[7] J. L. Massey "Error bounds for tree codes, trellis codes, and convolutional codes with encoding and decoding procedures," in *Coding and Complexity,* G. Longo, Ed. New York: Springer, 1976.
[8] A. J. Viterbi and J. K. Omura, *Principles of Digital Communication and Coding.* New York: McGraw-Hill, 1979.
[9] A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," *IEEE Trans. Inform. Theory,* vol. IT-13, Apr. 1967, pp. 260–269.
[10] R. Bellman and S. Dreyfus, *Applied Dynamic Programming.* Princeton, NJ: Princeton Univ. Press, 1962.
[11] G. J. Minty, "A comment on the shortest route problem," *Oper. Res.,* vol. 5, p. 724, Oct. 1957.
[12] R. S. Muller and T. I. Kamins, *Device Electronics for Integrated Circuits.* New York: Wiley, 1977.
[13] J. B. Dennis, *Mathematical Programming and Electrical Networks.* New York: Wiley, 1959.
[14] M. Iri, *Network Flow, Transportation and Scheduling—Theory and Algorithms.* New York: Academic Press, 1969.
[15] G. V. Karandakov, "Network shortest path detector—Is simplified using spark elektrodes between graph nodes," Soviet patent appl. SU 397 931, 1974.
[16] L. V. Fedotov, V. I. Mikhailenk, and S. V. Ozirskii, "Graph shortest path determination apparatus," Soviet patent appl. SU 1 488 824, 1989.
[17] A. V. Kholin, "Shortest path computing circuit," Soviet patent appl. SU 552 617, 1977.
[18] A. A. Lelis, V. A. Klishin, and G. S. Polishchuk, "Topological graph shortest path finder," Soviet patent appl. SU 1 314 354, 1987.

Normal and Abnormal Codes

Tuvi Etzion, *Member, IEEE*, Gadi Greenberg, and Iiro S. Honkala

***Abstract*—It is proved that codes of length n, covering radius R, and minimum Hamming distance $2R-1$ are normal if R does not divide n. Constructions for abnormal codes with covering radius R and minimum Hamming distance at least $R-1$ are given.**

***Index Terms*— BCH code, covering radius, Hamming code, normal code, Preparata code, quasi-perfect code.**

I. Introduction

Much research in the area of covering radius is on the normality of the codes. The main reason is that by using the amalgamated direct sum [1] one can generate from normal codes sparse covering codes with larger covering radius. For two words $x = x_1x_2\cdots x_n$, $y = y_1y_2\cdots y_n$ of length n the *Hamming distance* (distance in short) between x and y, $d(x,y)$ is defined by $d(x,y) = |\{i: x_i \neq y_i\}|$, the *support* of x, supp $(x) = \{i: x_i = 1\}$, and the weight of x, $W(x) = |\,supp\,(x)|$. The minimum distance of a code C, $d(C) = \min_{\substack{x,y\in C \\ x\neq y}} d(x,y)$. For a word x, $d(x,C) = \min_{c\in C} d(x,c)$ is the distance of x from C. The covering radius of C is R if $R = \max_{x\in F_2^n} d(x,C)$. An $(n,d)R$ code C is a code of length n, covering radius at most R, and minimum distance at least d. If $C_a^{(i)} = \{c \in C: c_i = a\}$ then C is *normal* if there exists a coordinate i such that

$$d(x, C_0^{(i)}) + d(x, C_1^{(i)}) \leq 2R+1, \qquad \text{for } x \in F_2^n, \tag{1}$$

where $d(x,\phi) = n$. If (1) holds for coordinate i we say that coordinate i is acceptable. If C is not normal then it is an *abnormal* code. An interesting question in this context is to determine which codes are normal and which codes are abnormal. One important factor is the ratio between the covering radius of the code and its minimum distance. van Wee [8] proved that all $(n,\ 2R)R$ codes and all $(n,\ 2R+1)R$ codes are normal. Hou [5] proved that all linear quasi-perfect codes (codes with covering radius R and minimum distance at least $2R-1$), are normal. In Section II we prove that an $(n,\ 2R-1)R$ code is normal, if R does not divide n. Frankl [6] proved that there are abnormal codes with covering radius 1. van Wee [8] (see also Honkala and Hämäläinen [3]) showed that for each R there exists n_0 such that for each $n \geq n_0$ there exists an abnormal code with covering radius R. It is not known whether linear abnormal codes exist. In Section III we give a construction for abnormal $(n,R)R$ codes if some conditions hold. We apply this construction to obtain such codes for $R \leq 6$. Another construction produce an abnormal $(n, d-1)R+1$ code if there exists an $(n,d)R$ code and some conditions hold. Consequences of this construction are that for each $R \geq 1$, there exists an n_0, such that for each $n \geq n_0$ there exists an abnormal $(n, R-1)R$ code, and for each $R \geq 1$ there exists an m_0 such that for all $m \geq m_0$ there exists either an abnormal $(2^m-1, R)R$ code or an abnormal $(2^m, R)R$ code. Another consequence is the existence of abnormal $(n,\ 3)2$, $(n,4)3$, and $(n,\ 5)4$ codes.

II. Normal Quasi-Perfect Codes

As previously stated it is known that all linear quasi-perfect codes are normal [5] and $(n,d)R$ codes with $d \geq 2R$ are normal [8]. These results are strengthened with the following theorem.

Theorem 1: If C is an $(n,\ 2R-1)R$ code, where R does not divide n, then C is normal and all its coordinates are acceptable.

Proof: Assume the contrary, i.e., that one of the coordinated is not acceptable. W.l.o.g. we can assume it is the first coordinate. Let $x \in F_2^n$ be a word for which

$$d(\boldsymbol{x}, C_0^{(1)}) + d(\boldsymbol{x}, C_1^{(1)}) > 2R+1. \tag{2}$$

Let $t = d(\boldsymbol{x}, C)$ and let $c \in C$ be a codeword for which $d(\boldsymbol{x}, c) = t$. W.l.o.g. we can assume that c is the all zero codeword and hence $t = W(\boldsymbol{x})$. We distinguish between two cases.

Case 1: $0 \leq t \leq R-1$. Again w.l.o.g. we can assume that the t 1's of $\boldsymbol{x}$ are in the first R coordinates. Consider the word

$$y_0 = 1^{R+1}0^{n-R-1}.$$

Let $z_0 \in C$ be the codeword for which $d(y_0, z_0) \leq R$. Since $W(y_0) = R+1$ and $d(C) = 2R-1$, it follows that $2R-1 \leq W(z_0) \leq 2R+1$. If $W(z_0) \geq 2R$ then z_0 covers all the 1's of y_0 and hence, $z_0 \in C_1^{(1)}$. Therefore, we have

$$\begin{aligned} d(\boldsymbol{x}, C_0^{(1)}) + d(\boldsymbol{x}, C_1^{(1)}) &\leq d(\boldsymbol{x}, 0) + d(\boldsymbol{x}, z_0) \\ &\leq t + 2R + 1 - t = 2R+1 \end{aligned}$$

in contradiction to (2) and therefore $W(z_0) = 2R-1$. Hence, z_0 has at least R ONES in the first $R+1$ coordinates and therefore z_0

Manuscript received March 26, 1992.
T. Etzion is with the Computer Science Department, Technion, Haifa 32000, Israel. This work was supported in part by Technion V.P.R. Fund and in part by the fund for the promotion of research at the Technion.
G. Greenberg is with the Mathematics Department, Technion, Haifa 32000, Israel.
I. S. Honkala is with the Department of Mathematics, University of Turku, 20500 Turku, Finland.
IEEE Log Number 9209054.

covers at least $t-1$ ONES of $\boldsymbol{x}$. If $z_0 \in C_1^{(1)}$ then

$$d(\boldsymbol{x}, C_0^{(1)}) + d(\boldsymbol{x}, C_1^{(1)}) \le d(\boldsymbol{x}, 0) + d(\boldsymbol{x}, z_0) \le t + 2R - 1 - (t-1) + 1 = 2R + 1$$

in contradiction to (2). If $z_0 \in c_0^{(1)}$ then w.l.o.g.,

$$z_0 = 01^{2R-1}0^{n-2R}.$$

Consider the word

$$y_1 = 1^R 0^R 1 0^{n-2R-1}.$$

Let $z_1 \in C$ be the codeword for which $d(y_1, z_1) \le R$. By using the same arguments on z_1 and y_1 as on z_0 and y_0 we have that $W(z_1) = 2R-1$, the first coordinate of z_1 is ZERO and the next $R-1$ coordinates are ONES. Since $d(z_0, z_1) \ge 2R-1$, it follows that w.l.o.g.,

$$z_1 = 01^{R-1}0^R 1^R 0^{n-3R}.$$

If we continue in the same manner we will obtain that the word

$$y_i = 1^R 0^{iR} 1 0^{n-(i+1)R-1}, \qquad 0 \le i \le \frac{n-2R}{R}$$

is covered by the codeword

$$z_i = 01^{R-1}0^{iR}1^R 0^{n-(i+2)R}, \qquad 0 \le i \le \frac{n-2R}{R}$$

which contradicts our assumption that R does not divide n.

Case 2: $t = R$.

If the first coordinate of $\boldsymbol{x}$ is ONE then we can assume that $\boldsymbol{x} = 1^R 0^{n-R}$ and this case is handled exactly as Case 1.

If the first coordinate of $\boldsymbol{x}$ is ZERO then we can assume that $\boldsymbol{x} = 01^R 0^{n-R-1}$. Again, consider the word

$$y = 1^{R+1}0^{n-R-1}.$$

Let $z \in C$ be the codeword for which $d(y, z) \le R$. By the same arguments as in Case 1, we can obtain that $W(z) = 2R-1$ and z has at least R ONES in the first $R+1$ coordinates.

If $z \in C_1^{(1)}$, then

$$d(\boldsymbol{x}, C_0^{(1)}) + d(\boldsymbol{x}, C_1^{(1)}) \le d(\boldsymbol{x}, 0) + d(\boldsymbol{x}, z) \le R + 2R - 1 - (R-1) + 1 = 2R + 1$$

in contradiction to (2).

If $z \in C_0^{(1)}$ then $d(\boldsymbol{x}, z) = R-1$ in contradiction to our assumption that $d(\boldsymbol{x}, C) = R$.

Thus, C is normal. □

As wee will see in the next section, it would be difficult to extend Theorem 1, since abnormal $(2^n, 3)2$ codes exist.

III. Abnormal Codes

It is interesting to know what is the largest possible minimum distance of an abnormal code with covering radius R. All the abnormal codes which are known [3], [6], [8] have minimum distance 1. First, we will present a construction which produces abnormal $(n, R)R$ codes if some conditions hold. This construction is especially good for small R, and we will apply this construction for each $R \le 6$ and most lengths. We also think that this construction and the discussion which follows it have their own independent interest. Then, we will strengthen this construction and show that abnormal $(n, R)R$ codes exist for all R. The construction that we use is a modification of the constructions of Frankl [6] and van Wee [8]. Our construction uses maximal codes, i.e., codes for which addition of words destroys the minimum distance. Cohen *et al.* [2] observed that an $(n, d)R$ code C is maximal if and only if $d > R$.

Construction A: Let C^* be a maximal $(n, d)R$ code. Suppose we have n words $x^{(i)} \in F_2^n$, $1 \le i \le n$, such that $x_i^{(i)} = 0$ and $d(x^{(r)}, x^{(s)}) \ge 6d+1$, for $r \ne s$. Then, let $T_i = \{y \in F_2^n : d(y, x^{(i)}) \le 2d \text{ and } y_i = 0\}$, $1 \le i \le n$, and define $C = C^* \backslash (T_1 \cup T_2 \cup \cdots \cup T_n)$.

Lemma 1: If one of the T_i's includes a codeword then the covering radius of C is at least d.

Proof: If $x \in C^* \cap T_i$ then $x \notin C$. Therefore, since the minimum distance of C^* is d it follows that $d(x, C) \ge d$ and the covering radius of C is at least d. □

Lemma 2: If C^* is normal then there exists a codeword $c \in C^* \cap T_i$ for some i.

Proof: Let coordinate i of C^* be acceptable and assume that all the members of T_i do not belong to C^*. Hence, and by the definitions of $x^{(i)}$ and T_i, we have that $d(x^{(i)}, (C^*)_0^{(i)}) > 2d$ and $d(x^{(i)}, (C^*)_1^{(i)}) \ge 1$. Therefore, $d(x^{(i)}, (C^*)_0^{(i)}) + d(x^{(i)}, (C^*)_1^{(i)}) > 2d+1 > 2R+1$, in contradiction to (1). Thus, since C^* is normal there exists a codeword $c \in C \cap T_i$ for some i. □

If our code C^* is not normal then we already have an abnormal code with minimum distance d and covering radius $R, R < d$. Henceforth, we will assume that C^* is normal. By Lemma 2, our construction removes a codeword from C^* if C^* is normal. Hence, by Lemma 1, the covering radius of the resulting code C is at least d. Our construction also needs a set of words $x^{(i)}$, $1 \le i \le n$, such that $x_i^{(i)} = 0$ and $d(x^{(i)}, x^{(j)}) \ge 6d+1$, for $i \ne j$. As in van Wee [8] one can easily verify that for any d there exists an n_0 such that for all $n \ge n_0$ such a set exists.

Theorem 2: If the covering radius of C is d then C is an abnormal code.

Proof: For each i, $1 \le i \le n$, by the definitions of $x^{(i)}$ and T_i we have that $d(x^{(i)}, C_0^{(i)}) > 2d$ and $d(x^{(i)}, C_1^{(i)}) \ge 1$. Thus, $d(x^{(i)}, C_0^{(i)}) + d(x^{(i)}, C_1^{(i)}) > 2d+1$, coordinate i is not acceptable for each i, and C is abnormal. □

By Lemmas 1 and 2 the covering radius of C obtained in construction A is a least d. Now we will give a sufficient condition that Construction A will produce a code C with covering radius d from a linear code C^*. for a simpler presentation we will use the following definition given in Hou [4]. Let C be a linear code of length n and dimension k with parity check matrix H. For a nonzero syndrome $s \in F_2^m (m = n-k)$, let $h^i(s) =$ the minimal number of columns of H, not containing the ith column, summing to s ($h^i(s) = n$ if no such sum exists).

Lemma 3: If C^* is an $(n, d)R$ linear code with parity check matrix H^*, and $h^i(s) \le d-1$ for each s and $1 \le i \le n$, then C, obtained by Construction A, is an abnormal code with covering radius d.

Proof: Given a word x, let i be an integer such that $d(x, T_i) \le d$. If no such i exists then for some $c \in C^*$, $d(x, c) \le R$, $c \in C$, and hence $d(x, c) \le R < d$. Since $d(x^{(i)}, x^{(j)}) \ge 6d+1$, for $i \ne j$, and the words of T_i are within radius $2d$ from $x^{(i)}$, if follows that i is unique. Let y be the word obtained from x by setting $y_j = x_j$, $1 \le j \le n$, $j \ne i$, and $y_i = 1$. Let $u = H^* y^T$ and let S be the set of $d-1$ or less coordinates, not containing the ith one, which sum to u. Let z the word obtained from y by changing the coordinates of S. Since $H^* y^T + u = 0$ and $z_i = 1$, it follows that $z \in C^*$ and $z \notin T_j$ for each j. Therefore $z \in C$, $d(x, z) \le d$ and the covering radius of C is d. □

Note that Lemma 3 gives sufficient condition that Construction A will obtain an abnormal code. But, this condition might not be a

necessary condition. Also note that the condition of Lemma 3 is not sufficient if n and d are such that no set of $x^{(i)}$'s exists. Construction A can be applied on different codes by using the sufficient condition of Lemma 3.

Before preceding, for two examples, we give the definitions of *shortened* and *punctured* codes [7, pp. 28–29]. A code is punctured by deleting a certain coordinate from each codeword. A code is shortened by taking all the codewords with $x_i = 0$, for a given i, and then deleting coordinate i. In the sequel, we also make use of the well known fact that the covering radius R of a linear code C is equal to the weight of the coset leader with the greatest weight. This means that if C has an $m \times n$ parity check matrix H, then each nonzero syndrome $s \in F_2^m$ can be represented as a linear combination of R of less columns from H.

A. The Hamming Code

This code of length $2^m - 1$ and minimum distance 3, has a parity check matrix which consists of $2^m - 1$ column vectors of length m. Column i, $1 \leq i \leq 2^m - 1$, is a binary representation of i. It is not difficult to see that Lemma 3 holds for this code.

If we delete the last $2^{m-1} - 2$ columns we can easily verify that Lemma 3 still holds and therefore, by shortening the Hamming code up to $2^{m-1} - 2$ times, we obtain codes on which we can apply Construction A to construct abnormal $(n, 3)3$ codes.

B. Double Error-Correcting Primitive BCH Code

The double error-correcting primitive BCH code has length $2^m - 1$, distance 5, covering radius 3, and hence it is a quasi-perfect code. We will discuss the case of odd m. In this case, it is known [7, pp. 171–172] that for each i, $1 \leq i \leq 3$, all the cosets with coset leader of weight i have the same weight distribution. Each coset with coset leader of weight 3 has $\frac{2^{m-1}-1}{3}$ words of weight 3. Each coset with coset leader of weight 2 has $\frac{2^{m-1}-1}{3} - 1$ words of weight 3. This implies that each two columns of C^* are covered exactly $\frac{2^{m-1}-1}{3} - 1$ times by codewords of weight 5. Assume column i of H^* was deleted and we want to find a linear combination of 4 or less columns which sums to a nonzero syndrome s. The only problem that we might have is if s can derived by a linear combination of t columns from H^*, $t \leq 3$, which includes column i. If $t = 3$, and s is a combination of columns i, j_1, and j_2, then there is a codeword c with $\text{supp}(c) = \{i, j_1, r_1, r_2, r_3\}$. Hence, the linear combination of columns j_2, r_1, r_2, and r_3 sums to s. Similar arguments hold for $t = 1$ and $t = 2$. Thus, Lemma 3 holds for this code.

Note that for each two different words x, y of weight less than 4 in a coset, $\text{supp}(x) \cap \text{supp}(y) = \phi$ since the code has minimum distance 5. Hence, if we delete $\frac{2^{m-1}-1}{3} - 2$ columns we still have the same arguments and therefore Lemma 3 holds also when the code is shortened at most $\frac{2^{m-1}-1}{3} - 2$ times, and by applying Construction A, we construct abnormal $(n, 5)5$ codes.

We have also applied Construction A on the following codes.

1) The even weight code to obtain abnormal $(n,2)2$ codes for each $n \geq n_0$ for some n_0.
2) From the extended Hamming code of length 2^m and its shortening up to $2^{m-1} - 2$ times we obtain abnormal $(n, 4)4$ codes.
3) From the extended double error-correcting primitive BCH code of length 2^m, m odd, and its shortenings up to $\frac{2^{m-1}-1}{3} - 2$ times we obtain abnormal $(n, 6)6$ codes.

Construction A can be also applied on some nonlinear codes.

1) From the punctured Preparata code of length $2^{2m} - 1$ and its shortenings up to $\frac{2^{2m}-1}{3} - 2$ times we obtain abnormal $(n, 5)5$ codes.
2) From the Preparata code of length 2^{2m} and its shortenings up to $\frac{2^{2m}-1}{3} - 2$ times we obtain abnormal $(n, 6)6$ codes.

We now give a more general construction for abnormal codes by a modification of Construction A.

Construction B: Let C^* be an $(n, d)R$ code. Suppose we have n words $x^{(i)} \in F_2^n$, $1 \leq i \leq n$, such that $x_i^{(i)} = 0$ and $d(x^{(r)}, x^{(s)}) \geq 4R+d+5$, $r \neq s$. Then, let $T_i = \{y \in F_2^n : d(y, x^{(i)}) \leq 2(R+1)$ and $y_i = 0\}$, $S_i = \{z \in F_2^n : d(y, z) = 1$, for some $y \in T_i \cap C^*$, and $z_i = 1\}$, $1 \leq i \leq n$, and define $C = C^* \cup (\cup_{i=1}^n S_i) \backslash (\cup_{i=1}^n T_i)$.

Theorem 3: C obtained by Construction B is an abnormal $(n, d-1)R + 1$ code.

Proof: Clearly, the covering radius of C is at most $R + 1$, and as in Theorem 2 we can prove that C is abnormal. The minimum distance of C follows from the facts that in each codeword of T_i we have changed the ith coordinate to obtain a codeword in S_i, and for $z_i \in T_i$, $z_j \in T_j$, $i \neq j$, $d(z_i, z_j) \geq 4R + d + 5 - 2(R + 1) - 2(R + 1) = d + 1$. □

Note, that if we can settle for minimum distance $d - 2$ instead of $d - 1$ then it is enough to require $d(x^{(r)}, x^{(s)}) \geq 4R + 6$, $r \neq s$ in Construction B ($4R + 5$ is not enough since we might have $d(x^{(i)}, y) = 2R + 2$ for $y \in S_j$, $j \neq i$, where $y_i = 0$ and the code might be normal). Again, as in van Wee [8], one can prove that for each R and d there exists an n_0, such that for all $n \geq n_0$, a set of $x^{(i)}$'s exists. Also if we have an $(n, d)R$ code, C, with $R \geq d$, then we can add codewords to C, without destroying the minimum distance d. Therefore, for each n and d, there exist a maximal code of length n and minimum distance at least d. Hence, by applying Construction B we have Theorem 4.

Theorem 4: For each $R \geq 1$, there exists an n_0 such that for each $n \geq n_0$ there exists and abnormal $(n, R-1)R$ code.

Vladuts and Skorobogatov [9] proved that for any given t, there exists an m_0 such that for all $m \geq m_0$ the covering radius of the primitive BCH code of length $2^m - 1$ with designed distance $2t+1$ is $2t-1$. The corresponding extended BCH code has minimum distance $2t + 2$ and covering radius $2t$. Hence, by applying Construction B on these codes we have Theorem 5.

Theorem 5: For each t there exists an m_0 such that for all $m \geq m_0$ there exists an abnormal $(2^m - 1, 2t)2t$ code and an abnormal $(2^m, 2t + 1)2t + 1$ code.

Finally, we if C^* has some more properties than we can obtain abnormal codes with larger covering radius.

Construction C: Let C^* be an $(n, d)R$ code for which the words of weight R, in each translate with translate leader of weight R, cover all coordinates, and their complements also cover all coordinates. Suppose we have n words $x^{(i)} \in F_2^n$, $1 \leq i \leq n$, such that $x_i^{(i)} = 0$ and $d(x^{(r)}, x^{(s)}) \geq 6R + 1$, $r \neq s$. Then, let $T_i = \{y \in F_2^n : d(y, x^{(i)}) \leq 2R$ and $y_i = 0\}$, $S_i = \{z \in F_2^n : d(y, z) = 1$, for some $y \in T_i \cap C^*$, and $z_i = 1\}$, $1 \leq i \leq n$, and define $C = C^* \cup (\cup_{i=1}^n S_i) \backslash (\cup_{i=1}^n T_i)$.

Theorem 6: the code C obtained in Construction C is an abnormal $(n, d-1)R$ code.

Proof: Obviously, each word with distance less that R from C^* has distance at most R from C. For a word z with distance R from C^*, let $z_1, z_2 \in C^*$ such that $d(z, z_1) = d(z, z_2) = R$. Similarly to the proof of Lemma 3, we can prove that if $z_1 \in T_i$ for some i then $z_2 \notin T_j$ for each j, $i \neq j$. By the properties of the translates of C^* it follows that for each i there exists at least one codeword $v \in C^*$, for which $d(z, v) = R$ and $v_i = 1$. Therefore, there exists a codeword $u \in C^*$, for which $d(z, u) = R$ and $u \in C$. Thus, C

is an $(n, d-1)R$ code. Similarly to Theorem 2, we prove that C is abnormal. □

There are three important consequences from Theorem 6.

Corollary 1: If Construction C is applied on the extended Hamming code of length 2^m, we obtain an abnormal $(2^m, 3)2$ code.

Corollary 2: If Construction C is applied on the punctured Preparata code of length $2^{2m}-1$, we obtain an abnormal $(2^{2m}-1, 4)3$ code.

Corollary 3: If Construction C is applied on the Preparata code of length 2^{2m}, we obtain an abnormal $(2^{2m}, 5)4$ code.

REFERENCES

[1] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, "Further results on the covering radius of codes," *IEEE Trans. Inform. Theory,* vol. IT-32, pp. 680–694, Sep. 1986.

[2] G. D. Cohen, M. G. Karpovsky, H. F. Mattson, and J. R. Schatz, "Covering radius—Survey and recent results," *IEEE Trans Inform. Theory,* vol. IT-31, pp. 328–343, May 1985.

[3] I. S. Honkala and H. O. Hämäläinen, "Bounds for abnormal binary codes with covering radius 1," *IEEE Trans. Inform. Theory,* vol. 37, pp. 372–375, Mar. 1991.

[4] X. Hou, "some results on the norm of codes," *IEEE Trans. Inform. Theory,* vol. 36, pp. 683–685, May 1990.

[5] ——, "Binary linear quasi-perfect codes are normal," *IEEE Trans. Inform. Theory,* vol. 37, pp. 378–379, Mar. 1991.

[6] K. E. Kilby and N. J. A. Sloane, "On the covering radius problem for code II. Codes of low dimension; normal and abnormal codes," *SIAM J. Algebraic Discrete Methods,* vol. 8, pp. 619–627, Oct. 1987.

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

[8] G. J. M. van Wee, "More binary covering codes are normal," *IEEE Trans Inform. Theory,* vol. 36, pp. 1466–1470, Nov. 1990.

[9] S. G. Vladuţ and A. N. Skorobogatov, "Covering radius for long BCH codes," *Probl. Peredach. Inform.*, vol. 25, pp. 38–45, Jan.–Mar. 1989.

Distributed Estimation and Quantization

John A. Gubner, *Member, IEEE*

***Abstract*— An algorithm is developed for the design of a nonlinear, n-sensor, distributed estimation system subject to communication and computation constraints. The algorithm uses only bivariate probability distributions and yields locally optimal estimators that satisfy the required system constraints. It is shown that the algorithm is a generalization of the classical Lloyd–Max results.**

***Index Terms*—Nonlinear estimation, distributed estimation, sensor fusion, Lloyd–Max algorithm.**

I. INTRODUCTION

Consider the distributed estimation system shown in Fig. 1. The system consists of n sensor platforms whose respective measurements, $Y_1, \cdots, Y_n$, are related to some unobservable quantity, say X. Each sensor platform processes its respective measurement and transmits the result over a communication channel to a common fusion center. The sensors do not communicate with each other, and there is no feedback from the fusion center to the sensor platforms. The task of the fusion center is to estimate the unobserved quantity X. We denote this estimate by $\hat{X}$. Clearly, $\hat{X}$ is a function of $Y_1, \cdots, Y_n$, and we can write $\hat{X} = f(Y_1, \cdots, Y_n)$ for some function f. The problem then is to choose the function f so that $\hat{X}$ is close to X in some sense. For example, it is well known that in the appropriate probabilistic setting, the minimum-mean-square-error estimate of X given $Y_1, \cdots, Y_n$ is the conditional expectation of X given $Y_1, \cdots, Y_n$, denoted $\mathsf{E}[X \mid Y_1, \cdots, Y_n]$. However, there are many situations in which the conditional expectation does not provide a satisfactory solution to the problem of choosing f.

1) In general, the functional form of $\mathsf{E}[X \mid Y_1, \cdots, Y_n]$ as a function of $Y_1, \cdots, Y_n$ is difficult to determine, and it requires knowledge of the joint probability distribution of $X, Y_1, \cdots, Y_n$. In practice this complete joint distribution may not be available.
2) To compute $\mathsf{E}[X \mid Y_1, \cdots, Y_n]$, the fusion center must in general have access to all of the sensor measurements $Y_1, \cdots, Y_n$. Hence, even if the sensor platforms have local processing capability, it is of little use in computing $\mathsf{E}[X \mid Y_1, \cdots, Y_n]$. If the number of sensor platforms is very large, the burden of computing $\mathsf{E}[X \mid Y_1, \cdots, Y_n]$ at the fusion center, even if the formula is relatively simple, may be prohibitive. Such considerations are important if the estimate of X must be computed in real time. By using a suboptimal estimator of X for which some of the processing can be done locally at the sensor platforms, it may be possible to design an acceptable estimator that can operate in real time.
3) As indicated in Fig. 1, the sensor platforms transmit their data to the fusion center. However, using any physical communication system, it is not possible to transmit real-valued quantities without distortion. In this situation, the conditional expectation, or even the best linear estimate, is generally a physically unrealizable solution.

In this correspondence, we develop an algorithm to design solutions to the distributed estimation problem that do not suffer from these difficulties.

II. BACKGROUND AND NOTATION

Our approach is to consider quantization for distributed estimation systems. The goal of quantization in such systems is to provide a good estimate of the unobservable, X, rather than to reconstruct the sensor measurements $Y_1, \cdots, Y_n$ as in [3]. Quantization for estimation has been studied for a single sensor by Ephraim and Gray [2] and by Ayanoglu [1]. The multisensor case has been studied by Lam and Reibman [5], and we discuss their work in more detail below. Zhang and Berger [9] considers an asymptotic estimation problem in which the observations are discrete random variables taking finitely many values and the unobservable quantity is not a random variable, but a deterministic and unknown parameter in some finite-dimensional Euclidean space.

A. System Model

Let $X, Y_1, \cdots, Y_n$ be real-valued random variables on some probability space $(\Omega, \mathcal{F}, \mathsf{P})$. Each sensor platform k processes its measurement Y_k to obtain an output Z_k. Each Z_k is then transmitted

Manuscript received August 10, 1992; revised December 15, 1992. This work was supported in part by the Air Force Office of Scientific Research under Grant AFOSR-90-0181. This work was presented in part at the 1990 IEEE International Symposium on Information Theory, San Diego, CA, January 14–19, 1990.

The author is with the Department of Electrical and Computer Engineering, University of Wisconsin, 1415 Johnson Drive, Madison, WI 53706–1691.

IEEE Log Number 9209594.