[4] R. Ash, *Information Theory.* New York: Wiley, 1965.
[5] R. J. McEliece, *The Theory of Information and Coding.* London: Addison-Wesley, 1977.
[6] D. Middleton, *An Introduction to Statistical Communication Theory.* New York: McGraw-Hill, 1960.
[7] M. R. D'Amato, *Experimental Psychology: Methodology, Psychophysics, and Learning.* New York: McGraw-Hill, 1970.
[8] P. J. Barber and D. Legge, *Perception and Information.* London: Methuen, 1976.
[9] T. B. Sheridan and W. R. Ferrell, *Man-Machine Systems: Information, Control and Decision Models of Human Performance.* Cambridge, MA: MIT, 1974.
[10] T. O. Kvålseth, "Note on information capacity of discrete motor responses," *Percept. Motor Skills*, vol. 49, pp. 291–296, 1979.
[11] ——, "Test of the 10 bits/sec channel-capacity hypothesis for human tracking," *Appl. Math. Model.*, vol. 3, pp. 307–308, 1979.

Independent Pairs of Good Self-Dual Codes

WILLIAM M. KANTOR

Abstract—**Let $n \equiv 0 \pmod 8$. Then there are two self-dual binary codes of length n having only the zero and all-one vectors in common, having all weights divisible by four, and having minimum distances asymptotically the same as that given by the Varshamov–Gilbert bound.**

I. Introduction

In [1] and [2], MacWilliams, Sloane, and Thompson studied the class $\boldsymbol{M}$ of binary self-dual $[n, n/2]$ codes in which all weights are divisible by four. (Here, $\boldsymbol{M} \neq \varnothing$ precisely when $n \equiv 0 \pmod 8$.) They showed that, for large block lengths $n \equiv 0 \pmod 8$, there are codes in $\boldsymbol{M}$ whose minimum distance is asymptotically the same as that given by the Varshamov–Gilbert bound.

In this correspondence, we extend their result slightly. Call two self-dual codes *independent* if their intersection consists only of $\mathbf{0}$ and the all-one vector $\mathbf{1}$. We will show that an independent pair of codes exists inside $\boldsymbol{M}$ such that the minimum distance of each behaves asymptotically as above. However, a triple of pairwise independent codes does not exist inside $\boldsymbol{M}$.

II. Results

We will prove the following results.

Theorem 1: Let $n \equiv 0 \pmod 8$. Then $\boldsymbol{M}$ contains an independent pair C_1, C_2 of codes whose minimum distances d_1 and d_2 both satisfy $d_i/n \approx 0.110$.

Theorem 2: Let $n \equiv 0 \pmod 8$. Let r be the largest integer such that

$$\binom{n}{4} + \cdots + \binom{n}{4(r-1)} < 2^{(n/2)-2}.$$

Then there exists a code C_1 in $\boldsymbol{M}$ whose minimum distance is at least $4r$. For each such code C_1 in $\boldsymbol{M}$ with this property, there is a second code C_2 in $\boldsymbol{M}$ with this property such that C_1 and C_2 are independent.

Proposition 1: Let $n \equiv 0 \pmod 8$, and let $C \in \boldsymbol{M}$. Let $w_{4i}(C)$ be the number of codewords in C of weight $4i$. If r is the largest integer such that $\sum_{i=1}^{r-1}\binom{n}{4i} < 2^{(n/2)-2} + \sum_{i=1}^{r-1} w_{4i}(C)$, then there is a code $C' \in \boldsymbol{M}$ such that C and C' are independent and C' has minimum distance at least $4r$.

Theorem 3: Let $n = 2m + 2 \equiv 0 \pmod 8$, and let $C \in \boldsymbol{M}$. Let C_0 be an $[n, s]$ code such that $C \cap C_0 = \{\mathbf{0}, \mathbf{1}\}$, all of whose weights are divisible by four. Then there are exactly $2^{(m-s)(m-s+1)/2}$ codes $C' \in \boldsymbol{M}$ such that $C_0 \subseteq C'$ and such that the codes C and C' are independent.

Proposition 2: There do not exist three pairwise independent members of $\boldsymbol{M}$.

Proposition 1 follows from Theorem 3 by a standard counting argument. In view of [1] and [2], Theorem 2 is a special case of Proposition 1, while Theorem 1 follows from Theorem 2.

Consequently, we only have to prove Theorem 3 and Proposition 2. This will be accomplished by translating them into the terminology of orthogonal geometry.

III. Orthogonal Geometry

Let $n \equiv 0 \pmod 4$. Write $n = 2m + 2$.

Let Z_2^n denote the vector space of all ordered binary n-tuples. The weight $\mathrm{wt}(\boldsymbol{v})$ of a vector $\boldsymbol{v}$ is its number of ones.

Set $V_1 = \{\mathbf{0}, \mathbf{1}\}$ and $V_{n-1} = \{\boldsymbol{v} \in Z_2^n \mid \mathrm{wt}(\boldsymbol{v}) \text{ is even}\}$. Then $V_1 \subseteq V_{n-1}$.

Set $V = V_{n-1}/V_1$.

If $\boldsymbol{x} \in V_{n-1}$, set $Q(\boldsymbol{x} + V_1) = \frac{1}{2}\mathrm{wt}(\boldsymbol{x}) \pmod 2$. Since $n \equiv 0 \pmod 4$, this is well-defined.

Set $(\boldsymbol{x} + V_1, \boldsymbol{y} + V_1) = Q(\boldsymbol{x} + \boldsymbol{y} + V_1) - Q(\boldsymbol{x} + V_1) - Q(\boldsymbol{y} + V_1)$ for $\boldsymbol{x}, \boldsymbol{y} \in V_{n-1}$. This is just the dot product (mod 2) of the vectors $\boldsymbol{x}$ and $\boldsymbol{y}$, and hence defines a bilinear form on V. Thus, Q is a quadratic form on V (cf. [3, p. 434]). If $(\boldsymbol{x} + V_1, \boldsymbol{y} + V_1) = 0$ for some $\boldsymbol{y}$ and all $\boldsymbol{x}$, then it is easy to see that $\boldsymbol{y} \in V_1$. Thus, Q is a nonsingular quadratic form.

Let W be a subspace of V. Write $W = X/V_1$ for a subspace X of V_{n-1}. By definition, $Q(W) = 0$ if and only if the weight of each vector in X is a multiple of four. Such a subspace W is called *totally singular*. Note that $W \subseteq W^{\perp}$, so that $\dim W \leq m$. Thus, there is a totally singular m-space if and only if $\boldsymbol{M} \neq \varnothing$, and this is the case precisely when $n \equiv 0 \pmod 8$ [1, lemma 4.6]. This uniquely determines the quadratic form Q, up to a change of variables ([4, pp. 197–199]; [5, p. 34]; [3, p. 438]). In particular, if $n \equiv 0 \pmod 8$ then there is a basis $\boldsymbol{e}_1, \cdots, \boldsymbol{e}_m, \boldsymbol{f}_1, \cdots, \boldsymbol{f}_m$ of V such that

$$Q\left(\sum_{i=1}^{m} a_i \boldsymbol{e}_i + \sum_{i=1}^{m} b_i \boldsymbol{f}_i\right) = \sum_{i=1}^{m} a_i b_i$$

whenever $a_i, b_i \in Z_2$. Note that $E = \langle \boldsymbol{e}_1, \cdots, \boldsymbol{e}_m \rangle$ and $\langle \boldsymbol{f}_1, \cdots, \boldsymbol{f}_m \rangle$ are totally singular m-spaces. Their preimages in V_{n-1} are an independent pair of elements of $\boldsymbol{M}$.

The orthogonal group $O^+(2m, 2)$ consists of all nonsingular linear transformations T of V such that $Q(T(\boldsymbol{v})) = Q(\boldsymbol{v})$ for all $\boldsymbol{v} \in V$. Note that T has nothing whatsoever to do with the coding theoretic structure of Z_2^n. Note also that $(T(\boldsymbol{u}), T(\boldsymbol{v})) = (\boldsymbol{u}, \boldsymbol{v})$ for all $\boldsymbol{u}, \boldsymbol{v} \in V$. The following standard result [5, p. 36] will be used in our proofs.

Witt's Theorem: Let W_1 and W_2 be subspaces of V. Let T_1: $W_1 \to W_2$ be a nonsingular linear transformation such that $Q(T_1(\boldsymbol{w})) = Q(\boldsymbol{w})$ for all $\boldsymbol{w} \in W_1$. Then there is an element of $O^+(2m, 2)$ which, when restricted to W_1, is just T_1.

IV. Proofs

Let $n \equiv 0 \pmod 8$. Then $n = 2m + 2$ with $m \equiv -1 \pmod 4$. Define $\boldsymbol{e}_1, \cdots, \boldsymbol{e}_m, \boldsymbol{f}_1, \cdots, \boldsymbol{f}_m$ as in the preceding section.

By Witt's theorem, $O^+(2m, 2)$ is transitive on the set of all totally singular k spaces for each $k \leq m$. Consequently, both Theorem 3 and Proposition 4 are simply concerned with the set of all totally singular subspaces having only $\mathbf{0}$ in common with $E = \langle \boldsymbol{e}_1, \cdots, \boldsymbol{e}_m \rangle$.

Manuscript received September 11, 1981; revised December 30, 1981.
The author was with Bell Laboratories, Murray Hill, NJ 07974. He is now with the Department of Mathematics, University of Oregon, Eugene, OR 97403.

0018-9448/82/1100-0966$00.75 ©1982 IEEE

Let G denote the subgroup of $O^+(2m,2)$ consisting of all elements sending E to itself.

Lemma 1: If $0 \le k \le m$, then G is transitive on the set of all totally singular k-spaces W such that $E \cap W = 0$.

Proof: Let W be such a subspace. Then $E_2 = E \cap W^\perp$ has dimension $m - k$. Let E_1 be any subspace of E such that E is the direct sum $E_1 \oplus E_2$ of E_1 and E_2. Let $\boldsymbol{u}_1,\cdots,\boldsymbol{u}_k$ be a basis of E_1. Note that $\boldsymbol{u}_i^\perp \cap W$ is a hyperplane of W. If $1 \le j \le k$, there is a nonzero vector $\boldsymbol{w}_j$ common to all the hyperplanes $\boldsymbol{u}_i^\perp \cap W$, $i \ne j$. Then

$$Q\left(\sum_{i=1}^{k} a_i\boldsymbol{u}_i + \sum_{i=1}^{k} b_i\boldsymbol{w}_i + \boldsymbol{e}\right) = \sum_{i=1}^{k} a_i b_i,$$

whenever $\boldsymbol{e} \in E_2$ and $a_i, b_i \in Z_2$.

If $\boldsymbol{u}_{k+1},\cdots,\boldsymbol{u}_m$ is a basis of E_2, then the linear transformation T_1: $E \oplus W \to E \oplus \langle \boldsymbol{f}_1,\cdots,\boldsymbol{f}_k\rangle$ sending $\boldsymbol{u}_i$ to $\boldsymbol{e}_i$ and $\boldsymbol{w}_i$ to $\boldsymbol{f}_i$ satisfies the hypotheses of Witt's theorem. Consequently, G contains an element sending W to $\langle \boldsymbol{f}_1,\cdots,\boldsymbol{f}_k\rangle$. (If $k = m$, Witt's theorem is irrelevant here.) This proves the lemma.

Lemma 2: Let W be a totally singular m-space such that $E \cap W = 0$. Then $W = \langle \boldsymbol{f}_i + \Sigma_{i=1}^m a_{ij}\boldsymbol{e}_j \mid 1 \le i \le m\rangle$, where (a_{ij}) is a skew-symmetric $m \times m$ matrix with zero diagonal. Conversely, if (a_{ij}) is any such skew-symmetric matrix then the subspace W defined using (a_{ij}) as before is a totally singular m-space such that $E \cap W = 0$.

Proof: Let W be a totally singular m-space such that $E \cap W = 0$. Since $V = E \oplus W$, for each i there is a vector $\boldsymbol{w} \in W$ such that $\boldsymbol{f}_i \in E + \boldsymbol{w}_i$. Set $\boldsymbol{w}_i = \boldsymbol{f}_i + \Sigma_{i=1}^m a_{ij}\boldsymbol{e}_j$. Then $\boldsymbol{w}_1,\cdots,\boldsymbol{w}_m$ is a basis for W, while $0 = Q(\boldsymbol{w}_i) = a_{ij}$ and $0 = (\boldsymbol{w}_i, \boldsymbol{w}_j) = a_{ij} + a_{ji}$ for all i, j. Reversing this argument, we deduce the lemma.

Proof of Theorem 3: By Lemma 2, there are $2^{m(m+1)/2}$ totally singular m-spaces W such that $E \cap W = 0$. By Lemma 1, in order to complete the proof of Theorem 3 it suffices to consider those subspaces W containing $\langle \boldsymbol{f}_1,\cdots,\boldsymbol{f}_s\rangle$. By Lemma 2, these arise from those skew-symmetric matrices (a_{ij}) whose first s rows are zero. There are thus $2^{(m-s)(m-s+1)/2}$ such subspaces W, as required.

Proof of Proposition 4: Assume that there are three totally singular m-spaces W, X, Y such that $W \cap X = W \cap Y = X \cap Y = 0$. By Lemma 1, we may assume that $X = E$ and $Y = F$. Define (a_{ij}) as in Lemma 2. Then $(b_1,\cdots,b_m)(a_{ij}) = 0$ for some m-tuple $(b_1,\cdots,b_m) \ne 0$, since m is odd and (a_{ij}) is skew-symmetric. By Lemma 2, $\Sigma_{i=1}^m b_i\boldsymbol{f}_i \in F \cap W$. Since $F \cap W = 0$, this is impossible.

V. Concluding Remarks

We used Witt's theorem in our proofs. However, it is not difficult to obtain short, direct proofs of those special cases we required.

Pless and Pierce [6] extended the results of MacWilliams, Sloane, and Thompson [1], [2] to codes over arbitrary finite fields. Our results can be extended in the same manner, using proofs similar to those of the preceding section.

References

[1] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, "Good self-dual codes exist," *Discrete Math.*, vol. 3, pp. 153–162, 1972.

[2] J. G. Thompson, "Weighted averages associated to some codes," *Scripta Math.*, vol. 29, pp. 449–452, 1973.

[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North Holland, 1978.

[4] L. E. Dickson, *Linear Groups, with an Exposition of the Galois Field Theory*. New York: Dover, 1958.

[5] J. Dieudonné, *La Géometrié des Groupes Classiques*. Berlin–Heidelberg–New York: Springer, 1971.

[6] V. Pless and J. N. Pierce, "Self-dual codes over GF(q) satisfy a modified Varshamov–Gilbert bound," *Inform. Contr.*, vol. 23, pp. 35–40, 1973.

The Acceptance of Information, Its Subjective Cost and the Measurement of Distortion

ROLAND G. WILSON

Abstract—**A suitable operational definition of the subjective acceptability of an information source to a human user is shown to be the "probability of acceptance in a multiple-choice test." It is shown that acceptance probability relates directly to the user's statistical dependence on a given source. The notion of subjective cost of information is introduced as a concise way of defining such acceptance probabilities and a general statistical model of decision behavior used to establish the relation between expected cost and probability of acceptance. Distortion is then defined as the marginal cost of accepting a replication over that of the original source. It is shown that this leads to a way of determining distortion functions from observation of acceptance decisions. The method is illustrated with an example of image noise evaluation.**

I. The Problem of Acceptability

Rate-distortion theory is widely accepted as a basis for the study of source-coding methods [1]–[10]. Its application requires knowledge of two measures: the source probability distribution and the distortion measure. The former may be inferred, under suitable assumptions (e.g., ergodicity), from observations of the source. There remains the problem of determining the distortion function: what are the observable events from which it may be inferred?

It is clear that the distortion function depends on the use to which the received information is put. In one of the most difficult cases, and one of the most common, the user is a human being. In this case, the distortion function is required to reflect the subjective acceptability of some set of replications of the source. Thus if a precise operational definition could be given for "subjective acceptability" it might provide a path to the distortion function.

The approach taken in this correspondence is that of operationally defining acceptability as "probability of acceptance in a multiple-choice test." This is a natural way of linking subjective opinions to experimental observations. It leads in general to a definition of the subjective cost of an information source, and in the specific case where the sources are all replications of a given source, to the average distortion associated with a replication. It will be shown that knowledge of the average distortions associated with a suitably chosen set of replications is sufficient to completely determine the distortion function. Finally the method is illustrated by an example of image noise evaluation.

II. Acceptance and Subjective Cost

The problem of determining the acceptabilities to human users of some set of replications of a given source is a special case of the more general one of determining the acceptabilities of an arbitrary set of sources of information.

Its solution requires a model of acceptance behavior, whose innate variability implies a statistical model. Consider, therefore,

Manuscript received March 27, 1978; revised June 4, 1982.

The author is with the Department of Electrical-Electronic Engineering, University of Aston, Birmingham, England B4 7PB.

0018-9448/82/1100-0967$00.75 ©1982 IEEE