(26.2.92 Preprint of paper to appear in a special issue of *Discrete Mathematics*)

LINEAR CODES WITH COMPLEMENTARY DUALS

James L. MASSEY
Signal and Information Processing Laboratory
Swiss Federal Institute of Technology
CH-8092 Zürich, Switzerland

Abstract: A linear code with a complementary dual (or an LCD code) is defined to be a linear code C whose dual code $C^{\perp}$ satisfies $C \cap C^{\perp} = \{\mathbf{0}\}$. The algebraic characterization of LCD codes is given, and it is shown that asymptotically good LCD codes exist. LCD codes are shown to provide an optimum linear coding solution for the two-user binary adder channel. The nearest-neighbor (or maximum-likelihood) decoding problem for LCD codes is shown to reduce to the problem: given a word in $C^{\perp}$, find the nearest codeword in C.

§ 1. Introduction

When introducing the dual code $C^{\perp}$ of a linear code C in his excellent textbook on coding theory, J. H. van Lint is quick to warn the reader to "be careful not to think of $C^{\perp}$ as an orthogonal complement in the sense of vector spaces over $\mathbb{R}$. In the case of a finite field Q, the subspaces C and $C^{\perp}$ can have an intersection larger than $\{\mathbf{0}\}$ and in fact they can even be equal" [2, p. 34]. The purpose of this paper is to explore the fate that awaits one who, daring to ignore this sage advice, chooses to consider only those linear codes C for which the dual code $C^{\perp}$ can be thought of as a genuine orthogonal complement, i.e., for which $C \cap C^{\perp} = \{\mathbf{0}\}$. To have a name for the subject of our investigation, we will say that C is a *linear* code with a *complementary dual* (or an *LCD code* for short) just in case C is a linear code for which $C \cap C^{\perp} = \{\mathbf{0}\}$. Of course, if C is an LCD code, then so also is $C^{\perp}$ because $(C^{\perp})^{\perp} = C$.

In Section 2, we give the algebraic characterization of LCD codes. In Section 3, we show that asymptotically good LCD codes exist, but we stop short of showing that LCD codes achieve the Varshamov-Gilbert Bound. Section 4 is devoted to showing the practical utility of LCD codes, first by showing that such codes provide an optimum linear coding solution for the two-user binary adder channel, then by showing that the nearest-codeword (or maximum-likelihood) decoding problem for an LCD code reduces to a problem that is apparently simpler than for a general linear code.

§ 2. Characterization of Codes with Complementary Duals

Recall that an (n, k) F-ary *linear code* C is just a k-dimensional subspace of the n-dimensional vector space F^n of n-tuples with components in the field F. As most of what we will say does not require that F be a finite field, we will not yet impose this restriction. Recall also that a *generator matrix* for the (n, k) linear code C is any matrix whose rows are a basis for C. Recall finally that the vectors **u** and **v** in F^n are said to be *orthogonal* if $\mathbf{u}\mathbf{v}^T = \mathbf{0}$ and that, if C is an (n, k) F-ary linear code, the *dual code* $C^\perp$ is the (n, n - k) linear F-ary code consisting of all vectors **v** that are orthogonal to every vector **u** in C.

It is immediate that C is a linear code with a complementary dual (or LCD code) just when

$$F^n = C \oplus C^\perp, \tag{1}$$

i.e., just when F^n is the direct sum of C and $C^\perp$ or, equivalently, just when every vector in F^n can be written uniquely as the sum of a vector in C and a vector in $C^\perp$. This follows from the fact that the n - k vectors in a basis for $C^\perp$, when adjoined to a basis for C, yield a set of n linearly independent vectors (and hence a basis for F^n) if and only if $C \cap C^\perp = \{\mathbf{0}\}$. It follows that the *orthogonal projector* Π_C from F^n onto C, i.e., the linear mapping from F^n onto C such that

$$\mathbf{v}\Pi_C = \begin{cases} \mathbf{v} & \text{if } \mathbf{v} \in C \\ \mathbf{0} & \text{if } \mathbf{v} \notin C^\perp \end{cases}$$

exists if and only if C is an LCD code.

The following rather trivial proposition gives a complete characterization of LCD codes.

Proposition 1: If G is a generator matrix for the (n, k) linear code C, then C is an LCD code if and only if the $k \times k$ matrix GG^T is nonsingular. Moreover, if C is an LCD code, then $\Pi_C = G^T(GG^T)^{-1}G$ is the orthogonal projector from F^n onto C.

Proof: Suppose that GG^T is nonsingular. Then if $\mathbf{v} \in C$, i.e., if $\mathbf{v} = \mathbf{u}G$ for some $\underline{u}$, it follows that

$$\mathbf{v}G^T(GG^T)^{-1}G = \mathbf{u}GG^T(GG^T)^{-1}G$$

$$= \mathbf{u}G = \mathbf{v}.$$

Moreover, if $\mathbf{v} \in C^\perp$, i.e., if $\mathbf{v}G^T = \mathbf{0}$, it follows that

$$\mathbf{v}G^T(GG^T)^{-1}G = \mathbf{0}(GG^T)^{-1}G = 0.$$

Thus $G^T(GG^T)^{-1}G$ is indeed the orthogonal projector Π_C and hence C must be an LCD code.

Conversely, suppose that GG^T is singular. Then there is a non-zero vector

u in F^k such that $\mathbf{u}GG^T = \mathbf{0}$. Now **u**G is a non-zero vector in C. But an arbitrary vector **v** in C can be written as **v** = **u**'G for some **u**' in F^k so that

$$(\mathbf{u}G)\mathbf{v}^T = (\mathbf{u}G)\,(\mathbf{u}'G)^T = \mathbf{u}GG^T(\mathbf{u}')^T = \mathbf{0}(\mathbf{u}')^T = 0$$

and hence **u**G is also a vector in $C^{\perp}$. It follows that $C \cap C^{\perp} \neq \{\mathbf{0}\}$, i.e., that C is not an LCD code. ❒

§ 3. Constructions of LCD Codes

When one restricts one's attention to any subclass of linear codes, an important first question is whether the subclass is rich enough to contain asymptotically good codes. In this section, we provide a positive answer to this question for LCD codes by showing how to modify an arbitrary (n, k) linear code to produce an LCD code whose minimum Hamming distance is at least as great. We recall that every linear code is equivalent (up to a permutation of the coordinates of the codewords) to a linear code having a generator matrix in the *standard form* $G = [I_k : P]$ where I_k denotes the $k \times k$ identity matrix [2, p. 33], so that one entails no loss of essential generality if one considers only generator matrices in standard form.

Proposition 2: Let $G = [I_k : P]$ be the generator matrix of an F-ary (n, k) linear code with minimum Hamming distance d_{min} where F is a field with characteristic 2. Then

$$G' = [I_k : P \ : P]$$

is the generator matrix of an F-ary (2n - k, k) LCD code C' with minimum distance $d'_{min} \geq d_{min}$.

Proof:
$$G'(G')^T = I_k + PP^T + PP^T$$
$$= I_k$$

as follows from the fact that F has characteristic 2. That C' is an LCD code now follows immediately from Proposition 1. The other claims of the proposition are trivial. ❒

The generalization of Proposition 2 to fields with prime characteristic p, $p \neq 2$, is easy when -1 is a quadratic residue modulo p [2, pp. 12-13], i.e., when there is an element α in the finite field of p elements such that $\alpha^2 = -1$. One simply chooses

$$G' = [I_k : P : \alpha P]$$

and Proposition 2 goes through unchanged. For general p, however, we require a theorem of Lagrange [2, p. 302], which states that every positive integer (and in particular every prime) can be written as the sum of four squares (some of which

may be repeated or may be zero). If

$$p = \alpha^2 + \beta^2 + \gamma^2 + \delta^2,$$

where now we consider α, β, γ and δ to be elements of the finite field of p elements, then the choice

$$G' = [I_k : \alpha P : \beta P : \gamma P : \delta P] \qquad (2)$$

gives a generator matrix in standard form for which

$$G'(G')^T = I_k$$

and hence which describes an LCD code. That $d'_{min} \geq d_{min}$, where d_{min} is the minimum Hamming distance of the code with generator matrix $G = [I_k : P]$, follows from (2) and the fact that at least one (in fact, at least two) of the elements α, β, γ and δ must be non-zero. We have proved the following proposition.

Proposition 3: For any F-ary (n, k) code C with minimum Hamming distance d_{min} where F is a field with prime characteristic p, there exists a corresponding (5n - 4k, k) LCD code C' with minimum Hamming distance $d'_{min} \geq d_{min}$.

The asymptotic goodness of LCD codes now follows trivially from that of general linear codes. We content ourselves with this indirect demonstration of the existence of asymptotically good LCD codes and leave open the interesting question of whether LCD codes can achieve the asymptotic Varshamov-Gilbert bound [2, pp. 56-57].

§ 4. Utility of LCD Codes

We have yet to demonstrate any practical utility for LCD codes. We now give one application, coding for the noiseless two-user binary adder channel (2-BAC), and suggest a much more interesting potential application.

If the two users of the 2-BAC send the binary n-tuples **u** and **v**, then the received sequence **r** is the digit-by-digit real sum of **u** and **v**, which we denote by $\mathbf{r} = \mathbf{u} + \mathbf{v}$ to distinguish it from the usual componentwise modulo-two sum that we now write as $\mathbf{u} \oplus \mathbf{v}$. Peterson and Costello [3] have shown that if users 1 and 2 employ linear (n, k_1) and (n, k_2) codes C_1 and C_2, respectively, then **r** cannot be uniquely decoded to **u** and to **v** if $k_1 + k_2 > n$. Thus, unique decodability implies $k_1 + k_2 \leq n$. But choosing C_1 to be an LCD (n, k) code C and choosing $C_2 = C^{\perp}$ gives a uniquely decodable code with $k_1 + k_2 = k + (n - k) = n$, the best possible. To decode, one simply forms the binary n-tuple $\mathbf{r}' = \mathbf{u} \oplus \mathbf{v}$ by taking the components of **r** modulo 2. Applying the orthogonal projector Π_C (cf. Proposition 1) to **r'** gives $\mathbf{r}'\Pi_C = \mathbf{u}$, and **v** is then obtained by subtracting **u** from **r'**.

The above simple construction of optimal codes for the 2-BAC with a very simple decoding algorithm suggests some practical utility for LCD codes. A much

more intriguing prospect, however, is incorporated in the following proposition, which suggests that the nearest-codeword (or maximum-likelihood) decoding problem for an LCD code may be simpler than that for a general linear code.

Proposition 4: Let C be an (n, k) LCD F-ary code and let φ be a mapping φ: $C^{\perp} \rightarrow C$ that maps each **u** in $C^{\perp}$ to (one of) the closest codeword(s) **v** in C. Then the mapping φ such that

$$\varphi(\mathbf{r}) = \mathbf{r}\Pi_C + \varphi(\mathbf{r}\Pi_{C^{\perp}})$$

maps each **r** in F^n to (one of) the closest codeword(s) **v** in C.

Proof: For each $\mathbf{r} \in F^n$, we wish to choose φ(**r**) as (one of) the codeword(s) **v** such that

$$\mathbf{r} = \mathbf{v} + \mathbf{e} \qquad (3)$$

gives an error pattern **e** with minimum Hamming weight. But

$$\mathbf{r} = \mathbf{r}\Pi_C + \mathbf{r}\Pi_{C^{\perp}} \qquad (4)$$

so that (3) gives

$$\mathbf{r}\Pi_{C^{\perp}} - (\mathbf{v} - \mathbf{r}\Pi_C) = \mathbf{e}.$$

This shows that the Hamming weight of **e** is also the Hamming distance between the word $\mathbf{u} = \mathbf{r}\Pi_{C^{\perp}}$ in $C^{\perp}$ and the codeword $\mathbf{v}' = (\mathbf{v} - \mathbf{r}\Pi_C)$ in C. Note that $\mathbf{v}' = (\mathbf{v} - \mathbf{r}\Pi_C)$ varies over all codewords in C as **v** varies over C. Thus, $\mathbf{e} = \mathbf{u} - \phi(\mathbf{u}) = \mathbf{r}\Pi_{C^{\perp}} - \varphi(\mathbf{r}\Pi_{C^{\perp}})$ provides a minimum weight solution for **e** in (3). The corresponding codeword is

$$\mathbf{v} = \mathbf{r} - \mathbf{r}\Pi_{C^{\perp}} + \varphi(\mathbf{r}\Pi_{C^{\perp}})$$

$$= \mathbf{r}\Pi_C - \varphi(\mathbf{r}\Pi_{C^{\perp}}),$$

where we have made use of (4). ❐

Proposition 4 shows that the nearest-codeword decoding problem for an LCD code C reduces to the apparently simpler problem: *given a word in* $C^{\perp}$, *find the nearest codeword in* C. The nearest-codeword decoding problem for a general linear code does not so reduce -- the decoding of self-dual codes where $C = C^{\perp}$ would be trivial if this reduction applied! It would be a happy outcome of this paper if it should lead an eminent coding theorist, e.g., J.H. van Lint, to discover a simple solution of this reduced nearest-codeword decoding problem for LCD codes.

Acknowledgement

The author gratefully acknowledges useful conversations on the topic of this paper with his colleagues Ueli Maurer and Thomas Mittelholzer.

References

[1] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers, 4th Ed.* (Oxford, London, 1965).

[2] J. H. van Lint, *Introduction to Coding Theory* (Springer, New York, 1982).

[3] R. Peterson and D. J. Costello, Jr., Binary Convolutional Codes for a Multiple Access Channel, *IEEE Trans. Inform. Theory* IT-25 (1979) 101-105.