Des. Codes Cryptogr. (2009) 51:231–243
DOI 10.1007/s10623-008-9257-8

Gold codes, Hadamard partitions and the security of CDMA systems

Derek H. Smith · Richard P. Ward · Stephanie Perkins

Received: 9 April 2008 / Revised: 2 October 2008 / Accepted: 26 November 2008 /
Published online: 19 December 2008

Abstract Let $V = \{1, 2, \ldots, M\}$ and let $\{H_i : i \in V\}$ be a set of Hadamard matrices with the property that the magnitude of the dot product of any two rows of distinct matrices is bounded above. A *Hadamard partition* is any partition of the set of all rows of the matrices H_i into Hadamard matrices. Such partitions have an application to the security of quasi-synchronous code-division multiple-access radio systems when loosely synchronized (LS) codes are used as spreading codes. A new generation of LS code can be used for each information bit to be spread. For each generation, a Hadamard matrix from some partition is selected for use in the code construction. This code evolution increases security against eavesdropping and jamming. One security aspect requires that the number of Hadamard partitions be large. Thus the number of partitions is studied here. If a Kerdock code construction is used for the set of matrices, the Hadamard partition constructed is shown to be unique. It is also shown here that this is not the case if a Gold (or Gold-like) code construction is used. In this case the number of Hadamard partitions can be enumerated, and is very large.

Keywords Gold codes · Hadamard matrices · Loosely synchronized codes

Mathematics Subject Classifications (2000) 05B20 · 94B99

Communicated by L. Teirlinck.

D. H. Smith (✉) · R. P. Ward · S. Perkins
Division of Mathematics and Statistics, University of Glamorgan,
Pontypridd CF37 1DL, Wales, UK
e-mail: dhsmith@glam.ac.uk

R. P. Ward
e-mail: rpward@glam.ac.uk

S. Perkins
e-mail: sperkins@glam.ac.uk

1 Introduction

A *Hadamard matrix* is an $n \times n$ matrix H with elements in $\{+1, -1\}$ such that $HH^T = nI$ [3]. Suppose that matrix H_i has rows $\mathbf{r}_j^{(i)}$ with $j \in \{0, \ldots, n-1\}$. Let $V = \{1, 2, \ldots, M\}$.

Definition 1 A set $\{H_i : i \in V\}$ of Hadamard matrices will be called *correlation constrained* if $\mathbf{r}_{j_1}^{(i_1)} \cdot \mathbf{r}_{j_2}^{(i_2)}$ $(j_1, j_2 \in \{0, \ldots, n-1\}, \quad i_1, i_2 \in V,\ i_1 \neq i_2)$ lies in an interval $[-\chi, \chi]$.

There are applications of correlation constrained sets of Hadamard matrices in both synchronous code-division multiple-access (S-CDMA) [10] and quasi-synchronous code-division multiple-access (QS-CDMA) radio systems [7]. The value of χ is usually chosen to be as small as can be achieved for a set of the required size. Here $n = 2^m$ and integer values of χ in the interval $[2^{m/2}, 2^{(m+2/2}]$ will be used.

Consider the union of rows $U = \cup_{i \in V, j \in \{0,\ldots,n-1\}} \mathbf{r}_j^{(i)}$. It is possible that $\{H_i : i \in V\}$ is the unique partition of U into Hadamard matrices. It is also possible that the number of ways of partitioning U into Hadamard matrices is very large. Here any such partition is referred to as a *Hadamard partition*.

In Sect. 2 a security concern for the use of loosely synchronized (LS) codes in QS-CDMA systems is described. These codes are constructed using Hadamard matrices. The security concern need not arise if the number of Hadamard partitions is large. In this paper constructions of sets of Hadamard matrices from [7,10] based on Kerdock codes (for m even) and based on Gold codes (for m odd) are considered. Additional constructions are proposed based on Gold codes for $m \equiv 2 \bmod 4$ and on Gold-like codes for $m \equiv 0 \bmod 4$. In the case of the Kerdock code construction the given Hadamard partition is unique. For the Gold code and Gold-like code construction lower bounds are developed for the number of Hadamard partitions, and this number is shown to be large. These are the first published lower bounds for the number of these Hadamard partitions. As a result of clique searches for small values of m it is conjectured that lower bounds given are tight.

2 Loosely synchronized codes and security

Loosely synchronized codes [1,6,7] are ternary codes that have been proposed for use as spreading codes in QS-CDMA radio systems. Codes designed for QS-CDMA exploit a level of synchronization intermediate between that of synchronous CDMA and asynchronous CDMA. The codewords are vectors $\mathbf{x} = (x_0, x_1, \ldots, x_{N-1})$ with elements in $\{0, +1, -1\}$. Low interference between users results from a zero correlation window for the *aperiodic correlation* [5]:

$$\theta_{\mathbf{x},\mathbf{y}}^{(a)}(\tau) = \begin{cases} \sum_{j=0}^{N-1-\tau} x_j y_{j+\tau \bmod N}, & 0 \leq \tau \leq N-1 \\ \sum_{j=0}^{N-1+\tau} x_{j-\tau \bmod N}\ y_j, & 1-N \leq \tau < 0 \\ 0, & |\tau| \geq N. \end{cases}$$

For some integer T, $\theta_{\mathbf{x},\mathbf{y}}^{(a)}(\tau) = 0$ for $0 \leq |\tau| < T$ (zero cross correlation) and $\theta_{\mathbf{x},\mathbf{x}}^{(a)}(\tau) = 0$ for $0 < |\tau| < T$ (zero off-peak autocorrelation).

Definition 2 Let (C_0, S_0) and (C_1, S_1) be two pairs of $\{+1, -1\}$ vectors, each vector being of length N. Suppose that $\theta_{C_0,C_0}^{(a)}(\tau) + \theta_{S_0,S_0}^{(a)}(\tau) = 0$ for $|\tau| > 0$, $\theta_{C_1,C_1}^{(a)}(\tau) + \theta_{S_1,S_1}^{(a)}(\tau) = 0$ for $|\tau| > 0$ and $\theta_{C_0,C_1}^{(a)}(\tau) + \theta_{S_0,S_1}^{(a)}(\tau) = 0$ for all τ. Then (C_0, S_0), (C_1, S_1) are each referred to as a *Golay pair* and the two pairs form a *cross-complementary sequence pair* [8].

Such pairs exist for all lengths $N = 2^r \times 10^s \times 26^t$, $(r, s, t \geq 0)$.

Let $\pi = [\pi_1, \pi_2, \ldots, \pi_n]$ be a binary vector of length n and let π^* be the complement of π. LS codes have codewords of the form:

$$00\ldots0 \pm C_{\pi_1} \pm C_{\pi_2} \pm C_{\pi_3} \ldots C_{\pi_n} 00\ldots0 \pm S_{\pi_1} \pm S_{\pi_2} \pm S_{\pi_3} \ldots S_{\pi_n}\ 00\ldots0$$

where the $\pm$ signs are determined by the rows of a Hadamard matrix. The same Hadamard matrix row is used for the S part as the C part. A second set of codewords is of the form

$$00\ldots0 \pm C_{\pi_1^*} \pm C_{\pi_2^*} \pm C_{\pi_3^*} \ldots C_{\pi_n^*} 00\ldots0 \pm S_{\pi_1^*} \pm S_{\pi_2^*} \pm S_{\pi_3^*} \ldots S_{\pi_n^*}\ 00\ldots0$$

The zeros are known as *external padding*. Modification of the LS code by the insertion of a small number of additional zeros (known as *internal padding*) is sometimes advantageous [4], but the total number of zeros should be small compared to the length of the code. With an $n \times n$ Hadamard matrix there are $2n$ codewords. The Golay pairs lead to zero aperiodic correlations for $0 < |\tau| < N$. For $\tau = 0$ the orthogonality of the rows of the Hadamard matrix guarantees zero aperiodic cross correlations. The reader is referred to [1,4,6,7] for more extensive treatments of the construction.

Sets of Hadamard matrices satisfying Definition 1 have been used in [7] to increase the number of codewords in LS codes. A full description of this generalized construction of LS codes and the way that the number of codewords can be increased can be found in [7]. Here the sets of Hadamard matrices are used for a different purpose; they are used to create many distinct generations of the code to enhance security.

LS codes have good interference properties, but at first sight it might appear that their relatively simple structure will lead to the possibility of spreading codewords being determined easily by observation, and therefore to the loss of some of the advantages of a CDMA system in terms of resistance to jamming and eavesdropping. This can be overcome by evolving the code. In any single generation users are assigned spreading codewords from a single new LS code, where the aperiodic correlation between spreading codewords assigned to users in different generations must be small. The evolution takes place by frequently changing one or more of the components in the construction of the LS code, i.e., the cross-complementary sequence pairs, the arrangement of zeros and the Hadamard matrix. If the condition on the aperiodic correlation is satisfied, an observer cannot use one generation of the code to predict another, and also cannot determine a spreading codeword in use by observation until it is too late to exploit it. An extensive study of ways to vary the construction is given in [9]. It is shown that many different variations of the code can be constructed with the required correlation property. If the change of Hadamard matrix alone is to lead to the correlation property being satisfied, it is necessary that the set of Hadamard matrices used is correlation constrained. However, one security concern remains. For the code to retain its zero correlation zone (and therefore its resistance to interference), it is necessary that in any single generation all users must be assigned the same arrangements of cross-complementary sequence pairs and the same arrangement of zeros in the padding. Only the actual Hadamard matrix row is specific to a user. Suppose that one radio transceiver and all the details of the code evolution relevant to the transceiver is obtained by a third party. It is important that this does not give information about the Hadamard matrix rows assigned to all other users, even if the third party has learned by observation of all the Hadamard matrix rows in use as the code evolves. If the partition of all Hadamard matrix rows in use into Hadamard matrices is unique (or is small enough for trial and error to be applied), the security concern is a real one. The third party can potentially put together all available information to reconstruct the spreading codewords of all users in each generation. On the other hand, if the partition of all

Hadamard matrix rows in use into Hadamard matrices is very large, no information about the spreading codewords of other users can be deduced. Thus it is important in this application to have good estimates of the number of Hadamard partitions possible.

Having explained the motivation in this section, the remainder of the paper will show that the partition is unique in the Kerdock code case and will develop lower bounds in the Gold code and Gold-like code cases.

3 Bent functions and almost bent functions

Bent and almost bent functions are $\{0, 1\}$ Boolean functions $f_i(x_1, x_2, \ldots, x_m)$ of $m\{0, 1\}$ Boolean variables. Arrange the set of all values of the vector $(x_1, x_2, \ldots, x_m)$ in binary order ranging from $(0, 0, 0, \ldots, 0)$ to $(1, 1, 1, \ldots, 1)$. These values index the columns of a matrix, and also define a vector $\hat{\boldsymbol{f}}_{\mathbf{i}} = (f_i(0, 0, \ldots, 0), \ldots, f_i(1, 1, \ldots, 1))$. The set of all Boolean functions of degree at most 1 gives a first-order Reed-Muller code in this way [3]. A $\{-1, +1\}$ function $\tilde{f}_i(x_1, x_2, \ldots, x_m) = (-1)^{f_i(x_1, x_2, \ldots, x_m)}$ can also be defined. Extending the mapping $g\colon x \mapsto (-1)^x$ to a mapping of vectors, $g(\hat{\boldsymbol{f}})$ is the vector obtained by mapping the component x_i of $\hat{\boldsymbol{f}}$ to $g(x_i)$. Thus g maps $\{0, 1\}$ vectors $\hat{\boldsymbol{f}}_{\mathbf{i}}$ to $\{-1, +1\}$ vectors, which for degree 1 functions form the rows of a Hadamard matrix H.

Definition 3 The Boolean function f_i of m variables is defined in [10] as bent (for m even) if the dot product between $g(\hat{\boldsymbol{f}}_i)$ and a row of H has magnitude $2^{m/2}$ and as almost bent (for m odd) if the magnitude of the dot product between $g(\hat{\boldsymbol{f}}_i)$ and a row of H is at most $2^{(m+1)/2}$.

Here the bent and almost bent functions used are second-order functions.

Definition 4 In a finite field $GF(2^m)$ the trace function $\mathrm{Tr}_m(x)\colon GF(2^m) \to GF(2)$ is defined by

$$\mathrm{Tr}_m(x) = \sum_{i=0}^{m-1} x^{2^i}.$$

The trace function is a linear function ($\mathrm{Tr}_m(\beta_1 + \beta_2) = \mathrm{Tr}_m(\beta_1) + \mathrm{Tr}_m(\beta_2)$ for $\beta_1, \beta_2 \in GF(2^m)$) and satisfies $\mathrm{Tr}_m(\beta^2) = \mathrm{Tr}_m(\beta)$ for all $\beta \in GF(2^m)$ [3]. It follows that $\mathrm{Tr}_m(\beta^{2^r}) = \mathrm{Tr}_m(\beta)$ for all r.

It is convenient to consider the correlation of vectors as

$$\textit{number of agreements} - \textit{number of disagreements}$$

taken over all positions, as this gives a uniform definition for correlation of codewords of $\{0, 1\}$ codes and dot products of rows of $\{+1, -1\}$ matrices.

4 The Kerdock code construction when the order of the Hadamard matrix is 2^m with m even

Let $\xi_2, \ldots, \xi_m$ be a basis for $GF(2^{m-1})$ and $x = \sum_{i=2}^{m} x_i \xi_i$ be an expression for an element $x \in GF(2^{m-1})$ in terms of this basis. Let α be a primitive element of $GF(2^{m-1})$. Let $\sigma_1(x) = \mathrm{Tr}_{m-1}(x)$ and $\sigma_2(x) = \sum_{i=1}^{(m-2)/2} \mathrm{Tr}_{m-1}(x^{1+2^i})$. Then, following [7,10], a bent function is defined for any $\gamma \in GF(2^{m-1})$ by

$$h_\gamma(x_1, x_2, \ldots, x_m) = x_1\sigma_1(\gamma x) + \sigma_2(\gamma x).$$

Theorem 1 [10] *Given the $2^m \times 2^m$ Hadamard matrix H obtained from first-order Boolean functions, the columns of H can be multiplied by the values of the $\{-1, +1\}$ functions $\tilde{h}_\gamma(x_1, x_2, \ldots, x_m) = (-1)^{h_\gamma(x_1, x_2, \ldots, x_m)}$ ($\gamma \in GF(2^{m-1})$) to obtain a set of 2^{m-1} Hadamard matrices $\{H_i\}$, with the dot product of rows of distinct matrices having magnitude $2^{m/2}$.*

Let the matrices $\{H_i\}$ be indexed by $i \in \{0, \ldots, 2^{m-1} - 1\}$ and the rows of each matrix H_i be indexed by $j \in \{0, \ldots, 2^m - 1\}$. Let Q be a $2^{2m-1} \times 2^{2m-1}$ matrix with dot products of Hadamard matrix rows as elements, with the rows and columns of Q indexed by $i \times 2^m + j$. Then the Hadamard matrix property shows that Q has diagonal blocks $2^m I_{2^m}$ and the known distance distribution of a Kerdock code [3] shows that all entries in the off diagonal blocks are $\pm 2^{m/2}$. It follows that the partition of the set of all rows of the Hadamard matrices $\{H_i\}$ into Hadamard matrices is unique.

5 Construction using a Gold code in the case of *m* odd

Choose an integer r with m, r relatively prime. Let $x = \sum_{i=1}^{m} x_i\xi_i$ be an expression for an element $x \in GF(2^m)$ in terms of a basis $\xi_1, \ldots, \xi_m$. Let α be a primitive element of $GF(2^m)$. In the example below $\xi_1 = 1$, $\xi_2 = \alpha, \ldots, \xi_m = \alpha^{m-1}$. Then an *almost bent* function is defined in [7] for any $\gamma \in GF(2^m)$ by

$$h_\gamma(x_1, x_2, \ldots, x_m) = \mathrm{Tr}_m\left(\gamma(x_1\xi_1 + x_2\xi_2 + x_3\xi_3 + \cdots + x_m\xi_m)^{1+2^r}\right) \tag{1}$$

Here the nonzero vectors $(x_1, x_2, \ldots, x_m)$ are arranged in binary order. If instead they were arranged as the representation (in terms of the basis) of powers of α, the expression (1) would give a decimated maximal length sequence, as used in the construction of Gold codes. The extra position $(x_1, x_2, \ldots, x_m) = (0, 0, \ldots, 0)$ is used to extend the Gold code. In a similar way, the functions given by $\mathrm{Tr}_m(\gamma(x_1\xi_1 + x_2\xi_2 + x_3\xi_3 + \cdots + x_m\xi_m))$ would generate a maximal length sequence code if this alternative order of positions were used.

It should be noted from Eq. 1 that (for odd m) the almost bent functions are linear functions on γ, i.e., $h_{\gamma_1} + h_{\gamma_2} = h_{\gamma_1+\gamma_2}$. For a Boolean variable x_i the notation $x_i + 1$ will be used for $x_i + 1 \bmod 2$.

If we take $m = 3$, $r = 2$, and construct the Galois field $GF(2^m)$ using the irreducible polynomial $\alpha^3 + \alpha + 1$, the almost bent functions can be computed and their properties determined.

$$\begin{array}{ll}
h_0 = 0 & \\
h_1 = x_2x_3 + x_3 + x_2 + x_1 & h_1(x_1, x_2, x_3) = h_1(x_1 + 1, x_2, x_3) + 1 \\
h_\alpha = x_1x_2 + x_1x_3 + x_2 & h_\alpha(x_1, x_2, x_3) = h_\alpha(x_1, x_2 + 1, x_3 + 1) + 1 \\
h_{\alpha^2} = x_2 + x_1x_3 + x_3 & h_{\alpha^2}(x_1, x_2, x_3) = h_{\alpha^2}(x_1, x_2 + 1, x_3) + 1 \\
h_{\alpha^3} = x_1x_3 + x_1x_2 + x_2x_3 + x_1 + x_3 & h_{\alpha^3}(x_1, x_2, x_3) = h_{\alpha^3}(x_1 + 1, x_2 + 1, x_3 + 1) + 1 \\
h_{\alpha^4} = x_3 + x_1x_2 & h_{\alpha^4}(x_1, x_2, x_3) = h_{\alpha^4}(x_1, x_2, x_3 + 1) + 1 \\
h_{\alpha^5} = x_1x_2 + x_2x_3 + x_2 + x_1 & h_{\alpha^5}(x_1, x_2, x_3) = h_{\alpha^5}(x_1 + 1, x_2, x_3 + 1) + 1 \\
h_{\alpha^6} = x_1 + x_2x_3 + x_1x_3 & h_{\alpha^6}(x_1, x_2, x_3) = h_{\alpha^6}(x_1 + 1, x_2 + 1, x_3) + 1
\end{array}$$

There are two alternative ways to consider the construction of the set of Hadamard matrices from these sets of almost bent functions. The first is to take the $2^m \times 2^m$ Hadamard matrix obtained from first-order Boolean functions and multiply the i th column of the matrix by

the value of $\tilde{h}_\gamma(x_1, x_2, \ldots, x_m)$ corresponding to that column. For each distinct choice of γ a new Hadamard matrix is obtained. The second way is to consider the subcode of the first-order Reed-Muller code S generated by the Boolean functions $x_1, x_2, \ldots, x_m$. The matrix with the codewords of this code as rows (in a certain order) is then the same as the above Hadamard matrix if each element is mapped to $+1$ or -1 by the mapping $g: x \mapsto (-1)^x$. The other Hadamard matrices are obtained in the same way from the cosets $S + \hat{\boldsymbol{h}}_\gamma$ for $\gamma \in \mathrm{GF}(2^m)$.

Theorem 2 [10] *The above construction gives 2^m Hadamard matrices with the dot product of rows of distinct matrices having magnitude at most $2^{(m+1)/2}$.*

Theorem 3 formalises the observed properties of the almost bent functions.

Theorem 3 *Let the expression:*

$$h_\gamma(x_1, x_2, \ldots, x_m) = \mathrm{Tr}_m\left(\gamma x^{1+2^r}\right) = \mathrm{Tr}_m\left(\gamma(x_1\xi_1 + x_2\xi_2 + x_3\xi_3 + \cdots + x_m\xi_m)^{1+2^r}\right)$$

be used to generate the almost bent functions. If $r = 2$ and $m \not\equiv 0 \bmod 4$ then for each nonzero γ in $GF(2^m)$ there exists a nonzero binary vector Δ such that $h_\gamma(\mathbf{x} + \Delta) = h_\gamma(\mathbf{x}) + \delta'$ with $\delta' \in \{0, 1\}$. If m is odd then $\delta' = 1$ and each nonzero value of Δ occurs for a distinct nonzero value of γ.

Proof Let $\Delta = (\delta_1, \delta_2, \ldots, \delta_m))$ and $\Lambda = \delta_1\xi_1 + \delta_2\xi_2 + \delta_3\xi_3 + \cdots + \delta_m\xi_m \in GF(2^m)$, so Δ is a representation of Λ in terms of the chosen basis. In a field of characteristic 2, $(x + y)^p = x^p + y^p$ when p is a power of 2, so $(x + y)^{1+2^r} = (x + y)(x^{2^r} + y^{2^r})$. Thus

$$\begin{aligned} h_\gamma(\mathbf{x} + \Delta) &= \mathrm{Tr}_m\left(\gamma(x + \Lambda)^{1+2^r}\right) = \mathrm{Tr}_m\left(\gamma(x^{1+2^r} + x^{2^r}\Lambda + x\Lambda^{2^r} + \Lambda^{1+2^r}\right) \\ &= \mathrm{Tr}_m\left(\gamma x^{1+2^r}\right) + \mathrm{Tr}_m\left(\gamma x^{2^r}\Lambda\right) + \mathrm{Tr}_m\left(\gamma x\Lambda^{2^r}\right) + \mathrm{Tr}_m\left(\gamma\Lambda^{1+2^r}\right). \end{aligned}$$

Recall that $\mathrm{Tr}_m(\beta^{2^r}) = \mathrm{Tr}_m(\beta)$ for all $\beta \in GF(2^m)$ and suppose $\gamma x^{2^r}\Lambda = (\gamma x\Lambda^{2^r})^{2^r}$, i.e., $1 = \gamma^{2^r-1}\Lambda^{2^{2r}-1}$. Then all but the first and last terms in the expression disappear and

$$h_\gamma(\mathbf{x} + \Delta) = h_\gamma(\mathbf{x}) + \delta' \text{ with } \delta' \in \{0, 1\}.$$

For $r = 2$, Λ can be determined from γ. It is required that $\gamma^{2^r-1} = \Lambda^{-(2^{2r}-1)}$. For $m \not\equiv 0 \bmod 4$, $2^m \equiv 2,\ 3,$ or $4 \bmod 5$ and there is a solution of $\gamma^3\Lambda^{15} = 1$ for each nonzero value of γ. There are three cases:

1. $2^m = 5t + 2$, $\gamma^{5t+1} = 1$ and $\Lambda = \gamma^t$ is a solution.
2. $2^m = 5t + 3$, $\gamma^{15t+6} = 1$ and $\Lambda = \gamma^{3t+1}$ is a solution.
3. $2^m = 5t + 4$, $\gamma^{10t+6} = 1$ and $\Lambda = \gamma^{2t+1}$ is a solution.

If m is odd then $2^m - 1 \not\equiv 0 \bmod 3$. Let $\Lambda = \alpha^j$ and $\gamma^3 = \Lambda^{-15} = \alpha^{i(2^m-1)} \times \alpha^{-15j}$. Thus $i = 0$ or i is divisible by 3 and the solution $\gamma = \Lambda^{-5}$ is unique. Thus each distinct vector Δ corresponds to a unique almost bent function h_γ. Also, $\delta' = \mathrm{Tr}_m(\gamma\Lambda^5) = \mathrm{Tr}_m(1)$. For m odd $\mathrm{Tr}_m(1) = 1$ so $\delta' = 1$. □

Although Δ is certainly unique for $m \leq 5$, it is conceivable that conditions other than $1 = \gamma^{2^r-1}\Lambda^{2^{2r}-1}$ could lead to different sets of vectors Δ with the property of the theorem for larger m. However this would simply lead to additional partitions, and the aim here is to derive lower bounds for the number of partitions.

5.1 Partitions into Hadamard matrices

Let S be the subcode of the first-order Reed-Muller code, generated by the linear Boolean functions $\phi_1(x_1, x_2, \ldots, x_m) = x_1, \phi_2(x_1, x_2, \ldots, x_m) = x_2, \ldots, \phi_m(x_1, x_2, \ldots, x_m) = x_m$ evaluated (using the vectors indexing the positions) to give codewords. Let $\hat{h}_\gamma$ be the codeword corresponding to the almost bent function h_γ, evaluated in the same way. The union of cosets $\cup_{\gamma \in \mathrm{GF}(2^m)}(S + \hat{h}_\gamma)$ of the $\{0, 1\}$ code then corresponds (using the mapping $g: x \mapsto (-1)^x$) to the initial partition into $\{+1, -1\}$ Hadamard matrices.

Now consider the two cosets $K' = S + \hat{h}_{\gamma_1}$ and $K'' = S + \hat{h}_{\gamma_2}$. From Eq. 1 and the linearity of the trace function, the bent functions are linear on γ and $h_{\gamma_1} + h_{\gamma_2} = h_{\gamma_3}$ where $\gamma_1 + \gamma_2 = \gamma_3$. Consider the vector $\Delta = (\delta_1, \delta_2, \ldots, \delta_m)$ corresponding to h_{ξ_3}. Let K_1 be the subcode of S generated by the linear Boolean functions $\sum_{i=1}^m \mu_i x_i$ which satisfy $\sum_{i=1}^m \delta_i \mu_i = 0$. Also, let K_2 be the coset of K_1 for which the functions satisfy $\sum_{i=1}^m \delta_i \mu_i = 1$. Then $S = K_1 \cup K_2$, $K' = (K_1 \cup K_2) + \hat{h}_{\gamma_1}$, $K'' = (K_1 \cup K_2) + \hat{h}_{\gamma_2}$ and the initial partition can be written $\cup_{\gamma \in \mathrm{GF}(2^m)}((K_1 \cup K_2) + \hat{h}_\gamma)$. Define also $S' = (K_1 \cup K_2) + \hat{h}_{\gamma_3}$.

Let $\mathbf{c}_1 \in S$, $\mathbf{c}_2 \in S'$, $\mathbf{c}_3 = \mathbf{c}_1 + \hat{h}_{\gamma_1} \in K'$, $\mathbf{c}_4 = \mathbf{c}_2 + \hat{h}_{\gamma_1} \in K''$. Denote by $A(\mathbf{c}_1, \mathbf{c}_2)$ the number of positions for which $\mathbf{c}_1$ and $\mathbf{c}_2$ agree and by $D(\mathbf{c}_1, \mathbf{c}_2)$ the number of positions for which $\mathbf{c}_1$ and $\mathbf{c}_2$ disagree. Note then that $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4$ satisfy $A(\mathbf{c}_1, \mathbf{c}_2) - D(\mathbf{c}_1, \mathbf{c}_2) = 0$ if and only if $A(\mathbf{c}_3, \mathbf{c}_4) - D(\mathbf{c}_3, \mathbf{c}_4) = 0$. Thus if it can be shown that S, S' lead to two different (sets of codewords which map to) Hadamard matrices then K', K'' lead to two different (sets of codewords which map to) Hadamard matrices. For each vector Δ create a partition $\{P, \bar{P}\}$ of the positions such that $(x_1, x_2, \ldots, x_m) \in P$ if and only if $(x_1+\delta_1, x_2+\delta_2, \ldots, x_m+\delta_m) \in \bar{P}$.

Starting from S and S' create two sets of codewords $L = K_1 \cup (K_1 + \hat{h}_{\gamma_3})$ and $L' = K_2 \cup (K_2 + \hat{h}_{\gamma_3})$. This will be referred to as a *switching* operation. Consider the first of these sets. For two codewords $\mathbf{c}$ and $\mathbf{c}'$ both in K_1 or both in $(K_1 + \hat{h}_{\gamma_3})$, $A(\mathbf{c}, \mathbf{c}') - D(\mathbf{c}, \mathbf{c}') = 0$ follows from the definition of S. Thus it is only necessary to consider $\mathbf{c} \in K_1$ and $\mathbf{c}' \in K_1 + \hat{h}_{\gamma_3}$. If $\mathbf{c} \in K_1$ corresponds to the function $\sum_{i=1}^m \mu_i x_i$ then $\sum_{i=1}^m \mu_i (x_i + \delta_i)$ has the same value as $\sum_{i=1}^m \mu_i x_i$. For $\mathbf{c}'$, $\sum_{i=1}^m \mu_i'(x_i + \delta_i) + h_{\gamma_3}(\mathbf{x} + \Delta) = \sum_{i=1}^m \mu_i' x_i + h_{\gamma_3}(\mathbf{x}) + 1$ follows from Theorem 3. Thus an agreement of these two codewords on a position within the set P gives a disagreement on the corresponding position of $\bar{P}$ and a disagreement on a position in P gives an agreement on the corresponding position of $\bar{P}$ as $h_{\gamma_3}(\mathbf{x}) = h_{\gamma_3}(\mathbf{x} + \Delta) + 1$. Considering all the positions of $P \cup \bar{P}$ it follows that $A(\mathbf{c}, \mathbf{c}') - D(\mathbf{c}, \mathbf{c}') = 0$. A similar argument deals with the case $L' = K_2 \cup (K_2 + \hat{h}_{\gamma_3})$. Thus L and L' both map to Hadamard matrices and in general $(K_1 + \hat{h}_{\gamma_1}) \cup (K_1 + \hat{h}_{\gamma_2})$ and $(K_2 + \hat{h}_{\gamma_1}) \cup (K_2 + \hat{h}_{\gamma_2})$ both map to Hadamard matrices.

Construct a complete graph G with 2^m vertices corresponding to cosets $(K_1 \cup K_2) + \hat{h}_\gamma$. Consider each (not necessarily perfect) matching of G, consisting of a set of edges for which no pair are incident with the same vertex. For such a matching, with between 1 and 2^{m-1} edges, a new partition into Hadamard matrices is obtained as indicated above. Each edge of the matching gives a pair of almost bent functions and from their sum an almost bent function corresponding to the edge is obtained. This almost bent function gives unique values of Δ and δ', which show how to split the cosets into halves and pair the halves. The number of partitions obtained by the above method is the number of matchings in G. There are

$$(2u-1)!! = (2u-1)(2u-3)(2u-5)\ldots 5.3.1 = \frac{(2u-1)!}{(u-1)!2^{u-1}}$$

perfect matchings in a complete graph K_{2u} with $2u$ vertices [2].

In general, for a complete graph with 2^m vertices containing a matching with u edges, we can select the vertices incident with edges of the matching in $\binom{2^m}{2u}$ ways. For the complete graph K_{2u} induced by these vertices, the perfect matching can be selected in $\frac{(2u-1)!}{(u-1)!2^{u-1}}$ ways. Thus the total number of partitions (including the original partition) obtained by the above method is

$$1+\sum_{u=1}^{2^{m-1}}\binom{2^m}{2u}\frac{(2u-1)!}{(u-1)!2^{u-1}}.$$

For $m=5$ this number is 22481059424730751232. Thus we have the following theorem.

Theorem 4 *If m is odd and $r=2$, the number of distinct partitions into Hadamard matrices obtained using the initial partition into Hadamard matrices given by the almost bent functions is at least*

$$1+\sum_{u=1}^{2^{m-1}}\binom{2^m}{2u}\frac{(2u-1)!}{(u-1)!2^{u-1}}.$$

Clique search has revealed another type of partition. Each Hadamard matrix in this type consists of exactly one row of each Hadamard matrix of the original partition. The way that such partitions arise will now be described.

Let $r=2$ and consider first the case $m=5$. For each $\gamma\in GF(2^m)$ the functions

$$H_\gamma(x_1,x_2,\ldots,x_m)=\mathrm{Tr}_m\left((\alpha^j\gamma+\alpha^{2j}\gamma^8)x\right)+h_\gamma(x_1,x_2,\ldots,x_m) \tag{2}$$

($j\in\{0,\ldots,2^m-2\}$), together with the function $H_\gamma(x_1,x_2,\ldots,x_m)=h_\gamma(x_1,x_2,\ldots,x_m)$, form a set of 2^m functions. For fixed j these functions $H_\gamma(x_1,x_2,\ldots,x_m)$ are linear on γ. By choosing distinct values of γ, one codeword $\hat{H}_\gamma(x_1,x_2,\ldots,x_m)$ is chosen from each coset of S, as the first term in (2) gives first-order Boolean functions. Linearity follows from $\gamma_1^{2^t}+\gamma_2^{2^t}=(\gamma_1+\gamma_2)^{2^t}$ and the linearity of the trace function [3]. If $H_\gamma(x_1,x_2,\ldots,x_m)=h_\gamma(x_1,x_2,\ldots,x_m)$ it has already been shown that for $\gamma\Lambda^5=1$, $H_\gamma(\mathbf{x}+\Delta)=H_\gamma(\mathbf{x})+1$. If $H_\gamma(x_1,x_2,\ldots,x_m)$ is as given in (2) then $H_\gamma(\mathbf{x}+\Delta)=H_\gamma(\mathbf{x})+\mathrm{Tr}_m((\alpha^j\gamma+\alpha^{2j}\gamma^8)\Lambda)+1$. But for $m=5$ the general condition $\gamma^6\Lambda^{30}=1$ implies $\Lambda=\gamma^6$ and so $\mathrm{Tr}_m((\alpha^j\gamma+\alpha^{2j}\gamma^8)\Lambda)=\mathrm{Tr}_m(\alpha^j\gamma^7)+\mathrm{Tr}_m(\alpha^{2j}\gamma^{14})=0$ as $\mathrm{Tr}_m(\beta)=\mathrm{Tr}_m(\beta^2)$ for all $\beta\in\mathrm{GF}(2^m)$. Thus $H_\gamma(\mathbf{x}+\Delta)=H_\gamma(\mathbf{x})+1$ in the general case. The result that

$$A(\hat{H}_{\gamma_1}(x_1,x_2,\ldots,x_m),\hat{H}_{\gamma_2}(x_1,x_2,\ldots,x_m))-D(\hat{H}_{\gamma_1}(x_1,x_2,\ldots,x_m),\hat{H}_{\gamma_2}(x_1,x_2,\ldots,x_m))$$

is zero follows in the same way as previously. Thus the set of codewords $\hat{H}_\gamma(x_1,x_2,\ldots,x_m)$ for $\gamma\in\mathrm{GF}(2^m)$ forms a subspace corresponding to a Hadamard matrix. This subspace and its cosets in the extended Gold code map to a new partition into Hadamard matrices, with exactly one row of each Hadamard matrix chosen from each of the original Hadamard matrices. In the case $m=5$, $r=2$ there are 2^m such subspaces and therefore 2^m such Hadamard matrix partitions. Thus for $m=5$ the number of partitions counted becomes

$$1+\sum_{u=1}^{2^{m-1}}\binom{2^m}{2u}\frac{(2u-1)!}{(u-1)!2^{u-1}}+2^m. \tag{3}$$

In the case $m = 5$ the 31 values $\{0, 1, \ldots, 30\}$ for j together with the case given by $H_\gamma(\mathbf{x}) = h_\gamma(\mathbf{x})$ explain precisely the 32 cases of the "one row of each Hadamard matrix" type observed by clique search. However, the precise structure may be different for different (odd) values of m. Pairs of values of $\gamma^{2^i}\Lambda$, $\gamma^{2^k}\Lambda$ are required in the same cyclotomic coset (i.e., so that $\gamma^{2^k}\Lambda = (\gamma^{2^i}\Lambda)^{2^t}$).

5.1.1 The case (m=3)

Here $\gamma^7 = \Lambda^7 = 1$ and so $\gamma\Lambda^5 = 1$ implies $\Lambda = \gamma^4$. The cyclotomic cosets are:

$$\gamma^l\Lambda \in \{\gamma, \gamma^2, \gamma^4\} \text{ so } \gamma^l \in \{\gamma^4, \gamma^5, 1\}$$
$$\gamma^l\Lambda \in \{\gamma^5, \gamma^3, \gamma^6\} \text{ so } \gamma^l \in \{\gamma, \gamma^6, \gamma^2\}.$$

Thus the only possibility which gives the necessary linearity is to use γ^2 and γ for γ^l (corresponding to the second cyclotomic coset). Note that the choice γ and γ^2 gives the same result. If the zero function is included, this gives a set of 2^m functions

$$\mathrm{Tr}_m\left((\alpha^j\gamma^2 + \alpha^{2j}\gamma)x\right)$$

giving $H_\gamma(x_1, x_2, \ldots, x_m) = h_\gamma(x_1, x_2, \ldots, x_m)$ and

$$H_\gamma(x_1, x_2, \ldots, x_m) = \mathrm{Tr}_m\left((\alpha^j\gamma^2 + \alpha^{2j}\gamma)x\right) + h_\gamma(x_1, x_2, \ldots, x_m) \tag{4}$$

and the number of partitions obtained is again given by (3).

5.1.2 The case m = 5 (to check completeness)

Here $\gamma^{31} = \Lambda^{31} = 1$ and so $\gamma\Lambda^5 = 1$ implies $\Lambda = \gamma^6$. The cyclotomic cosets are:

$$\gamma^l\Lambda \in \{\gamma^7, \gamma^{14}, \gamma^{28}, \gamma^{25}, \gamma^{19}\}; \quad \gamma^l \in \{\gamma, \gamma^8, \gamma^{22}, \gamma^{19}, \gamma^{13}\}$$
$$\gamma^l\Lambda \in \{\gamma^8, \gamma^{16}, \gamma, \gamma^2, \gamma^4\}; \quad \gamma^l \in \{\gamma^2, \gamma^{10}, \gamma^{26}, \gamma^{27}, \gamma^{29}\}$$
$$\gamma^l\Lambda \in \{\gamma^9, \gamma^{18}, \gamma^5, \gamma^{10}, \gamma^{20}\}; \quad \gamma^l \in \{\gamma^3, \gamma^{12}, \gamma^{30}, \gamma^4, \gamma^{14}\}$$
$$\gamma^l\Lambda \in \{\gamma^{11}, \gamma^{22}, \gamma^{13}, \gamma^{26}, \gamma^{21}\}; \quad \gamma^l \in \{\gamma^5, \gamma^{16}, \gamma^7, \gamma^{20}, \gamma^{15}\}$$
$$\gamma^l\Lambda \in \{\gamma^{12}, \gamma^{24}, \gamma^{17}, \gamma^3, \gamma^6\}; \quad \gamma^l \in \{\gamma^6, \gamma^{18}, \gamma^{11}, \gamma^{28}, 1\}$$
$$\gamma^l\Lambda \in \{\gamma^{15}, \gamma^{30}, \gamma^{29}, \gamma^{27}, \gamma^{23}\}; \quad \gamma^l \in \{\gamma^9, \gamma^{24}, \gamma^{23}, \gamma^{21}, \gamma^{17}\}$$

It can be seen that the use of γ and γ^8 for γ^l (as in 2) is the only possibility.

5.1.3 The case $m = 7$

Here $\gamma^{127} = \Lambda^{127} = 1$ and so $\gamma\Lambda^5 = 1$ implies $\Lambda = \gamma^{76}$. The cyclotomic cosets are:

$$\begin{aligned}
\gamma^l\Lambda &\in \{\gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^{16}, \gamma^{32}, \gamma^{64}\}; \quad \gamma^l \in \{\gamma^{52}, \gamma^{53}, \gamma^{55}, \gamma^{59}, \gamma^{67}, \gamma^{83}, \gamma^{115}\}\\
\gamma^l\Lambda &\in \{\gamma^9, \gamma^{18}, \gamma^{36}, \gamma^{72}, \gamma^{17}, \gamma^{34}, \gamma^{68}\}; \quad \gamma^l \in \{\gamma^{60}, \gamma^{69}, \gamma^{87}, \gamma^{123}, \gamma^{68}, \gamma^{85}, \gamma^{119}\}\\
\gamma^l\Lambda &\in \{\gamma^{77}, \gamma^{27}, \gamma^{54}, \gamma^{108}, \gamma^{89}, \gamma^{51}, \gamma^{102}\}; \quad \gamma^l \in \{\gamma, \gamma^{78}, \gamma^{105}, \gamma^{32}, \gamma^{13}, \gamma^{102}, \gamma^{26}\}\\
\gamma^l\Lambda &\in \{\gamma^{78}, \gamma^{29}, \gamma^{58}, \gamma^{116}, \gamma^{105}, \gamma^{83}, \gamma^{39}\}; \quad \gamma^l \in \{\gamma^2, \gamma^{80}, \gamma^{109}, \gamma^{40}, \gamma^{29}, \gamma^7, \gamma^{90}\}\\
\gamma^l\Lambda &\in \{\gamma^{79}, \gamma^{31}, \gamma^{62}, \gamma^{124}, \gamma^{121}, \gamma^{115}, \gamma^{103}\}; \quad \gamma^l \in \{\gamma^3, \gamma^{82}, \gamma^{113}, \gamma^{48}, \gamma^{45}, \gamma^{39}, \gamma^{27}\}\\
\gamma^l\Lambda &\in \{\gamma^{80}, \gamma^{33}, \gamma^{66}, \gamma^5, \gamma^{10}, \gamma^{20}, \gamma^{40}\}; \quad \gamma^l \in \{\gamma^4, \gamma^{84}, \gamma^{117}, \gamma^{56}, \gamma^{61}, \gamma^{71}, \gamma^{91}\}\\
\gamma^l\Lambda &\in \{\gamma^{81}, \gamma^{35}, \gamma^{70}, \gamma^{13}, \gamma^{26}, \gamma^{52}, \gamma^{104}\}; \quad \gamma^l \in \{\gamma^5, \gamma^{86}, \gamma^{121}, \gamma^{64}, \gamma^{77}, \gamma^{103}, \gamma^{28}\}\\
\gamma^l\Lambda &\in \{\gamma^{82}, \gamma^{37}, \gamma^{74}, \gamma^{21}, \gamma^{42}, \gamma^{84}, \gamma^{41}\}; \quad \gamma^l \in \{\gamma^6, \gamma^{88}, \gamma^{125}, \gamma^{72}, \gamma^{93}, \gamma^8, \gamma^{92}\}\\
\gamma^l\Lambda &\in \{\gamma^{85}, \gamma^{43}, \gamma^{86}, \gamma^{45}, \gamma^{90}, \gamma^{53}, \gamma^{106}\}; \quad \gamma^l \in \{\gamma^9, \gamma^{94}, \gamma^{10}, \gamma^{96}, \gamma^{14}, \gamma^{104}, \gamma^{30}\}\\
\gamma^l\Lambda &\in \{\gamma^{87}, \gamma^{47}, \gamma^{94}, \gamma^{61}, \gamma^{122}, \gamma^{117}, \gamma^{107}\}; \quad \gamma^l \in \{\gamma^{11}, \gamma^{98}, \gamma^{18}, \gamma^{112}, \gamma^{46}, \gamma^{41}, \gamma^{31}\}\\
\gamma^l\Lambda &\in \{\gamma^{88}, \gamma^{49}, \gamma^{98}, \gamma^{69}, \gamma^{11}, \gamma^{22}, \gamma^{44}\}; \quad \gamma^l \in \{\gamma^{12}, \gamma^{100}, \gamma^{22}, \gamma^{120}, \gamma^{62}, \gamma^{73}, \gamma^{95}\}\\
\gamma^l\Lambda &\in \{\gamma^{91}, \gamma^{55}, \gamma^{110}, \gamma^{93}, \gamma^{59}, \gamma^{118}, \gamma^{109}\}; \quad \gamma^l \in \{\gamma^{15}, \gamma^{106}, \gamma^{34}, \gamma^{17}, \gamma^{110}, \gamma^{42}, \gamma^{33}\}\\
\gamma^l\Lambda &\in \{\gamma^{95}, \gamma^{63}, \gamma^{126}, \gamma^{125}, \gamma^{123}, \gamma^{119}, \gamma^{111}\}; \quad \gamma^l \in \{\gamma^{19}, \gamma^{114}, \gamma^{50}, \gamma^{49}, \gamma^{47}, \gamma^{43}, \gamma^{35}\}\\
\gamma^l\Lambda &\in \{\gamma^{96}, \gamma^{65}, \gamma^3, \gamma^6, \gamma^{12}, \gamma^{24}, \gamma^{48}\}; \quad \gamma^l \in \{\gamma^{20}, \gamma^{116}, \gamma^{54}, \gamma^{57}, \gamma^{63}, \gamma^{75}, \gamma^{99}\}\\
\gamma^l\Lambda &\in \{\gamma^{97}, \gamma^{67}, \gamma^7, \gamma^{14}, \gamma^{28}, \gamma^{56}, \gamma^{112}\}; \quad \gamma^l \in \{\gamma^{21}, \gamma^{118}, \gamma^{58}, \gamma^{65}, \gamma^{79}, \gamma^{107}, \gamma^{36}\}\\
\gamma^l\Lambda &\in \{\gamma^{99}, \gamma^{71}, \gamma^{15}, \gamma^{30}, \gamma^{60}, \gamma^{120}, \gamma^{113}\}; \quad \gamma^l \in \{\gamma^{23}, \gamma^{122}, \gamma^{66}, \gamma^{81}, \gamma^{111}, \gamma^{44}, \gamma^{37}\}\\
\gamma^l\Lambda &\in \{\gamma^{100}, \gamma^{73}, \gamma^{19}, \gamma^{38}, \gamma^{76}, \gamma^{25}, \gamma^{50}\}; \quad \gamma^l \in \{\gamma^{24}, \gamma^{124}, \gamma^{70}, \gamma^{89}, 1, \gamma^{76}, \gamma^{101}\}\\
\gamma^l\Lambda &\in \{\gamma^{101}, \gamma^{75}, \gamma^{23}, \gamma^{46}, \gamma^{92}, \gamma^{57}, \gamma^{114}\}; \quad \gamma^l \in \{\gamma^{25}, \gamma^{126}, \gamma^{74}, \gamma^{97}, \gamma^{16}, \gamma^{108}, \gamma^{38}\}
\end{aligned}$$

Thus the only possibility is to use γ and γ^{32} for γ^l (corresponding to the third cyclotomic coset). This gives a set of 2^m functions for each γ, consisting of $h_\gamma(x_1, x_2, \ldots, x_m)$ and (for the $2^m - 1$ choices of j)

$$H_\gamma(x_1, x_2, \ldots, x_m) = \mathrm{Tr}_m\left((\alpha^j\gamma + \alpha^{8j}\gamma^{32})x\right) + h_\gamma(x_1, x_2, \ldots, x_m) \tag{5}$$

and again the number of partitions is counted by (2).

It is unclear whether there will always be an appropriate choice of γ^{2^i} and γ^{2^k} for odd $m \geq 9$, or whether there may be more than one choice.

Theorem 5 *If $r = 2$ and m is 3, 5 or 7 then the number of distinct partitions into Hadamard matrices obtained using the initial partition into Hadamard matrices given by the almost bent functions is at least*

$$1 + \sum_{u=1}^{2^{m-1}} \binom{2^m}{2u} \frac{(2u-1)!}{(u-1)!2^{u-1}} + 2^m.$$

Of course there could be other partitions into Hadamard matrices obtained by less regular methods, but clique searches have not revealed any. Thus it can be conjectured:

Conjecture 1 *The inequality of Theorem 5 is an equality.*

Conjecture 2 *If the study of cyclotomic cosets gives exactly W distinct cases, then the number of distinct partitions into Hadamard matrices is exactly*

$$1 + \sum_{u=1}^{2^{m-1}} \binom{2^m}{2u} \frac{(2u-1)!}{(u-1)!2^{u-1}} + W \times 2^m.$$

6 The case of $m \equiv 2 \bmod 4$

Gold codes exist whenever m is odd or $m \equiv 2 \bmod 4$ [5]. In the case $m \equiv 2 \bmod 4$ there are still 2^m second-order Boolean functions constructed using

$$h_\gamma(x_1, x_2, \ldots, x_m) = \mathrm{Tr}_m\left(\gamma x^5\right) \tag{6}$$

but the maximum modulus of the dot product is $2^{(m+2)/2}$ [5], so they can no longer be referred to as almost bent functions. The correlation is double that for a Kerdock code (for which it is $2^{m/2}$), but the number of partitions will be shown to be large. The analysis is similar to that in Sect. 5 with two exceptions. Firstly, the solutions for Λ are not unique. As $2^m - 1 \equiv 0 \bmod 3$ the field has cube roots of unity 1, $\omega = \alpha^{(2^m-1)/3}$, $\omega^2 = \alpha^{2(2^m-1)/3}$, and $\gamma^3\Lambda^{15} = 1$ has solutions $\gamma = \Lambda^{-5}$, $\gamma = \omega\Lambda^{-5}$ and $\gamma = \omega^2\Lambda^{-5}$. Similarly, for each solution $\Lambda^{(1)}$ there are two further solutions $\Lambda^{(2)} = \omega\Lambda^{(1)}$ and $\Lambda^{(3)} = \omega^2\Lambda^{(1)}$. Thus three vectors Δ exist for each nonzero value of γ, which allow switching to take place. In fact it will be seen below that there are 7 switchings for each edge of the graph. Secondly, it can be observed that $\delta' = 0$ for $\gamma = (\Lambda^{(1)})^{-5}$ as $\mathrm{Tr}_m(1) = 0$ for m even, whereas $\delta' = 1$ for the other two solutions as $\mathrm{Tr}_m(\omega) = \mathrm{Tr}_m(\omega^2) = 1$. When $\delta' = 0$ for particular values of γ and Λ it is necessary in Sect. 5.1 to replace $L = K_1 \cup (K_1 + \hat{h}_{\gamma_3})$ and $L' = K_2 \cup (K_2 + \hat{h}_{\gamma_3})$ by $L = K_1 \cup (K_2 + \hat{h}_{\gamma_3})$ and $L' = K_2 \cup (K_1 + \hat{h}_{\gamma_3})$. With this change, agreements on P will still correspond to disagreements on the corresponding value of $\bar{P}$ (and vice versa) and the argument works as before. The argument used to generate a partition into Hadamard matrices with each Hadamard matrix consisting of exactly one row of each Hadamard matrix of the original partition no longer works when $\delta' = 0$ for some values of γ. However, the subcode given by vectors $\hat{h}_\gamma$ is an (extended) 5th decimation of an m-sequence and so is an (extended) m-sequence [5]. Thus it and its cosets in the (extended) Gold code correspond to a partition into Hadamard matrices.

As a result of the non-uniqueness of the solutions for Λ there is more than one switching for each function $h_\gamma(x_1, x_2, \ldots, x_m)$. The three solutions for Λ give three vectors $\Delta^{(1)}$, $\Delta^{(2)}$ and $\Delta^{(3)}$, with $\Delta^{(1)} + \Delta^{(2)} + \Delta^{(3)} = 0$ as $1 + \omega + \omega^2 = 0$. Replace K_1 by the subcode A for which the Boolean functions satisfy $\sum_{i=1}^m \delta_i^{(1)}\mu_i = 0$ and $\sum_{i=1}^m \delta_i^{(2)}\mu_i = 0$. Let the cosets of A in S be B, C and D (where $A \cup C$ corresponds to K_1 for $\Delta^{(1)}$ and $A \cup B$ corresponds to K_1 for $\Delta^{(2)}$). There are then three switchings of $\{A, B, C, D\}, \{A+\hat{h}_\gamma, B+\hat{h}_\gamma, C+\hat{h}_\gamma, D+\hat{h}_\gamma\}$ of the form

1. $\{A, B + \hat{h}_\gamma, C, D + \hat{h}_\gamma\}, \{A + \hat{h}_\gamma, B, C + \hat{h}_\gamma, D\}$;
2. $\{A, B, A + \hat{h}_\gamma, B + \hat{h}_\gamma\}, \{C + \hat{h}_\gamma, D + \hat{h}_\gamma, C, D\}$;
3. $\{A, A + \hat{h}_\gamma, D, D + \hat{h}_\gamma\}, \{B, B + \hat{h}_\gamma, C, C + \hat{h}_\gamma\}$.

There are also four switchings of the form

1. $\{A, C, D, D + \hat{h}_\gamma\}, \{A + \hat{h}_\gamma, B, B + \hat{h}_\gamma, C + \hat{h}_\gamma\}$;
2. $\{A, A + \hat{h}_\gamma, B, D\}, \{B + \hat{h}_\gamma, C, C + \hat{h}_\gamma, D + \hat{h}_\gamma\}$;

3. $\{B, C, C + \hat{h}_\gamma, D\}, \{A, A + \hat{h}_\gamma, B + \hat{h}_\gamma, D + \hat{h}_\gamma\}$;
4. $\{A, B, B + \hat{h}_\gamma, C\}, \{A + \hat{h}_\gamma, C + \hat{h}_\gamma, D, D + \hat{h}_\gamma\}$.

with $3 \times 2^{m-2}$ rows of one Hadamard matrix and 2^{m-2} rows of the second Hadamard matrix. Thus there are 7 switchings in total for each edge. Then the lower bound is:

$$1 + \sum_{u=1}^{2^{m-1}} \binom{2^m}{2u} \frac{(2u-1)!}{(u-1)!2^{u-1}} 7^u + 1. \tag{7}$$

Conjecture 3 *In the case* $m \equiv 2 \bmod 4$ *the number of Hadamard partitions is given exactly by expression* (7).

7 The case of $m \equiv 0 \bmod 4$

A Kerdock code again exists if $m \equiv 0 \bmod 4$, but no Gold code exists. Whereas a Kerdock code leads to a unique partition, a code with similar properties to a Gold code could allow large numbers of partitions. Candidates include the Gold-like codes described in [5]. These are again constructed from a maximal length sequence and a qth decimation of a maximal length sequence and it is required that $\gcd(q, 2^m - 1) = 3$. Note that in this case $2^m - 1 \equiv 0 \mod 3$ and $\gcd(1 + 2^{\lfloor (m+2)/2 \rfloor}, 2^m - 1) = 3$. Then the second-order Boolean functions are obtained as:

$$h_\gamma(x_1, x_2, \ldots, x_m) = \mathrm{Tr}_m\left(\gamma x^{1+2^{\lfloor (m+2)/2 \rfloor}}\right). \tag{8}$$

Theorem 6 [5] *The above construction gives* 2^m *second-order Boolean functions leading to* 2^m *Hadamard matrices, with the dot product of rows of distinct matrices having values* 0, $-2^{\lfloor (m+2)/2 \rfloor}$, $2^{\lfloor (m+2)/2 \rfloor}$, $2^{m/2}$, $-2^{m/2}$.

Following Sect. 5, the equation $\gamma^{2^r-1}\Lambda^{(2^{2r}-1)} = 1$ (with $r = \lfloor (m+2)/2 \rfloor$) simplifies in this case to $\gamma^{2^r-1}\Lambda^3 = 1$ with $\gcd(2^r - 1, 2^m - 1) = 1$. It can be observed that solutions $\Lambda^{(1)}$, $\Lambda^{(2)} = \omega\Lambda^{(1)}$ and $\Lambda^{(3)} = \omega^2\Lambda^{(1)}$, exist if and only if γ is of the form α^{3j} for a primitive element α of the field. As $\mathrm{Tr}_m(\gamma\Lambda^{1+2^r}) = \mathrm{Tr}_m(1) = 0$, $\delta' = 0$ for all switchings and it is necessary in Sect. 5.1 to replace $L = K_1 \cup (K_1 + \hat{h}_{\gamma_3})$ and $L' = K_2 \cup (K_2 + \hat{h}_{\gamma_3})$ by $L = K_1 \cup (K_2 + \hat{h}_{\gamma_3})$ and $L' = K_2 \cup (K_1 + \hat{h}_{\gamma 3})$. The same graph can be constructed as in the previous cases, but only one third of the edges (those corresponding to functions $h_{\alpha^{3i}}(x_1, x_2, \ldots, x_m)$) allow switching and can be included in the matching. It appears that there is no partition with matrices consisting of one row from each matrix in this case. It is hard to envisage a single formula for the number of matchings but they could be counted in individual cases. Again as in the $m \equiv 2 \bmod 4$ case there are three vectors $\Delta^{(1)}$, $\Delta^{(2)}$ and $\Delta^{(3)}$, with $\Delta^{(1)} + \Delta^{(2)} + \Delta^{(3)} = 0$, although now for each value of Λ the value of γ is unique and $\delta' = 0$. Thus for each edge that allows switching (corresponding to a solution for γ) there are 3 switchings of $\{A, B, C, D\}, \{A + \hat{h}_\gamma, B + \hat{h}_\gamma, C + \hat{h}_\gamma, D + \hat{h}_\gamma\}$ of the form $\{A, B, C + \hat{h}_\gamma, D + \hat{h}_\gamma\}, \{A + \hat{h}_\gamma, B + \hat{h}_\gamma, C, D\}$ and 4 switchings of the form $\{A, B, C, D + \hat{h}_\gamma\}, \{A + \hat{h}_\gamma, B + \hat{h}_\gamma, C + \hat{h}_\gamma, D\}$ with $3 \times 2^{m-2}$ rows of one Hadamard matrix and 2^{m-2} rows of the second Hadamard matrix. This gives 7 switchings for each edge for which switchings are possible.

Conjecture 4 *In the case* $m \equiv 0 \bmod 4$ *the only Hadamard partitions that arise are those identified in this section.*

8 Conclusion

The motivation for the study of the number of Hadamard partitions has been explained in Sect. 2. In Sect. 4 it has been shown that the initial partition is unique for the Kerdock code construction, which is therefore unsatisfactory from the perspective of Sect. 2. In the remainder of the paper lower bounds have been developed for the Gold and Gold-like constructions. These lower bounds explain the partitions observed by computer search, and it has been conjectured that the bounds are tight. The number of partitions is certainly very large in these cases.

Acknowledgments R.P. Ward was supported by EPSRC and BAE SYSTEMS under a CASE award. The authors are grateful to G. Wyman and R.A. Jones for many helpful discussions.

References

1. Fan P.Z.: Spreading sequence design and theoretical limits for quasisynchronous CDMA systems. EURASIP J. Wireless Commun. Networking **1**, 19–31 (2004).
2. Godsil C.D.: Algebraic Combinatorics. Chapman and Hall, New York (1993).
3. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam, The Netherlands (1977).
4. Sanusi S.O.: Assignment of spreading codes in code division multiple access radio systems. PhD thesis, University of Glamorgan (2006).
5. Sarwate D.V., Pursley M.B.: Crosscorrelation properties of pseudorandom sequences. Proc. IEEE **68**(5), 593–619 (1980).
6. Stańczak S., Boche H., Haardt M.: Are LAS codes a miracle? In: 2001 IEEE Global Communications Conference (GLOBECOM), BWS05-4, San Antonio, TX, USA (November 25–29), pp. 589–593 (2001).
7. Tang X., Mow W.H.: Design of spreading codes for quasi-synchronous CDMA with intercell interference. IEEE J. Select. Area Commun. **24**(1), 84–93 (2006).
8. Tseng C.C., Liu C.L.: Complementary sets of sequences. IEEE Trans. Inf. Theory **18**(5), 644–652 (1972).
9. Ward R.P.: Evolution of loosely synchronized spreading codes in code-division multiple-access systems. PhD thesis, University of Glamorgan (2008).
10. Yang K., Kim Y.-K., Kumar P.V.: Quasi-orthogonal sequences for code-division multiple-access systems. IEEE Trans. Inf. Theory **46**(3), 982–993 (2000).