Reprinted from INFORMATION AND CONTROL, Volume 13, No. 1, July 1968

INFORMATION AND CONTROL **13**, 46–52 (1968)

An Upper Bound on Minimum Distance for a k-ary Code

A. D. WYNER AND R. L. GRAHAM

Bell Telephone Laboratories, Incorporated, Murray Hill, New Jersey

We obtain an upper bound on the maximum attainable minimum distance for a k-ary code for a certain class of distance functions. This class includes the αth power of the Lee distance ($0 < \alpha \leq 1$).

In this paper we consider the problem of constructing block codes (for the discrete channel with k inputs and outputs) which maximize the minimum "distance" between code words.

Let us label the input and output levels $\{0, 1, 2, \cdots, k-1\}$. A *code* of dimension n and size M is a set of M n-sequences $\mathbf{a}_r = (a_{r1}, a_{r2}, \cdots, a_{rn})$ $(r = 1, 2, \cdots, M)$ where $a_{rs} \in \{0, 1, \cdots, k-1\}$. Often it is meaningful to define a *discrepancy* or *distance* d_{ij}, $i, j = 0, 1, 2, \cdots, k-1$, between the k levels. Two examples are the Hamming distance h_{ij} and the Lee distance ℓ_{ij} where

$$h_{ij} = \begin{cases} 0 & i = j \\ 1 & i \neq j \end{cases} \tag{1a}$$

and

$$\ell_{ij} = \min \{ |i-j|, k - |i-j| \}. \tag{1b}$$

We shall assume that d_{ij} satisfies

$$d_{ii} = 0, \tag{2a}$$

$$d_{ij} = d_{ji}, \tag{2b}$$

$$\sum_{j=0}^{k-1} d_{ij} = S \quad \text{for each } i = 0, 1, \cdots, k-1, \tag{2c}$$

where S is some fixed number. Note that (2) does not require d_{ij} to be a metric. Conditions (2b) and (2c) are always satisfied when $d_{ij} = f(h_{ij})$ or $d_{ij} = f(\ell_{ij})$ where f is an arbitrary function. Let $\mathbf{a} = (a_1, a_2,$

$\cdots, a_n)$ and $\mathbf{b} = (b_1, b_2, \cdots, b_n)$ be n-sequences (where $a_s, b_s \in \{0, 1, \cdots, k-1\}$). We define the distance between $\mathbf{a}$ and $\mathbf{b}$ as

$$d(\mathbf{a}, \mathbf{b}) = \sum_{s=1}^{n} d_{a_s b_s}. \tag{3}$$

The *minimum distance* of a code is the smallest distance between the code sequences. We are interested in the quantity $d^*(M, n)$ the largest attainable minimum distance for a code with parameters M and n.

Our main results are the following

THEOREM 1. *If d_{ij} satisfies conditions* (2), *and if the* $(k-1) \times (k-1)$ *matrix* $(q_{ij})_{i,j=1}^{k-1}$ *is non-negative definite, where* $q_{ij} = d_{0i} + d_{0j} - d_{ij}$, *then*

$$d^*(M, n) \leq \frac{SMn}{k(M-1)}.$$

THEOREM 2. *If* $d_{ij} = \ell_{ij}^{\alpha}$, *where* ℓ_{ij} *is the Lee distance, and* $0 < \alpha \leq 1$, *the hypotheses of Theorem* 1 *are valid.*

For the Lee distance, $S = k^2/4$ (k even) and $(k^2 - 1)/4$ (k odd), we consequently have

$$d^*(M, n) \leq \begin{cases} kMn/4(M-1), & k \text{ even} \\ (k^2-1)Mn/4k(M-1), & k \text{ odd.} \end{cases} \tag{4}$$

Inequality (4) was conjectured by Lee (1958).

Theorem 1 is a bound of the Plotkin type (Plotkin, 1960) for Hamming distance. In fact, since $\lim_{\alpha \to 0} \ell_{ij}^{\alpha} = h_{ij}$, Theorems 1 and 2 are generalizations of Plotkin's result. Theorem 2 is actually a consequence of some general theorems due to von Neumann and Schoenberg (1941) and Beurling (1950), and although the proof in Section II is complete, it depends on their ideas.

SECTION II. PROOFS OF THEOREMS

Theorem 1 will follow directly from a lemma on the maximization of a certain quadratic form which we will now derive.

Let $D = (d_{ij})_{i,j=0}^{k-1}$ be a symmetric $k \times k$ real matrix with diagonal elements zero and such that the sum of the elements in each row (and column) is equal to S. Thus the d_{ij} satisfy (2). Consider the quadratic form

$$F(x_0, x_1, \cdots, x_{k-1}) = \sum_{j=0}^{k-1} \sum_{i=0}^{k-1} x_i x_j d_{ij}. \tag{5}$$

We shall try to maximize F under the constraint that

$$\sum_{i=0}^{k-1} x_i = \nu. \tag{6}$$

In what follows we shall find a condition on D under which F attains its maximum when all the x_i are equal, i.e., $x_i = \nu/k$ $(i = 0, 1, \cdots, k-1)$. Rewrite (5) as

$$\begin{aligned} F(x_0, x_1, \cdots, x_{k-1}) &= \sum_{i,j} x_i x_j d_{ij} \\ &= \sum_{i,j} x_i x_j (d_{ij} - d_{0i} - d_{0j}) \\ &\quad + \sum_{i,j} x_i x_j (d_{0i} + d_{0j}), \end{aligned} \tag{7}$$

which from (6) is

$$F = 2\nu \sum_{i=0}^{k-1} x_i d_{0i} - \sum_{i,j} x_i x_j q_{ij}, \tag{8a}$$

where

$$q_{ij} = d_{0i} + d_{0j} - d_{ij}. \tag{8b}$$

Now, we may write

$$\begin{aligned} \sum_{i,j} x_i\, x_j\, q_{ij} &= \sum_{i,j} \left(x_i - \frac{\nu}{k}\right)\left(x_j - \frac{\nu}{k}\right) q_{ij} \\ &\quad + \frac{2\nu}{k} \sum_i x_i \sum_j q_{ij} - \frac{\nu^2}{k^2} \sum_{i,j} q_{ij}. \end{aligned} \tag{9}$$

Further, from (2c),

$$\sum_j q_{ij} = \sum_j (d_{0i} + d_{0j} - d_{ij}) = kd_{0i} + S - S = kd_{0i}, \tag{10}$$

and again from (2c) and (10)

$$\sum_{i,j} q_{ij} = kS. \tag{11}$$

Hence, combining equations 8–11 and noting that $q_{0j} = q_{i0} = 0$, we obtain

$$F(x_0, x_1, \cdots, x_{k-1}) = \frac{\nu^2 S}{k} - \sum_{j=1}^{k-1} \sum_{i=1}^{k-1} \left(x_i - \frac{\nu}{k}\right)\left(x_j - \frac{\nu}{k}\right) q_{ij}. \tag{12}$$

We have immediately from (12) that F attains a maximum at $x_i = \nu/k$ $(i = 0, 1, \cdots, k-1)$ if and only if the $(k-1) \times (k-1)$ matrix (q_{ij}) is non-negative definite. If (q_{ij}) is positive-definite, then F attains its maximum at this point uniquely. If (q_{ij}) is non-negative definite and singular, then F attains its maximum whenever the $(x_i - \nu/k)$ are in the null-space of (q_{ij}).

We state the result which we will need for Theorem 1 as

LEMMA 1. *Let $(d_{ij})_{i,j=0}^{k-1}$ be a matrix which satisfies* (2). *Then, if the matrix $(q_{ij})_{i,j=1}^{k-1}$ (where the q_{ij} are defined by* (8b)) *is non-negative definite,*

$$\sum_{j=0}^{k-1} \sum_{i=0}^{k-1} x_i x_j d_{ij} \leq \frac{S}{k} \left(\sum_{i=0}^{k-1} x_i \right)^2, \tag{13}$$

for arbitrary x_i.

Proof of Theorem 1.

Let $\{\mathbf{a}_r\}_{r=1}^{M}$ be a code with parameters M and n with minimum distance $d^*(M, n)$. Arrange the code words in an array

$$\begin{aligned} \mathbf{a}_1 &= a_{11}a_{12} \cdots a_{1n} \\ &\cdot \quad \cdot \ \cdot \quad \cdot \\ &\cdot \quad \cdot \ \cdot \quad \cdot \\ &\cdot \quad \cdot \ \cdot \quad \cdot \\ \mathbf{a}_M &= a_{M1}a_{M2} \cdots a_{Mn}. \end{aligned} \tag{14}$$

Denote by x_{si} the number of times symbol i $(i = 0, 1, 2, \cdots, k-1)$ appears in column s. Note that $\sum_i x_{si} = M$. Since the code has minimum distance d^*,

$$\begin{aligned} \binom{M}{2} d^* &\leq \sum_{1 \leq r < t \leq M} d(\mathbf{a}_r, \mathbf{a}_t) = \sum_{s=1}^{n} \tfrac{1}{2} \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} x_{si} x_{sj} d_{ij} \\ &\leq SM^2 n/2k \end{aligned} \tag{15}$$

where the last inequality follows from Lemma 1. Theorem 1 follows on dividing through by $\binom{M}{2}$.

We now turn our attention to Theorem 2. We must show that the matrix $(q_{ij})_{i,j=1}^{k-1}$ where

$$q_{ij} = \ell_{0i}^{\alpha} + \ell_{0j}^{\alpha} - \ell_{ij}^{\alpha} \tag{16}$$

is non-negative definite. Let us define the function $\varphi(t)$ by

$$\varphi(t) = \begin{cases} k + t & -k \leq t \leq -\frac{k}{2} \\ -t & -\frac{k}{2} \leq t \leq 0 \\ t & 0 \leq t \leq \frac{k}{2} \\ k - t & \frac{k}{2} \leq t \leq k. \end{cases} \tag{17}$$

Clearly

$$l_{ij} = \varphi(i - j), \tag{18}$$

so that it will suffice to show that for any set $\{t_k\}_{k=1}^N$, where $-k \leq t_k \leq k$ and any set $\{\rho_i\}_{i=1}^N$ of real numbers

$$\sum_{i,j=1}^{N} \rho_i \rho_j \{f(t_i) + f(t_j) - f(t_i - t_j)\} \geq 0 \tag{19}$$

for the special case of $f(t) = (\varphi(t))^\alpha$.

The following lemma is a special case of a Theorem due to von Neumann and Schoenberg (1941).*

LEMMA 2. *If $f(t)$, $-k \leq t \leq k$, satisfies $f(0) = 0$, and has Fourier series representation*

$$f(t) = A - \sum_{n=1}^{\infty} a_n \cos n\omega_0 t, \qquad -k \leq t \leq k, \tag{20}$$

where $a_n \geq 0$, then f satisfies (19).

*Their theorem states that for any function $f(t)$ defined on $(-\infty, \infty)$, the quantity $\sum_{i,j} \rho_i \rho_j \{f(t_i) + f(t_j) - f(t_i - t_j)\} \geq 0$ if and only if $f(t)$ is representable as

$$f(t) = \int_{-\infty}^{\infty} \frac{\sin^2 xt}{x^2} \, d\sigma(x)$$

where $\sigma(x)$ is non-decreasing and

$$\int_{-\infty}^{\infty} \frac{d\sigma(x)}{x^2} < \infty.$$

Proof. Since $f(0) = 0$, $A = \Sigma a_n$, and we can write

$$f(t) = \sum_{n=1}^{\infty} a_n(1 - \cos n\omega_0 t) = \sum_{n=1}^{\infty} 2a_n \sin^2 \frac{n\omega_0 t}{2}. \tag{21}$$

From the identity

$$\sin^2 A + \sin^2 B - \sin^2 (A - B) = 2 \sin^2 A \sin^2 B + \tfrac{1}{2}\sin 2A \sin 2B, \tag{22}$$

we have (using (21))

$$\begin{aligned}
&\sum_{i,j} \rho_i \rho_j \{f(t_i) + f(t_j) - f(t_i - t_j)\} \\
&= \sum_{i,j} \rho_i \rho_j \sum_n 2a_n \left\{\sin^2 \frac{n\omega_0}{2} t_i + \sin^2 \frac{n\omega_0}{2} t_j - \sin^2 \frac{n\omega_0}{2} (t_i - t_j)\right\} \\
&= \sum_n 2a_n \sum_{i,j} \rho_i \rho_j \left\{2 \sin^2 \frac{n\omega_0}{2} t_i \sin^2 \frac{n\omega_0}{2} t_j + \frac{1}{2} \sin n\omega_0 t_i \sin n\omega_0 t_j\right\} \\
&= \sum_n 2a_n \left\{2 \left(\sum_i \rho_i \sin^2 \frac{n\omega_0}{2} t_i\right)^2 + \frac{1}{2} \left(\sum_i \rho_i \sin n\omega_0 t_i\right)^2\right\} \geq 0.
\end{aligned} \tag{23}$$

Hence the lemma follows.

In particular the Fourier expansion for $\varphi(t)$ is

$$\varphi(t) = \frac{k}{4} - \sum_{n \text{ odd}} \frac{2k}{\pi^2 n^2} \cos \frac{n2\pi t}{k}, \qquad -k \leq t \leq k, \tag{24}$$

so that (19) is satisfied when $f(t) = \varphi(t)$ and we have proved Theorem 2 for $\alpha = 1$. To establish the theorem for $\alpha < 1$, note the following facts. Say

$$\psi_1(t) = \sum_n a_n \cos n\omega_0 t \tag{25a}$$

and

$$\psi_2(t) = \sum_n b_n \cos n\omega_0 t \tag{25b}$$

where a_n, $b_n \geq 0$. Then since $\cos n\omega_0 t \cos m\omega_0 t = \frac{1}{2} \cos (n - m)\omega_0 t + \frac{1}{2} \cos (n + m)\omega_0 t$, the product $\psi_1(t)\psi_2(t)$ is of the form

$$\psi_1(t)\psi_2(t) = \sum_n c_n \cos n\omega_0 t, \tag{26}$$

where $c_n \geq 0$. Since we can write

$$\varphi(t) = \frac{k}{4}(1 - \psi(t)) \tag{27}$$

where $\psi(t)$, given by (24), is of the form of (25), then

$$\varphi^\alpha(t) = \left(\frac{k}{4}\right)^\alpha (1 - \psi)^\alpha = \left(\frac{k}{4}\right)^\alpha \left(1 - \alpha\psi + \frac{\alpha(\alpha - 1)}{2!}\psi^2 - \frac{\alpha(\alpha - 1)(\alpha - 2)}{3!}\psi^3 + \cdots\right). \tag{28}$$

By the above observation, ψ^k $(k = 1, 2, \cdots)$ is also of the form of (25). Since $0 < \alpha < 1$, the coefficients of the ψ^k are all negative. We conclude that φ^α is of the form of (20), and Theorem 2 follows.

RECEIVED: July 14, 1967

REFERENCES

BEURLING, A. (1950). Lectures at Harvard University, (from notes taken by H. O. Pollak).

LEE, C. Y. (1958). Some properties of nonbinary error-correcting codes, *IRE Trans. Inform. Theory* **IT-4**, 77–82.

PLOTKIN, M. (1960). Binary codes with specified minimum distance, *IRE Trans. Inform. Theory* **IT-6**, 445–450.

VON NEUMANN, J. AND I. J. SCHOENBERG (1941). Fourier-integrals and metric geometry, *Trans. of AMS*, 226–251.