]} = g^{n_0,1}_{[i-1]} \ (1 \leq i \leq 2^{n_0} - 1). \tag{15}$$

By construction, $\gamma^{n_0,1}$ and $\rho^{n_0,1}$ are σ_1-Gray cycles over A^{n_0}. Moreover we have:

$$\gamma^{n_0,1}_{[0]} = 0^{n_0} \text{ and } \rho^{n_0,1}_{[0]} = 10^{n_0-1}. \tag{16}$$

$$\gamma^{n_0,1}_{[2^{n_0}-1]} = g^{n_0,1}_{[1]} = 0^{n_0-1}1 \text{ and } \rho^{n_0,1}_{[2^{n_0}-1]} = g^{n_0,1}_{[2^{n_0}-2]} = 10^{n-2}1. \tag{17}$$

Example 5.1. *Taking $n_0 = 2$, according to Eqs. 15, the corresponding sequences $\gamma^{2,1}$ and $\rho^{n_0,1}$ are the following ones:*

$g^{2,1}$	$\gamma^{2,1}$	$\rho^{2,1}$
00	00	10
01	10	00
11	11	01
10	01	11

Example 5.2. *For $n_0 = 3$ we obtain the following sequences:*

$g^{3,1}$	$\gamma^{3,1}$	$\rho^{3,1}$
000	000	100
001	100	000
011	101	001
010	111	011
110	110	010
111	010	110
101	011	111
100	001	101

– In view of the induction step, we assume that we have computed the σ_k-Gray cycles $\gamma^{n,k}$ and $\rho^{n,k}$. Note that we have $n + 2 = n_0 + 2(k' + 1) = n_0 + (k + 2) - 1$: below we explain the construction of the two corresponding 2^{n+2}-term sequences $\gamma^{n+2,k+2}$ and $\rho^{n+2,k+2}$. Given $i \in [0, 2^{n+2}-1]$, let $q \in [0, 3]$, $r \in [0, 2^n - 1]$ be the unique integer pair st. $i = q2^n + r$. By assigning to q the value 0 (resp., 1, 2, 3), we state the corresponding Eq. (18) (resp., Eqs. (18),(18),(18)):

$$\gamma^{n+2,k+2}_{[r]} = \theta^r(00)\gamma^{n,k}_{[r]} \tag{18a}$$
$$\gamma^{n+2,k+2}_{[2^n+r]} = \theta^r(01)\rho^{n,k}_{[r]} \tag{18b}$$
$$\gamma^{n+2,k+2}_{[2\cdot 2^n+r]} = \theta^r(11)\gamma^{n,k}_{[r]} \tag{18c}$$
$$\gamma^{n+2,k+2}_{[3\cdot 2^n+r]} = \theta^r(10)\rho^{n,k}_{[r]} \tag{18d}$$

Similarly the sequence $\rho^{n+2,k+2}$ is computed by substituting, in the preceding Eqs., the 4-tuple $(10, 11, 01, 00)$ to $(00, 01, 11, 10)$:

$$\rho^{n+2,k+2}_{[r]} = \theta^r(10)\gamma^{n,k}_{[r]} \tag{19a}$$
$$\rho^{n+2,k+2}_{[2^n+r]} = \theta^r(11)\rho^{n,k}_{[r]} \tag{19b}$$
$$\rho^{n+2,k+2}_{[2\cdot 2^n+r]} = \theta^r(01)\gamma^{n,k}_{[r]} \tag{19c}$$
$$\rho^{n+2,k+2}_{[3\cdot 2^n+r]} = \theta^r(00)\rho^{n,k}_{[r]}. \tag{19d}$$

Example 5.3. *(Example 5.2 continued)* $\gamma^{5,3}$ *is the concatenation, in this order, of the* 4 *following subsequences:*

$\overbrace{}^{\gamma^{3,1}}$	$\overbrace{}^{\rho^{3,1}}$	$\overbrace{}^{\gamma^{3,1}}$	$\overbrace{}^{\rho^{3,1}}$
00 000	01 100	11 000	10 100
11 100	10 000	00 100	01 000
00 101	01 001	11 101	10 001
11 111	10 011	00 111	01 011
00 110	01 010	11 110	10 010
11 010	10 110	00 010	01 110
00 011	01 111	11 011	10 111
11 001	10 101	00 001	01 101

Lemma 5.4. *Both the sequences* $\gamma^{n,k}$, $\rho^{n,k}$ *satisfy each of the conditions* (G1), (G3).

Proof. Recall that we set $k = 2k' + 1$: we argue by induction over $k' \geq 0$. The base case corresponds to $k' = 0$ that is, $k = 1$ and $n = n_0$: as indicated above, $\gamma^{n_0,1}$ and $\rho^{n_0,1}$ are σ_1-Gray cycles over A^n. In view of the induction step we assume that, for some $k' \geq 0$, both the sequences $\gamma^{n,k}$ and $\rho^{n,k}$ are σ_k-Gray cycles over A^n.

(i) In order to prove that $\gamma^{n+2,k+2}$ satisfies Cond. (G3), we consider an integer pair $i, i' \in [0, 2^{n+2} - 1]$ st. $\gamma^{n+2,k+2}_{[i]} = \gamma^{n+2,k+2}_{[i']}$. Let $q, q' \in [0, 3]$, $r, r' \in [0, 2^n - 1]$ st. $i = q2^n + r$, $i' = q'2^n + r'$. According to Eqs. (18)–(18) there are words $x, x' \in A^2$, $w, w' \in A^n$ st. $\gamma^{n+2,k+2}_{[i]} = \theta^r(x)w$ and $\gamma^{n+2,k+2}_{[i']} = \theta^{r'}(x')w'$ that is, $\theta^r(x) = \theta^{r'}(x') \in A^2$ and $w = w'$. By the definition of θ, this implies

either $x, x' \in \{00, 11\}$ or $x, x' \in \{01, 10\}$ that is, by construction, either $q, q' \in \{0, 2\}$, $x, x' \in \{00, 11\}$, $w = \gamma^{n,k}_{[r]} = \gamma^{n,k}_{[r']}$, or $q, q' \in \{1, 3\}$, $x, x' \in \{01, 10\}$, $w = \rho^{n,k}_{[r]} = \rho^{n,k}_{[r']}$. Since $\gamma^{n,k}$ and $\rho^{n,k}$ satisfies Cond. (G3), in any case we have $r = r'$. This implies $\theta^r(x) = \theta^r(x')$, thus $x = x'$. With regard to Eqs. (18)–(18), this corresponds to $q = q'$, thus $i = q2^n + r = q'2^n + r = i'$, therefore $\gamma^{n+2,k+2}$ satisfies Cond. (G3).

(ii) By substituting $(10, 11, 01, 00)$ to $(00, 01, 11, 10)$, according to (19)–(19), similar arguments lead to prove that $\rho^{n+2,k+2}_{[i]} = \rho^{n+2,k+2}_{[i']}$ implies $i = i'$ that is, the sequence $\rho^{n+2,k+2}$ also satisfies Cond. (G3).

(iii) Since $\gamma^{n+2,k+2}$ satisfies (G3), we have $\bigcup_{0 \le i \le 2^{n+2}-1} \{\gamma^{n+2,k+2}_i\} = A^{n+2}$, hence our sequence satisfies (G1). Similarly, since $\rho^{n+2,k+2}$ satisfies Cond. (G3) it satisfies Cond. (G1). □

In order to prove that both the sequences $\gamma^{n,k}$ and $\rho^{n,k}$ satisfy Condition (G2), beforehand we establish the following prop.:

Lemma 5.5. *We have* $\gamma^{n,k}_{[0]} \in \sigma_{k+1}\left(\rho^{n,k}_{[2^n-1]}\right)$ *and* $\rho^{n,k}_{[0]} \in \sigma_{k+1}\left(\gamma^{n,k}_{[2^n-1]}\right)$.

Proof. We argue by induction over $k' \ge 0$.

– The base case corresponds to $k' = 0$, thus $k = 1$ and $n = n_0$. According to the identity (16) we have $\gamma^{n_0,1}_{[0]} = 0^{n_0} \in \sigma_2\left(10^{n_0-2}1\right)$ thus $\gamma^{n_0,1}_{[0]} \in \sigma_2\left(\rho^{n,k}_{[2^n-1]}\right)$. Similarly, according to (17) we have $\rho^{n_0,1}_{[0]} = 10^{n_0-1} \in \sigma_2\left(0^{n_0-1}1\right)$ that is, $\rho^{n_0,1}_{[0]} \in \sigma_2\left(\gamma^{n_0,1}_{[2^{n_0}-1]}\right)$.

– For the induction step, we assume that, for some $k' \ge 0$, we have $\gamma^{n,k}_{[0]} \in \sigma_{k+1}\left(\rho^{n,k}_{[2^n-1]}\right)$ and $\rho^{n,k}_{[0]} \in \sigma_{k+1}\left(\gamma^{n,k}_{[2^n-1]}\right)$.

(i) In Eq. (18), by setting $r = 0$ we obtain $\gamma^{n+2,k+2}_{[0]} = 00\gamma^{n,k}_{[0]}$, hence by induction: $\gamma^{n+2,k+2}_{[0]} \in 00\sigma_{k+1}\left(\rho^{n,k}_{[2^n-1]}\right) \subseteq \sigma_{k+3}\left(11\rho^{n,k}_{[2^n-1]}\right)$. By setting $r = 2^n - 1$ in Eq. (19), we obtain $\rho^{n+2,k+2}_{[2^{n+2}-1]} = 11\rho^{n,k}_{[2^n-1]}$: this implies $\gamma^{n+2,k+2}_{[0]} \in \sigma_{k+3}\left(\rho^{n+2,k+2}_{[2^{n+2}-1]}\right)$.

(ii) Similarly, by setting $r = 0$ in Eq. (19), and by induction we have: $\rho^{n+2,k+2}_{[0]} = 10\gamma^{n,k}_{[0]} \in \sigma_{k+3}\left(01\rho^{n,k}_{[2^n-1]}\right)$. By taking $r = 2^n - 1$ in Eq. (18) we obtain $\gamma^{n+2,k+2}_{[2^{n+2}-1]} = 01\rho^{n,k}_{[2^n-1]}$, therefore we have $\rho^{n+2,k+2}_{[0]} \in \sigma_{k+3}\left(\gamma^{n+2,k+2}_{[2^{n+2}-1]}\right)$. □

Since Eqs. (18)–(19) look alike, one may be tempted to compress them by substituting to them some unique generic Formula. Based on our tests, such a formula needs to introduce at least two additional technical parameters, with tedious handling. In the proof of the following result, we have opted to report some case-by-case basis argumentation: this has the advantage of making use of arguments which, although being similar, are actually easily legible.

Proposition 5.6. *Both the sequences $\gamma^{n,k}$ and $\rho^{n,k}$ are σ_k-Gray cycles over A^n.*

Proof. Once more we argue by induction over $k' \geq 0$. Since $\gamma^{n_0,1}$ and $\rho^{n_0,1}$ are σ_1-Gray cycles over A^n, the prop. holds for $k' = 0$. In view of the induction stage, we assume that, for some $k' \geq 0$ both the sequences $\gamma^{n,k}$ and $\rho^{n,k}$ are σ_k-Gray cycles over A^n. According to Lemma 5.4, it remains to establish that $\gamma^{n+2,k+2}$ and $\rho^{n+2,k+2}$ satisfy Cond. (G2) that is:

$$(\forall q \in \{0,1,2,3\})(\forall r \in [1, 2^n - 1])\ \gamma^{n+2,k+2}_{[q2^n+r]} \in \sigma_{k+2}\left(\gamma^{n+2,k+2}_{[q2^n+r-1]}\right); \tag{20}$$

$$(\forall q \in \{1,2,3\})\ \gamma^{n+2,k+2}_{[q2^n]} \in \sigma_{k+2}\left(\gamma^{n+2,k+2}_{[q2^n-1]}\right); \tag{21}$$

$$\gamma^{n+2,k+2}_{[0]} \in \sigma_{k+2}\left(\gamma^{n+2,k+2}_{[2^{n+2}-1]}\right). \tag{22}$$

$$(\forall q \in \{0,1,2,3\})(\forall r \in [1, 2^n - 1])\ \rho^{n+2,k+2}_{[q2^n+r]} \in \sigma_{k+2}\left(\rho^{n+2,k+2}_{[q2^n+r-1]}\right); \tag{23}$$

$$(\forall q \in \{1,2,3\})\ \rho^{n+2,k+2}_{[q2^n]} \in \sigma_{k+2}\left(\rho^{n+2,k+2}_{[q2^n-1]}\right); \tag{24}$$

$$\rho^{n+2,k+2}_{[0]} \in \sigma_{k+2}\left(\rho^{n+2,k+2}_{[2^{n+2}-1]}\right). \tag{25}$$

Condition (20)

(i) At first assume $q = 0$. According to Eq. (18) and since by induction $\gamma^{n,k}$ satisfies Cond. (G2), we have $\gamma^{n+2,k+2}_{[r]} = \theta^r(00)\,\gamma^{n,k}_{[r]} \in \theta^r(00)\sigma_k\left(\gamma^{n,k}_{[r-1]}\right)$, thus $\gamma^{n+2,k+2}_{[r]} \in \sigma_{k+2}\left(\theta^{r-1}(00)\gamma^{n,k}_{[r-1]}\right)$. In Eq. (18), by substituting $r-1$ to r (we have $0 \leq r-1 < 2^n - 1$): we obtain $\gamma^{n+2,k+2}_{[r-1]} = \theta^{r-1}(00)\gamma^{n,k}_{[r-1]}$: this implies $\gamma^{n+2,k+2}_{[r]} \in \sigma_{k+2}\left(\gamma^{n+2,k+2}_{[r-1]}\right)$.

(ii) Now assume $q = 1$. According to Eq. (18), and since by induction $\rho^{n,k}$ satisfies Cond. (G2), we have $\gamma^{n+2,k+2}_{[2^n+r]} = \theta^r(01)\rho^{n,k}_{[r]} \in \sigma_{k+2}\left(\theta^{r-1}(01)\rho^{n,k}_{[r-1]}\right)$. In Eq. (18), substitute $r-1$ to r: we obtain $\gamma^{n+2,k+2}_{[2^n+r-1]} = \theta^{r-1}(01)\rho^{n,k}_{[r-1]}$, therefore we have $\gamma^{n+2,k+2}_{[2^n+r]} \in \sigma_{k+2}\left(\gamma^{n+2,k+2}_{[2^n+r-1]}\right)$.

(iii) For $q = 2$, we make use of arguments very similar to those applied in (i): according to Eq. (18) and since by induction $\gamma^{n,k}$ satisfies Cond. (G2), we have $\gamma^{n+2,k+2}_{[2\cdot 2^n+r]} = \theta^r(11)\gamma^{n,k}_{[r]} \in \theta^r(11)\sigma_k\left(\gamma^{n,k}_{[r-1]}\right) \subseteq \sigma_{k+2}\left(\theta^{r-1}(11)\gamma^{n,k}_{[r-1]}\right)$. Once more in Eq. (18), by substituting $r-1$ to r, we obtain $\gamma^{n+2,k+2}_{[r-1]} = \theta^{r-1}(11)\gamma^{n,k}_{[r-1]}$: this implies $\gamma^{n+2,k+2}_{[r]} \in \sigma_{k+2}\left(\gamma^{n+2,k+2}_{[r-1]}\right)$.

(iv) Finally, with the condition $q = 3$, according to Eq. (18), and since $\rho^{n,k}$ satisfies Cond. (G2), we have $\gamma^{n+2,k+2}_{[3\cdot 2^n+r]} = \theta^r(10)\rho^{n,k}_{[r]} \in \sigma_{k+2}\left(\theta^{r-1}(10)\rho^{n,k}_{[r-1]}\right)$. In Eq. (18), substitute $r-1$ to r: we obtain $\gamma^{n+2,k+2}_{[3\cdot 2^n+r-1]} = \theta^{r-1}(10)\rho^{n,k}_{[r-1]}$, therefore we have $\gamma^{n+2,k+2}_{[3\cdot 2^n+r]} \in \sigma_{k+2}\left(\gamma^{n+2,k+2}_{[3\cdot 2^n+r-1]}\right)$.

Condition (21)

(i) Assume $q = 1$ and take $r = 0$ in Eq. (18): we obtain $\gamma_{[2^n]}^{n+2,k+2} = 01\rho_{[0]}^{n,k}$. It follows from Lemma 5.5, that $\gamma_{[2^n]}^{n+2,k+2} \in 01\sigma_{k+1}\left(\gamma_{[2^n-1]}^{n,k}\right)$, thus $\gamma_{[2^n]}^{n+2,k+2} \in \sigma_{k+2}\left(11\gamma_{[2^n-1]}^{n,k}\right)$. By taking $r = 2^n - 1$ in (18), we obtain: $\gamma_{[2^n-1]}^{n+2,k+2} = \theta^{2^n-1}(00)\,\gamma_{[2^n-1]}^{n,k} = 11\gamma_{[2^n-1]}^{n,k}$: this implies $\gamma_{[2^n]}^{n+2,k+2} \in \sigma_{k+2}\left(\gamma_{[2^n-1]}^{n+2,k+2}\right)$.

(ii) Now, assume $q = 2$, and set $r = 0$ in Eq. (18): we obtain $\gamma_{[2\cdot 2^n]}^{n+2,k+2} = 11\gamma_{[0]}^{n,k}$. According to Lemma 5.5 we have $\gamma_{[2\cdot 2^n]}^{n+2,k+2} \in 11\sigma_{k+1}\left(\rho_{[2^n-1]}^{n,k}\right) \subseteq \sigma_{k+2}\left(10\rho_{[2^n-1]}^{n,k}\right)$. By taking $r = 2^n - 1$ in (18), we obtain $\gamma_{[2^n+2^n-1)]}^{n+2,k+2} = 10\rho_{[2^n-1]}^{n,k}$, which implies $\gamma_{[2\cdot 2^n]}^{n+2,k+2} \in \sigma_{k+2}\left(\gamma_{[2\cdot 2^n-1]}^{n+2,k+2}\right)$.

(iii) Finally, for $q = 3$, we take $r = 0$ in Eq. (18). Once more according to Lemma 5.5, we have $\gamma_{[3\cdot 2^n]}^{n+2,k+2} = 10\rho_{[0]}^{n,k} \in 10\sigma_{k+1}\left(\gamma_{[2^n-1]}^{n,k}\right) \subseteq \sigma_{k+2}\left(01\gamma_{[2^n-1]}^{n,k}\right)$. On the other hand, by taking $r = 2^n - 1$ in Eq. (18): we obtain $\gamma_{[2\cdot 2^n+2^n-1]}^{n+2,k+2} = \theta^{2^n-1}(10)\,\gamma_{[2^n-1]}^{n,k} = 01\gamma_{[2^n-1]}^{n,k}$ that is, $\gamma_{[3\cdot 2^n]}^{n+2,k+2} \in \sigma_{k+2}\left(\gamma_{[3\cdot 2^n-1]}^{n+2,k+2}\right)$.

Condition (22)

Take $r = 0$ in Eq. (18). According to Lemma 5.5, we have $\gamma_{[0]}^{n+2,k+2} = 00\gamma_{[0]}^{n,k} \in 00\sigma_{k+1}\left(\rho_{[2^n-1]}^{n,k}\right) \subseteq \sigma_{k+2}\left(01\rho_{[2^n-1]}^{n,k}\right)$. By taking $r = 2^n - 1$ in Eq. (18) we obtain $\gamma_{[3\cdot 2^n+2^n-1]}^{n,k} = 01\rho_{[2^n-1]}^{n,k}$, thus $\gamma_{[0]}^{n+2,k+2} \in \sigma_{k+2}\left(\gamma_{[2^{n+2}-1]}^{n,k}\right)$.

Condition (23)– (25)

According to the structures of Eqs. (19)–(19), for proving these conditions the method consists in substituting the word $\rho_{[r]}^{n+2,k+2}$ to $\gamma_{[r]}^{n+2,k+2}$, the 4-tuple $(10, 11, 01, 00)$ to $(00, 01, 11, 10)$, and Eq. (19) (resp., (19), (19), (19)) to Eq. (18) (resp., (18), (18), (18)). □

6 Condition k odd: a non recursive method for computing $\gamma^{n,k}$

Recall that we set $k = 2k' + 1$, $n_0 = n - 2k' = n - k + 1 \geq 2$. Let $J = \bigcup_{0\leq \ell \leq k'}\{n_0 + 2\ell\} = \{n_0, n_0 + 2, \cdots n - 2, n\}$. As in Sect. 4, we will establish an eq. that allows to compute the word $\gamma_{[i]}^{n,k}$ starting from $\gamma_{[i-1]}^{n,k}$, for every $i \in [1, 2^n - 1]$. Beforehand, it is convenient to summarize such an approach.

– At first, some combinatorial study is drawn: for each $j \in J$ we describe, in term of periodicity, the structure of the sequence $A^{j-n}\gamma^{n,k}$ (Lemma 6.1).

– In order to provide some map of the whole family of words $\gamma_{[i]}^{n,k}$ ($1 \leq i \leq 2^n - 1$), a first matrix, namely $C = \left(C_{[i]}^{[j]}\right)_{0 \leq i \leq 2^n-1, j \in J}$, is introduced. The components of C are words that can be computed, on the one hand by applying Eqs. (30), (31) (such formulas actually come from the preceding eqs. (18)–(19)), and on the other hand, by applying Lemma 6.1.

– Actually the matrix C cannot be directly computed through an iteration-based method. To remedy this situation, a second matrix namely Q is introduced. From this point of view, Eqs. (33), (34) provide precision on Eqs. (30), (31).

–At this stage, we have gathered sufficient material to obtain a first computation formula, which is presented in Lemma 6.4. Some precision: in the case where i is not a multiple of 2^{j-2}, our formula allows to compute the matrix $\left(Q_{[i]}^{[j]}, C_{[i]}^{[j]}\right)$ by directly starting from $\left(Q_{[i-1]}^{[j]}, C_{[i-1]}^{[j]}\right)$. In the case where i is a multiple of 2^{j-2}, the formula requires to start the computation from the pair $\left(Q_{[i-2^{j-2}-1]}^{[j]}, C_{[i-2^{j-2}-1]}^{[j]}\right)$: we have not yet achieved our goal.

– Furthermore, Proposition 6.6 sets a second formula: in any case, it allows the computation of $\left(Q_{[i]}^{[j]}, C_{[i]}^{[j]}\right)$ by directly starting with the pair $\left(Q_{[i-1]}^{[j]}, C_{[i-1]}^{[j]}\right)$.

– Regarding the implementation of the above method, some pseudo-code is provided in Algorithm 2.

6.1 A property involving periodicity

We start by establishing the following result:

Lemma 6.1. *Wrt. the sequence concatenation, for every $j \in J$ the sequence $A^{j-n}\gamma^{n,k}$ is 2^{j+1}-periodic. More precisely, given $j \in J \setminus n$, $A^{j-n}\gamma^{n,k}$ is a power of the sequences concatenation $\left(\gamma_{[0..2^j-1]}^{j,k-n+j}, \rho_{[0..2^j-1]}^{j,k-n+j}\right)$.*

Proof. With the condition $j = n$, trivially the sequence $A^{j-n}\gamma^{n,k} = \gamma^{n,k}$ is 2^{j+1}-periodic. For $j \in J \setminus \{n\}$, by making use of a top-down induction-based argument over j, we prove that $A^{j-n}\gamma^{n,k}$ is a concatenation power of $\gamma_{[0..2^j-1]}^{j,k-n+j}\rho_{[0..2^j-1]}^{j,k-n+j}$.

– The base case corresponds to $j = n - 2$. Let $i \in [0, 2^n - 1]$, $q \in [0, 3]$, and $r \in [0, 2^{n-2} - 1]$ st. $i = q2^{n-2} + r$. By substituting $n - 2$ to n and $k - 2$ to k in Eqs. (18)–(19), we obtain the following identities:

$$\begin{aligned}
A^{-2}\gamma_{[r]}^{n,k} &= \gamma_{[r]}^{n-2,k-2} \\
A^{-2}\gamma_{[2^{n-2}+r]}^{n,k} &= \rho_{[r]}^{n-2,k-2} \\
A^{-2}\gamma_{[2\cdot 2^{n-2}+r]}^{n,k} &= \gamma_{[r]}^{n-2,k-2} \\
A^{-2}\gamma_{[3\cdot 2^{n-2}+r]}^{n,k} &= \rho_{[r]}^{n-2,k-2}.
\end{aligned}$$

As a consequence, regarding sequences of words, each of the following eqs. holds:

$$\begin{aligned} A^{-2}\gamma^{n,k}_{[0..2^{n-2}-1]} &= \gamma^{n-2,k-2}_{[0..2^{n-2}-1]} \\ A^{-2}\gamma^{n,k}_{[2^{n-2}..2\cdot 2^{n-2}-1]} &= \rho^{n-2,k-2}_{[0..2^{n-2}-1]} \\ A^{-2}\gamma^{n,k}_{[2\cdot 2^{n-2}..3\cdot 2^{n-2}-1]} &= \gamma^{n-2,k-2}_{[0..2^{n-2}-1]} \\ A^{-2}\gamma^{n,k}_{[3\cdot 2^{n-2}..2^{n}-1]} &= \rho^{n-2,k-2}_{[0..2^{n-2}-1]}. \end{aligned}$$

Wrt. sequence concatenation, this implies:

$$A^{-2}\gamma^{n,k} = A^{-2}\gamma^{n,k}_{[0..2^{n}-1]} = \left(\gamma^{n-2,k-2}_{[0..2^{n-2}-1]}, \rho^{n-2,k-2}_{[0..2^{n-2}-1]}\right)^2.$$

Since the length of each of the sequences $\gamma^{n-2,k-2}_{[0..2^{n-2}-1]}, \rho^{n-2,k-2}_{[0..2^{n-2}-1]}$ is $2^{n-2} = 2^j$, the prop. of Lemma 6.1 holds.

– For the induction stage, we assume that, for some $j \in J \setminus \{n_0, n\}$, the sequence $A^{j-n}\gamma^{n,k}$ is a concatenation power of $\left(\gamma^{j,k-n+j}_{[0..2^j-1]}, \rho^{j,k-n+j}_{[0..2^j-1]}\right)$. With this condition, the sequence $A^{j-n-2}\gamma^{n,k} = A^{-2}\left(A^{j-n}\gamma^{n,k}\right)$, for its part, is a power of $A^{-2}\left(\gamma^{j,k-n+j}_{0..2^j-1}, \rho^{j,k-n+j}_{0..2^j-1}\right)$. Let $i \in [0, 2^j - 1]$, $q \in [0, 3]$, and $r \in [0, 2^{j-2} - 1]$ st. $i = q2^{j-2} + r$. By substituting j to $n+2$ and $k-n+j$ to $k+2$ in Eqs. (18)–(19), we obtain:

$$\begin{aligned} A^{-2}\gamma^{j,k-n+j}_{[r]} &= \gamma^{j-2,k-n+j-2}_{[r]} \\ A^{-2}\gamma^{j,k-n+j}_{[2^{j-2}+r]} &= \rho^{j-2,k-n+j-2}_{[r]} \\ A^{-2}\gamma^{j,k-n+j}_{[2\cdot 2^{j-2}+r]} &= \gamma^{j-2,k-n+j-2}_{[r]} \\ A^{-2}\gamma^{j,k-n+j}_{[3\cdot 2^{j-2}+r]} &= \rho^{j-2,k-n+j-2}_{[r]}. \end{aligned}$$

Therefore, the following equations hold:

$$\begin{aligned} A^{-2}\gamma^{j,k-n+j}_{[0..2^{j-2}-1]} &= \gamma^{j-2,k-n+j-2}_{[0..2^{j-2}-1]} \\ A^{-2}\gamma^{j,k-n+j}_{[2^{j-2}..2\cdot 2^{j-2}-1]} &= \rho^{j-2,k-n+j-2}_{[0..2^{j-2}-1]} \\ A^{-2}\gamma^{j,k-n+j}_{[2\cdot 2^{j-2}..3\cdot 2^{j-2}-1]} &= \gamma^{j-2,k-n+j-2}_{[0..2^{j-2}-1]} \\ A^{-2}\gamma^{j,k-n+j}_{[3\cdot 2^{j-2}..2^{j}-1]} &= \rho^{j-2,k-n+j-2}_{[0..2^{j-2}-1]}. \end{aligned}$$

This implies $A^{-2}\gamma^{j,k-n+j}_{[0..2^{j-2}-1]} = \left(\gamma^{j-2,k-n+j-2}_{[0..2^{j-2}-1]}, \rho^{j-2,k-n+j-2}_{[0..2^{j-2}-1]}\right)^2$.
Similarly, we have:

$$\begin{aligned} A^{-2}\rho^{j,k-n+j}_{[0..2^{j-2}-1]} &= \gamma^{j-2,k-n+j-2}_{[0..2^{j-2}-1]} \\ A^{-2}\rho^{j,k-n+j}_{[2^{j-2}..2\cdot 2^{j-2}-1]} &= \rho^{j-2,k-n+j-2}_{[0..2^{j-2}-1]} \\ A^{-2}\rho^{j,k-n+j}_{[2\cdot 2^{j-2}..3\cdot 2^{j-2}-1]} &= \gamma^{j-2,k-n+j-2}_{[0..2^{j-2}-1]} \\ A^{-2}\rho^{j,k-n+j}_{[3\cdot 2^{j-2}..2^{j}-1]} &= \rho^{j-2,k-n+j-2}_{[0..2^{j-2}-1]} \end{aligned}$$

Therefore we have $A^{-2}\rho^{j,k-n+j}_{[0..2^{j-2}-1]} = \left(\gamma^{j-2,k-n+j-2}_{[0..2^{j-2}-1]}, \rho^{j-2,k-n+j-2}_{[0..2^{j-2}-1]}\right)^2$. We obtain:

$$A^{-2}\left(\gamma^{j,k-n+j}_{[0..2^j-1]}, \rho^{j-n,k-n+j}_{[0..2^j-1]}\right) = \left(\gamma^{j-2,k-n+j-2}_{[0..2^{j-2}-1]}, \rho^{j-2,k-n+j-2}_{[0..2^{j-2}-1]}\right)^4.$$

Consequently, since it is a concatenation power of $A^{-2}\left(\gamma^{j,k-n+j}_{[0..2^j-1]}, \rho^{j,k-n+j}_{[0..2^j-1]}\right)$, the sequence $A^{j-n-2}\gamma^{n,k}$ is a concatenation power of the sequence:

$\left(\gamma^{j-2,k-n+j-2}_{[0..2^{j-2}-1]}, \rho^{j-2,k-n+j-2}_{[0..2^{j-2}-1]}\right)$. Since the length of this last sequence is $2 \cdot 2^{j-2} = 2^{(j-2)+1}$, the sequence $A^{j-n-2}\gamma^{n,k}$ itself has period $2^{(j-2)+1}$ that is, the prop. of Lemma 6.1 also holds for $j-2$. This completes the proof. □

6.2 Mapping the structure of $\gamma^{n,k}$

Eqs. (18)–(19) leads to compute $\gamma^{n,k}$ by recursively applying a series of left-concatenation by words in A^2. As previously announced, in the spirit of Sect. 4 we introduce a matrix, namely C. The row index is $i \in [0, 2^n-1]$, the column index being $j \in J = \{n, n-2, \cdots, n_0+2, n_0\}$. More precisely, given $i \in [0, 2^n-1]$ we set:

$$\gamma^{n,k}_{[i]} = C^{[n]}_{[i]} C^{[n-2]}_{[i]} \cdots C^{[j+2]}_{[i]} C^{[j]}_{[i]} \cdots C^{[n_0+2]}_{[i]} C^{[n_0]}_{[i]}, \tag{26}$$
$$\text{with } C^{[n_0]}_{[i]} \in A^{n_0}, \text{ and } C^{[j]}_{[i]} \in A^2 \text{ for every } j \in J \setminus \{n_0\}.$$

The reasons that can be invoked for adopting such a reverse-order notation are the same that for the matrix H from Sect. 4. The row of index is $i \in [0, 2^n-1]$ is:

$$\left(C^{[n]}_{[i]}, C^{[n-2]}_{[i]}, \cdots C^{[j+2]}_{[i]}, C^{[j]}_{[i]}, \cdots, C^{[n_0+2]}_{[i]}, C^{[n_0]}_{[i]}\right) \tag{27}$$

In addition, we denote by $\mu(i,j)$ the unique integer in $[0, 2^{j+1}-1]$ st. $i = \mu(i,j) \bmod 2^{j+1}$. As a consequence of Lemma 6.1, we obtain the following result, which is the counterpart of Lemma 4.2 from Sect. 4:

Lemma 6.2. *With the preceding notation each of the following props. holds:*

(i) *For every $j \in J \setminus \{n_0, n\}$, we have $C^{[j]}_{[0..2^n-1]} = \mathrm{P}_2\left(A^{j-n}\gamma^{n,k}\right)$. In addition the sequence $C^{[j]}_{[0..2^n-1]}$ is a concatenation power of $C^{[j]}_{[0..2^{j+1}-1]}$.*

(ii) *For every $i \in [0, 2^n-1]$ we have:*

$$C^{[n_0]}_{[i]} = \begin{cases} C^{[n_0]}_{[i]} = \gamma^{n_0,1}_{[\mu(i,n_0)]} & \text{if } \ \mu(i,n_0) \in [0, 2^{n_0}-1] \\ C^{[n_0]}_{[i]} = \rho^{n_0,1}_{[\mu(i,n_0)-2^{n_0}]} & \text{if } \ \mu(i,n_0) \in [2^{n_0}, 2^{n_0+1}-1]. \end{cases}$$

(iii) *For every index pair $i \in [0, 2^n-1]$, $j \in J \setminus \{n_0\}$, we have:*

$$C^{[j]}_{[i]} = \begin{cases} \mathrm{P}_2\left(\gamma^{j,n-j+k}_{[\mu(i,j)]}\right) & \text{if } \ \mu(i,j) \in [0, 2^j-1] \\ \mathrm{P}_2\left(\rho^{j,n-j+k}_{[\mu(i,j)]-2^j}\right) & \text{if } \ \mu(i,j) \in [2^j, 2^{j+1}-1]. \end{cases}$$

Proof. (i) Let $j \in J \setminus \{n_0, n\}$ and $i \in [0, 2^{n-1}]$. According to Eq. (26) we have $C^{[j]}_{[i]} = \mathrm{P}_2\left(\left(C^{[n]}_{[i]} \cdots C^{[j+2)]}_{[i]}\right)^{-1} \gamma^{n,k}_{[i]}\right)$.

Since the sequence $\left(C^{[n]}_{[i]}, C^{[n-2]}_{[i]}, \cdots, C^{[n-(n-j-2])}_{[i]}\right)$ has length $\frac{n-j-2}{2}+1$, we have $\left|C^{[n]}_{[i]} \cdots C^{[j+2])}_{[i]}\right| = 2\left(\frac{n-j-2}{2}+1\right) = n-j$, thus $C^{[j]}_{[i]} = \mathrm{P}_2\left(A^{j-n}\gamma^{n,k}_{[i]}\right)$. As a consequence, we obtain $C^{[j]}_{[0..2^n-1]} = \mathrm{P}_2\left(A^{j-n}\gamma^{n,k}\right)$.

As a direct consequence, we have $C^{[j]}_{[0\cdots 2^{j+1}-1]} = \mathrm{P}_2\left(A^{j-n}\gamma^{n,k}_{[0..2^{j+1}-1]}\right)$. According to Lemma 6.1, the sequence $A^{j-n}\gamma^{n,k}$ is a power of $\left(\gamma^{j,k-n+j}_{[0..2^j-1]}, \rho^{j,k-n+j}_{[0..2^j-1]}\right)$, whence $C^{[j]}_{[0..2^n-1]} = \mathrm{P}_2\left(A^{j-n}\gamma^{n,k}\right)$ is a power of $\mathrm{P}_2\left(\gamma^{j,k-n+j}_{[0..2^j-1]}, \rho^{j,k-n+j}_{[0..2^j-1]}\right)$. In addition, since the sequence $A^{j-n}\gamma^{n,k}_{[0..2^{j+1}-1]}$ has length 2^{j+1}, we have $A^{j-n}\gamma^{n,k}_{[0..2^{j+1}-1]} = \left(\gamma^{j,k-n+j}_{[0..2^j-1]}, \rho^{j,k-n+j}_{[0..2^j-1]}\right)$.

This implies $C^{[j]}_{[0\cdots 2^{j+1}-1]} = \mathrm{P}_2\left(A^{j-n}\gamma^{n,k}_{[0..2^{j+1}-1]}\right) = \mathrm{P}_2\left(\gamma^{j,k-n+j}_{[0..2^j-1]}, \rho^{j,k-n+j}_{[0..2^j-1]}\right)$. Consequently, $\mathrm{P}_2\left(A^{j-n}\gamma^{n,k}\right)$ is a power of $\mathrm{P}_2\left(\gamma^{j,k-n+j}_{[0..2^j-1]}, \rho^{j,k-n+j}_{[0..2^j-1]}\right)$ that is, $C^{[j]}_{[0..2^n-1]}$ is a concatenation power of $C^{[j]}_{[0..2^{j+1}-1]}$. This completes the proof of prop. (i).

(ii) According to Eq. (26), we have $C^{[n_0]}_{[0\cdots 2^{n_0+1}-1]} = \left(\gamma^{n_0,1}_{[0\cdots 2^{n_0}-1]}, \rho^{n_0,1}_{[0\cdots 2^{n_0}-1]}\right)$. By taking $j = n_0 \in J$ in the statement of Lemma 6.1, we observe that the sequence $A^{n_0-n}\gamma^{n,k}$ is a power of $\left(\gamma^{n_0,1}_{[0..2^{n_0}-1]}, \rho^{n_0,1}_{[0..2^{n_0}-1]}\right)$ (we have $k-n+n_0 = 1$). Consequently, the condition $\mu(i, n_0) \in [0, 2^{n_0}-1]$, implies $C^{[n_0]}_{[i]} = \gamma^{n_0,1}_{[\mu(i,n_0)]}$. Similarly, the condition $\mu(i, n_0) \in [2^{n_0}, 2^{n_0+1}-1]$, implies $C^{[n_0]}_{[i]} = \rho^{n_0,1}_{[\mu(i,n_0)-2^{n_0}]}$. This establishes the prop. (ii) of Lemma 6.2.

(iii) Let $i \in [0, 2^n-1]$. According to the prop. (i) of our lemma, $C^{[j]}_{[0..2^n-1]}$ is 2^{j+1}-periodic. By the definition of $\mu(i,j)$ this implies $C^{[j]}_{[i]} = C^{[j]}_{[\mu(i,j)]}$. In addition, $C^{[j]}_{[\mu(i,j)]}$ is the term of index $\mu(i,j)$ in the sequence $\mathrm{P}_2\left(\gamma^{j,k-n+j}_{[0..2^j-1]}\rho^{j,k-n+j}_{[0..2^j-1]}\right)$, hence the prop. (iii) holds. □

According to Lemma 6.2, given $i \in [0, 2^{n_0+1}-1]$ the following equations hold :

$$C^{[n_0]}_{[i]} = \begin{cases} \gamma^{n_0,1}_{[i]} & \text{if} \quad i \in [0, 2^{n_0}-1] \\ \rho^{n_0,1}_{[i]} & \text{if} \quad i \in [2^{n_0}, 2^{n_0+1}-1] \end{cases} \tag{28}$$

In particular, we have $C^{[n_0]}_{[0]} = \gamma^{n_0,1}_{[0]}$.

Let $i \in [0, 2^n-1]$, $j \in J \setminus \{n, n_0\}$, and let q', r' be the unique integer pair st. $\mu(i,j) = q'2^{j-2} + r'$, with $r' \in [0, 2^{j-2}-1]$. It follows from $\mu(i,j) \in [0, 2^{j+1}-1]$ that we have $q' \in [0, 7]$, furthermore according to Eqs. (18)–(19) each of the following identities holds:

$$
\begin{array}{rl}
\gamma^{j,k-n+j}_{[r']} & = \theta^{r'}(00)\gamma^{j-2,k-n+j-2}_{[r']} \\
\gamma^{j,k-n+j}_{[2^{j-2}+r']} & = \theta^{r'}(01)\rho^{j-2,k-n+j-2}_{[r']} \\
\gamma^{j,k-n+j}_{[2.2^{j-2}+r']} & = \theta^{r'}(11)\gamma^{j-2,k-n+j-2}_{[r']} \\
\gamma^{j,k-n+j}_{[3.2^{j-2}+r']} & = \theta^{r'}(10)\rho^{j-2,k-n+j-2}_{[r']} \\
\rho^{j,k-n+j}_{[4\cdot 2^{j-2}+r']} & = \theta^{r'}(10)\gamma^{j-2,k-n+j-2}_{[r']} \\
\rho^{j,k-n+j}_{[5\cdot 2^{j-2}+r']} & = \theta^{r'}(11)\rho^{j-2,k-n+j-2}_{[r']} \\
\rho^{j,k-n+j}_{[6.2^{j-2}+r']} & = \theta^{r'}(01)\gamma^{j-2,k-n+j-2}_{[r']} \\
\rho^{j,k-n+j}_{[7.2^{j-2}+r']} & = \theta^{r'}(00)\rho^{j-2,k-n+j-2}_{[r']}.
\end{array}
\tag{29}
$$

According to the prop. (iii) of Lemma 6.2, we obtain the following equations:

$$
\begin{array}{rl}
C^{[j]}_{[r']} & = \theta^{r'}(00); \\
C^{[j]}_{[2^{j-2}+r']} & = \theta^{r'}(01); \\
C^{[j]}_{[2\cdot 2^{j-2}+r']} & = \theta^{r'}(11); \\
C^{[j]}_{[3\cdot 2^{j-2}+r']} & = \theta^{r'}(10); \\
C^{[j]}_{[4\cdot 2^{j-2}+r']} & = \theta^{r'}(10); \\
C^{[j]}_{[5\cdot 2^{j-2}+r']} & = \theta^{r'}(11); \\
C^{[j]}_{[6\cdot 2^{j-2}+r']} & = \theta^{r'}(01); \\
C^{[j]}_{[7\cdot 2^{j-2}+r']} & = \theta^{r'}(00).
\end{array}
\tag{30}
$$

In addition, for $j = n$, the following identities holds:

$$
\begin{array}{rl}
C^{[n]}_{[r']} & = \theta^{r'}(00); \\
C^{[n]}_{[2^{n-2}+r']} & = \theta^{r'}(01); \\
C^{[n]}_{[2\cdot 2^{n-2}+r']} & = \theta^{r'}(11); \\
C^{[n]}_{[3\cdot 2^{n-2}+r']} & = \theta^{r'}(10).
\end{array}
\tag{31}
$$

Thanks to the prop. (i) of Lemma 6.2, the eqs. (30), (31) directly provide the value of the component $C^{[j]}_{[i]}$, for every $i \in [0, 2^{n-1}]$. However, from an algorithmic point of view, in order to compute the whole matrix C, all the words $C^{[j]}_{[i]}$ should be memorized, for all the integer pairs $i \in [0, 2^{j+1}-1]$, $j \in J$. In other words we are still a long way from our goal. In view of that, in what follows we shall deepen the structure of Eqs. (30), (31). First of all we note that, given some index $i \in [1, 2^{n-1}]$, exactly one of the two following conds. occurs:

Condition $i \neq 0 \bmod 2^{j+1}$

With the preceding notation, this condition corresponds to $\mu(i,j) \geq 1$, thus $r' \geq 1$. According to Eqs. (30), (31), for every $j \in J \setminus \{n_0\}$ and for each integer pair $q' \in [0,7]$, $r' \in [0, 2^{j-2}-1]$, a unique word $x \in A^2$ exists st. $C^{[j]}_{[q'^{j-2}+r']} = \theta^{r'}(x)$

and $C^{[j]}_{[q'^{j-2}+(r'-1)]} = \theta^{r'-1}(x)$, therefore the following equation holds:

$$C^{[j]}_{[q'2^{j-2}+r']} = \theta\left(C^{[j]}_{[q'2^{j-2}+(r'-1)]}\right) \quad (1 \leq r' \leq 2^{j-2}-1). \tag{32}$$

Condition $i = 0 \bmod 2^{j+1}$

Actually, with this condition, which is equivalent to $r' = 0$, i.e. $\mu(i,j) = 0$, we are not able to directly establish a formula similar to Eq. (32). For instance in Eqs. (30), on the first hand, by taking $q' = 3$, we have $C^{[j]}_{[3\cdot 2^{j-2}-1]} = C^{[j]}_{[2\cdot 2^{j-2}+(2^{j-2}-1)]} = \theta^{2^{j-2}-1}(11) = 00$ and $C^{[j]}_{[q'3\cdot 2^{j-2}]} = 10$. On the other hand, by taking $q' = 6$, although still we have $C^{[j]}_{[6\cdot 2^{j-2}-1]} = C^{[j]}_{[5\cdot 2^{j-2}+(2^{j-2}-1)]} = \theta^{5^{j-2}-1}(11) = 00$, we have in fact $C^{[j]}_{[q'6^{j-2}]} = 01$. In other words, under current conditions, the formulas (30) and (31) cannot provide sufficient information to express $C^{[j]}_{[q'2^{j-2}]}$ directly, starting with $C^{[j]}_{[q'2^{j-2}-1]}$.

6.3 Some breakthrough thanks to a new matrix

In order to gather the missing information, we introduce a second matrix, namely Q. With the above notation, given an index pair $i \in [0, 2^n-1]$, $j \in J$, we set $Q^{[j]}_{[i]} = q'$ that is, $\mu(i,j) = Q^{[j]}_{[i]}2^{j-2} + r'$. The following equations come from Eqs. (30):

$$\begin{aligned}
\left(Q^{[j]}_{[r']}, C^{[j]}_{[r']}\right) &= \left(0, \theta^{r'}(00)\right)\\
\left(Q^{[j]}_{[2^{j-2}+r']}, C^{[j]}_{[2^{j-2}+r']}\right) &= \left(1, \theta^{r'}(01)\right)\\
\left(Q^{[j]}_{[2\cdot 2^{j-2}+r']}, C^{[j]}_{[2\cdot 2^{j-1}+r']}\right) &= \left(2, \theta^{r'}(11)\right)\\
\left(Q^{[j]}_{[3\cdot 2^{j-2}+r']}, C^{[j]}_{[3\cdot^{j-2}+r']}\right) &= \left(3, \theta^{r'}(10)\right)\\
\left(Q^{[j]}_{[2^j+r']}, C^{[j]}_{[2^j+r']}\right) &= \left(4, \theta^{r'}(10)\right)\\
\left(Q^{[j]}_{[5\cdot 2^{j-2}+r']}, C^{[j]}_{[5\cdot 2^{j-2}+r']}\right) &= \left(5, \theta^{r'}(11)\right)\\
\left(Q^{[j]}_{[6\cdot 2^{j-2}+r']}, C^{[j]}_{[6\cdot 2^{j-2}+r']}\right) &= \left(6, \theta^{r'}(01)\right)\\
\left(Q^{[j]}_{[7\cdot 2^{j-2}+r']}, C^{[j]}_{[7\cdot 2^{j-2}+r']}\right) &= \left(7, \theta^{r'}(00)\right).
\end{aligned} \tag{33}$$

In addition, for $j = n$, the following equations come from Eqs. (31):

$$\begin{aligned}
\left(Q^{[n]}_{[r']}, C^{[n]}_{[r']}\right) &= \left(0, \theta^{r'}(00)\right)\\
\left(Q^{[n]}_{[2^{n-2}+r']}, C^{[n]}_{[2^{n-2}+r']}\right) &= \left(1, \theta^{r'}(01)\right)\\
\left(Q^{[n]}_{[2^{n-1}+r']}, C^{[n]}_{[2^{n-1}+r']}\right) &= \left(2, \theta^{r'}(10)\right)\\
\left(Q^{[n]}_{[3\cdot 2^{n-2}+r']}, C^{[n]}_{[3\cdot 2^{n-2}+r']}\right) &= \left(3, \theta^{r'}(11)\right).
\end{aligned} \tag{34}$$

Regarding periodicity of the sequences, the following prop. comes from Lemma 6.2:

Lemma 6.3. *For every $j \in J \setminus \{n_0\}$ the sequence $\left(Q_{[i]}^{[j]}, C_{[i]}^{[j]}\right)_{0 \leq i \leq 2^n - 1}$ is 2^{j+1}-periodic.*

Proof. Let $i_1, i_2 \in [0, 2^n - 1]$ st. $i_1 - i_2 = 0 \bmod 2^{j+1}$. By definition the integers $\mu(i_1, j), \mu(i_2, j) \in [0, 2^{j+1} - 1]$ are equal, whence $Q_{[i_1]}^{[j]}$, $Q_{[i_2]}^{[j]}$, their corresponding euclidian quotients by 2^{j-2} are equal. In addition, according to prop. (i) of Lemma 6.2, the sequence $C_{[0 \cdot \cdot 2^n - 1]}^{[j]}$ is 2^{j+1}-periodic, therefore we have $C_{[i_1]}^{[j]} = C_{[i_2]}^{[j]}$. □

In view of Eqs. (33), (34), and Lemma 6.3, we introduce the following 8-element cycle:

$$\pi = ((0, 00), (1, 01), (2, 11), (3, 10), (4, 10), (5, 11), (6, 01), (7, 00))$$

that is, $\pi((0, 00) = (1, 01), \pi(1, 01) = (2, 11), \cdots, \pi(6, 01) = (7, 00), \pi(7, 00) = ((0, 00)$.

Recall that we have $\mu(i, j) = Q_{[i]}^{[j]} 2^{j-2} + r'$.

Lemma 6.4. *With the preceding notation, for every integer pair $i \in [1, 2^n - 1]$, $j \in J \setminus \{n_0\}$, the following equation holds:*

$$\left(Q_{[i]}^{[j]}, C_{[i]}^{[j]}\right) = \begin{cases} \left(Q_{[i-1]}^{[j]}, \theta\left(C_{[i-1]}^{[j]}\right)\right) & \text{if } \ r' \neq 0, \\ \pi\left(Q_{[i-2^{j-2}]}^{[j]}, C_{[i-2^{j-2}]}^{[j]}\right) & \text{otherwise.} \end{cases}$$

Proof. Let $j \in J \setminus \{n_0\}$. According to the value of $r' \in [0, 2^j - 1]$ exactly one of the two following conditions occurs:

(i) *Condition $r' \neq 0$*
According to Eqs. (33), (34), we obtain $\left(Q_{[\mu(i,j)]}^{[j]}, C_{[\mu(i,j)]}^{[j]}\right) = \left(Q_{[\mu(i,j)-1]}^{[j]}, \theta\left(C_{[\mu(i,j)-1]}^{[j]}\right)\right) = \left(Q_{[\mu(i-1,j)]}^{[j]} \theta\left(C_{[\mu(i-1,j)]}^{[j]}\right)\right)$. According to Lemma 6.3, we have $C_{[i]}^{[j]} = C_{[\mu(i,j)]}^{[j]}$ and $C_{[i-1]}^{[j]} = C_{[\mu(i-1,j)]}^{[j]}$: this implies $\left(Q_{[i]}^{[j]}, C_{[i]}^{[j]}\right) = \left(Q_{[i-1]}^{[j]}, \theta\left(C_{[i-1]}^{[j]}\right)\right)$.

(ii) *Condition $r' = 0$*
According to the value of the index i, exactly one of the three following cases occurs:

(ii.i) *The case where we have $i \in [1, 2^{j+1} - 1]$*
According to Eqs. (33) each of the following identities hold (in the case

where we have $j = n$, only the first four hold):

$$\begin{aligned}
\left(Q^{[j]}_{[2^{j-2}]}, C^{[j]}_{[2^{j-2}]}\right) &= (1, 01)\\
\left(Q^{[j]}_{[2\cdot 2^{j-2}]}, C^{[j]}_{[2\cdot 2^{j-1}]}\right) &= (2, 11)\\
\left(Q^{[j]}_{[3\cdot 2^{j-2}]}, C^{[j]}_{[3\cdot j-2]}\right) &= (3, 10)\\
\left(Q^{[j]}_{[2^{j}]}, C^{[j]}_{[2^{j}]}\right) &= (4, 10)\\
\left(Q^{[j]}_{[5\cdot 2^{j-2}]}, C^{[j]}_{[5\cdot 2^{j-2}]}\right) &= (5, 11)\\
\left(Q^{[j]}_{[6\cdot 2^{j-2}]}, C^{[j]}_{[6\cdot 2^{j-2}]}\right) &= (6, 01)\\
\left(Q^{[j]}_{[7\cdot 2^{j-2}]}, C^{[j]}_{[7\cdot 2^{j-2}]}\right) &= (7, 00)\,.
\end{aligned} \tag{35}$$

According to Eqs. (35), for every $q' \in [1, 7]$ we have:

$$\left(Q^{[j]}_{[q'\cdot 2^{j-2}]}, C^{[j]}_{[q'\cdot 2^{j-2}]}\right) = \pi\left(Q^{[j]}_{[(q'-1)\cdot 2^{j-2}]}, C^{[j]}_{[(q'-1)\cdot 2^{j-2}]}\right).$$

On the other hand, by definition $i \in [1, 2^{j+1} - 1]$ implies $i = \mu(i, j) = Q^{[j]}_{[i]} \cdot 2^{j-2} + r' = q' \cdot 2^{j-2} + r' = q' \cdot 2^{j-2}$, thus $i - 2^{j-2} = (q' - 1)2^{j-2}$. We obtain:

$$\left(Q^{[j]}_{[i]}, C^{[j]}_{[i]}\right) = \left(Q^{[j]}_{[q'\cdot 2^{j-2}]}, C^{[j]}_{[q'\cdot 2^{j-2}]}\right) = \pi\left(Q^{[j]}_{[i-2^{j-2}]}, C^{[j]}_{[i-2^{j-2}]}\right).$$

(ii.ii) *The case where $i = 0 \bmod 2^{j+1}$*

On the one hand, according to Lemma 6.3, we have $\left(Q^{[j]}_{[i]}, C^{[j]}_{[i]}\right) = \left(Q^{[j]}_{[0]}, C^{[j]}_{[0]}\right) = (0, 00)$. On the other hand, we have $i - 2^{j-2} = -2^{j-2} \bmod 2^{j+1} = 2^{j+1} - 2^{j-2} \bmod 2^{j+1}$, thus $i - 2^{j-2} = 8 \cdot 2^{j-2} - 2^{j-2} \bmod 2^{j+1} = 7 \bmod 2^{j+1}$. According to Lemma 6.3 and Eqs. (35), we obtain $\left(Q^{[j]}_{[i-2^{j-2}]}, C^{[j]}_{[i-2^{j-2}]}\right) = \left(Q^{[j]}_{[7\cdot 2^{j-2}]}, C^{[j]}_{[7\cdot 2^{j-2}]}\right) = (7, 00)$: once more we have $\left(Q^{[j]}_{[i]}, C^{[j]}_{[i]}\right) = \pi\left(Q^{[j]}_{[i-2^{j-2}]}, C^{[j]}_{[i-2^{j-2}]}\right)$.

(ii.iii) *The case where $i \in [2^{j+1} + 1, 2^n - 1]$, with $i \neq 0 \bmod 2^{j+1}$*

By definition we have $\mu(i, j) \in [1, 2^{j+1} - 1]$. On the one hand, by substituting $\mu(i, j)$ to i in the preceding case (ii.i), we obtain: $\left(Q^{[j]}_{[\mu(i,j)]}, C^{[j]}_{[\mu(i,j)]}\right) = \left(Q^{[j]}_{[\mu(i,j)-2^{j-2}]}, C^{[j]}_{[\mu(i,j)-2^{j-2}]}\right)$. On the other hand, by the definition of μ we have $i = q\cdot 2^{j+1} + \mu(i, j)$, thus $i - 2^{j-2} = q\cdot 2^{j+1} + \big(\mu(i, j) - 2^{j-2}\big)$. Since we have $r' = 0$ and $\mu(i, j) \geq 1$ a positive integer $q' \geq 1$ exists st. $\mu(i, j) = q' \cdot 2^{j-2}$. It follows from $\mu(i, j) - 2^{j-2} = (q' - 1)2^{j-2} \geq 0$ and $\mu(i, j) - 2^{j-2} \leq 2^{j+1} - 1$ that $\mu(i, j) - 2^{j-2} \in [0, 2^{j+1} - 1]$. By the definition of μ we obtain $\mu(i - 2^{j-2}, j) = \mu(i, j) - 2^{j-2}$, thus $\left(Q^{[j]}_{[\mu(i,j)-2^{j-2}]}, C^{[j]}_{[\mu(i,j)-2^{j-2}]}\right) = \left(Q^{[j]}_{[\mu(i-2^{j-2},j)]}, C^{[j]}_{[\mu(i-2^{j-2},j)]}\right)$. According to Lemma 6.3, we obtain:

$$\left(Q^{[j]}_{[i]}, C^{[j]}_{[i]}\right) = \left(Q^{[j]}_{[\mu(i,j)]}, C^{[j]}_{[\mu(i,j)]}\right) = \left(Q^{[j]}_{[\mu(i-2^{j-2},j)]}, C^{[j]}_{[\mu(i-2^{j-2},j)]}\right) = \pi\left(Q^{[j]}_{[i-2^{j-2}]}, C^{[j]}_{[i-2^{j-2}]}\right).$$

This completes the proof of Lemma 6.4. □

Lemma 6.4 shows that the condition $r' = 0$ plays a prominent part in the computation of $\left(Q_{[i]}^{[j]}, C_{[i]}^{[j]}\right)$. The following result provides some precision:

Lemma 6.5. *With the preceding notation, the three following conditions are equivalent:*
(i) $r' = 0$*;*
(ii) $\mu(i,j) = 0 \bmod 2^{j-2}$*;*
(iii) $i = 0 \bmod 2^{j-2}$.

Proof. It follows from $\mu(i,j) = Q_{[i]}^{[j]} 2^{j-2} + r'$, with $r' \in [0, 2^{j-2} - 1]$, that the two conditions $\mu(i,j) = 0 \bmod 2^{j-2}$ and $r' = 0$ are equivalent. According to the definition of μ, some integer $m \in \mathbb{N}$ exists st. $i = \mu(i,j) + m2^{j+1}$. As a consequence, if we have $i = 0 \bmod 2^{j-2}$, some integer $m' \in \mathbb{N}$ exists st. $\mu(i,j) + m2^{j+1} = m'2^{j-2}$, thus $\mu(i,j) = (m' - 8m)2^{j-2}$ that is, $\mu(i,j) = 0 \bmod 2^{j-2}$. Conversely if $m' \in \mathbb{N}$ exists st. $\mu(i,j) = m'2^{j-2}$, we obtain $i = m'2^{j-2} + m2^{j+1}$ that is, $i = (m' + 8m)2^{j-2}$, thus $i = 0 \bmod 2^{j-2}$. □

6.4 The loopless algorithm

Nevertheless, we have not fully achieved our objective: indeed, in the statement of Lemma 6.4, in order to compute $\left(Q_{[i]}^{[j]}, C_{[i]}^{[j]}\right)$, the condition $i = 0 \bmod 2^{j-2}$ imposes to memorize the component $\left(Q_{[i-2^{j-2}]}^{[j]}, C_{[i-2^{j-2}]}^{[j]}\right)$. Our goal is to prove that such a computation can be actually done by only referring to the pair $\left(Q_{[i-1]}^{[j]}, C_{[i-1]}^{[j]}\right)$. In order to do so we need to introduce some additional concept: we denote by ϕ be the partial mapping onto $[0,7] \times A^2$ defined by $\phi\left(q', \theta^{-1}(c)\right) = \pi\left(q', c\right)$, for each pair (q', c) in the cycle π. By definition ϕ takes the following values:

(q', c)	$(0,11)$	$(1,10)$	$(2,00)$	$(3,01)$	$(4,01)$	$(5,00)$	$(6,10)$	$(7,11)$
$\phi(q', c)$	$(1,01)$	$(2,11)$	$(3,10)$	$(4,10)$	$(5,11)$	$(6,01)$	$(7,00)$	$(0,00)$

(36)

The following property is the basis to an iterative algorithm to compute the whole sequence $\gamma^{n,k}$:

Proposition 6.6. *With the preceding notation, for every $i \in [1, 2^n - 1]$, $j \in J \setminus \{n_0\}$, the following identity holds:*

$$\left(Q_{[i]}^{[j]}, C_{[i]}^{[j]}\right) = \begin{cases} \left(Q_{[i-1]}^{[j]}, \theta\left(C_{[i-1]}^{[j]}\right)\right) & \text{if } \ i \neq 0 \bmod 2^{j-2} \\ \phi\left(Q_{[i-1]}^{[j]}, C_{[i-1]}^{[j]}\right) & \text{otherwise.} \end{cases}$$

Proof. According to Lemmas 6.4, 6.5 we restrain to the case where we have $i = 0 \bmod 2^{j-2}$ that is, with the preceding notation, $r' = 0$ and $\mu(i,j) = q' \cdot 2^{j-2}$. As in proof of Lemma 6.3 exactly one of the three following conditions holds:

(i) *The case where we have* $i \in [1, 2^{j+1}-1]$
With this condition we have $i = \mu(i,j) \geq 1$. Firstly, we assume $j < n$. According to Eqs. (35), and by the definition of ϕ each of the following identities holds:

$$\begin{aligned}
\left(Q^{[j]}_{[2^{j}-2]}, C^{[j]}_{[2^{j}-2]}\right) &= (1,01) = \pi(0,00) = \phi\,(0,11)\\
\left(Q^{[j]}_{[2\cdot 2^{j}-2]}, C^{[j]}_{[2\cdot 2^{j}-1]}\right) &= (2,11) = \pi(1,01) = \phi\,(1,10)\\
\left(Q^{[j]}_{[3\cdot 2^{j}-2]}, C^{[j]}_{[3\cdot 2^{j}-2]}\right) &= (3,10) = \pi(1,11) = \phi\,(2,00)\\
\left(Q^{[j]}_{[4\cdot 2^{j}-2]}, C^{[j]}_{[4\cdot 2^{j}-2]}\right) &= (4,10) = \pi(3,10) = \phi\,(3,01)\\
\left(Q^{[j]}_{[5\cdot 2^{j}-2]}, C^{[j]}_{[5\cdot 2^{j}-2]}\right) &= (5,11) = \pi(4,10) = \phi\,(4,01)\\
\left(Q^{[j]}_{[6\cdot 2^{j}-2]}, C^{[j]}_{[6\cdot 2^{j}-2]}\right) &= (6,01) = \pi(5,11) = \phi\,(5,00)\\
\left(Q^{[j]}_{[7\cdot 2^{j}-2]}, C^{[j]}_{[7\cdot 2^{j}-2]}\right) &= (7,00) = \pi(6,01) = \phi\,(6,10)\,.
\end{aligned} \tag{37}$$

In the case where we have $j = n$, only the first four equations hold. It is straightforward to verify that , for each $q' \in [1,7]$, we have, $\left(Q^{[j]}_{[q'2^{j}-2]}, C^{[j]}_{[q'2^{j}-2]}\right) = \phi\left(Q^{[j]}_{[q'2^{j}-2-1)]}, C^{[j]}_{[q'2^{j}-2-1)]}\right)$ that is, $\left(Q^{[j]}_{i}, C^{[j]}_{[i]}\right) = \phi\left(Q^{[j]}_{[i-1]}, (Q^{[j]}_{[i-1]}\right)$.

(ii) *The case where* $i = 0 \bmod 2^{j+1}$
Let q be the unique positive integer st. $i = q \cdot 2^{j+1}$. On the one hand, according to Lemma 6.3, we have $\left(Q^{[j]}_{[i]}, C^{[j]}_{[i]}\right) = \left(Q^{[j]}_{[0]}, C^{[j]}_{[0]}\right) = (0,00) = \phi(7,11)$. On the other hand, we have $i - 1 = q \cdot 2^{j+1} - 1 = (q-1)2^{j+1} + (2^{j+1}-1)$. It follows from $j \geq 1$ that $2^{j+1} - 1 \in [0, 2^{j+1}-1]$, whence we have $\mu(i-1,j) = 2^{j+1}-1$. This implies $\left(Q^{[j]}_{[i-1]}, C^{[j]}_{[i-1]}\right) = \left(Q^{[j]}_{[2^{j+1}-1]}, C^{[j]}_{[2^{j+1}-1]}\right)$: we are in the condition of Eqs. (33) with $q' = 7$ and $r' = 2^{j-2} - 1$. We obtain $\left(Q^{[j]}_{[2^{j+1}-1]}, C^{[j]}_{[2^{j+1}-1]}\right) = \left(Q^{[j]}_{7\cdot 2^{j-2}+(2^{j-2}-1)]}, C^{[j]}_{[7\cdot 2^{j-2}+(2^{j-2}-1)]}\right) = \left(7, \theta^{2^{j-2}-1}(00)\right) = (7,11)$. As a consequence, once more we have $\left(Q^{[j]}_{[i]}, C^{[j]}_{[i]}\right) = \phi\left(Q^{[j]}_{[i-1]}, C^{[j]}_{[i-1]}\right)$.

(iii) *The case where* $i \in [2^{j+1}+1, 2^{n}-1]$ *and* $i \neq 0 \bmod 2^{j+1}$
On the one hand, with this condition we have $\mu(i,j) \in [1, 2^{j+1}-1]$. By substituting $\mu(i,j)$ to i in the preceding case (i) we obtain:
$\left(Q^{[j]}_{[\mu(i,j)]}, C^{[j]}_{[\mu(i,j)]}\right) = \phi\left(Q^{[j]}_{[\mu(i,j)-1]}, C^{[j]}_{[\mu(i,j)-1]}\right)$.

On the other hand, by the definition of μ we have $i = q \cdot 2^{j+1} + \mu(i,j)$: this implies $i - 1 = q \cdot 2^{j+1} + (\mu(i,j) - 1)$. It follows from $i \neq 0 \bmod 2^{j+1}$ that $\mu(i,j) - 1 \in [0, 2^{j+1}-1]$, therefore we have $\mu(i,j) - 1 = \mu(i-1,j)$. As a consequence, we obtain $\left(Q^{[j]}_{[\mu(i,j)]}, C^{[j]}_{[\mu(i,j)]}\right) = \phi\left(Q^{[j]}_{[\mu(i-1,j)]}, C^{[j]}_{[\mu(i-1,j)]}\right)$. According to Lemma 6.3, this implies $\left(Q^{[j]}_{[i]}, C^{[j]}_{[i]}\right) = \phi\left(Q^{[j]}_{[i-1]}, C^{[j]}_{[i-1]}\right)$: this completes the proof. □

According to the result of Proposition 6.6 we obtain an iteration-based method for computing the sequence $\gamma^{n,k}$ (see Algorithm 2). Recall that we set $C^{[n_0]}_{[0]} =$

$\gamma^{n_0,1}$. From the point of view of implementation, in the spirit of Algorithm 1, for every $i \in [0, 2^n - 1]$ the two following objects:

– The component $C_{[i]}^{[n_0]}$

– the row $\left(\left(Q_{[i]}^{[n]}, C_{[i]}^{[n]}\right), \left(Q_{[i]}^{[n-2]}, C_{[i]}^{[n-2]}\right), \cdots, \left(Q_{[i]}^{[n_0+2]}, C_{[i]}^{[n_0+2]}\right)\right)$,

are memorized in the corresponding generic components:

– $\mathcal{C}^{[n_0]}$

– $\left(\left(\mathcal{Q}^{[n]}, \mathcal{C}^{[n]}\right), \left(\mathcal{Q}^{[n-2]}, \mathcal{C}^{[n-2]}\right), \cdots, \left(\mathcal{Q}^{[n_0+2]}, \mathcal{C}^{[n_0+2]}\right)\right)$.

Each time the counter i is incremented these generic components are updated. According to Eqs. 28, the column $C^{[n_0]}$ takes the following expression:

$$C_{[0\cdot\cdot 2^{n_0+1}-1]}^{[n_0]} = \left(\gamma^{n_0,1}, \rho^{n_0,1}\right), \quad C^{[n_0]} = \left(\gamma^{n_0,1}, \rho^{n_0,1}\right)^{2^{n-n_0-1}}. \tag{38}$$

From this point of view, we start the computation by setting: $\mathcal{C}^{n_0} = C_{[0]}^{[n_0]} = \gamma_{[0]}^{n_0,1}$.

Some comments about Algorithm 2

The variable b takes values in the two-symbol set $\{\gamma, \rho\}$: its role is to determine which of Eqs. (33), (34) should be applied in order to compute the value of the pair $\left(Q_{[i]}^{[n_0}, C_{[i]}^{[n_0]}\right)$ (lines 7–11). According to the prop. (ii) of Lemma 6.2, the variable b, which is initialized to γ, is actualized each time the integer $\mu_0 = \mu(i, 2^{n_0+2})$ meets some element of $\{2^{n_0}, 2^{n_0+1}\}$ (lines 12–17). The result of Proposition 6.6, for its part, is applied at lines 19–26.

Questions related to complexity

The study is similar to the one of Sect. 4, and it leads to similar conclusions. Beforehand we note that, in any case, the alphabet A and the permutation θ should be computed in a preprocessing phase.

– Regarding the generic row $\left(\left(\mathcal{Q}^{[n]}, \mathcal{C}^{[n]}\right), \cdots, \left(\mathcal{Q}^{[n_0+1]}, \mathcal{C}^{[n_0+1]}\right)\right)$, there is a positive integer, say ℓ (the maximum cost of each operation over every component), st. updating the sequence requires at most $\ell(n - n_0 - 1) = \ell k$ insertions. Consequently, when the counter i reaches the value $i_{max} + 1$, the total amount of operations is at most $2^n \ell k$.

– In order to compute the component $\mathcal{C}^{[n_0]}$, as for Algorithm 1 there are two possible approaches:

(a) Firstly, for each value of $i \in [1, 2^{n_0} - 1]$ we apply the instruction (2) from Algorithm (b) (see the preliminaries). Computing each of the finite sequences $\gamma^{n_0,1}$, $\rho^{n_0,1}$, classically requires an amount of $2^{n_0} + 2^{n_0-1} + \cdots + 2 \leq 2^{n_0}$ one-character substitutions, therefore for computing the whole column $C^{[n_0]}$, the total cost of the preceding operations is bounded by $2^{n-n_0} \cdot 2 \cdot 2^{n_0} = 2^{n+1}$. Consequently the total amount of operations is bounded by $2^{n+1}\ell k + 2^{n+1} = 2^{n+1}(\ell k+1)$. This leads to a computation in amortized time of $2^{-n}2^{n+1}(\ell k+1) = O(1)$, with space linear in n.

(b) The second approach consists in implementing in a preprocessing phase the sequences $\gamma^{n_0,1}$, $\rho^{n_0,1}$ and the mappings π, ϕ : such an implementation

requires space $O(n_0 2^{n_0})$ and, as indicated above, a total amount of $O(2^{n_0})$ substitutions, with space $O(n_0 2^{n_0})$. After that, in the processing phase, updating $\mathcal{C}^{n_0}$ will be performed by a constant number of requests to $\gamma^{n_0,1}$, $\gamma^{n_0,1}$, π and ϕ, say ℓ_1 (see lines 19-23). Consequently, in the processing phase updating the matrices $\mathcal{C}^{[n..n_0+1]}$, $\mathcal{Q}^{[n..n_0+1]}$ requires at most $\ell + \ell_1 k$ operations: with this second strategy of implementation Algorithm 2 is loopless and requires space linear in $n + n_0 2^{n_0}$.

Algorithm 2

1: $n_0 \leftarrow n - k + 1$; $i \leftarrow 0$; $b \leftarrow \gamma$; $j \leftarrow n_0 + 2$; $\mathcal{C}^{[n_0]} \leftarrow \gamma_{[0]}^{n_0,1}$
2: **while** $j \leq n$ **do**
3: $\quad \left(\mathcal{Q}^{[j]}, \mathcal{C}^{[j]}\right) \leftarrow (0, 00)$; $\gamma_{[i]}^{n,k} \leftarrow \mathcal{C}^{[j]} \gamma_{[i]}^{n,k}$; $j \leftarrow j + 2$
4: **end while**
5: $max \leftarrow 2^n - 1$; $i \leftarrow 1$; $\mu_0 \leftarrow 1$
6: **while** $i \leq max$ **do**
7: $\quad$ **if** $b = \gamma$ **then**
8: $\quad\quad \mathcal{C}^{[n_0]} \leftarrow \gamma_{[i]}^{n_0,1}$
9: $\quad$ **else**
10: $\quad\quad \mathcal{C}^{[n_0]} \leftarrow \rho_{[i-2^{n_0}]}^{n_0,1}$
11: $\quad$ **end if**;
12: $\quad$ **if** $\mu_0 = 2^{n_0}$ **then**
13: $\quad\quad b \leftarrow \rho$
14: $\quad$ **end if**;
15: $\quad$ **if** $\mu_0 = 2^{n_0+1}$ **then**
16: $\quad\quad \mu_0 \leftarrow 1$; $b \leftarrow \gamma$
17: $\quad$ **end if**
18: $\quad j \leftarrow n_0 + 2$
19: $\quad$ **while** $j \leq n$ **do**
20: $\quad\quad$ **if** $i \neq 0 \bmod 2^{j-2}$ **then**
21: $\quad\quad\quad \left(\mathcal{Q}^{[j]}, \mathcal{C}^{[j]}\right) \leftarrow \left(\mathcal{Q}^{[j]}, \theta\left(\mathcal{C}^{[j]}\right)\right)$
22: $\quad\quad$ **else**
23: $\quad\quad\quad \left(\mathcal{Q}^{[j]}, \mathcal{C}^{[j]}\right) \leftarrow \phi\left(\mathcal{Q}^{[j]}, \mathcal{C}^{[j]}\right)$
24: $\quad\quad$ **end if**;
25: $\quad\quad \gamma_{[i]}^{n,k} \leftarrow \mathcal{C}^{[j]} \gamma_{[i]}^{n,k}$; $j \leftarrow j + 2$
26: $\quad$ **end while**
27: $\quad i \leftarrow i + 1$; $\mu_0 \leftarrow \mu_0 + 1$
28: **end while**

$(0,00)$	$(0,00)$	00	$(1,01)$	$(4,10)$	00	$(2,11)$	$(0,00)$	00	$(3,10)$	$(4,10)$	00
$(0,11)$	$(0,11)$	10	$(1,10)$	$(4,01)$	10	$(2,00)$	$(0,11)$	10	$(3,01)$	$(4,01)$	10
$(0,00)$	$(0,00)$	11	$(1,01)$	$(4,10)$	11	$(2,11)$	$(0,00)$	11	$(3,10)$	$(4,10)$	11
$(0,11)$	$(0,11)$	01	$(1,10)$	$(4,01)$	01	$(2,00)$	$(0,11)$	01	$(3,01)$	$(4,01)$	01
$(0,00)$	$(1,01)$	10	$(1,01)$	$(5,11)$	10	$(2,11)$	$(1,01)$	10	$(3,10)$	$(5,11)$	10
$(0,11)$	$(1,10)$	00	$(1,10)$	$(5,00)$	00	$(2,10)$	$(1,10)$	00	$(3,01)$	$(5,00)$	00
$(0,00)$	$(1,01)$	01	$(1,01)$	$(5,11)$	01	$(2,11)$	$(1,01)$	01	$(3,10)$	$(5,11)$	01
$(0,11)$	$(1,10)$	11	$(1,10)$	$(5,00)$	11	$(2,00)$	$(1,10)$	11	$(3,01)$	$(5,00)$	11
$(0,00)$	$(2,11)$	00	$(1,01)$	$(6,01)$	00	$(2,11)$	$(2,11)$	00	$(3,10)$	$(6,01)$	00
$(0,11)$	$(2,00)$	10	$(1,10)$	$(6,10)$	10	$(2,00)$	$(2,00)$	10	$(3,01)$	$(6,10)$	10
$(0,00)$	$(2,11)$	11	$(1,01)$	$(6,01)$	11	$(2,11)$	$(2,11)$	11	$(3,10)$	$(6,01)$	11
$(0,11)$	$(2,00)$	01	$(1,10)$	$(6,10)$	01	$(2,00)$	$(2,00)$	01	$(3,01)$	$(6,10)$	01
$(0,00)$	$(3,10)$	10	$(1,01)$	$(7,00)$	10	$(2,11)$	$(3,10)$	10	$(3,10)$	$(7,00)$	10
$(0,11)$	$(3,01)$	00	$(1,10)$	$(7,11)$	00	$(2,00)$	$(3,01)$	00	$(3,01)$	$(7,11)$	00
$(0,00)$	$(3,10)$	01	$(1,01)$	$(7,00)$	01	$(2,11)$	$(3,10)$	01	$(3,10)$	$(7,00)$	01
$(0,11)$	$(3,01)$	11	$(1,10)$	$(7,11)$	11	$(2,00)$	$(3,01)$	11	$(3,01)$	$(7,11)$	11

7 The case where we have $|A| = 2$ and k even

Let k be a positive even integer. Beforehand, we remind some classical algebraic interpretation of the substitution σ_k in the framework of the binary alphabet $A = \{0, 1\}$. Denote by $\oplus$ the addition in the group $\mathbb{Z}/2\mathbb{Z}$ with identity 0. Given a positive integer n, and $w, w' \in A^n$, define $w \oplus w'$ as the unique word of A^n st. $(w \oplus w')_i = w_i \oplus w'_i$, for each $i \in [1, n]$. With this notation the sets A^n and $(\mathbb{Z}/2\mathbb{Z})^n$ are in one-to-one correspondence. Moreover we have $w' \in \sigma_k(w)$ iff. some word $u \in A^n$ exists st. $|u|_1 = k$ and $w = w' \oplus u$: since k is even, we obtain $|w|_1 = |w'|_1 \bmod 2$. Consequently, given a σ_k-Gray cycle $\left(\alpha_{[i]}\right)_{0 \le i \le m}$, for each $i \in [0, m]$ the equation $\left|\alpha_{[i]}\right|_1 = \left|\alpha_{[0]}\right|_1 \bmod 2$ holds. As a corollary, setting $\mathrm{Even}_1^n = \{w \in A^* : |w|_1 = 0 \bmod 2\}$ and $\mathrm{Odd}_1^n = \{w \in A^* : |w|_1 = 1 \bmod 2\}$, we obtain the following property:

Lemma 7.1. *With the condition of Section 7, given a σ_k-Gray cycle α over X, either we have $X \subseteq \mathrm{Even}_1^n$, or we have $X \subseteq \mathrm{Odd}_1^n$.*

Given an even integer n, we define the sequences $\gamma^{n,k}$ and $\underline{\gamma}^{n,k}$ as indicated in the following:

$$(\forall i \in [0, 2^{n-1} - 1]) \quad \gamma_{[i]}^{n,k} = \theta^i(0)\gamma_{[i]}^{n-1,k-1} \quad \text{and} \quad \underline{\gamma}_{[i]}^{n,k} = \theta^i(1)\gamma_{[i]}^{n-1,k-1}. \tag{39}$$

According to Proposition 5.6, since $k-1$ is an odd integer the sequence $\gamma^{n-1,k-1}$ is a σ_{k-1}-Gray cycle over A^{n-1}.

For instance, we have $\gamma_{[0]}^{6,4} = 000000$, $\underline{\gamma}_{[0]}^{6,4} = 100000$, $\gamma_{[1]}^{6,4} = 111100$, and $\underline{\gamma}_{[1]}^{6,4} = 011100$.

Proposition 7.2. *The sequence $\gamma^{n,k}$ (resp., $\underline{\gamma}^{n,k}$) is a σ_k-Gray cycle over* Even_1^n *(resp.,* Odd_1^n*).*

Proof. (i) According to Eqs. (39), since $\gamma^{n-1,k-1}$ satisfies Cond. (G3), by construction both the sequences $\gamma^{n,k}$ and $\underline{\gamma}^{n,k}$ also satisfy (G3).

(ii) By Lemma 7.1, we have $\bigcup_{0\leq i\leq 2^n-1}\left\{\gamma^{n,k}\right\}\subseteq \mathrm{Even}_1^n$ and $\bigcup_{0\leq i\leq 2^n-1}\left\{\underline{\gamma}^{n,k}\right\}\subseteq \mathrm{Odd}_1^n$. In addition, according to Eqs. (39), we have $\left|\gamma^{n,k}\right| = \left|\underline{\gamma}^{n,k}\right| = \left|\gamma^{n-1,k-1}\right| = 2^{n-1} = |\mathrm{Even}_1^n|$. This implies $\bigcup_{0\leq i\leq 2^n-1}\left\{\gamma^{n,k}\right\} = \mathrm{Even}_1^n$ and $\bigcup_{0\leq i\leq 2^n-1}\left\{\underline{\gamma}^{n,k}\right\} = \mathrm{Odd}_1^n$ that is, both the sequences $\gamma^{n,k}$ and $\underline{\gamma}^{n,k}$ satisfy Cond. (G1).

(iii) Let $i\in[1,2^{n-1}-1]$. Since $\gamma^{n-1,k-1}$ satisfies (G2), we have $\gamma_{[i]}^{n-1,k-1}\in\sigma_{k-1}\left(\gamma_{[i-1]}^{n-1,k-1}\right)$. According to Eqs. (39), the initial characters of $\gamma_{[i]}^{n,k}$ and $\gamma_{[i-1]}^{n,k}$ (resp., $\underline{\gamma}_{[i]}^{n,k}$ and $\underline{\gamma}_{[i-1]}^{n,k}$) are different, hence we have $\gamma_{[i]}^{n,k}\in\sigma_k\left(\gamma_{[i-1]}^{n,k}\right)$ and $\underline{\gamma}_{[i]}^{n,k}\in\sigma_k\left(\underline{\gamma}_{[i-1]}^{n,k}\right)$. In addition, once more according to Eqs. (39) it follows from $\gamma_{[0]}^{n-1,k-1}\in\sigma_{k-1}\left(\gamma_{[2^{n-1}-1]}^{n-1,k-1}\right)$ that $\gamma_{[0]}^{n,k}=0\gamma_{[0]}^{n-1,k-1}\in\sigma_k\left(1\gamma_{[2^{n-1}-1]}^{n-1,k-1}\right)\subseteq\sigma_k\left(\gamma_{[2^{n-1}-1]}^{n,k}\right)$, hence $\gamma^{n,k}$ satisfies Cond. (G2). Similarly, $\underline{\gamma}_{[0]}^{n-1,k-1}\in\sigma_{k-1}\left(\underline{\gamma}_{[2^{n-1}-1]}^{n-1,k-1}\right)$ implies $\underline{\gamma}_{[0]}^{n,k}\in\sigma_k\left(\underline{\gamma}_{[2^{n-1}-1]}^{n,k}\right)$, hence $\underline{\gamma}^{n,k}$ satisfies Cond. (G2). □

We have now examined each of the different possibilities. The following statement summarizes the results.

Theorem 7.3. *Given a finite alphabet A, $k\geq 1$, and $n\geq k$, there is a loopless algorithm that allows to compute some specific maximum length σ_k-Gray cycle. In addition exactly one the following conditions holds:*

$$\lambda_{A,\sigma_k}(n)=\begin{cases}|A^n| & |A|\geq 3, n\geq k\\ 2 & |A|=2, n=k\\ |A|^n & |A|=2, n\geq k+1, k \text{ is odd}\\ |A|^{n-1} & |A|=2, n\geq k+1, k \text{ is even.}\end{cases}$$

Proof. Notice that, in the case where we have $|A|=2$, with n being an even integer, according to Eqs. (39), and Proposition 5.6, Algorithm 2 can be easily extended in a method computing $\gamma_{[i]}^{n,k}$ by starting with $\gamma_{[i-1]}^{n,k}$. As a consequence, according to the studies in Sects. 4, 6, in any case there is an iterated-basis algorithms generating some specific maximum length σ_k-Gray cycle. As indicated above, according to the implementation of $h^{n_0,1}$, $\gamma^{n_0,1}$, and $\rho^{n_0,1}$, that algorithm can run in constant amortized-time or in constant time.

In what follows, we examine the length of the corresponding σ_k-Gray cycles. Recall that if some σ_k-Gray cycle exists over $X\subseteq A^{\leq n}$, necessarily X is a uniform set that is, the inclusion $X\subseteq A^m$ holds for some $m\leq n$, whence in any case we have $\lambda_{A,\sigma_k}(n)\leq|A|^n$.

– According to Proposition 7.3, if we have $|A|\geq 3$ and $n\geq k$, a σ_k-Gray cycle exists over A^n, whence we have $\lambda_{A,\sigma_k}(n)=[A|^n$.

– Similarly, according to Proposition 5.6, the cond. $|A| = 2$, $n \geq k+1$, k is odd implies that a σ_k-Gray cycle exists over A^n, hence we have $\lambda_{A,\sigma_k}(n) = [A|^n$.

– As indicated in the preamble of Sect. 5, the cond. $|A| = 2$ with $n = k$ trivially implies $\lambda_{A,\sigma_k}(n) = 2$.

– Finally, according to Lemma 7.1, given a binary alphabet A, if k is even we have $\lambda_{A,\sigma_k}(n) \leq 2^{n-1}$ therefore, according to Proposition 7.2 the cond. $|A| = 2, n \geq k+1$, k is even implies that a σ_k-Gray cycle exists in A^{n-1} that is we have $\lambda_{A,\sigma_k}(n) = |A|^{n-1}$. □

Algorithms (c) and (d) allow to construct maximum length Gray sequences st. the Hamming distance of two consecutive terms is exactly k. We close the study by examining the case where Gray cycles are defined with a weaker constraint.

k-Gray codes

These sequences are commonly defined as Gray sequences where two consecutive terms have distance at most k. In the context of our study, k-Gray cycles are actually Σ_k-Gray cycles, where we set $(w, w') \in \Sigma_k$ iff. the Hamming distance of w and w' is not greater than k.

Note that we have $\Sigma_k = id_{A^*} \cup \sigma_1 \cup \cdots \cup \sigma_k$, thus $\sigma_1 \subseteq \Sigma_k$. As a consequence, the two notions of σ_1-Gray cycle and k-Gray cycle are identical. In particular, we have $|A^n| = \lambda_{A,\Sigma_k}(n) = \lambda_{A,\sigma_1}(n)$. Furthermore, according to Theorem 7.3, each of Algorithms (c), (d) generates a k-Gray cycle of length $|A|^n$ iff. exactly one of the two following conds. holds:

$|A| \geq 3$, $n \geq k$

$|A| = 2$, $n \geq k+1$, k is odd.

In the case where we have $|A| = 2$, $n \geq k+1$, k is even or $A = 2$, $n = k$, once more according to Theorem 7.3, our algorithms cannot compute any k-Gray cycle.

Further development

The present investigations could be done in the framework of other word binary relations τ, such as other edit relations, as defined in [28], or relations connected to the so-called prefix or factor distances [6, 29]. One could also characterize maximum length Gray cycles over X, with X describing some noticeable families of sets such as variable-length codes.

References

[1] E. Barcucci, A. Del Lungo, E. Pergola, and R. Pinzani. ECO: a methodology for the enumeration of combinatorial objects. *J. of Dif. Equ. and Appl.*, 5:435–490, 1999.

[2] J.-L. Baril and V. Vajnovszki. Gray codes for derangements. *Discr. Appl. Math.*, 140:207–221, 2004.

[3] J.L Baril, S. Kirgizov, and V. Vajnovszki. Gray codes for fibonacci q-decreasing words. *Theoret. Comput. Sci.*, 927:120–132, 2022.

[4] A. Bernini, S. Bilotta, R. Pinzani, A. Sabri, and V. Vajnovszki. Prefix partitioned gray codes for particular cross-bifix-free sets. *Cryptography and Communications*, 6:359–369, 2014.

[5] P. Burcsi, G. Fici, Z. Lipták, R. Raman, and J. Sawada. Generating a gray code for prefix normal words in amortized polylogarithmic time per word. *Theoret. Comp. Sci.*, 842:86–99, 2020.

[6] C. Choffrut and G. Pighizzini. Distances between languages and reflexivity of relations. *Theoret. Comp. Sci.*, 286:117–138, 2002.

[7] Fan Chung, P. Diaconis, and R. Graham. Universal cycles for combinatorial structures. *Discrete Math.*, 110:43–59, 1992.

[8] M. Cohn. Affine m-ary gray codes. *Inf. Control*, 6, 1963.

[9] P. Eades and B. McKay. An algorithm for generating subsets of fixed size with a strong minimal change property. *Inf. Proc. Letter*, 19:131–133, 1984.

[10] G. Ehrlich. Loopless algorithms for generating permutations, combinations, and other combinatorial configurations. *J. ACM*, 20:500–513, 1973.

[11] M. C. Er. On generating the n-ary reflected gray codes. *IEEE Transactions on Computers*, C-33:739–741, 1984.

[12] H. Fredricksen and J. Maiorana. Necklaces of beads in k colors and k-ary de Bruijn sequences. *Discrete Math.*, 23:207–210, 1978.

[13] E.N. Gilbert. Gray codes and paths on the n-cube. *Bell Sys. Tech. J.*, 37:815–826, 1958.

[14] R. J. Gould. Updating the hamiltonian problem – a survey. *J. Graph Theory*, 15:121–157, 1991.

[15] J.T. Joichi and Dennis E. White. Gray codes in graphs of subsets. *Discrete Math.*, 31:29–41, 1980.

[16] J.T. Joichi, Dennis E. White, and S. G. Williamson. Combinatorial Gray codes. *SIAM J. Comput.*, 9:130–141, 1980.

[17] H. Jürgensen and S. Konstantinidis. Codes. In *Handbook of Formal Languages*, volume 1, chapter 8, pages 511–607. Springer Verlag, Berlin, Heidelberg, 1997.

[18] H. Jürgensen, K. Salomaa, and S. Yu. Transducers and independence in free monoids. *Theor. Comput. Sci.*, 134:107–117, 1994.

[19] R. Kaye. A gray code for set partitions. *Inform. Process. Lett.*, 5:171–173, 1976.

[20] D.E. Knuth. *The Art of Computer programming, Vol.4, Fascicle 2: Generating All Tuples and Permutations*. Addison Wesley, 2005. ISBN-13: 978-0-201-85393-3.

[21] K. Kutnar and D. Marušič. Hamilton cycles and paths in vertex-transitive graphs—current directions. *Discrete Math.*, 309:5491–5500, 2009.

[22] G. H. J. Lanel, H. K. Pallage, J. K. Ratnayake, S. Thevasha, and B. A. K. Welihinda. A survey on hamiltonicity in Cayley graphs and digraphs on different groups. *Discrete Math. Algorithms Appl.*, 11:1930002, 2019.

[23] D H. Lehmer. The machine tools of combinatorics. In E. Beckenbach, editor, *Applied Combinatorial Mathematics*, pages 5–31. John Wiley and Sons, 1964.

[24] Z. Lipták, F. Masillo, G. Navarro, and A. Williams. Constant time and space updates for the sigma-tau problem. In Nardini Franco Maria, Pisanti Nadia, and Venturini Rossano, editors, *String Processing and Information Retrieval: 30th International Symposium, SPIRE 2023, Pisa, Italy, September 26–28, 2023, Proceedings*, volume 14240. Lect. Notes in Comp. Sci., 2023. Expected publication October 30, 2023 by Springer.

[25] J. Ludman. Gray code generation for MPSK signals. In *IEEE Transactions on Communication, COM-29*, volume 29, pages 1519–1522, 1981.

[26] T. Mütze. Combinatorial gray codes–an updated survey. arXiv:2202.01280, 2023.

[27] J. Néraud. Gray cycles of maximum length related to k-character substitutions. In H.-S Han and S.-K Ko, editors, *Deterministic Complexity of Formal Systems, 23 rd International Conference, DCFS 2021*, volume 13037, pages 137–149. Lect. Notes in Comp. Sci., 2021.

[28] J. Néraud. Variable-length codes independent or closed with respect to edit relations. *Inf. Comput.*, 288:104747, 2022.

[29] J. Néraud. When variable-length codes meet the field of error detection. In D. Poulakis, G. Rahonis, and P. Tzounakis, editors, *9th International Conference on Algebraic Informatics: CAI 2022, Proceedings*, volume 13706, pages 203–222. Lect. Notes in Comp. Sci., 2022.

[30] D. Richard. Data compression and gray-code sorting. *Inform. Process. Lett.*, 22:201–205, 1986.

[31] F. Ruskey, C. Savage, and T. Min Yih Wang. Generating necklaces. *J. Algorithms*, 13:414–430, 1992.

[32] F. Ruskey, J. Sawada, and A. Williams. Binary bubble languages and cool-lex order. *J. of Comb. Theory, Series A*, 119:155–169, 2012.

[33] C. Savage. A survey of combinatorial Gray codes. *SIAM Rev.*, 39:605–629, 1997.

[34] J. Sawada and Williams A. A hamilton path for the sigma-tau problem. In *Proceedings of the 2018 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2018.

[35] J. Sawada and A. Williams. A gray code for fixed-density necklaces and Lyndon words in constant amortized time. *Theoret. Comp. Sci.*, 502:46–54, 2013.

[36] V. Vajnovski and T. Walsh. A loop-free two-close Gray-code algorithm for listing k-ary Dyck words. *J. Discrete Algorithms*, 4:633–648, 2006.

[37] V. Vajnovszki. Gray visiting Motzkins. *Acta Inform.*, 38:793–811, 2002.

[38] V. Vajnovszki. A loopless algorithm for generating the permutations of a multiset. *Theoretic. Comput. Sci.*, 307:415–431, 2003.

[39] V. Vajnovszki. More restrictive gray codes for necklaces and Lyndon words. *Inform. Process. Letters*, 106:96–99, 2008.

[40] J. van den Heuvel. The complexity of change. In S. R. Blackburn, S. Gerke, and M. Wildon, editors, *Surveys in Combinatorics 2013*, volume 409 of London Mathematical Society Lecture Note Series, page 127–160. Cambridge University Press, 2013.

[41] A. Williams. Loopless generation of multiset permutations using a constant number of variables by prefix shifts. In C. Mathieu, editor, *Proc. of the 2009 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, page 987–996. Society for Industrial and Applied Mathematics, 3600 University City Science Center Philadelphia, PA, United States, 2009.

[42] Jun-Ming Xu and Meijie Ma. Survey on path and cycle embedding in some networks. *Front. Math. China*, 4:217–252, 2009.