so our constant is

$$(-1)^{\sum_{k=1}^{m} j_k + \binom{m}{2}} \cdot \left(\prod_{k=1}^{m} (k-1)! \right)^{-1}.$$

This constant is nonzero in F (this follows from the facts that $m < p$ and p is a prime number), so the determinant is nonzero.

We want to show that at least $(m+1)$ of the v_j are nonzero. Suppose this is *not* the case. Then at most m of the v_j are nonzero. From the p equations $Cv = u$, we consider the first m equations. The left side is a linear combination of at most m column vectors $(c_{0j_k}, c_{1j_k}, \cdots, c_{m-1,j_k})^T$, while by definition of the vector u the right side is zero. From the previously proven property of the matrix C, we conclude that $v = 0$. This leads to $u = Cv = 0$, contradicting the fact that $u_m \neq 0$.

We have shown that at least $(m+1)$ of the v_j are nonzero and thereby have proven that $W[P(x)] \geq (m+1)W[Q_m(x)]$. From the definition of m it follows that $m \cdot p^n \leq i_{\min} < (m+1) \cdot p^n$. From the induction hypothesis we see that

$$W[Q_m(x)] \geq W\left[(x+c)^{i_{\min} - m \cdot p^n}\right],$$

so

$$W[P(x)] \geq (m+1) \cdot W\left[(x+c)^{i_{\min} - m \cdot p^n}\right].$$

However,

$$\begin{aligned}(x+c)^{i_{\min}} &= (x+c)^{m \cdot p^n} \cdot (x+c)^{i_{\min} - m \cdot p^n} \\ &= \left(x^{p^n} + c^{p^n}\right)^m \cdot (x+c)^{i_{\min} - m \cdot p^n} \\ &= \sum_{j=0}^{m} \binom{m}{j} \left(x^{p^n}\right)^j \left(c^{p^n}\right)^{m-j} (x+c)^{i_{\min} - m \cdot p^n}.\end{aligned}$$

In this expression we have $j \leq m < p$, so p does not divide any of the $\binom{m}{j}$, also we have $i_{\min} - m \cdot p^n < p^n$, so

$$W\left[(x+c)^{i_{\min}}\right] = (m+1) \cdot W\left[(x+c)^{i_{\min} - m \cdot p^n}\right].$$

This means that $W[P(x)] \geq W[(x+c)^{i_{\min}}]$, and the proof is finished.

References

[1] J. L. Massey, D. J. Costello, and J. Justesen, "Polynomial weights and code constructions," *IEEE Trans. Inform. Theory*, vol. IT-19, no. 1, pp. 101–110, 1973.

Superimposed Codes in R^n

THOMAS ERICSON, MEMBER, IEEE, AND
LASZLO GYÖRFI, MEMBER, IEEE

***Abstract*—Superimposed codes in R^n are introduced, and some existence bounds are obtained. In particular, asymptotic properties of long codes are studied.**

I. Introduction

Superimposed codes were first considered by Kautz–Singleton [1], who considered their application to some retrieval problems in data bases. The concept is, however, also useful in multiple-access communication, and various generalizations and results concerning it have been obtained in recent times by Dyachkov–Rykov [2]–[4], Basalygo–Pinsker [5], Nguyen Quang *et al.* [6], [7], and others. Mathematically superimposed codes are closely related to so-called B_s sequences, which have been considered by Lindström [8]–[11], Frankl–Füredi [12], and others.

We introduce the concept of superimposed codes in Euclidean n-space R^n. Roughly speaking, a superimposed code in R^n is a set $\mathscr{C}$ of vectors x with the property that all possible sums of any m or fewer of these vectors form a set of points all of which are separated by a certain minimum distance d. For such codes we derive in this correspondence an asymptotic existence bound. The proof uses the idea of random coding. It turns out that our existence bound differs only by a factor of four from a nonexistence bound obtained by a simple sphere-packing argument.

II. The Problem

Suppose T users share a communication channel that accepts and reproduces real-valued n vectors. More precisely, suppose the T input signals are of the form

$$x^{(i)} = \left(x_1^{(i)}, x_2^{(i)}, \cdots, x_n^{(i)}\right) \in R^n, \qquad i = 1, 2, \cdots, T$$

where R^n denotes Euclidean n-space and where $x^{(i)} \in R^n$ denotes the input generated by the ith user. The output $y \in R^n$ is given by the ordinary sum of the input vectors

$$y = \sum_{i=1}^{T} x^{(i)}.$$

Now suppose that each one of the T users is equipped with precisely two codewords, one of which is the all-zero sequence $\mathbf{0} = (0, 0, \cdots, 0) \in R^n$, which consequently is shared among all T users. Moreover, suppose that at each transmission at most m of the T inputs are nonzero, where m is usually much smaller than T. Such a situation might arise in a local area data network, or in digital mobile radio, where the common zero codeword is used to indicate a state of inactiveness, while the various nonzero signals are used for identification purposes by those users who are active at the moment. (Other interpretations are possible, see [6], [7], [13], [14].) The problem arises as to how the T nonzero codewords should be chosen to assure that the receiver is always able to determine which codewords have been transmitted, even if the received sequence y is further contaminated by some disturbance.

The communication situation described here is usually referred to as multiple access communication [13, ch. 5.7–5.8]. A central problem is to determine the trade-off between the codelength n, the total number of users T, the maximal allowable number of active users m, and the minimum distance between different received vectors. This is the problem we address. The mathematical formulation follows.

III. The Basic Notations

Let $\mathscr{C}$ be a finite set of unit norm vectors in R^n. For any subset A of $\mathscr{C}$ let $|A|$ denote the cardinality of A, and denote by $f(A)$ the sum of the vectors x in A:

$$f(A) \triangleq \sum_{x \in A} x.$$

Also, for $m = 0, 1, \cdots, T$ define

$$\mathscr{A}(m) \triangleq \{A \subseteq \mathscr{C} : |A| \leq m\}$$

$$\mathscr{C}^{(m)} \triangleq \{f(A) : A \in \mathscr{A}(m)\}$$

$$d_E(\mathscr{C}^{(m)}) \triangleq \min_{A \neq B} \|f(A) - f(B)\|; \qquad A, B \in \mathscr{A}(m).$$

Manuscript received November 4, 1986; revised October 6, 1987. This correspondence was presented at the Third Joint USSR-Swedish International Workshop, Sochi, USSR, May 24–30, 1987.

T. Ericson is with the Department of Electrical Engineering, Institute of Technology, S-581 83 Linköping, Sweden.

L. Györfi is with the Institute for Communication, Technical University of Budapest, Stoczek u.2, H-1521 Budapest, Hungary.

IEEE Log Number 8822700.

The set $\mathscr{C}$ will be said to be a superimposed code with parameters (n, m, T, d) if $|\mathscr{C}| = T$ and $d_E(\mathscr{C}^{(m)}) \geq d$. Clearly, this means that any two sums $f(A)$ and $f(B)$ of at most m vectors in $\mathscr{C}(|A|, |B| \leq m)$ are separated by at least distance d. The norm $\|x\|$ is the usual Euclidean norm

$$\|x\|^2 = \sum_{i=1}^{n} x_i^2,$$

so "distance" simply means ordinary Euclidean distance. Notice that one possible choice for the pair $(A, B) \in \mathscr{A}(m)^2$ is $A = \{x\}$ (a singleton) and $B = \phi$ (the empty set). In that case, $\|f(A) - f(B)\| = \|x\| = 1$. It follows that $d_E(\mathscr{C}^{(m)})$ is never larger than unity, so we restrict the parameter d to the interval $0 < d \leq 1$. The set of all superimposed codes $\mathscr{C}$ with parameters (n, m, T, d) will be denoted $B(n, m, T, d)$. Our problem is to determine for which values of the parameters (n, m, T, d) this set is nonempty. Equivalently, we want to determine the function

$$T(n, m, d) \triangleq \max\{T: B(n, m, T, d) \neq \phi\},$$

and in particular we are interested in the asymptotic behavior of $T(n, m, d)$ as n tends to infinity with m and d fixed. It turns out that $T(n, m, d)$ increases exponentially in n under these circumstances. Let the exponent of increase be defined as

$$E(m, d) \triangleq \limsup_{n \to \infty} \frac{1}{n} \log T(n, m, d).$$

We proceed to obtain upper and lower bounds for this quantity.

IV. A Sphere-Packing Bound

The upper bound is easy. Let $\mathscr{C} \in B(n, m, T, d)$, and consider the induced code $\mathscr{C}^{(m)}$. As each vector $f(A) \in \mathscr{C}^{(m)}$ clearly must be located inside a sphere of radius m, and as different vectors $f(A)$ are separated by at least distance d, we have the following sphere-packing (SP) bound:

$$|\mathscr{C}^{(m)}| = \sum_{i=0}^{m} \binom{T}{i} \leq \left(\frac{m + d/2}{d/2}\right)^n = \left(1 + \frac{2m}{d}\right)^n.$$

From this follows immediately that the exponent $E(m, d)$ is bounded above by the function

$$E_{\mathrm{SP}}(m, d) \triangleq \frac{1}{m} \log\left(1 + \frac{2m}{d}\right).$$

For large m this bound has the form

$$E_{\mathrm{SP}}(m, d) = \frac{1}{m} \log m[1 + 0(1)], \qquad m \to \infty.$$

V. A Random-Coding (RC) Theorem

The lower bound is given by the following result.

Theorem 1: We have $E(m, d) \geq E_{\mathrm{RC}}(m, d)$, where

$$E_{\mathrm{RC}}(m, d) \triangleq \max_{\lambda \geq 0} \min_{1 \leq l \leq m} \frac{1}{2l}\left[F_\lambda(l) - \lambda d^2\right]$$

$$F_\lambda(l) = -\log \sum_{k=-l}^{l} e^{-4\lambda k^2} \binom{2l}{l+k} 2^{-2l}.$$

The function $E_{\mathrm{RC}}(m, d)$ is positive for all (m, d), $m = 0, 1, \cdots$; $0 < d \leq 1$. For large m it has the form

$$E_{\mathrm{RC}}(m, d) = \frac{1}{4} \frac{\log m}{m}[1 + 0(1)].$$

Proof: Consider a sequence $\{\mathscr{C}_n\}_{n=1}^{\infty}$ of codes $\mathscr{C}_n \in B(n, m, T_n, d)$, where the T_n satisfy

$$e^{nR} - 1 < T_n \leq e^{nR}, \qquad n = 1, 2, \cdots$$

for some fixed constant R. We intend to show that $B(n, m, T_n, d) \neq \phi$ for all large enough n as long as R is less than $E_{\mathrm{RC}}(m, d)$. The proof utilizes the idea of random coding. This means that we are going to choose the codes $\mathscr{C}_n$ in a random fashion in such a way that, for large enough n, a positive probability exists that all points in $\mathscr{C}_n^{(m)}$ are separated by at least distance d.

We start by deriving a union bound. Let $\mathscr{C}$ be a randomly selected code (we suppress the index n for the moment), and let $\mathscr{C}^{(m)}$ be the corresponding induced code with elements $f(A)$, $A \in \mathscr{A}(m)$. We have

$$\Pr\left[d(\mathscr{C}^{(m)}) < d\right] = \Pr\left[\bigcup_{A,B} \{\|f(A) - f(B)\| < d\}\right] \leq \sum_{A,B} \Pr\left[\|f(A) - f(B)\| < d\right]$$

where the union and the sum extend over all $A, B \in \mathscr{A}(m)$, $A \neq B$. In fact, it is enough to consider disjoint sets A, B. To see this, simply observe the following obvious identity:

$$f(A) - f(B) = f(A \setminus B) - f(B \setminus A).$$

We will show that $\Pr[d(\mathscr{C}^m) < d]$ is less than unity for large n by providing an exponential bound for each one of the terms $\Pr[\|f(A) - f(B)\| < d]$. The obvious conclusion is then that at least one code $\mathscr{C}$ exists such that the induced code $\mathscr{C}^{(m)}$ satisfies $d(\mathscr{C}^{(m)}) \geq d$, with the consequence $B(n, m, T, d) \neq \phi$. The next step is to specify the code ensemble.

A code $\mathscr{C}$ can be specified by its codeword matrix $X = \{X_{ij}\}$, where X_{ij} is the jth component in the ith codeword, $i = 1, 2, \cdots, T$, $j = 1, 2, \cdots, n$. We specify X (and hence $\mathscr{C}$) by the prescription that all the components X_{ij} shall be chosen independently, with

$$\Pr\left[X_{ij} = \frac{1}{\sqrt{n}}\right] = \Pr\left[X_{ij} = -\frac{1}{\sqrt{n}}\right] = \frac{1}{2}.$$

The resulting code will obviously satisfy the requirement that all codewords should be on the surface of the unit sphere in R^n.

Now let A and B be two fixed disjoint sets of (randomly chosen) code-words, corresponding to the row indices $\{i_1, i_2, \cdots, i_r\}$ and $\{i_{r+1}, i_{r+2}, \cdots, i_{r+s}\}$ of the codeword matrix X. Define the random variables $\{Z_{lj}\}$ according to

$$Z_{lj} \triangleq \begin{cases} X_{i_l j} \cdot \sqrt{n}, & 1 \leq l \leq r \\ -X_{i_l j} \cdot \sqrt{n}, & r+1 \leq l \leq r+s \end{cases}.$$

Then we have

$$\|f(A) - f(B)\|^2 = \frac{1}{n} \sum_{j=1}^{n} \left(\sum_{l=1}^{r+s} Z_{lj}\right)^2.$$

Notice that the variables $\{Z_{lj}\}$ are independent, and distributed according to

$$\Pr[Z_{lj} = 1] = \Pr[Z_{lj} = -1] = \frac{1}{2}.$$

We notice next that if $r + s$ is odd, then certainly $\|f(A) - f(B)\| \geq 1$, so this case can be excluded because of the assumption $0 < d \leq 1$. Hence assume $r + s = 2k$ for some integer k; $1 \leq k \leq m$. By the Chernoff bound (see, for instance, Gallager [15, ch. 5.4])

we have for any $\lambda \geq 0$,

$$\begin{aligned}
&\Pr\left[\|f(A)-f(B)\|<d\right] \\
&\quad=\Pr\left[\sum_{j=1}^{n}\left(\sum_{l=1}^{2k} Z_{lj}\right)^2 < n\cdot d^2\right] \\
&\quad\leq e^{n\lambda d^2}\cdot E\exp\left\{-\lambda\sum_{j=1}^{n}\left(\sum_{l=1}^{2k} Z_{lj}\right)^2\right\} \\
&\quad= e^{n\lambda d^2}\prod_{j=1}^{n} E\exp\left\{-\lambda\left(\sum_{l=1}^{2k} Z_{lj}\right)^2\right\}.
\end{aligned}$$

However, the Z_{lj} are identically distributed, so for each j we have

$$\begin{aligned}
&E\exp\left\{-\lambda\left(\sum_{l=1}^{2k} Z_{lj}\right)^2\right\} \\
&\quad=\sum_{\nu=-k}^{k} e^{-4\lambda\nu^2}\Pr\left[\sum_{l=1}^{2k} Z_{lj}=2\nu\right] \\
&\quad=\sum_{\nu=-k}^{k} e^{-4\lambda\nu^2}\binom{2k}{k+\nu}2^{-2k}.
\end{aligned}$$

Denote this quantity by $G_\lambda(k)$. We obviously have

$$0<G_\lambda(k)<1, \qquad 1<k<m, 0<\lambda<1.$$

Further, define

$$F_\lambda(k) \triangleq -\log G_\lambda(k).$$

We clearly have $F_\lambda(k)>0$, and our Chernoff bound takes the form

$$\Pr\left[\|f(A)-f(B)\|<d\right] \leq \exp\left\{-n\left[F_\lambda(k)-\lambda d^2\right]\right\}.$$

A set A of size $|A|=r$ can be chosen from a set $\mathscr{C}$ of size $|\mathscr{C}|=T$ in $\binom{T}{r}$ different ways, and a disjoint *ordered* pair (A, B) with $|A|=r$, $|B|=s$ can be chosen in

$$\binom{T}{r}\binom{T-r}{s}$$

different ways. Observing the simple bound

$$\binom{T}{r}\binom{T-r}{s} < T^{r+s}=T^{2k}$$

and neglecting the fact that we actually need only to consider *unordered* pairs $\{A, B\}$, we get the bound

$$\begin{aligned}
&\Pr\left[d\left(\mathscr{C}_n^{(m)}\right)<d\right] \\
&\quad\leq\sum_{k=1}^{m} T_n^{2k}\exp\left\{-n\left[F_\lambda(k)-\lambda d^2\right]\right\} \\
&\quad\leq\sum_{k=1}^{m}\exp\left\{-n\left[F_\lambda(k)-\lambda d^2-2kR\right]\right\}.
\end{aligned}$$

We have also neglected the obvious condition $2m \leq T$. We have reintroduced the index n, and in the last step we have utilized the assumption

$$T_n < e^{nR}.$$

By straightforward computations the following relations are established:

$$\left[F_\lambda(k)\right]_{\lambda=0}=0$$

$$\left[\frac{\partial}{\partial\lambda}F_\lambda(k)\right]_{\lambda=0}>1.$$

As $d<1$, it follows by continuity that for each k the inequality

$$F_\lambda(k)+\lambda d^2>0$$

is satisfied for some $\lambda>0$. In particular, we have

$$E_{\mathrm{RC}}(m,d) \triangleq \max_{\lambda\geq 0}\min_{1\leq k\leq m}\frac{1}{2k}\left[F_\lambda(k)-\lambda d^2\right]>0,$$

for all (m,d), $m=0,1,2,\cdots[T/2]$, $0<d\leq 1$.

As our bound on $\Pr[d(\mathscr{C}_n^{(m)})<d]$ holds for any $\lambda\geq 0$, we have for all large enough n the bound

$$\Pr\left[d\left(\mathscr{C}_n^{(m)}\right)<d\right] \leq \exp\left\{-n\left[E_{\mathrm{RC}}(m,d)-R-\delta\right]\right\}$$

where $\delta>0$ is arbitrary. It follows that as long as R is strictly less than $E_{\mathrm{RC}}(m,d)$ there is, for all large enough n, a positive probability of finding a code $\mathscr{C}_n$ such that the induced code $\mathscr{C}_n^{(m)}$ has minimal distance $d(\mathscr{C}_n^{(m)})\geq d$. Hence such codes do exist. The exponent $E(m,d)$ is the supremum of all constants R such that $B(n,m,T_n,d)\neq\phi$ for all large enough n and all $T_n\leq e^{nR}$. It follows that $E(m,d)\geq E_{\mathrm{RC}}(m,d)$.

It remains to derive the asymptotic form of $E_{\mathrm{RC}}(m,d)$ as $m\to\infty$. We defer this straightforward computation to the Appendix. This concludes the proof.

VI. Concluding Remarks

It is interesting to notice that for large m the random-coding bound and the sphere-packing bound differ only by a factor of four. It is also interesting that, asymptotically for large m, both bounds are independent of the distance parameter d. We have not been able to determine whether this is also the case with the true exponent $E(m,d)$, but we conjecture this is the case.

Appendix
Asymptotic Bounds on $E_{\mathrm{RC}}(m,d)$ as $m\to\infty$

Recall the definition of $G_\lambda(l)$:

$$\begin{aligned}
G_\lambda(l) &\triangleq \sum_{k=-l}^{l} e^{-4\lambda k^2}\binom{2l}{l+k}2^{-2l} \\
&=\binom{2l}{l}2^{-2l}+2\cdot 2^{-2l}\sum_{k=1}^{l} e^{-4\lambda k^2}\binom{2l}{l+k}.
\end{aligned}$$

Using $e^{-4\lambda k^2}\leq e^{-4\lambda k}$ and $\binom{2l}{l+k}\leq\binom{2l}{l}$, we get

$$\begin{aligned}
G_\lambda(l) &\leq \binom{2l}{l}2^{-2l}\left[1+2\sum_{k=1}^{l} e^{-4\lambda k}\right] \\
&\leq \binom{2l}{l}2^{-2l}\left[1+\frac{2\cdot e^{-4\lambda}}{1-e^{-4\lambda}}\right]=c_l\frac{1+x}{1-x}
\end{aligned}$$

where we have introduced

$$c_l \triangleq \binom{2l}{l}2^{-2l}, \qquad x\triangleq e^{-4\lambda}.$$

We get

$$F_\lambda(l)=-\log G_\lambda(l)\geq\log\frac{1}{c_l}\frac{1-x}{1+x}.$$

By definition we have for each $\lambda\geq 0$ (or, which is the same, for each x, $0\leq x<1$)

$$\begin{aligned}
E_{\mathrm{RC}}(m,d) &\geq \min_{1\leq l\leq m}\frac{1}{2l}\left[F_\lambda(l)-\lambda d^2\right] \\
&\geq \min_{1\leq l\leq m}\frac{1}{2l}\left[\log\frac{1}{c_l}\frac{1-x}{1+x}+\frac{d^2}{4}\log x\right] \\
&= \min_{1\leq l\leq m}\frac{1}{2l}\log\frac{1}{c_l}\frac{1-x}{1+x}x^{d^2/4}.
\end{aligned}$$

In particular, the bound holds for $x = x_0$, where x_0 satisfies

$$\max_{0 \le x < 1} \frac{1-x}{1+x} x^{d^2/4} = \frac{1-x_0}{1+x_0} x_0^{d^2/4} \triangleq A(d).$$

Thus

$$E_{RC}(m,d) \ge \min_{1 \le l \le m} \frac{1}{2l} \log \frac{A(d)}{c_l}.$$

The quantity c_l is bounded as follows:

$$\sqrt{\frac{1}{4l}} < c_l < \sqrt{\frac{1}{\pi l}}$$

(see Gallager [17, p. 430]), and as a consequence we have

$$E_{RC}(m,d) \ge \min_{1 \le l \le m} \frac{1}{2l} \log \sqrt{\pi l} A(d).$$

Clearly, for large m this bound reads

$$E_{RC}(m,d) \ge \frac{1}{4m} \log \pi m A^2(d) \sim \frac{1}{4} \frac{\log m}{m}.$$

On the other hand, we also have

$$G_\lambda(l) \ge \binom{2l}{l} 2^{-2l} = c_l \ge \sqrt{\frac{1}{4l}},$$

and thus

$$F_\lambda(l) \le \log \sqrt{4l}.$$

We generally have

$$E_{RC}(m,d) \triangleq \max_{\lambda \ge 0} \min_{1 \le l \le m} \frac{1}{2l} \left[F_\lambda(l) - \lambda d^2 \right]$$

$$\le \min_{1 \le l < m} \max_{\lambda \ge 0} \frac{1}{2l} \left[F_\lambda(l) - \lambda d^2 \right].$$

Thus for each l, $1 \le l \le m$, we have

$$E_{RC}(m,d) \le \max_{\lambda \ge 0} \frac{1}{2l} \left[F_\lambda(l) - \lambda d^2 \right]$$

$$\le \max_{\lambda \ge 0} \frac{1}{2l} \left[\log \sqrt{4l} - \lambda d^2 \right]$$

$$= \frac{1}{2l} \log \sqrt{4l}.$$

In particular, choosing $l = m$, we get

$$E_{RC}(m,d) \le \frac{1}{2m} \log \sqrt{4m} \sim \frac{1}{4} \frac{\log m}{m}.$$

REFERENCES

[1] W. K. Kautz and R. C. Singleton, "Nonrandom binary superimposed codes," *IEEE Trans. Inform. Theory*, vol. IT-10, pp. 363–377, Oct. 1964.

[2] A. G. Dyachkov and V. V. Rykov, "Bounds on the length of disjunctive codes," *Probl. Peredach. Inform.*, vol. 18, no. 3, pp. 7–13, 1982.

[3] ____, "On a coding model for adder multiple-access channel," *Probl. Peredach Inform.*, vol. 17, no. 2, pp. 26–38 (English translation pp. 94–104), 1981.

[4] ____, "Survey of superimposed code theory," *PCIT*, vol. 12, no. 4, pp. 229–244, 1983.

[5] L. A. Bassalygo and M. S. Pinsker, "Limited multiple-access of a non-synchronous channel," *Probl. Peredach. Inform.*, vol. 19, no. 4, pp. 92–96, 1983.

[6] A. Nguyen Quang, L. Györfi, and J. L. Massey, "Some constructions of protocol sequences for collision channel without feedback and a class of optimal cyclic constant weight codes," in *Proc. IEEE Int. Symp. Information Theory*, June 1985, Brighton, England.

[7] ____, "Some constructions of cyclic sets, constant weight codes," unpublished.

[8] B. Lindström, "On a combinatorial detection problem I," *Pub. Math. Inst. Hungarian Acad. Sci.*, vol. 19, pp. 195–207, 1964.

[9] ____, "On a combinatorial detection problem II," *Studia Sci. Math., Hungary*, vol. 1, pp. 353–361, 1965.

[10] ____, "A theorem on families of sets," *J. Comb. Theory*, vol. 13, no. 2, Sept. 1972.

[11] ____, "On B_2-sequences of vectors," *J. Number Theory*, vol. 4, no. 3, pp. 261–265, 1972.

[12] P. Frankl and Z. Füredi, "Union-free hypergraphs and probability theory," *Europ. J. Comb.*, vol. 5, pp. 127–131, 1984.

[13] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, vol. I, Rockville, MD: Computer Science Press, 1985.

[14] J. E. Mazo, "Some theoretical observations on spread spectrum communications," *Bell Syst. Tech. J.*, vol. 58, no. 9, pp. 2013–2023, 1979.

[15] R. G. Gallager, *Information and Reliable Communication*. New York: Wiley, 1968.

On Decoding Rules to Minimize the Probability of Information Bit Errors

BRUCE L. MONTGOMERY, MEMBER, IEEE, AND
B. V. K. VIJAYA KUMAR, MEMBER IEEE

***Abstract*—Decoding rules to minimize the probability of information bit errors in binary linear block codes are investigated. A new rule is proposed and is shown to be the best possible according to a certain criterion.**

1. INTRODUCTION

Let C be a binary linear block code of length n, dimension k, and minimum distance $2e+1$. We shall refer to C as an $[n, k, 2e+1]$ code. Let H be a parity check matrix for C. In the decoding of C by a standard array with coset leaders of minimum weight, the syndrome $\boldsymbol{s} = \boldsymbol{r}H^T$ of the received word $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ is computed, where $\boldsymbol{e}$ is the error pattern (all vectors are row vectors). Since $\boldsymbol{c}H^T = \boldsymbol{0}$ iff $\boldsymbol{c} \in C$, then $\boldsymbol{s} = \boldsymbol{e}H^T$. The coset determined by $\boldsymbol{s}$ is $\{\boldsymbol{x}: \boldsymbol{x}H^T = \boldsymbol{s}\}$. An array, which gives for each syndrome $\boldsymbol{s}$ a minimum-weight element $\boldsymbol{z}^*$ (the coset leader) in the coset determined by $\boldsymbol{s}$, is searched (for $\boldsymbol{s}$), and the received word $\boldsymbol{r}$ is decoded $\boldsymbol{r} + \boldsymbol{z}^*$.

The decoding of binary linear block codes by the use of a standard array with coset leaders of minimal weight has been shown [1] to minimize the average probability of codeword error on the binary symmetric channel (BSC). This decoding scheme, denoted S_1, does not necessarily minimize the average probability P_b of information bit error [2]. The following decoding rule, denoted S_2, was shown in [2] to yield a smaller value of P_b than S_1 (at least for sufficiently small p, the probability of a bit error on the BSC) for several classes of quasi-perfect codes.

S_2: For systematic $[n, k, 2e+1]$ codes, correct (using the standard array) any error pattern if the coset leader has weight e or less. Otherwise, take the information bits as received.

The number of cosets of an $[n, k, 2e+1]$ code is 2^{n-k}, and the number of cosets having a coset leader of weight e or less is $\sum_{i=0}^{e} \binom{n}{i} = F(n, e)$. Thus in implementing S_2 it is not necessary to store the $2^{n-k} - F(n,e)$ (>0 for any nonperfect code) syndromes and coset leaders. Also, the resulting smaller array can be searched more quickly than the complete array. Hence S_2 is

Manuscript received February 17, 1987; revised August 21, 1987.

B. Montogmery was with Carnegie Mellon University, Pittsburg, PA. He is now with the Department of Electrical Engineering, University of Pittsburg, Pittsburg, PA 15261.

B. V. K. Vijaya Kumar is with the Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA 15213.

IEEE Log Number 8822699.