Greedy Generation of Non-Binary Codes

by Laura Monroe and Vera Pless

Department of Mathematics, Statistics, and Computer Science
University of Illinois at Chicago
Chicago, IL 60607

We get a B-ordering of all binary n-tuples $\mathbf{V}_n$ by choosing an ordered basis $\{y_1,...,y_n\}$ of V_n and ordering the n-tuples as follows: 0, y_1, y_2, y_2+y_1, y_3, y_3+y_1, y_3+y_2, $y_3+y_2+y_1$, y_4,... Given a minimum distance d, choose a set of vectors $\mathbf{S}$ with the zero vector first, then go through the vectors in their B-ordering and choose the next vector which has distance d or more from all vectors already chosen. The surprising result that $\mathbf{S}$ is linear has been shown in several different ways [1, 2, 3, 4, 6]. Linear codes found in this fashion are called greedy codes.

An ordered basis $\{y_i\}$ of $\mathbf{V}_n$ is called triangular [1] if $y_i = (0,..., 0, 1, *,..., *)$, with the 1 in the ith position. When the y_i are unit vectors, the order is the lexicographic order. The columns $\mathbf{h}_n, \mathbf{h}_{n-1},...\mathbf{h}_1$ of the g-parity check matrix $\mathbf{H}_n$ are constructed one by one. We associate numbers with their binary representations. We let $\mathbf{h}_1$ be the number 1. Let $y_{i+1} = (0,..., 0, 1, \varepsilon_i,..., \varepsilon_1)$, where the ε_i are 0 or 1. If $\mathbf{H}_i = [\mathbf{h}_i,...\mathbf{h}_1]$ is known, we let β be the smallest number so that $\mathbf{h}_{i+1} = \beta + (\varepsilon_i\mathbf{h}_i + ...+\varepsilon_1\mathbf{h}_1)$ is not a sum of d-1 or fewer columns of $\mathbf{H}_i$. Then $\mathbf{H}_{i+1} = [\mathbf{h}_{i+1},...\mathbf{h}_1]$. Each $\mathbf{H}_i$ is a parity check matrix of the greedy code chosen using the ordered basis $\{y_1,...,y_i\}$ [1]. Further, the syndrome of any vector with regard to $\mathbf{H}_i$ is the g-value which is assigned to it by generalizing the greedy algorithm for choosing vectors in the code, hence the name g-parity check matrix.

The non-binary case has also aroused quite a bit of interest. One may generalize the concept of B-ordering to the case of an arbitrary base field. For example, in the case $\mathbf{GF}(4) = \{0, 1, \omega, \underline{\omega}\}$, the B-ordering is generated by choosing an ordered basis $\{y_1,...,y_n\}$ of V_n and ordering the n-tuples as follows: 0, y_1, ωy_1, $\underline{\omega} y_1$, y_2, y_2+y_1, $y_2+\omega y_1$, $y_2+\underline{\omega} y_1$, ωy_2, ωy_2+y_1, $\omega y_2+\omega y_1$, $\omega y_2+\underline{\omega} y_1$, $\underline{\omega} y_2$, $\underline{\omega} y_2+y_1$, $\underline{\omega} y_2+\omega y_1$ $\underline{\omega} yy_2\underline{\omega} y_1$,... The greedy code is then generated from the B-ordering as in the binary case. It has been shown by Conway and Sloane in the case of lexicodes [2], and independently by Fon-Der-Flaass [3], and Van Zanten [6] in the case of general greedy codes that those codes for which the base field is of order 2^{2^a} is linear. When the base field is not of order 2^{2^a}, the situation is a little less clear. In general, the greedy codes generated in this case have been linear only for small n. In every case examined, linearity breaks down at some point early in the generation of the code. It is possible, however, to extend the parity check matrix generating algorithm to this case. Although this algorithm does not produce the greedy code itself, it still produces a very good code which is generated in a greedy-like fashion.

The parity check matrix is generated in the same way as in the binary case. This algorithm also assumes that the ordered basis $\{y_i\}$ of $\mathbf{V}_n$ being used is triangular, and that the first non-zero entry in each basis vector is 1. Then if $\mathbf{H}_i = [\mathbf{h}_i,...\mathbf{h}_1]$ is known, we let β be the smallest number so that $\mathbf{h}_{i+1} = \beta + (\varepsilon_i\mathbf{h}_i + ...+\varepsilon_1\mathbf{h}_1)$ is not a linear combination of d-1 or fewer columns of $\mathbf{H}_i$. Then $\mathbf{H}_{i+1} = [\mathbf{h}_{i+1},...\mathbf{h}_1]$.

Many interesting codes are generated via the parity check algorithm. We have generated many such parity check matrices via the computer for base fields of orders 3, 4, and 5. In all examined cases, the codes generated have had dimension within 1 of the best known codes, for a given n and d, and most of the codes generated had dimension equal to that of the best known codes. Better yet, we have generated more than 100 record breaking codes over the base field of order 4 [5]. Most of these are shortened codes of larger greedy codes. The following table lists the parameters of the codes from which the shortened codes are derived.

Table. Parameters of record breaking codes over **GF**(4) obtained via the parity check matrix algorithm.

n	k	d
52	44	5
128	118	5
35	26	6
71	60	6

This work was supported in part by NSA grant MDA 904-91-H-0003.

REFERENCES

1. R. A. Brualdi and V. Pless, *Greedy Codes*, JCT(A) 64 (1993), 10-30.

2. J. H. Conway and N. J. A. Sloane, *Lexicographic Codes: Error Correcting Codes from Game Theory*, IEEE Trans. Inform. Theory IT-32 (1986), 337-348.

3. D. Fon-Der-Flaass, *A Note on Greedy Codes,* to appear.

4. L. Monroe, *Binary Greedy Codes*, to appear in Congressus Numerantium, vol.100-104.

5. N. J. A. Sloane, *Table of Lower Bounds on dmax (n, k) for Linear Codes over Fields of Order 4*, The Handbook of Coding Theory, edited by R. A. Brualdi, C. Huffman, and V. Pless, published by Elsevier Science Publishers, to appear.

6. A. J. van Zanten, *Lexicodes Over Fields of Characteristic 2,* to appear.