Matrices of Varied Orthogonality and Their Codes
(Submitted for short presentation at ISIT'98.)

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

Abstract

Orthogonal matrices over arbitrary fields are defined together with their non-square analogs, which are termed row-orthogonal matrices. Antiorthogonal and self-orthogonal square matrices are introduced together with their non-square analogs. The relationships of these matrices to such codes as self-dual codes and linear codes with complementary duals are given.

1 Introduction

The aim of this paper is to define a number of different types of matrices over an arbitrary field that are similar to the familiar orthogonal matrices over the real field or to natural extensions of orthogonal matrices, then to show the relationships between these matrices and some familiar linear codes.

2 Orthogonal Matrices

Let $\mathcal{F}^n$ denote the vector space of n-tuples (or row vectors) with components in an arbitrary field $\mathcal{F}$. The *scalar product* of the vectors $\mathbf{u}$ and $\mathbf{v}$ is the field element $\mathbf{u}\mathbf{v}^T$, where here and hereafter the superscripted T denotes transposition. The vectors $\mathbf{u}$ and $\mathbf{v}$ are said to be *orthogonal* when $\mathbf{u}\mathbf{v}^T = 0$.

A square matrix $\mathbf{A}$ over $\mathcal{F}$ is said to be *orthogonal* if

$$\mathbf{A}\mathbf{A}^T = \mathbf{I},$$

where here and hereafter $\mathbf{I}$ denotes an identity matrix of appropriate dimension. Equivalently, $\mathbf{A}$ is orthogonal just when each row of $\mathbf{A}$ is orthogonal to every *other* row of $\mathbf{A}$ but has a scalar product of 1 with itself. Note that $\mathbf{A}$ is orthogonal just when $\mathbf{A}^T = \mathbf{A}^{-1}$, and hence $\mathbf{A}^T\mathbf{A} = \mathbf{I}$ so that $\mathbf{A}^T$ is also orthogonal. An orthogonal matrix is not only nonsingular but always has a determinant that is either $+1$ or -1 because $1 = \det(\mathbf{I}) = \det(\mathbf{A}\mathbf{A}^T) = \det(\mathbf{A})\det(\mathbf{A}^T) = (\det(\mathbf{A}))^2$. An example of an orthogonal matrix over the finite field GF(2) is

$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}.$$

Orthogonal matrices over the field $\mathcal{R}$ of real numbers are of great importance in the theory of isometries of $\mathcal{R}^n$, cf. [?].

It seems natural, for an in general non-square, matrix $\mathbf{A}$, to say that $\mathbf{A}$ is *row-orthogonal* if

$$\mathbf{A}\mathbf{A}^T = \mathbf{I},$$

as this is equivalent to the condition that each row of $\mathbf{A}$ is orthogonal to every *other* row of $\mathbf{A}$ but has a scalar product of 1 with itself. A row-orthogonal matrix always has full row rank and thus must have at least as many columns as rows. If $\mathbf{A}$ is row-orthogonal but nonsquare, then $\mathbf{A}^T$ cannot have full row rank and thus cannot also be row-orthogonal. Deleting rows of an orthogonal matrix gives a row-orthogonal matrix, but not every row-orthogonal matrix can be so constructed. For instance, over the field GF(2), the matrix $\mathbf{A} = [1\ 1\ 1]$ is trivially row-orthogonal but there is no orthogonal matrix having $[1\ 1\ 1]$ as a row.

3 Antiorthogonal Matrices

The notion of an "anticode" was introduced by P. G. Farrell [?]. A "code" is usually designed to have a large minimum distance between its codewords. Because the opposite of "large minimum distance" is surely "small maximum distance," it was natural for Farrell to use the term *anticode* to describe a set n-tuples designed to have small maximum distance between its "codewords". [We note that sometimes anticodes are defined in such a manner that their "codewords" are all the n-tuples formed by linear combinations of the rows of some matrix, which need not have full row rank so that the "codewords" need not all be different.] The concept of an anticode has found numerous applications both in coding theory and in combinatorics, cf. pp. 548-556 in [?].

Inspired by Farrell's creative terminology, we seek to define an "antiorthogonal matrix" in an appropriate way. Because the opposite of $\mathbf{I}$ is surely $-\mathbf{I}$ [at least if we overlook fields of characteristic 2 for which $\mathbf{I} = -\mathbf{I}$], it seems natural to call a square matrix $\mathbf{B}$ *antiorthogonal* if

$$\mathbf{B}\mathbf{B}^T = -\mathbf{I},$$

i.e., if the rows of $\mathbf{B}$ are pairwise orthogonal but each row has a scalar product of -1 with itself. It follows that $\mathbf{B}$ is antiorthogonal if and only if $\mathbf{B}^{-1} = -\mathbf{B}^T$, and thus $\mathbf{B}^T\mathbf{B} = -\mathbf{I}$ so that $\mathbf{B}^T$ is also antiorthogonal. An example of an antiorthognal matrix over GF(3) is

$$\mathbf{B} = \left[\begin{array}{cc} 1 & 1 \\ 1 & 2 \end{array} \right].$$

In a field of characteristic 2, and only in such a field, $-1 = 1$ so that an antiorthogonal matrix is also an orthogonal matrix. Over the real field, the scalar product of a vector with itself is nonnegative, which implies that no antiorthogonal real matrices exist. However, if $\mathbf{A}$ is an orthogonal matrix and i is the imaginary number, then the complex matrix $\mathbf{B} = i\mathbf{A}$ is antiorthogonal.

We now relate antiorthogonal matrices to codes. We first recall that a q-ary code [i.e., a code in which the components of codewords lie in GF(q)] with q^k codewords is *systematic* if it possess an *information set*, i.e., if there is a set of k coordinates such that no two distinct codewords have components that agree in all k of these coordinates. By a permutation of coordinates, which does not affect the Hamming distance between codewords, one obtains an *equivalent code* for which the first k coordinates are an information set, which we shall call a *leading-systematic* code. Every linear code is systematic and hence equivalent to a leading-systematic linear code. Moreover, a linear code is leading-systematic if and only if it has a generator matrix of the form $\mathbf{G} = [\mathbf{I} \,:\, \mathbf{P}]$, which generator matrix is easily seen to be unique and is called the *systematic generator matrix* of the code. We recall further that a linear code V is said to be self-dual if $V = V^\perp$ where $V^\perp$ is the dual code of V. If the code length is n, then the dimension of a self-dual code must be $k = n/2$ so that n must be even. We can now give a very simple, but apparently not previously stated, characterization of self-dual codes.

Proposition 1 *A leading-systematic linear code V is self-dual if and only if, in its systematic generator matrix*

$$\mathbf{G} = [\mathbf{I} \,:\, \mathbf{P}],$$

the matrix $\mathbf{P}$ is antiorthogonal.

Proof: Because the code length of a self-dual code satisfies $n = 2k$ where k is the code dimension, the matrix $\mathbf{P}$ must be square. Moreover, V will be self-dual just when $\mathbf{G}$ is also a parity-check matrix of the code, i.e., when $\mathbf{G}\mathbf{G}^T = \mathbf{0}$. But $\mathbf{G}\mathbf{G}^T = \mathbf{I} + \mathbf{P}\mathbf{P}^T$ so that V is self-dual just when $\mathbf{P}\mathbf{P}^T = -\mathbf{I}$, as was to be shown.

It seems entirely natural, for an in general nonsquare matrix $\mathbf{B}$, to say that $\mathbf{B}$ is *row-antiorthogonal* if

$$\mathbf{B}\mathbf{B}^T = -\mathbf{I},$$

as this is equivalent to the condition that each row of $\mathbf{B}$ is orthogonal to every *other* row of $\mathbf{B}$ but has a scalar product of -1 with itself. A row-antiorthogonal matrix always has full row rank and thus must have at least as many columns as rows. If $\mathbf{B}$ is row-antiorthogonal but non-square, $\mathbf{B}^T$ cannot also be row-antiorthogonal. In a field of characteristic 2 and only in such a field, a row-antiorthogonal matrix is also a row-orthogonal matrix. Deleting rows of an antiorthogonal matrix gives a row-antiorthogonal matrix, but not every row-orthogonal matrix can be so constructed, as our previous example of the binary matrix $\mathbf{B} = [1\ 1\ 1]$ demonstrates.

Recalling that a linear code V is said to be *weakly self-dual* if $V \subseteq V^\perp$, we obtain a simple generalization of Proposition **??**.

Proposition 2 *A leading-systematic linear code V is weakly self-dual if and only if, in its systematic generator matrix*

$$\mathbf{G} = [\mathbf{I} \ : \ \mathbf{P}],$$

the matrix $\mathbf{P}$ is row-antiorthogonal.

Proof: The code V will be self-dual just when the row space of $\mathbf{G}$ is a subset of $V^\perp$, i.e., when $\mathbf{G}\mathbf{G}^T = \mathbf{0}$. But $\mathbf{G}\mathbf{G}^T = \mathbf{I} + \mathbf{P}\mathbf{P}^T$ so that V is self-dual just when $\mathbf{P}\mathbf{P}^T = -\mathbf{I}$, i.e., when $\mathbf{P}$ is row-antiorthogonal.

4 Self-Orthogonal Matrices

It seems a natural extension of terminology to say that a square matrix $\mathbf{C}$ over an arbitrary field $\mathcal{F}$ is *self-orthogonal* if

$$\mathbf{C}\mathbf{C}^T = \mathbf{O},$$

where here and hereafter $\mathbf{O}$ denotes a zero matrix of appropriate dimension. Equivalently, $\mathbf{C}$ is self-orthogonal just when each row of $\mathbf{C}$ is orthogonal to *every row* of $\mathbf{C}$ including itself. It follows from $\mathbf{C}\mathbf{C}^T = \mathbf{O}$ that $\det(\mathbf{C}) = 0$ and hence that a self-orthogonal matrix is always singular. An example of a self-orthogonal matrix over the field GF(2) is

$$\mathbf{C} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Note that

$$\mathbf{C}^T\mathbf{C} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

so that $\mathbf{C}^T$ is *not* self-orthogonal in this example.

We are now virtually forced to say, for an in general non-square matrix $\mathbf{C}$, that $\mathbf{C}$ is *row-self-orthogonal* if

$$\mathbf{C}\mathbf{C}^T = \mathbf{O},$$

as this is equivalent to the condition that each row of $\mathbf{C}$ is orthogonal to *every row* of $\mathbf{C}$ including itself. A row-self-orthogonal matrix, which is not square (and hence not also a self-orthogonal matrix) can have full row rank. Indeed any matrix obtained by deleting rows from a self-orthogonal matrix is row-self-orthogonal so that deleting the second row from the above-displayed self-orthogonal matrix $\mathbf{C}$ gives a 3×4 matrix that is row-self-orthogonal and has full row rank.

The proofs of Propositions **??** and **??** imply the following alternative characterization of self-dual and weakly self-dual codes.

Proposition 3 *A linear code V with generator matrix $\mathbf{G}$ is self-dual or weakly self-dual if and only if $\mathbf{G}$ is self-orthogonal or row-self-orthogonal, respectively.*

5 Applications to LCD Codes

We now show some connections between the above-defined matrices and *linear codes with complementary duals* (or LCD codes for short). An LCD code is a linear code V such that $V \cap V^{\perp} = \{\mathbf{0}\}$. The reader is referred to [**?**] for proofs of the basic properties of LCD codes including the fact that if $\mathbf{G}$ is a generator matrix for a linear code V, then V is self-dual if and only if $\mathbf{G}\mathbf{G}^T$ is a nonsingular matrix.

We now show a first connection between LCD codes and the above-defined matrices.

Proposition 4 *A leading-systematic linear code V is an LCD code if (but not only if), in its systematic generator matrix*

$$\mathbf{G} = [\mathbf{I} \;:\; \mathbf{P}],$$

the matrix $\mathbf{P}$ is row-self-orthogonal or, equivalently, if $\mathbf{G}$ is row-orthogonal.

Proof: Because $\mathbf{G}\mathbf{G}^T = \mathbf{I} + \mathbf{P}\mathbf{P}^T$, it follows that $\mathbf{G}$ is row-orthogonal just when $\mathbf{P}$ is row-self-orthogonal. Moreover, if $\mathbf{P}$ is row-self-orthogonal, then $\mathbf{G}\mathbf{G}^T = \mathbf{I}$ so that V is indeed an LCD code.

As an application of Proposition **??**, we first note that, for any $k \times m$ matrix $\mathbf{Q}$ over a field of characteristic 2, the $k \times 2m$ matrix $\mathbf{P} = [\mathbf{Q} \;:\; \mathbf{Q}]$ is row-self-orthogonal. Thus $\mathbf{G} = [\mathbf{I} \;:\; \mathbf{Q} \;:\; \mathbf{Q}]$ generates a leading-systematic LCD code of length $n = k + 2m$ and dimension k. In fact, these are the codes used in Proposition 2 of [**?**] to establish the asymptotic goodness of LCD codes over a finite field of characteristic 2.

More generally, if $\mathbf{Q}$ is any $k \times m$ matrix over a field of characteristic p such that -1 is a quadratic residule modulo p, i.e., such that there exists α in GF(p) for which $\alpha^2 = -1$, then $\mathbf{P} = [\mathbf{Q} \;:\; \alpha\mathbf{Q}]$ is row-self-orthogonal and hence $\mathbf{G} = [\mathbf{I} \;:\; \mathbf{Q} \;:\; \alpha\mathbf{Q}]$ generates a leading-systematic LCD code of length $n = k + 2m$ and dimension k. A theorem of Lagrange (cf. p. 302 in [**?**]), implies that, for any prime p, one can find elements α, β, γ and δ in GF(p) such that $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = -1$. The corresponding matrix $\mathbf{P} = [\alpha\mathbf{Q} \;:\; \beta\mathbf{Q} \;:\; \gamma\mathbf{Q} \;:\; \delta\mathbf{Q}]$ is thus row-self-orthogonal. Hence $\mathbf{G} = [\mathbf{I} \;:\; \alpha\mathbf{Q} \;:\; \beta\mathbf{Q} \;:\; \gamma\mathbf{Q} \;:\; \delta\mathbf{Q}]$ generates a leading-systematic LCD code of length $n = k + 4m$ and dimension k. These are the codes used in [?] to establish the asymptotic goodness of LCD codes over an arbitrary finite field.

A stronger consequence of Proposition **??** in the same vein as the previous examples is the following.

Proposition 5 *If* $\mathbf{B}$ *is any* $m \times m$ *antiorthogonal matrix and* $\mathbf{Q}$ *is any* $k \times m$ *matrix, then*

$$\mathbf{G} = [\mathbf{I} \ : \ \mathbf{Q} : \ \mathbf{QB}],$$

is the generator matrix of a leading-systematic LCD code of length $n = k + 2m$ *and dimension* k.

Proof: The proposition follows immediately from Proposition **??** upon noting that $\mathbf{P} = [\mathbf{Q} : \ \mathbf{QB}]$ satisfies $\mathbf{PP}^T = \mathbf{QQ}^T + \mathbf{QBB}^T\mathbf{Q}^T = \mathbf{QQ}^T - \mathbf{QQ}^T = \mathbf{O}$ so that $\mathbf{P}$ is indeed a row-self-orthogonal matrix.

The class of codes defined in Proposition **??** is rich enough to meet the asymptotic Varshamov-Gilbert bound as even a crude lower bound on the the number of orthogonal matrices suffices to establish, but we omit details of this argument here.

The following is another consequence of Proposition **??**.

Proposition 6 *If* $\mathbf{Q}$ *is any* $k \times k$ *matrix,* $\mathbf{C}$ *is any* $k \times m$ *row-self-orthogonal matrix, and* $\mathbf{A}$ *is any* $m \times m$ *orthogonal matrix, then*

$$\mathbf{G} = [\mathbf{I} \ : \ \mathbf{QCA}],$$

is the generator matrix of a leading-systematic LCD code of length $n = k + m$ *and dimension* k*. The same holds true if* $\mathbf{A}$ *is any* $m \times m$ *antiorthogonal matrix*

Proof: Letting $\mathbf{P} = \mathbf{QCA}$, we have $\mathbf{PP}^T = \mathbf{QCAA}^T\mathbf{C}^T\mathbf{Q}^T = \mathbf{QCC}^T\mathbf{Q}^T = \mathbf{O}$ so that $\mathbf{P}$ is indeed row-self-orthogonal.

References

[1] G. A. Jones, “Symmetry,” in Handbook of Applicable Mathematics, Vol.5, Combinatorics and Geometry (Eds. W. Lederman and S. Vajda). Chichester and New York: Wiley, 1985, pp. 329-422.

[2] P. G. Farrell, “Linear Binary Anticodes,’ *Electronics Letters*, Vol. 6, pp. 419-21, 1970.

[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes.* Amsterdam: North-Holland, 1977.

[4] J. L. Massey, ”Linear Codes with Complementary Duals,” *Discrete Math.*, Vol. 106/107, pp. 337-342, 1992. [Also appears as 337-342 in *A Collection of Contributions in Honor of Jack van Lint* (Eds. P. J. Cameron and H. C. A. van Tilborg), Topics in Discrete Math. 7. Amsterdam: Elsevier 1992.]

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers.* London: Oxford Univ. Press, 4th Ed., 1965.