ELSEVIER

Journal of Statistical Planning and Inference 62 (1997) 39–41

journal of statistical planning and inference

A conjecture on the existence of cyclic Hadamard difference sets

Solomon W. Golomb [a,1], Hong-Yeop Song [b,*]

[a] *Department of EE-Systems, University of Southern California, Los Angeles, CA 90089-2565, USA*
[b] *Department of Electronic Engineering, Yonsei University, Seoul 120-749, South Korea*

Received 8 October 1993; revised 15 February 1996

Abstract

If there exists a cyclic Hadamard difference set of length v, then $v = 4n - 1$ is conjectured to be either a prime, or a product of "twin primes", or one less than a power of 2.

AMS classification: primary 05B10; secondary 62K05

Keywords: Cyclic Hadamard Difference Sets, Balanced Binary Sequences with Two-level Autocorrelation.

A cyclic (v,k,λ) difference set D is a set of k residues modulo v such that for each non-zero residue $d \bmod v$, the equation $x - y \equiv d \,(\mathrm{mod}\, v)$ has exactly λ solution pairs (x, y) where $x, y \in D$ (Baumert, 1971). In particular, cyclic *Hadamard* difference sets have the parameters $v = 4n - 1$, $k = 2n - 1$ and $\lambda = n - 1$ for a positive integer n, and are known to be important because of their applications to various digital communications systems (Golomb, 1981, 1982, 1992; Scholtz and Welch, 1984; Simon et al., 1995).

The main questions are: (1) for what values of $v = 4n - 1$ do these cyclic Hadamard difference sets exist, and (2) what constructions are known to generate them? In Baumert's (1971) book, it is mentioned that all *known* examples of cyclic Hadamard difference sets 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', or (c) $v = 2^t - 1$, for $t = 2,3,4,\ldots$ It is also reported in Baumert (1971) that there are no other values for $v < 1000$ with cyclic Hadamard difference sets, with 6 *possible* exceptions which are $v = 399, 495, 627, 651, 783$, and 975. It turned out that these six cases are also ruled out for the existence of cyclic Hadamard difference sets (Song and Golomb, 1994). In conclusion, there are no counterexamples to the following conjecture for $v < 1000$: *if there exists a cyclic Hadamard difference set of length v, then*

* Corresponding author.

[1] Supported in part by the United States Office of Naval Research under Grant No. N00014-90-J-1341.

PII S0378-3758(96)00165-6

$v = 4n - 1$ 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 symbol' (quadratic residue) construction, in *all* such cases (Golomb, 1982).

(a2) Hall's 'sextic residue' construction, when the prime number v is of the form $4A^2 + 27$ for some integer A (Hall, 1956).

(b) $v = p(p + 2)$ is a product of 'twin primes'.

(b1) The 'Jacobi symbol' construction (generalization of the Legendre symbol idea) as first described by Stanton and Sprott (1958).

(c) $v = 2^t - 1$ for some integer $t = 2, 3, 4, \ldots$

(c1) The linear shift register sequences (also called m-sequences) construction for *all* values of $t > 1$ (Golomb, 1982).

(c2) The Gordon–Mills–Welch construction (GMW sequences) for certain composite values of t (Gordon et al., 1962; Scholtz and Welch, 1984).

(c3) Three miscellaneous examples at $v = 2^7 - 1 = 127$ found by Baumert and Fredricksen (1967), two miscellaneous examples at $v = 2^8 - 1 = 255$ found by Cheng (types 2 and 3 in Cheng (1983)), and three miscellaneous examples at $v = 2^9 - 1 = 511$ found by Dreier. These examples are not otherwise explained. (A complete search for $v = 2^t - 1$ has been done only for $t \leqslant 9$, $v \leqslant 511$ (Cheng, 1983; Cheng and Golomb, 1983; Dreier, 1992; Golomb, 1982; Welch, 1996)).

Recently, by using several of the known non-existence tests (both non-constructive and constructive) and a computer, the above conjecture was reconfirmed for *all* $v < 1000$ and the six cases $v = 399, 495, 627, 651, 783$, and 975 were ruled out for the existence of cyclic Hadamard difference sets (Song and Golomb, 1994). Furthermore, it was verified up to $v < 10000$ except for the following 17 cases: 1295, 1599, 1935, 3135, 3439, 4355, 4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, and 9423 (Song and Golomb, 1994).

Considering that there seems to be no simple property common to the above three families of integers, the conjecture could conceivably be false but the evidence for it is becoming impressive. We believe that the existence of the miscellaneous examples (c3) above might shed some light on the truth/falsity of this conjecture if these examples are carefully investigated.

References

Baumert, L.D. (1971). *Cyclic Difference Sets*. Lecture Notes in Math., Vol. 182, Springer, Berlin.

Baumert, L.D. and H. Fredricksen (1967). The cyclotomic numbers of order eighteen with applications to difference sets. *Math. Comput.* **21**, 204–219.

Cheng, U. (1983). Exhaustive construction of (255, 127, 63)-cyclic difference sets. *J. Combin. Theory* **A-35**, 115–125.

Cheng, U. and S.W. Golomb (1983). On the characterization of PN sequences. *IEEE Trans. Inform. Theory* **IT-29**, 600.

Dreier, R. (1992). (511, 255, 127) cyclic difference sets. IDA Talk.

Golomb, S.W. (1982). On the classification of balanced binary sequences of period $2^n - 1$. *IEEE Trans. Inform. Theory* **IT-26**, 730–732.

Golomb, S.W., Ed. (1965). *Digital Communications with Space Applications*. Prentice-Hall, Englewood Cliffs, NJ (Peninsula Publishing Company, Los Altos, CA, 1981).

Golomb, S.W. (1967). *Shift Register Sequences*. Holden-Day, San Francisco, CA (Revised Edition, Aegean Park Press, Laguna Hills, CA, 1982).

Golomb, S.W. (1992). Two-valued sequences with perfect periodic autocorrelation. *IEEE Trans. Aerospace Electron. Systems*. **AES-28**, 383–386.

Gordon, B., W.H. Mills and L.R. Welch (1962). Some new difference sets. *Canad. J. Math.* **14**, 614–625.

Hall, M. Jr. (1956). A survey of difference sets. *Proc. Amer. Math. Soc.* **7**, 975–986.

Hall, M. Jr. (1974). Difference sets. In: M. Hall, Jr. and J.H. van Lint, Eds., *Combinatorics; Proc. NATO Advanced Study Institute*, Nijenrode Castle, Breukelen, Netherlands, 8–20 July.

Hall, M. Jr. (1986). *Combinatorial Theory*, 2nd ed. Wiley, New York.

Hall, M. Jr. and H.J. Ryser (1951). Cyclic incidence matrices. *Canad. J. Math.* **3**, 495–502.

Jungnickel, D. (1992). Difference sets. In: J.H. Dinitz and D.R. Stinson, Eds., *Contemporary Design Theory*. Wiley, New York, 241–324.

Mann, H.B. (1964). Balanced incomplete block designs and Abelian difference sets. *Illinois J. Math.* **8**, 252–261.

Scholtz, R.A. and L.R. Welch (1984). GMW sequences. *IEEE Trans. Inform. Theory* **IT-30**, 548–553.

Simon, M.K., J.K. Omura, R.A. Scholtz and B.K. Levitt (1985). *Spread Spectrum Communications*. Computer Science Press, Rockville, MD.

Song, H.Y. and S.W. Golomb (1994). On the existence of cyclic Hadamard difference sets. *IEEE Trans. Inform. Theory* **40**, 1266–1268.

Stanton, R.G. and D.A. Sprott (1958). A family of difference sets. *Canad. J. Math.* **10**, 73–77.

Welch, L. (1996). Private communication.