The covering radius of Hadamard codes in odd graphs

Patrick Solé

CNRS, INS, 250, rue Albert Einstein, bâtiment 4, 06 560 Valbonne, France

Arif Ghafoor

Department of Electrical and Computer Engineering, Syracuse University, Syracuse, NY 13244-1240, USA

Sohail A. Sheikh

Department of Electrical Engineering, Widener University, Chester, PA 19013, USA

Received 9 June 1989
Revised 22 January 1990

Abstract


The use of odd graphs has been proposed as fault-tolerant interconnection networks. The following problem originated in their design: what is the graphical covering radius of an Hadamard code of length $2k-1$ and size $2k-1$ in the odd graph $O_k$? Of particular interest is the case of $k = 2^m - 1$, where we can choose this Hadamard code to be a subcode of the punctured first order Reed-Muller code $RM(1, m)$. We define the $w$-covering radius of a binary code as the largest Hamming distance from a binary word of Hamming weight $w$ to the code. The above problem amounts to finding the $k$-covering radius of a $(2k, 4k, k-1)$ Hadamard code. We find upper and lower bounds on this integer, and determine it for small values of $k$. Our study suggests a new isomorphism test for Hadamard designs.

Keywords. Interconnection networks, coding theory, covering radius, odd graphs, Hadamard matrices, Hadamard designs, first order Reed-Muller code, coset weight distribution.

1. Introduction

A number of considerations must be taken into account while designing interconnection networks for multiprocessor systems. One such important consideration is the capability of the interconnection network for future expansion. An interconnection network can be modelled as a finite, simple, undirected graph, $\Gamma$, where vertices
represent nodes of the network, and the edges the physical links between the nodes. Suppose we want to expand the network \( \Gamma \) by interconnecting several of its copies. There are two extreme ways of interconnecting the copies:

- connect every node in a copy to all its images belonging to the rest of the copies,
- connect one node in each copy to all its images.

The first solution is costly since it requires many links, while the second is very fragile: if one particular node in one particular copy fails, then the whole network is disconnected. A middle way between these two extremes is to use a semidistributed approach by selecting a set of centers in \( \Gamma \) which can cover each copy of \( \Gamma \) by spheres for the graphical distance, and interconnect these centers of the spheres in some desired fashion. The centers in a given copy of \( \Gamma \) can act as gateway nodes, to handle message traffic going in and out of that copy of the network. In any case the parameter of interest in the choice of the centers is the radius of the spheres, as it affects the overall diameter of the expanded network. We are thus led to a covering problem in the graph \( \Gamma \). From the preceding discussion, it can be noted that the number of centers cannot be less than the connectivity of \( \Gamma \), without decreasing the fault-tolerance capability of the network.

2. The odd graphs

In this paper we take \( \Gamma \) to be the odd graph \( O_k \) [15]. The study of odd graphs in this paper is motivated by the fact that these graphs have been proposed as interconnection networks and have been shown to possess a number of interesting features such as high degree of fault-tolerance, low complexity for routing message etc. [1, 13]. An odd graph is constructed using binary vectors with constant Hamming weight. A weight of a binary vector \( x \) of \( F_2^k \) is the number of its nonzero coordinates and is denoted by \( w(x) \). The Hamming distance of two vectors \( x, y \) is the weight of their difference and is denoted by \( d(x, y) \). The odd graph \( O_k \) has for vertex set the binary words of length \( 2k - 1 \) and Hamming weight \( k - 1 \). Two vertices are connected if and only if they have disjoint support or, equivalently, if they are at Hamming distance \( 2k - 2 \). The graph \( O_3 \) is the celebrated Petersen graph [9]. Odd graphs are selected due to their higher density than various other interconnection networks: they have degree \( k \), diameter \( k - 1 \), and \( \binom{2k - 1}{k - 1} \) nodes [9]. Specifically, the following holds:

**Lemma 2.1.** The degree and the diameter of \( O_k \) are of asymptotic order \( \log(\sqrt{N}) \), where \( N = \binom{2k - 1}{k - 1} \) is the number of nodes in \( O_k \), and \( \log \) is binary.

**Proof.** We provide the proof by using the following classical Stirling approximation [17] to the binomial coefficient \( \binom{2k - 1}{k - 1} \), which counts the number of nodes, \( N \), as a function of the degree \( k \). Given

\[
N = \binom{X}{\lambda X},
\]
for a fixed $\lambda$ and very large $X$ (that is $X \to \infty$), we have

$$N = \binom{X}{\lambda X} \approx 2^{\frac{X^2}{2\lambda} / \sqrt{2\pi\lambda(1-\lambda)}}$$  \hspace{1cm} (1)

where $\theta$ is the binary entropy function whose asymptotic expansion of the functional inverse (for $x$ near zero) can be given as [17]:

$$\theta^{-1}(1-x) = \frac{1}{2} - 0.589\sqrt{x} + \cdots$$  \hspace{1cm} (2)

(We quote this result for future use; for now, we only need the value $\theta(\frac{1}{2}) = 1$.) Putting $X = 2k - 1$, $x = 0$, and $\lambda = \frac{1}{2}$, we get the desired result for the degree $k$, and the diameter $k - 1$.

As mentioned earlier, there is a number of reasons for selecting odd graphs as interconnection networks. For example, these graphs possess a higher density, which is given as $\log(N) / \text{diam} \log(\text{deg})$, where diam is the diameter of the network with $N$ nodes and maximum degree $\text{deg} + 1$. Note that, this quantity is always less than 1 by the Moore bound [6]. Intuitively, graphs with higher density are more desirable since they have more nodes for a given degree and diameter than graphs with a lower density.

It follows from Lemma 2.1 that $O_k$ has density asymptotically equal to $2 / \log(k)$, which is denser than many known interconnection networks such as mesh, and ring, [21], since their density asymptotically approaches $2 \log(N) / N$, and $\log(N) / 4\sqrt{N}$, respectively. Also, the chordal ring has density $\log(N) / \log(3)\sqrt{\tilde{N}}$ [2]. It is also denser than the binary hypercube graph [3] which, with both degree and diameter equal to $n$, has density asymptotically equal to $1 / \log(n)$.

Other important design considerations for an interconnection network include symmetry and the connectivity of the network. The latter property ensures fault-tolerance. It is known that edge transitive graphs have optimal edge and vertex connectivity [20]. But the graphs $O_k$ are distance transitive which is much stronger. By comparing odd graphs with the de Bruijn [6] graphs, we see that although the latter have $q^m$ nodes, diameter $m$, and degree $2q$, which results in a density of $(1 + (\log(q))^{-1})^{-1}$, a number close to 1 for large $q$, they are not distance regular, and not even vertex transitive.

Finally, for implementation reasons (space and time restrictions) both the degree and diameter should be reasonably small as compared to the number of nodes. This excludes for instance the complete graph which is both distance transitive and of density one.

The next lemma provides an important relationship between the Hamming distance and the graphical distance of two vertices in $O_k$ [12]. We recall that the graphical distance between two vertices of a finite connected graph is the length of a shortest path between these two vertices. This simple but crucial result is used in Sections 5 and 6, where the problem of finding an upper bound for the covering radius of the gateway nodes in $O_k$ is solved by means of coding theory.
Lemma 2.2. The graphical distance $d_G(x, y)$ and the Hamming distance $d_H(x, y)$ between any two vertices $x$ and $y$ in $O_k$ are related by:

$$d_G(x, y) = \min(d_H(x, y), d_H(x, 1 + y)),$$

where $1$ is the all-one vector and $+$ is the addition law in $Z_2^{2k-1}$.

Proof. When the graphical distance takes the values:

$$d_G(x, y) = 1, 2, 3, 4, ..., k - 1,$$

then the Hamming distance takes the values:

$$d_H(x, y) = 2k - 2, 2k - 4, 2k - 6, 6, ..., J$$

with

$$d_H(x, 1 + y) = 1, 2k - 3, 3, 2k - 5, 5, ..., (2k - i - J),$$

where

$$J = \begin{cases} k, & \text{if } k \text{ is even}, \\ k + 1, & \text{if } k \text{ is odd}. \end{cases}$$

This is straightforward to check by induction, and also well known [4, p. 239; 12]. From equations (4), (5) and (6) we note that for the even graphical distances $d_G(x, y) = d_H(x, y)$, otherwise $d_G(x, y) = d_H(x, 1 + y)$. Furthermore, it is also obvious that for even graphical distances $d_H(x, y) < d_H(x, 1 + y)$, while the reverse is true for odd distances. Therefore, $d_G(x, y) = \min(d_H(x, y), d_H(x, 1 + y)).$ \hfill $\square$

3. The graphical covering radius of a Hadamard code in $O_k$

An Hadamard matrix of order $n$ is an $n \times n$ real matrix with $\pm 1$ entries such that its rows are pairwise orthogonal for the usual Euclidean scalar product. Hadamard matrices of order $n, n \geq 3$, can exist only if $n$ is a multiple of 4, and the converse is widely believed [12]. If the first row and the first column are the all-one vector, the matrix is said to be normalized.

Let us suppose that $k$ is even, and that a normalized Hadamard matrix $M$ [17, p. 44] of order $2k$ exists. Removing the first row and the first column of $-M$, we are left with a set $M^*$ of $2k - 1$ rows of Hamming weight $k - 1$ (in binary notation, mapping 1 to 0, and $-1$ to 1), that can be identified with nodes of the graph. The nodes associated with $M^*$ can be shown to be at graphical distance $k - 1$ from each other [12] and can be effectively used to act as gateway nodes for the system expansion. We define the graphical distance of a node to a code $C$ as the smallest graphical distance of an element of $C$ to this node. We can then define the graphical covering radius ($r$) of a code $C$ as the largest graphical distance of a node to $C$. In this paper we find upper and lower bounds on $r$ in the case of $C = M^*$, and accordingly describe an expansion scheme for the interconnection system.
In the following "log" is binary. All codes are binary but not necessarily linear. An \((n, K, w)\) code is a code of length \(n\), minimum weight \(w\), and \(K\) codewords.

4. Lower bounds

Let \(w_i\) count the number of nodes at graphical distance \(i\) from a given node in \(O_k\). Using the classical sphere-covering argument in \(O_k\), we have the bound:

\[
\sum_{i=0}^{r} w_i \geq \left(\frac{2k-1}{k-1}\right) / (2k-1)
\]

(7)

where the \(w_i\) are given by:

\[
u_0, v_{k-1}, v_1, v_{k-2}, v_2, \ldots
\]

(8)

with the \(v_i = \binom{k}{i} \binom{k-1}{i-1}\) (see, for example, the equation on p. 219 of \([4]\), and problem 10 of Chapter 21 of \([17]\)). This bound is most useful for small values of \(r\) (cf. Section 7). We now derive an asymptotic lower bound for large values of \(r\).

Letting \(r' = \left\lceil \frac{r}{k} \right\rceil\), we note that

\[
\sum_{i=0}^{r} w_i = \sum_{i=0}^{r'} v_i + \sum_{i=k-1-r'}^{k-1} v_i.
\]

(9)

Bounding a sum of products by a product of sums, we obtain:

\[
\left(\sum_{i=0}^{r'} v_i\right) \leq \left(\sum_{i=0}^{r'} \binom{k-1}{i}\right) \left(\sum_{i=0}^{r'} \binom{k}{i}\right).
\]

(10)

The same approach can be used to evaluate the second sum in the RHS of equation (9). Using classical estimates like

\[
\sum_{i=0}^{r'} \binom{k}{i} \leq 2^{k\theta(r/k)}
\]

(11)

for sums of binomial coefficients \([17, p. 310]\), the covering bound (equation (7)) reduces to

\[
\left(\frac{2k-1}{k-1}\right) \leq (2k-1)2^{k\theta(r/2k)+1}.
\]

(12)

Using the estimate:

\[
\log\left(\binom{2k-1}{k-1}\right) = 2k + O(1)
\]

(13)

(an immediate consequence of equation (1)), and taking logs of both sides of equation (12), we get an asymptotic lower bound on \(r\):

\[
\theta(r/2k) \geq 1 - (\log(k)/2k) + O(1/k),
\]

(14)
where $\theta$ is the binary entropy function. For large $k$, we can use the asymptotic expansion of equation (2), and we obtain:

$$r \geq k - c \sqrt{k \log(k)} + O(\sqrt{k}),$$

(15)

where $c = 0.833$.

Bounds like equation (10) may seem quite crude, but they are sufficient for our asymptotic purposes.

5. Equivalent formulations

We define the $w$-covering radius of a binary code as the farthest possible Hamming distance of a binary word of weight $w$ to the code. This is at most equal to the usual covering radius [17, p. 172]. Then we have the characterization:

**Theorem 5.1.** The graphical covering radius of $C$ in $O_k$ is equal to the $(k - 1)$-covering radius of the code $D = C \cup 1 + C$ of length $2k - 1$.

**Proof.** The proof directly follows from Lemma 2.2. □

Let us suppose that $D$ is linear. Let $A_j(x)$ denote the number of words of weight $j$ in the coset $x + D$ of $D$. The weight of the coset $x + D$ is the smallest $j$ such that $A_j(x) \neq 0$. We are in a position to state the following obvious but useful lemma:

**Lemma 5.2.** Let $T$ be the coset of the largest weight among all the cosets $x + D$ with the property $A_{k - 1}(x) \neq 0$. Then the $(k - 1)$-covering radius of $D$ is the weight of $T$.

This simple property allows us to use known facts on coset weight distribution of binary codes [18, 5]. The numerical values for $r$ are given in Table 1.

6. Upper bounds

The problem of finding an upper bound for the graphical covering radius of $C$ in $O_k$ amounts to giving an upper bound on the $(k - 1)$-covering radius of an Hadamard code of length $2k - 1$ and size $2^{k - 2}$. Since all its codewords have weight $k$ or $k - 1$, which is more than the usual covering radius, the presence or absence of the zero or all-one vector is clearly immaterial. When $k$ is a power of 2, we assume that this code is the punctured first order Reed-Muller. We recall that the strength of a code is the largest integer $t$ such that every binary $t$-tuple appears the same number of times amongst any $t$-subset of its coordinates. For more information on this important concept, we refer to p. 133 of [17], or to [11].
Theorem 6.1. The \((k - 1)\)-covering radius of a \((2k - 1, 4k, k - 1)\) Hadamard code \(H\) is at most \(2\delta + 1\), where \(\delta\) is the largest minimum weight of a self-complementary \((k - 1, 4k)\) binary code of strength 2.

Proof. The proof uses a suitable generalization of the concept of leader code [18]. We define the leader code associated to a binary code \(C\) and a binary vector \(y\) as the restriction of \(C\) to the nonzero coordinates of \(y\). We denote it by \(C_y\). Clearly the strength of \(C_y\) is at least the strength of \(C\). For more information on this important concept, we refer to p. 139 of [17], or to [11].

Let \(y\) be any vector of weight \(k - 1\). \(H\) is of strength 2, since the kernel of an Hadamard matrix of size \(2k\) is a \(2 - (2k - 1, k - 1, k/2 - 1)\) design [8]. Moreover \(H_y\) is a self-complementary \((k - 1, 4k, w)\) code. Let us show that the distance of \(y\) to \(H\), \(d(y, H)\), is at most \(2w + 1\).

By permutation of the coordinate places, we can write any codeword of \(H\) as \((l | y)\) (where \(|\) stands for juxtaposition) with \(l\) in \(H_y\), and \(r\) a binary vector of length \(k\). The weight of \(y\) is at most \(k - w(l)\), since the codewords of \(H\) have weight \(k\) or \(k - 1\). The distance of \(y\) to this codeword is \((k - 1 - w(l)) + w(r)\), which is at most \(2(k - 1 - w(l)) + 1\). But \(H_y\) is self-complementary, and we come up with a bound of \(2w + 1\). □

Now we can use a second moment argument analogous to that of [16] to prove:

Theorem 6.2. The \((k - 1)\)-covering radius of a \((2k - 1, 4k, k - 1)\) Hadamard code is at most \(k - \sqrt{k} - 1\).

Proof. By [16] the covering radius of a self-complementary binary code of strength 2 and length \(n\) is at most \(\frac{1}{2}(n - \sqrt{n})\), hence a fortiori its minimum weight, which is the distance of the origin to the code. Using the previous theorem, the result follows. □

7. Numerical values

The few known values of \(r\) show that the true value of \(r\) is closer to the lower than to the upper bound (see Table 1). The lower bounds are obtained by computing

<table>
<thead>
<tr>
<th>(k)</th>
<th>Lower bound on (r)</th>
<th>Upper bound on (r)</th>
<th>(r)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>a perfect code in (O_4) [15]</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>(r = 4) from Lemma 5.2 and [18]</td>
</tr>
<tr>
<td>10</td>
<td>5</td>
<td>7</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>6</td>
<td>8</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>8</td>
<td>10</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>9</td>
<td>12</td>
<td>10</td>
<td>(r = 10) from Lemma 5.2 and [5]</td>
</tr>
</tbody>
</table>
numerically both sides of equation (7) (the covering bound). The exact values of $r$ for $k = 10, 12$ were found through a computer search. The entry upper bound is calculated from Theorem 6.2. When $k = 12$ the Hadamard matrix was constructed by using Paley construction and the quadratic residues modulo 23.

8. An expansion scheme

For interconnection networks an important design consideration is a provision for its future expansion which does not require any change in the original topology of the network. In this section we present a simple but highly flexible expansion mechanism for networks using $O_k$ graphs. In this technique we connect a given number of copies of $O_k$ (say $Q$) by connecting together all the gateway nodes in all the copies according to a certain graph $\Omega$ with $N'$ nodes ($N' = Q(2k - 1)$), diameter $D'$ and degree $A'$. We proceed to derive inequalities on these parameters in order to maintain the density of the extended network within the same range as the density of $O_k$.

First, we see that the new value of the diameter is $D = D' + 2r$, which means that, as long as $D' \leq 2\sqrt{k}$, we shall have $D \leq 2k$. Note that this result depends directly on the availability of good upper bounds on $r$.

Second, the maximum degree becomes $A = A' + k$. This means that as long as $A'$ is not too large compared with $k$, we have $\ln(A) - \ln(k)$.

Finally the number of nodes becomes $N = QN_O$, where $N_O = (\frac{2k - 1}{k})$. Denoting the density of $O_k$ by $\delta_O$, the new density appears to be, in view of the preceding remarks

$$\delta \geq \left( \frac{\delta_O}{2} + \frac{\ln(Q)}{2k \ln(k)} \right)(1 + o(1)).$$

This is a graceful degradation. In particular, if we can find an $\Omega$ with $N' \geq 2k + 1(2k - 1)$, we will have $\delta \geq \delta_O$. The problem of finding such dense graphs is analyzed in [6].

9. The unicity problem

So far, we have not been concerned with the fact that for a given length there may exist several nonequivalent Hadamard matrices, hence several possible covering radii in $O_k$. Since codes with the same weight distribution may have a different coset weight distribution [5], this phenomenon could be expected. For small values of $k$, however, this cannot happen, since then, the general bounds we have developed for any Hadamard code are sufficient. $k = 8$ is the first value for which such a phenomenon might have happened. It is known that there are five nonequivalent Hadamard designs on 15 points [19, p. 421]. However, all five designs have been verified to yield the same value of the covering radius which is 4. The same
phenomenon has been partially observed for \( k = 10 \), for which there are three non-equivalent Hadamard matrices [14], and at least four nonequivalent 2-(19,9,5) designs, all with covering radius 6. Hence, we make the following conjecture:

**Conjecture.** For every \( k \) such that a Hadamard matrix of order \( 2^k \) exists, all Hadamard designs have the same covering radius in \( O_k \).

For a given Hadamard design \( H \), denote by \( u = \{u_0, u_1, \ldots, u_r\} \), the covering vector of \( H \), that is,

\[
u_i = |\{x \in O_k : d_2(x, H) = i\}|.
\]  

(16)

Clearly, \( u_i/(2k-1) \) coincides with the \( i \)th valency of \( O_k \) for \( i \leq \left\lfloor \frac{1}{2}(k-1) \right\rfloor \). For \( k = 10 \), the ordered pair \( (u_5, u_6) \) takes four values for the four designs we considered. Many more may exist.

Following Hall, we denote by \( Q, N, P \) the three classes of Hadamard matrices of order 20. Note that two equivalent Hadamard matrices can yield inequivalent Hadamard designs [19].

- **Class Q:** \( u_5 = 46470, u_6 = 5514 \) and \( u_5 = 46398, u_6 = 5586 \).
- **Class N:** \( u_5 = 46524, u_6 = 5460 \).
- **Class P:** \( u_5 = 46452, u_6 = 5532 \).

Of course in all four cases

\[ u_5 + u_6 = 51984 = 19 \left( \binom{19}{9} - 1 - u_1 - u_2 - u_3 - u_4 \right). \]

So the covering vector seems to be an interesting invariant to classify Hadamard designs. A finer invariant would be the Delsarte matrix \( B \) [11] where \( B_{u,i} \) counts the number of blocks at distance \( i \) from \( x \) in \( O_k \).

### 10. Conclusion

The problem we considered in this paper is to find the graphical covering radius of the Hadamard code in the graph \( O_k \). This determination is essential as we propose the use of a Hadamard code set \( C \) for expanding interconnection networks based on the graphs \( O_k \).

The overall diameter of the proposed expansion scheme is shown to be dependent on the covering radius of \( C \). The approach is expected to be applicable to a large class of distance transitive graphs. The covering radius problem is shown to be related to the coset weight enumeration of the first order Reed-Muller and more generally, of Hadamard codes. Even if the bounds we obtained are susceptible of improvement, they are sufficient to ensure a good covering of the graph \( O_k \) with a very few links needed for the proposed expansion scheme, as compared to a complete node to node interconnection of each copy of \( O_k \).
Acknowledgement

Discussion with Professor H.F. Mattson Jr led us to use the concept of leader code (see [10]).

References