the cross-correlation function, which equals 1. It follows $S = (p^J - 1)p^{M-2J}$ for $k \neq 0 \bmod T$.

We proceed with the proof of Lemma 10 since the result is easily read from Theorme 19:

$$\#\{i|\operatorname{tr}_J^M(\alpha^i) = 0 \wedge \operatorname{tr}_J^M(\alpha^{i+k_1}) = 0\} = P((0,0),k) = \begin{cases} p^{M-J} - 1, & \text{if } k \equiv 0 \bmod T \\ p^{M-2J} - 1, & \text{if } k \not\equiv 0 \bmod T \end{cases}.$$

Since the sum of the cardinalities of all three sets equals $p^M - 1$, the cardinality of the outstanding set is readily calculated as

$$\begin{aligned}\#\{i|\operatorname{tr}_J^M(\alpha^i) = 0 \dot{\vee} \operatorname{tr}_J^M(\alpha^{i+k_1}) = 0\} &= p^M - 1 - N_1(k_1) - \#\{i|\operatorname{tr}_J^M(\alpha^i) = 0 \wedge \operatorname{tr}_J^M(\alpha^{i+k_1}) = 0\} \\ &= \begin{cases} 0, & \text{if } k \equiv 0 \bmod T \\ 2p^{M-2J}(p^J - 1), & \text{if } k \not\equiv 0 \bmod T \end{cases}\end{aligned}$$

and the proof for Lemma 9 is completed.

Remark: The determination of $\#\{i|\operatorname{tr}_J^M(\alpha^i) = 0 \wedge \operatorname{tr}_J^M(\alpha^{i+k_1}) = 0\}$ may also be performed with cyclic difference sets: a set of elements, annihilated by a linear function from GF(p^M) onto GF(p^J)—which may be given as the trace function—constitutes a (v, k', λ) cyclic difference set CDS, whereby the parameters are given by [21]

$$v = T, k' = \frac{p^{M-J} - 1}{p^J - 1}, \lambda = \frac{p^{M-2J} - 1}{p^J - 1}.$$

The cardinality of the set equals k', and the number of solutions to the equation $u - v \equiv t \bmod v, u, v \in \text{CDS}$ equals λ. We obtain

$$\#\{i|\operatorname{tr}_J^M(\alpha^i) = 0 \wedge \operatorname{tr}_J^M(\alpha^{i+k_1}) = 0\} = \begin{cases} k'(p^J - 1), & \text{if } k \equiv 0 \bmod T \\ \lambda(p^J - 1), & \text{if } k \not\equiv 0 \bmod T. \end{cases}$$

(We have to multiply λ and k' by $p^J - 1$ since i runs over $P^M - 1 = (p^J - 1)t$ values.)

References

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

[2] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, pp. 593–619, 1980.

[3] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 858–864, 1982.

[4] J.-S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Trans. Inform. Theory*, vol. 35, pp. 371–379, 1989.

[5] P. V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," *IEEE Trans. Inform. Theory*, vol. 37, pp. 603–616, 1991.

[6] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 397–399, 1974.

[7] M. Antweiler and L. Bömer, "Correlation of complex sequences derived from BCH codes and their duals," in *IEEE Symp. Inform. Theory*, Budapest, Hungary, 1991, p. 278.

[8] S.-C. Liu and J. Komo, "Nonbinary Kasami sequences over GF(p)," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1409–1412, 1992.

[9] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 619–621, 1967.

[10] ——, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 154–156, 1968.

[11] T. Kasami, S. Lin, and W. W. Peterson, "Some reuslts on cyclic codes which are invariant under the affine group and their applications," *Inform. Contr.*, vol. 11, pp. 475–496, 1968.

[12] T. Kasami, "Weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes," *Inform. Contr*, vol. 18, pp. 369–394, 1971.

[13] F. J. MacWilliams and N. J. A. Sloane, "Pseudo-random sequences and arrays," *Proc. IEEE*, vol. 64, pp. 1715–1729, 1976.

[14] H. M. Trachtenberg, "On the cross-correlation function of maximal linear recurring sequences," Ph.D. dissertation, Dep. Elec. Eng., Univ. Southern California, Los Angeles, Jan. 1970.

[15] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Math.*, vol. 16, pp. 209–232, 1976.

[16] R. A. Games, "Crosscorrelation of m-sequences and GMW-sequences with same primitive polynomial," *Discrete Appl. Math.*, vol. 12, pp. 139–146, 1985.

[17] A. H. Chan, M. Goresky, and A. Klapper, "Correlation functions of geometric sequences," in *Advances in Cryptology—Eurocrypt'90*, Springer-Verlag, 1990, pp. 214–221.

[18] M. Antweiler and L. Bömer, "Complex sequences over GF(p^M) with a two-level autocorrelation function and large linear span," *IEEE Trans. Inform. Theory*, vol. 38, pp. 120–130, 1992.

[19] R. Lidl and H. Niederreiter, *Finite Fields*. Reading, MA: Addison-Wesley, 1983.

[20] S. W. Golomb, "Correlation properties of periodic and aperiodic sequences, and applications to multi-user systems," in *New Concepts in Communication*, J. K. Skwirzynski, Ed. Sijthoff & Noordhoff, 1981, pp. 161–1197.

[21] L. D. Baumert, *Cyclic Difference Sets*. Berlin: Springer-Verlag, 1971.

[22] Y. Niho, "Multi-valued cross-correlation function between two maximal linear recursive sequences," Ph.D. dissertation, Univ. Southern California, Los Angeles, 1972.

[23] M. Antweiler, "Correlation of GMW sequences," in *IEEE Symp. Inform. Theory*, San Antonio, TX, 1993, p. 411.

[24] ——, *Rekursive Sequenzen mit gutem Korrelationsverhalten und hoher linearer Rekursionstiefe. Reihe 10: Informatik/Kommunikationstechnik Nr. 173*, VDI-Verlag GmbH Düsseldorf, 1992.

Optimum Sequence Multisets for Synchronous Code-Division Multiple-Access Channels

Marcel Rupf, *Member, IEEE*,
and James L. Massey, *Fellow, IEEE*

***Abstract*—It is shown that the sum capacity of the symbol-synchronous code-division multiple-access channel with equal average-input-energy constraints is maximized precisely by those spreading sequence multisets that meet Welch's lower bound on total squared correlation. It**

Manuscript received August 16, 1993; revised November 16, 1993. This work was supported in part by COST 231, by the Swiss PTT, and by the European Space Research and Technology Center under ESTEC Contract 8696/89/NL/US. This work was presented in part at the IEEE International Symposium on Information Theory, San Antonio, TX, January 17–22, 1993.

M. Rupf was with the Signal and Information Processing Laboratory, ETH Zürich, CH-8092 Zürich, Switzerland. He is now with the IBM Research Laboratory, CH-8803 Rüschlikon, Switzerland.

J. L. Massey is with the Signal and Information Processing Laboratory, ETH Zürich, CH-8092 Zürich, Switzerland.

IEEE Log Number 9403849.

is further shown that the symmetric capacity of the channel determined by these same sequence multisets is equal to the sum capacity.

Index Terms—**CDMA, capacity region, sum capacity, symmetric capacity, Welch's bound.**

I. Introduction

Code-division multiple-access (CDMA) is a multiplexing technique in which several independent users access a common communications channel by modulating their channel-input symbols with preassigned spreading sequences. In this correspondence, we consider synchronous CDMA (S-CDMA) systems, where in each symbol interval, the receiver observed the sum of the transmitted signals from one symbol interval embedded in additive white Gaussian noise (AWGN). Although such complete synchronization of the users rarely holds in practice, its study gives insight into the limits of CDMA systems.

In this correspondence, we consider the spreading sequences to be part of the specification of the S-CDMA channel. These spreading sequences should be chosen to create the best (in an appropriate sense) channel for the users. In conventional CDMA systems, the decoder for a given user treats the sum of the interfering signals from the other users as noise. The spreading sequences are chosen to create good single-user channels for the individual coding systems. In fact, however, the channel created by the spreading sequences is a multiple-access channel (or MAC for short). To transmit data reliably from all users at the maximum sum rate possible for a MAC requires the use of a "joint decoder" that knows all channel codes. Since the joint decoder can separate the users, the spreading sequences themselves need not all be different, i.e., they may form a multiset rather than a set. In the following, we show that, when all users have the same average-channel-input energy constraint, then the sequence multisets that achieve Welch's lower bound on total squared correlation are precisely the sequence sets that maximize the "capacity" of the S-CDMA channel.

II. S-CDMA Channel Model

We consider the discrete-time, baseband S-CDMA channel model depicted in Fig. 1, where the K users encode their information sequences into the complex-valued, channel-input sequences $X_k[\cdot]$, $k = 1,\cdots, K$. As in any multiple-access problem, the sequences $X_k[\cdot]$ are assumed to be independent random processes. We assume further that there is an average-input-energy constraint

$$E\left[|X_k[n]|^2\right] \le w_k \tag{1}$$

for all time instants n on the k-th user, $k = 1,\cdots, K$. Without loss of essential generality, we may assume that $E[X_k[n]] = 0$, all n. For convenience, we define the diagonal energy-constraint matrix $W = \mathrm{diag}(w_1,\cdots, w_K)$. The maximum total average-input-energy

$$w_{\mathrm{tot}} = \sum_{k=1}^{K} w_k \tag{2}$$

is just the trace of W.

In the n-th symbol period, the k-th user transmits the signal $X_k[n]\,\underline{s}_k$, where $\underline{s}_k$ is his complex L-chip spreading sequence. The sequence multiset $\mathcal{S} = \{\underline{s}_1,\cdots, \underline{s}_K\}$ will conveniently be represented by the $L \times K$ sequence matrix S whose k-th column is $\underline{s}_k$. Each spreading sequence $\underline{s}_k$, or equivalently each column of S, is assumed to have energy L, i.e.,

$$\underline{s}_k^H \underline{s}_k = L, \tag{3}$$

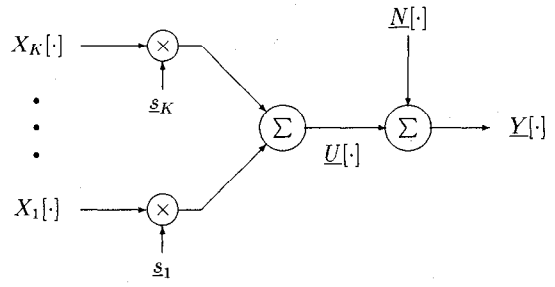

Fig. 1. Discrete-time, baseband S-CDMA channel model.

where the superscript "H" denotes transposition and complex conjugation. It follows from (1) and (3) that the average energy of the spread symbol $X_k[n]\,\underline{s}_k$, all n, is at most Lw_k.

Omitting the symbol-time index, we can write the sum of the transmitted symbols at a given time as the L-chip vector

$$\underline{U} = S\underline{X}, \tag{4}$$

where the MAC input vector $\underline{X} = [X_1,\cdots, X_K]^T$ and where the superscript "T" denotes transposition. The receiver observes this L-chip sum signal embedded in AWGN, i.e., the output of the MAC is the L-chip vector

$$\underline{Y} = \underline{U} + \underline{N}, \tag{5}$$

where $\underline{N} = [N_1,\cdots, N_L]^T$ is a zero-mean, *proper*[1]. complex Gaussian vector with covariance matrix $E[\underline{N}\underline{N}^H] = N_0 I_L$ and where I_L denotes the $L \times L$ identity matrix. Together, (4) and (5) specify the MAC corresponding to the S-CDMA channel as

$$\underline{Y} = S\underline{X} + \underline{N}. \tag{6}$$

III. Sum Capacity and Symmetric Capacity

The S-CDMA channel determined by a given sequence matrix S is a special case of the K user Gaussian MAC (GMAC) with average-input-energy constraints [2, pp. 403–404], whose capacity region is the closure of the convex hull of the union over $p_{\underline{X}}(\underline{x})$ in $\pi_{\underline{X}}$ of the rate regions

$$\mathcal{R}(S, p_{\underline{X}}(\underline{x})) = \bigcap_{\substack{J\subseteq\{1,\cdots,K\}\\ J\neq\{\,\}}} \left\{(R_1,\cdots, R_K)\,|\,0 \le \sum_{k\in J} R_k \le I(\underline{X}_J; \underline{Y}|\underline{X}_{J^c})\right\}, \tag{7}$$

where, here and hereafter, $\pi_{\underline{X}}$ denotes the set of product probability densities $p_{\underline{X}}(\underline{x}) = p_{X_1}(x_1)\cdot p_{X_2}(x_2)\cdots p_{X_K}(x_K)$ on the channel-input symbols that satisfy the average-input-energy constraint (1). Here, J^c denotes the complement of the non-empty subset J of $\{1, 2,\cdots, K\}$, $I(\cdot;\cdot|\cdot)$ denotes conditional mutual information, and the vectors $\underline{X}_J$ and $\underline{X}_{J^c}$ are obtained by striking out the components of $\underline{X}$ whose indices do not lie in J and J^c, respectively. Equation (6) can be rewritten as $\underline{Y} = S_J\underline{X}_J$

[1] In [1], a complex random vector $\underline{Z}$ is called *proper* if its pseudocovariance matrix vanishes, i.e., if $E[(\underline{Z} - E[\underline{Z}])(\underline{Z} - E[\underline{Z}])^T] = O$. The properness of the zero-mean, complex noise vector $\underline{N}$ with $E[\underline{N}\underline{N}^H] = N_0 I_L$ means simply that the real and the imaginary part of its components N_l, $l = 1,\cdots, L$, are uncorrelated and have the same average energy $N_0/2$.

$+ S_{J^c}\underline{X}_{J^c} + \underline{N}$, where the $L \times |J|$ matrix S_J and the $L \times (K - |J|)$ matrix S_{J^c} are obtained by striking out the columns of S whose indices do not belong to the subsets J and J^c, respectively, and where $|J|$ is the cardinality of J. The conditional mutual information in (7) is thus given in terms of differential entropies $h(\cdot)$ as

$$I(\underline{X}_J; \underline{Y}|\underline{X}_{J^c}) = h(\underline{Y}|\underline{X}_{J^c}) - h(\underline{Y}|\underline{X}) = h(S_J\underline{X}_J + \underline{N}) - h(\underline{N}). \quad (8)$$

Proceeding essentially as in [3] by applying the maximum-entropy lemma for complex random vectors [1] to $h(S_J\underline{X}_J + \underline{N})$ in (8) and dividing by L to obtain rates in bits per chip, we get

$$I(\underline{X}_J; \underline{Y}|\underline{X}_{J^c}) \le \frac{1}{L}\log\left[\det\left(I_L + \frac{1}{N_0}S_J W_J S_J^H\right)\right] \quad (9)$$

with equality if and only if $S_J\underline{X}_J$ is a zero-mean, proper complex Gaussian vector with covariance matrix $S_J W_J S_J^H$. Here, the $|J| \times |J|$ matrix W_J is obtained by striking out both the columns and rows of W whose indices do not belong to J. A sufficient condition [1] for equality in (9) is that $\underline{X}_J$ be a zero-mean, proper complex Gaussian vector with covariance matrix $E[\underline{X}_J\underline{X}_J^H] = W_J$. The corresponding $p_{\underline{X}}(\underline{x})$ is in $\pi_{\underline{X}}$ and maximizes $I(\underline{X}_J; \underline{Y}|\underline{X}_{J^c})$ for all choices of J. Thus, the capacity region $\mathscr{C}(S)$ [in bits/chip] of the S-CDMA channel is given simply by

$$\mathscr{C}(S) = \bigcap_{\substack{J\subseteq\{1,\cdots,K\}\\ J\neq\{\ \}}} \left\{(R_1,\cdots,R_K)\,|\,0 \le \sum_{k\in J} R_k \le \frac{1}{L}\log\left[\det\left(I_L + \frac{1}{N_0}S_J W_J S_J^H\right)\right]\right\} \quad (10)$$

and is usually an irregularly beveled box that strongly depends on the particular choice of the sequence matrix S (cf. Example 1 below).

One reasonable criterion of goodness for the sequence multiset $\mathscr{S}$ is the resultant *sum capacity* $C_{\text{sum}}(S)$, which is defined by

$$C_{\text{sum}}(S) = \max_{(R_1,\cdots,R_K)\in\mathscr{C}(S)} \sum_{k=1}^{K} R_k \quad (11)$$

and can be computed as [4]

$$C_{\text{sum}}(S) = \max_{p_{\underline{X}}(\underline{x})\in\pi_{\underline{X}}} I(\underline{X};\underline{Y}). \quad (12)$$

Therefore, it follows from (9) and the choice $J = \{1,\cdots,K\}$ that

$$C_{\text{sum}}(S) = \frac{1}{L}\log\left[\det\left(I_L + \frac{1}{N_0}SWS^H\right)\right]. \quad (13)$$

In practice, however, the criterion of goodness of greatest interest for the sequence multiset $\mathscr{S}$ is usually the *symmetric capacity* $C_{\text{sym}}(S)$, which we define as the sum rate of the maximum achievable equal-rate point in the capacity region $\mathscr{C}(S)$, i.e.,

$$C_{\text{sym}}(S) = \max_{(R,\cdots,R)\in\mathscr{C}(S)} K'R'. \quad (14)$$

Because the K tuple $(R,\cdots,R)$ has to fulfill all the inequalities in (10), it follows that the symmetric capacity $C_{\text{sym}}(S)$ can be computed as

$$C_{\text{sym}}(S) = \min_{\substack{J\subseteq\{1,\cdots,K\}\\ J\neq\{\ \}}} \frac{K}{|J|}C_{\text{sum}}(S_J), \quad (15)$$

where $C_{\text{sum}}(S_J)$ is given by

$$C_{\text{sum}}(S_J) = \frac{1}{L}\log\left[\det\left(I_L + \frac{1}{N_0}S_J W_J S_J^H\right)\right]. \quad (16)$$

It follows immediately that $C_{\text{sym}}(S) \le C_{\text{sum}}(S)$ with equality if and only if $J = \{1,\cdots,K\}$ is among the minimizing subsets in (15).

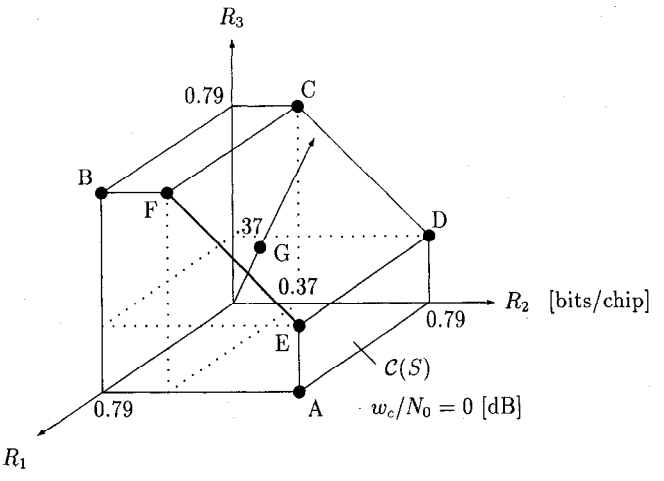

Fig. 2. Capacity region $\mathscr{C}(S)$ of the S-CDMA channel given in Example 1.

Example 1: Consider the S-CDMA system in which $K = 3$ users employ the bipolar sequence multiset $\mathscr{S}$ of length $L = 2$ sequences corresponding to the sequence matrix

$$S = \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & -1 \end{bmatrix}.$$

Note that users 2 and 3 have the same spreading sequence. Fig. 2 shows the resultant capacity region $\mathscr{C}(S)$ of this S-CDMA channel when $W = w_c I_K$, so that all users have equal average-input-energy, and when the signal-to-noise ratio (SNR) w_c/N_0 is 0 dB.

Because user 1 and user 2 have mutually orthogonal spreading sequences, both can reliably communicate at the single-user capacity 0.79 bits per chip when user 3 is silent; see point A in Fig. 2. The same conclusion holds for users 1 and 3 when user 2 is silent; see point B. However, this is not the case for user 2 and user 3 when user 1 is silent, because the sequences of users 2 and 3 are not uncorrelated (and in fact coincide), see line $C - D$. The rate tuples $(R_1, R_2, R_3) \in \mathscr{C}(S)$ with the maximum sum rate $C_{\text{sum}}(S) = 1.95$ bits per chip lie on the line $E - F$. The maximum achievable equal-rate point is G and the corresponding sum capacity is $C_{\text{sym}}(S) = 1.74$ bits per chip. Note that $C_{\text{sym}}(S)$ is strictly less than $C_{\text{sum}}(S)$ in this example.

IV. Upper Bound on Sum Capacity

A trivial upper bound on the sum capacity $C_{\text{sum}}(S)$ of the S-CDMA channel is the sum capacity of the "unrestricted" S-CDMA channel, where all spreading sequences have length $L = 1$. This latter channel, however, is the K user GMAC and its sum capacity $C_{\text{GMAC}}(K)$ in the case of the average-energy-constraint (1) is given by $C_{\text{GMAC}}(K) = \log(1 + w_{\text{tot}}/N_0)$ bits per chip [2, p. 378]. We now show that $C_{\text{sum}}(S)$ can indeed achieve $C_{\text{GMAC}}(K)$ even when $L > 1$ and we determine the necessary and sufficient conditions for equality.

Proposition 1: Let $\mathscr{S} = \{\underline{s}_1, \cdots, \underline{s}_K\}$ be a sequence multiset consisting of K complex sequences of energy L, let S be the corresponding sequence matrix and let W be the diagonal energy-constraint matrix. Then,

$$C_{\text{sum}}(S) \le \log\left(1 + \frac{w_{\text{tot}}}{N_0}\right) \quad \text{[bits/chip]},$$

where w_{tot} is given by (2), with equality if and only if $SWS^H = w_{\text{tot}} I_L$, i.e., if and only if the modified sequence matrix $SW^{1/2} = [\sqrt{w_1}\,\underline{s}_1, \cdots, \sqrt{w_K}\,\underline{s}_K]$ has mutually orthogonal and equal-energy rows.

Proof: The proposition can be proved by applying first Hadamard's inequality [2, p. 502] on the determinant in (13) and then using Jensen's inequality [2, p. 25]. The following alternative proof, however, gives more insight into the condition for equality.

From Fig. 1 and the data processing inequality [2, p. 32], it follows that $I(\underline{X};\underline{Y}) \le I(\underline{U};\underline{Y})$. Conversely, since $\underline{U} = S\underline{X}$ is uniquely determined by $\underline{X}$, we also have $I(\underline{U};\underline{Y}) \le I(\underline{X};\underline{Y})$ [2, p. 33] so that $I(\underline{X};\underline{Y}) = I(\underline{U};\underline{Y})$. It now follows from (12) that

$$C_{\text{sum}}(S) = \max_{p_{\underline{U}}(\underline{u}) \in T_{\underline{U}}} \frac{1}{L} I(\underline{U};\underline{Y}) \tag{17}$$

where $T_{\underline{U}}$ denotes the set of all probability densities for $\underline{U}$ that correspond to product probability densities for $\underline{X}$ satisfying (1). However, $\underline{Y} = \underline{U} + \underline{N}$ can be viewed as the output of L parallel, proper complex AWGN channels. The constraint (1) implies the total average-input-energy constraint $E[\underline{U}^H\underline{U}] \le Lw_{\text{tot}}$ on these parallel channels. The corresponding capacity C_P is given by [2, p. 250]

$$C_P = \log\left(1 + \frac{w_{\text{tot}}}{N_0}\right) \quad \text{[bits/chip]} \tag{18}$$

so that $I(\underline{U};\underline{Y})/L \le C_P$ and equality is achieved if and only if the inputs U_l, $l = 1, \cdots, L$, are uncorrelated, zero-mean, proper complex Gaussian random variables with the same average energy w_{tot}, i.e., if and only if these zero-mean, proper complex Gaussian random variables satisfy $E[\underline{U}\underline{U}^H] = w_{\text{tot}} I_L$. It now follows that

$$C_{\text{sum}}(S) \le C_p \tag{19}$$

with equality if and only if, for some maximizing $p_{\underline{X}}(\underline{x})$ in (12), $\underline{U} = S\underline{X}$ is a zero-mean, proper complex Gaussian vector with $E[\underline{U}\underline{U}^H] = w_{\text{tot}} I_L$. But our derivation of the capacity region $\mathscr{C}(S)$ in (10) showed that for every such maximizing $p_{\underline{X}}(\underline{x})$, $E[\underline{U}\underline{U}^H] = SWS^H$. We conclude that equality holds in (19) just when $SWS^H = w_{\text{tot}} I_L$. □

If the K users of an S-CDMA system do not have equal average-input-energy constraints, i.e., if $W \ne w_c I_K$, it is generally difficult to determine the sequence multisets $\mathscr{S}$ that maximize $C_{\text{sum}}(S)$ in Proposition 1. For example, if $L = K$, the optimum sequence multisets with respect to sum capacity do *not* consist of mutually orthogonal sequences when $W \ne w_c I_K$. If all users have equal average-input-energy constraints, however, the design of optimum sequence multisets becomes much simpler.

Corollary 1: Let $\mathscr{S}$, S, and W be as in Proposition 1. If $W = w_c I_K$, then

$$C_{\text{sum}}(S) \le \log\left(1 + K\frac{w_c}{N_0}\right) \quad \text{[bits/chip]}$$

with equality if and only if $SS^H = KI_L$, i.e., if and only if the sequence matrix $S = [\underline{s}_1, \cdots, \underline{s}_K]$ has mutually orthogonal and equal-energy rows.

We will call the sequence multisets $\mathscr{S}$ satisfying the conditions for equality in Corollary 1 Welch-bound-equality (WBE) sequence multisets, since these are sequence multisets that were proved in [5] to yield equality in Welch's bound [6]

$$\sum_{i=1}^{K}\sum_{j=1}^{K} |\underline{s}_i^H \underline{s}_j|^2 \ge K^2 L \tag{20}$$

on total squared correlation.[2] It is important to note that the orthogonality of the *rows* of S as required for a WBE sequence multiset does generally not imply the orthogonality of the sequences in S because these sequences appear as the *columns* of S. When $W = w_c I_K$, the orthogonality of the *rows* of S is equivalent to the uncorrelatedness of the components of $\underline{U}$, which is the crucial requirement for maximizing capacity.

Note that a necessary condition for a sequence multiset $\mathscr{S}$ to be WBE is that $K \ge L$. In [5], many constructions of bipolar WBE sequence multisets were given. There are also large classes of non-bipolar WBE sequence multisets. For example, the sequence set obtained by choosing one of each antipodal pair of the sequences in a permutation modulation code with sign changes [8] is a WBE sequence set.

V. Upper Bound on Symmetric Capacity

If the K users do not have equal average-input-energy constraints, i.e., if $W \ne w_c I_K$, then $C_{\text{sum}}(S)$ is often smaller than $C_{\text{sym}}(S)$ and thus smaller than the upper bound on $C_{\text{sum}}(S)$ given in Proposition 1. If the users have equal average-input-energy constraints, however, we have the somewhat surprising result that the symmetric capacity for WBE sequence multisets achieves the upper bound on sum capacity.

Proposition 2: Let $\mathscr{S}$, S, and W have the same meaning as in Proposition 1. If $W = w_c I_K$, then

$$C_{\text{sym}}(S) \le \log\left(1 + K\frac{w_c}{N_0}\right) \quad \text{[bits/chip]}$$

with equality if and only if the sequence multiset $\mathscr{S}$ is a WBE sequence multiset, i.e., if and only if the sequence matrix $S = [\underline{s}_1, \cdots, \underline{s}_K]$ has mutually orthogonal and equal-energy rows.

Proof: Since $C_{\text{sym}}(S) \le C_{\text{sum}}(S)$ and because of Corollary 1, we have only to prove that $C_{\text{sym}}(S) = C_{\text{sum}}(S)$ for all WBE sequence multisets. Equivalently, from (15), we must show that the value $R = \log(1 + Kw_c/N_0)/K$ of the maximum achievable equal-rate point $(R, \cdots, R)$ satisfies

$$|J|R \le C_{\text{sum}}(S_J) \tag{21}$$

for every non-empty subset $J \subseteq \{1, \cdots, K\}$ when $SS^H = KI_L$. The following lemma will be useful. □

Lemma 1: Let λ_l, $l = 1, \cdots, L$, be the L eigenvalues of the complex $L \times L$ matrix $S_J S_J^H$ and let $C_{\text{sum}}(S_J)$ be defined by (16). If $W = w_c I_K$, then

$$C_{\text{sum}}(S_J) = \frac{1}{L}\sum_{l=1}^{L} \log\left(1 + \frac{w_c}{N_0}\lambda_l\right).$$

[2] The bound (20) on total squared correlation was proved earlier by Sidelnikov [7] for more restricted sequence multisets. For even powers of the correlations greater than 2, Sidelnikov's bound is often stronger than Welch's.

Proof: The following two simple facts about a complex $L \times L$ matrix M and its corresponding L eigenvalues λ_l, $l = 1,\cdots, L$, will be used:

1) $\det(M) = \prod_{l=1}^{L} \lambda_l$ [9, p. 658];
2) If $p(M)$ is a polynomial in M, then $p(\lambda_l)$, $l = 1,\cdots, L$, are the L eigenvalues of $p(M)$ [9, p. 661].

Setting $M = S_J S_J^H$ and $p(M) = I_L + (w_c/N_0)M$ gives $\det[p(M)] = \prod_{l=1}^{L}(1 + \lambda_l w_c/N_0)$. The lemma now follows from (16). □

We return now to the proof of Proposition 2. It follows from Lemma 1 that $C_{\text{sum}}(S_J)$ is a function of $\underline{\lambda}$, where $\underline{\lambda} = [\lambda_1,\cdots, \lambda_L]^T$ is the vector of eigenvalues of $S_J S_J^H$. These eigenvalues are real and non-negative because $S_J S_J^H$ is Hermitian [9, p. 663] and positive semidefinite [9, p. 667]. Note that $C_{\text{sum}}(S_J)$ as given in Lemma 1 is convex-$\cap$ on the convex set $\{\underline{\lambda}: \lambda_l \geq 0,\ l = 1,\cdots, L\}$ and is a symmetric function of $\underline{\lambda}$.

Because the trace of a square matrix equals the sum of its eigenvalues [9, p. 658], we have $\sum_{l=1}^{L} \lambda_l = \text{tr}(S_J S_J^H) = \text{tr}(S_J^H S_J) = \sum_{k \in J} s_k^H s_k = |J|L$. Here, we used the fact that $\text{tr}(M_1 M_2) = \text{tr}(M_2 M_1)$ whenever the matrix products are meaningful [9, p. 658]. Thus, $\underline{\lambda} \in \mathscr{F}_{|J|}$ where $\mathscr{F}_{|J|}$ is the convex set given by

$$\mathscr{F}_{|J|} = \left\{ \underline{\lambda} \,|\, \sum_{l=1}^{L} \lambda_l = |J|L \text{ and } \lambda_l \geq 0 \text{ for } l = 1,\cdots, L \right\}.$$

For WBE sequence multisets, the set of $\underline{\lambda}$ vectors can be further restricted. Let α_l, $l = 1,\cdots, L$, denote the L eigenvalues of $S_{J^c} S_{J^c}^H$ and note that these eigenvalues are real and non-negative. Since $S_J S_J^H + S_{J^c} S_{J^c}^H = SS^H$, it follows for all WBE sequence multisets $\mathscr{S}$ that $S_J S_J^H + S_{J^c} S_{J^c}^H = KI_L$. Multiplying from the right by the eigenvector $\underline{q}_l$ corresponding to the eigenvalue λ_l gives $S_{J^c} S_{J^c}^H \underline{q}_l = (K - \lambda_l)\underline{q}_l$. It follows for all WBE sequence multisets $\mathscr{S}$ that the eigenvalues of $S_{J^c} S_{J^c}^H$ and of $S_J S_J^H$ are related as $\alpha_l = K - \lambda_l$ for $l = 1,\cdots, L$. Moreover, since both λ_l and α_l are real and non-negative, it follows that $\underline{\lambda} \in \mathscr{H}$ where $\mathscr{H}$ is the convex set given by

$$\mathscr{H} = \{\underline{\lambda} \,|\, 0 \leq \lambda_l \leq K \text{ for } l = 1,\cdots, L\}.$$

Thus, $\underline{\lambda}$ must belong to the convex set $\mathscr{F}_{|J|} \cap \mathscr{H}$ if S corresponds to a WBE sequence multiset.

Because $C_{\text{sum}}(S_J)$ is convex-$\cap$ and symmetric when considered as a function of $\underline{\lambda}$, it takes its minimum value on the extrema of the convex set $\mathscr{F}_{|J|} \cap \mathscr{H}$. But the extrema of $\mathscr{F}_{|J|} \cap \mathscr{H}$ are just the points $\underline{\lambda}$ where $\lfloor |J|L/K \rfloor$ components are equal to K, one component is equal to $\gamma = |J|L - K\lfloor |J|L/K \rfloor$ (so that $0 \leq \gamma < K$) and all other components are 0, where $\lfloor x \rfloor$ denotes the largest integer not larger than x. Thus, for every non-empty subset J of $\{1,\cdots, K\}$,

$$\begin{aligned}
&\min_{\underline{\lambda} \in (\mathscr{F}_{|J|} \cap \mathscr{H})} C_{\text{sum}}(S_J) \\
&\quad = \frac{1}{L}\left[\left\lfloor \frac{|J|L}{K} \right\rfloor \log\left(1 + K\frac{w_c}{N_0}\right) + \log\left(1 + \gamma\frac{w_c}{N_0}\right) \right] \\
&\quad = \frac{1}{L}\left[\frac{|J|L - \gamma}{K} \log\left(1 + K\frac{w_c}{N_0}\right) + \log\left(1 + \gamma\frac{w_c}{N_0}\right) \right].
\end{aligned}$$

But, since $0 \leq \gamma/K < 1$, the simple inequality, $(1 + x)^a \leq 1 + ax$ for $0 \leq a \leq 1$ and $x \geq -1$, can be applied to give

$$\log\left(1 + \gamma\frac{w_c}{N_0}\right) \geq \frac{\gamma}{K} \log\left(1 + K\frac{w_c}{N_0}\right).$$

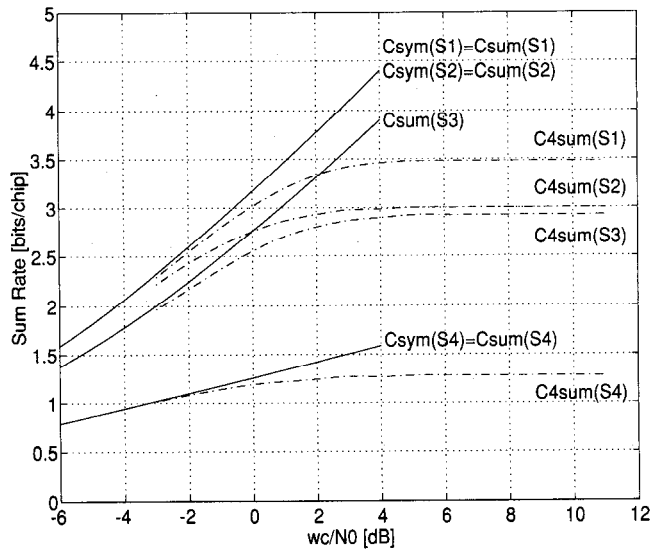

Fig. 3. Sum capacity $C_{\text{sum}}(S)$, symmetric capacity $C_{\text{sym}}(S)$ and $C_{4\text{sum}}(S)$ in terms of S_i, $i = 1,\cdots, 4$, given in Example 2 versus the SNR w_c/N_0 when $W = w_c I_K$.

It follows that

$$\min_{\underline{\lambda} \in (\mathscr{F}_{|J|} \cap \mathscr{H})} C_{\text{sum}}(S_J) \geq \frac{|J|}{K} \log\left(1 + K\frac{w_c}{N_0}\right)$$

which implies the inequality (21) that was to be shown. □

Example 2: Consider the bipolar sequence multisets $\mathscr{S}_1$, $\mathscr{S}_2$, $\mathscr{S}_3$, and $\mathscr{S}_4$ with $K = 8$ sequences of length $L = 4$ and corresponding sequence matrices

$$S_1 = \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & + & + & + & - & - & - & - \\ + & + & - & - & + & + & - & - \\ + & - & + & - & + & - & + & - \end{bmatrix}$$

$$S_2 = \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \end{bmatrix}$$

$$S_3 = \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & + & + & - & + & + & + & + \\ + & + & - & + & - & - & - & - \\ + & - & + & + & - & - & - & - \end{bmatrix}$$

$$S_4 = \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & + & + & + & + & + & + & + \\ + & + & + & + & + & + & + & + \\ + & + & + & + & + & + & + & + \end{bmatrix}$$

where "+" and "−" denote 1 and −1, respectively. The set $\mathscr{S}_1$ is a WBE sequence set and the multiset $\mathscr{S}_2$ is a WBE sequence multiset, i.e., $S_1 S_1^T = S_2 S_2^T = KI_L$. $\mathscr{S}_3$ is a "good" sequence multiset whose total squared correlation is close to Welch's bound (20) and whose corresponding sequence matrix S_3 has full rank. Finally, $\mathscr{S}_4$ is a worst sequence multiset with respect to the sum capacity and the total squared correlation.

Fig. 3 shows the sum and the symmetric capacities for these sequence multisets versus the SNR w_c/N_0 when $W = w_c I_K$. As was proved in Corollary 1, we see that the sum capacity is indeed maximized by the WBE sequence multisets $\mathscr{S}_1$ and $\mathscr{S}_2$, respectively. In accordance with Proposition 2, the symmetric capacity is this same maximum for $\mathscr{S}_1$ and $\mathscr{S}_2$. It is easily seen that $C_{\text{sym}}(S_4) = C_{\text{sum}}(S_4)$. The symmetric capacity $C_{\text{sym}}(S_3)$ is not shown, but it can be verified that $C_{\text{sym}}(S_3) < C_{\text{sum}}(S_3)$.

VI. Concluding Remarks

In our derivation of the capacity region of the S-CDMA channel, we allowed the channel-input symbols to take any values in the complex field. In practice, one generally wishes to use proper complex, discrete-valued channel-input symbols. It is intuitively obvious that such equiprobable, discrete-valued symbols achieve capacity when the SNR is sufficiently small, since the condition for approximately achieving capacity is that $\underline{Y} = \underline{U} + \underline{N}$ be approximately Gaussian, not that $\underline{U}$ be approximately Gaussian. This is confirmed in Fig. 3 where we show the sum capacity $C_{4\text{sum}}(S)$ of the S-CDMA channel specified by the sequence sets $\mathcal{S} = \mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$, and $\mathcal{S}_4$ given in Example 2, when the quaternary phased-shift keying (QPSK) modulated channel-input symbols X_k, $k = 1, \cdots, K$, have average energy $E[|X_k|^2] = w_c$ and are in phase synchronism. Note that the sequence multiset $\mathcal{S}_2$ contains two repetitions of four orthogonal sequences. This means that the four-dimensional S-CDMA channel decomposes into four 2-user GMAC's having quaternary channel-input symbols, which is why the asymptotic (for large SNR) sum capacity $C_{4\text{sum}}(\mathcal{S}_2)$ is $2 \cdot 1.5$ bits per chip [2, p. 392]. In this case, the joint decoder can be split into four separate decoders, each of which jointly decodes only two users.

Although we have considered only synchronous CDMA, our upper bound on the sum capacity applies also to general (i.e., asynchronous) CDMA systems of bandwidth $W = 1/(2T_c)$, where T_c is the chip period. The proof of Proposition 1 can be modified to show in this case that the upper bound on the sum capacity is achieved when the samples $U(nT_c)$, all n, of the transmitted sum signal $U(t)$ are zero-mean, proper complex, Gaussian random variables that are uncorrelated and have the same variance. This happens, for example, whenever $L = 1$, the spectrum of the chip waveform is flat over the specified frequency band, and the channel-input sequences $X_k[\cdot]$, $k = 1, \cdots, K$, are sequences of independent and zero-mean, proper complex, Gaussian random variables.

References

[1] F. D. Neeser and J. L. Massey, "Proper complex random processes with applications to information theory," *IEEE Trans. Inform. Theory*, vol. IT-39, pp. 1293–1302, July 1993.

[2] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[3] S. Verdú, "Capacity region of Gaussian CDMA channels: The symbol-synchronous case," in *Proc. 24th Allerton Conf.*, Oct. 1986, pp. 1025–1034.

[4] J. K. Wolf, "Coding techniques for multiple access communication channels," in *New Concepts in Multi-User Communication*, J. K. Skwirzynski, Ed. Alphen aan de Rijn: Sijthoff & Noordhoff, 1981, pp. 83–103.

[5] J. L. Massey and Th. Mittelholzer: "Welch's bound and sequence sets for code-division multiple-access systems," in *Sequences II, Methods in Communication, Security, and Computer Science*, R. Capocelli, A. De Santis, and U. Vaccaro, Eds. New York: Springer-Verlag, 1993.

[6] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 397–399, May 1974.

[7] V. M. Sidelnikov, "On mutual correlation of sequences," *Soviet Math. Dokl.*, vol. 12, pp. 197–201, 1971.

[8] D. Slepian, "Permutation Modulation," *Proc. IEEE*, pp. 228–236, Mar. 1965.

[9] T. Kailath, *Linear Systems*. Englewood Cliffs, NJ: Prentice-Hall, 1980.

On the Existence of Cyclic Hadamard Difference Sets

Hong Y. Song and Solomon W. Golomb

***Abstract*—The main conjecture of this note is the following: if a cyclic $(v = 4n - 1, k = 2n - 1, \lambda = n - 1)$ Hadmard difference set exists, the *the value of v must be either a prime, or a product of "twin primes," or* one less than a power of 2. Six cases, $v = 399, 495, 627, 651, 783,$ and 975, which were once listed as the possible exceptions for $v < 1000$, are now fully investigated, and all the cases of $v < 10\,000$ are now verified relative to this conjecture, with at most 17 possible exceptions.**

***Index Terms*—Cyclic Hadamard difference sets, classification of balanced binary PN sequences, two-level autocorrelation sequences.**

I. Introduction

Consider a binary sequence a_i of length v for $a_i \in \{+1, -1\}$. The (unnormalized) periodic autocorrelation function $f(\tau)$ for $\tau = 0, 1, 2, \cdots, v - 1$ is defined to be

$$f(\tau) \triangleq \sum_{i=0}^{v-1} a_i a_{i+\tau} \tag{1.1}$$

where the subscripts are taken modulo v. Balanced binary sequences for which the function $f(\tau)$ has only two distinct values are known to be important because of their applications to various digital communications systems [7]–[9], [11], [17]. This property of balanced binary sequences is called the *two-level autocorrelation property* [8], and can be stated as follows:

$$f(\tau) = \begin{cases} v - 1, & \text{for } \tau = 0 \\ -1, & \text{for } \tau = 1, 2, \cdots, v - 1. \end{cases} \tag{1.2}$$

A balanced binary "two-level autocorrelation sequence" of length v is also known as a "cyclic Hadamard sequence" because of its relation to cyclic Hadamard matrices of order $v + 1$, and hence to $(v = 4n - 1, k = 2n - 1, \lambda = n - 1)$ cyclic differences sets [1], [7], [14]. Specifically, such a sequence has length $v = 4n - 1$ for some positive integer n, consists of $k = 2n - 1 + 1$'s (and $k + 1 = 2n - 1$'s), and has out-of-phase autocorrelation $f(\tau \not\equiv 0) = -1$ for all out-of-phase positions $\tau \not\equiv 0 \pmod{v}$. The question is then: 1) for which values of $v = 4n - 1$ do these "cyclic Hadamard sequences" of length v exist?, and 2) what constructions can be used to generate these sequences? In Baumert's book [1], it is mentioned that all *known* examples of cyclic Hadamard sequences have values of v from only three different "families":

(A) $v = 4n - 1$ is a prime number,

(B) $v = p(p + 2)$ is a product of "twin primes,"

(C) $v = 2^t - 1$, for $t = 2, 3, 4, \cdots$.

It is also reported in [1] that there are no other values of $v < 1000$ with cyclic Hadamard sequences, except for the six cases $v = 399, 495, 627, 651, 783,$ and 975, not fully investigated. It turned out that these six cases are also ruled out (Section II) for the existence of cyclic Hadamard sequences. In conclusion,

Manuscript received March 11, 1993; revised March 11, 1994. This work was supported in part by the U.S. Office of Naval Research under Grant N00014-90-J-1341. This paper was presented in part at the 14th British Combinatorial Conference, University of Keele, England, July 1993.

The authors are with the Communication Sciences Institute, Department of Electrical Engineering—Systems, University of Southern California, Los Angeles, CA 90089.

IEEE Log Number 9403717.