New Bounds on a Hypercube Coloring Problem and Linear Codes

Hung Quang Ngo*

Computer Science and Engineering Department,

University of Minnesota,

Minneapolis, MN 55455, USA.

Email: hngo@cs.umn.edu,

Ding-Zhu Du*

Computer Science and Engineering Department,
University of Minnesota,
Minneapolis, MN 55455, USA.
Email: dzd@cs.umn.edu,

Ronald L. Graham

Department of Computer Science, University of California at San Diego, La Jolla, CA 92093-0114, USA. Email: graham@ucsd.edu

December 19, 2000

Abstract

In studying the scalability of optical networks, one problem arising involves coloring the vertices of the n-dimensional hypercube with as few colors as possible such that any two vertices whose Hamming distance is at most k are colored differently. Determining the exact value of $\chi_{\bar{k}}(n)$, the minimum number of colors needed, appears to be a difficult problem. In this paper, we improve the known lower and upper bounds of $\chi_{\bar{k}}(n)$ and indicate the connection of this coloring problem to linear codes.

Keywords: hypercube, coloring, linear codes.

1 Introduction

An n-cube (or n-dimensional hypercube) is a graph whose vertices are the vectors of the n-dimensional vector space over the field GF(2). There is an edge between two vertices of the n-cube whenever their Hamming distance is exactly 1, where the Hamming distance between two vectors is the number of coordinates in which they differ. Given n and k, the problem we consider is that of finding $\chi_{\bar{k}}(n)$, the minimum number of colors needed to color the vertices of the n-cube so that any two vertices of (Hamming) distance at most k have different colors. This problem originated from the study of the scalability of optical networks [1].

It was shown by Wan [2] that

$$n+1 \le \chi_{\bar{2}}(n) \le 2^{\lceil \log_2(n+1) \rceil},\tag{1}$$

and it was conjectured that the upper bound is also the true value, i.e.,

$$\chi_{\bar{2}}(n) = 2^{\lceil \log_2(n+1) \rceil}.$$

Kim et al. [3] showed that

$$2n \le \chi_{\bar{3}}(n) \le 2^{\lceil \log_2 n \rceil + 1},\tag{2}$$

$$\left(\binom{n}{k/2} \right) \le \chi_{\bar{k}}(n) \le (k+1) \left(\frac{k+2}{2} \right)^{\frac{k(k+2)}{8} \lceil \log_2 n \rceil},$$
(3)

and

$$2\left(\binom{n-1}{\frac{k-1}{2}}\right) \le \chi_{\bar{k}}(n) \le (k+1)\left(\frac{k+2}{2}\right)^{\frac{k(k+2)}{8}\lceil \log_2 n \rceil} \tag{4}$$

where
$$\binom{n}{m} = \sum_{i=0}^{m} \binom{n}{i}$$
.

The upper bounds in (1) and (2) are fairly tight. In (1), the upper and lower bounds coincide when n+1 is an exact power of 2, and the same assertion holds for (2) when n is a power of 2. However, the upper bounds in (3) and (4) are not very tight. In fact, when k=2 and 3, they are already different from those of (1) and (2). A natural approach for getting an upper bound for $\chi_{\overline{k}}(n)$ is to find a valid coloring of the n-cube with as few colors as possible. We shall use this idea and various properties of linear codes (to be introduced in the next section) to give tighter bounds for general k which imply (1) when k=2 and (2) when k=3. In fact, the upper bounds in (1) and (2) are straightforward applications of this idea using the well-known Hamming code [4]. Moreover, all the lower bounds can be improved slightly by applying known results from coding theory [4].

The paper is organized as follows. Section 2 introduces concepts and results from coding theory needed for the rest of the paper, Section 3 discusses our bounds and Section 4 gives a general discussion about the problem.

2 Preliminaries

The following concepts and results can be found in standard texts on coding theory (e.g., see [4]).

Let $A = \{0, 1, \dots, q-1\}$ where $q \ge 2$ is an integer, and let A^n denote the set of all n-dimensional vectors (or strings of length n) over A. Any non-empty subset C of

^{*}Support in part by the National Science Foundation under grant CCR-9530306.

 A^n is called a q-ary block code. Our main concern is when $A=\{0,1\}=GF(2)$, in which case C is called a binary code. From here on, the term code refers to a binary code unless specified otherwise. Each element of C is called a codeword. If |C|=M then C is called an (n,M)-code. The Hamming distance between any two codewords $u=u_1u_2\ldots u_n$ and $v=v_1v_2\ldots v_n$ is defined to be $d(u,v)=|\{i:u_i\neq v_i\}|$. For $u\in C$, the weight of u denoted by u(u) is the number of 1's in u. The minimum distance d(u) of a code u0 is the least Hamming distance between two different codewords in u1. If u2 is called an u3, and u4 is called an u4, and u5 is called an u6.

One of the most important problems in coding theory is to determine $A_q(n,d)$, the largest integer M such that a q-ary (n,M,d)-code exists. For the case q=2, we will write A(n,d) instead of $A_2(n,d)$. The following theorems are standard results from coding theory and the reader is referred to [4] for their proofs.

Theorem 2.1. A(n, 2t + 1) = A(n + 1, 2t + 2)

Theorem 2.2.

$$A(n, 2t+1) \le \frac{2^n}{\sum_{i=0}^t \binom{n}{i} + \frac{1}{\left\lfloor \frac{n}{t+1} \right\rfloor} \binom{n}{t} \left(\frac{n-t}{t+1} - \left\lfloor \frac{n-t}{t+1} \right\rfloor \right)}$$

Theorem 2.2 is a special case of the Johnson bound [4].

The set of all n-dimensional vectors over GF(2) forms an n-dimensional vector space, which we denote by $V_n(2)$. A code $C \subset V_n(2)$ is called a $linear\ code$ if it is a linear subspace of $V_n(2)$. Moreover, C is called a [n,m]-code if it has dimension m. A [n,m]-code with minimum distance d is called an [n,m,d]-code. The square brackets will automatically refer to linear codes. An $m \times n$ matrix G is called a $generator\ matrix$ of an [n,m]-code C if its rows form a basis for C. Given an [n,m]-code C, an $(n-m) \times n$ matrix H is called a $generator\ matrix$ for C if C if

Given an [n, m, d]-code C, the standard array of C is a $2^{n-m} \times 2^m$ table where each row is a (left) coset of C. This table is well defined since elements of C form an Abelian subgroup in $V_2(n)$ under addition (and the cosets of a group partition the group uniformly). The first row of the standard array contains C itself. The first column of the standard array contains the minimum weight elements from each coset. These are called coset leaders. Each entry in the table is the sum of the codeword on the top of its column and its coset leader. Since each pair of distinct codewords has Hamming distance at least d, each pair of elements in the same row also has Hamming distance at least d. It is a basic fact from coding theory that all elements in the same row of the standard array have the same syndrome and different rows have different syndromes.

We conclude this section with a well-known result. Again, the reader is referred to [4] for a proof.

Theorem 2.3. If H is an $(n - m) \times n$ matrix where any d-1 columns of H are linearly independent and there exist d linearly dependent columns in H, then H is the parity check matrix of an [n, m, d]-code.

3 Main Results

Lemma 3.1. Let k = 2t, then

$$\chi_{\bar{k}}(n) \ge \sum_{i=0}^{t} \binom{n}{i} + \frac{1}{\left|\frac{n}{t+1}\right|} \binom{n}{t} \left(\frac{n-t}{t+1} - \left\lfloor\frac{n-t}{t+1}\right\rfloor\right)$$

If k = 2t + 1, we have

$$\chi_{\bar{k}}(n) \ge 2 \left(\sum_{i=0}^{t} \binom{n-1}{i} + \frac{1}{\left\lfloor \frac{n-1}{t+1} \right\rfloor} \binom{n-1}{t} \left(\frac{n-1-t}{t+1} - \left\lfloor \frac{n-1-t}{t+1} \right\rfloor \right) \right)$$

Proof. Given a valid coloring of the n-cube with parameters n and k using m colors, let $S_i, 1 \leq i \leq m$, be the set of vertices which are colored i. Clearly for each i, S_i forms an $(n, |S_i|, d)$ -code where $d \geq k + 1$. With the observation that A(n, d) is a decreasing function of d, we have

$$2^{n} = \sum_{i=1}^{m} |S_{i}| \le \sum_{i=1}^{m} A(n, k+1) = mA(n, k+1)$$

Thus, in particular we have $\chi_{\bar{k}}(n) \geq \frac{2^n}{A(n,k+1)}$. When k=2t, Theorem 2.2 yields

$$\chi_{\bar{k}}(n) \geq \sum_{i=0}^t \binom{n}{i} + \frac{1}{\left\lfloor \frac{n}{t+1} \right\rfloor} \binom{n}{t} \left(\frac{n-t}{t+1} - \left\lfloor \frac{n-t}{t+1} \right\rfloor \right)$$

When k = 2t + 1 then we can combine Theorems 2.1 and 2.2 to get

$$\begin{array}{lcl} \chi_{\bar{k}}(n) & \geq & \displaystyle \frac{2^n}{A(n,k+1)} = \frac{2^n}{A(n,2t+2)} \\ & = & \displaystyle \frac{2^n}{A(n-1,2t+1)} \\ & \geq & \displaystyle 2 \left(\sum_{i=0}^t \binom{n-1}{i} + \frac{1}{\left\lfloor \frac{n-1}{t+1} \right\rfloor} \binom{n-1}{t} \right) \times \\ & & \displaystyle \left(\frac{n-1-t}{t+1} - \left\lfloor \frac{n-1-t}{t+1} \right\rfloor \right) \right) \end{array}$$

Lemma 3.2. Let $\binom{n}{m}$ denote $\sum_{i=0}^{m} \binom{n}{i}$. Then we have

$$\chi_{\bar{k}}(n) \leq 2^{\lfloor \log_2(\binom{n-1}{k-1})\rfloor + 1}$$
 when k is even,

and

$$\chi_{\bar{k}}(n) \leq 2^{\lfloor \log_2(\binom{n-2}{k-2}) \rfloor + 2}$$
 when k is odd

Proof. Let C be an [n, m, k+1]-code. As we have noticed in the previous section, any two elements in the same row of the standard array of C are at a distance of at least k + 1. Thus, coloring each row of C's standard array by a different color would give us a valid coloring. The number of colors used is 2^{n-m} , which is the number of rows of C's standard array. Consequently, one way to obtain a good coloring of the ncube is to find a linear [n, m, k+1]-code with as large an m as possible. Moreover, by Theorem 2.3 we can construct a linear [n, m, d] code by trying to build its parity check matrix H, which is an $(n-m) \times n$ matrix with the property that d is the largest number such that any d-1 columns of H are linearly independent and there exist d dependent columns. Also, since all elements of a coset of the code (a row of its standard array) have the same syndrome, we can use H to color each vector $x \in V_2(n)$ with $synd(x) = xH^T$.

Let

$$p = \left\lfloor \log_2 \left(1 + \binom{n-1}{1} + \dots \binom{n-1}{d-2} \right) \right\rfloor + 1$$
$$= \left\lfloor \log_2 \left(\binom{n-1}{d-2} \right) \right\rfloor + 1$$

Then clearly we have

$$\binom{n-1}{1} + \binom{n-1}{2} + \dots \binom{n-1}{d-2} < 2^p - 1.$$

Now, we describe a procedure for constructing a $p \times n$ parity check matrix H by choosing its column vectors sequentially. The first column vector can be any non-zero vector. Suppose we already have a set V of i vectors so that any d-1 of them are linearly independent. The $(i+1)^{th}$ vector can be chosen as long as it is not in the span of any d-2 vectors in V. In other words, since we are working over the field GF(2), the new vector cannot be the sum of any d-2 or fewer vectors in V. The total number of undesirable vectors is at most $\binom{i}{1}+\binom{i}{2}+\ldots\binom{i}{d-2}$, which is an increasing function of i. Consequently, as long as $\binom{i}{1}+\binom{i}{2}+\ldots\binom{i}{d-2}<2^p-1$ then we can still add a new column to H. This is a special case of the Gilbert-Varshamov bound.

The linear code C whose parity check matrix is H has minimum distance at least d and size $|C|=2^{n-p}$. The number of rows of the standard array for C is 2^p .

For our problem of looking for an upper bound of $\chi_{\bar{k}}(n)$, we want d=k+1. The linear code C constructed gives a valid coloring using 2^p colors, so

$$\begin{array}{rcl} \chi_{\bar{k}}(n) & \leq & 2^{p} \\ & = & 2^{\left\lfloor \log_{2}\left(1+\binom{n-1}{1}+\binom{n-1}{2}+\cdots\binom{n-1}{k-1}\right)\right\rfloor+1} \\ & = & 2^{\left\lfloor \log_{2}\left(\binom{n-1}{k-1}\right)\right\rfloor+1} \end{array}$$

This inequality holds regardless of k being odd or even and thus proves our lemma for the even k case. However, when k is odd we are able to do better.

Notice that if we add an even parity bit to each vector of $V_2(n-1)$ then we get half of $V_2(n)$. Adding an odd parity bit would give us the other half. When k is odd, we just proved that we can color the (n-1)-cube using $a=2^{\left\lfloor\log_2\left(\binom{n-2}{k-2}\right)\right\rfloor+1}$ colors so that if two vertices have the same color then their distance is at least k. From this, we can obtain a coloring of the n-cube as follows. We first add an even parity bit to each vertex of the (n-1)-cube, color them using a colors, and then add an odd parity bit and color them using a completely different set of a colors. This is clearly a coloring of the n-cube using $2a=2^{\left\lfloor\log_2\left(\binom{n-2}{k-2}\right)\right\rfloor+2}$ colors. What remains to be shown is that this coloring is valid with parameters n and k.

For any vertex x of the n-cube, let x' be the vector obtained from x by deleting the parity bit just added. By the way we constructed the coloring, if two vertices x and y of the n-cube have the same color then $d(x',y') \geq k$, and the same type of parity bit (even or odd) was added to them to get x and y. It is clear that if $d(x',y') \geq k+1$, then $d(x,y) \geq k+1$. If d(x',y') = k, then since k is odd, x' and y' must have had different bits added. Consequently, d(x,y) = k+1. In other words, if two vertices x and y of the n-cube have the same color then $d(x,y) \geq k+1$, and so we have a valid coloring with parameters n and k.

Lemmas 3.1 and 3.2 can be summarized by the following theorem.

Theorem 3.3. Let $t = \lfloor \frac{k}{2} \rfloor$ and let $\binom{n}{m}$ denote $\sum_{i=0}^{m} \binom{n}{i}$. Then, when k is even, we have

$$\sum_{i=0}^{t} \binom{n}{i} + \frac{1}{\left\lfloor \frac{n}{t+1} \right\rfloor} \binom{n}{t} \left(\frac{n-t}{t+1} - \left\lfloor \frac{n-t}{t+1} \right\rfloor \right)$$

$$\leq \chi_{\bar{k}}(n) \leq 2^{\left\lfloor \log_2\left(\binom{n-1}{k-1}\right)\right\rfloor + 1}$$

and when k is odd, we have

$$2\left(\sum_{i=0}^{t} \binom{n-1}{i} + \frac{1}{\left\lfloor \frac{n-1}{t+1} \right\rfloor} \binom{n-1}{t} \times \left(\frac{n-1-t}{t+1} - \left\lfloor \frac{n-1-t}{t+1} \right\rfloor\right)\right) \le \chi_{\bar{k}}(n) \le 2^{\left\lfloor \log_2\left(\binom{n-2}{k-2}\right)\right\rfloor + 2}$$

Note that since

$$2^{\left\lfloor \log_2\left(\binom{n-1}{2-1}\right)\right\rfloor+1}=2^{\left\lfloor \log_2 n\right\rfloor+1}=2^{\left\lceil \log_2(n+1)\right\rceil}$$

and

$$2^{\left\lfloor \log_2\left(\binom{n-2}{3-2}\right)\right\rfloor+2} = 2^{\left\lfloor \log_2\left(n-1\right)\right\rfloor+2} = 2^{\left\lceil \log_2n\right\rceil+1}$$

then inequalities (1) and (2) are direct consequences of this theorem.

4 Discussions

The key to get a good coloring is to find the parity check matrix H when k is even. As can be seen, the proof of Theorem 3.3 implicitly gave us an algorithm to construct H, but it is still not very constructive. However, in the case k=2 (and thus in case k=3) we can explicitly construct H. To see this, consider the Hamming code $\mathcal{H}_2(r)$, which is a $[2^r-1,2^r-1-r,3]$ code. Its parity check matrix H(r,2) has dimensions $r\times(2^r-1)$. Let $r=\lceil\log_2(n+1)\rceil$, then $2^r-1\geq n$. So, if we remove the last 2^r-1-n columns of H(r,2), then we get a parity check matrix of an $[n,n-\lceil\log_2(n+1)\rceil,3]$ code. This code gives us a coloring of the n-cube with parameters n and n using n0 colors. This proves the upper bounds in (1) and (2).

Besides the *Johnson bound* we used, other known upper bounds of A(n,d) might give us better lower bound of $\chi_{\bar{k}}(n)$ such as the *Plotkin bound*, the *Elias bound* and the *Linear Programming bound*. However, applying these bounds breaks the problem into various cases and doesn't give us a significantly better result.

For some special values of n and k, we can get better results by considering some specially good linear codes. The Golay \mathcal{G}_{24} code is a binary [24, 12, 8]-code whose generator matrix has the form $G = [I_{12} \mid A]$ where A was "magically" given by Golay in 1949 (see [5]).

This shows that $\chi_{7}(24) \leq 2^{12}$, while our theorem gives

$$2^{12} \le \chi_{\bar{7}}(24) \le 2^{17}$$

Thus, in fact $\chi_{7}(24)=2^{12}$ (!!!), and our upper bound is far off in this case. Puncturing \mathcal{G}_{24} (i.e. removing any coordinate position) at any coordinate gives us \mathcal{G}_{23} , a [23,12,7]-code. This implies $\chi_{\tilde{6}}(23)\leq 2^{11}$, while again our theorem gives too large an upper bound:

$$2^{11} \le \chi_{\bar{6}}(23) \le 2^{15}$$

However, again we obtain $\chi_{\bar{6}}(23)=2^{11}$. We summarize the cases where the exact values of $\chi_{\bar{k}}(n)$ are known as follows

- $\chi_{\bar{7}}(24) = 2^{12}$ (shown above).
- $\chi_{\bar{6}}(23) = 2^{11}$ (shown above).
- $\chi_{\bar{2}}(2^m 1) = 2^m$ (immediate from Theorem 3.3)
- $\chi_{\bar{2}}(2^m-2)=2^m$ (immediate from Theorem 3.3)
- $\chi_{\bar{3}}(2^m) = 2^{m+1}$ (immediate from Theorem 3.3)
- $\chi_{\bar{3}}(2^m-1)=2^{m+1}$ (immediate from Theorem 3.3)

One might wonder if we can get more exact values of $\chi_{\bar{k}}(n)$ using the same method. Our lower bound was proven using Johnson's bound, a slight extension of the sphere packing bound. To construct a linear code that matches the sphere packing bound, the code has to be perfect, namely there exist a radius r such that the spheres $S(c,r)=\{a\mid d(c,a)\leq r\}$ around each codeword c covers the whole space. The binary $[2^r-1,2^r-1-r,3]$ Hamming code $\mathcal{H}(r)$ and the Golay [23,12,7]-code are perfect. This is why we were able to obtain the exact values as above. Thus, the question comes down to "does there exist any other binary perfect codes besides the Hamming codes and the Golay codes?". The answer was given by Tietäväinen ([6], 1973) with most of the work done previously by van Lint:

Theorem 4.1. A nontrivial perfect q-ary code C, where q is a prime power, must have the same parameters as either a Hamming code or one of the Golay codes \mathcal{G}_{23} (binary) or \mathcal{G}_{11} (ternary).

However, as we have mentioned the Johnson bound is slightly better than the sphere packing bound. That is how we got two additional values $\chi_{\bar{2}}(2^m-2)=2^m$ and $\chi_{\bar{3}}(2^m-1)=2^{m+1}$. This comes from the fact that the shorten Hamming $[2^m-2,2^m-2-m,3]$ is nearly perfect, i.e. it gives equality in the Johnson bound. Again, does there exist any other nearly perfect codes? Lindström ([7], 1975) answered in the affirmative: the only other nearly perfect code is the punctured Preparata code. This code has parameter $(2^m-1,2^{2^m-2m},5)$. Unfortunately, this is not a binary linear code, so our coloring doesn't quite work.

That is not the end of our hope. Hammons, Kumar, Calderbank, Sloane and Sole [8, 9, 10] showed that the Preparata code is Z_4 -linear, namely it can be constructed easily from a linear code over Z_4 as the binary image under the Gray map. This map transforms Lee distance in Z_4 to Hamming distance in Z_2 . The mapping is simple, but the construction of the code is quite involved. We hope to be able to apply their work to find nice upper bounds for $\chi_{\bar{4}}(n)$ and $\chi_{\bar{5}}(n)$.

References

[1] A. Pavan, P.-J. Wan, S.-R. Tong, and D. H. C. Du, "A new multihop lightwave network based on the generalized 1De-Bruijn graph," in 21st IEEE Conference on Local Computer

- Networks: October 13–16, 1996, Minneapolis, Minnesota, vol. 21, pp. 498–507, IEEE Computer Society Press, 1996.
- [2] P.-J. Wan, "Near-optimal conflict-free channel set assignments for an optical cluster-based hypercube network," J. Comb. Optim., vol. 1, no. 2, pp. 179–186, 1997.
- [3] D. S. Kim, D.-Z. Du, and P. M. Pardalos, "A coloring problem on the *n*-cube," *Discrete Appl. Math.*, vol. 103, no. 1-3, pp. 307–311, 2000.
- [4] S. Roman, Coding and Information Theory. New York: Springer-Verlag, 1992.
- [5] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*. I. Amsterdam: North-Holland Publishing Co., 1977. North-Holland Mathematical Library, Vol. 16.
- [6] A. Tietäväinen, "On the nonexistence of perfect codes over finite fields," *SIAM J. Appl. Math.*, vol. 24, pp. 88–96, 1973.
- [7] K. Lindström, "The nonexistence of unknown nearly perfect binary codes," *Ann. Univ. Turku. Ser. A I*, no. 169, p. 28, 1975.
- [8] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The z₄-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 2, pp. 301–319, 1994.
- [9] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "On the apparent duality of the Kerdock and Preparata codes," in *Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993)*, pp. 13–24, Berlin: Springer, 1993.
- [10] A. R. Calderbank, A. R. Hammons, Jr., P. V. Kumar, N. J. A. Sloane, and P. Solé, "A linear construction for certain Kerdock and Preparata codes," *Bull. Amer. Math. Soc. (N.S.)*, vol. 29, no. 2, pp. 218–222, 1993.