Minimal-Change Order and Separability in Linear Codes

A. J. van Zanten

Abstract—**A linear code $\mathscr{C}$ is said to be in minimal-change order if each codeword differs from its predecessor by a word of minimum weight. A rule is presented to construct such an order in case that $\mathscr{C}$ has a basis of codewords with minimum weight. Some consequences concerning the ranking and separability in $\mathscr{C}$ are mentioned.**

Index Terms—**Minimal-change order, Gray codes, ranking problem, separability.**

I. Preliminaries

It is well known that the set of all binary words of length n can be ordered in a list such that each word differs from its predecessor by precisely 1 bit. Such a list is called a Gray code. For any value of n, there are many such lists possible. The best known example is the so-called *binary reflected* or *normal Gray code* (cf. [3, pp. 172–177]). We denote this code by the matrix

$$G(n) = \begin{bmatrix} \boldsymbol{g}_0 \\ \boldsymbol{g}_1 \\ \vdots \\ \boldsymbol{g}_{2^n-1} \end{bmatrix}. \tag{1}$$

If we write $\boldsymbol{g}_i := g_{in-1}g_{in-2}\cdots g_{i0}$, and if $\boldsymbol{b}_i = b_{in-1}b_{in-2}\cdots b_{i0}$ is the binary representation of the index i, then the following rules hold for $0 \le i < 2^n$ and $0 \le j < n$:

$$g_{ij} = b_{ij+1} + b_{ij} \pmod 2 \tag{2}$$

and

$$b_{ij} = \sum_{l=j}^{n-1} g_{il} \pmod 2 \tag{3}$$

with $b_{in} := 0$ (cf., e.g., [3]). Rules (2) and (3) solve the *ranking problem* of $G(n)$.

A related question in this context is the *separability problem*. If two codewords $\boldsymbol{g}_i$ and $\boldsymbol{g}_j$ have Hamming distance m, one can ask how they are located with respect to each other in the ordered list $G(n)$ or, more specifically, one can ask for bounds for their *Gray distance* $|i-j|$. Actually, one has

$$\lceil 2^m/3 \rceil \le |i-j| \le \lfloor 2^n - 2^m/3 \rfloor. \tag{4}$$

Both bounds are sharp. The lower bound was derived by Yuen [6] and the upper bound by Cavior in [1].

Similar results have been obtained for the *constant weight Gray code* $G(n,k)$, consisting of words of length n and weight k (cf. [7]). In this code, each word differs from its predecessor by precisely 2 bits.

Both $G(n)$ and $G(n,k)$ are examples of lists ordered by a *minimal-change principle*. There are many more combinatorial objects (permutations, compositions, graphs, etc.) which can be ordered according to a minimal-change principle. For a review, we refer to [5].

Manuscript received July 30, 1992.

The author is with the Faculty of Technical Mathematics and Informatics, Delft University of Technology, 2600 GA Delft, The Netherlands.

IEEE Log Number 9212919.

In Section II, we show that there is also a wide class of *linear error-correcting codes*, which can be ordered in this way.

II. Linear Codes in Minimal-Change Order

Let $\mathscr{C}$ be an arbitrary linear binary code, and let this code be ordered. We shall say that $\mathscr{C}$ is in a minimal-change order, or is ordered according to a minimal-change principle, if each codeword differs from its predecessor by a word of minimum weight. A necessary and sufficient criterion for the existence of such an order in a given code can easily be given. It is the special case with $w = d$ of the following theorem.

Theorem: A linear $[n,k,d]$-code $\mathscr{C}$ can be ordered such that each codeword differs from its predecessor by precisely w bits if and only if $\mathscr{C}$ has a basis of codewords by weight w.

Proof: It is obvious that the condition is necessary, since the existence of the described order implies that $\mathscr{C}$ can be generated by codewords of weight w.

The condition is also sufficient. To show this, we assume that $A := (\boldsymbol{a}_0, \boldsymbol{a}_1, \cdots, \boldsymbol{a}_{k-1})$ is a basis, such that each $\boldsymbol{a}_j$ has weight w, for $0 \le j \le k-1$. Let $\boldsymbol{g}_i$ be the ith codeword of the normal Gray code $G(k)$ (cf. Section I). We define

$$\boldsymbol{c}_i = \sum_{j=0}^{k-1} g_{ij}\boldsymbol{a}_j, \qquad 0 \le i < 2^k. \tag{5}$$

If i runs through its value set, we obtain all linear combinations of the words of A. Furthermore, since $\boldsymbol{g}_i$ and $\boldsymbol{g}_{i+1}$ differ by 1 bit, it follows that $\boldsymbol{c}_i$ and $\boldsymbol{c}_{i+1}$ differ by one word of the basis A, which has weight w, for all relevant values of i. This completes the proof. □

From now on, we assume that A is a basis of words of minimum weight d, and furthermore, that the code $\mathscr{C}$ is in minimal-change order according to the construction in the above proof. The ranking problem for $\mathscr{C}$ can easily be solved. To determine $\boldsymbol{c}_i$ for a given value of i, one first converts i to its Gray representation, using (2), and next applies (5). As an alternative, one can equally well use the generator matrix

$$G(\mathscr{C}) = \begin{bmatrix} \boldsymbol{a}_{k-1} + \boldsymbol{a}_{k-2} \\ \vdots \\ \boldsymbol{a}_1 + \boldsymbol{a}_0 \\ \boldsymbol{a}_0 + \boldsymbol{0} \end{bmatrix} \tag{6}$$

and apply the relation

$$\boldsymbol{c}_i = \boldsymbol{b}_i G(\mathscr{C}), \tag{7}$$

which directly converts the binary representation of i to the ith codeword of $\mathscr{C}$.

Finally, we present bounds for the Gray distance in $\mathscr{C}$. These follow from the inequalities (4). If $\boldsymbol{c}_i$ and $\boldsymbol{c}_j$ are codewords of the ordered code $\mathscr{C}$ with Hamming distance m, then

$$\lceil 2^{m'}/3 \rceil \le |i-j| \le \lfloor 2^n - 2^{m'}/3 \rfloor \tag{8}$$

where $m' := \lceil m/d \rceil$. Whether these bounds are sharp depends on the code $\mathscr{C}$ and on the chosen basis A.

Remark: There are many codes that have a basis of words of minimum weight, e.g., Hamming codes and Reed–Muller codes. Furthermore, all codes that meet the Griesmer bound have such a basis (cf. [2], [4]).

References

[1] S. R. Cavior, "An upper bound associated with errors in Gray code," *IEEE Trans. Inform. Theory*, vol. IT-21, p. 596, 1975.

[2] S. M. Dodunekov and N. L. Manev, "An improvement of the Griesmer bound for small minimum distances," *Discrete Appl. Math.*, vol. 12, pp. 103–114, 1983.

[3] E. M. Reingold, J. Nievergelt, and N. Deo, *Combinatorial Algorithms: Theory and Practice*. Englewood Cliffs, NJ: Prentice-Hall, 1977.
[4] H. van Tilborg, "On the uniqueness resp. nonexistence of certain codes meeting the Griesmer bound," *Discrete Math.*, vol. 44, pp. 16–35, 1980.
[5] H. S. Wilf, "Combinatorial algorithms: An update," in *CBMS–NSF Regional Conf. Ser. Appl. Math.*, Soc. Indust. Appl. Math., Philadelphia, PA, 1989.
[6] C. K. Yuen, "The separability of Gray code," *IEEE Trans. Inform. Theory*, vol. IT-20, p. 668, 1974.
[7] A. J. van Zanten, "Index system and separability of constant weight Gray codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1229–1233, 1991.

The Number of Nonlinear Shift Registers That Produce All Vectors of Weight $\leq t$

Harold Fredricksen, *Member, IEEE*

Abstract—**It has been shown that it is possible to generate a cycle on a nonlinear shift register to contain all vectors of length n and Hamming weight $\leq t$. We show how to count the number of different ways this can be done on a truth table of minimum density.**

Index Terms—**BEST theorem, binary sequence, de Bruijn graph, cycle joining, shift register, spanning tree, truth table.**

I. Introduction

In [1], it is shown that a nonlinear shift register can be designed to generate all of the vectors of length n having no more than a Hamming weight of t ones. Applications for such functions are discussed there. Examples for all $n \leq 7$ and $1 \leq t \leq n$ are given. The authors also give an example of a shift register feedback function to produce one such sequence, with each binary vector appearing exactly once for each appropriate n and t. Similar approaches were used [2]–[4] to connect all vectors of length n into a single de Bruijn cycle. In this note, we show in how many ways cycles of a given length and weight may be joined for a certain subclass of shift register feedback functions. Our class is that for which each feedback truth table contains the minimum possible density of ones.

In order to ensure that any feedback function $f(x_0, x_1, \cdots, x_{n-1})$ produces only cycles, it suffices that f be of the form $f = x_0 + g(x_1, \cdots, x_{n-1})$ [5]. The feedback function $f = x_0$ is of the branchless type with $g(x_1, \cdots, x_{n-1}) \equiv 0$ and is called the pure cycling register. The factor created consists of cycles defined as the cyclotomic cosets of vectors formed as equivalence classes under the cyclic rotation of the bits of the vectors of $GF(2)^n$. The density of the truth table of this pure cycling register is zero. The cycles formed are enumerated by $Z(n)$, $Z(n) = (1/n)\sum_{d|n} \phi(d) 2^{n/d}$ where the summation is over all positive integer divisors d of n and ϕ is Euler's totient function. The cycles are all cycles of vectors of length d for each divisor d of n. These cycles form the fundamental building blocks for the theory developed in [1]. Here, we note simply that two of these pure cycles may be joined together if there is an adjacency between them.

We refer the reader to [1], [3]–[5] for any additional required shift register theory. The cycle decompositions of the underlying de Bruijn graph, cycle adjacencies, and joins are well covered there and need not be duplicated here.

II. Sequences of Vectors of Weight $\leq t$

The sequences of [1] are formed by joining all of the cyclotomic cycles of vectors of length n and having $\leq t$ ones. If there are C such cycles, they may be joined together in several ways, but this surgery will always require that at least $C - 1$ positions of the truth table of g be changed from zero to one. If we restrict the truth tables to have no more than a density of $C - 1$ ones, then we can count the number of ways to generate such a sequence. We employ a result of de Bruijn, Ehrenfest, Smith, and Tutte described in [6]–[8], and used in [4] to generate de Bruijn cycles by joining all of the cycles of the pure cycling register together.

Theorem 1 (BEST): The number of spanning subtrees of a labeled connected graph is evaluated by computing the determinant of the cofactor of a root in the associated adjacency matrix of the graph.

To use the theorem to find the number of sequences we seek, we call each cyclotomic coset a node in a graph, and we label the edge between cosets C_i and C_j with the number of vectors on C_i having a conjugate on C_j. The problem of adjacencies in the pure cycling register has been studied previously [9], [10]. Then, the spanning subtrees give the smallest number of changes to g that can be made to join all of the cycles into a single cycle. It may be possible to join cycles in another way by splitting the cycle created and then rejoining the pieces in a different way. We do not include these cycles in our count.

Two examples of cycles formed in this way are given in [1]. See also [4], where all of the pure cycles are joined to form a de Bruijn cycle. For the case at hand, only the subset of the cycles of weight $\leq t$ are used. Then, the subgraph $H(n, w)$ is constructed. $H(n, w)$ is obtained from the graph $G(n)$ of all pure cycles and their edges under adjacency by removing all vertices of weight bigger than w. Thus, the vertices of the graph $H(n, t)$ are the cycles of the pure cycling register with weight less than $t + 1$. There is an edge in $H(n, t)$ between nodes x and y if there is an adjacency between the cycles represented.

The BEST theorem states that the number of spanning trees of these graphs is found by computing the determinant of the cofactor of a root of the graph. In all such graphs, the node 0 will be a root, so we need only evaluate the determinant of the cofactor of the $(0, 0)$ entry of the matrix.

The matrix size grows with n and t, but the determinants are easily evaluated with Maple. In Table I, the factored forms of the determinants are given. No obvious patterns emerge for the cosets of weight $t = 3$ and higher. For any n, when $t = 1$, there is obviously only one way to add the coset $(00 \cdots 01)$ to the coset (0). For $t = 2$, there is a twofold choice of how to add each of the cosets of weight 2 when n is odd. When n is even, there is also a coset of size $n/2$ which can be added to the cycle in a unique way. Hence, the number $N(n, 2) = 2^{[n-2/2]}$.

III. Conclusions

We have shown how a theorem on spanning subtrees on a graph can be used to evaluate the number of sequences that

Manuscript received **December 10, 1992; revised February 16, 1993.**
The author was on leave at the Institute for Defense Analyses, Center for Communications Research, San Diego, CA 92121. He was with the Department of Mathematics, Naval Postgraduate School, Monterey, CA 93943.
IEEE Log Number 9213028.