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

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 not only on the coordinates but 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 $A_2(24, 5) \geq 17920$.

Keywords: binary codes, cliques, error-correcting codes, transitive groups

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*

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

Email addresses: antti.2.laaksonen@aalto.fi (Antti Laaksonen), patric.ostergard@aalto.fi (Patric R. J. Östergård)

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 [16]. 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 [6, 11, 17, 23]. 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 [6, 11, 23] 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 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, 8, 17, 18, 19, 24]. 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.

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

Old Lower Bound	New Lower Bound
$A_2(17, 3) \geq 5312$ [5, p. 58]	$A_2(17, 3) \geq 5632$
$A_2(20, 3) \geq 36864$	$A_2(20, 3) \geq 40960$
$A_2(21, 3) \geq 73728$	$A_2(21, 3) \geq 81920$
$A_2(22, 3) \geq 147456$	$A_2(22, 3) \geq 163840$
$A_2(23, 3) \geq 294912$ [25]	$A_2(23, 3) \geq 327680$
$A_2(23, 9) \geq 128$ [9]	$A_2(23, 9) \geq 136$
$A_2(24, 5) \geq 16384$ [3]	$A_2(24, 5) \geq 17920$

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

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, [6, 23]; 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 [4, 10] up to degree 47. For example, the groups up to degree 30 are available in GAP [7]. Consequently, we have an exhaustive catalogue of transitive groups for the cases $2n \leq 47$, that is, $n \leq 23$.

Note, however, that we may not consider arbitrary permutation groups, but the group should stabilize the partition (1). Actually, it suffices that the group stabilizes some partition of $\{1, 2, \ldots, 2n\}$ into 2-element subsets because then there is a conjugate subgroup of S_{2n} that stabilizes (1). In group-theoretic terms, the group should be *imprimitive* and have a *block system* with blocks of size 2. It is a standard task to find such block systems; note that one group may have several block systems.

Given the length of a code, n, we can now consider all transitive permutation groups of degree $2n$ and all possible block systems with blocks of size 2. Regardless whether we prefer to consider the objects as set systems or codes, we have arrived at the classical setting of constructing codes with a prescribed automorphism, and the approach described, for example, in [13, Sect. 9.3.2] can be applied. That is, having specified the minimum distance d, orbits of words with pairwise distances smaller than d are disregarded and the *admissible* orbits become vertices in a weighted graph G. The weight of a vertex in G is the length of the corresponding orbit. There is an edge between two vertices in G exactly when all pairwise distances between the words in the two orbits are greater than or equal to d. A clique in G gives a desired code, and the weight of a clique is the size of the code. Consequently, software for finding weighted cliques can now be employed to construct codes.

There are several obvious modifications of this idea. By the equality

$A(n,d) = A(n+1, d+1)$ for d odd, one may consider both the odd-weight and the even-weight case. One may further let a group fix some (typically one) coordinates and their values. Finally, one may let a group act on half of the coordinates with an identical copy of the group acting on the other half (this can obviously be generalized to more than two parts, but for small parameters two parts is the most promising choice).

3. Results

We applied the method described in Section 2 and used the Cliquer [20] software to search for maximum weight cliques. Since too large graphs cannot be processed within a reasonable time, we did not consider graphs with more than 5000 vertices. In total, the search took many years of CPU time, but the time was not evenly distributed amongst the cases. Actually, all the successful searches were quite fast.

The new codes found improve seven lower bounds on $A_2(n,d)$, as we have seen in Table 1. These bounds follow from the existence of four codes and the application of $A_2(n-1,d) \geq A_2(n,d)/2$. The codes are described in Appendix A together with some information about the prescribed group. Also the recent bound $A_2(16,3) \geq 2816$, from [17], follows directly from the new bound $A_2(17,3) \geq 5632$.

In particular, the code attaining $A_2(24,4) \geq 327680$ is very good; it would be interesting to know whether this code has some algebraic or combinatorial explanation. This code was found using two copies of a transitive group of degree 24 (recall that the authors only had the transitive groups up to degree 47 available). It then turned out that the automorphism group of one of the codes found (which is listed in the Appendix) is larger than the prescribed group and in fact is transitive of degree 48. The codes attaining $A_2(24,5) \geq 17920$ and $A_2(24,10) \geq 136$ were found in a similar manner; the automorphism group of the former is also transitive.

The new codes lead to infinite families of codes, as the following theorems show. Note, however, that due to the results of [12], for each such family there is an integer n' such that none of the codes of length $n \geq n'$ is optimal. Theorem 1 follows from the well-known $|u|u+v|$ construction [16, p.76] (see also [25]), and Theorem 2 is a reformulation of [21, Theorem 2].

Theorem 1. $A_2(2n+1,3) \geq A_2(n,3) \cdot 2^n$.

Theorem 2. *If there is an* $(n, m2^k, 3)$ *code consisting of* m *cosets of a linear* $(n, 2^k, 3)$ *code, then* $A_2(m-1,3) \geq (n+1) \cdot 2^{m+k-n-1}$.

The linear code in Theorem 2 can be found by determining the *kernel* of a code C, defined as $K(C) = \{x : x + C \in C\}$. One can actually deduce the kernel by finding the subgroup of the automorphism group of the code that stabilizes each coordinate. Then it is indeed necessary to consider the automorphism group rather than the prescribed group of automorphisms (since the latter may be a proper subgroup of the former).

Corollary 1. $A_2(79,3) \geq 3 \cdot 2^{71}$.

Proof. By puncturing the code in the Appendix that attains $A_2(24,4) \geq 327680$ in (any) one coordinate, we get a code that attains $A_2(23,3) \geq 327680$ and has a kernel of size 2^{12}. The result follows by applying Theorem 2. □

Note that the kernel of the code in the Appendix that attains $A_2(24,4) \geq 327680$ has the same length and dimension as the extended binary Golay code, but the minimum distance is 4 here.

The results for the best known codes with length n and minimum distance 3 are summarized in Table 3 for $15 \leq n \leq 512$. The new results are shown in boldface. The table updates a table published in [14]; all subsequent improvements follow either from [15] (with the additional observation that a code of length 66 leads to a code of length 133 by Theorem 1) or from the results of the current paper.

Appendix A. Codes for the new lower bounds

Bound: $A_2(17,3) \geq 5632$

Generators of G:

(2 5 3 4 19 22 20 21)(6 34 7 33 23 17 24 16)
(8 15 9 14 25 32 26 31)(10 13 28 29 27 30 11 12),
(2 34 3 33 19 17 20 16)(4 14 22 32 21 31 5 15)
(6 12 7 13 23 29 24 30)(8 27 9 11 25 10 26 28),
(2 33 28 9 19 16 11 26)(3 34 27 8 20 17 10 25)
(4 15 13 7 21 32 30 24)(5 14 12 23 22 31 29 6),
(2 6 3 24 19 23 20 7)(4 34 22 16 21 17 5 33)
(8 29 26 30 25 12 9 13)(10 32 28 14 27 15 11 31).

Fixed coordinates: 1

Transitive on non-fixed coordinates: yes

Order of G: 512

Orbit representatives:

1000111111111111101110000000000000, 0010011111111111111011000000000000,

Table 3: Lower bounds for $A_2(n,3)$, $15 \leq n \leq 512$

n	$A_2(n,3)$
15	$1 \cdot 2^{11}$
17	$\mathbf{11 \cdot 2^{9}}$
18	$41 \cdot 2^{8}$
23	$\mathbf{5 \cdot 2^{16}}$
31	$1 \cdot 2^{26}$
35	$\mathbf{11 \cdot 2^{26}}$
37	$41 \cdot 2^{26}$
47	$\mathbf{5 \cdot 2^{39}}$
63	$1 \cdot 2^{57}$
64	$414253 \cdot 2^{39}$
66	$828505 \cdot 2^{40}$
70	$1657009 \cdot 2^{43}$
79	$\mathbf{3 \cdot 2^{71}}$
95	$\mathbf{5 \cdot 2^{86}}$
127	$1 \cdot 2^{120}$
129	$414253 \cdot 2^{102}$
133	$828505 \cdot 2^{106}$
141	$1657009 \cdot 2^{113}$
159	$\mathbf{3 \cdot 2^{150}}$
191	$\mathbf{5 \cdot 2^{181}}$
255	$1 \cdot 2^{247}$
256	$127659128537782365 \cdot 2^{191}$
258	$255318257075564729 \cdot 2^{192}$
262	$510636514151129457 \cdot 2^{195}$
270	$1021273028302258913 \cdot 2^{202}$
283	$1657009 \cdot 2^{254}$
319	$\mathbf{3 \cdot 2^{309}}$
383	$\mathbf{5 \cdot 2^{372}}$
511	$1 \cdot 2^{502}$
512	$127659128537782365 \cdot 2^{446}$

01001011111111111110110100000000000, 10110011111111111101001100000000000, 01110101111111111110001010000000000, 01010110111111111101010010000000000, 10011100111111111011000110000000000, 11101100111111111100010011000000000, 00000100111111111111111011000000000, 01011101011111111101000101000000000, 10000000011111111011111111100000000, 10010110101111111101101001010000000, 00110110100111111111001001011000000.

Bound: $A_2(24,4) \geq 327680$

Generators of G:

(1 19)(2 21)(3 23)(4 22)(5 24)(6 20)(7 13)(8 18)(9 14)(10 16)(11 15)(12 17)(25 43)(26 45)(27 47)(28 46)(29 48)(30 44)(31 37)(32 42)(33 38)(34 40)(35 39)(36 41),
(1 26 30)(2 6 25)(3 28 5 27 4 29)(7 35 36 31 11 12)(8 9 34)(10 32 33)(13 38 18)(14 42 37)(15 16 41 39 40 17)(19 47 24)(20 45 22 44 21 46)(23 48 43),
(1 28 25 4)(2 26)(3 27)(7 34 31 10)(8 11)(9 12)(13 40 37 16)(17 41)(18 42)(19 22 43 46)(20 23)(21 48)(24 45)(32 35)(33 36)(44 47),
(1 16 25 40)(2 38)(3 42 27 18)(4 37 28 13)(5 41)(6 15 30 39)(7 22 31 46)(8 23 32 47)(9 45)(10 43 34 19)(11 44 35 20)(12 48)(14 26)(17 29)(21 33)(24 36).

Fixed coordinates: 0

Transitive on non-fixed coordinates: yes

Order of G: 1572864

Orbit representatives:

111111111111111111111111000000000000000000000000,
000011001111111111111111111110011000000000000000,
000101011111011111111111111101010000001000000000,
011001001111011111111111110011011000001000000000.

Bound: $A_2(24,5) \geq 17920$

Generators of G:

(1 37)(2 38)(3 39)(4 16)(5 17)(6 42)(7 43)(8 44)(9 45)(10 22)(11 47)(12 48)(13 25)
(14 26)(15 27)(18 30)(19 31)(20 32)(21 33)(23 35)(24 36)(28 40)(29 41)(34 46),
(1 8 11 25 32 35)(2 30 12)(3 31 9)(4 5 10 28 29 34)(6 36 26)(7 33 27)
(13 20 23 37 44 47)(14 42 24)(15 43 21)(16 17 22 40 41 46)(18 48 38)(19 45 39),
(1 27 25 3)(2 4)(5 8 29 32)(6 7)(9 34)(10 33)(11 36 35 12)(13 39 37 15)(14 16)
(17 20 41 44)(18 19)(21 46)(22 45)(23 48 47 24)(26 28)(30 31)(38 40)(42 43).

Fixed coordinates: 0

Transitive on non-fixed coordinates: yes

Order of G: 3072

Orbit representatives:

110111010111111111111111001000101000000000000000,
011111101101111111111111100000010010000000000000,
100000010010111111111111011111101101000000000000,
011001000111011111111111100110111000100000000000,
011101011001011111111111100010100110100000000000,
100010101001011111111111011101010110100000000000,
101001110001011111111111010110001110100000000000,
010110001110011111111111101001110001100000000000,
100000100100000111111111011111011011110000000000,
010101001011110111111111101010110100001000000000,
111011000110110111111111000100111001001000000000,
011001110010110111111111100110001101001000000000.

Bound: $A_2(24, 10) \geq 136$

Generators of G:

(1 29 6 35)(2 10 31 28)(3 32 12 33)(4 26 34 7)(5 30 11 25)(8 36 9 27)(13 47 21 48)

(14 38)(15 42 17 44)(16 22)(18 41 20 39)(19 43)(23 45 24 37)(40 46),

(1 25)(2 11 26 35)(3 28 27 4)(5 10 29 34)(6 32)(7 36 31 12)(8 30)(9 33)

(13 44 21 42)(14 15 22 48)(16 23 19 41)(17 40 47 43)(18 37 20 45)(24 38 39 46).

Fixed coordinates: 0

Transitive on non-fixed coordinates: no

Order of G: 192

Orbit representatives:

100101010010000111111111011010101101111000000000,

000110101111000110101111111001010000111001010000,

010010111001011101101101101101000110100010010010.

References

[1] E. Agrell, A. Vardy, K. Zeger, A table of upper bounds for binary codes, IEEE Trans. Inform. Theory 47 (2001) 3004–3006.

[2] M. Best, A. E. Brouwer, F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, Bounds for binary codes of length less than 25, IEEE Trans. Inform. Theory 24 (1978) 81–93.

[3] R. C. Bose, D. K. Ray-Chaudhuri, On a class of error correcting binary group codes, Inform. Contr. 3 (1960) 68–79.

[4] J. J. Cannon, D. F. Holt, The transitive permutation groups of degree 32, Exp. Math. 17 (2008) 307–314.

[5] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein, Covering codes, North-Holland, Amsterdam, 1997.

[6] K. Elssel, K.-H. Zimmermann, Two new nonlinear binary codes, IEEE Trans. Inform. Theory 51 (2005) 1189–1190.

[7] GAP – Groups, Algorithms, Programming – a System for Computational Discrete Algebra, http://www.gap-system.org/

[8] D. C. Gijswijt, H. D. Mittelmann, A. Schrijver, Semidefinite code bounds based on quadruple distances, IEEE Trans. Inform. Theory 58 (2012) 2697–2705.

[9] A. A. Hashim, V. S. Pozdniakov, Computerised search for binary linear codes, Electron. Lett. 12 (1976) 350–351.

[10] A. Hulpke, Constructing transitive permutation groups, J. Symbolic Comput. 39 (2005) 1–30.

[11] M. K. Kaikkonen, Codes from affine permutation groups, Des. Codes Cryptogr. 15 (1998) 183–186.

[12] G. A. Kabatyanskii, V. I. Panchenko, Unit sphere packings and coverings of the Hamming space, (in Russian), Probl. Peredach. Inform. 24 (1988) 3–16. English translation in: Probl. Inform. Trans. 24 (1988) 261–272.

[13] P. Kaski, P. R. J. Östergård, Classification Algorithms for Codes and Designs, Springer, Berlin, 2006.

[14] S. Litsyn, An updated table of the best binary codes known, in: V. S. Pless, W. C. Huffman, R. A. Brualdi (Eds.), Handbook of Coding Theory. Vol. I, North-Holland, Amsterdam, 1998, pp. 463–498.

[15] S. Litsyn, B. Mounits, Improved lower bounds on sizes of single-error correcting codes, Des. Codes Cryptogr. 42 (2007) 67–72.

[16] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.

[17] M. Milshtein, A new binary code of length 16 and minimum distance 3, Inform. Process. Lett. 115 (2015) 975–976.

[18] B. Mounits, T. Etzion, S. Litsyn, Improved upper bounds on sizes of codes, IEEE Trans. Inform. Theory 48 (2002) 880–886.

[19] B. Mounits, T. Etzion, S. Litsyn, New upper bounds on codes via association schemes and linear programming, Adv. Math. Commun. 1 (2007) 173.

[20] S. Niskanen, P. R. J. Östergård, Cliquer User's Guide, Version 1.0, Communications Laboratory, Helsinki University of Technology, Espoo, Finland, Tech. Rep. T48, 2003.

[21] P. R. J. Östergård, M. K. Kaikkonen, New single-error-correcting codes, IEEE Trans. Inform. Theory 42 (1996) 1261–1262.

[22] P. R. J. Östergård, T. Baicheva, and E. Kolev, Optimal binary one-error-correcting codes of length 10 have 72 codewords, IEEE Trans. Inform. Theory 45 (1999) 1229–1231.

[23] P. R. J. Östergård, Two new four-error-correcting binary codes, Des. Codes Cryptogr. 36 (2005) 327–329.

[24] P. R. J. Östergård, On the size of optimal three-error-correcting binary codes of length 16, IEEE Trans. Inform. Theory 57 (2011) 6824–6826.

[25] N. J. A. Sloane, D. S. Whitehead, New family of single-error correcting codes, IEEE Trans. Inform. Theory 16 (1970) 717–719.