RESEARCH ANNOUNCEMENTS

The purpose of this department is to provide early announcement of significant new results, with some indications of proof. Although ordinarily a research announcement should be a brief summary of a paper to be published in full elsewhere, papers giving complete proofs of results of exceptional interest are also solicited. Manuscripts more than eight typewritten double spaced pages long will not be considered as acceptable. All papers to be communicated by a Council member should be sent directly to M. H. Protter, Department of Mathematics, University of California, Berkeley, California 94720.

SPHERE-PACKING IN THE HAMMING METRIC[1]

BY ROBERT J. MCELIECE AND HOWARD RUMSEY, JR.

Communicated by R. Creighton Buck, July 31, 1968

Let $V_n(2)$ be the n-dimensional vector space over GF(2), with vectors represented as n-tuples of 0's and 1's. The *Hamming metric* $d(x, y)$ is defined to be the number of coordinates in which x and y disagree. If $A=\{a_1, a_2, \cdots, a_M\}$ is a set of M vectors, we define $d(A)=\min_{i\neq j} d(a_i, a_j)$, and $\bar{d}(A)=\mathrm{mean}_{i\neq j}\, d(a_i, a_j)$. Finally define

$$D(n, M) = \max_{|A|=M} d(A).$$

We present in this paper a method of obtaining an upper bound on $D(n, M)$ which is always at least as good as the well-known bounds, and which is frequently better. At the same time, the method gives a satisfactory explanation of the relationship between the various known upper bounds on $D(n, M)$ (Hamming [1], Plotkin [1], and Elias [2]). The weakness of the method seems to be that for the most part it deals only with the average distance between vectors, and further progress probably awaits a technique which is able to deal more directly with the minimum distance.

We need three theorems. Throughout $A=\{a_1, a_2, \cdots, a_M\}$ is a set of M vectors from $V_n(2)$.

THEOREM 1. *Let $S_r(x)$ be the sphere of radius r centered at x. Then the mean value of $|S_r(x)\cap A|$ as x varies over $V_n(2)$ is*

$$M_r = \frac{M}{2^n}\sum_{k\leq r}\binom{n}{k}.$$

[1] This paper presents the results of one phase of research carried out at the Jet Propulsion Laboratory, California Institute of Technology, under Contract No. NAS 7-100, sponsored by the National Aeronautics and Space Administration.

PROOF. Each a_i appears in exactly

$$\sum_{k \leq r} \binom{n}{k}$$

spheres of radius r, so that

$$\sum_x |S_r(x) \cap A| = M \sum_{k \leq r} \binom{n}{k}.$$

THEOREM 2 (PLOTKIN). *Suppose* $A \subseteq S_r(x)$, *and let the mean distance of vectors in A to x be* $\bar{r}$. *Then*

$$\bar{d}(A) \leqq \min(2r, 2(M/(M-1))\bar{r}(1-\bar{r}/n)).$$

PROOF. The value $2r$ is obvious. We assume $x=0$, and arrange the M vectors in an $M \times n$ array (a_{ij}) with column sums s_k. In column k, a pair of entries (a_{ik}, a_{jk}) contribute 1 to $d(a_i, a_j)$ if and only if $a_{ik} \neq a_{jk}$. Hence

$$\binom{M}{2}\bar{d} = \sum d(a_i, a_j) = \sum s_k(M - s_k) = M \sum s_k - \sum s_k^2.$$

But $\sum s_k = M\bar{r}$ and by Schwarz's inequality, $\sum s_k^2 \geqq 1/n(\sum s_k)^2 = M^2\bar{r}^2/n$, so that

$$\binom{M}{2}\bar{d} \leqq M^2\bar{r} - M^2\bar{r}^2/n,$$

and the theorem follows.

THEOREM 3. $D(n, M) \leqq D(n-t, \{M/2^t\})$, $t=0, 1, 2, \cdots$.

PROOF. There must be a set of at least $\{M/2^t\}$ ($\{M\}$ is the smallest integer $\geqq M$) vectors from A which agree on the first t coordinates.

Using Theorems 1, 2, and 3, it is possible to obtain a two-parameter (r and t) family of upper bounds on $D(n, M)$, as follows. For each r, Theorem 1 guarantees that we can find a sphere of radius r which contains at least $\{M_r\}$ vectors from A; Theorem 2 (with $\bar{r}$ replaced by min $(r, n/2)$) then gives an upper bound on the average distance of this subset which is also an upper bound on $d(A)$. And Theorem 3 allows us to repeat this procedure for the parameters $(n-t, \{M/2^t\})$, $t=1, 2, \cdots$.

The explanation of the relationship between this procedure and the other known bounds is easily stated: If we locate the smallest r for which Theorems 1 and 2 give any upper bound at all ($M_r > 1$) and apply the $2r$ part of Theorem 2, the result is numerically the same as

Hamming's bound. If we apply Theorems 1 and 2 with the largest allowable r $(r=n)$ to the sequence of pairs $(n-t, \{M/2^t\})$ as per Theorem 3, the result is Plotkin's bound. (We conjecture that only Plotkin's bound is improved by an application of Theorem 3.) Finally, if instead of spheres of radius r we use *shells* of radius $r \leqq n/2$, we obtain a somewhat weaker bound. This bound is the same as the version of Elias' bound given in [2].

This procedure improves known bounds on $D(n, M)$ for even modest values of the parameters. For example $D(22, 2^{14}) \leqq 6$ is given by the Hamming, Plotkin, and Elias bounds, while the procedure of this paper gives $D(22, 2^{14}) \leqq 5$. Another interesting example is $D(53, 2^{23}) \leqq 18$ (Hamming, Plotkin), $\leqq 17$ (Elias), and $D(53, 2^{23}) \leqq 16$ by our methods. It is known [2] that Elias' bound is asymptotically better than both the Hamming and the Plotkin bounds. The bound of this paper is not asymptotically better than Elias'.

REFERENCES

1. W. W. Peterson, *Error-correcting codes*, Wiley, New York, 1961.
2. A. D. Wyner, *On coding and information theory*, J. SIAM (to appear).

JET PROPULSION LABORATORY, CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA, CALIFORNIA 91109