On the dual distance and the gap of a binary code

Patrick Solé\textsuperscript{a,}\textsuperscript{*}, Jean-Pierre Tillich\textsuperscript{b,1}

\textsuperscript{a} C.N.R.S-I3.S., ESSI, BP 145, Lab. d'Informatique 650, Route des Colles, F-06 903 Sophia - Antipolis, France
\textsuperscript{b} Université de Caen, Département d'informatique 14 032 Caen Cedex, France

Received 8 January 1997; revised 10 July 1997; accepted 25 July 1997

Abstract

The coset graph of a nondegenerate cyclic code is orbital regular. This yields a lower bound on its average distance, a parameter which measures the average distortion of a code used in data compression. Using results of Shahrokhi and Székely we generalize this bound to binary codes with a transitive automorphism group. © 1998 Elsevier Science B.V. All rights reserved

1. Introduction

The gap of a code \cite{12} like the covering radius is a parameter occurring naturally in rate distortion theory \cite{3,1}, which has been little explored so far by combinatorialists. While the covering radius measures the worst-case distortion, the gap is the average distortion. In terms of coset graph of a linear code the covering radius is the diameter \cite{5}, while the gap is the average distance. In this note we use some results of \cite{9} on the average distance of sufficiently symmetric graphs to derive a lower bound on the gap of sufficiently symmetric codes.

2. Main result

The gap of an unrestricted code $C$ is

$$g := \frac{1}{2^n} \sum_{x \in F_2^n} d(x, C).$$

\textsuperscript{*} Corresponding author. E-mail: sole@alto.unice.fr.
\textsuperscript{1} The work of the second author has been supported by a postdoctoral grant given by the 'Conseil régional de Caen'.
Table 1

<table>
<thead>
<tr>
<th>Code</th>
<th>$n$</th>
<th>$n-k$</th>
<th>$d^\perp$</th>
<th>$g$</th>
<th>Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hamming</td>
<td>$2^m-1$</td>
<td>$m$</td>
<td>$2^{m-1}$</td>
<td>$1-2^{-m}$</td>
<td>$1-2^{-m}$</td>
</tr>
<tr>
<td>Ext. Ham.</td>
<td>$2^m$</td>
<td>$m+1$</td>
<td>$2^{m-1}$</td>
<td>$3/2-2^{-m}$</td>
<td>$1$</td>
</tr>
<tr>
<td>Golay</td>
<td>$23$</td>
<td>$11$</td>
<td>$8$</td>
<td>$2.85$</td>
<td>$1.437$</td>
</tr>
<tr>
<td>Ext. Golay</td>
<td>$24$</td>
<td>$12$</td>
<td>$8$</td>
<td>$3.35$</td>
<td>$3/2$</td>
</tr>
<tr>
<td>Ext. 2-err. cor. BCH</td>
<td>$2^{2t+1}$</td>
<td>$4t+3$</td>
<td>$2^{2t}-2^t$</td>
<td>$3-(2^{2t+1}+4)/2^{2t+1}$</td>
<td>$1/(1-2^{-t})$</td>
</tr>
</tbody>
</table>

For a linear code of dimension $k$ with coset weight distribution $x_i$ and covering radius $R$ \[ R \] this specializes to

$$g := \frac{1}{2^{n-k}} \sum_{i=0}^{R} i x_i.$$  

We relate this quantity to the dual distance of $C$, by using a graph theoretic approach and considering the coset graph of $C$. Recall that the coset graph $[2, 5]$ of a binary linear code $C$ has vertex set the cosets of $C$, two cosets $x+C$ and $y+C$ being connected if $x+y+C$ has weight one. Alternatively, the coset graph is a Cayley graph on the syndrome space, two syndromes being connected if they differ by a column of the parity check matrix. This graph is $n$-regular (provided the code is projective), with diameter $R$ on $2^{n-k}$ vertices. The spectrum of its adjacency matrix is given by the set \{ $n-2w(x) \mid x \in C^\perp$ \} where $w(x)$ is the Hamming weight of $x$, and $C^\perp$ the dual code. The mean distance of a graph with vertex set $V$ is by definition

$$\bar{D} - \frac{1}{|V|(|V| - 1)} \sum_{a,b \in V} d(a, b),$$

so that there is a simple relationship between the mean distance of the coset graph of $C$ and the gap of $C$, i.e

$$g = \frac{2^{n-k} - 1}{2^{n-k} \bar{D}}.$$  

Our main result is

**Theorem 1.** Let $C$ be a binary linear $[n,k]$ code with a transitive automorphism group and dual distance $d^\perp$. Then its gap is bounded below

$$g \geq \frac{n}{2d^\perp}.$$  

The examples are given in Table 1 taken amongst completely regular codes $[2]$ where $D$ can be computed exactly. Observe that the first two coset graphs are the complete and bipartite complete graph.

This theorem is proved by using the fact that the coset graph of such a code is edge-transitive, and results about the edge-expansion of edge-transitive graphs which
are due to Shahrokhi and Székely (see [9]). We observe that with a slightly stronger hypothesis on \( C \), namely that \( C \) is a cyclic code of length \( n \) with no word of period \(< n\), there is another proof of our theorem which uses results on orbital regular graphs of [10,11] instead of results on the edge-expansion of edge-transitive graphs of [9]. Indeed in the latter case the coset graph is orbital regular (Theorem 6 in [11]), and we use lower bounds on the edge-expansion of orbital regular graphs (Theorem 2 in [11]).

The relevance of the slightly more general Theorem 1 lies in the fact that many classical extended cyclic codes have a transitive automorphism group: the affine group for BCH and Reed–Muller codes and \( \text{PSL}(2, p) \) for quadratic residue codes of length \( p + 1 \) [8].

3. Proof of the main result

We shall need to consider the expansion properties of an undirected graph on \( v \) vertices with adjacency spectrum [4]

\[
\lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{v-1}.
\]

Let \( \delta X \) denote the edge cut induced by a set of vertices \( X \). Then the Cheeger constant \( h \) is the minimum over all \( |X| \leq v/2 \) of the ratio \( |\delta X|/|X| \).

**Theorem 2.** For a Cayley graph with \( d \) generators on an elementary abelian 2-group, with the above notations we have \( h = (d - \frac{d}{2})/2 \).

**Proof.** For an arbitrary \( d \)-regular graph (we denote its vertex set by \( V \), its edge set by \( E \), and its adjacency matrix by \( A \)) one always has \( h \geq (d - \lambda_1)/2 \) [7]. To prove the reverse inequality let \( u \) denote an eigenvector attached to \( \lambda_1 \) and set \( X = \{ x \in V \mid u_x = 1 \} \).

We may choose \( u \) with only \( \pm 1 \) entries. This follows from the (folklore) result (see for instance problem 8 Section 11 p. 72 of [6]) which asserts that an orthogonal basis of eigenvectors of the adjacency matrix of an abelian Cayley graph is given by the vectors \( (\chi(x))_{x \in V} \) where \( \chi \) ranges over all characters of the group. For an abelian 2-group, characters take only \( \pm 1 \) values. Note that, by orthogonality with the trivial eigenspace \( \sum_{x \in V} u_x = 0 \) which entails, since \( u \) has entries \( \pm 1 \), the property \( |X| = |V|/2 \).

A standard property of the Laplacian \( \Delta = dI - A \) (which is equal for a \( d \)-regular graph to \( dI - A \)) [7] yields

\[
\langle (dI - A)u, u \rangle = \sum_{x \in X} (u_x^2 - u_x u_y)^2 = 4|\delta X|,
\]

which equals by hypothesis on \( u \)

\[
(d - \lambda_1)(u, u) = (d - \lambda_1)|V| = 2(d - \lambda_1)|X|.
\]

The preceding result applies in particular to the coset graph of a binary linear code with \( d = n \) and \( \lambda_1 = n - 2d^+ \). In order to prove Theorem 1, we observe now that:
Lemma 1. The coset graph of a binary linear code with transitive automorphism group is edge-transitive.

Proof. The vertices $x + C$ of the coset graph are adjacent if and only if their difference contains a word of weight 1, that we denote by $e_i$ if the non-zero entry is in the $i$th position. Since $I(C)$ is a Cayley graph, $I(C)$ is vertex-transitive ($\text{Aut}(G)$ acts transitively on the set of vertices), so we just have to prove that for any $i \neq j$, there exists an automorphism which takes the edge linking $C$ to $C + e_i$ to the edge linking $C$ to $C + e_j$. Since the automorphism group of the code is transitive, there exists a permutation of the coordinates of the codewords $\sigma$ which maps $e_i$ to $e_j$, and such that $\sigma(C) = C$. Indeed it is straightforward to check that this one-to-one mapping maps a coset $C + x$ to the coset $\sigma(C + x) = \sigma(C) + \sigma(x) = C + \sigma(x)$. $\sigma$ is therefore an automorphism of $I(C)$ which maps $C$ to itself and $C + e_i$ to $C + e_j$.

We conclude the proof of Theorem 1 by a multflow argument of [9] (Corollary 4.3) which asserts that for an edge-transitive graph with $e$ edges $h \geq e/(v - 1)D$. Theorem 1 follows from applying Theorem 2 to the coset graph: $h = (d_1 - 1)/2 \geq e/(v - 1)D$, and noticing that in this case $h = d_1$, $v = 2^{n-k}$ and $e = n2^{n-k-1}$.

References