

HAMILTON CYCLES FOR INVOLUTIONS OF CLASSICAL TYPES

GONÇALO GUTIERRES, RICARDO MAMEDE, AND JOSÉ LUIS SANTOS

ABSTRACT. Let \mathcal{W}_n denote any of the three families of classical Weyl groups: the symmetric groups \mathcal{S}_n , the hyperoctahedral groups (signed permutation groups) \mathcal{S}_n^B , or the even-signed permutation groups \mathcal{S}_n^D . In this paper we give an uniform construction of a Hamilton cycle for the restriction to involutions on these three families of groups with respect to a inverse-closed connecting set of involutions. This Hamilton cycle is optimal with respect to the Hamming distance only for the symmetric group \mathcal{S}_n .

We also recall an optimal algorithm for a Gray code for type B involutions. A modification of this algorithm would provide a Gray Code for type D involutions with Hamming distance two, which would be optimal. We give such a construction for \mathcal{S}_4^D and \mathcal{S}_5^D .

Keywords: Weyl group; Hamilton cycle; Cayley graph; Gray code.

1. INTRODUCTION

The efficient generation of all objects of a certain class of combinatorial objects is a central problem in enumerative combinatorics, with applications in a vast range of areas ranging from computer science and hardware or software testing, to biology and biochemistry [7, 8]. It can be used to test hypotheses or to exhibit combinatorial properties of a class of objects, to count the object in a class, and to analyze and prove programs.

A usual approach to this problem has been the generation of the objects of a class as a list in which successive elements differ by a well-defined closeness condition. An example of such approach is the Binary Reflected Gray Code, or simply Gray code, described and patented in 1953 by Frank Gray [5], a researcher at Bell Telephone Laboratories, which generates all 2^n n -bit strings so that successive strings differ in exactly one bit. Gray used this code to prevent spurious output from electromechanical switches, but this code has been widely used in many other areas, such as in circuit design, data compression and error correction in digital communications. The theory of Gray codes has evolved substantially since F. Gray original work, and the term is now used in a broader sense to describe a complete and non-repeating listing of the elements of some class of combinatorial objects such that successive objects in the listing differ by a well-defined closeness condition.

The concept of a Gray code can be easily translated into graph-theoretical terms. If \mathcal{W} is a class of combinatorial objects, let $G(\mathcal{W})$ be the graph with vertex set \mathcal{W} , where two vertices i and j are joined by an edge whenever i and j satisfy the closeness condition. The problem of finding a Gray code for \mathcal{W} is equivalent to find a Hamiltonian path in $G(\mathcal{W})$. If we demand that the Gray code be closed, that is the initial and final elements in the list must also satisfy the closeness condition, then the problem is equivalent to the problem of finding a Hamiltonian cycle in $G(\mathcal{W})$.

In this paper we will focus our attention on involutions over the three families of classical Weyl groups: the symmetric groups \mathcal{S}_n^A , the hyperoctahedral groups (signed permutation groups) \mathcal{S}_n^B , and the even-signed permutation groups \mathcal{S}_n^D . If \mathcal{W} is one of these groups, we consider the Cayley graph $G(\mathcal{W}, T)$, for an inverse-closed connecting set $T \subset \mathcal{W} \setminus \{1\}$

This work was partially supported by the Centre for Mathematics of the University of Coimbra (funded by the Portuguese Government through FCT/MCTES, DOI 10.54499/UIDB/00324/2020).

(see [6]). The vertices of this graph are the elements of \mathcal{W} , and the edges are given by all possible sets $\{w, w \cdot t\}$, where $w \in \mathcal{W}$ and $t \in T$. The inverse-closed condition of T means that the graph $G(\mathcal{W}, T)$ is undirected, since if $\{w, v\}$ is an edge in $G(\mathcal{W}, T)$, then $v = w \cdot t$, and also $w = v \cdot t^{-1}$, so that $\{v, w\}$ is also an edge of $G(\mathcal{W}, T)$. Moreover, the graph $G(\mathcal{W}, T)$ is connected if and only if T is a generating set for \mathcal{W} [2, 6].

We will show that the restriction to involutions of the graph $G(\mathcal{W}, T)$ has a Hamiltonian cycle. The choice of the set T is made in order to minimize the maximal distance between two consecutive elements of the cycle. We adopt as distance between two involutions their Hamming distance, that is, the number of positions in which the words of these two involutions differ. Using group terminology, the Hamming distance between the involutions w and v is the number of non-fixed points in the composition $w \cdot v$. The maximal distance between any two consecutive elements of an Hamilton cycle is the Hamming distance of that cycle. We will use the Gray codes for types A and B constructed in [4] and [3] to generate the Hamilton cycles for these types, and for type D to construct a Gray code with distance 2 up to $n = 5$. These Gray codes are proven to be optimal in relation to the Hamming distance between consecutive elements of the code.

The paper is organized as follows. In Section 2 we describe the classical Weyl groups and its usual combinatorial realizations as the symmetric group, the group of signed permutations, and the even-signed permutation group. Notations and some enumerative results on involutions are addressed for each type. In Section 3 we describe an uniform construction of a Gray code for the involutions in types A , B and D , based on iterative formulas for their cardinalities, which translates into Hamilton cycles in the restriction to involutions of the Cayley graph $G(\mathcal{S}_n^\psi, T^\psi)$, with T^ψ a specific set of reflections of type $\psi \in \{A, B, D\}$. This construction is optimal for type A , but not for the other types. Nevertheless, this approach has the advantage of being an uniform construction over the three types, with a simple implementation procedure. In Section 4 we describe a Gray code for type B with optimal Hamming distance, obtained in [3], and generalize this construction to a optimal Gray code for type D involutions. The translation of these codes into Hamilton cycles for the restriction to involutions of the Cayley graph $G(\mathcal{S}_n^B, T^B)$ and $G(\mathcal{S}_n^D, T^D)$ are also given.

2. INVOLUTIONS IN CLASSICAL WEYL GROUPS

Let \mathcal{W} be an (irreducible) finite Weyl group with presentation

$$\langle s_1, s_2, \dots, s_n \mid (s_i s_j)^{m_{ij}} = 1, m_{ii} = 1, \text{ and } m_{ij} = m_{ji} \rangle.$$

For a Weyl group, the integers m_{ij} take values in the set $\{1, 2, 3, 4, 6\}$, and are specified by the Dynkin diagrams represented in Figure 1. The vertices correspond to the generators s_i of \mathcal{W} with an edge between i and j when $m_{ij} \geq 3$, being that edge marked with m_{ij} when $m_{ij} \geq 4$.

In this paper we focus on the classical Weyl groups, which correspond to the three infinite families of types A_n , B_n and D_n . The symmetric group \mathcal{S}_n , the hyperoctahedral group \mathcal{S}_n^B , also known as the group of signed permutations, and the even-signed permutation group \mathcal{S}_n^D are Weyl groups of types A_n , B_n and D_n , respectively.

An involution in \mathcal{W} is an element $w \in \mathcal{W}$ such that $w^2 = 1$. The elements ws_iw^{-1} , with $w \in \mathcal{W}$, are called reflections. Each generator s_i is a reflection, and any reflection is an involution. We denote by I_n^A , I_n^B and I_n^D the set of all involutions of \mathcal{S}_n^A , \mathcal{S}_n^B and \mathcal{S}_n^D , respectively, and by i_n^A , i_n^B and i_n^D their cardinality.

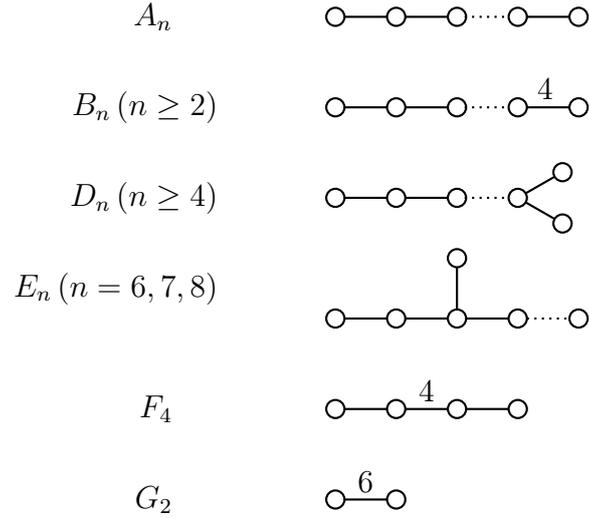


FIGURE 1. Dynkin diagrams for irreducible finite Weyl groups.

The symmetric group \mathcal{S}_n^A is a Weyl group of type A_{n-1} , generated by the transpositions of consecutive integers $s_i^A = (i \ i+1)$, $i \in [n-1] := \{1, \dots, n-1\}$, which satisfy

$$(s_i^A s_j^A)^2 = 1 \text{ if } |i-j| > 1, \quad \text{and} \quad (s_i^A s_{i+1}^A)^3 = 1.$$

The composition of permutations is performed from left to right. We use both the decomposition in disjoint cycles and the one-line notation $\pi_1 \pi_2 \cdots \pi_n$ to represent a permutation $\pi \in \mathcal{S}_n$, where we set $\pi_i = \pi(i)$ for all i . It will be clear from the context which notation is being used. Multiplying an element $\pi \in \mathcal{S}_n$ on the right by s_i has the effect of exchanging the values in positions i and $i+1$ in the one-line notation. The number i_n^A of involutions of \mathcal{S}_n satisfies the relation

$$(2.1) \quad i_n^A = i_{n-1}^A + (n-1)i_{n-2}^A,$$

with $i_0^A = i_1^A = 1$ (see [1]).

Denote by $[\pm n]$ the set $\{\pm 1, \pm 2, \dots, \pm n\}$ and by \bar{i} the integer $-i$. The hyperoctahedral group \mathcal{S}_n^B is the group of all permutations π of the set $[\pm n]$ such that

$$(2.2) \quad \pi(\bar{i}) = \overline{\pi(i)},$$

for all $i \in [\pm n]$, with composition as group operation, performed from left to right. Equation (2.2) indicates that an element of \mathcal{S}_n^B is entirely defined by its values on $[n]$. For that reason, we will write the elements $\pi \in \mathcal{S}_n^B$ in one-line notation as $\pi = \pi_1 \pi_2 \cdots \pi_n$, and call them sign permutations of $[n]$. For example, $\pi = \bar{3} 2 \bar{1} 6 5 4 \bar{7}$ is an element of \mathcal{S}_7^B . Every permutation $\pi \in \mathcal{S}_n^B$ can be written as a product of disjoint cycles, called the cycle decomposition of π , obtained by first writing $|\pi| = |\pi_1| \cdots |\pi_n| \in \mathcal{S}_n^A$ as a disjoint union of cycles, and then placing bars on the letters which have bars in π . In this setting, if $i, j > 0$, the cycle $(i \ j)$ is the permutation that transposes i with j , and \bar{i} with \bar{j} , the cycle $(\bar{i} \ \bar{j})$ is the permutation that transposes i with \bar{j} and \bar{i} with j , and (\bar{j}) is the permutation that transposes j with \bar{j} . For instance, for $\pi = \bar{3} 2 \bar{1} 6 5 4 \bar{7}$ we have $|\pi| = (13)(2)(46)(5)(7)$ and thus the cycle decomposition of π is $(\bar{1} \ \bar{3})(2)(46)(5)(\bar{7})$. Note that the cycle decomposition of a sign involution is a composition of transpositions and cycles of length one. Moreover, using the above notation, the sign of each letter in a transposition $(i \ j)$ with $|i| \neq |j|$ must be the same.

The group \mathcal{S}_n^B is generated by the involutions

$$s_i^B = (i\ i+1), \text{ for } i \in [n-1], \quad \text{and} \quad s_n^B = (\bar{n}),$$

which satisfy

$$(s_i^B s_{i+1}^B)^3 = 1 \text{ for } i \in [n-2], \quad (s_i^B s_j^B)^2 = 1 \text{ if } |i-j| > 1 \quad \text{and} \quad (s_{n-1}^B s_n^B)^4 = 1.$$

Multiplying an element $\pi \in \mathcal{S}_n^B$ on the right by s_i^B , $i \in [n-1]$, has the effect of exchanging the values in positions i and $i+1$ in the one-line notation. When the generator is s_n^B the multiplication changes the sign of the value in position n . For instance, the permutation $s_5^B s_6^B s_7^B s_6^B s_5^B$ changes the sign of the letter in position 5 when applied to an element of \mathcal{S}_7^B :

$$(\bar{3}2\bar{1}654\bar{7}) \cdot s_5^B s_6^B s_7^B s_6^B s_5^B = \bar{3}2\bar{1}6\bar{5}4\bar{7}.$$

The number i_n^B of involutions of \mathcal{S}_n^B satisfies the relation

$$(2.3) \quad i_{n+1}^B = 2i_n^B + 2ni_{n-1}^B,$$

with $i_0^B = 1$ and $i_1^B = 2$ (see [1]).

The even-signed permutation group \mathcal{S}_n^D is the subgroup of \mathcal{S}_n^B consisting of all of the signed permutations having an even number of negative entries in their one-line notation. As a set of generators, we take

$$s_i^D = s_i^B = (i\ i+1), \text{ for } i \in [n-1], \quad \text{and} \quad s_n^D = s_n^B s_{n-1}^B s_n^B = (\overline{n-1}\ \bar{n}),$$

which satisfy

$$(s_i^D s_{i+1}^D)^3 = (s_{n-2}^D s_n^D)^3 = 1 \text{ for } i \in [n-2], \quad (s_i^D s_j^D)^2 = (s_{n-1}^D s_n^D)^2 = 1 \text{ if } |i-j| > 1.$$

Multiplying an element $\pi \in \mathcal{S}_n^D$ on the right by s_n^D has the effect of exchanging the values and the signs in positions $n-1$ and n in the one-line notation. For example,

$$(\bar{3}2\bar{1}6\bar{5}4\bar{7}) \cdot s_7^D = \bar{3}2\bar{1}6\bar{5}7\bar{4}.$$

The number of i_n^D of involutions of \mathcal{S}_n^D can be given by the following recursive formula that uses the number of involutions of type B . This formula will allow us to give an uniform construction for the Hamilton cycles in the three types.

Proposition 2.1. *For $n \geq 2$, we have*

$$(2.4) \quad i_{n+1}^D = i_n^B + 2n \cdot i_{n-1}^D.$$

Proof. Let $\pi = \pi_1 \cdots \pi_{n+1} \in \mathcal{S}_{n+1}^D$ be an involution. Then, either $\pi_{n+1} = \pm(n+1)$ or $\pi_{n+1} = \pm j$, for some $j \in [n]$. In the first case, $\pi_1 \cdots \pi_n$ is an involution in \mathcal{S}_n^B with π_{n+1} positive if $\pi_1 \cdots \pi_n \in \mathcal{S}_n^D$, and negative otherwise. In the second case, $\pi = (j\ n+1) \cdot \sigma$ or $\pi = (\bar{j}\ \overline{n+1}) \cdot \sigma$, where $\sigma \in \mathcal{S}_n^D$ with $\sigma_j = j$. The formula now follows from the bijective correspondence between these involutions σ and the involutions of \mathcal{S}_{n-1}^D . \square

3. RECURSIVE HAMILTON CYCLES

Let $\psi \in \{A, B, D\}$. In this section we give an uniform construction of an Hamilton cycle for the restriction to involutions of the Cayley graph $G(\mathcal{S}_n^\psi, T^\psi)$, for a specific generating set T^ψ of reflections. The Hamilton cycles are achieved by a recursive construction of a Gray code $\text{GC}\psi(n)$ for I_n^ψ , which satisfy the following two **properties**:

A1: The first and last involution of $\text{GC}\psi(n)$ are, respectively, the identity and the transposition $(n-1\ n)$ or $(\overline{n-1}\ \bar{n})$ (if $\psi \neq A$).

A2: Any involution in $\text{GC}\psi(n)$ is obtained from its predecessor by a transposition or a rotation of three letters with at most two sign changes (when $\psi \neq A$), or one or two sign changes (when $\psi = A$).

To achieve this goal we have to introduce some notation.

Consider an ordered list $L = (w_1, w_2, \dots, w_m)$ of involutions over some alphabet N over the integers, which is closed to negation in types B and D . Given letters i, j, k not in N , let

$$L \cdot k := (w_1 \cdot k, w_2 \cdot k, \dots, w_m \cdot k)$$

be the ordered list where each involution $w_\ell \cdot k$ is the extension of w_ℓ to the alphabet $N \cup \{k\}$ in type A , or $N \cup \{\pm k\}$ otherwise, leaving the letter k fixed. Similarly, define

$$L \cdot (ij) := (w_1 \cdot (ij), w_2 \cdot (ij), \dots, w_m \cdot (ij)),$$

where each involution $w_\ell \cdot (ij)$ is the composition of the involution w_ℓ with the transposition (ij) , now considered over the alphabet $N \cup \{i, j\}$ in type A , or $N \cup \{\pm i, \pm j\}$ otherwise. Running over the elements of L from right to left we get the list

$$\overleftarrow{L} = (w_m, \dots, w_2, w_1).$$

Example 3.1. If $L = (12, 21)$, then $L \cdot 3 = (123, 213)$ and $L \cdot (34) = (1243, 2143)$.

Let $N = \{a_1, a_2, \dots, a_n\}$ be an alphabet with n letters, and consider an involution $\pi \in I_n^A$. Replacing each letter i of π by a_i produces an involution π' in N . Formally, this amounts to defining the bijection $F : [n] \rightarrow N$, where $F(i) = a_i$, which satisfies the composition

$$\pi' = F^{-1} \cdot \pi \cdot F,$$

evaluated from left to right. Thus, if $\pi = (x_1 y_1) \cdots (x_k y_k)$, then $\pi' = (a_{x_1} a_{y_1}) \cdots (a_{x_k} a_{y_k})$. To simplify notation, we will write the bijection F in one-line notation $F = a_1 a_2 \cdots a_n$.

Example 3.2. Consider the involution $\pi = 321 \in I_3^A$, the alphabet $N = \{1, 2, 4\}$ and the bijection $F : [3] \rightarrow N$ defined by $F = 412$. Then,

$$F^{-1} \cdot \pi \cdot F = 142$$

is an involution over the alphabet N .

This construction extends naturally to case of sign permutations. For instance, if $\pi = 3\bar{2}1 \in I_3^B$, and \tilde{F} is the extension to type B of the permutation used in Example 3.2, then

$$\tilde{F}^{-1} \cdot \pi \cdot \tilde{F} = \bar{1}42$$

is a sign involution over the alphabet N .

Given a list $L = (w_1, w_2, \dots, w_m)$ of involutions in I_n^ψ , and alphabet N with n letters and a bijection $F : [n] \rightarrow N$, we denote by L^F the list

$$L^F = (F^{-1} \cdot w_1 \cdot F, F^{-1} \cdot w_2 \cdot F, \dots, F^{-1} \cdot w_m \cdot F)$$

of involutions over the alphabet N . The following result follows from the definitions.

Lemma 3.1. *Let N be an alphabet with n letters and $F = a_1 a_2 \cdots a_n$ a bijection between the sets $[n]$ and N . If L is a list of involutions in I_n^ψ , $\psi \in \{A, B, D\}$, satisfying properties **A1** and **A2**, then the sequence L^F is a list of involutions over the alphabet N that also satisfies properties **A1** and **A2**, with a_{n-1} and a_n replaced by $n-1$ and n .*

3.1. Hamilton cycle of type A. Consider the Cayley graph $G(\mathcal{S}_n^A, T^A)$, where T^A is formed by reflections and product of two reflections $T^A = X_1^A \cup X_2^A$, where

$$X_1^A = \{t_{i,j} : i \leq j\}$$

$$X_2^A = \{t_{i,j-1} \cdot t_{j,k-1}, t_{j,k-1} \cdot t_{i,j-1} : i < j < k\},$$

with $t_{i,j} = s_i^A s_{i+1}^A \cdots s_{j-1}^A s_j^A s_{j-1}^A \cdots s_{i+1}^A s_i^A$ if $i < j$, and $t_{i,i} = s_i^A$. Note that a transposition of the letters in positions $i < j$ in a permutation π is obtained by the multiplication on the right of π by the reflection $t_{i,j-1}$, while the rotation of three letters $i < j < k$ of π is obtained by multiplication on the right of π by $t_{i,j-1} \cdot t_{j,k-1}$ in the case of the rotations $ijk \rightarrow jik \rightarrow jki$, or by $t_{j,k-1} \cdot t_{i,j-1}$ in the case of the rotations $ijk \rightarrow ikj \rightarrow kij$.

We can now describe the construction of the Gray code $\text{GCA}(n)$ for the type A involutions of order $n \geq 5$. This construction is achieved by the implementation of the Algorithms 1 and 2 below, one for each parity of n , whose recursive calls are triggered by the Gray codes $\text{GCA}(3)$ and $\text{GCA}(4)$, which satisfy properties **A1** and **A2**:

$$\text{GCA}(3) = (\text{id}, (12), (13), (23))$$

$$(3.1) \quad \text{GCA}(4) = (\text{id}, (13), (13)(24), (24), (14), (14)(23), (23), (12), (12)(34), (34)).$$

Algorithm 1 Gray code for the involutions in \mathcal{S}_n^A , n odd ($n \geq 5$)

- 1: **procedure** $\text{GCA}(n)$
 - 2: Set $F = 23 \cdots (n-1)1$ and write $\text{GCA}^F(n-1) \cdot n$;
 - 3: **for** $i = 1$ to $\frac{n-1}{2}$ **do**
 - 4: Set $F = (2i)12 \cdots (2i-2)(2i+1) \cdots (n-1)$ and write $\text{GCA}^F(n-2) \cdot (2i-1)n$;
 - 5: Set $F = (2i-1)12 \cdots (2i-2)(2i+1) \cdots (n-1)$ and write $\overleftarrow{\text{GCA}}^F(n-2) \cdot (2i)n$;
-

Algorithm 2 Gray code for involutions in \mathcal{S}_n^A , n even ($n \geq 6$)

- 1: **procedure** $\text{GCA}(n)$
 - 2: Write $\text{GCA}(n-1) \cdot n$;
 - 3: Set $F = 23 \cdots (n-1)$ and write $\overleftarrow{\text{GCA}}^F(n-1) \cdot (1n)$;
 - 4: **for** $i = 1$ to $\frac{n}{2} - 1$ **do**
 - 5: Set $F = (2i+1)12 \cdots (2i-1)(2i+2) \cdots (n-1)$ and write $\text{GCA}^F(n-2) \cdot (2i)n$;
 - 6: Set $F = (2i)12 \cdots (2i-1)(2i+2) \cdots (n-1)$ and write $\overleftarrow{\text{GCA}}^F(n-2) \cdot (2i+1)n$;
-

Table 3.1 shows the code $\text{GCA}(5)$ generated by Algorithm 1. The table should be read top to bottom along columns, starting in the leftmost column. Each column contains the involutions generated in the various steps of the algorithm.

Theorem 3.2. *The application of Algorithm 1 or 2 triggered by Gray codes $\text{GCA}(n-2)$ and $\text{GCA}(n-1)$ satisfying properties **A1** and **A2**, produces a cyclic Gray code for the type A involutions of order $n \geq 5$, which satisfies properties **A1** and **A2**.*

Proof. We consider the n odd case, since the even case is analogous. If $\text{GCA}(n-2)$ and $\text{GCA}(n-1)$ are Gray codes for I_{n-2}^A and I_{n-1}^A satisfying properties **A1** and **A2** then, by Lemma 3.1, each involution in any of the sequences generated in Steps 2, 3 and 4 of Algorithm 1 is obtained from its predecessor by a transposition or a rotation of three

12345	52341	15432	12543	21354
14325	53241	45312	42513	13254
34125	54321	35142	14523	32154
32145	52431	15342	21543	12354
21345				
21435				
12435				
13245				
43215				
42315				

TABLE 3.1. The Gray code $\text{GCA}(5)$.

letters. Note that the leftmost and rightmost involution in each one of these sequences are, respectively:

- the identity and the transposition $(n-2\ n-1)$ in the sequence $\text{GCA}(n-1)^F \cdot n$ obtained in Step 2;
- $(2i-1\ n)$ and $(2i-1\ n)(n-2\ n-1)$ in the sequence $\text{GCA}(n-2)^F \cdot (2i-1\ n)$ for $i = 1, \dots, (n-1)/2 - 1$;
- $(2in)(n-2\ n-1)$ and $(2in)$ in the sequence $\overleftarrow{\text{GCA}}(n-2)^F \cdot (2i-1\ n)$ for $i = 1, \dots, (n-1)/2 - 1$;
- $(n-2\ n)$ and $(n-2\ n)(n-4\ n-3)$ in the sequence $\text{GCA}(n-2)^F \cdot (2i-1\ n)$ for $i = (n-1)/2$;
- $(n-1\ n)(n-4\ n-3)$ and $(n-1\ n)$ in the sequence $\overleftarrow{\text{GCA}}(n-2)^F \cdot (2i-1\ n)$ for $i = (n-1)/2$.

It follows that $\text{GCA}(n)$ is a cyclic Gray code for I_n^A satisfying properties **A1** and **A2**.

Finally, notice that by its construction, all involutions generated by the algorithm are pairwise distinct. Moreover, the number of involutions in all these sequences is equal to $t_{n-1}^A + (n-1)t_{n-2}^A$, which gives the total amount of involutions in I_n^A by equation (2.1). \square

The Gray code $\text{GCA}(n)$ translates into an Hamilton cycle in the restriction to involutions of the Cayley graph $G(\mathcal{S}_n^A, T^A)$.

Corollary 3.3. *The Gray code $\text{GCA}(n)$ produced by Algorithm 1 or 2 is an Hamilton cycle in the restriction to involutions of the Cayley graph $G(\mathcal{S}_n^A, T^A)$, with Hamming distance three, for $n \geq 3$. This is the minimal Hamming distance of any Gray code for I_n^A with $n \geq 3$.*

Proof. Since $\text{GCA}(n)$ satisfies properties **A1** and **A2**, each involution in the list is obtained from its predecessor by a transposition or a rotation of three letters. Since a transposition of two letters in an involution π is obtained by the multiplication on the right of π by the reflection $t_{i,j}$, and the rotation of three letters is obtained by multiplication on the right of π by the product of two reflections $t_{i,j-1} \cdot t_{j,k-1}$ or $t_{j,k-1} \cdot t_{i,j-1}$, it follows that any two consecutive involutions in the code $\text{GCA}(n)$ are connected by an edge in the Cayley graph $G(\mathcal{S}_n^A, T^A)$. The same is true for the initial and final elements of the code. Thus, $\text{GCA}(n)$ is an Hamilton cycle in the restriction to involutions of the Cayley graph $G(\mathcal{S}_n^A, T^A)$.

It follows that the Hamming distance of this code is three. We will prove that three is the minimal distance in a code for I_n^A . The distance between two involutions is at least two, and this number is achieved when the involutions differ by exactly one transposition. Thus, a code for I_n^A with distance two must be a sequence of involutions that differ by

exactly one transposition, that is an alternating sequence of even and odd involutions. But since the excess of even to odd involutions is greater than 1 for $n > 2$ (see [9]), there cannot be such sequence. Therefore, we conclude that three is the minimal distance for a code for I_n^A . \square

3.2. Hamilton cycle of type B. The Cayley graph $G(\mathcal{S}_n^B, T^B)$ for the involutions of type B are generated by the set of reflections and product of two reflections $T^B = X_1^B \cup X_2^B \cup X_3^B \cup X_4^B$, where

$$\begin{aligned} X_1^B &= \{t_{i,j} : i \leq j\} \\ X_2^B &= \{t_{i,n} \cdot t_{j,n} : i < j < n\} \\ X_3^B &= \{t_{i,j} \cdot t_{j+1,n} : i < j < n\} \\ X_4^B &= \{t_{j,k-1} \cdot t_{i,j-1} : i < j < k\}, \end{aligned}$$

with $t_{i,j} = s_i^B s_{i+1}^B \cdots s_{j-1}^B s_j^B s_{j-1}^B \cdots s_{i+1}^B s_i^B$ if $i \leq j$, and $t_{i,i} = s_i^B$. The construction of the Gray code $\text{GCB}(n)$ for the involutions of order $n \geq 4$ in \mathcal{S}_n^B is obtained implementing Algorithm 3, whose recursive calls are triggered by the Gray codes

$$\text{GCB}(2) = (id, (\bar{1}), (\bar{1})(\bar{2}), (\bar{2}), (\bar{1}\bar{2}), (12))$$

and

$$\begin{aligned} \text{GCB}(3) = & (id, (\bar{1}), (\bar{1})(\bar{2}), (\bar{2}), (\bar{1}\bar{2}), (12), (12)(\bar{3}), (\bar{1}\bar{2})(\bar{3}), (\bar{2})(\bar{3}), (\bar{1})(\bar{2})(\bar{3}), (\bar{1})(\bar{3}), (\bar{3}), \\ & (\bar{1}\bar{3}), (\bar{1}\bar{3})(\bar{2}), (13)(\bar{2}), (13), (23), (\bar{1})(23), (\bar{1})(\bar{2}\bar{3}), (\bar{2}\bar{3})) \end{aligned}$$

which satisfy properties **A1** and **A2**.

Algorithm 3 Gray code for the involutions in \mathcal{S}_n^B ($n \geq 4$)

```

1: procedure GCB( $n$ )
2:   Write  $\text{GCB}(n-1) \cdot n$ ;
3:   Write  $\overleftarrow{\text{GCB}(n-1)} \cdot \bar{n}$ ;
4:   for  $i = 1$  to  $n-1$  do
5:     Set  $F = 12 \cdots (i-1)(i+1) \cdots (n-1)$ ;
6:     if  $i$  is odd then
7:       Write  $\text{GCB}^F(n-2) \cdot (\bar{i}\bar{n}), \overleftarrow{\text{GCB}^F(n-2)} \cdot (in)$ ;
8:     else
9:       Write  $\text{GCB}^F(n-2) \cdot (in), \overleftarrow{\text{GCB}^F(n-2)} \cdot (\bar{i}\bar{n})$ ;

```

Table 3.2 shows the Gray code $\text{GCB}(4)$ obtained by Algorithm 3, which should be read down columns, from left to right. Each column contains the involutions generated in a different step of the algorithm.

Theorem 3.4. *The application of Algorithm 3 with input the Gray codes $\text{GCB}(n-2)$ and $\text{GCB}(n-1)$, which satisfy properties **A1** and **A2**, produces a cyclic Gray code for the type B involutions of order $n \geq 4$, which satisfies properties **A1** and **A2**.*

Proof. As in the proof of Theorem 3.2 for the type A case, now using the recursive formula (2.3) for the number of type B involutions, we can show that $\text{GCB}(n)$ is a list of all involutions in \mathcal{S}_n^B . Assume that $\text{GCB}(n-2)$ and $\text{GCB}(n-1)$ satisfies properties **A1** and **A2**. Moreover, assume that whenever two consecutive elements of one of these codes differ by a rotation of three letters, there is no sign change, and whenever there is a transposition of two letters, at most one of these letters changes its sign. Notice that this is certainly

1234	1 $\bar{3}$ 2 $\bar{4}$	$\bar{4}$ 23 $\bar{1}$	1432	12 $\bar{4}$ 3
$\bar{1}$ 234	$\bar{1}$ 3 $\bar{2}$ 4	$\bar{4}$ 23 $\bar{1}$	$\bar{1}$ 432	$\bar{1}$ 2 $\bar{4}$ 3
$\bar{1}$ 2 $\bar{3}$ 4	$\bar{1}$ 32 $\bar{4}$	$\bar{4}$ 2 $\bar{3}$ 1	$\bar{1}$ 4 $\bar{3}$ 2	$\bar{1}$ 2 $\bar{4}$ 3
1 $\bar{2}$ 34	132 $\bar{4}$	$\bar{4}$ 2 $\bar{3}$ 1	14 $\bar{3}$ 2	12 $\bar{4}$ 3
2 $\bar{1}$ 34	321 $\bar{4}$	$\bar{4}$ 3 $\bar{2}$ 1	34 $\bar{1}$ 2	2 $\bar{1}$ 43
2134	3 $\bar{2}$ 1 $\bar{4}$	$\bar{4}$ 32 $\bar{1}$	3412	21 $\bar{4}$ 3
21 $\bar{3}$ 4	$\bar{3}$ 2 $\bar{1}$ 4	4321	3 $\bar{4}$ 1 $\bar{2}$	2143
2 $\bar{1}$ 3 $\bar{4}$	$\bar{3}$ 2 $\bar{1}$ 4	4 $\bar{3}$ 21	3 $\bar{4}$ 1 $\bar{2}$	2 $\bar{1}$ 43
12 $\bar{3}$ 4	123 $\bar{4}$	42 $\bar{3}$ 1	14 $\bar{3}$ 2	1243
$\bar{1}$ 2 $\bar{3}$ 4	$\bar{1}$ 23 $\bar{4}$	42 $\bar{3}$ 1	$\bar{1}$ 4 $\bar{3}$ 2	$\bar{1}$ 243
$\bar{1}$ 23 $\bar{4}$	$\bar{1}$ 2 $\bar{3}$ 4	4 $\bar{2}$ 31	$\bar{1}$ 43 $\bar{2}$	$\bar{1}$ 243
12 $\bar{3}$ 4	12 $\bar{3}$ 4	4231	14 $\bar{3}$ 2	1243
3 $\bar{2}$ 14	2 $\bar{1}$ 3 $\bar{4}$			
3 $\bar{2}$ 14	213 $\bar{4}$			
3 $\bar{2}$ 14	2134			
3214	2 $\bar{1}$ 3 $\bar{4}$			
1324	1 $\bar{2}$ 3 $\bar{4}$			
$\bar{1}$ 324	$\bar{1}$ 234			
$\bar{1}$ 3 $\bar{2}$ 4	$\bar{1}$ 234			
1 $\bar{3}$ 24	1234			

TABLE 3.2. The Gray code GCB(4).

true for the trigger cases GCB(2) and GCB(3). We will show that the same is true for the sequence GCB(n) generated by Algorithm 3. A rotation of three letters between two consecutive involutions in GCB(n) only occurs between two iterations of the cycle **for** in Step 4 of the algorithm, with no sign changes. Similarly, when a transposition occur between two consecutive involutions, there is at most one sign change. This situation only occurs between the involutions (\bar{n}) and ($\bar{1}\bar{n}$), generated in Step 3 and in the first iteration of the cycle **for** in Step 4, respectively, with the letter 1 changing its sign. By Lemma 3.1 we conclude that GCB(n) satisfy properties **A1** and **A2**, and whenever two consecutive letters of one of these codes differ by a rotation of three letters, there is no sign change, and whenever there is a transposition of two letters, at most one of these letters changes its sign. \square

As in the type *A* case, the Gray code GCB(n) translates into an Hamilton cycle in the restriction to involutions of the Cayley graph $G(\mathcal{S}_n^B, T^B)$ with Hamming distance three, for $n \geq 3$. However, in this case, this distance is not the minimal possible distance for such a Gray code, as it will be discussed in Section 4.

Corollary 3.5. *The Gray code GCB(n) produced by Algorithm 3 is an Hamilton cycle in the restriction to involutions of the Cayley graph $G(\mathcal{S}_n^B, T^B)$, with Hamming distance three, for $n \geq 4$.*

Proof. Since GCB(n) satisfies properties **A1** and **A2**, each involution in the list is obtained from its predecessor by a transposition or a rotation of three letters and at most two sign changes. Moreover, by the proof of Theorem 3.4 a rotation of three letters only occur with no sign changes. Additionally, when a transposition between letters occurs, there is at most one sign change on the smallest of the two letters. Since a sign change in position i of a involution π is obtained by the multiplication on the right of π by $t_{i,n}$, a transposition

of two letters in positions $i < j + 1$ in π followed by a sign change of the letter in position $j + 1$ is obtained by the multiplication on the right of π by $t_{i,j} \cdot t_{j+1,n}$, and the rotation of three letters in positions $i < i + 1 < j$ is obtained by multiplication on the right of π by the product of two reflections $t_{i+1,j-1} \cdot t_{i,i}$, it follows that any two consecutive involutions in the code $\text{GCB}(n)$ have Hamming distance at most 3 and are connected by an edge in the Cayley graph $G(\mathcal{S}_n^B, T^B)$. The same is true for the initial and final elements of the code. Thus, $\text{GCB}(n)$ is an Hamilton cycle in the restriction to involutions of the Cayley graph $G(\mathcal{S}_n^B, T^B)$, and their Hamming distance is three. \square

3.3. Hamilton cycle of type D. To generate an Hamilton cycle for the involutions in \mathcal{S}_n^D , consider the generating set $T^D = X_1^D \cup X_2^D \cup X_3^D \cup X_4^D$, where

$$X_1^D = \{t_{i,j} : i \leq j < n\}$$

$$X_2^D = \{t_{i,n} \cdot t_{j,n} : i < j < n\}$$

$$X_3^D = \{t_{i,j} \cdot t_{j+1,n} \cdot t_{k,n} : i < j < k - 1\}$$

$$X_4^D = \{t_{j,k-1} \cdot t_{i,j-1}, t_{j,k-1} \cdot t_{i,j-1} \cdot t_{i,n} \cdot t_{j,n}, t_{j,k-1} \cdot t_{i,j-1} \cdot t_{i,n} \cdot t_{k,n} : i < j < k\},$$

with $t_{i,j} = s_i^D s_{i+1}^D \cdots s_{j-1}^D s_j^D s_{j-1}^D \cdots s_{i+1}^D s_i^D$ if $i < j < n$, and $t_{i,i} = s_i^D$ for $i < n$,

$$t_{n-1,n} = s_{n-1}^D s_n^D \quad \text{and} \quad t_{i,n} = s_i^D s_{i+1}^D \cdots s_{n-2}^D \cdot (s_{n-1}^D s_n^D) \cdot s_{n-2}^D \cdots s_{i+1}^D s_i^D,$$

for $i \in [n - 2]$.

Given a list $L = (w_1, w_2, \dots, w_m)$ of involutions of \mathcal{S}_{n-1}^B we write $L \cdot \tilde{n} = (w_1 \cdot \tilde{n}, w_2 \cdot \tilde{n}, \dots, w_m \cdot \tilde{n})$, where each $w_i \cdot \tilde{n}$ is $w_i \cdot n$ if the involution w_i has an even number of negative signs, and is $w_i \cdot \bar{n}$ otherwise. Each permutation in $L \cdot \tilde{n}$ is an involution in \mathcal{S}_n^D .

The construction of the Gray code $\text{GCD}(n)$ for the involutions of order $n \geq 4$ in $G(\mathcal{S}_n^D, T^D)$ is obtained implementing Algorithm 4, whose recursive calls are triggered by the type B Gray codes $\text{GCB}(n)$ and the codes

$$\text{GCD}(1) = (id) \quad \text{and} \quad \text{GCD}(2) = (id, (\bar{1})(\bar{2}), (\bar{1}\bar{2}), (12)).$$

Algorithm 4 Gray code for the involutions in \mathcal{S}_n^D ($n \geq 3$)

- 1: **procedure** $\text{GCD}(n)$
 - 2: Set $F = 23 \cdots (n - 1)1$ and write $\text{GCB}^F(n - 1) \cdot \tilde{n}$;
 - 3: **for** $i = 1$ to $n - 1$ **do**
 - 4: Set $F = 12 \cdots (i - 1)(i + 1) \cdots (n - 1)$;
 - 5: Write $\text{GCD}^F(n - 2) \cdot (in)$;
 - 6: Write $\overleftarrow{\text{GCD}}^F(n - 2) \cdot (\bar{i}\bar{n})$;
-

Tables 3.3 and 3.4 show the Gray codes $\text{GCD}(3)$ and $\text{GCD}(4)$ obtained by Algorithm 3, which as before, should be read down columns, from left to right. Each column contains the involutions generated in a different step of the algorithm.

Theorem 3.6. *If the Gray codes $\text{GCD}(n - 2)$ and $\text{GCB}(n - 1)$ satisfy properties **A1** and **A2**, then the Algorithm 4 produces a cyclic Gray code $\text{GCD}(n)$ for the type D involutions of order $n \geq 3$, which satisfies properties **A1** and **A2**.*

Proof. As in the proof of Theorem 3.2 for the type A case, now using the formula (2.4) for the number of type D involutions, obtained in Proposition 2.1, we can show that the sequence $\text{GCD}(n)$ given by Algorithm 4 contains all involutions in \mathcal{S}_n^D , each appearing exactly once.

123	321	132
1 $\bar{2}$ 3	3 $\bar{2}$ 1	1 $\bar{3}$ 2
$\bar{1}$ 23		
$\bar{1}$ 2 $\bar{3}$		
2 $\bar{1}$ 3		
213		

TABLE 3.3. The Gray code GCD(3).

1234	4231	1432	1243
1 $\bar{2}$ 34	4 $\bar{2}$ 31	1 $\bar{4}$ 32	1 $\bar{2}$ 43
1 $\bar{2}$ 3 $\bar{4}$	4 $\bar{3}$ 21	3 $\bar{4}$ 12	2 $\bar{1}$ 43
12 $\bar{3}$ 4	4321	3412	2143
1 $\bar{3}$ 24	4 $\bar{3}$ 2 $\bar{1}$	3 $\bar{4}$ 1 $\bar{2}$	21 $\bar{4}$ 3
1324	4 $\bar{3}$ 2 $\bar{1}$	3 $\bar{4}$ 1 $\bar{2}$	2 $\bar{1}$ 4 $\bar{3}$
$\bar{1}$ 324	4 $\bar{2}$ 3 $\bar{1}$	1 $\bar{4}$ 3 $\bar{2}$	1 $\bar{2}$ 4 $\bar{3}$
$\bar{1}$ 3 $\bar{2}$ 4	423 $\bar{1}$	1 $\bar{4}$ 3 $\bar{2}$	12 $\bar{4}$ 3
$\bar{1}$ 2 $\bar{3}$ 4			
$\bar{1}$ 23 $\bar{4}$			
$\bar{1}$ 234			
$\bar{1}$ 23 $\bar{4}$			
2 $\bar{1}$ 34			
2 $\bar{1}$ 3 $\bar{4}$			
21 $\bar{3}$ 4			
2134			
3214			
3 $\bar{2}$ 14			
3 $\bar{2}$ 1 $\bar{4}$			
3 $\bar{2}$ 14			

TABLE 3.4. The Gray code GCD(4).

If $\text{GCD}(n-2)$ and $\text{GCB}(n-1)$ satisfy properties **A1** and **A2**, then by construction the sequences $\text{GCB}^F(n-1) \cdot \tilde{n}$, $\text{GCD}^F(n-2) \cdot (in)$ and $\overleftarrow{\text{GCD}}^F(n-2) \cdot (\bar{i}\bar{n})$ generated in Steps 2, 5 and 6 of the algorithm, are formed by pairwise distinct involutions and also satisfy property **A2**. It remains to check that the involutions connecting these sequences also satisfy property **A2**. The last element of $\text{GCB}^F(n-1) \cdot \tilde{n}$ is the involution

$$u_1 = (n-1)2 \cdots 1n \quad \text{or} \quad u_2 = (\overline{n-1})2 \cdots \bar{1}n,$$

and the first element of $\text{GCD}^F(n-2) \cdot (in)$ is $v = n2 \cdots (n-2)(n-1)1$. It follows that v is obtained from either u_1 or u_2 by a rotation of the integers in positions $1, n-1, n$, with possible sign changes of the integers in positions 1 and $n-1$. The same happens between the last and first elements of the sequences generated in consecutive iterations of the **for** cycle in Step 3 of the algorithm, $(\bar{i}\bar{n})$ and $(i+1n)$, respectively, which differ by the rotation of the letters in positions $i, i+1, n$, and sign changes of the letters in positions i and n . The transitions between Steps 5 and 6 are involutions that differ by two sign changes. Finally, notice that property **A1** is clearly satisfied by the sequence $\text{GCD}(n)$. \square

Corollary 3.7. *The Gray code $GCD(n)$ produced by Algorithm 4 is an Hamilton cycle in the restriction to involutions of the Cayley graph $G(\mathcal{S}_n^D, T^D)$, with Hamming distance three, for $n \geq 3$.*

Proof. We will show by induction on $n \geq 2$ that each element of $GCD(n)$ is obtained multiplying on the right the previous element of the code by an element of T^D . This is certainly true for $n = 2$, where each element differ by the previous by two sign changes or a transposition. Fix $n \geq 3$ and assume the result is valid for integers less than n . We start by noticing that by the proof of Corollary 3.5, each two consecutive elements of the code $GCB(n - 1)$ differ by a cycle of three letters in positions $i < j < k$ with the same sign, a transposition of two letters in positions $i < j$, with at most a sign change of the letter in position i , or one or two sign changes. This means that each involution generated in Step 2 of Algorithm 4 is obtained by multiplying the previous element on the right by the generators $t_{j,k-1} \cdot t_{i,j-1}$, $t_{i,j} \cdot t_{j+1,n} \cdot t_{n-1,n}$, $t_{i,n} \cdot t_{j,n}$, or $t_{i,n}$. The same happens with each involution of $GCD^F(n - 2) \cdot (i n)$ and $\overleftarrow{GCD}^F(n - 2) \cdot (\bar{i} \bar{n})$, generated in each iteration of the cycle **for** of the algorithm. Finally, notice that by the proof of Theorem 3.6, the involutions connecting each one of factors $GCB^F(n - 1) \cdot \tilde{n}$, $GCD^F(n - 2) \cdot (i n)$ and $\overleftarrow{GCD}^F(n - 2) \cdot (\bar{i} \bar{n})$, for $i = 1, \dots, n - 1$, are obtained by a rotation of three letters in positions $i < j < k$, with possibly sign changes of the letters in positions i and j , or in positions i and k . This is achieved by right multiplication of the correspondent involution by $t_{j,k-1} \cdot t_{i,j-1}$, or $t_{j,k-1} \cdot t_{i,j-1} \cdot t_{i,n} \cdot t_{j,n}$, or $t_{j,k-1} \cdot t_{i,j-1} \cdot t_{i,n} \cdot t_{k,n}$. \square

4. AN OPTIMAL ALGORITHM FOR THE INVOLUTIONS OF TYPE B

In the previous section we have seen that the Gray Code presented for involutions of type A is optimal with respect to Hamming distance. The same is not true for the codes presented for involutions of types B and D . In [4] it is proven that the minimal Hamming distance of a Gray Code for type B involutions is two and a Gray Code with Hamming distance two is given. In this section we will briefly describe that algorithm and, alongside with the description, we will construct the code for \mathcal{S}_4^B to better illustrate the steps of algorithm. A modification of this algorithm would provide a Gray Code for type D involutions with Hamming distance two, which would be optimal. We give such a construction for \mathcal{S}_4^D and \mathcal{S}_5^D . Before starting the description of the code, we introduce some notation for type B involutions. Since $\mathcal{S}_n^D \subset \mathcal{S}_n^B$, the same notation is valid for both types.

Given $i \in [\pm n]$, we define the sign function $\text{sgn}(i) = 0$ if $i > 0$, and $\text{sgn}(i) = 1$ otherwise. A sign permutation π can also be represented by the pair (p, g) , where $p \in \mathcal{S}_n$ is defined by $p(i) = |\pi(i)|$ for all $i \in [n]$, and $g = g_1 \cdots g_n \in B_n$, the set of binary words of length n , is defined by $g_i = \text{sgn}(\pi(i))$ for all $i \in [n]$. For example, $\pi = \bar{3} 2 \bar{1} 6 5 4 \bar{7} \in \mathcal{S}_7^B$ corresponds to the pair $(3216547, 1010001) \in \mathcal{S}_7 \times B_7$.

Since the elements of \mathcal{S}_n^B are permutations of $[\pm n]$, we can write them in disjoint cycle form. In particular, if $\pi = (p, g)$ is an involution in \mathcal{S}_n^B , then p is also an involution in \mathcal{S}_n , and the cycle decomposition of $\pi = (p, g)$ is obtained by writing p as the disjoint union of transpositions and position fixed points, *i.e.* integers i for which $p(i) = i$, and then associating the respective signs. For our running example $\pi = (3216547, 1010001)$, we have $3216547 = (13)(46)(2)(5)(7) \in \mathcal{S}_7$, and thus $\pi = (\bar{1} \bar{3})(46)(2)(5)(\bar{7})$. When writing a transposition (ab) we adopt the convention that $|a| < |b|$. The integers a and b are called, respectively, the *opener* and *closure* of the transposition (ab) and, as part of an involution,

must have the same sign. The common sign of both elements in a transposition is called a *paired sign*.

Our approach is based on the successive application of the Binary Reflected Gray Code [5], $BRGC_n$, on the set of all binary words that can be associated to a particular involution of \mathcal{S}_n to form a signed involution. We recall now what is the Binary Reflected Gray Code. The $BRGC_1$ is the list $(0, 1)$, and the $BRGC_{n+1}$ is obtainable by first listing $BRGC_n$, with each word prefixed by 0, and then listing the $BRGC_n$ in reverse order with each word prefixed by 1. For instance, $BRGC_2 = (00, 01, 11, 10)$ and $BRGC_3 = (000, 001, 011, 010, 110, 111, 101, 100)$. Each one of the 2^n elements of the sequence $BRGC_n$ differs from the previous one by only one bit, and the same is true for the last and the first elements of the sequence.

This second Gray code, designated by $OGCB_n$, for the involutions in \mathcal{S}_n^B is constructed by layers. Each layer consists in all involutions with a fix number of transpositions. Given $n \in \mathbb{N}$, and $0 \leq k \leq \lfloor n/2 \rfloor$, let L_k denote the set of all involutions in \mathcal{S}_n having exactly k transpositions. For a sign involution $\sigma = (p, g)$, we say that σ is in L_k^B whenever $p \in L_k$. The only element in L_0 is the identity, and any element in L_0^B is written as (id, g) with $g \in B_n$.

(L_0^B) In the first stage we construct the code for the involutions in L_0^B as the sequence $(id, g^1), \dots, (id, g^{2^n})$, where $(g^1, \dots, g^{2^n}) = BRGC_n$.

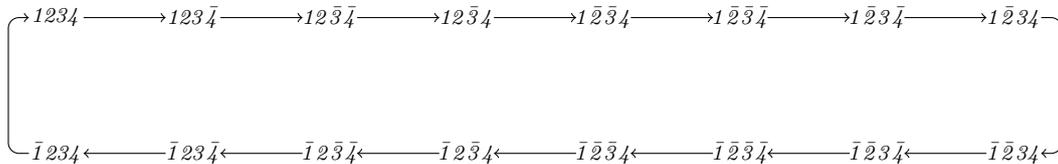


FIGURE 2. Gray code scheme for L_0^B with $n = 4$.

(L_1^B) After having the code for L_0^B , we construct the code for $L_0^B \cup L_1^B$ by inserting sequences of involutions in L_1^B between two consecutive elements of L_0^B . Each one of these sequences is of the form

$$\left((p, h^1), \dots, (p, h^{2^{n-1}}) \right),$$

where $p = (st)$ is a transposition in L_1 and $h = (h^1, \dots, h^{2^{n-1}})$ is a sequence of binary words of length n , obtained from the $BRGC_{n-1}$. The position ℓ where the insertion of this sequence will occur correspond to an involution (id, g^ℓ) where the sign of the letters s and t is the same, and remain unchanged in the involution in position $\ell + 1$. In [3] a procedure was given to compute distinct places for each of these insertions, as well as the correspondent sequence of binary words.

For instance, with $n = 4$ and $p = (12)$, the associated binary sequence is $h = (1100, 0000, 0010, 1110, 1111, 0011, 0001, 1101)$, which will be inserted in positions

$\ell = 9$ of L_0^B . Figure 3 shows the insertion of the involutions associated with transposition (12) into L_0^B .

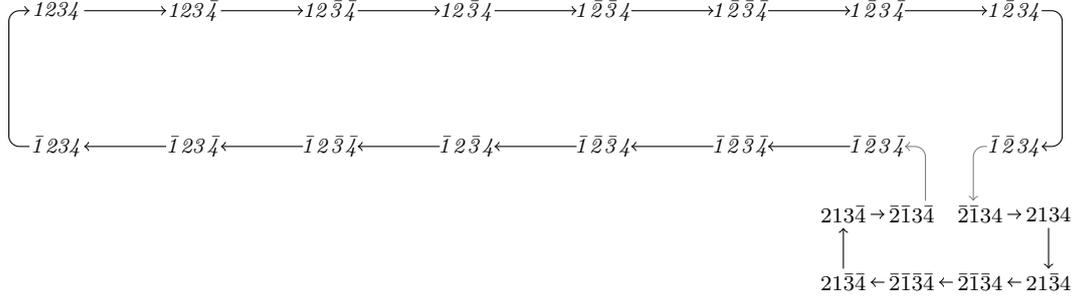


FIGURE 3. Insertion of the sign involutions associated with (12) into L_0^B .

(L_2^B) Next, we have to insert the elements of L_2^B into the code for $L_0^B \cup L_1^B$ computed in the previous step. Each permutation in L_2 is the product of two transpositions, which will be sorted by the lexicographic order of the openers. As in the previous case, for each permutation $p' \in L_2$, we can compute a sequence of binary words $(f^1, \dots, f^{2^{n-2}})$ such that $((p', f^1), \dots, (p', f^{2^{n-2}}))$ contains all sign involutions associated with p , as well as distinct places in the code for $L_0^B \cup L_1^B$ to insert such sequences, satisfying the same property as in the previous layer.

In our running example, with $n = 4$, $p = (12)$ and $p' = p \cdot (34)$, the associated binary code is (1111, 1100, 0000, 0011). The sequence

$$((p', 1111), (p', 1100), (p', 0000), (p', 0011))$$

will be inserted in position $\ell = 5$, that is between involutions (p, h^5) and (p, h^6) . Figure 4 shows the insertion of the sign involutions associated with $p \cdot (34)$ into $L_0^B \cup L_1^B$.

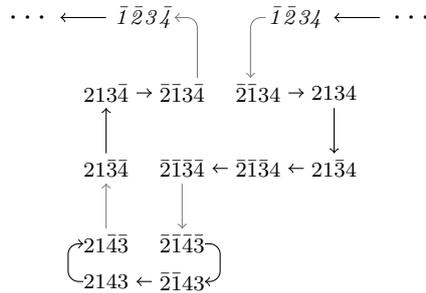


FIGURE 4. Insertion of the sign involutions associated with (12)(34) into $L_0^B \cup L_1^B$.

(L_k^B) The insertion of the involutions of L_k^B into the code for $L_0^B \cup \dots \cup L_{k-1}^B$ is similar to the insertion of the involutions of L_2^B into the previous layer. Each sequence is

associated to an element of

$$L_k(q) := \{q \cdot (ij) : m(q) < i < j, q_i = i, q_j = j\} \subseteq L_k,$$

where $m(q)$ is the largest opener amongst all transpositions in the cycle decomposition of q , and $m(q) = 0$ when q is the identity. Each sequence will be inserted into the correspondence sequence associated with the involution q , following the same rules as before. Notice that the sets $L_k(q)$ form a partition of L_k .

The code $OGCB_n$ is obtained when the last layer is inserted.

Theorem 4.1. *The code $OGCB_n$ produces an Hamilton cycle in the restriction to involutions of the Cayley graph $G(\mathcal{S}_n^B, X_1^B \cup X_2^B)$, with Hamming distance two, for $n \geq 3$. This is the minimal Hamming distance of any Gray code for I_n^B .*

Proof. In [4] it was proven that the sequence produced by the code $OGCB_n$ is a cyclic Gray code with Hamming distance two for \mathcal{S}_n^B , where two consecutive involutions differ by one sign change, two sign changes - in this case, a paired sign -, or a transposition without any sign change. This means that each involution, in the code, is obtained by multiplying the previous element on the right by one reflections of the set $X_1^B \cup X_2^B$. Note that the Hamming distance for any code can only be one if there are only single sign changes between consecutive involutions. Thus this code has the minimal Hamming distance for I_n^B . \square

Table 4.1 shows the Gray code with Hamming distance 2 for the sign involutions in I_4^B using the algorithm defined above. The code should be read down columns, from left to right.

1234	$\bar{1}324$	1432	$\bar{2}\bar{1}4\bar{3}$	4231	$\bar{1}2\bar{3}4$	3214	$\bar{1}24\bar{3}$
$\bar{1}234$	132 $\bar{4}$	$\bar{1}43\bar{2}$	$\bar{2}\bar{1}43$	$\bar{4}23\bar{1}$	$\bar{3}2\bar{1}4$	$\bar{3}214$	$\bar{1}243$
$\bar{1}2\bar{3}4$	$\bar{1}\bar{3}2\bar{4}$	$\bar{1}\bar{2}3\bar{4}$	2143	$\bar{4}2\bar{3}\bar{1}$	$\bar{3}21\bar{4}$	$\bar{3}2\bar{1}4$	$\bar{1}\bar{2}43$
$\bar{1}2\bar{3}4$	$\bar{1}\bar{2}\bar{3}\bar{4}$	$\bar{1}\bar{2}34$	$\bar{2}\bar{1}4\bar{3}$	42 $\bar{3}1$	321 $\bar{4}$	$\bar{1}\bar{2}\bar{3}4$	$\bar{1}\bar{2}4\bar{3}$
$\bar{1}2\bar{3}4$	$\bar{1}4\bar{3}\bar{2}$	$\bar{1}\bar{2}34$	$\bar{2}\bar{1}\bar{3}\bar{4}$	42 $\bar{3}1$	$\bar{3}2\bar{1}4$	$\bar{1}\bar{2}\bar{3}4$	$\bar{1}24\bar{3}$
$\bar{1}\bar{3}\bar{2}4$	14 $\bar{3}2$	$\bar{2}\bar{1}34$	213 $\bar{4}$	4 $\bar{3}\bar{2}1$	$\bar{3}2\bar{1}4$	$\bar{1}\bar{2}\bar{3}\bar{4}$	1243
1324	$\bar{1}4\bar{3}\bar{2}$	2134	$\bar{2}\bar{1}\bar{3}\bar{4}$	4321	$\bar{3}4\bar{1}2$	$\bar{1}\bar{2}3\bar{4}$	
$\bar{1}324$	$\bar{1}4\bar{3}\bar{2}$	2134	$\bar{1}\bar{2}\bar{3}\bar{4}$	432 $\bar{1}$	$\bar{3}4\bar{1}2$	$\bar{1}\bar{2}34$	
$\bar{1}\bar{3}\bar{2}4$	$\bar{1}4\bar{3}\bar{2}$	$\bar{2}\bar{1}\bar{3}4$	$\bar{4}2\bar{3}\bar{1}$	$\bar{4}\bar{3}\bar{2}\bar{1}$	$\bar{3}4\bar{1}\bar{2}$	$\bar{1}\bar{2}43$	
$\bar{1}\bar{3}\bar{2}\bar{4}$	$\bar{1}432$	$\bar{2}\bar{1}\bar{3}\bar{4}$	4 $\bar{2}31$	$\bar{4}2\bar{3}\bar{1}$	3412	$\bar{1}24\bar{3}$	

TABLE 4.1. Gray code for I_4^B with Hamming distance 2.

4.1. Towards an optimal algorithm for the involutions of type D . In section 3.3 we constructed an Hamilton cycle with Hamming distance 3 for the involutions in I_n^D . In this section we analyze the existence of such Hamilton cycle with distance 2, which would be optimal since is clear that such code cannot have distance 1. So, consider the graph $G(I_n^D)$, where two involutions are connected if their Hamming distance is 2. When $n = 2$ the Hamming distance between any two involutions in I_2^D is 2, and thus $G(I_2^D)$ has an Hamilton cycle with Hamming distance 2. The graph $G(I_3^D)$ is displayed in Figure 5, where we have omitted all but three of the edges linking the identity 123 to all other involutions. It is easy to check that there is no Hamilton cycle in $G(I_3^D)$, but there are

Hamilton paths. One Hamilton path starts with the involution $1\bar{2}\bar{3}$, and can be read off of the graph by following the solid edges:

$$(1\bar{2}\bar{3}, 1\bar{3}\bar{2}, 132, 213, \bar{1}\bar{2}3, \bar{2}\bar{1}3, 123, 321, \bar{1}2\bar{3}, \bar{3}2\bar{1}).$$

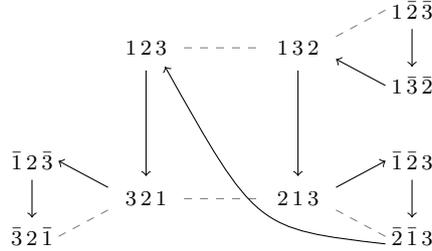


FIGURE 5. An Hamilton path in $G(I_3^D)$ with Hamming distance 2.

Our approach for the general case is based on the successive application of a Binary Code, BCE_n , on the set of all 2^{n-1} binary words with an even number of 1's that can be associated to a particular involution of \mathcal{S}_n to form an involution of type D . This Binary Code is constructed by recursion for $n \geq 2$, triggered by $BCE_2 = (00, 11)$, as follows: if

$$BCE_{n-1} = (u_1, u_2, \dots, u_k) \quad \text{and} \quad BRGC_{n-2} = (v_1, v_2, \dots, v_k),$$

where $k = 2^{n-2}$, then let

$$BCE_n = (0 \cdot u_1, 0 \cdot u_2, \dots, 0 \cdot u_k, 10 \cdot v_k, 11 \cdot v_{k-1}, 10 \cdot v_{k-2}, 11 \cdot v_{k-3}, \dots, 11 \cdot v_1).$$

Each one of the 2^{n-1} elements of the sequence BCE_n differs from the previous one by two bits, and the same is true for the last and the first elements of the sequence. For instance, the BCE_n code for $n = 3, 4, 5$ is given in Table 4.2.

BCE_3	BCE_4	BCE_5
000	0000	00000
011	0011	00011
101	0101	00101
110	0110	00110
	1010	01010
	1111	01111
	1001	01001
	1100	01100
		10100
		11101
		10111
		11110
		10010
		11011
		10001
		11000

TABLE 4.2. BCE_n , for $n = 3, 4, 5$.

The construction of an Hamilton cycle for $G(I_4^D)$ with distance 2 can be obtained as follows. We start by constructing a path with distance 2 for the sign involution in the set $\{(p, g) : g \in B_4\} \cap I_4^D$, for each $p \in L_2$:

$$\begin{aligned} L_2^{(12)(34)} &= (21\bar{4}\bar{3}, \bar{2}\bar{1}\bar{3}\bar{4}, \bar{2}\bar{1}43, 2143), \\ L_2^{(13)(24)} &= (3412, \bar{3}4\bar{1}2, \bar{3}\bar{4}\bar{1}\bar{2}, 3\bar{4}1\bar{2}), \\ L_2^{(14)(23)} &= (4\bar{3}\bar{2}1, 4321, \bar{4}32\bar{1}, \bar{4}\bar{3}\bar{2}\bar{1}). \end{aligned}$$

Each one of these sequences will be inserted between the paths with distance 2 for two sets $\{(p, g) : g \in B_4\} \cap I_4^D$, with $p \in L_1$, such that the elements linking the three paths differ by a single transposition of two letters:

$$\begin{aligned} L_1^{(12)} \cdot L_2^{(12)(34)} \cdot L_1^{(34)} &= (2134, \bar{2}\bar{1}34, \bar{2}\bar{1}\bar{3}\bar{4}, 21\bar{3}\bar{4}, L_2^{(12)(34)}, 1243, \bar{1}\bar{2}43, \bar{1}\bar{2}\bar{4}\bar{3}, 12\bar{4}\bar{3}), \\ L_1^{(13)} \cdot L_2^{(13)(24)} \cdot L_1^{(24)} &= (\bar{3}2\bar{1}4, \bar{3}\bar{2}\bar{1}\bar{4}, \bar{3}\bar{2}1\bar{4}, 3214, L_2^{(13)(24)}, 1\bar{4}3\bar{2}, 1432, \bar{1}4\bar{3}\bar{2}, \bar{1}\bar{4}\bar{3}\bar{2}), \\ L_1^{(23)} \cdot L_2^{(23)(14)} \cdot L_1^{(14)} &= (\bar{1}\bar{3}\bar{2}\bar{4}, \bar{1}32\bar{4}, 1324, 1\bar{3}\bar{2}4, L_2^{(14)(23)}, \bar{4}\bar{2}\bar{3}\bar{1}, 4\bar{2}\bar{3}1, 4231, \bar{4}23\bar{1}). \end{aligned}$$

The final step consists in the insertion of these paths into the level L_0 path

$$((1234, g_1), \dots, (1234, g_8)),$$

where $(g_1, \dots, g_8) = BCE_4$, such that the elements linking the different paths differ by a single transposition of two letters. The resulting code is an Hamilton cycle with distance 2 in the graph $G(I_4^D)$, where two consecutive involutions differ either by two sign changes or by a transposition of two letters:

$$\begin{aligned} I_4^D &= (1234, L_1^{(12)} \cdot L_2^{(12)(34)} \cdot L_1^{(34)}, 12\bar{3}\bar{4}, 1\bar{2}\bar{3}\bar{4}, 1\bar{2}\bar{3}4, \bar{1}\bar{2}\bar{3}4, \\ &L_1^{(13)} \cdot L_2^{(13)(24)} \cdot L_1^{(24)}, \bar{1}\bar{2}\bar{3}\bar{4}, L_1^{(23)} \cdot L_2^{(23)(14)} \cdot L_1^{(14)}, \bar{1}23\bar{4}, \bar{1}\bar{2}34). \end{aligned}$$

The same process can be used to obtain an Hamilton cycle for $G(I_5^D)$ with distance 2. Start with paths the L_i^p with distance 2 for the sign involutions in the sets

$$\{(p, g) : g \in BRGC_5\} \cap I_5^D,$$

for each $p \in L_i$, $i = 2, 1$, displayed in Table 4.3, and

$$L_0 = \{(1234, g_1), \dots, (1234, g_{16}) : (g_1, \dots, g_{16}) = BCE_5\}.$$

Then, insert each path L_2^p into a path $L_1^{p'}$, and finally each one of these paths into L_0 , such that the words linking the paths differ by a single transposition of two letters, as indicated in the Table 4.3, which should be read top to bottom, starting in the left column.

Computational evidence suggests that the process described above can be generalized for any integer $n \geq 6$, since the availability of connection words that are used to link two distinct paths L_i^α and $L_{i+1}^{(ab)\alpha}$ together, satisfying the distance requirement, will increase in number as n gets bigger. This leads to the following conjecture.

word	layer	word	layer	word	layer	word	layer
12345	L_0	12435	$L_1^{(34)}$	12345	L_0	52431	$L_2^{(15)(34)}$
12354	$L_1^{(45)}$	15432	$L_2^{(34)(25)}$	12345	L_0	52431	$L_2^{(15)(34)}$
12354	$L_1^{(45)}$	15432	$L_2^{(34)(25)}$	42315	$L_1^{(14)}$	52341	$L_1^{(15)}$
12354	$L_1^{(45)}$	15432	$L_2^{(34)(25)}$	43215	$L_2^{(14)(23)}$	52341	$L_1^{(15)}$
12354	$L_1^{(45)}$	15432	$L_2^{(34)(25)}$	43215	$L_2^{(14)(23)}$	52341	$L_1^{(15)}$
13254	$L_2^{(45)(23)}$	15342	$L_1^{(25)}$	43215	$L_2^{(14)(23)}$	53241	$L_2^{(15)(23)}$
13254	$L_2^{(45)(23)}$	15342	$L_1^{(25)}$	43215	$L_2^{(14)(23)}$	53241	$L_2^{(15)(23)}$
13254	$L_2^{(45)(23)}$	15342	$L_1^{(25)}$	42315	$L_1^{(14)}$	53241	$L_2^{(15)(23)}$
13254	$L_2^{(45)(23)}$	15342	$L_1^{(25)}$	42315	$L_1^{(14)}$	53241	$L_2^{(15)(23)}$
13245	$L_1^{(23)}$	12345	L_0	42513	$L_2^{(14)(35)}$	52341	$L_1^{(15)}$
13245	$L_1^{(23)}$	12345	L_0	42513	$L_2^{(14)(35)}$	52341	$L_1^{(15)}$
13245	$L_1^{(23)}$	12345	L_0	42513	$L_2^{(14)(35)}$	12345	L_0
13245	$L_1^{(23)}$	32145	$L_1^{(13)}$	42513	$L_2^{(14)(35)}$	12345	L_0
12345	L_0	35142	$L_2^{(13)(25)}$	42315	$L_1^{(14)}$	21345	$L_1^{(12)}$
12345	L_0	35142	$L_2^{(13)(25)}$	42315	$L_1^{(14)}$	21435	$L_2^{(12)(34)}$
12345	L_0	35142	$L_2^{(13)(25)}$	42315	$L_1^{(14)}$	21435	$L_2^{(12)(34)}$
12345	L_0	35142	$L_2^{(13)(25)}$	45312	$L_2^{(14)(25)}$	21435	$L_2^{(12)(34)}$
12543	$L_1^{(35)}$	32145	$L_1^{(13)}$	45312	$L_2^{(14)(25)}$	21435	$L_2^{(12)(34)}$
12543	$L_1^{(35)}$	34125	$L_2^{(13)(24)}$	45312	$L_2^{(14)(25)}$	21345	$L_1^{(12)}$
12543	$L_1^{(35)}$	34125	$L_2^{(13)(24)}$	45312	$L_2^{(14)(25)}$	21345	$L_1^{(12)}$
12543	$L_1^{(35)}$	34125	$L_2^{(13)(24)}$	42315	$L_1^{(14)}$	21345	$L_1^{(12)}$
14523	$L_2^{(35)(24)}$	34125	$L_2^{(13)(24)}$	42315	$L_1^{(14)}$	21354	$L_2^{(12)(45)}$
14523	$L_2^{(35)(24)}$	32145	$L_1^{(13)}$	42315	$L_1^{(14)}$	21354	$L_2^{(12)(45)}$
14523	$L_2^{(35)(24)}$	32145	$L_1^{(13)}$	12345	L_0	21354	$L_2^{(12)(45)}$
14523	$L_2^{(35)(24)}$	32145	$L_1^{(13)}$	12345	L_0	21354	$L_2^{(12)(45)}$
14325	$L_1^{(24)}$	32145	$L_1^{(13)}$	12345	L_0	21354	$L_2^{(12)(45)}$
14325	$L_1^{(24)}$	32154	$L_2^{(13)(45)}$	12345	L_0	21354	$L_2^{(12)(45)}$
14325	$L_1^{(24)}$	32154	$L_2^{(13)(45)}$	52341	$L_1^{(15)}$	21354	$L_2^{(12)(45)}$
14325	$L_1^{(24)}$	32154	$L_2^{(13)(45)}$	52341	$L_1^{(15)}$	21354	$L_2^{(12)(45)}$
14325	$L_1^{(24)}$	32154	$L_2^{(13)(45)}$	54321	$L_2^{(15)(24)}$	21345	$L_1^{(12)}$
14325	$L_1^{(24)}$	32154	$L_2^{(13)(45)}$	54321	$L_2^{(15)(24)}$	21345	$L_1^{(12)}$
14325	$L_1^{(24)}$	32154	$L_2^{(13)(45)}$	54321	$L_2^{(15)(24)}$	21345	$L_1^{(12)}$
12345	L_0	32145	$L_1^{(13)}$	54321	$L_2^{(15)(24)}$	21543	$L_2^{(12)(35)}$
12345	L_0	32145	$L_1^{(13)}$	54321	$L_2^{(15)(24)}$	21543	$L_2^{(12)(35)}$
12435	$L_1^{(34)}$	32145	$L_1^{(13)}$	52341	$L_1^{(15)}$	21543	$L_2^{(12)(35)}$
12435	$L_1^{(34)}$	32145	$L_1^{(13)}$	52341	$L_1^{(15)}$	21543	$L_2^{(12)(35)}$
12435	$L_1^{(34)}$	32145	$L_1^{(13)}$	52431	$L_2^{(15)(34)}$	21543	$L_2^{(12)(35)}$
12435	$L_1^{(34)}$	32145	$L_1^{(13)}$	52431	$L_2^{(15)(34)}$	21543	$L_2^{(12)(35)}$
12435	$L_1^{(34)}$	12345	L_0	52431	$L_2^{(15)(34)}$	21345	$L_1^{(12)}$

TABLE 4.3. Hamilton cycle with distance 2 for $G(I_5^D)$.

Conjecture 4.2. *There is an Hamilton cycle in the restriction to involutions of the Cayley graph $G(\mathcal{S}_n^B, X_1^D \cup X_2^D)$, with Hamming distance two, for $n \geq 4$, where*

$$X_1^D = \{t_{i,j} : i \leq j < n\}$$

$$X_2^D = \{t_{i,n} \cdot t_{j,n} : i < j < n\}$$

This is the minimal Hamming distance of any Gray code for I_n^D .

REFERENCES

- [1] C.-O. Chow (2006). Counting involutory, unimodal, and alternating signed permutations. *Discrete Math.* 306, no. 18, 2222–2228.
- [2] A. Björner and F. Brenti (2005). *Combinatorics of Coxeter Groups*. Graduate Texts in Mathematics Vol. 231, Springer.
- [3] G. Gutierrez, Ricardo Mamede and J.L. Santos (2018). Gray codes for signed involutions. *Discrete Mathematics*, Vol. 341, N.9, pp. 2590-2601.
- [4] G. Gutierrez, Ricardo Mamede and J.L. Santos (2019). Optimal Gray code for involutions. *Information Processing Letters*, Vol. 148, pp. 19-22.
- [5] F. Gray (1953). Pulse code communications, U. S. Patent 2632 058, March 17.
- [6] J. Meier (2008). *Groups, Graphs and Trees: An Introduction to the Geometry of Infinite Groups*. London Mathematical Society Student Texts, Cambridge University Press.
- [7] T. Mütze (2023), Combinatorial Gray Codes — an Updated Survey. *The Electronic Journal of Combinatorics*. DS26, Dynamic Surveys, 93 pp.
- [8] C. Savage (1997). A survey of combinatorial Gray codes. *SIAM Rev.* 39 (4), 605–629.
- [9] F. Schmidt, R. Simion (1992). Even minus odd involutions in the symmetric group. *SIAM Rev.* 34 (2), 315–317.

UNIVERSITY OF COIMBRA, CMUC, DEPARTMENT OF MATHEMATICS
Email address: ggutc@mat.uc.pt

UNIVERSITY OF COIMBRA, CMUC, DEPARTMENT OF MATHEMATICS
Email address: mamede@mat.uc.pt

UNIVERSITY OF COIMBRA, CMUC, DEPARTMENT OF MATHEMATICS
Email address: zeluis@mat.uc.pt