The Structure of Single-Track Gray Codes

Moshe Schwartz and Tuvi Etzion, *Senior Member, IEEE*

***Abstract*—Single-track Gray codes are cyclic Gray codes with codewords of length n, such that all the n tracks which correspond to the n distinct coordinates of the codewords are cyclic shifts of the first track. We investigate the structure of such binary codes and show that there is no such code with 2^n codewords when n is a power of 2. This implies that the known codes with $2^n - 2n$ codewords, when n is a power of 2, are optimal. This result is then generalized to codes over GF(p), where p is a prime. A subclass of single-track Gray codes, called single-track Gray codes with k-spaced heads, is also defined. All known systematic constructions for single-track Gray codes result in codes from this subclass. We investigate this class and show it has a strong connection with two classes of sequences, the full-order words and the full-order self-dual words. We present an iterative construction for binary single-track Gray codes which are asymptotically optimal if an infinite family of asymptotically optimal seed-codes exists. This construction is based on an effective way to generate a large set of distinct necklaces and a merging method for cyclic Gray codes based on necklaces representatives.**

***Index Terms*—Cyclic Gray codes, feedback shift-register, linear complexity, necklaces, self-dual sequences, single-track codes.**

I. Introduction

GRAY codes were found by Gray [15] and introduced by Gilbert [14] as a listing of all the binary n-tuples in a list such that any two successive n-tuples in the list differ in exactly one position. Generalization of Gray codes were given during the years. Such generalizations include the arrangements of other combinatorial objects in a such way that any two consecutive elements in the list differ in some prespecified, usually small way [14], [15]. Other generalizations include listing subsets of the binary n-tuples in a Gray code manner, in such a way that the list has some more prespecified properties. These properties were usually forced by a specific application for the Gray code. As an example we have the uniformly balanced Gray codes. In certain applications, it is needed that the number of bit changes will be uniformly distributed among the bit positions. Uniformly balanced Gray codes were shown to exist for n which is a power of 2 by Wagner and West [25]. Recently, Bhat and Savage [2] have shown that such codes exist for all n. During the years Gray codes and their generalizations have found applications in a variety of areas such as information storage and retrieval [4], processor allocation in the hypercube [5], statistics [7], codes for certain memory devices [8], hashing [10], puzzles, such as the Chinese Rings and Tower of Hanoi [13], ordering of documents on shelves [19], signal encoding [20], data compression [22], and circuit testing [23]. Finally, for an excellent survey on Gray codes the interested reader is referred to [24].

The classic example of a Gray code is the *reflected Gray code* [14], [15]. This code is a list of the 2^n binary n-tuples in the following way. For $n = 1$ the list consists of the words 0 and 1. Given the list $\mathcal{X}$ of the 2^{n-1} binary $(n-1)$-tuples, we generate the list of the 2^n binary n-tuples by attaching a ZERO as a prefix to every element of the list $\mathcal{X}$ in its order, and then attaching a ONE as a prefix to every element of the same list $\mathcal{X}$ in reversed order. As an example, for $n = 3$ the list of the reflected Gray code is 000, 001, 011, 010, 110, 111, 101, 100. One of the properties of the reflected Gray code is that there is a change in the last coordinate of every other word. We will use this property later.

In this paper we discuss another class of Gray codes, single-track Gray codes. A single-track Gray code is a list of P distinct binary words of length n, such that each two consecutive words, including the last and the first, differ in exactly one position and when looking at the list as an $P \times n$ array, each column of the array is a cyclic shift of the first column. These codes were defined by Hiltgen, Paterson, and Brandestini [16] who also gave their main application. A length n, period P Gray code can be used to record the absolute angular positions of a rotating wheel by encoding (e.g., optically) the codewords on n concentrically arranged tracks. Then n reading heads, mounted in parallel across the tracks suffice to recover the codewords. When the heads are nearly aligned with the division between two codewords, any components which change between those words will be in doubt and a spurious position value may result. Such quantization errors are minimized by using a Gray code encoding, for then exactly one component can be in doubt and the two codewords that could possibly result identify the positions bordering the division, resulting in a small angular error. When high resolution is required, the need for a large number of concentric tracks results in encoders with large physical dimensions. This poses a problem in the design of small-scale or high-speed devices. Single-track Gray codes were proposed in [16] as a way of overcoming these problems. Note, that since all the columns in these codes are cyclic shifts of the first one, it follows that the code is also a uniformly balanced Gray code, which again can be described by a single column. Not many constructions for single-track Gray codes are known. All these constructions are given in [9] and [16]. None of the known constructions is known to produce an infinite family of optimal codes, where by the word optimal we

Manuscript received April 20, 1998; revised May 15, 1999. This work was supported by the Fund for the Promotion of Research at the Technion.

The authors are with the Computer Science Department, Technion–Israel Institute of Technology, Haifa 32000, Israel (e-mail: {moosh, etzion}@cs.technion.ac.il).

Communicated by T. E. Fuja, Associate Editor at Large.
Publisher Item Identifier S 0018-9448(99)07312-5.

mean that the code has the largest period for a given length n. The main goal of this paper is to study the structure of these codes and to construct codes with period P as large as possible. In this context we will say that codes of an infinite family are asymptotically optimal if

$$\lim_{n\to\infty} \frac{P_n}{2^n} = 0 \tag{1}$$

where n is the code length and P_n is its period.

In Section II, we present the formal definitions for single-track Gray codes. Then, we discuss the known construction methods and structure of single-track Gray codes mainly of those generated by the known construction methods. We discuss all the main known results in this area. In Section III, we present an improvement to one of the known upper bounds, i.e., we show that single-track Gray codes with words of length n and period 2^n do not exist even if n is a power of 2. This proof establishes as a corollary that Etzion and Paterson [9] have constructed an infinite family of optimal single-track Gray codes. In Section IV, we present an iterative construction for Gray codes of length nk from specific classes of Gray codes of lengths n and k. This class is infinite and the codes constructed are asymptotically optimal, given infinite families of asymptotically optimal seed-codes for the construction. For example, if we have infinite families of optimal seed-codes for length p_1^n and length p_2^n, $n \to \infty$, then our construction produces an infinite family of optimal codes for length $p_1^{n_1} p_2^{n_2}$, $n_1, n_2 \to \infty$.

II. The Structure of Single-Track Gray Codes

In this section we present the formal definitions for single-track Gray codes. Then, we present some basic properties of such codes and the idea of the main two known methods to construct such codes. These two methods provide single-track Gray codes with additional special properties. We further investigate these properties. We also outline the results of past work in this area.

Let $W=[w_0, w_1, \cdots, w_{n-1}]$ be a length n word. The *cyclic shift operator*, $\boldsymbol{E}$, is defined by $\boldsymbol{E}W = [w_1, w_2, \cdots, w_{n-1}, w_0]$ and the *complementary cyclic shift operator* $\overline{\boldsymbol{E}}$ is defined similarly by $\overline{\boldsymbol{E}}W = [w_1, w_2, \cdots, w_{n-1}, \overline{w_0}]$, where $\bar{b}$ is the binary complement of b. Two length n words W_1, W_2 are said to be *equivalent* if there exists an integer i such that $\boldsymbol{E}^i W_1 = W_2$, where $\boldsymbol{E}^i$ is i consecutive applications of $\boldsymbol{E}$. The equivalence classes under the shift operator are called *necklaces*. Efficient algorithms for producing necklaces of a given length are given in [11], [12], and [21]. A length $2n$ word $W = [w_0, w_, \cdots, w_{2n-1}]$ is called *self-dual* if for each i, $0 \le i \le n-1$, $w_{n+i} = \overline{w_i}$. Finally, for any two positive integers a and b, $\gcd(a, b)$ denotes the greatest common divisor of a and b.

Definition 1: Let W be a length n word. We define the *cyclic order* of W as

$$o(W) \triangleq \min\left\{i \mid \boldsymbol{E}^i W = W,\ i \ge 1\right\}$$

and the *complementary cyclic order* of W as

$$\overline{o}(W) \triangleq \min\left\{i \mid \overline{\boldsymbol{E}}^i W = W,\ i \ge 1\right\}.$$

If $o(W) = n$ we say that W has *full cyclic order* (or *full-order* in short), and if $\overline{o}(W) = 2n$ we say that $W\overline{W}$ is a full-order self-dual word.

Definition 2: A *length* n period P *Gray code* is an ordered list of P distinct binary length n words

$$W_0, W_1, \cdots, W_{P-1}$$

such that each two adjacent words differ in exactly one coordinate. If W_{P-1} and W_0 also satisfy this condition, we say the code is *cyclic*.

Definition 3: Let C be an ordered list of P length n words

$$W_0, W_1, \cdots, W_{P-1}.$$

For each $0 \le i < P$ we denote the components of W_i as

$$W_i = \left[w_i^0, w_i^1, \cdots, w_i^{n-1}\right].$$

The jth track of C, for $0 \le j < n$, is defined as

$$t_j(C) \triangleq \left[w_0^j, w_1^j, \cdots, w_{P-1}^j\right].$$

We say that C has the *single-track property* if there exist integers

$$k_0, k_1, \cdots, k_{n-1}$$

called the *head positions*, where $k_0 = 0$, such that $t_i(C) = \boldsymbol{E}^{k_i} t_0(C)$ for each $0 \le i < n$. For each $0 \le i < n$, k_i is called the *position of the* ith head. The first track is called the *generating track* of the code.

Definition 4: Let C be an ordered list of P length n words

$$W_0, W_1, \cdots, W_{P-1}.$$

We say that C is a *length* n*, period* P *single-track Gray code* if C is a cyclic Gray code and C has the single-track property.

The main goal is now to construct a length n, period P single-track Gray code, where P is as large as possible. Bounds on P are of a special interest and a very straightforward result is the following lemma.

Lemma 1 [16, Lemma 2]: If C is a length n, period P single-track Gray code, then $2n|P$ and $2n \le P \le 2^n$.

There are only a few constructions for single-track Gray codes [9], [16]. None of them attains the upper bound forced by Lemma 1 for infinitely many values of n. Each of these constructions is based on one of the following methods.

Theorem 1 [9, Theorem 4]: Let $S_0, S_1, \cdots, S_{r-1}$ be r length n binary pairwise nonequivalent full-order words, such that for each $0 \le i < r-1$, S_i, and S_{i+1} differ in exactly one coordinate, and there also exists an integer l, $\gcd(l, n) = 1$, such that S_{r-1} and $E^l S_0$ differ in exactly one coordinate, then the following words form a length n, period nr single-track Gray code

$$\begin{array}{llll} S_0, & S_1, & \cdots & S_{r-1}, \\ \boldsymbol{E}^l S_0, & \boldsymbol{E}^l S_1, & \cdots & \boldsymbol{E}^l S_{r-1}, \\ \boldsymbol{E}^{2l} S_0, & \boldsymbol{E}^{2l} S_1, & \cdots & \boldsymbol{E}^{2l} S_{r-1}, \\ & \vdots & \vdots & \\ \boldsymbol{E}^{(n-1)l} S_0, & \boldsymbol{E}^{(n-1)l} S_1, & \cdots & \boldsymbol{E}^{(n-1)l} S_{r-1}. \end{array}$$

Theorem 2 [9, Theorem 15]: Let $S_0, S_1, \cdots, S_{r-1}$ be r length $2n$ self-dual full-order pairwise nonequivalent words. For each i, $1 \le i \le r-1$, let $S_i = [s_i^0, s_i^1, \cdots, s_i^{2n-1}]$ and let

$$F^j S_i = \left[s_i^j, s_i^{j+1}, \cdots, s_i^{j+n-1}\right]$$

where superscripts are taken modulo $2n$.

If for each $0 \le i < r-1$, S_i and S_{i+1} differ in exactly two coordinates, and there also exists an integer l, $\gcd(l, 2n) = 1$, such that S_{r-1} and $E^l S_0$ differ in exactly two coordinates, then the following words form a length n, period $2nr$ single-track Gray code:

$$\begin{array}{llll} F^0 S_0, & F^0 S_1, & \cdots & F^0 S_{r-1}, \\ F^l S_0, & F^l S_1, & \cdots & F^l S_{r-1}, \\ F^{2l} S_0, & F^{2l} S_1, & \cdots & F^{2l} S_{r-1}, \\ & \vdots & \vdots & \\ F^{(2n-1)l} S_0, & F^{(2n-1)l} S_1, & \cdots & F^{(2n-1)l} S_{r-1}. \end{array}$$

Now, in order to construct a single-track Gray code we want to order as many as possible full-order words of length n, or full-order self-dual words of length $2n$ in a way which satisfies either Theorems 1 or 2, respectively. Hiltgen, Paterson, and Brandestini [16] suggested a method for ordering length n full-order words in a way which satisfies the conditions of Theorem 1. Their result is summarized in the following theorem.

Theorem 3 [16, Theorem 3]: If $n \ge 4$, then there exists a length n, period nt single-track Gray code for each even t which satisfies

$$2 \le t \le 2^{n-\left\lceil \sqrt{2(n-3)} \right\rceil - 1}.$$

Etzion and Paterson [9] supplied three iterative constructions. The first construction produces a special arrangement of $2^{n-1}r$ pairwise nonequivalent full-order words of length $2n$, which satisfies the conditions of Theorem 1 from a special arrangement of r full-order words of length n which satisfies the same conditions. If p is prime and such arrangement of the $\frac{2^p-2}{p}$ pairwise nonequivalent full-order words is known, then the construction produces a length $2p$, period $2^{2p} - 2^{p+1}$ single-track Gray code. This is an optimal code based on Theorem 1, but by using Theorem 2 it might be possible to obtain a length $2p$ period $2^{2p} - 4$ single-track Gray code. Such a code may exist since there are exactly four words of length $2p$ which are lying in nonfull-order self-dual necklaces. This comparison is important as all the known codes are obtained from these two constructions and no code which is not obtained by these construction or a variant of Theorem 2, which will be mentioned later in this section, is known.

The second construction of [9] which is a generalization of the first one in a certain sense produces a length kn, period $rs(2^n - s)^{k-1}(k+1)n$ single-track Gray code, where $n + 1 \le s \le 2^{n-1}$, from a code of length n and period rn. This code is far from being optimal in any sense. In Section IV, we improve this result for most cases, by producing better codes for similar parameter lengths.

The third construction of [9] is based on Theorem 2 and generates an infinite family of asymptotically optimal codes. These codes have length $n = 2^m$, $m \ge 3$, and period $2^n - 2n$. As we will see in the next section, this construction actually produces optimal codes since the upper bound given in Lemma 1 on the period of length n, period P single-track Gray code, for n which is a power of 2, can be improved. A similar construction can be given for n's which are not powers of 2. Unfortunately, we need some seed-codes with some given properties to obtain better codes for other parameters, and these seed-codes have not been found yet.

Definition 5: Let C be a length n, period P single-track Gray code, and let the head positions be $k_0, k_1, \cdots, k_{n-1}$. We say that C has *k-spaced heads* if

$$k_{i+1} \equiv k_i + k \pmod{P}$$

for each $0 \le i \le n-2$.

It is important to note that all the constructions for single-track Gray codes known today produce codes which are either with k-spaced heads or with a self-dual generating track which can produce a single-track Gray code with k-spaced heads, as will be proved later in this section. As a first step we want to show that all k-spaced heads single-track Gray codes are generated by the construction method of either Theorems 1 or 2.

Definition 6: Let C be a set of words. The *cyclic order* and *complementary cyclic order* of the code C are defined as

$$o(C) \triangleq \min\{o(W) | \; W \in C\}$$
$$\overline{o}(C) \triangleq \min\{\overline{o}(W) | \; W \in C\}.$$

Theorem 4: Let C be a length n, period P single-track Gray code with k-spaced heads.

- If k is even then
  - — $\gcd(k, P) = P/(o(C))$.
  - — $o(W) = o(C) = n$ for each $W \in C$.
  - — There exists an ordering of $P/(o(C))$ length n necklace representatives of cyclic order n, which satisfies the requirements of Theorem 1.
- If k is odd then
  - — $\gcd(k, P) = P/(\overline{o}(C))$.
  - — $\overline{o}(W) = \overline{o}(C) = 2n$ for each $W \in C$.
  - — There exists an ordering of $P/(\overline{o}(C))$ length $2n$ self-dual necklace representatives of full cyclic order $2n$, which satisfies the requirements of Theorem 2.

Proof: Without loss of generality (w.l.o.g.) we assume that $k_0 = 0$. Let C be a length n, period P single-track Gray code with k-spaced heads. Let $s = [s_0, s_1, \cdots, s_{P-1}]$ be the generating track of C. The ith word, W_i, of C has the form

$$W_i = [s_i, s_{i+k}, s_{i+2k}, \cdots, s_{i+(n-1)k}]$$

and hence

$$W_{i+k} = [s_{i+k}, s_{i+2k}, \cdots, s_{i+(n-1)k}, s_{i+nk}].$$

We now distinguish between two cases.

Case 1: k is even. Since C is a Gray code, it follows that the parity of W_i and W_{i+k} is the same, and hence $s_i = s_{i+nk}$ and $W_{i+k} = \boldsymbol{E} W_i$. Therefore, for each j_1, j_2, which satisfy $j_1 \equiv j_2 (\bmod \gcd(k, P))$ there exists an l such that $\boldsymbol{E}^l W_{j_1} = W_{j_2}$. Now, let W_m be a word in C for which $o(W_m) = o(C)$. Since $W_{i+jk} = \boldsymbol{E}^j W_i$, it follows that

$$W_{m+o(C)k} = \boldsymbol{E}^{o(C)} W_m = W_m$$

and

$$W_{m+jk} = \boldsymbol{E}^j W_m \neq W_m$$

for each $0 < j < o(C)$. Since each word appears at most once in the code, it follows that $o(C)k \equiv 0 (\bmod P)$ and hence $\boldsymbol{E}^{o(C)} W = W$ for each $W \in C$, and $\boldsymbol{E}^i W \neq W$ for each $0 < i < o(C)$, which means that $o(W) = o(C)$ and, therefore, $\gcd(k, P) \cdot o(C) = P$.

It is well known that $o(C)$ divides n, and if $o(C) < n$, then the weight of all the words is divisible by $n/o(C) > 1$. Therefore, no two words differ in exactly one coordinate. Thus $o(C) = n$.

It is obvious that the list $W_0, W_1, \cdots, W_{P/o(C)-1}$ forms a Gray code, and since $\gcd(k, P) = P/o(C)$, it follows that all the words in it are pairwise nonequivalent. Moreover, there exists l_1 such that $W_{P/o(C)} = \boldsymbol{E}^{l_1} W_0$. Therefore, there exists l_2 such that $l_1 k = l_2 P + P/o(C)$ which implies

$$\frac{o(C)k}{P} \cdot l_1 - l_2 \cdot o(C) = 1.$$

Since $o(C)k/P$ is an integer, it follows that $\gcd(o(C), l_1) = 1$. Thus the list $W_0, W_1, \cdots, W_{P/o(C)-1}$ satisfies all the requirements of Theorem 1.

Case 2: k is odd. The parity of W_i is different from the parity of W_{i+k}, and hence $s_i = \overline{s_{i+nk}}$. The rest of the proof is similar to the one of Case 1, where we use $\overline{o}(\cdot)$ and $\overline{\boldsymbol{E}}$ instead of $o(\cdot)$ and $\boldsymbol{E}$, respectively. □

Single-track Gray codes with k-spaced heads have some additional properties as the one given in the following lemma.

Lemma 2: If C is a length n, period P single-track Gray code with k-spaced heads, k odd, then the generating track of the code is self-dual.

Proof: Let C be a length n, period P single-track Gray code with k-spaced heads, k odd, and s its generating track. From the proof of Theorem 4 there exists an integer l, for which $\gcd(l, \overline{o}(C)) = 1$, such that

$$W_{i+P/\overline{o}(C)} = \overline{\boldsymbol{E}}^l W_i$$

for each $0 \leq i < P$. Since $\overline{o}(C)$ is even, it follows that l is odd and, therefore,

$$W_{i+P/2} = \overline{\boldsymbol{E}}^{l \cdot \overline{o}(C)/2} W_i = \overline{\boldsymbol{E}}^{\overline{o}(C)/2} W_i = \overline{W_i}$$

and the generating track is self-dual. □

When the generating track of a single-track Gray code is self-dual, many other single-track Gray codes can be generated by selecting any subset of the columns and complementing them. These new single-track Gray codes do not necessarily have k-spaced heads. These are the only known single-track Gray codes which cannot be constructed directly by the use of either Theorems 1 or 2. However, they are, of course, constructed by a straightforward variant of Theorem 2. Moreover, as an immediate consequence from Theorem 4 we can conclude that there is no similar arrangements as in Theorems 1 and 2 of feedback shift-register sequences of order n. It is a very interesting problem to construct single-track Gray codes which do not have k-spaced heads and are not constructed by this variant of Theorem 2. Note, that if n is odd then by complementing every other column of the code generated by Theorem 2 we obtain a code which can be constructed via Theorem 1.

III. Nonexistence Result

Let C be a single-track Gray code of length n and period P. By Lemma 1, there is a theoretical possibility that $P = 2^n$, but then, necessarily, n is a power of 2. The only known code with these parameters is the length 2 period 4 single-track Gray code. In this section we show that there is no other code with such parameters. The proof will consider the track as a sequence of length 2^n and investigate the polynomial of minimal degree which generates this sequence. In the literature, the degree of this polynomial is often called the linear complexity of the sequence. Hence, we first present the necessary definitions for this discussion.

Definition 7: Let $S = [s_0, s_1, \cdots, s_{r-1}]$ be a length r sequence, and let

$$S(x) \triangleq \sum_{i=0}^{r-1} s_i x^i$$

be a polynomial. We say the $S(x)$ is the *associated polynomial* of S, and S is the *associated word* of $S(x)$.

Definition 8: Let S be a length r sequence over GF(q). The *linear complexity* of S is defined as

$$c(S) \triangleq \min\{\deg f(x) \mid f(x) \not\equiv 0,\, f(x) \cdot S(x) \equiv 0 \\ (\bmod x^r - 1)\}.$$

The linear complexity as defined here is the same as the degree of the minimal degree linear recursion which generates the sequence. This is the more common definition as given in [18].

Lemma 3: Let S be a length $r = p^{l_1}$ sequence over GF(q), where $q = p^{l_2}$, p prime. The linear complexity of S is c if and only if

$$(x-1)^{c-1}S(x) \equiv d(1+x+x^2+\cdots+x^{r-1}) \pmod{x^r - 1} \quad (2)$$

for some $d \neq 0$.

Lemma 4 [3, Theorem 2]: Let S be a length $n = 2^m$ binary sequence. S is self-dual if and only if $c(S) = 2^{m-1}+1$.

We will prove now a result which is stronger than the nonexistence result that we actually want to prove.

Theorem 5: There is no ordering of all the 2^n words of length $n = 2^m$, $m \geq 2$, in a list which satisfies all the following requirements.

1) Each two adjacent words have different parity.
2) The list has the single-track property.
3) Each word appears exactly once.

Proof: Let us assume the contrary, i.e., let s be the track of a single-track code in which each n-tuple appears exactly once and each two adjacent words have different parity. Let $s(x)$ be the associated polynomial of s and θ_1 the largest integer for which there exists a polynomial $p_1(x)$ which satisfies

$$s(x) \equiv (x+1)^{\theta_1} p_1(x) \pmod{x^{2^n}+1}. \quad (3)$$

Let $k_0, k_1, \cdots, k_{n-1}$ be the locations of the heads in the list

$$h(x) \triangleq \sum_{i=0}^{n-1} x^{k_i}$$

the *head locator* polynomial of the list, and h the associated length 2^n word of $h(x)$. Let θ_2 be the largest integer for which there exists a polynomial $p_2(x)$ which satisfies

$$h(x) \equiv (x+1)^{\theta_2} p_2(x) \pmod{x^{2^n}+1}. \quad (4)$$

Since $x^{2^n}+1 = (x+1)^{2^n}$ over GF(2), it follows that $0 \leq \theta_1, \theta_2 \leq 2^n - 1$. Since each two adjacent words have different parity it follows that

$$(x+1)h(x)s(x) \equiv 1+x+x^2+\cdots+x^{2^n-1} \pmod{x^{2^n}+1}. \quad (5)$$

Since $(x+1)^{2^n} = x^{2^n}+1$ and

$$(x+1)^{2^n-1} = 1+x+x^2+\cdots+x^{2^n-1} \pmod{x^{2^n}+1}$$

it follows from (2)–(5) that

$$\theta_1 + \theta_2 = 2^n - 2. \quad (6)$$

Equations (2)–(5) also imply that $\theta_1 + 2$ is the linear complexity of h, and $\theta_2 + 2$ is the linear complexity of s. Since each word appears in the list exactly once, it follows that s must be of full cyclic order, and hence

$$\theta_2 \geq 2^{n-1} - 1. \quad (7)$$

If we assume that h is not a full-order word, then

$$\{k_i\}_{i=0}^{n-1} = \{2^{n-1} + k_i\}_{i=0}^{n-1}$$

and the ith word and the $(i+2^{n-1})$th word contain exactly the same components of the generating track s. The all-zero word appears somewhere in the list, and hence it will appear at least twice, which is a contradiction. Thus h is of full-order and, therefore, $\theta_1 \geq 2^{n-1} - 1$.

Self-dual sequences of length 2^n have weight 2^{n-1} and since h has weight n, it follows that h is not self-dual when $2^n \geq 4$, and hence by Lemma 4 the linear complexity of h is not $2^{n-1}+1$. Therefore,

$$\theta_1 \geq 2^{n-1}. \quad (8)$$

Summing (7) and (8) we get that

$$\theta_1 + \theta_2 \geq 2^n - 1$$

in contradiction to (6). Thus no such single-track code with track s exists. □

Corollary 1: There are no single-track Gray codes of length $n \geq 3$ and period 2^n.

As mentioned in Section II, Etzion and Paterson [9] have constructed single-track Gray codes of length $n = 2^m$ and period $2^n - 2n$.

Corollary 2: The single-track Gray codes of length $n = 2^m$ and period $2^n - 2n$ are optimal.

The nonexistence theorem can be generalized in a very interesting way to single-track Gray codes over GF(p), where p is a prime. We discuss nonbinary codes and present this generalization of the nonexistence theorem in Appendix A.

IV. An Iterative Construction

In this section we describe an iterative construction which generates long-period single-track Gray codes. We are given two pairs of disjoint Gray codes, of lengths n and k, of pairwise nonequivalent full-order words. Each pair satisfies a set of properties needed for the construction. The construction itself is made of five stages. The first stage is an iterative generation of a large number of pairwise nonequivalent, full-order words. The second is ordering of the necklaces into many Gray codes. The third stage consists of merging these Gray codes into two sets of Gray codes. In the fourth stage, the Gray codes of each set are concatenated into two cyclic Gray codes which satisfy the properties needed for the construction. The last stage is a simple merging of these two Gray codes into one Gray code.

A. Nonequivalent Necklaces Generation

The first step in generating a long single-track Gray code based on necklaces, is to generate a large set of pairwise nonequivalent full-order words, known also as Lyndon words [1]. This construction should generate the necklaces in such a way that it will be easy to order them into a Gray code. The construction of these pairwise nonequivalent words will be iterative, i.e., given two sets of pairwise nonequivalent full-order words of length n and length k, respectively, we generate a set of pairwise nonequivalent full-order words of length nk. We first partition the set of all binary m-tuples into two sets, those ending in a ZERO and those ending in a ONE, i.e., for each $b \in \{0, 1\}$, we define

$$\mathcal{X}_m^b \triangleq \{[x_0, x_1, \cdots, x_{m-2}, x_{m-1}] \in \{0, 1\}^m | \, x_{m-1} = b\}.$$

Construction 1: For each $b \in \{0, 1\}$, let

$$\mathcal{N}_n^b \triangleq \{S_0^b, S_1^b, \cdots, S_{r_b-1}^b\} \subseteq \mathcal{X}_n^b$$
$$\mathcal{N}_k'^b \triangleq \left\{S_0'^b, S_1'^b, \cdots, S_{r_b'-1}'^b\right\} \subseteq \mathcal{X}_k^b$$

be sets of pairwise nonequivalent, full-order words, such that

$$\mathcal{N}_n^0 \bigcap \bigcup_{i=0}^{n-1} \{E^i S | \, S \in \mathcal{N}_n^1\} = \mathcal{N}_k'^0 \bigcap \bigcup_{i=0}^{k-1} \{E^i S' | \, S' \in \mathcal{N}_k'^1\} = \emptyset.$$

From these sets we generate the following set:

$$\mathcal{N}_{n,k} \triangleq \left\{ \left[X_0, X_1, \cdots, X_{k-2}, S + \sum_{i=0}^{k-2} X_i\right] \middle| \, [b_0, b_1, \cdots, b_{k-1}] \in \mathcal{N}_k'^0 \cup \mathcal{N}_k'^1, \, X_i \in \mathcal{X}_n^{b_i}, \, 0 \le i < k-1, \; S \in \mathcal{N}_n^p, \, p = \sum_{i=0}^{k-1} b_i \right\}.$$

Theorem 6: The set $\mathcal{N}_{n,k}$ of Construction 1 contains pairwise nonequivalent full-order words of length kn.

Proof: Let

$$Y = [y_0, y_1, \cdots, y_{kn-1}]$$

and

$$Z = [z_0, z_1, \cdots, z_{kn-1}]$$

be two words in the defined set $\mathcal{N}_{n,k}$. Let us assume that $\boldsymbol{E}^c Y = Z$ for some $0 \le c < kn$. Now

$$\sum_{j=0}^{k-1} \boldsymbol{E}^{jn} \boldsymbol{E}^c Y = [\boldsymbol{E}^c S_{m_1}, \boldsymbol{E}^c S_{m_1}, \cdots, \boldsymbol{E}^c S_{m_1}]$$
$$\sum_{j=0}^{k-1} \boldsymbol{E}^{jn} Z = [S_{m_2}, S_{m_2}, \cdots, S_{m_2}]$$

where $S_{m_1} \in \mathcal{N}_n^{a_1}$ and $S_{m_2} \in \mathcal{N}_n^{a_2}$, $a_1, a_2 \in \{0, 1\}$.

For $a_1 \ne a_2$, S_{m_1} and S_{m_2} are nonequivalent, and hence $a_1 = a_2$. For $m_1 \ne m_2$, S_{m_1} and S_{m_2} are nonequivalent, and, therefore, $m_1 = m_2$, which implies $S_{m_1} = \boldsymbol{E}^c S_{m_1}$.

S_{m_1} is a full-order word, and hence $n|c$. This implies, that if we look at

$$S'_{m'_1} = [y_{n-1}, y_{2n-1}, \cdots, y_{kn-1}]$$
$$S'_{m'_2} = [z_{n-1}, z_{2n-1}, \cdots, z_{kn-1}]$$

then $\boldsymbol{E}^{c/n} S'_{m'_1} = S'_{m'_2}$. As before, $S'_{m'_1}$ and $S'_{m'_2}$ are nonequivalent full-order words, and hence $k|c/n$ or $kn|c$. Therefore, $Y = Z$ and thus all the words in $N_{n,k}$ are pairwise nonequivalent. □

Construction 1 produces iteratively a large set of pairwise nonequivalent, full-order words. This set is generated in a way which makes it relatively easy to order its necklaces in a cyclic Gray code, provided that the elements of $\mathcal{N}_n^0$, $\mathcal{N}_n^1$, $\mathcal{N}_k'^0$, $\mathcal{N}_k'^1$ can be ordered as cyclic Gray codes.

B. Generation and Merging of Gray Codes

Given a Gray code of length n, we will generate many Gray codes of the same period and length nk, for which all words belong to distinct necklaces. Those Gray codes will be then merged into two sets of Gray codes. The generation of one such short Gray code and the merging of some of these Gray codes will be based on the following two trivial lemmas whose proofs are omitted.

Lemma 5: If the words $S_0, S_1, \cdots, S_{r-1} \in \{0, 1\}^n$ form a cyclic Gray code, then the following words form a cyclic Gray code:

$$\left[X_0, X_1, \cdots, X_{k-2}, S_0 + \sum_{i=0}^{k-2} X_i\right]$$
$$\left[X_0, X_1, \cdots, X_{k-2}, S_1 + \sum_{i=0}^{k-2} X_i\right]$$
$$\vdots$$
$$\left[X_0, X_1, \cdots, X_{k-2}, S_{r-1} + \sum_{i=0}^{k-2} X_i\right]$$

where $X_i \in \{0, 1\}^n$ for each $0 \le i < k-1$.

Lemma 6: Let $X_l \in \{0, 1\}^n$ for each $0 \le l < k-1$ and for some j, $0 \le j < k-1$, let $X'_j \in \{0, 1\}^n$ be a word such that X'_j differs from X_j in exactly the dth coordinate. Furthermore, the necklaces $S_0, S_1, \cdots, S_{r-1} \in \{0, 1\}^n$ form a cyclic Gray code in which, for some i, S_i and S_{i+1} differ in the dth coordinate. Then, the necklaces shown at the top of the following page form a cyclic Gray code in which the last and first pair of necklaces differ in the $(d + jn)$th coordinate.

C. A Set of Properties for the Codes

In order to make an iterative construction of Gray codes based on pairwise nonequivalent full-order words we need our Gray codes to satisfy certain additional properties. One of the important properties concerns the positions in which adjacent words in the code differ.

Definition 9: Let W_1, W_2 be words of length n which differ only in the ith coordinate. We define

$$\Delta(W_1, W_2) \triangleq i.$$

We are now in a position to state the set of properties required for some Gray codes based on distinct necklaces in order to obtain the iterative construction. Let

$$\mathcal{N}_n^0 = S_0, S_1, \cdots, S_{r_0-1}^0$$
$$\mathcal{N}_n^1 = S_0, S_1, \cdots, S_{r_1-1}^1$$
$$\mathcal{N}_k'^0 = S_0'^0, S_1'^1, \cdots, S_{r_0'-1}'^1$$
$$\mathcal{N}_k'^1 = S_0'^1, S_1'^1, \cdots, S_{r_1'-1}'^1$$

$$\begin{gathered}
[X_0, X_1, \cdots, X_j, \cdots, X_{k-2}, S_i + X_0 + X_1 + \cdots + X_j + \cdots + X_{k-2}] \\
[X_0, X_1, \cdots, X_j', \cdots, X_{k-2}, S_{i+1} + X_0 + X_1 + \cdots + X_j' + \cdots + X_{k-2}] \\
\vdots \\
[X_0, X_1, \cdots, X_j', \cdots, X_{k-2}, S_{r-1} + X_0 + X_1 + \cdots + X_j' + \cdots + X_{k-2}] \\
[X_0, X_1, \cdots, X_j', \cdots, X_{k-2}, S_0 + X_0 + X_1 + \cdots + X_j' + \cdots + X_{k-2}] \\
\vdots \\
[X_0, X_1, \cdots, X_j', \cdots, X_{k-2}, S_i + X_0 + X_1 + \cdots + X_j' + \cdots + X_{k-2}] \\
[X_0, X_1, \cdots, X_j, \cdots, X_{k-2}, S_{i+1} + X_0 + X_1 + \cdots + X_j + \cdots + X_{k-2}]
\end{gathered}$$

be cyclic Gray codes such the following properties are satisfied.

(p.1) The sets of necklaces which belong to $\mathcal{N}_n^0$, $\mathcal{N}_n^1$, $\mathcal{N}_k'^0$, $\mathcal{N}_k'^1$, respectively, satisfy the conditions of Construction 1.

(p.2)

- The words $[0^{n-1}1]$, $[0^{n-2}11]$ are adjacent in $\mathcal{N}_n^1$.
- $[0^{k-1}1] \in \mathcal{N}_k'^1$.

(p.3)

- There exist i_0, i_1 such that $S_{i_1}^1$ and $S_{i_0+1}^0$ differ in exactly the last coordinate, and also $S_{i_0}^0$ and $S_{i_1+1}^1$ differ in exactly the last coordinate. We say that i_0 and i_1 are the *bridging indices* of $\mathcal{N}_n^0$ and $\mathcal{N}_n^1$, respectively, and that $S_{i_0}^0$, $S_{i_0+1}^0$, $S_{i_1}^1$, $S_{i_1+1}^1$ are the *bridging words* of their respective codes.
- There exist i_0', i_1' such that $S_{i_1'}'^1$ and $S_{i_0'+1}'^0$ differ in exactly the last coordinate, and also $S_{i_0'}'^0$ and $S_{i_1'+1}'^1$ differ in exactly the last coordinate. We say that i_0' and i_1' are the *bridging indices* of $\mathcal{N}_k'^0$ and $\mathcal{N}_k'^1$, respectively, and that $S_{i_0'}'^0$, $S_{i_0'+1}'^0$, $S_{i_1'}'^1$, $S_{i_1'+1}'^1$ are the *bridging words* of their respective codes.

(p.4)

- Let j be the index for which $\{S_j^1, S_{j+1}^1\} = \{[0^{n-1}1], [0^{n-2}11]\}$, and let i_0 and i_1 be the bridge indices of $\mathcal{N}_n^0$ and $\mathcal{N}_n^1$, respectively, then
$$\begin{aligned}
&\{\Delta(S_l^0, S_{l+1}^0) \,|\, 0 \le l < r_0,\ l \ne i_0\} \\
&\quad = \{\Delta(S_l^1, S_{l+1}^1) \,|\, 0 \le l < r_1,\ l \ne i_1,\ l \ne j\} \\
&\quad = \{0, 1, 2, \cdots, n-2\}.
\end{aligned}$$
- Let i_0' and i_1' be the bridge indices of $\mathcal{N}_k'^0$ and $\mathcal{N}_k'^1$, respectively, then
$$\begin{aligned}
&\{\Delta(S_l'^0, S_{l+1}'^0) \,|\, 0 \le l < r_0',\ l \ne i_0'\} \\
&\quad = \{\Delta(S_l'^1, S_{l+1}'^1) \,|\, 0 \le l < r_1',\ l \ne i_1'\} \\
&\quad = \{0, 1, 2, \cdots, k-2\}.
\end{aligned}$$

For $k = n$, we say that $\mathcal{N}_n^0$ and $\mathcal{N}_n^1$ satisfy property **(p.i),** $1 \le \mathbf{i} \le 4$, if $\mathcal{N}_n^0$, $\mathcal{N}_n^1$, $\mathcal{N}_k'^0$, $\mathcal{N}_k'^1$, satisfy **(p.i)**.

D. Generation of Short Gray Codes

We are given the four cyclic Gray codes $\mathcal{N}_n^0$, $\mathcal{N}_n^1$, $\mathcal{N}_k'^0$, $\mathcal{N}_k'^1$ based on pairwise nonequivalent full-order words of period n and k, respectively. We partition the necklaces generated by Construction 1 into disjoint Gray codes, where each Gray code corresponds to a necklace $B = [b_0, b_1, \cdots, b_{k-1}] \in \mathcal{N}_k'^b$ ($b = b_{k-1}$). Let $p \triangleq \sum_{i=0}^{k-1} b_i$ be the parity of B. For any choice of $W_i \in \mathcal{X}_n^{b_i}$, for each $0 \le i < k-1$, we use Lemma 5 to construct a cyclic Gray code with the words

$$\left[W_0, W_1, \cdots, W_{k-2}, S_j^p + \sum_{i=0}^{k-2} W_i\right] \qquad (0 \le j < r_p).$$

This code is of length kn and period r_p and will be denoted by

$$\mathcal{C}(B, [W_0, W_1, \cdots, W_{k-2}]).$$

By Theorem 6, all the words in this code are pairwise nonequivalent, full-order words.

For the given B we continue and merge all its cyclic Gray codes into one Gray code. There are $2^{(n-1)(k-1)}$ Gray codes which are related to B and we want to order them in such a way that it will be simple to merge them in the given order. The merging will be performed as done in Lemma 6. To apply this lemma we need two Gray codes

$$\mathcal{C}(B, [W_0, W_1, \cdots, W_j, \cdots, W_{k-2}])$$

and

$$\mathcal{C}(B, [W_0, W_1, \cdots, W_j', \cdots, W_{k-2}])$$

such that W_j and W_j' differ in exactly one coordinate. This coordinate is not the last one since the last coordinate is predetermined by B. Thus we should order the $2^{(n-1)(k-1)}$ sequences of the form

$$W_0, W_1, \cdots, W_{k-2}$$

in such a way that any two differ in exactly one coordinate. This is a Gray code ordering and most (and usually all) Gray codes are good for this purpose. But, for simplicity of construction we will choose the reflected Gray code, which was introduced in Section I, and in the appropriate positions we will plug in the predetermined values of B. We call this code, the *merging Gray code* and we require another property from the merging Gray code (and this property can be removed if we request some more properties from the four Gray codes of length n and k, which can be easily obtained). As said in the Introduction, half of the changes in a reflected Gray code are in one specified coordinate (usually the last one). We require that this coordinate will not be congruent modulo n to $\Delta(S^1_{i_1}, S^1_{i_1+1})$, or $\Delta(S^0_{i_0}, S^0_{i_0+1})$, or $n-2$. This can be done easily by an appropriate permutation on the code coordinates. After this is done in the generated merging Gray code no two consecutive changes are in a coordinate congruent to $\Delta(S^1_{i_1}, S^1_{i_1+1})$, or $\Delta(S^0_{i_0}, S^0_{i_0+1})$, or $n-2$, modulo n. Our Gray code of length $n(k-1)$ and period $2^{(n-1)(k-1)}$ will be denoted by

$$\mathcal{X}^B \triangleq X_0, X_1, \cdots, X^B_{2^{(n-1)(k-1)}-1}.$$

We note that in $\mathcal{X}^B$

$$\left\{\Delta\left(X^B_i, X^B_{i+1}\right)\right\}_{i=0}^{2^{(n-1)(k-1)}-1} = \{0, 1, 2, \cdots, n(k-1)-1\}\setminus \bigcup_{i=1}^{k-1} \{ni-1\}.$$

We are now in a position to merge all the Gray codes which are related to B. During this merging we make sure that each two adjacent words of length nk constructed from either bridging words or the words $[0^{n-1}1]$ and $[0^{n-2}11]$ will remain adjacent. The merging starts with the code $\mathcal{C}(B, X^B_0)$ and the code $\mathcal{C}(B, X^B_1)$. Since X^B_0 and X^B_1 differ in exactly one coordinate, say, the dth coordinate, $(0 \le d < (k-1)n$, $d \not\equiv n-1 \pmod{n})$ then it is possible to merge the latter into the former using **(p.4)** and Lemma 6. The resulting code will be called the *main code*. In a typical step of the merging we have a main code obtained by merging the following Gray codes:

$$\begin{array}{c}\mathcal{C}(B, X^B_0)\\ \mathcal{C}(B, X^B_1)\\ \vdots\\ \mathcal{C}(B, X^B_l)\end{array}$$

and we merge to it the Gray code $\mathcal{C}(B, X^B_{l+1})$. Let

$$d_1 \triangleq \Delta\left(X^B_{l-1}, X^B_l\right)$$
$$d_2 \triangleq \Delta\left(X^B_l, X^B_{l+1}\right).$$

$\mathcal{X}^B$ was chosen in a way that if $d_1 \equiv d_2 \pmod{n}$ then $d_2 \not\equiv \Delta(S^1_{i_1}, S^1_{i_1+1}), d_2 \not\equiv \Delta(S^0_{i_0}, S^0_{i_0+1})$, and $d_2 \not\equiv n-2 \pmod{n}$. Hence, in this case and also when $d_1 \not\equiv d_2 \pmod{n}$, by **(p.4)** and Lemma 6 there is a pair of adjacent words in $\mathcal{C}(B, X^B_l)$, originated from a pair of adjacent words in $\mathcal{N}^p_n$, which are not the bridging words or the words $[0^{n-1}1]$, $[0^{n-2}11]$. Therefore, $\mathcal{C}(B, X^B_{l+1})$ can be merged by Lemma 6. This merging process ends when all the Gray codes

$$\begin{array}{c}\mathcal{C}(B, X^B_0)\\ \mathcal{C}(B, X^B_1)\\ \vdots\\ \mathcal{C}(B, X^B_{2^{(n-1)(k-1)}-1})\end{array}$$

are merged together. The resulting code is called $\mathcal{C}(B)$.

Lemma 7: For each $B = [b_0, b_1, \cdots, b_{k-1}] \in \mathcal{N}'^0_k \cup \mathcal{N}'^1_k$, $p \triangleq \sum_{i=0}^{k-1} b_i$, the code $\mathcal{C}(B) = Y_0, Y_1, \cdots, Y_{P-1}$ is a cyclic Gray code of length kn and period $P = 2^{(k-1)(n-1)} r_p$ which satisfies

$$\{\Delta(Y_i, Y_{i+1}) |\ 0 \le i < P\} = \{0, 1 \cdots, kn-1\} \setminus \bigcup_{i=1}^{k} \{ni-1\}.$$

Proof: It is obvious that $\mathcal{C}(B)$ is of length kn, and since we merged $2^{(k-1)(n-1)}$ codes of period r_p, it follows that the period of the resulting code is $P = 2^{(k-1)(n-1)} r_p$. By Lemma 6, the resulting code is a cyclic Gray code. Finally, since

$$\left\{\Delta\left(X^B_i, X^B_{i+1}\right)\right\}_{i=0}^{2^{(n-1)(k-1)}} = \{0, 1, 2, \cdots, n(k-1)-1\}\setminus \bigcup_{i=1}^{k-1} \{ni-1\},$$

it follows by Lemma 6, and **(p.4)** that

$$\{\Delta(Y_i, Y_{i+1}) |\ 0 \le i < P\} = \{0, 1 \cdots, kn-1\} \setminus \bigcup_{i=1}^{k} \{ni-1\}. \quad \square$$

E. Concatenation of the Short Gray Codes

Now we have a set of $r'_0 + r'_1$ cyclic Gray codes, each corresponds to a different member of $\mathcal{N}'^0_k \bigcup \mathcal{N}'^1_k$. Recall that the bridging indices of $\mathcal{N}^0_n$, $\mathcal{N}^1_n$, $\mathcal{N}'^0_k$, $\mathcal{N}'^1_k$ are i_0, i_1, i'_0, i'_1, respectively. Let $V_0, V_1, \cdots, V_{k-2} \in \{0, 1\}^{n-1}$ be $k-1$ words of length $n-1$ chosen arbitrarily. For each

$$B = [b_0, b_1, \cdots, b_{k-1}] \in \mathcal{N}'^0_k \cup \mathcal{N}'^1_k$$

and

$$p \triangleq \sum_{i=0}^{k-1} b_i$$

we define $Z_i = [V_i, b_i]$ for each $0 \le i < k-1$. We cyclically shift the rows of the cyclic Gray code $C(B)$, in such a way that the first word will be

$$\left[Z_0, Z_1, \cdots, Z_{k-2}, S^p_{i_p+1} + \sum_{i=0}^{k-2} Z_i\right]$$

and the last word will, therefore, be

$$\left[Z_0, Z_1, \cdots, Z_{k-2}, S^p_{i_p} + \sum_{i=0}^{k-2} Z_i\right].$$

We look at the following two concatenations of our cyclic Gray codes:

$$\begin{aligned}\mathcal{N}^0_{nk} =& \mathcal{C}(S'^0_{i'_0+1}), \mathcal{C}(S'^0_{i'_0+2}), \cdots, \mathcal{C}(S'^0_{r'_0-1}), \mathcal{C}(S'^0_0),\\ & \cdots, \mathcal{C}(S'^0_{i'_0})\\ \mathcal{N}^1_{nk} =& \mathcal{C}(S'^1_{i'_1+1}), \mathcal{C}(S'^1_{i'_1+2}), \cdots, \mathcal{C}(S'^1_{r'_1-1}), \mathcal{C}(S'^1_0),\\ & \cdots, \mathcal{C}(S'^1_{i'_1}).\end{aligned}$$

In the rest of this subsection and in the next subsection we will prove that $\mathcal{N}^0$ and $\mathcal{N}^1$ is a pair of cyclic Gray codes of pairwise nonequivalent full-order words, which satisfies properties **(p.1)–(p.4)** and thus can be used for further iterations of the construction.

Lemma 8: $\mathcal{N}_{nk}^0$ and $\mathcal{N}_{nk}^1$ are cyclic Gray codes of length kn and period

$$2^{(n-1)(k-1)-1}(r_0+r_1)r'_0 \text{ and } 2^{(n-1)(k-1)-1}(r_0+r_1)r'_1$$

respectively. Furthermore, $\mathcal{N}_{nk}^0$ and $\mathcal{N}_{nk}^1$ contain pairwise nonequivalent full-order words.

Proof: All the necklaces of $\mathcal{N}_{nk}^0$ and $\mathcal{N}_{nk}^1$ were produced as in Construction 1 and hence, by Theorem 6, all the words are pairwise nonequivalent full-order and of length nk.

For a given

$$B=[b_0, b_1, \cdots, b_{k-1}]$$

and

$$W_0, W_1, \cdots, W_j, \cdots, W_{k-2},$$

clearly

$$\mathcal{C}(B, [W_0, W_1, \cdots, W_j, \cdots, W_{k-2}])$$

has period r_p, where p is the parity of B. $\mathcal{C}(B)$ was constructed by merging $2^{(n-1)(k-1)}$ Gray codes of the form

$$\mathcal{C}(B, [W_0, W_1, \cdots, W_j, \cdots, W_{k-2}])$$

and hence its period is $2^{(n-1)(k-1)}r_p$. Since S'^1_j and S'^1_{j+1} have different parity, it follows that $\mathcal{C}(S'^1_j)$ and $\mathcal{C}(S'^1_{j+1})$ together have $2^{(n-1)(k-1)}(r_0+r_1)$ necklaces, and $\mathcal{N}_{nk}^b$ has $2^{(n-1)(k-1)-1}(r_0+r_1)r'_b$ words. To complete the proof we have to show that $\mathcal{N}_{nk}^b$ is a cyclic Gray code. As said before the last word in $\mathcal{C}(S'^b_j)$ is

$$\left[Z_0,\, Z_1,\, \cdots,\, Z_{k-2},\, S^p_{i_p}+\sum_{i=0}^{k-2} Z_i\right]$$

where p is the parity of S'^b_j, and the first word in $\mathcal{N}(S'^b_{j+1})$ is

$$\left[Z'_0,\, Z'_1,\, \cdots,\, Z'_{k-2},\, S^{\overline{p}}_{i_{\overline{p}+1}}+\sum_{i=0}^{k-2} Z'_i\right].$$

Clearly, these two words differ in exactly one coordinate. If S'^b_j and S'^b_{j+1} differ in the dth coordinate, $0 \le d < k-1$, then for each $0 \le j < k-1$, $j \ne d$, $Z_j = Z'_j$, and Z_d and Z'_d differ in the last coordinate. Since by **(p.3)** $S^p_{i_p}$ and $S^{\overline{p}}_{i_{\overline{p}}+1}$ differ in exactly the last coordinate, it follows that the last word of $\mathcal{C}(S'^b_j)$ and the first word of $\mathcal{C}(S'^b_{j+1})$ differ in exactly the $(n(d+1)-1)$th coordinate. Thus $\mathcal{N}_{nk}^b$ is a cyclic Gray code of length nk and period $2^{(n-1)(k-1)-1}(r_0+r_1)r'_b$. □

F. Properties of the Generated Gray Codes

In this section we will prove that the generated Gray codes $\mathcal{N}_{nk}^0$ and $\mathcal{N}_{nk}^1$ satisfy **(p.1)–(p.4)** and, therefore, can be used for further iterations of the construction. The first lemma is an immediate consequence of Lemma 8.

Lemma 9: $\mathcal{N}_{nk}^0$ and $\mathcal{N}_{nk}^1$ satisfy **(p.1)**.

Lemma 10: The words $[0^{nk-1}1]$ and $[0^{nk-2}11]$ are adjacent in $\mathcal{N}_{nk}^1$.

Proof: By **(p.2)** we have that $[0^{k-1}1] \in \mathcal{N}'^1_k$ and $[0^{n-1}1]$ and $[0^{n-2}11]$ are adjacent in $\mathcal{N}_n^1$. Therefore, the words $[0^{nk-1}1]$ and $[0^{nk-2}11]$ are adjacent in $\mathcal{C}([0^{k-1}1], [0^{(k-1)n}])$. Since during the merging process we did not separate these words, it follows that they are also adjacent in $\mathcal{C}([0^{k-1}1])$. To complete the proof we have to show that these two words were not separated during the concatenation. This is an immediate consequence from the fact that $[0^{n-1}1]$ is not a bridging word since $[0^n]$ is not a full-order word. □

Lemma 11: $\mathcal{N}_{nk}^0, \mathcal{N}_{nk}^1$ satisfy **(p.3)**.

Proof: Observe that the last word of $\mathcal{N}_{nk}^1$, which is also the last word of $\mathcal{C}(S'^1_{i'_1})$ is

$$\left[Z_0,\, Z_1,\, \cdots,\, Z_{k-2},\, S^p_{i_p}+\sum_{i=0}^{k-2} Z_i\right]$$

where p is the parity of $S'^1_{i'_1}$. The first word of $\mathcal{N}_{nk}^0$, which is also the first word of $\mathcal{C}(S'^0_{i'_0+1})$ is

$$\left[Z_0,\, Z_1,\, \cdots,\, Z_{k-2},\, S^{\overline{p}}_{i_{\overline{p}+1}}+\sum_{i=0}^{k-2} Z_i\right]$$

where clearly $\overline{p}$ is the parity of $S'^0_{i'_0+1}$. Since $S^p_{i_p}$ and $S^{\overline{p}}_{i_{\overline{p}}+1}$ differ in exactly the last coordinate, it follows that these two words differ exactly in the last coordinate. Similarly, the first word of $\mathcal{N}_{nk}^1$ and the last word of $\mathcal{N}_{nk}^0$ differ in exactly the last coordinate. Therefore, these four words can serve as bridging words of $\mathcal{N}_{nk}^0$ and $\mathcal{N}_{nk}^1$. □

Lemma 12: Let $\mathcal{N}_{nk}^b = S_0^{*b}, S_1^{*b}, \cdots, S_{P_b-1}^{*b}$, j^* be the index such that

$$\{S_j^{*1}, S_{j+1}^{*1}\} = \{[0^{nk-1}1], [0^{nk-2}11]\}$$

and i_0^* and i_1^* be the bridging indices of $\mathcal{N}_{nk}^0$ and $\mathcal{N}_{nk}^1$, respectively. Then

$$\begin{aligned}&\left\{\Delta\left(S_l^{*0}, S_{l+1}^{*0}\right) \middle|\, 0 \le l < r_0^*,\, l \ne i_0^*\right\}\\ &\quad = \left\{\Delta\left(S_l^{*1}, S_{l+1}^{*1}\right) \middle|\, 0 \le l < r_1^*,\, l \ne i_1^*,\, l \ne j^*\right\}\\ &\quad = \{0,\, 1,\, 2,\, \cdots,\, nk-2\}.\end{aligned}$$

Proof: If $B \in \mathcal{N}'^b_k$, then by Lemma 7

$$\{\Delta(Y_i, Y_{i+1}) |\, 0 \le i < P\} = \{0, 1 \cdots, kn-1\} \setminus \bigcup_{i=1}^{k} \{in-1\}$$

where $\mathcal{C}(B) = Y_0, Y_1, \cdots, Y_{P-1}$. By the proof of Lemma 8 we obtain the changes in all positions which are congruent to $n-1$ modulo n in the concatenation of the short Gray codes, and thus by taking into consideration **(p.3)** for $\mathcal{N}'^0_k$ and $\mathcal{N}'^1_k$, and the fact that one change in a coordinate implies at least two changes in the same coordinate we have

$$\left\{\Delta\left(S_l^{*b}, S_{l+1}^{*b}\right) \middle|\, 0 \le l < r_b^*,\, l \ne i_b^*,\, l \ne j^*\right\} = \{0,\, 1,\, 2,\, \cdots,\, nk-2\}. \quad □$$

In Lemmas 9–12, we have proved that the pair of codes $\mathcal{N}_{nk}^0$, $\mathcal{N}_{nk}^1$ satisfy properties **(p.1)–(p.4)**. Thus we can use this pair of codes for another iteration of the construction.

G. Optimality of the Code

Lemma 13: Concatenating the two codes given by the construction

$$\mathcal{C}_{nk} \triangleq \mathcal{N}_{nk}^0, \mathcal{N}_{nk}^1$$

produces a Gray code of pairwise nonequivalent, full-order words of length nk and period $2^{(k-1)(n-1)-1}(r_0+r_1)(r_0'+r_1')$ which satisfies the conditions of Theorem 1.

Proof: By Lemmas 8 and 11, $\mathcal{C}_{nk}$ is a cyclic Gray code of pairwise nonequivalent full-order words of the required parameters. In addition, by Lemma 10, the words $[0^{nk-1}1]$, $[0^{nk-2}11]$ are adjacent in the code. The code can be cyclically shifted so they become the first and last words. Since $[0^{nk-2}11]$ and $\boldsymbol{E}[0^{nk-1}1]$ differ in exactly one coordinate, the conditions of Theorem 1 are satisfied. □

The code of Lemma 13 can be used in Theorem 1 to produce a single-track Gray code of length nk and period

$$2^{(k-1)(n-1)-1}(r_0+r_1)(r_0'+r_1')nk.$$

In order to use the construction, we need seed-codes which satisfy properties **(p.1)–(p.4)**. Such seed-codes may exist only for $n \geq 9$. A simple computer search has found such seed-codes, which contain all full-period words, for length 9–13. The seed-codes for $n = 9, 10$, and 11, are presented in Appendix B.

Example 1: Let $n = k = p$ be a prime for which $r_0 + r_1 = (2^p - 2)/p$. We conjecture that this assumption holds for all primes greater than 9 and we know it holds for $p = 11$ and $p = 13$. We obtain a code of length p^2 and period

$$2^{(p-1)(p-1)-1}(2^p-2)(2^p-2)p^2 = 2^{p^2-2p+2}(2^{p-1}-1)^2.$$

Applying the construction iteratively we obtain a code of length p^i and period $2^{p^i-i\cdot p+i}(2^{p-1}-1)^i$. The ratio between the period and the total number of words of length p^i is $(2^{p-1}-1/2^{p-1})^i$.

If we assume that

$$r_0 + r_1 = (2^n - c_n)/n$$

and

$$r_0' + r_1' = (2^k - c_k)/k$$

then, by Lemma 13, one iteration of the construction gives a single-track Gray code of length nk and period

$$P^* = 2^{nk}\Big(1 - c_k 2^{-k} - c_n 2^{-n} + c_k c_n 2^{-(n+k)}\Big).$$

If we further assume that

$$\lim_{n\to\infty} \frac{c_n}{2^n} = 0 \qquad \lim_{k\to\infty} \frac{c_k}{2^k} = 0 \tag{9}$$

then the period P^* asymptotically reaches the upper bound of Lemma 1

$$\lim_{n,\,k\to\infty} P^* = 2^{nk}.$$

When $P^* = 2^{nk} - c_{nk}$ we have that

$$c_{nk} = 2^{nk}(c_k 2^{-k} + c_n 2^{-n} - c_k c_n 2^{-(n+k)}).$$

Under assumption (9), we get, again, that

$$\lim_{n,\,k\to\infty} \frac{c_{nk}}{2^{nk}} = 0$$

which means that the family of codes generated by any number of iterations of the construction is still asymptotically optimal. Of course, as said before, one needs an infinite family of optimal seed-codes to make the resulting sequence of codes also optimal. If we start with "good" codes which are not optimal we obtain codes which are usually better than the best known codes.

H. Generalization

As mentioned before, seed-codes for our construction exist only for length $n \geq 9$. This fact limits the list of lengths for which we can obtain good single-track Gray codes by our construction. We can overcome this limitation by weakening the requirements induced by the properties **(p.1)–(p.4)**. Let

$$\begin{aligned}\mathcal{N}_n^0 &= S_0^0, S_1^0, \cdots, S_{r_0-1}^0\\ \mathcal{N}_n^1 &= S_0^1, S_1^1, \cdots, S_{r_1-1}^1\\ \mathcal{N}_k' &= S_0', S_1', \cdots, S_{r'-1}'\end{aligned}$$

be cyclic Gray codes, such that the following properties hold.

(q.1) The sets of sequences which belong to $\mathcal{N}_n^0, \mathcal{N}_n^1$ satisfy the conditions of Construction 1, and $\mathcal{N}_k'$ contains pairwise nonequivalent, full-order words.

(q.2)
- The words $[0^{n-1}1]$, $[0^{n-2}11]$ are adjacent in $\mathcal{N}_n^1$.
- $[0^{k-1}1] \in \mathcal{N}_k'$

(q.3) There exist i_0, i_1 such that $S_{i_1}^1$ and $S_{i_0+1}^0$ differ in exactly the last coordinate, and also $S_{i_0}^0$ and $S_{i_1+1}^1$ differ in exactly the last coordinate. We say that i_0 and i_1 are the *bridging indices* of $\mathcal{N}_n^0$ and $\mathcal{N}_n^1$, respectively, and that $S_{i_0}^0$, $S_{i_0+1}^0$, $S_{i_1}^1$, $S_{i_1+1}^1$ are the *bridging words* of their respective codes.

(q.4) Let j be the index for which

$$\{S_j^1, S_{j+1}^1\} = \{[0^{n-1}1], [0^{n-2}11]\}$$

and let i_0 and i_1 be the bridging indices of $\mathcal{N}_n^0$ and $\mathcal{N}_n^1$, respectively, then

$$\begin{aligned}&\{\Delta(S_l^0, S_{l+1}^0) \,|\, 0 \leq l < r_0,\ l \neq i_0\}\\ &\quad = \{\Delta(S_l^1, S_{l+1}^1) \,|\, 0 \leq l < r_1,\ l \neq i_1,\ l \neq j\}\\ &\quad = \{0, 1, 2, \cdots, n-2\}.\end{aligned}$$

Unlike our first construction, this one is not symmetric relative to the parameters n and k of the seed-codes. Therefore, we say that $\mathcal{N}_n^0$, $\mathcal{N}_n^1$ are the *multiplied codes* and $\mathcal{N}_k'$ is the *multiplier code*. The construction process itself is very similar to our first construction. We start by constructing for each $B \in \mathcal{N}_k'$, the code $\mathcal{C}(B)$. As before, we concatenate the codes to get the main code

$$\mathcal{N}_{nk}' \triangleq \mathcal{C}(S_0'), \mathcal{C}(S_1'), \mathcal{C}(S_2'), \cdots, \mathcal{C}(S_{r'-1}').$$

This code contains pairwise nonequivalent full-order words of length nk and satisfies all the properties of a multiplier code. Using Theorem 1 we can obtain a length nk, period

$$2^{(n-1)(k-1)-1}(r_0+r_1)r'nk$$

single-track Gray code, when $k>3$. If $k=2$ then the only word of length 2 used is [01] and we use only $\mathcal{N}_1$. In this case, the construction coincides with the first construction of [9] and we obtain a length $2n$, period $2^n r_1 n$ single-track Gray code. Unlike our first construction, this construction has multiplier seed-codes for length $k\geq 3$ and they are given in Appendix C.

Example 2: For $n=9$ and $k=7$ we obtain a code of length 63 and period $2^{8\cdot 6-1}56\cdot 18\cdot 9\cdot 7=3969\cdot 2^{51}=0.969\cdot 2^{63}$ compared to a code of the same length and period $0.435\cdot 2^{63}$ obtained in [9].

APPENDIX A

We discuss the generalization of Gray codes over nonbinary alphabets. Let $\mathcal{Z}_a$, $a\geq 2$ be the group of residues $\{0, 1, \cdots, a-1\}$ modulo a, and $\mathcal{Z}_a^n$ the set of a^n n-tuples over $\mathcal{Z}_a$.

Definition 10: For

$$X=[x_0, x_1, \cdots, x_{n-1}]$$
$$Y=[y_0, y_1, \cdots, y_{n-1}]\in\mathcal{Z}_a^n.$$

We define

$$d_m(X, Y)=\sum_{i=0}^{n-1}(y_i-x_i)$$

where the subtraction is done in $\mathcal{Z}_a$ and the addition is an integer addition.

Definition 11: A *length n period P Gray code over $\mathcal{Z}_a$* is an ordered list of P distinct length n words over $\mathcal{Z}_a$

$$W_0, W_1, \cdots, W_{P-1}$$

such that for each $0\leq i<P-1$, W_i and W_{i+1} differ in exactly one coordinate and $d_m(W_i, W_{i+1})=d$, for a given $d\in\mathcal{Z}_a$. If W_{P-1} and W_0 satisfy this condition, we say that the code is *cyclic*.

Single-track Gray codes are cyclic Gray codes which have the single-track property. A single-track Gray code over $\mathcal{Z}_a$ is equivalent to a single-track Gray code over $\mathcal{Z}_{a/\gcd(a, d)}$. For this reason we only consider the case where $\gcd(a, d)=1$. The following lemma is a straightforward generalization of its binary equivalent.

Lemma 14: If C is a length n, period P single-track Gray code over $\mathcal{Z}_a$, then $na|P$ and $na\leq P\leq a^n$.

All the results regarding single-track Gray codes with k-spaced heads can be easily generalized in a very natural way. The nonexistence theorem can be proved for certain cases, with an interesting generalization of the proof.

Theorem 7: Except for $p=2$ and $m=1$, there is no ordering of all the p^n words of length $n=p^m$ over GF(p), where $m\geq 1$ and p is a prime, in a list which satisfies all the following requirements.

1) There exists a nonzero constant $d\in$ GF(p), such that for any two consecutive words in the list W_i and W_{i+1} we have $d_m(W_{i+1}, W_i)=d$, $0\leq i\leq p^n-1$.
2) The list has the single-track property.
3) Each word appears exactly once.

Proof: Let us assume the contrary, i.e., that such a code with a track s exists. Let $s(x)$ be the associated polynomial of s, and θ_1 be the largest integer such that there exists a polynomial $p_1(x)$ which satisfies

$$s(x)\equiv(x-1)^{\theta_1}p_1(x)\pmod{x^{p^n}-1}.$$

Let $k_0, k_1, \cdots, k_{n-1}$ be the locations of the heads in the list

$$h(x)\triangleq\sum_{i=0}^{n-1}x^{k_i}$$

the *head locator* polynomial of the list, and h the associated length p^n word of $h(x)$. Let θ_2 be the largest integer for which there exists a polynomial $p_2(x)$ which satisfies,

$$h(x)\equiv(x-1)^{\theta_2}p_2(x)\pmod{x^{p^n}-1}.$$

$x^{p^n}-1=(x-1)^{p^n}$ over GF(p) and hence $0\leq\theta_1, \theta_2\leq p^n-1$. Since the distance between any two adjacent words is d, it follows that

$$\begin{aligned}&(x-1)h(x)s(x)\\&\quad\equiv d\Big(1+x+x^2+\cdots+x^{p^n-1}\Big)\pmod{x^{p^n}-1}\end{aligned}\tag{10}$$

and, therefore,

$$\theta_1+\theta_2=p^n-2.\tag{11}$$

Equation (10) also implies that θ_1+2 is the linear complexity of h, and θ_2+2 is the linear complexity of s. Since each word appears in the list exactly once, s must be of full cyclic order, and hence

$$\theta_2\geq p^{n-1}-1.\tag{12}$$

In order to restrict the linear complexity of h, we notice that

$$\sum_{i=0}^{p-1}x^{i\cdot p^{n-1}}=(x-1)^{(p-1)p^{n-1}}.$$

Now, let us assume that $\theta_1<(p-1)p^{n-1}-1$, i.e.,

$$h(x)\sum_{i=0}^{p-1}x^{i\cdot p^{n-1}}\equiv 0\pmod{x^{p^n}-1}.$$

Since h contains only zeros and ones, and the calculations are performed over GF(p), it follows that h has the following form:

$$h=[\underbrace{AA\cdots A}_{p}],\qquad A\in\text{GF}^{p^{n-1}}(p).$$

This means that

$$\{k_i\}_{i=0}^{n-1} = \{p^{n-1} + k_i\}_{i=0}^{n-1}$$

and then, the ith word and the $(i + p^{n-1})$th word contain exactly the same components of the generating track s. Since the all-zero word appears somewhere in the list, it will appear at least twice, which is a contradiction. Therefore,

$$\theta_1 \geq (p-1)p^{n-1} - 1.$$

The linear complexity of h cannot be $(p-1)p^{n-1} + 1$, otherwise,

$$h(x) \sum_{i=0}^{p-1} x^{i \cdot p^{n-1}} \equiv \alpha \cdot \sum_{i=0}^{p^n - 1} x^i \pmod{x^{p^n} - 1}$$

for some $\alpha \in \mathrm{GF}(p)$, $\alpha \neq 0$. The polynomial on the right has p^n nonzero components. $h(x)$ has exactly p^m nonzero components, and hence, the left side has at most p^{m+1} nonzero components. Thus

$$p^{m+1} \geq p^{p^m - 1}$$

but this equation can hold only if $p = 2$ and $m = 1$. Therefore,

$$\theta_1 \geq (p-1)p^{n-1}. \tag{13}$$

Summing (12) and (13) we get that

$$\theta_1 + \theta_2 \geq p^n - 1$$

and this contradicts (11). □

Corollary 3: There are no single-track Gray codes over $\mathrm{GF}(p)$, p prime, of length $n \geq 2$ and period p^n, except for the trivial binary code of length 2 and period 4.

Appendix B

In this appendix we present the seed-codes for $9 \leq n \leq 11$ as shown in at the bottom of this and the top of the following page.

[010001010]	[010001000]	[011001000]	[011011000]	[011010000]
[011110000]	[011111000]	[111111000]	[111111100]	[111101100]
[111101110]	[111111110]	[111111010]	[101111010]	[001111010]
[011111010]	[011011010]	[011011110]	[011010110]	[010010110]
[010110110]	[010111110]	[010011110]	[010001110]	[110001110]
[110001100]	[110001000]	[110001010]	[110001011]	[110001001]
[110000001]	[110100001]	[010100001]	[010000001]	[000000001]
[000000011]	[000001011]	[000001001]	[100001001]	[101001001]
[101001011]	[100001011]	[100101011]	[100101001]	[100111001]
[110111001]	[110101001]	[010101001]	[010101101]	[011101101]
[111101101]	[110101101]	[110001101]	[010001101]	[010001001]
[010001011]				

Seed-codes for $n = 9$

[0110101110]	[0111101110]	[0111101010]	[0101101010]	[0101111010]
[0101111110]	[0101110110]	[0001110110]	[0011110110]	[0011111110]
[0011111100]	[0011110100]	[0111110100]	[0111010100]	[0101010100]
[0101010110]	[0101000110]	[0101100110]	[1101100110]	[1101100010]
[1101110010]	[1101111010]	[1100111010]	[0100111010]	[0100110010]
[0101110010]	[0111110010]	[0111100010]	[0111100000]	[0111100100]
[0111100110]	[0110100110]	[0110100010]	[0110110010]	[0010110010]
[0010100010]	[0010000010]	[0110000010]	[1110000010]	[1100000010]
[1100001010]	[1100001000]	[1110001000]	[1110001100]	[1100001100]
[1000001100]	[1000011100]	[1000011000]	[1010011000]	[1010010000]
[1010010010]	[1010000010]	[1010000110]	[1010100110]	[1010101110]
[0010101110]	[0010101111]	[0010100111]	[0110100111]	[1110100111]
[1110110111]	[1110110011]	[1110111011]	[1110101011]	[1111101011]
[1111101111]	[1111001111]	[1111001101]	[1110001101]	[0110001101]
[0110001001]	[0010001001]	[0000001001]	[0100001001]	[0100000001]
[0000000001]	[0000000011]	[1000000011]	[1010000011]	[1010000001]
[1010010001]	[1011010001]	[1011000001]	[1111000001]	[1111000101]
[1101000101]	[1101001101]	[1101011101]	[1100011101]	[1100001101]
[1100001001]	[1100001011]	[0100001011]	[0100101011]	[0110101011]
[0110101111]				

Seed-codes for $n = 10$

[10101110000] [10101010000] [10001010000] [11001010000] [11001110000]
[11101110000] [11101010000] [11111010000] [11011010000] [11011110000]
[11011100000] [11010100000] [11110100000] [10110100000] [10100100000]
[10101100000] [11101100000] [11101000000] [10101000000] [10111000000]
[10111100000] [00111100000] [00111110000] [00111111000] [01111111000]
[11111111000] [11111111100] [11111111110] [11011111110] [11011011110]
[11111011110] [10111011110] [10111111110] [10101111110] [10101101110]
[10101101010] [10111101010] [10111101000] [10111111000] [10111111100]
[10011111100] [10010111100] [10010111110] [10010101110] [10010101010]
[10010111010] [10010011010] [10010011110] [10010010110] [10010010100]
[10010011100] [10110011100] [11110011100] [11010011100] [11010111100]
[11010101100] [11011101100] [11011001100] [11111001100] [11101001100]
[11101011100] [11101010100] [11101110100] [11101111100] [11101101100]
[11111101100] [11111101000] [11111001000] [11101001000] [11101101000]
[11001101000] [11001001000] [11011001000] [11011101000] [11010101000]
[11110101000] [11110111000] [10110111000] [10110011000] [10100011000]
[10100111000] [10100101000] [10110101000] [10010101000] [10010111000]
[10010011000] [10011011000] [10011111000] [10011110000] [10011010000]
[10111010000] [10111110000] [10111110001] [10011110001] [10001110001]
[10001111001] [10001111101] [11001111101] [11001101101] [11001101111]
[01001101111] [01001101011] [01001111011] [01001111111] [01001111101]
[01001101101] [01101101101] [01111101101] [01011101101] [11011101101]
[11011101111] [11011101011] [01011101011] [01111101011] [00111101011]
[00111101111] [00101101111] [00101101101] [00101001101] [00101001111]
[00101011111] [00101010111] [00101010011] [00101110011] [00101111011]
[00101101011] [00101001011] [00101011011] [00101011001] [00111011001]
[00110011001] [00110111001] [01110111001] [01110110001] [01110010001]
[01010010001] [01010110001] [01011110001] [01011010001] [00011010001]
[00111010001] [00110010001] [00010010001] [00010110001] [00011110001]
[00001110001] [00001111001] [00001111011] [00001110011] [00001100011]
[00001101011] [00001101001] [00001001001] [00001011001] [00001010001]
[00001010011] [00001011011] [00001001011] [00001000011] [00001000111]
[00000000111] [00000000101] [00000001101] [00000001001] [00000001011]
[00000000011] [00000000001] [00010000001] [10010000001] [10110000001]
[00110000001] [00111000001] [00101000001] [00001000001] [00011000001]
[10011000001] [10001000001] [11001000001] [11001010001] [11001110001]
[11011110001] [11010110001] [10010110001] [10110110001] [10100110001]
[10101110001]

Seed-codes for $n = 11$

Appendix C

In this appendix we present the seed-codes of the second construction for $3 \leq n \leq 8$ as shown on this page and the top of the following page.

[001] [011]

Seed-codes for $n = 3$

[0001] [0011]

Seed-codes for $n = 4$

[00001] [00011] [00111] [01111] [01101] [00101]

Seed-codes for $n = 5$

[000001]	[000011]	[000111]	[001111]	[011111]	[011101]	[001101]	[000101]

Seed-codes for $n = 6$

[0000001]	[0000101]	[0001101]	[0001001]	[1001001]	[1011001]
[1111001]	[1111101]	[0111101]	[0110101]	[0110111]	[0100111]
[0100101]	[1100101]	[1000101]	[1000111]	[0000111]	[0000011]

Seed-codes for $n = 7$

[00000001]	[00000011]	[00000111]	[00010111]	[00010011]	[00011011]
[00011001]	[00011101]	[00010101]	[00101011]	[00100101]	[00100111]
[00101111]	[00101101]	[00111101]	[00111111]	[00111011]	[01101111]
[00110111]	[00110101]	[01010111]	[01011111]	[00011111]	[00001111]
[00001101]	[00001001]	[00001011]	[00000101]		

Seed-codes for $n = 8$

References

[1] J. Berstel and M. Pocchiola, "Average codes of Duval's algorithm for generating Lyndon words," *Theor. Comput. Sci.*, vol. 132, pp. 415–425, 1994.

[2] G. S. Bhat and C. D. Savage, "Balanced Gray codes," *Elec. J. Combin.*, vol. 3, 1996.

[3] A. H. Chan, R. A. Games, and E. L. Key, "On the complexities of de Bruijn sequences," *J. Combin. Theory, Ser. A*, vol. 33, pp. 233–246, 1985.

[4] C. C. Chang, H. Y. Chen, and C. Y. Chen, "Symbolic Gray code as a data allocation scheme for two-disc systems," *Comput. J.*, vol. 35, pp. 299–305, 1992.

[5] M. Chen and K. G. Shin, "Subcube allocation and task migration in hypercube machines," *IEEE Trans. Comput.*, vol. 39, pp. 1146–1155, 1990.

[6] F. Chung, P. Diaconis, and R. Graham, "Universal cycles for combinatorial structures," *Discr. Math.*, vol. 110, pp. 43–60, 1992.

[7] P. Diaconis and S. Holmes, "Gray codes for randomization procedures," *Statist. Comput.*, vol. 4, pp. 287–302, 1994.

[8] T. Etzion, "Optimal codes for correcting single errors and detecting adjacent errors," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1357–1360, 1992.

[9] T. Etzion and K. G. Paterson, "Near optimal single-track Gray codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 779–789, 1996.

[10] C. Faloutsos, "Gray codes for partial match and range queries," *IEEE Trans. Software Eng.*, vol. 14, pp. 1381–1393, 1988.

[11] H. Fredricksen and I. J. Kessler, "An algorithm for generating necklaces of beads in two colors," *Discr. Math.*, vol. 61, pp. 181–188, 1986.

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

[13] M. Gardner, "The curious properties of the Gray code and how it can be used to solve puzzles," *Scientif. Amer.*, vol. 227, pp. 106–109, 1972.

[14] E. N. Gilbert, "Gray codes and paths on the n-cube," *Bell Syst. Tech. J.*, vol. 37, pp. 815–826, 1958.

[15] F. Gray, "Pulse code," U.S. Patent Application 94 111 237.7, Mar. 1953.

[16] A. P. Hiltgen, K. G. Paterson, and M. Brandestini, "Single-track Gray codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1555–1561, 1996.

[17] J. T. Joichi, D. E. White, and S. G. Williamson, "Combinatorial Gray codes," *IEEE SIAM J. Comput.*, vol. 9, pp. 130–141, 1980.

[18] E. L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 732–736, 1976.

[19] R. M. Losee, "A Gray code based ordering for documents on shelves: Classification for browsing and retrieval," *J. Amer. Soc. Inform. Sci.*, vol. 43, pp. 312–322, 1992.

[20] J. M. Ludman, "Gray codes generation for MPSK signals," *IEEE Trans. Commun.*, vol. COM-29, pp. 1519–1522, 1981.

[21] F. Ruskey, C. Savage, and T. M. Y. Wang, "Generating necklaces," *J. Algorithms*, vol. 13, pp. 414–430, 1996.

[22] D. Richards, "Data compression and Gray-code sorting," *Inform. Process. Lett.*, vol. 22, pp. 201–205, 1986.

[23] J. Robinson and M. Cohn, "Counting sequences," *IEEE Trans. Comput.*, vol. C-30, pp. 17–23, May 1981.

[24] C. Savage, "A survey of combinatorial Gray codes," *SIAM Rev.*, vol. 39, pp. 605–629, 1997.

[25] D. G. Wagner and J. West, "Construction of uniform Gray codes," *Congr. Numer.*, vol. 80, pp. 217–223, 1994.