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 $\mathscr{S} = \mathscr{S}_1$, $\mathscr{S}_2$, $\mathscr{S}_3$, and $\mathscr{S}_4$ 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 $\mathscr{S}_2$ 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 $C_{4\text{sum}}(S_2)$ 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 $f(\tau \neq 0) = -1$ 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.

there are no counterexamples to the following conjecture for $v < 1000$: *if there exists a cyclic Hadamard sequence of length v then $v = 4n - 1$ must be either a prime, or a product of "twin primes," or one less than a power of 2.*

The known *constructions* corresponding to these values of v are as follows.

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

A1: The "Legendre sequence" (quadratic residue) construction in *all* such cases [8].
A2: Hall's "sextic residue" construction, when the prime number v is of the form $4A^2 + 27$ for some integer A [12].

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

B1: The "Jacobi sequence" construction (generalization of the Legendre sequence idea) as first described by Stanton and Sprott [18].

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

C1: The linear shift register sequences (also called m-sequences) for *all* values of $t > 1$ [8].
C2: The Gordon–Mills–Welch sequences (GMW sequences) for certain composite values of t [10], [11].
C3: Three miscellaneous examples at $v = 2^7 - 1 = 127$ found by Baumert and Fredricksen [2], two miscellaneous examples at $v = 2^8 - 1 = 255$ found by Cheng (Type 2 and Type 3 in [3]), and two miscellaneous examples at $v = 2^9 - 1 = 511$ found by Dreier (first and third non-Singer types in [5]). These examples are not otherwise explained. (A complete search [3]–[6] has been done only for $t \leq 9, v \leq 511$.)

By using several of the known nonexistence tests (both nonconstructive and constructive) and a computer, the above conjecture is now reconfirmed for *all* $v < 1000$, including those six new cases. Furthermore, it is verified up to $v < 10\,000$, except for the following 17 cases: 1295, 1599, 1935, 3135, 3439, 4355, 4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, 9423.

This conjecture could conceivably be false (considering that there seems to be no simple property common to the above three families of integers), but the evidence for it is becoming impressive. A brief summary of the computer search is discussed in the next section.

II. Some Computations

Up to 10 000, there are 2500 values of $v = 4n - 1$ which are congruent to 3 mod 4. Of these, 619 numbers are primes, 8 numbers are products of twin primes, and 12 numbers are one less than a power of 2. There are 5 numbers which are both prime and one less than $2^t[v = 3, 7, 31, 127, 8191$, known as "Mersenne primes"]. The number $v = 15$ is the only case which is both a twin prime product and one less than 2^t. Therefore, there are $2500 - 633 = 1867$ cases remaining which are the initial targets for the existence/nonexistence test.

It turned out that the following two theorems (for nonconstructive test) are most powerful in initially screening out most of the 1867 cases. Application of these theorems is rather easy, and all the terminologies are from either [1] or [14].

Theorem 1 (Hall and Ryser, 1951 [15]): If a nontrivial (v, k, λ) difference set exists for odd v, then, for every divisor w of v, the following equation

$$z^2 = nx^2 + (-1)^{(w-1)/2} wy^2 \qquad \text{where } (n = k - \lambda) \quad (2.3)$$

has a solution in integers x, y, z, not all zero.

TABLE I
Decomposition of Integers mod 27 into 7 Cyclotomic Cosets

name	size	rep.	rep. (mod 3)	a_i	class
C1	1	0	0	a_1	1
C2	1	9	0		
C3	1	18	0		
C4	3	3	0	a_2	2
C5	3	6	0		
C6	9	1	1	a_3	3
C7	9	2	2	a_4	4

Theorem 2 (Mann, 1964 [16]): Let $w > 1$ be a divisor of v, and assume a nontrivial (v, k, λ) difference set exists with w-multiplier $t \geq 1$. Let p be a prime divisor of $n = k - \lambda$ for which $(p, w) = 1$. If there exists an integer $f \geq 0$ such that $tp^f \equiv -1 \pmod{w}$, then n is strictly divisible by an even power of p.

Theorem 1 rules out 1271 cases, and fails to rule out the remaining 596 cases. Of these 596 cases, Theorem 2 rules out 353 cases, and leaves open 243 cases. Of these 243 cases, two more theorems [1, Theorems 2.15 and 2.16] are used to rule out 17 cases. To handle the remaining 226 cases, the following necessary condition (for constructive test) is used.

Theorem 3 (Baumert, 1971 [1]): If a cyclic (v, k, λ) difference set exists, then, for every divisor w of v, there exist integers $b_i (i = 0, 1, 2, \cdots, w - 1)$ satisfying the diophantine equations

$$\sum_{i=0}^{w-1} b_i = k, \qquad \sum_{i=0}^{w-1} b_i^2 = n + \frac{\lambda v}{w}, \qquad 0 \leq b_i \leq v/w \quad (2.4)$$

where $n = k - \lambda$ and

$$\sum_{i=0}^{w-1} b_i b_{i-j} = \frac{\lambda v}{w} \quad (2.5)$$

for $j = 1, 2, \cdots, w - 1$. (Here, the subscript $i - j$ is taken mod v.)

The cases in which there are only three cyclotomic cosets modulo w for some divisor w of v are easy to test systematically by applying Theorem 3 (we call this a "3-cosets-test"). The smallest such case is $v = 27$ and will be ruled out by the following argument. By Theorem 3, if there exists a $(27, 13, 6)$ difference set D, then there exist integers b_0, b_1, b_2 satisfying

$$\begin{gathered} b_0 + b_1 + b_2 = 13 \\ b_0^2 + b_1^2 + b_2^2 = 61 \\ 0 \leq b_0, b_1, b_2 \leq 9. \end{gathered} \quad (2.6)$$

These equations have exactly six solutions, which are all the permutations of $\{3, 4, 6\}$. To show the nonexistence, note that $n = k - \lambda = 7$ is a multiplier in this case, and there are seven cyclotomic cosets mod 27 whose sizes and smallest representatives are shown in Table I. It also shows four variables a_1, a_2, a_3, and a_4, each of which indicates how many cosets in each class must be in the (possible) difference set D. Therefore, $a_1 \in \{0, 1, 2, 3\}$, $a_2 \in \{0, 1, 2\}$, and $a_3, a_4 \in \{0, 1\}$. Note that b_j for $j = 0, 1, 2$ in Theorem 3 counts the number of residues (which must be in D) which are congruent to j mod 3. This leads to some additional constraints on b_i's as follows:

$$b_0 = a_1 + 3a_2, \qquad b_1 = 9a_3, \qquad b_2 = 9a_4. \tag{2.7}$$

Now, it is not hard to determine that there are no solutions (a_1, a_2, a_3, a_4) from the values $\{b_0, b_1, b_2\} = \{3, 4, 6\}$. This guarantees the nonexistence of a $(27, 13, 6)$ cyclic difference set. Note that the analysis could have determined possible values of a_i's. In that case, one must check all the possible choices of cosets determined by a_i's. This will either lead to the proof of nonexistence or find a counterexample to the conjecture.

The "3-cosets-test" rules out 171 cases ($v = 627$ is one of these cases), but cannot settle the final 55 cases. The remaining 55 cases are treated individually using Baumert's necessary condition (above) and various other combinations of divisors of v. It turned out that the following 38 cases are ruled out: 175, 343, 399, 651, 975, 1155, 1331, 1387, 2223, 2263, 2299, 2415, 2703, 2883, 3055, 3567, 3663, 3887, 4015, 4303, 4495, 4687, 4975, 5047, 5475, 5551, 6351, 6399, 6859, 7231, 7375, 7923, 8883, 8899, 9331, 9583, 9647, 9711; and the following 17 cases remain open: 1295, 1599, 1935, 3135, 3439, 4355, 4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, 9423.

Finally, all of these results were obtained by computer, and await independent confirmation by others to fully establish their validity.

References

[1] L. D. Baumert, *Cyclic Difference Sets (Lecture Note in Mathematics 182)*. New York: Springer-Verlag, 1971.

[2] L. D. Baumert and H. Fredricksen, "The cyclotomic numbers of order eighteen with applications to difference sets," *Math. Computation*, vol. 21, no. 98, pp. 204–219, 1967.

[3] U. Cheng, "Exhaustive construction of (255, 127, 63)-cyclic difference sets," *J. Combinatorial Theory*, vol. A-35, pp. 115–125, 1983.

[4] U. Cheng and S. W. Golomb, "On the characterization of PN sequences," *IEEE Trans. Inform. Theory*, vol. IT-29, p. 600, 1983.

[5] R. Dreier, "(511, 255, 127) cyclic difference sets," IDA talk, July 1992.

[6] S. W. Golomb, "On the classification of balanced binary sequences," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 730–732, 1982.

[7] S. W. Golomb, Ed., *Digital Communications with Space Applications*. Englewood Cliffs, NJ: Prentice-Hall, 1965; Peninsula, Los Altos, CA: 1981.

[8] ——, *Shift Register Sequences*. San Francisco, CA: Holden-Day, 1967; Laguna Hills, CA: Aegean Park Press, 1982 (revised ed.).

[9] ——, "Two-valued sequences with perfect periodic autocorrelation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-28, pp. 383–386, 1992.

[10] B. Gordon, W. H. Mills, and L. R. Welch, "Some new difference sets," *Canadian J. Math.*, vol. 14, pp. 614–625, 1962.

[11] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, no. 3, pp. 548–553, 1984.

[12] M. Hall, Jr., "A survey of difference sets," *Proc. Amer. Math. Soc.*, vol. 7, pp. 975–986, 1956.

[13] ——, "Difference sets," in *Combinatorics*, M. Hall, Jr. and J. H. van Lint, Eds. *Proc. NATO Adv. Study Inst.*, Nijenrode Castle, Breukelen, The Netherlands, July 1974.

[14] ——, *Combinatorial Theory*, 2nd ed. New York: Wiley, 1986.

[15] M. Hall, Jr. and H. J. Ryser, "Cyclic incidence matrices," *Canadian J. Math.*, vol. 3, pp. 495–502, 1951.

[16] H. B. Mann, "Balanced incomplete block designs and Abelian difference sets," *Illinois J. Math.*, vol. 8, pp. 252–261, 1964.

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

[18] R. G. Stanton and D. A. Sprott, "A family of difference sets," *Canadian J. Math.*, vol. 10, pp. 73–77, 1958.

Further Results on Difference Triangle Sets

Zhi Chen

Abstract—**Further results on the upper bounds for difference triangle sets (DTS) are derived from disjoint difference sets and additive sequences of permutations, which greatly improve the known bounds.**

Index Terms—**Codes and coding, combinatorial theory, convolutional codes.**

I. Introduction

Difference triangle sets (DTS) were first introduced in the construction of convolutional self-orthogonal codes by Robinson and Bernstein [1]. Up to now, many constructions of DTS have been proposed by many researchers [2]–[6]. The best known lower bounds and upper bounds on the size of DTS can be found in [4], [6]. For the applications of DTS, see [4] and the references given there.

In this correspondence, we present further results on the upper bounds of DTS. In [6], we have proposed a construction of DTS from so-called disjoint difference sets (DDS), and obtained many new upper bounds. Here, we obtain new upper bounds of DTS from DDS derived from the finite Euclidean geometry and difference families [13]. Also, additive sequences of permutations are used to construct new DTS. These new results greatly improve the best known upper bounds.

II. Difference Triangle Sets Constructed from Disjoint Difference Sets

An (I, J)-DTS is a set of $\Delta = \{\Delta_1, \Delta_2, \cdots, \Delta_I\}$, where

$$\Delta_i = \{a_{ij} | 0 \le j \le J\}, \qquad 1 \le i \le I,$$

have integer elements such that

$$0 = a_{i0} < a_{i1} < \cdots < a_{iJ}$$

for all i and such that the integers a_{ij} and $a_{ij'}$ with $1 \le i \le I$ and $0 \le j' < j \le J$ are distinct. Let

$$m = m(\Delta) = \max\{a_{iJ} | 1 \le i \le I\}, \tag{1}$$

$$M(I, J) = \min\{m(\Delta) | \Delta \text{ is a } (I, J)\text{-DTS'}\}. \tag{2}$$

An (I, J)-DTS Δ such that $m(\Delta) = M(I, J)$, is called optimal. A convolutional self-orthogonal $(I + 1, I, m)$ code with minimum distance $d = J + 2$ can be constructed from an (I, J)-DTS. It has generator polynomials:

$$g_i(D) = \sum_{j=0}^{J} D^{a_{ij}}, \qquad 1 \le i \le I. \tag{3}$$

Since m determines the length of the encoding and decoding shift registers, it is desirable to make m as small as possible. For other applications of DTS, see [4].

Many constructions for DTS have been proposed. In [6], the author presented a construction from disjoint difference sets (DDS). By a (v, k, t)-DDS of order v, we mean a family $(B_i | i \in I$, $t = |I|)$ of subsets of Z_v, each of cardinality k, and such that

Manuscript received August 3, 1993.

The author was with the Department of Electrical Engineering, Linköping University, S-581 83 Linköping, Sweden. Now, he is with the Technical Department, University of Kristianstad, S-281 39 Hassleholm, Sweden.

IEEE Log umber 9402456.