REFERENCES

[1] L. E. Dickson, "On the cyclotomic function," *Amer. Math. Monthly,* vol. 12, pp. 86–89, 1905.
[2] R. Gold, "Optimal Binary sequences for spread spectrum multiplexing," *IEEE Trans. Inform. Theory,* vol. IT-13, pp. 619–621, 1967.
[3] B. Gordon, "On the existence of perfect maps," *IEEE Trans. Inform. Theory,* vol. IT-12, pp. 486–487, 1966.
[4] R. Lidl and H. Niederreiter, *Finite Fields* (Encyclopedia of Mathematics and its Applications), vol. 20, 1983.
[5] D. Lin and M. Liu, "Linear Recurring m-Arrays," *Lecture Notes in Comput. Sci.,* no. 330, pp. 351–357, 1988.
[6] F. J. MacWilliams and N. J. A. Sloane, "Pseudo-random sequences and arrays," *Proc. IEEE,* vol. PROC-64, pp. 1715–1729, 1976.
[7] T. Nomura and A. Fukuda, "Linear recurring planes and two-dimensional cyclic codes," *Trans. Inst. Electron. Commun. Eng. Jap.,* vol. 54-A, pp. 147–154, Mar. 1971.
[8] T. Nomura, H. Miyakawa, H. Imai, and A. Fukuda, "A theory of two-dimensional linear recurring arrays," *IEEE Trans. Inform. Theory,* vol. IT-18, pp. 775–785, 1972.
[9] M. K. Siu, "m-Arrays and M-Arrays (in chinese)," *Math. in Practice and Theory,* vol. 1, pp. 77–86, 1989.
[10] Z.-X. Wan, *Algebra and Coding Theory* (in chinese). Beijing, Science Press, 1980, revised ed.
[11] N. Zierler, "Linear recurring sequences," *J. Soc. Indust. Appl. Math.,* vol. 7, pp. 31–48, 1959.

Constructions of Protocol Sequences for Multiple Access Collision Channel without Feedback

László Györfi and István Vajda

***Abstract*—Constructions of protocol sequences for multiple-access collision channel without feedback are given. These constructions are the extensions of those described by A, Györfi, and Massey. If the basic code in their constructions, a Reed–Solomon code, is replaced by a BCH code then the resulting protocol sequences have the feature that, for a given sum rate, the ratio of the total user population to the block length becomes much larger.**

***Index Terms*— BCH codes, collision channel, constant-weight codes, cyclically permutable codes, protocol sequences.**

I. CYCLICALLY PERMUTABLE CODES AND PROTOCOL SEQUENCES

A Györfi, and Massey [1] have given a general way to construct *constant-weight cyclically permutable codes.* A cyclically permutable code $CPC(N, T, d_c)$ is a binary block code with block length N, size T, and positive cyclic minimum distance d_c. The cyclic minimum distance d_c of a code is defined as the minimum Hamming distance from a codeword to its own cyclic shifts or to some cyclic shift of another codeword. The condition $d_c > 0$ implies that each codeword has N distinct cyclic shifts and that no codeword can be obtained by cyclic shifting another codeword one or more times. These constructions are the so-called cyclic concatenations of a subcode of a linear cyclic code over GF(p) (p is a prime) with the pulse-position-modulation (PPM) code consisting of all weight-one sequences of length p.

These codes can be the set of protocol sequences for the T possible users of the collision channel without feedback when it is known that at most M users are actively using the channel at any given time. According to a reiteration of the model from the paper [1] the traffic to send over a common communications channel is in the form of "packets" of some fixed length that we assume take values in the finite field GF(Q) for some, in general large, Q. The time axis is assumed to be partitioned into slots whose duration corresponds to the transmission time for one packet; it is further assumed that all users know the slot boundaries but are otherwise unsynchronized. When a user transmits a packet, he must transmit it exactly within a slot.

The channel is assumed to be the collision-channel without feedback [5], [6]. If, in a particular slot, none of the users are sending a packet (in which case we say each user "sends" the silence symbol), then the channel output in that slot is the silence symbol. If exactly one user is sending a packet in a particular slot, then the channel output in that slot is this packet value, which will be an element of GF(Q). If two or more users are sending packets in a particular slot, then the channel output in that slot is the collision symbol. There is no feedback available to inform the senders of the channel outputs in previous slots.

Each user, say user i, has a *protocol sequence*, which is a binary sequence $\boldsymbol{s}_i = [s_{i1}, s_{i2}, \cdots, s_{iN}]$ of length N that controls his sending of packets in the following manner. When user i becomes active (after some period of inactivity), he must send a packet in the jth slot of this activity ($1 \leq j \leq N$) if $s_{ij} = 1$ and must be silent in this slot if $s_{ij} = 0$. He continues to use his protocol sequence periodically in this manner until he has no more packets to send, in which case he again becomes inactive, and he must then remain inactive for at least $N - 1$ slots. If each $\boldsymbol{s}_i$ has Hamming weight w, then user i will send w packets in each frame of N slots where his protocol sequence appears. User i will code his packets (i.e., transmit redundant packets) in such a way that those of his packets that were "lost" in collisions can, under specified conditions, be recovered at the receiver. The task of the receiver in each received frame is three-fold, viz.:

1) to determine the set of active users (identification),
2) to find the beginnings of their frames (synchronization), and
3) for each active user, to determine the packets sent by this user in the w slots of this frame where the user sent packets (decoding).

The random-accessing problem, where in each received frame at most M out of the T users can be active in the sense of sending at least one packet in this frame, was introduced in [7] and [8]. The set $\{\boldsymbol{s}_1, \boldsymbol{s}_2, \cdots, \boldsymbol{s}_T\}$ of binary sequences is said to be a (T, M, N, σ) protocol sequence set if these sequences all have length N and, when used as protocol sequences, have the property that each active user can be identified by the receiver, the receiver can synchronize and each active user achieves at least σ successful packet transmissions in that frame, provided that at most M out of the T users are active. The users can code their packets so that each user can send σ information packets in each frame of his activity and the receiver can correctly decode these packets. Each user uses an $(n' = w, k' = \sigma, d' = n' - k' + 1 = w - \sigma + 1)$ shortened RS code over GF(Q) to code his σ information packets into his w transmitted packets. Such a code exists provided only that $n' = w \leq Q + 1$. If a user is active and has σ successful packet transmissions, the

Manuscript received March 16, 1992; revised February 6, 1993. This work was supported by Grant OTKA T 4360. This work was presented at the IEEE International Symposium on Information Theory, San Antonio, TX, Jan. 17–22, 1993.

The authors are with the Technical University of Budapest, Stoczek u. 2, H-1521 Budapest, Hungary.

IEEE Log Number 9210708.

decoding problem at the receiver is equivalent to having erasures in the at most $n' - \sigma = w - \sigma$ positions where this user's packets suffer collision. Because $d' = w - \sigma + 1$, the receiver can always correct these erasures by a standard erasure-correcting algorithm for the RS code, and hence, can correctly recover the σ information packets from this user.

A, Györfi, Massey [1] showed how *constant-weight cyclically-permutable codes* can be used as (T, M, N, σ) *protocol-sequence sets*: for any integer σ with $1 \leq \sigma \leq w$, a binary constant-weight-w cyclically-permutable code CPC(N, T, d_c) is a (T, M, N, σ) protocol-sequence set for

$$M = \min\left\{T, \left\lfloor \frac{w-1}{w - d_c/2} \right\rfloor, \left\lfloor \frac{w-\sigma}{w-d_c/2} \right\rfloor + 1\right\} \tag{1}$$

where $\lfloor \cdot \rfloor$ denotes rounding down to the nearest integer.

II. CPC Based on RS Codes Over GF(p)

In this section, we briefly describe the construction from [1]. Let $p \geq 5$ be a prime, let α be a primitive element of GF(p), and let V be the (n, k, d) Reed–Solomon (RS) code (where $n = p - 1$, $k (3 \leq k < p - 1)$ and $d = n - k - 1$ are the blocklength, dimension, and minimum (Hamming) distance, respectively) such that its parity check polynomial $h(x)$ can be written as

$$h(x) = \prod_{j=0}^{k-1} M_j(x), \tag{2}$$

where

$$M_j(x) = x - \alpha^{-j}.$$

Note that $M_j(x)$ is the minimal polynomial of α^{-j}, $j = 0, 1, \cdots, k-1$.

It is easy to see that V can be written as the direct sum ([4, theorem 2]):

$$V = V_0 + V_1 + V_2 + \cdots + V_{k-1},$$

where V_i is the RS code of length n over GF(p) with parity check polynomial $M_j(x)$, $j = 0, 1, \cdots, k-1$.

In the sequel we will use the following properties:

- P1 V is a linear cyclic code and each $\boldsymbol{c} \in V$ can be written uniquely in the form $\boldsymbol{c} = \boldsymbol{v}_0 + \boldsymbol{v}_1 + \cdots + \boldsymbol{v}_{k-1}$ where $\boldsymbol{v}_i \in V_i$ $i = 0, 1, \cdots, k-1$ ([4], Theorem 2).
- P2 $V_0 = \{u\mathbf{1};\ u \in \text{GF}(p)\}$, where $\mathbf{1}$ is the all-one n-tuple, since $M_0(x) = x - 1$.
- P3 V_1 has an element $\boldsymbol{c}^*$, the cyclic shifts of which are all distinct (for example $\boldsymbol{c}^* = (1, \alpha, \alpha^2, \cdots, \alpha^{n-1})$, since α is a primitive element).

Consider the following subcodes of V:

$$\tilde{V} = V_0 + \{\boldsymbol{c}^*\} + V_2 + \cdots + V_{k-1}$$

and

$$\hat{V} = \{\boldsymbol{c}^*\} + V_2 + \cdots + V_{k-1}.$$

Fact 1: Each codeword of $\tilde{V}$ has n distinct shifts and no codeword can be obtained by cyclic shifting another codeword one or more times.

The proof of Fact 1 is by contradiction. Suppose that $S^r\boldsymbol{u} = \boldsymbol{v}$ for two elements $\boldsymbol{u}$ and $\boldsymbol{v}$ of the code $\tilde{V}$ such that either $\boldsymbol{u} = \boldsymbol{v}$ and $0 < r < n$ or $\boldsymbol{u} \neq \boldsymbol{v}$. Obviously $\boldsymbol{u}$, $\boldsymbol{v}$, and $S^r\boldsymbol{u}$ can be decomposed into the forms: $\boldsymbol{u} = \boldsymbol{c}^* + \boldsymbol{x}$, $\boldsymbol{v} = \boldsymbol{c}^* + \boldsymbol{y}$ and $S^r\boldsymbol{u} = S^r\boldsymbol{c}^* + S^r\boldsymbol{x}$, where $\boldsymbol{x}$, $\boldsymbol{y}$, $S^r\boldsymbol{x} \in V_0 + V_2 + \cdots + V_{k-1}$. Thus,

$$\mathbf{0} = S^r\boldsymbol{u} - \boldsymbol{v} = (S^r\boldsymbol{c}^* - \boldsymbol{c}^*) + (S^r\boldsymbol{x} - \boldsymbol{y}),$$

where $(S^r\boldsymbol{c}^* - \boldsymbol{c}^*) \in V_1$ and $(S^r\boldsymbol{x} - \boldsymbol{y}) \in V_0 + V_2 + \cdots + V_{k-1}$. This contradicts P1).

Cyclic concatenation of $\hat{V}$ and the PPM code: Let each codeword $\boldsymbol{c} = [c_0, c_1, \cdots, c_{n-1}]$ in $\hat{V}$ determine a $p \times n$ array A in the manner that the ith column of A is the transpose of the p-tuple that is a weight-one vector having 1 at the c_ith position:

$$A = \begin{bmatrix} a(0,0) & \cdots & a(0, n-1) \\ \vdots & & \vdots \\ a(p-1, 0) & \cdots & a(p-1, n-1) \end{bmatrix}.$$

Here, p and n are assumed to be relatively prime, i.e., $\gcd(p, n) = 1$. Therefore, the Chinese remainder theorem [3, p. 285] specifies a one-to-one correspondence between the binary array A and the binary $N = pn$-tuple $\boldsymbol{b} = [b_0, b_1, \cdots, b_{N-1}]$ in the manner that

$$b_i = a(i \bmod p, i \bmod n),$$

where, here and hereafter, "$i \bmod p$" denotes the remainder when i is divided by p. Let B denote the set of binary N-tuples $\boldsymbol{b}$ corresponding to n-tuples $\boldsymbol{c}$ in $\hat{V}$.

Fact 2: There is a one-to-one correspondence between the sets

$$\{S^t\boldsymbol{b};\ \boldsymbol{b} \in B,\ t = 0, 1, \cdots, N-1\}$$

and

$$\{S^i\boldsymbol{c} + j\mathbf{1};\ \boldsymbol{c} \in \hat{V},\ i = 0, 1, \cdots, n-1,\ j \in \text{GF}(p)\} \subset V,$$

from which it follows that the cyclic minimum distance of B is at least twice the minimum distance of V. Thus, B is a constant-weight $w = n$ $CPC(N, T, d_c)$ code with $T = p^{k-2}$, $N = p(p-1)$ and $d_c \geq 2(n - k + 1)$.

Fact 2 can be proved in the same manner as Construction V in [1] such that $S^t\boldsymbol{b}$ corresponds to $S^i\boldsymbol{c} + j\mathbf{1}$ if $\boldsymbol{b}$ corresponds to $\boldsymbol{c}$ and t corresponds to (i, j) with $i = t \bmod n$, $j = t \bmod p$.

III. CPC Based on BCH Codes Over GF(p)

Obviously we can get a code B' with the same parameters if in Section II $M_j(x)$ is the minimal polynomial of α^j, $j = 0, 1, \cdots, k-1$. In this section, we give an extension. Again let α be a primitive element of GF(p^r), where p is a prime number and $r \geq 1$. A primitive Bose–Chaudhuri–Hocquenghem (BCH) code V of length $n = p^r - 1$ is then defined by the parity-check polynomial $h(x)$:

$$h(x) = \text{l.c.m.}\{M_0(x), \cdots, M_{k-1}(x)\},$$

where $M_j(x)$ is the minimal polynomial of α^j over GF(p), and $3 \leq k < p - 1$, $j = 0, 1, \cdots, k-1$. The minimum distance of code V can be bounded below by examining the set of roots of $h(x)$. If A_j denotes the set of logs of roots for $M_j(x)$ $(j = 0, 1, \cdots, k-1)$, then

$$\begin{aligned} A_0 &= \{0\} \\ A_1 &= \{1, p, p^2, \cdots, p^{r-1}\} \\ A_2 &= \{2, 2p, 2p^2, \cdots, 2p^{r-1}\} \\ &\vdots \\ A_{k-1} &= \{k-1, (k-1)p, (k-1)p^2, \cdots, (k-1)p^{r-1}\} \end{aligned} \tag{3}$$

([3], p. 105). We mention that $A_i \cap A_j = \varnothing$, for $i \neq j$, $i, j = 0, 1, \cdots, k-1$. It follows that

$$h(x) = \prod_{j=0}^{k-1} M_j(x)$$

and

$$\deg h(x) = (k-1)r + 1. \tag{4}$$

Note that for the particular case $r = 1$ we get the RS code defined in Section II. Introducing the generator polynomial $g(x)$ by

$$x^n - 1 = g(x)h(x),$$

we get from (3) that

$$\{(k-1)p^{r-1}+1,\ (k-1)p^{r-1}+2, \cdots, p^r - 2\} \subseteq \{\text{logs of roots of } g(x)\}. \tag{5}$$

Furthermore, from (4), it follows that

$$\deg g(x) = p^r - 1 - ((k-1)r + 1). \tag{6}$$

It is known that if $\alpha^{j_0}, \alpha^{j_0+1}, \cdots, \alpha^{j_0+2t-1}$ are different roots of $g(x)$ for some j_0, $j_0 \in \{0, 1, \cdots, p^r - 2\}$, then the minimum distance of the BCH code is at least $2t + 1$ ([3, p. 166]). Therefore, from (5), we get the following lower bound for the minimum distance of code V:

$$d \geq (p^r - 2 - (k-1)p^{r-1}) + 1 = p^r - 1 - (k-1)p^{r-1}. \tag{7}$$

The parameters of the code V are as follows:

$$\begin{aligned} &\text{length: } n = p^r - 1, \\ &\text{size: } |V| = p^{(k-1)r+1}, \\ &\text{distance: } d \geq p^r - 1 - (k-1)p^{r-1}. \end{aligned} \tag{8}$$

We show the properties P1), P2), and P3). It is easy to see ([4] Theorem 2) that V is given by the direct sum

$$V = V_0 + V_1 + \cdots + V_{k-1},$$

where V_j is the code over GF(p) of length n with parity check polynomial $M_j(x)$, $j = 0, 1, \cdots, k-1$. Because $M_0(x) = x - 1$,

$$V_0 = \{u\mathbf{1};\ u \in \text{GF}(p)\}, \tag{9}$$

i.e., $|V_0| = p$. Furthermore because $\deg M_j(x) = r$, it follows that $|V_j| = p^r$, $j = 1, 2, \cdots, k-1$. Because α is a primitive element of GF(p^r), $M_1(x)$ is a primitive polynomial and consequently V_1 contains an m-sequence $\boldsymbol{c}^*$ ([4, theorem 7]), which has the well-known property that all of its n cyclic shifts are different.

Consider the following subcodes of V:

$$\tilde{V} = V_0 + \{\boldsymbol{c}^*\} + V_2 + \cdots + V_{k-1} \tag{10}$$

and

$$\hat{V} = \{\boldsymbol{c}^*\} + V_2 + \cdots + V_{k-1}.$$

If B^* is the cyclic concatenation of $\hat{V}$ and the PPM code, then in the same way as in Section III the properties P1), P2), and P3) imply Fact 1 and Fact 2. Therefore, B^* is a binary constant-weight cyclically-permutable code with length $p(p^r - 1)$, size $p^{(k-2)r}$ and cyclic minimum distance $d_c \geq 2(p^r - 1 - (k-1)p^{r-1})$.

It is easy to see that B' is the special case of B^* when $r = 1$. The question is are there possible advantages of the choice $r > 1$ when B^* is used as protocol sequence set for collision channel without feedback?

IV. Protocol Sequences for the M-Out-of-T-User Collision Channel

In this section, we will show how the constant-weight cyclically-permutable code given in Section III, performs as a protocol sequence set for an M active out of the T users multiple access collision channel without feedback. Because a (T, M, N, σ) protocol-sequence set allows each of the M active users to send successfully σ information packets in a frame of N slots when the users code their packets as described above, it follows that R_{sum}, the total information transmission rate that can be achieved is

$$R_{\text{sum}} = \frac{M\sigma}{N} \text{ (packets/slots)}. \tag{11}$$

The code B^* can be used as a (T, M, N, σ) protocol sequence set with parameters:

$$\begin{aligned} T &= p^{(k-2)r} \\ N &= p(p^r - 1) \\ w &= p^r - 1. \end{aligned}$$

For $\sigma - 1 \geq (k-1)p^{r-1}$ the third term in (1) is the smallest one, thus

$$\begin{aligned} M &= \min\left\{T, \left\lfloor \frac{w-1}{w - d_c/2} \right\rfloor, \left\lfloor \frac{w-\sigma}{w - d_c/2} \right\rfloor + 1\right\} \\ &\geq \min\left\{T, \left\lfloor \frac{w-1}{(k-1)p^{r-1}} \right\rfloor, \left\lfloor \frac{w-\sigma}{(k-1)p^{r-1}} \right\rfloor + 1\right\} \\ &= \left\lfloor \frac{w-\sigma}{(k-1)p^{r-1}} \right\rfloor + 1. \end{aligned} \tag{12}$$

Therefore,

$$M \geq \frac{w-\sigma}{(k-1)p^{r-1}}.$$

Thus, for the sum rate (11),

$$R_{\text{sum}} \geq \frac{\sigma(w-\sigma)}{N(k-1)p^{r-1}},$$

the maximum of which is for $\sigma = w/2$ when for $w/2 - 1 \geq (k-1)p^{r-1}$. Choosing $\sigma = w/2$, we get

$$\begin{aligned} M &\geq \left\lfloor \frac{w/2}{(k-1)p^{r-1}} \right\rfloor + 1 = \left\lfloor \frac{(p^r-1)/2}{(k-1)p^{r-1}} \right\rfloor + 1 \\ &= \left\lfloor \frac{p}{2(k-1)} - \frac{1}{2(k-1)p^{r-1}} \right\rfloor + 1. \end{aligned} \tag{13}$$

The right side of (13) is usually independent of r and equals either to $\left\lfloor \frac{p}{2(k-1)} \right\rfloor + 1$ or $\left\lfloor \frac{p}{2(k-1)} \right\rfloor$. The sum rate is

$$R_{\text{sum}} = \frac{M\sigma}{N} = \frac{Mw/2}{pw} = \frac{M/2}{p}, \tag{14}$$

which is independent of r if M is independent of r. In any case, (13) and (14) imply that

$$R_{\text{sum}} \approx \frac{1}{4(k-1)},$$

for large p, so R_{sum} remains the same for RS ($r = 1$) and BCH ($r \geq 1$) codes.

The ratio of the total population T to the block length N is $(p^{(k-2)r})/(p(p^r - 1))$. For $k = 3$, this ratio is $\approx p^{-1}$. For $r = 1$, we get the results on the protocol sequence construction based on RS code [1]. For $r > 1$ T/N increases considerably, i.e., for fixed $k > 3$, it is a monotone increasing function of r and is $\approx p^{(k-3)r-1}$,

so the BCH code is better than the RS code. Note however that the increase in the number of potential users per slot does have a price: The increase in the code length $n' = w$ (and, therefore, in the frame length N and in the number $\sigma = w/2$ of successful packets per slot) increases the decoding complexity per slot, since the erasure-decoding algorithm of the other shortened RS code is super linear in w (it is quadratic in w for most standard erasure-decoding algorithms).

Example: Consider the numerical Example 5 in [1]. Take $p = 13$, $k = 4$. The following table illustrates the parameters of the protocol sequence sets for RS and BCH codes, resp.:

	RS ($r = 1$)	BCH ($r = 2$)
T	169	28561
M	3	3
N	156	2184
σ	6	84
R_{sum}	3/26	3/26
T/N	1.08	13.08

REFERENCES

[1] N. Q. A., L. Györfi, J. L. Massey, "Constructions of binary constant-weight cyclic codes and cyclically permutable codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 940–948, May 1992.

[2] E. N. Gilbert, "Cyclically permutable error-correcting codes," *IEEE Trans. Inform. Theory*, vol. 9, pp. 175–182, July 1963.

[3] R. E. Blahut, *Theory and Practice of Error Control Codes.* Reading, MA: Addison-Wesley, 1984.

[4] N. Zierler, "Linear recurring sequences," *J. SIAM*, vol. 7, no. 1, pp. 31–48, Mar. 1959.

[5] J. L. Massey, "The capacity of the collision channel without feedback," in *Abstracts of Papers, IEEE Int. Symp. Inform. Theory*, 1982, p. 101.

[6] J. L. Massey and P. Mathys, "The collision channel without feedback," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 192–204, Mar. 1985.

[7] B. S. Tsybakov and N. B. Likhanov, "Packet communication on a channel without feedback," *Probl. Inform. Transm.*, (in Russian), vol. XIX, no. 2, pp. 64–84, 1983.

[8] L. A. Bassalygo and M. S. Pinsker "Limited multiple-access of a nonsynchronous channel," *Probl. Inform. Transm.* (in Russian), vol. XIX, no. 4, pp. 92–96, 1983.

A Note on Distributed Estimation and Sufficiency

R. Viswanathan

***Abstract*—In relation to distributed parameter estimation, the notion of local and global sufficient statistics is introduced. It is shown that when a sufficiency condition is satisfied by the probability distribution of a random sample, a global sufficient statistic is obtainable as a function of local sufficient statistics. Several standard distributions satisfy the said sufficiency condition.**

***Index Terms*—Estimation, sufficiency, fusion of estimates.**

Manuscript received April 15, 1992; revised December 10, 1992. This work was supported by ONR under Grant N00014–93–1–1092.

The author is with the Department of Electrical Engineering, Southern Illinois University at Carbondale, Carbondale, IL 62901-6603.

IEEE Log Number 9210707.

I. INTRODUCTION

In distributed estimation, inferences about a parameter are to be made based on partial information. A typical situation is the following. Several partial (local) data sets are available and separate inferences based on local data sets, such as local estimates or sufficient statistics pertaining to local data, are used to obtain an overall assessment of the parameter. If all the local data are available together, then the problem is one of classical estimation [1]. In distributed detection and estimation, some interesting and counter intuitive results are possible [2], [6]. Here, only those probability distributions that admit sufficient statistics are considered [1]. The utility of the sufficient statistic is that it is of reduced dimension as compared to the dimension of the data and that it achieves this reduction without any loss of information, because it carries all the relevant information that the data has, regarding the parameter. (The whole data is trivially sufficient, but this has no dimensionality reduction. Hence, it is assumed that those distributions that admit only the trivial sufficient statistic do not possess any sufficient statistic). In this discussion it is assumed that conditioned on the parameter, the data samples are statistically independent. In the next section we have some preliminaries that define the terminologies. In Section III, we pose the question: Given several local sufficient statistics and a global sufficient statistic pertaining to the whole data, does a function of local sufficient statistics exist such that this function is the global sufficient statistic? A sufficient condition on the probability distribution assures the existence of such a function. Also, several standard distributions are shown to satisfy this condition.

II. PRELIMINARIES

Consider the problem of estimating a parameter Θ using the observations $Z_1, Z_2, \cdots, Z_N$. In the context of distributed processing, the whole data can be called global data and any proper subset of the global set local data. Whenever several local data sets are considered, we assume them to be mutually exclusive and collectively exhaustive. Hence, the conditional distribution of the global data given the parameter Θ and the prior distribution of Θ provide a complete characterization of the estimation problem. Any sufficient statistic [1] that pertains to the whole data will be called a global sufficient statistic. A sufficient statistic that pertains to local data will be called a local sufficient statistic. One could similarly define local and global likelihood functions, local estimates, and global estimates. The definition of local and global sufficiency given here is different from the one used by Barankin and Katz [7]. In [7], the variation of the dimensionality of a sufficient statistic as the sample $(z_1, z_2, \cdots, z_N)$ ranges over Euclidean N-space, leads to the definition of local and global sufficient statistics.

III. LOCAL AND GLOBAL SUFFICIENCY

Using the terminology of distributed sensor processing [2], [3], let us consider a group of n sensors, with the ith sensor receiving observations $\{Z_{i1}, Z_{i2}, \cdots, Z_{in_i}\}$, for $i = 1, 2, \cdots, n$. Let G denote the global data set $\{Z_{ij}, i = 1, 2, \cdots, n, j = 1, 2, \cdots, n_i\}$ and let each Z_{ij} be independent and identically distributed with either a probability mass function $f(z \mid \Theta)$, when the observations are discrete, or with a probability density function $f(z \mid \Theta)$, when the observations are continuous. Here Θ denotes a one-dimensional parameter defined on an appropriate parametric space. For the sake of notational convenience, $f(\cdot)$ is used to denote both the marginal