ARTICLE IN PRESS

Discrete Applied Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

]

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Constructing error-correcting binary codes using transitive permutation groups☆

Antti Laaksonen *, Patric R.J. Östergård

Department of Communications and Networking, Aalto University School of Electrical Engineering, P.O. Box 15400, 00076 Aalto, Finland

ARTICLE INFO

Article history:
Received 14 December 2016
Accepted 23 August 2017
Available online xxxx

Keywords:
Binary codes
Cliques
Error-correcting codes
Transitive groups

ABSTRACT

Transitive permutation groups are recurrent in the study of automorphism groups of combinatorial objects. For binary error-correcting codes, groups are here considered that act transitively on the pairs of coordinates and coordinate values. By considering such groups in an exhaustive manner and carrying out computer searches, the following new bounds are obtained on $A_2(n, d)$, the maximum size of a binary code of length n and minimum distance d: $A_2(17, 3) \geq 5632$, $A_2(20, 3) \geq 40960$, $A_2(21, 3) \geq 81920$, $A_2(22, 3) \geq 163840$, $A_2(23, 3) \geq 327680$, $A_2(23, 9) \geq 136$, and $A_2(24, 5) \geq 17920$.

1. Introduction

A binary *code* C of length n is a set of binary vectors of length n, the elements $c = (c_1, c_2, \ldots, c_n)$ of which are called *codewords*. The *minimum distance* of a code C is $\min\{d_H(c, c') : c, c' \in C, c \neq c'\}$, where $d_H(c, c')$ is the *Hamming distance*, which is defined as the number of coordinates where c and c' differ. The *size* (or *cardinality*) of C is the number of codewords that it contains. A code with length n, size M, and minimum distance at least d is called an (n, M, d) code.

Let $A_2(n, d)$ denote the maximum size of a binary code of length n and minimum distance d. The problem of determining the value of $A_2(n, d)$ for different parameters is a long-standing problem in information theory [15]. The exact values of $A_2(n, d)$ for $n \leq 15$ are known, but for $n > 15$ only lower and upper bounds on $A_2(n, d)$ are generally known.

Lower bounds on $A_2(n, d)$ can be obtained by constructing corresponding binary codes. Computers have been employed to get most of the recent new results on lower bounds for binary error-correcting codes, such as [5,11,16,20]. Also when using computers to search for codes, it is necessary to limit the search, for example, by making assumptions about the structure of the codes. A common technique, used in the studies [5,11,20] mentioned above, is to prescribe automorphisms of the codes.

Two binary codes are said to be *equivalent* if one of the codes can be obtained from the other by a permutation of the coordinates and permutations of the coordinate values (0 and 1), separately for each coordinate. Such a mapping from a code onto itself is called an *automorphism* of the code; all automorphisms form a group under composition, called the *automorphism group*. A subgroup of the automorphism group is called a *group of automorphisms*.

In the current work, we search for binary error-correcting codes with prescribed groups of automorphisms. The groups considered are transitive permutation groups that act transitively on the pairs of coordinates and coordinate values. The approach and the groups are discussed in detail in Section 2. The search leads to new codes that improve seven currently best known lower bounds on $A_2(n, d)$ when $n \leq 24$ and d is odd. These bounds are summarized in Table 1, and an up-to-date

☆ This work was supported in part by the Academy of Finland, Grant Number 289002.

* Corresponding author.
E-mail addresses: antti.2.laaksonen@aalto.fi (A. Laaksonen), patric.ostergard@aalto.fi (P.R.J. Östergård).

http://dx.doi.org/10.1016/j.dam.2017.08.022
0166-218X/

Please cite this article in press as: A. Laaksonen, P.R.J. Östergård, Constructing error-correcting binary codes using transitive permutation groups, Discrete Applied Mathematics (2017), http://dx.doi.org/10.1016/j.dam.2017.08.022.

Table 1
New lower bounds for $A_2(n, d)$.

Old lower bound	New lower bound
$A_2(17, 3) \geq 5312$ [4]	$A_2(17, 3) \geq 5632$
$A_2(20, 3) \geq 36864$	$A_2(20, 3) \geq 40960$
$A_2(21, 3) \geq 73728$	$A_2(21, 3) \geq 81920$
$A_2(22, 3) \geq 147456$	$A_2(22, 3) \geq 163840$
$A_2(23, 3) \geq 294912$ [24]	$A_2(23, 3) \geq 327680$
$A_2(23, 9) \geq 128$ [8]	$A_2(23, 9) \geq 136$
$A_2(24, 5) \geq 16384$ [2]	$A_2(24, 5) \geq 17920$

Table 2
Lower and upper bounds for $A_2(n, d)$.

n	$d = 3$	$d = 5$	$d = 7$	$d = 9$
16	2816–3276	256–340	36	6
17	**5632**–6552	512–673	64–72	10
18	10496–13104	1024–1237	128–135	20
19	20480–26168	2048–2279	256	40
20	**40960**–43688	2560–4096	512	42–47
21	**81920**–87333	4096–6941	1024	64–84
22	**163840**–172361	8192–13674	2048	80–150
23	**327680**–344308	16384–24106	4096	**136**–268
24	524288–599184	**17920**–47538	4096–5421	192–466

table of bounds on $A_2(n, d)$ for $16 \leq n \leq 24$ and $3 \leq d \leq 9$, d odd, is shown in Table 2, where the old results are combined from [1,7,16–18,21]. It is well known that $A_2(n, d) = A_2(n + 1, d + 1)$ when d is odd, so it suffices to consider odd d. The new lower bounds are shown in boldface. No references are given in Table 1 for bounds that follow from $A_2(n, d) \geq A_2(n+1, d)/2$ and other bounds in the table.

2. Code construction

Although the definition of an automorphism group of a binary code allows both permutations of coordinates and permutations of coordinate values, in earlier studies only one of these two types of automorphisms has typically been considered when prescribing automorphisms. For example, in the search of cyclic codes one has only permutations of coordinates; see [11] for examples of prescribing larger groups permuting only coordinates. On the other hand, only permutations of coordinate values are considered in, for example, [5,20]; then we get binary codes that are cosets of a linear code.

One obvious reason why arbitrary automorphism groups have not been studied to a greater extent is the very large number of such groups, so one would need some further ideas about what groups to consider. The motivation for our choice of groups is as follows.

In the study of automorphisms of binary codes, it is convenient to consider codes in the framework of set systems by mapping a codeword $c = (c_1, c_2, \ldots, c_n)$ to a set $\{i + nc_i : 1 \leq i \leq n\}$. That is, every codeword is then a transversal of the sets

$$\{1, n + 1\}, \{2, n + 2\}, \ldots, \{n, 2n\}. \tag{1}$$

This idea is inherent in the mapping of a binary code to a graph in [22].

Example. With the defined mapping, the binary code $\{000, 111\}$ leads to the set system $\{\{1, 2, 3\}, \{4, 5, 6\}\}$ over $\{1, 2, \ldots, 6\}$.

When studying equivalence and automorphism groups in the set system formalism, the subgroup of the symmetric group S_{2n} to consider is now precisely the stabilizer of the partition (1).

Example (cont.). The binary code $\{000, 111\}$ has an automorphism that permutes all coordinates in a cyclic manner. This corresponds to the permutation $(1\,2\,3)(4\,5\,6)$ of the set system. Another automorphism transposes the coordinate values in all coordinates simultaneously, and corresponds to $(1\,4)(2\,5)(3\,6)$.

Transitive permutation groups are recurrent in the study of automorphism groups of combinatorial objects. Indeed, one of the main ideas of the current work is to search for codes with an automorphism group that acts transitively on the $2n$ elements in the set system formalism. In the original setting, this means that the automorphism group acts transitively on the $2n$ pairs of coordinates and coordinate values. By looking at codes attaining $A(n, 3)$ or $A(n + 1, 4)$, for each length $n \leq 15$ there is indeed an optimal code that can be derived from codes with an automorphism group of this type.

The number of elements in the set on which a permutation group acts is called the *degree* of the group. All transitive permutation groups have been classified [3,9] up to degree 47. For example, the groups up to degree 30 are available in GAP [6]. Consequently, we have an exhaustive catalogue of transitive groups for the cases $2n \leq 47$, that is, $n \leq 23$.

Please cite this article in press as: A. Laaksonen, P.R.J. Östergård, Constructing error-correcting binary codes using transitive permutation groups, Discrete Applied Mathematics (2017), http://dx.doi.org/10.1016/j.dam.2017.08.022.