JOURNAL OF COMBINATORIAL THEORY, Series A 64, 10–30 (1993)

Greedy Codes

RICHARD A. BRUALDI*

Department of Mathematics,
University of Wisconsin, Madison, Wisconsin 53706

AND

VERA S. PLESS†

Department of Mathematics,
University of Illinois at Chicago, Chicago, Illinois 60680

Communicated by the Editors

Received June 10, 1991

Given an ordered basis of F_2^n and an integer d, we define a greedy algorithm for constructing a code of minimum distance at least d. We show that these greedy codes are linear and construct a parity check matrix for them. For ordered bases which have a triangular form we are able to give a lower bound on the dimension of greedy codes. Lexicodes are instances of greedy codes. There are examples of greedy codes which are better than lexicodes. © 1993 Academic Press, Inc.

1. INTRODUCTION

In this paper we are concerned with binary codes which are defined by means of a greedy algorithm. Let n and d be integers with $0 \leqslant d \leqslant n$ and suppose that the set F_2^n of binary n-tuples has been listed in some order. Choosing the first vector on the list and then applying recursively the rule

> choose the next vector on the list whose (Hamming) distance to each previously chosen vector is at least d

defines a binary code with minimum distance at least d. We first learned of greedy codes from [3] where the binary n-tuples are listed in lexicographic order. These *lexicodes* were shown to be closely related to the

* Research partially supported by NSF Grant DMS-8901445 and NSA Grant MDA904-89-H-2060.

† Research partially supported by NSA Grant MDA904-91-H-0003.

0097-3165/93 $5.00

Sprague–Grundy theory of impartial games and that theory had many implications for lexicodes. In particular lexicodes are linear codes, the lexicodes for $n=2^m-1$ and $d=3$ are the Hamming codes, and the lexicode for $n=23$ and $d=7$ is the binary Golay code. After we completed our work we learned that in 1960 Levenšteĭn [7] (see also van Lint [4]) had proved the linearity of the lexicodes and the fact that the Hamming codes are lexicodes.[1] Further work on lexicodes is contained in [2].

Throughout we identify a nonnegative integer with a binary vector by means of its base 2 numeral. We use $\oplus$ to denote addition of binary vectors. Thus for integers a and b,

$$a \oplus b$$

is the sum of a and b regarded as binary vectors, and this sum is commonly called the *nim-sum* of a and b. For instance, $12 \oplus 5 = 9$, since $(1, 1, 0, 0) \oplus (0, 1, 0, 1) = (1, 0, 0, 1)$. Note that for integers a and b, $a<b$ is equivalent to the statement that a comes before b in the lexicographic order (of their base 2 numerals).

Let $\mathscr{B}$ denote an ordered basis $y_1, y_2, ..., y_n$ of F_2^n. The ordered basis $\mathscr{B}$ induces an order of the vectors of F_2^n defined recursively as follows: Let $V_0 = \{(0, 0, ..., 0)\}$ and let

$$V_i = \langle y_1, ..., y_i \rangle \qquad (i=1, 2, ..., n)$$

be the subspace of F_2^n spanned by the vectors $\{y_1, ..., y_i\}$. The subspace V_0 contains a unique vector and hence its vectors are ordered. Suppose the vectors in V_{i-1} have been ordered

$$x_1, x_2, ..., x_m \qquad (m=2^{i-1}).$$

We have the partition

$$V_i = V_{i-1} \cup (y_i \oplus V_{i-1})$$

and we order the vectors in V_i by following the vectors $x_1, x_2, ..., x_m$ with the vectors $y_i \oplus x_1, y_i \oplus x_2, ..., y_i \oplus x_m$:

$$x_1, x_2, ..., x_m, y_i \oplus x_1, y_i \oplus x_2, ..., y_i \oplus x_m.$$

Since $V_n = F_2^n$, this defines an order for the vectors of F_2^n which we call the *order induced by* $\mathscr{B}$ or, for short, the *$\mathscr{B}$-order* of F_2^n. For $n=3$, the $\mathscr{B}$-order of F_2^3 is

$$0, y_1, y_2, y_2 \oplus y_1, y_3, y_3 \oplus y_1, y_3 \oplus y_2, y_3 \oplus y_2 \oplus y_1.$$

[1] We are indebted to G. A. Kabatyanskii for bringing Levenšteĭn's work to our attention.

Suppose we take for $\mathscr{B}$ the standard unit basis in the order

$$e_1 = (0, ..., 0, 1), e_2 = (0, ..., 1, 0), ..., e_n = (1, 0, ..., 0). \tag{1}$$

(Thus we are considering the first coordinate of an n-tuple to be its rightmost coordinate.) In this case the $\mathscr{B}$-order of F^n is the standard *lexicographic order* of binary n-tuples. Each n-tuple $x = (x_{n-1}, ..., x_1, x_0)$ in F_2^n can be regarded as the base 2 numeral of an integer between 0 and $2^n - 1$. Throughout this paper we identify an n-tuple with the integer it represents:

$$x = (x_{n-1}, ..., x_1, x_0) \leftrightarrow x = x_{n-1}2^{n-1} + \cdots + x_1 2 + x_0.$$

In this identification the lexicographic order of n-tuples coincides with the natural order of integers.

Now take the ordered basis $\mathscr{B}$ to be

$$(0, ..., 0, 1), (0, ..., 0, 1, 1), (0, ..., 0, 1, 1, 0), ..., (1, 1, 0, ..., 0). \tag{2}$$

In this case the $\mathscr{B}$-order of F^n is the order of n-tuples given by the reflected Gray code[2] of order n. (Surprisingly, we have been unable to find this particular algebraic generating scheme for the reflected Gray code in the literature.) We call this order the *Gray order* of F_2^n. We also call the ordered basis (2) the *Gray ordered basis* of F_2^n.

In general the $\mathscr{B}$-order of F_2^n coincides with the lexicographic order of the coordinate vectors relative to the ordered basis $\mathscr{B}$.

Both the lexicographic order and the Gray order are instances of what we call a triangular order of F_2^n. Consider an ordered basis $y_1, y_2, ..., y_n$ of F_2^n for which each $V_i = \langle y_1, ..., y_i \rangle$ is the coordinate subspace consisting of all n-tuples with 0's in the $n-i$ leftmost positions. Thus the n by n matrix

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 & * \\ 0 & 0 & \cdots & 1 & * & * \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 1 & * & \cdots & * & * & * \end{bmatrix}$$

has a triangular pattern, and we call $y_1, y_2, ..., y_n$ a *triangular ordered basis* of F_2^n. If $\mathscr{B}$ is a triangular ordered basis of F_2^n, then we call the $\mathscr{B}$-order

[2] The use of the word *code* here is different from that used otherwise in this paper.

a *triangular order* of F_2^n. Another special triangular order is obtained by choosing the *complementary ordered basis*

$$(0, ..., 0, 1), (0, ..., 0, 1, 1), (0, ..., 0, 1, 1, 1), ..., (1, ..., 1, 1). \tag{3}$$

The resulting order of F_2^n is called the *complementary order.*

Let $\mathscr{B}$ be an ordered basis of F_2^n and let d be an integer with $0 \leqslant d \leqslant n$. Applying the greedy algorithm (for the chosen d) to the $\mathscr{B}$-order of F_2^n we obtain a code $C = C(\mathscr{B}, d)$ whose minimum distance is at least d. The code C is the *$\mathscr{B}$-greedy code of length n and designed distance d.* The lexicodes of [3] are a special case of $\mathscr{B}$-greedy codes.

We now summarize some of the main conclusions of this paper. In the next section we show that $\mathscr{B}$-greedy codes are always linear. An equivalent result was stated by Levenšteĭn [7]. We also show how to enhance the greedy algorithm in order to determine a parity check matrix. We further show that it suffices to consider only $\mathscr{B}$-greedy codes of even designed distance.

In the third section we consider $\mathscr{B}$-greedy codes for which $\mathscr{B}$ is a triangular ordered basis. We call such codes *triangular-greedy* codes. The lexicodes, the *Gray-greedy codes* (the $\mathscr{B}$-greedy codes for a Gray ordered basis $\mathscr{B}$), and the *complementary-greedy codes* (the $\mathscr{B}$-greedy codes for a complementary ordered basis) are triangular-greedy codes. The triangular-greedy codes of designed distance d have minimum distance equal to d. We obtain a simple lower bound on the dimension of triangular-greedy codes and show that all triangular-greedy codes of length $n = 2^m$ and designed distance $d = 4$ are extended Hamming codes. We also present computer data which verify that the Gray-greedy code and the complementary-greedy code of length $n = 24$ and designed distance $d = 8$ equal the binary Golay code (the corresponding statement for the lexicode was verified in [3]) and demonstrate that Gray-greedy codes and complementary-greedy codes are sometimes better (that is, have a larger dimension) than lexicodes (see Table II). These data also show that these codes have dimension within one of the best codes known.

2. Linearity of Greedy Codes

We begin with an example which illustrates the construction of the Gray-greedy code of length $n = 5$ and designed distance $d = 3$. We choose the Gray ordered basis $y_1 = (0, 0, 0, 0, 1)$, $y_2 = (0, 0, 0, 1, 1)$, $y_3 = (0, 0, 1, 1, 0)$, $y_4 = (0, 1, 1, 0, 0)$, $y_5 = (1, 1, 0, 0, 0)$ and obtain the Gray order of F_2^5 as shown in Table I (we omit the commas between coordinates). For $i = 1, 2, 3, 4, 5$ the first 2^i vectors are the vectors of the

TABLE I

Gray-Greedy Code of Designed Distance 3

Gray order of F_2^5	g-values	g-values as vectors	Gray-greedy code
00000	0	000	♠
$y_1 =$ 00001	1	001	
$y_2 =$ 00011	2	010	
00010	3	011	
$y_3 =$ 00110	1	001	
00111	0	000	♠
00101	3	011	
00100	2	010	
$y_4 =$ 01100	4	100	
01101	5	101	
01111	6	110	
01110	7	111	
01010	5	101	
01011	4	100	
01001	7	111	
01000	6	110	
$y_5 =$ 11000	1	001	
11001	0	000	♠
11011	3	011	
11010	2	010	
11110	0	000	♠
11111	1	001	
11101	2	010	
11100	3	011	
10100	5	101	
10101	4	100	
10111	7	111	
10110	6	110	
10010	4	100	
10011	5	101	
10001	6	110	
10000	7	111	

subspace $V_i = \langle y_1, ..., y_i \rangle$. The Gray-greedy code of length 5 and designed distance 3 is the linear code

$$C = \{(0, 0, 0, 0, 0), (0, 0, 1, 1, 1), (1, 1, 0, 0, 1), (1, 1, 1, 1, 0)\} \quad (4)$$

consisting of those vectors with a ♠ in their row.

We now describe a more detailed greedy algorithm for a given ordering of the vectors in F^n.

Let d be an integer with $0 \leqslant d \leqslant n$. Assume that the vectors in F_2^n have been listed in some order: $z_1, z_2, ..., z_{2^n}$. We recursively define a function

$$g : F_z^n \to Z_{(\geqslant 0)}$$

with domain F_2^n and target the nonnegative integers $Z_{(\geqslant 0)}$ as follows. First we define $g(z_1) = 0$. Let $i \geqslant 2$ and suppose that $g(z_1), ..., g(z_{i-1})$ have been defined. Then we define $g(z_i)$ by

> $g(z_i)$ is the smallest integer t such that $\mathrm{dist}(z_i, x) \geqslant d$ for all vectors x in $\{z_1, ..., z_{i-1}\}$ which satisfy $g(x) = t$. If no such t exists then we define $g(z_i)$ to be the smallest integer not in $\{g(z_1), ..., g(z_{i-1})\}$.

In other words, z_i is assigned g-value equal to the first integer t such that z_i has distance at least d to all vectors which have already been assigned the g-value t. If z_i has distance less than d to at least one vector of each previously assigned integer, then the g-value assigned to z_i equals the first integer not yet assigned as a g-value. The *greedy code C of designed distance d* equals the set

$$\{z \in F_2^n : g(z) = 0\},$$

of all vectors whose g-value equals 0. By construction the covering radius of C is at most $d-1$, that is, every vector not in C has distance at most $d-1$ to some vector in C. If the vectors of F_2^n are listed in lexicographic order, then the g-values are the Grundy numbers for the associated heap game and the greedy code C is a lexicode [3].

Let m be the smallest integer such that

$$g(z) \leqslant 2^m - 1 \qquad \text{for all } z \text{ in } F_2^n.$$

We call m the *index* of the given ordering of F_2^m relative to the designed distance d. Each integer $g(z)$ can be regarded as a vector in F_2^m by taking its base 2 numeral and then including leading 0's as necessary. Hence we may also regard g as a map

$$g : F_2^n \to F_2^m$$

with target space F_2^m. In this case, since the natural order of integers is the same as the lexicographic order of their corresponding vectors in F_2^m, in the definition of g, smallest means lexicographically smallest. In Table I the g-value of each vector in F_2^5 has been computed both as an integer and as a vector in F_2^3 $(m = 3)$. It can be checked that the set of all vectors with a particular g-value is a coset of the Gray-greedy code C in (4). This means that the map

$$g: F_2^5 \to F_2^3$$

is a homomorphism with kernel equal to C. Hence the 3 bv 5 matrix

$$H = [g(e_5)\ g(e_4)\ g(e_3)\ g(e_2)\ g(e_1)]$$

is a parity check matrix for C, and the g-value of a vector in F_2^5 is its syndrome relative to this parity check matrix. Here we are treating the g-values as column vectors, and our convention for identifying column vectors with integers is that lower coordinates correspond to smaller powers of 2:

$$\begin{bmatrix} x_{n-1} \\ \vdots \\ x_1 \\ x_0 \end{bmatrix} \leftrightarrow x_{n-1}2^{n-1} + \cdots x_1 2 + x_0.$$

We now show that similar properties hold for any $\mathscr{B}$-order of F_2^n and any d. The proof of the following lemma is a simple consequence of the definition of the sum $\oplus$.

LEMMA 2.1. *Let α and β be two integers such that $\beta < \beta \oplus \alpha$. The number of integers x such that $\beta \leqslant x < \beta \oplus \alpha$ is at most α with equality if and only if (in their base 2 representations) β and α have no powers of 2 in common. In particular, $\beta < \beta \oplus 2^k$ implies that there are exactly 2^k integers x with $\beta \leqslant x < \beta \oplus 2^k$, and hence there do not exist integers α and β such that either $\alpha < \beta < \beta \oplus 2^k \leqslant \alpha \oplus 2^k$ or $\alpha < \beta \oplus 2^k < \beta \leqslant \alpha \oplus 2^k$ holds.*

THEOREM 2.2. *Let $\mathscr{B}$ be an ordered basis of F_2^n and let d be an integer with $0 \leqslant d \leqslant n$. Let m be the index of the $\mathscr{B}$-order of F_2^n. Then*

$$g: F_2^n \to F_2^m$$

is a surjective homomorphism whose kernel equals the $\mathscr{B}$-greedy code C of length n and designed distance d. In particular, C is a linear code of dimension $n - m$.

A parity check matrix for C is the m by n matrix

$$H = [g(e_n) \cdots g(e_2)\ g(e_1)]$$

and for each z in F_2^n, $g(z)$ is the syndrome of z relative to H.

Proof. Let the ordered basis $\mathscr{B}$ be $y_1, y_2, ..., y_n$, and let $V_i = \langle y_1, ..., y_i \rangle$ $(i = 0, 1, ..., n)$. We prove by induction on i that

$$g: V_i \to F^m$$

is a homomorphism. Since $V_n = F_2^n$, we get that $g: F_2^n \to F_2^m$ is a homomorphism, from which all the conclusions of the theorem easily follow.

For each α which occurs as a g-value of a vector in V_i, let

$$C_i^\alpha = \{x \in V_i : g(x) = \alpha\} \qquad (i = 0, 1, ..., n).$$

If $\alpha = (0, ..., 0)$ we write C_i in place of C_i^α.

We have $V_0 = \{(0, ..., 0)\}$ and $g(0, ..., 0) = (0, ..., 0)$. Hence $g: V_0 \to F_2^m$ is indeed a homomorphism. Let $i \geqslant 0$ and assume that $g: V_i \to F_2^m$ is a homomorphism. Thus C_i is a linear code and its cosets are the C_i^α. Moreover, for any two cosets C_i^α and $C_i^{\alpha'}$ of C_i we have

$$C_i^\alpha \oplus C_i^{\alpha'} = C_i^{\alpha \oplus \alpha'}. \tag{5}$$

We now consider the map

$$g: V_{i+1} \to F_2^m, \tag{6}$$

where

$$V_{i+1} = V_i \cup (y_{i+1} \oplus V_i).$$

To conclude that (6) is a homomorphism it suffices to prove that

$$g(y_{i+1} \oplus z) = g(y_{i+1}) \oplus g(z) \qquad \text{for all } z \text{ in } V_i.$$

We consider two cases.

Case 1. $\operatorname{dist}(y_{i+1}, C_i^\alpha) < d$ for all C_i^α.

Consider any vector $y_{i+1} \oplus z$ with z in V_i. For each C_i^α we have

$$\operatorname{dist}(y_{i+1} \oplus z, C_i^\alpha) = \operatorname{dist}(y_{i+1}, z \oplus C_i^\alpha) = \operatorname{dist}(y_{i+1}, C_i^\beta)$$

for some β. Hence

$$\operatorname{dist}(y_{i+1} \oplus z, C_i^\alpha) < d \qquad \text{for all } C_i^\alpha.$$

From the algorithm for computing g, it follows that no vector in $y_{i+1} \oplus V_i$ receives the same g-value as a vector in V_i. Let γ be the smallest integer (in base 2 form) which is not a g-value of any vector in V_i.[3] Then we have $g(y_{i+1})=\gamma$. Since

$$\mathrm{dist}(y_{i+1}\oplus z,\ y_{i+1}\oplus z')=\mathrm{dist}(z,z') \qquad \text{for all} \quad z,z'\in V_i,$$

it follows from the definition of the $\mathscr{B}$-order and the definition of g that computing the g-values of vectors in $y_{i+1}\oplus V_i$ is the same as computing the g-values of vectors in V_i using the initial value γ. Hence

$$g(y_{i+1}\oplus z)=\gamma\oplus g(z)=g(y_{i+1})\oplus g(z) \qquad \text{for all } z \text{ in } V_i. \tag{7}$$

Hence (6) is a homomorphism in this case.

Case 2. There is a β such that $\mathrm{dist}(y_{i+1}, C_i^\beta)\geqslant d$.

We choose β to be the smallest integer satisfying the assumption of this case, and hence

$$g(y_{i+1})=\beta.$$

Suppose $z\in C_i^\alpha$. Then by (5), for all τ

$$\mathrm{dist}(y_{i+1}\oplus z,\ C_i^\tau)=\mathrm{dist}(y_{i+1},\ z\oplus C_i^\tau)=\mathrm{dist}(y_i,\ C_i^{\alpha\oplus\tau}).$$

Thus for each α and for each τ, all of the vectors in $y_{i+1}\oplus C_i^\alpha$ have the same distance to the coset C_i^τ. Since the vectors in $y_{i+1}\oplus V_i$ are considered in the same order as the vectors in V_i, each of the vectors in $y_{i+1}\oplus C_i^\alpha$ has the same g-value and for $\alpha\neq\alpha'$, vectors in $y_{i+1}\oplus C_i^\alpha$ have different g-values from vectors in $y_{i+1}\oplus C_i^{\alpha'}$. For $x\in C_i^\alpha$ we now write $g(y_{i+1}\oplus C_i^\alpha)$ in place of $g(y_{i+1}\oplus x)$.

Consider a g-value γ of V_i. By (5),

$$C_i^\beta\oplus C_i^\gamma=C_i^{\beta\oplus\gamma}.$$

We have

$$\mathrm{dist}(y_{i+1}\oplus C_i^\gamma,\ C_i^{\beta\oplus\gamma})=\mathrm{dist}(y_{i+1},\ C_i^\beta)\geqslant d,$$

which implies that $\beta\oplus\gamma$ is a possible g-value for the vectors in $y_{i+1}\oplus C_i^\gamma$.

[3] Since we are assuming inductively that $g\colon V_i\to F^m$ is a homomorphism, it follows that γ is a power of 2.

By taking $\gamma=\beta$ and using the fact that 0 is the smallest possible g-value, we now conclude that

$$C_{i+1}=C_{i+1}^{0}=C_{i}^{0}\cup(y_{i+1}\oplus C_{i}^{\beta}), \tag{8}$$

and thus that C_{i+1} is a linear code.[4]

We now start another induction on increasing values of γ and show that

$$g(y_{i+1}\oplus C_{i}^{\gamma})=\beta\oplus\gamma, \tag{9}$$

that is, the cosets of the linear code C_{i+1} are given by

$$C_{i+1}^{\beta\oplus\gamma}=C_{i}^{\beta\oplus\gamma}\cup(y_{i+1}\oplus C_{i}^{\gamma}).$$

In particular, this implies that each vector in $y_{i+1}\oplus V_i$ gets the same g-value as a vector in V_i. For $\gamma=0$, (9) holds by the definition of β. Now suppose that $\tau\neq 0$ and that (9) holds for all $\gamma<\tau$. This implies that

$$g(y_{i+1}\oplus C_{i}^{\gamma})\neq\beta\oplus\tau, \qquad \text{for all} \quad \gamma<\tau. \tag{10}$$

Let

$$\rho=g(y_{i+1}\oplus C_{i}^{\tau}).$$

Since $\beta\oplus\tau$ is a possible g-value for $y_{i+1}\oplus C_{i}^{\tau}$ and since by (10), $\beta\oplus\tau$ has not been given away by the time we reach the first vector in $y_{i+1}\oplus C_{i}^{\tau}$, we now conclude that

$$\rho\leqslant\beta\oplus\tau.$$

There is a smallest power 2^k such that $\tau\oplus 2^k<\tau$. Let

$$\mu=g(y_{i+1}\oplus C_{i}^{\tau\oplus 2^k})=\beta\oplus(\tau\oplus 2^k).$$

Then

$$\rho\leqslant\beta\oplus\tau=\mu\oplus 2^k.$$

We also have

$$\operatorname{dist}(y_{i+1}\oplus C_{i}^{\tau\oplus 2^k}, C_{i}^{\rho\oplus 2^k})=\operatorname{dist}(y_{i+1}\oplus C_{i}^{\tau}, C_{i}^{\rho})\geqslant d. \tag{11}$$

We claim that $\mu\leqslant\rho\oplus 2^k$. Assume to the contrary that $\rho\oplus 2^k<\mu$. Then using (11) we see that there exists an $\alpha<\tau\oplus 2^k$ such that $g(y_{i+1}\oplus C_{i}^{\alpha})=$

[4] Note that we know that C_{i+1} is a linear code only under the strong induction hypothesis that the C_i^{γ} are cosets of C_i. It does not suffice with this argument to assume only that C_i is a linear code to conclude that C_{i+1} is a linear code.

$\rho \oplus 2^k$ and hence $\beta \oplus \alpha = \rho \oplus 2^k$. Now $\alpha < \tau \oplus 2^k < \tau$ and Lemma 2.1 imply that $\alpha \oplus 2^k < \tau$ and so

$$g(y_{i+1} \oplus C_i^{\alpha \oplus 2^k}) = \beta \oplus \alpha \oplus 2^k = \rho,$$

contradicting $g(y_i \oplus C_i^\tau) = \rho$. Hence

$$\mu \leqslant \rho \oplus 2^k.$$

We now claim that $\rho = \mu \oplus 2^k$. Assume to the contrary that $\rho \neq \mu \oplus 2^k$. Since $g(y_{i+1} \oplus C_i^{\tau \oplus 2^k}) = \mu$, we also have that $\rho \neq \mu$. Using Lemma 2.1 we see that one of the following holds:

$$\mu < \rho < \mu \oplus 2^k < \rho \oplus 2^k, \tag{12}$$

$$\rho < \mu < \rho \oplus 2^k < \mu \oplus 2^k. \tag{13}$$

By choice of 2^k each of the integers $\tau \oplus 2^k \oplus 1, \tau \oplus 2^k \oplus 2, ..., \tau \oplus 2^k \oplus (2^k - 1)$ is less than τ and hence by the induction hypothesis

$$\rho \neq \mu \oplus 1, \mu \oplus 2, ..., \mu \oplus (2^k - 1).$$

We first suppose that (12) holds. Then ρ must be one of the numbers $\mu \oplus 2^k \oplus 1, \mu \oplus +2^k \oplus 2, ..., \mu \oplus 2^k \oplus (2^k - 1)$ and hence $\rho \oplus 2^k$ is one of the numbers

$$\mu \oplus 1, \mu \oplus 2, ..., \mu \oplus (2^k - 1).$$

But by Lemma 2.1 there are 2^k integers x with $\rho \leqslant x < \rho \oplus 2^k$, and at most 2^k integers y with $\mu \leqslant y < \mu \oplus l$ for each $l = 1, 2, ..., 2^k - 1$. This gives a contradiction and implies that

$$\rho = \mu \oplus 2^k$$

in this case.

We now assume that (13) holds. An argument similar to that above implies that $\rho \oplus 2^k$ is one of the integers

$$\mu \oplus 1, \mu \oplus 2, ..., \mu \oplus (2^k - 1),$$

and applying Lemma 2.1 again we obtain a contradiction. Thus

$$\rho = \mu \oplus 2^k$$

in this case also.

Since $\mu = \beta \oplus (\tau \oplus 2^k)$ we now conclude that $\rho = \beta \oplus \tau$. Therefore $g\colon V_{i+1} \to F_2^m$ is a homomorphism. ∎

The specific parity check matrix H in Theorem 2.2 for the greedy code C is called the *g-parity check matrix* for C.

We observe that every linear code C with minimum distance at least d and covering radius at most $d-1$ is a $\mathscr{B}$-greedy code of designed distance d for some ordered basis $\mathscr{B}$. Indeed we may choose for $\mathscr{B}$ any ordered basis whose first k vectors are a basis of C where k is the dimension of C. The fact that a $\mathscr{B}$-greedy code of designed distance d has covering radius at most $d-1$ implies that $\mathscr{B}$-greedy codes attain the Varshamov–Gilbert bound for binary linear codes [5].

COROLLARY 2.3. *Let d be a positive integer. For each positive integer n let $\mathscr{B}_n$ be an ordered basis of F_2^n. Then the family of codes $C(\mathscr{B}_n, d)$ $(n=1, 2, ...)$ meets the Varshamov–Gilbert bound.*

If y is a vector in F_2^n, then $\hat{y}$ denotes the vector in F_2^{n+1} obtained from y by adding an overall parity check. For $A \subseteq F_2^n$, $\hat{A} = \{\hat{y} : y \in A\}$.

THEOREM 2.4. *Let $y_1, y_2, ..., y_n$ be an ordered basis $\mathscr{B}$ of F_2^n and let d be an odd integer. Let z be any odd weight vector of F_2^{n+1}, and let $\mathscr{B}'$ be the ordered basis $\hat{y}_1, \hat{y}_2, ..., \hat{y}_n, z$ of F_2^{n+1}. Then the $\mathscr{B}'$-greedy code of designed distance $d+1$ is obtained from the $\mathscr{B}$-greedy code of designed distance d by adding an overall parity check.*

Proof. We first note that $\{\hat{y}_1, \hat{y}_2, ..., \hat{y}_n, z\}$ is a basis of F_2^{n+1}, and that $\{\hat{y}_1, \hat{y}_2, ..., \hat{y}_n\}$ spans the subspace E of all even weight vectors of F_2^{n+1}. Let C be the $\mathscr{B}$-greedy code of designed distance d and let C' be the $\mathscr{B}'$-greedy code of designed distance $d+1$. Since d is odd, we see that for all $x, y \in F_2^n$, $\operatorname{dist}(x, y) \geqslant d$ if and only if $\operatorname{dist}(\hat{x}, \hat{y}) \geqslant d+1$. Hence

$$C' \cap E = \hat{C}.$$

For each vector $u \in E$ there is a vector $v \in C' \cap E$ such that $\operatorname{dist}(u, v) < d+1$. Since d is odd, $\operatorname{dist}(u, v) \leqslant d-1$. Hence for each vector $w \in F_2^{n+1}$ there is a vector $v \in C' \cap E$ such that $\operatorname{dist}(w, v) \leqslant d$. This implies that $C' \cap E = C'$, that is, $C' \subseteq E$, and hence C' is obtained from C by adding an overall parity check. ∎

A special case of the above theorem is that if $\mathscr{B}$ is an ordered basis of F_2^n whose first $n-1$ vectors have even weight, then the $\mathscr{B}$-greedy code of designed distance $d=2$ is the even weight subcode of F_2^n.

We close this section with the following remark concerning a game that can be associated with the greedy algorithm. Let $\mathscr{B}$ be an ordered basis of F_2^n and let d be a positive integer. We define a game $G(\mathscr{B}, d)$ whose positions are the binary n-tuples and where the move from x to y is a *legal move* provided that y comes before x in the $\mathscr{B}$-order and the distance between x and y is strictly less than d. The *winner* of the game $G(\mathscr{B}, d)$ is the player who makes the last legal move. From the greedy algorithm we get the following:

(i) If $g(x)=0$ and the move from x to y is a legal move, then $g(y) \neq 0$. (This is so because all binary n-tuples y which come before x in the $\mathscr{B}$-order and which satisfy $g(y)=0$ have distance at least d to x.)

(ii) If $g(x) \neq 0$, then there is some y which comes before x in the $\mathscr{B}$-order and which satisfies $g(y)=0$ such that the move from x to y is a legal move.

As a consequence, the winning positions of this game are the positions y with $g(y)=0$ and a winning strategy is always to move from a position x with $g(x) \neq 0$ to a position y with $g(y)=0$. The Grundy number [1] of a position x equals $g(x)$ as computed by the greedy algorithm. This is because the Grundy number of x equals the smallest integer not equal to the Grundy number of any position z for which the move from x to z is legal, that is, the smallest integer a such that the distance from x to all earlier positions z with Grundy number a is at least d. But this is the way the g-values are computed by the greedy algorithm.

3. Triangular-Greedy Codes

In this section we consider special properties of greedy codes corresponding to a triangular ordered basis, that is, triangular-greedy codes. Triangular-greedy codes of designed distance d have minimum distance exactly d, and so we omit the word designed. We first show that triangular-greedy codes of even distance contain only even weight vectors. This property is not satisfied by all greedy codes of even designed distance. For example, if $n=3$, $d=2$, and $\mathscr{B}$ is the ordered basis $(1, 1, 1)$, $(0, 0, 1)$, $(0, 1, 0)$, then the $\mathscr{B}$-greedy code is $\{(0, 0, 0), (1, 1, 1)\}$.

Theorem 3.1. *A triangular-greedy code of positive even distance contains only even weight vectors.*

Proof. Let $y_1, y_2, ..., y_n$ be a triangular ordered basis $\mathscr{B}$ of F_2^n and let d be a positive even integer. We prove by induction on n that the $\mathscr{B}$-greedy code C of distance d has only even weight vectors.

If $n=1$, then the greedy code obtained contains only the zero vector. A triangular order of F_2^n has the property that the vectors with leftmost coordinate equal to 0 precede those with leftmost coordinate equal to 1. Since $y_1, ..., y_{n-1}$ is an ordered basis of $(0, F_2^{n-1})$ (F_2^{n-1} with an appended leftmost coordinate equal to 0), it follows by induction that $C \cap (0, F_2^{n-1})$

has only even weight vectors. Suppose that $z=(1, z')$ is an odd weight vector in C. Then z' has even weight and

$$\operatorname{dist}((0, z'), C \cap (0, F_2^{n-1})) \geqslant d-1.$$

Since d is even and since all vectors in $C \cap (0, F_2^{n-1})$ have even weight, this implies that

$$\operatorname{dist}((0, z'), C \cap (0, F_2^{n-1})) \geqslant d.$$

Hence $(0, z') \in C$ which is a contradiction since $\operatorname{dist}((0, z'), (1, z')) = 1 < d$. ▮

COROLLARY 3.2. *Let $y_1, y_2, ..., y_n$ be a triangular ordered basis $\mathscr{B}$ of F_2^n and let d be an odd integer. Let $\mathscr{B}'$ be the triangular ordered basis of F_2^{n+1} defined by*

$$y_1' = (0, ..., 0, 1),\ y_2' = (y_1, \varepsilon_1), ..., y_{n+1}' = (y_n, \varepsilon_n),$$

where each ε_i equals 0 or 1. Then the $\mathscr{B}'$-greedy code C' of distance $d+1$ is obtained from the $\mathscr{B}$-greedy code of distance d by adding an overall parity check bit as a rightmost coordinate.

Proof. If $x_1, x_2, ..., x_{2^n}$ is the $\mathscr{B}$-order of F_2^n, then in the $\mathscr{B}'$-order of F_2^{n+1}, $(x_i, 1)$ follows $(x_i, 0)$ or vice versa. The corollary now follows by an easy induction using Theorem 3.1 and the fact that for $\varepsilon = 0$ or 1, $\operatorname{dist}(x, y) \geqslant d$ if and only if

$$\max\{\operatorname{dist}((x, \varepsilon), (y, 0)), \operatorname{dist}((x, \varepsilon), (y, 1))\} \geqslant d+1. \quad ▮$$

Special cases of Corollary 3.2 are: (1) $(\varepsilon_1 = \varepsilon_2 = \cdots = \varepsilon_n = 0)$ the lexicodes of even distance $d+1$ are obtained from the lexicodes of odd distance d by adding an overall parity check as a rightmost coordinate [3], (2) $(\varepsilon_1 = 1, \varepsilon_2 = \cdots = \varepsilon_n = 0)$ the Gray-greedy codes of even distance $d+1$ are obtained from the Gray-greedy codes of odd distance d by adding an overall parity check as a rightmost coordinate, and (3) $(\varepsilon_1 = \varepsilon_2 = \cdots = \varepsilon_n = 1)$ the complementary codes of even distance $d+1$ are obtained from the complementary codes of odd distance d by adding an overall parity check as a rightmost coordinate.

Let $y_1, y_2, ..., y_n$ be a triangular ordered basis $\mathscr{B}$ of F_2^n and let d be an integer. As shown in the proof of Theorem 2.2, the greedy algorithm constructs a nested sequence of codes

$$C_0 = \{0\} \subseteq C_1 \subseteq \cdots \subseteq C_n = C.$$

The subspace V_i equals F_2^i with $n-i$ 0's appended to each vector, and we henceforth identify V_i with F_2^i. Thus we may consider C_i as a code in F_2^i, in which case C_i is a shortened C_j for $i<j$. The code C_i has covering radius at most $d-1$, that is, each vector in F_2^i has distance $d-1$ or less to some vector in C_i.

LEMMA 3.3. *For a triangular ordered basis*

$$\dim C_{i+1} \leqslant 1+\dim C_i$$

with equality if and only if C_i *has covering radius* $d-1$. *If* $\dim C_{i+1} = \dim C_i$ *then the covering radius of* C_{i+1} *is one more than the covering radius of* C_i.

Proof. The lemma is an immediate consequence of the greedy algorithm. ∎

COROLLARY 3.4. *Every triangular-greedy code of length* n *and distance* $d=2$ *equals the set of all even weight vectors of* F_2^n.

Proof. By Theorem 3.1 each C_i contains only even weight vectors. Hence $C_i \neq F_2^i$ for $i \geqslant 1$. By Lemma 3.3, $\dim C_{i+1} = 1+\dim C_i$ $(i \geqslant 1)$. Hence $\dim C_n = n-1$ and the corollary follows. ∎

A lower bound for the dimension of triangular-greedy codes is given in the next theorem. From the data presented at the end of this paper, this lower bound, based on worst case analysis, appears to be weak.

THEOREM 3.5. *Let* n *and* d *be integers with* d *even satisfying* $4 \leqslant d \leqslant n$. *Let* C *be a triangular-greedy code of length* n *and distance* d. *If* $d \leqslant n < 3d/2$, *then* $\dim C = 1$. *If* $n = 3d/2$, *then* $\dim C = 2$. *If* $n > 3d/2$, *we have*

$$\dim C = n-2-\lfloor \log_2(n-1) \rfloor, \qquad \textit{if} \quad d=4$$

(*in this case* C *is an extended Hamming code or a shortened extended Hamming code*)

$$\dim C \geqslant \begin{cases} \left\lfloor \dfrac{4n-d-12}{2d-4} \right\rfloor, & \textit{if} \quad d \equiv 0 \bmod 4, \qquad d \neq 4, 8, \\[2ex] \left\lfloor \dfrac{n}{3} \right\rfloor, & \textit{if} \quad d=8 \quad \textit{and} \quad n > 18, \\[2ex] \left\lfloor \dfrac{4n-d-14}{2d-4} \right\rfloor, & \textit{if} \quad d \equiv 2 \bmod 4. \end{cases}$$

(*If* $d=8$ *and* $n \leqslant 18$, *the exact value of the dimension of* C *is given in Table* II.)

Proof. The assertions for $d \leqslant n \leqslant 3d/2$ are easily checked. If $n = 3d/2$ then the code C is the unique (up to equivalence) code of length $3d/2$ and minimum distance d and it has covering radius $\lfloor 3d/4 \rfloor$. The covering radius of a code of even minimum distance d is at least $d/2+1$ unless the code is extended perfect (in which case $d = 4$ or 8 and the covering radius is $d/2$). First assume that $d \neq 4, 8$. According to Lemma 3.3 by the time we get to $C_{3d/2+\lfloor d/4 \rfloor}$ we will have increased the dimension by 1. After that it takes at most $(d/2)-1$ steps to increase the dimension. Hence the dimension of the greedy code $C = C_n$ is at least $k+3$ where k is the largest integer such that

$$\frac{3d}{2} + \left\lfloor \frac{d}{4} \right\rfloor + k\left(\frac{d}{2} - 1\right) \leqslant n,$$

from which the inequalities for $d \neq 4$ in the theorem follow.

If $d = 8$, it is not difficult to show that all triangular-greedy codes of length 16 are equivalent, in fact they are equivalent to the first order Reed–Muller code $R(1, 4)$ which has covering radius 6. Hence all triangular-greedy codes of distance 8 and length 18 have dimension 6. By an argument similar to the above we find that $\dim(C) \geqslant \lfloor n/3 \rfloor$ if $n > 18$. (In case the code C_{24} is the extended binary Golay code then one extra step may be necessary to increase the dimension. But since the dimension of the Golay code is 12, the calculation still holds.)

If $d = 4$, the codes $C_4, C_8, ..., C_{2^t}$ $(t = \log_2(n-1))$ are extended Hamming codes in which case we must adjust the above calculation using the fact that the extended Hamming codes have covering radius 2. The dimension is as given in the theorem. ∎

In the case of triangular-greedy codes of distance $d \geqslant 2$, we can view the greedy algorithm as an algorithm for the construction of the g-parity check matrix H of a code C of distance d. The columns of H (the g-values of the unit vectors) can be constructed by the following recursive algorithm.

Algorithm for a g-Parity Check Matrix. Let

$$H_1 = [1],$$

the parity check matrix for C_1. Suppose a parity check matrix

$$H_i = [h_i \cdots h_1]$$

of size m_i by i has been constructed for C_i (whose columns are the g-values of the unit vectors in F_2^i). Consider

$$y_{i+1} = (\varepsilon_{i+1} = 1, \varepsilon_i, ..., \varepsilon_1).$$

Let β be the smallest integer such that

$$h_{i+1}=\beta \oplus (\varepsilon_i h_i \oplus \cdots \oplus \varepsilon_1 h_1) \tag{14}$$

is not a sum of fewer than $d-1$ columns of H_i. (Here we must allow the empty sum and hence $h_{i+1} \neq 0$.) We then let

$$H_{i+1}=[h_{i+1} h_i \cdots h_1]. \tag{15}$$

In the algorithm if $\beta < 2^{m_i}$ then H_{i+1} has the same number m_i of rows as H_i. Otherwise $\beta = 2^{m_i}$ and then H_{i+1} (using actual column vectors and not integers) is obtained from H_i by redefining h_j using

$$h_j \leftarrow \begin{bmatrix} 0 \\ h_j \end{bmatrix} \qquad (j=1, ..., i),$$

and then defining H_{i+1} by (15) using the new h_j's and using the identification of β with the m_i+1-tuple

$$\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

THEOREM 3.6. *The algorithm for a g-parity check matrix correctly computes the g-parity check matrix of a triangular-greedy code of distance* $d \geq 2$.

Proof. We prove by induction on i that the code C_i with parity check matrix H_i is the same as the code constructed by the greedy algorithm. If i is such that $\beta = 2^{m_i}$ then the covering radius of C_i is less than $d-1$ and the conclusion follows from Lemma 3.3. Suppose that $\beta < 2^{m_i}$. Then the covering radius of C_i is $d-1$. Consider C_i to be embedded in C_{i+1} with leftmost coordinate equal to 0. Then C_{i+1} has minimum distance d since h_{i+1} is not the sum of fewer than $d-1$ columns of H_i. The vector y_{i+1} has the same syndrome β as each vector x in C_i^{β} and hence $\text{dist}(x, y_{i+1}) \geq d$. Since in both algorithms β is chosen to be minimum, C_{i+1} is the same as the code constructed by the greedy algorithm. ∎

For the lexicodes, $y_{i+1}=e_{i+1}$ and hence by (14), $h_{i+1}=\beta$. In this case the above algorithm for constructing the g-parity check matrix H is an algorithm for constructing Grundy numbers of heap games (see [1]). Assume that $d=3$. Then in the algorithm, h_{i+1} is the smallest integer such that $h_{i+1} \neq h_1, ..., h_i$. Hence it follows by the induction that $h_i = i$ for all i. That the Grundy numbers for $d=3$ satisfy $g(i)=i$ is a well known fact [1, p. 433].

The g-values of the unit vectors for the Gray-greedy code with $d=3$ are given in the next theorem.

THEOREM 3.7. *Let $y_1, ..., y_n$ be the Gray ordered basis $\mathscr{B}$ of F_2^n and let $d=3$. Then $g(e_i)$ is the ith integer in the Gray order and hence the columns of the g-parity check matrix from right to left are the first n integers in the Gray order.*

Proof. We have $y_{i+1} = e_{i+1} \oplus e_i$. Assume that $d=3$. Then in the algorithm for a g-parity check matrix

$h_{i+1} = \beta \oplus h_i$ where β is the smallest integer such that $\beta \oplus h_i \neq h_1, ..., h_i$. (*)

We now show that starting with $h_0 = 0$ the above algorithm generates nonnegative integers in Gray order which will complete the proof of the theorem. Suppose that $i+1 = 2^r$ for some r. Then by induction $h_i = 2^{r-1}$. Thus $h_{i+1} = 2^r \oplus 2^{r-1}$ which is the $(i+1)$st integer in Gray order. Now suppose that $2^r < i+1 < 2^{r+1}$. By induction $h_0, h_1, ..., h_{2^r-1}$ are the first 2^r nonnegative integers in Gray order and $h_j = y_{r+1} \oplus h_{j-2^r}$ for $2^r \leqslant j \leqslant i$. The smallest β such that

$$\beta \oplus h_i (= \beta \oplus y_{r+1} \oplus h_{i-2^r}) \neq h_0, h_1, ..., h_i$$

is less than 2^r, and hence equals the smallest integer such that

$$\beta \oplus h_{i-2^r} \neq h_0, h_1, ..., h_{i-2^r}.$$

Hence $h_{i+1} = y_{r+1} \oplus h_{i+1-2^r}$ which is the $(i+1)$st number in Gray order. ▮

The proof of Theorem 3.7 contains an apparently new algorithm for generating the binary n-tuples in reflected Gray code order. The ith integer in Gray order can be shown to be the integer

$$i \oplus \left[\frac{i}{2}\right].$$

For the lexicode and the Gray-greedy code, if the distance d is odd, then the Grundy numbers of the unit vectors $e_n, ..., e_1$ of F_2^n determine the Grundy numbers of the unit vectors $e'_{n+1}, ..., e'_1$ of F_2^{n+1} for distance $d+1$ in a very simple way. The following theorem is equivalent to the Mock Turtles theorem [1, 3].

THEOREM 3.8. *Let H be the g-parity check matrix for the lexicode C of length n and odd distance d. Then the g-parity check matrix for the lexicode C' of length $n+1$ and distance $d+1$ is*

TABLE II

Dimensions of Gray-Greedy Codes Compared to Lexicodes and Complementary Greedy Codes

$n:d$	4	6	8	10	12
4	1	0	0	0	0
5	1	0	0	0	0
6	2	1	0	0	0
7	3	1	0	0	0
8	4	1	1	0	0
9	4	2	1	0	0
10	5	2	1	1	0
11	6	3	1	1	0
12	7	4	2	1	1
13	8	4	2	1	1
14	9	5	3	1	1
15	10	6	4	2	1
16	11	7	5	2	1
17	11	8[7]	5	2	1
18	12	9[8]	6	3	2
19	13	9	7	3	2
20	14	10	8	4	2
21	15	11	9	5	3
22	16	12	10	5	3
23	17	13(12)	11	6	4
24	18	13	12	7(6)[6]	5
25	19	14	12	7	5
26	20	15	12	8	6
27	21	16	12	9	7
28	22	17	13	9	7
29	23	18	13	10	8
30	24	19	14	11	8
31	25	20(19)[19]	15	12	9
32	26	20	16	12	10
33	26	21	16	13	10(11)[11]
34	27	22	17	14	
35	28	23	18	14	
36	29	24	19	15	
37	30	25	20	16	
38	31	26	21	17	
39	32	27	22	17[18]	
40	33	28(27)	23	18	

$$H' = \begin{bmatrix} & H & & 0 \\ & & & \vdots \\ & & & 0 \\ \delta_n & \cdots & \delta_1 & 1 \end{bmatrix},$$

where the δ_i are chosen so that each column of H' contains an odd number of 1's.

Proof. First note that H' is a parity check matrix for C', since by Corollary 3.2, C' can be obtained from C by adding an overall parity check bit as a rightmost coordinate and the sum of the rows of H' is the all 1's vector. That H' is the g-parity check matrix of C' follows by an easy induction using the algorithm for a g-parity check matrix. ▮

In terms of Grundy numbers, Theorem 3.8 says the following: For d odd, the Grundy numbers of $e'_{n+1}, ..., e'_1$ for distance $d+1$ can be computed using ordinary integer arithmetic from the Grundy numbers of $e_n, ..., e_1$ for distance d as

$$g(e'_1) = 1$$
$$g(e'_{i+1}) = 2g(e_i) + \delta_i \qquad (i = 1, ..., n-1),$$

where $\delta_i = 0$ if $g(e_i)$ has an odd number of binary bits equal to 1 and $\delta_i = 1$ otherwise.

If in Theorem 3.8 we use the Gray-greedy code instead of the lexicode, then all the $\delta_i = 1$. In this case we get

$$g(e'_1) = 1$$
$$g(e'_{i+1}) = 2g(e_i) + 1 \qquad (i = 1, ..., n-1),$$

In Table II we give the dimensions of the Gray-greedy codes of length $n \leqslant 40$ for even distance $d \leqslant 10$, and of length $n \leqslant 33$ for $d = 12$. Numbers in round brackets are the dimensions of the lexicode when they differ from those for the Gray-greedy code, and the numbers in square brackets are those for the complementary code when they differ from those for the Gray-greedy code. The dimensions for the lexicodes for $d = 4, 6, 8, 10$ are given in Table VII of [3].

By Table II both the Gray-greedy code and the complementary greedy code of length 24 and distance 8 have dimension 12, and hence by [5, Theorem 100, p. 172] are the extended binary Golay codes, as is the lexicode in this case. Notice that the Gray-greedy code is always at least as good as the lexicode, and with one exception is always at least as good as the complementary code. The complementary greedy code is sometimes better and sometimes worse than the lexicode. The dimensions of the lexicodes for $d = 12$ are not computed in [3], but we computed them in order to make the comparison given in Table II.

We note that the dimensions of the Gray-greedy codes computed in Table II are progressively better than the bound given in Theorem 3.5. We do not know whether all triangular-greedy codes of length 24 and designed distance 8 equal the extended binary Golay code. We also note that all three triangular-greedy codes have the same dimension for those lengths computed when d is divisible by 4. But there are several values of $n > 60$ for which computation showed that the Gray-greedy code is better than the complementary greedy code when $d = 8$.

Comparing Table II with Table I in [6], we see that Gray-greedy codes are surprisingly good. In fact in the common range of both tables, the Gray-greedy codes have dimension at most 1 less than the dimension of the best codes known.

ACKNOWLEDGMENT

The data given in Table II and elsewhere were computed by Jesse Nemoyer to whom we are very grateful.

REFERENCES

1. E. R. BERLEKAMP, J. H. CONWAY, AND R. K. GUY, "Winning Ways," Vols. 1, 2, Academic Press, New York, 1982.
2. J. H. CONWAY, Integral lexicographic codes, *Discrete Math.* **83** (1990), 219–235.
3. J. H. CONWAY AND N. J. A. SLOANE, Lexicographic codes: Error-correcting codes from game theory, *IEEE Trans. Inform. Theory* **32** (1986), 337–348.
4. J. VAN LINT, "Introduction to Coding Theory," Springer-Verlag, New York, 1982.
5. V. PLESS, "Introduction to the Theory of Error Correcting Codes," 2nd ed., Wiley, New York, 1989.
6. T. VERHOEFF, An updated table of minimum-distance bounds for binary linear codes, *IEEE Trans. Inform. Theory* **33** (1987), 665–680.
7. V. I. LEVENŠTEĬN, A class of systematic codes, *Soviet Math. Dokl.* **1**, No. 1 (1960), 368–371.