# New Lower Bounds on Binary Constant Weight Error-Correcting Codes

Michael Braun
Faculty of Computer Sciences
University of Applied Sciences, Darmstadt, Germany
michael.braun@h-da.de

Joshua Humpich
Faculty of Computer Sciences
University of Applied Sciences, Darmstadt, Germany
joshua.humpich@onlinehome.de

Antti Laaksonen
Department of Communications and Networking
Aalto University School of Electrical Engineering
P.O. Box 15400, 00076 Aalto, Finland
antti.2.laaksonen@aalto.fi

Patric R. J. Östergård
Department of Communications and Networking
Aalto University School of Electrical Engineering
P.O. Box 15400, 00076 Aalto, Finland
patric.ostergard@aalto.fi

**Abstract**

Let $A(n,d,w)$ denote the maximum size of a binary code with length $n$, minimum distance $d$ and constant weight $w$. The following lower bounds are here obtained in computer searches for codes with prescribed automorphisms: $A(16,4,6) \geq 624$, $A(19,4,8) \geq 4698$, $A(20,4,8) \geq 7830$, $A(21,4,6) \geq 2880$, $A(22,6,6) \geq 343$, $A(24,4,5) \geq 1920$, $A(24,6,9) \geq 3080$, $A(24,6,11) \geq 5376$, $A(24,6,12) \geq 5558$, $A(25,4,5) \geq 2380$, $A(25,6,10) \geq 6600$, $A(26,4,5) \geq 2816$ and $A(27,4,5) \geq 3456$.

## 1 Introduction

A binary code $C$ of length $n$ is a subset of $\{0,1\}^n$. Each element $c \in C$ is called a *codeword*. The *size* of $C$ is $|C|$ and the *minimum distance* of $C$ is

$$\min_{a,b \in C, a \neq b} d_H(a,b)$$

where $d_H$ denotes the Hamming distance. The *weight* of a codeword is the number of coordinates with value 1, and in a *constant weight* code, each codeword has the same weight. A binary code with length $n$, size $M$, minimum distance at least $d$ and constant weight $w$ is called an $(n, M, d, w)$ code.

Let $A(n, d, w)$ denote the maximum size of a binary code with length $n$, minimum distance $d$ and constant weight $w$. It is difficult to determine exact values of $A(n, d, w)$, and for most parameters $n$, $d$ and $w$, only lower and upper bounds on $A(n, d, w)$ are known [1, 2, 3]. A typical way to obtain lower bounds is to discover new codes: if an $(n, M, d, w)$ code exists, then we know that $A(n, d, w) \geq M$.

In this work, automorphisms of codes are prescribed and codes that improve lower bounds on $A(n, d, w)$ are found. In [6], binary codes whose automorphism groups act transitively on (coordinate,value) pairs were systematically generated. Here similar ideas are applied to binary constant weight codes.

## 2 Search and Results

We represent a codeword $c_1 c_2 \cdots c_n$ as a set

$$\{k \in \{1, 2, \ldots, n\} \mid c_k = 1\}$$

and consider codes of the form

$$\{gw_1 \mid g \in G\} \cup \{gw_2 \mid g \in G\} \cup \cdots \cup \{gw_m \mid g \in G\}$$

where $G$ is a group of automorphisms and $w_1, w_2, \ldots, w_m$ are codewords. Consequently, a code is a union of orbits of codewords.

Consider the problem of creating an $(n, M, d, w)$ code, based on a group of automorphisms $G$, where $n$, $d$ and $w$ are fixed and $M$ should be maximized. This problem equals the problem of finding a maximum-weight clique in the following graph [5, Sect. 9.3.2]: The vertices of the graph are the orbits in which the distance between any two words is at least $d$ and each word has weight $w$. The weight of a vertex is the number of words in the corresponding orbit. There is an edge between two vertices exactly when the distance between any two words in the corresponding orbits is at least $d$.

For given parameters $n$, $d$ and $w$, we search for codes by prescribing a group of automorphisms $G$ that acts on $\{1, 2, \dots, n\}$ and use the *Cliquer* software [7] to find a maximum-weight clique in the graph obtained in the aforementioned manner. We focus on groups up to degree 28, which are available in the GAP system [4].

An $(n, M, d, w)$ code $C$ can be *shortened* in the $i$th coordinate by taking all codewords that have a 0 in the $i$th coordinate or all codewords that have a 1 in the $i$th coordinate. Cancelling the $i$th coordinate in the resulting set of codewords then yields an $(n-1, M', d, w)$ code and an $(n-1, M'', d, w-1)$ code, respectively, where $M' + M'' = M$ and $M'$ and $M''$ can be determined by inspection. It is well known [3, Eq. (5)], and can be shown by double counting, that there are always such codes with

$$M' \geq M(n-w)/n \quad \text{and} \quad M'' \geq Mw/n.$$

For the new obtained codes it was checked whether the shortened codes also yield new lower bounds. In two cases, $A(19, 4, 8) \geq 4698$ and $A(26, 4, 5) \geq 2816$, improvements are obtained.

Table 1 presents the new lower bounds found using the above approach, and the corresponding groups and orbit representatives are given in the Appendix. In three cases, $A(20, 4, 8) \geq 7830$, $A(21, 4, 6) \geq 2880$ and $A(22, 6, 6) \geq 343$, we can include additional codewords in the code, which are also listed in the Appendix.

Note that our result $A(24, 6, 12) \geq 5558$ does not improve the previous lower bound $A(24, 6, 12) \geq 5616$; however, the code that yields the better lower bound is not available any more [1].

# Appendix

**Bound:** $A(16, 4, 6) \geq 624$
**Generators of** $G$:
(1 9 16 12 4 13)(2 10 15 11 3 14)(5 8)(6 7),
(1 11)(2 12)(3 13)(4 14)(5 7)(6 8)(9 15)(10 16),
(1 12)(2 11)(3 14 6 10 15 7)(4 13 5 9 16 8)
**Order of** $G$: 48

| Old result | New result |
| --- | --- |
| $A(16,4,6) \geq 616$ [2] | $A(16,4,6) \geq 624$ |
| $A(19,4,8) \geq 4667$ [1] | $A(19,4,8) \geq 4698$ |
| $A(20,4,8) \geq 7730$ [3] | $A(20,4,8) \geq 7830$ |
| $A(21,4,6) \geq 2856$ [3] | $A(21,4,6) \geq 2880$ |
| $A(22,6,6) \geq 319$ [1] | $A(22,6,6) \geq 343$ |
| $A(24,4,5) \geq 1895$ [3] | $A(24,4,5) \geq 1920$ |
| $A(24,6,9) \geq 3041$ [3] | $A(24,6,9) \geq 3080$ |
| $A(24,6,11) \geq 5267$ [3] | $A(24,6,11) \geq 5376$ |
| $A(24,6,12) \geq 5616$ [3] | $A(24,6,12) \geq 5558$ |
| $A(25,4,5) \geq 2334$ [3] | $A(25,4,5) \geq 2380$ |
| $A(25,6,10) \geq 6036$ [3] | $A(25,6,10) \geq 6600$ |
| $A(26,4,5) \geq 2670$ [1] | $A(26,4,5) \geq 2816$ |
| $A(27,4,5) \geq 3276$ [1] | $A(27,4,5) \geq 3456$ |

Table 1: New lower bounds

**Orbit representatives:**
0111111000000000, 1010111100000000, 1110101010000000, 0111010110000000, 0011101110000000, 1101001101000000, 0110101101000000, 1001011010100000, 0110011001100000, 1011011000001000, 1011100100001000, 1110010100001000, 0101101100001000, 0101010101001000, 1100001011001000, 1000101010101000, 0100011010101000, 0001010110101000, 1100000110011000

**Bound:** $A(20,4,8) \geq 7830$
**Generators of $G$:**
(1 2)(3 5)(6 8)(9 10)(11 12)(13 15)(17 20)(18 19),
(1 6 15 16 2 9 12 17 3 7 14 18 4 10 11 19 5 8 13 20),
(1 7 15 16)(2 8 13 19)(3 9 11 17)(4 10 14 20)(5 6 12 18)
**Order of $G$:** 400
**Orbit representatives:**
11101101001100000000, 10100111101100000000, 10101110001110000000, 10110101001110000000, 01100110001111000000, 11111100001000010000, 01110111001000010000, 10101111001000010000, 10110101101000010000, 11001101101000010000, 01101011101000010000, 10011011101000010000, 11101010001100010000, 11000111001100010000, 11011000101100010000, 10001110101100010000, 00011101101100010000, 00110011101100010000, 01100100111100010000, 11000010111100010000, 01110100001110010000, 11100001001110010000, 01011001001110010000, 00110110001100011000, 10010101001100011000, 10001011001100011000, 01010100101100011000,

11000101001010011000, 00011101001010011000
**Additional codewords:**
11111011100000000000, 11110111010000000000, 11101110110000000000,
01111101110000000000, 10011111110000000000, 11011000001111000000,
00000110111111000000, 10111000001110100000, 00000101111110100000,
01111000001101100000, 00000011111101100000, 11111000000011100000,
00000111110011100000, 11100000001111100000, 00000111001111100000,
11011000000000011110, 00000110110000011110, 00000000001101111110,
10111000000000011101, 00000101110000011101, 00000000001011111101,
01111000000000011011, 00000011110000011011, 00000000000111111011,
11111000000000000111, 00000111110000000111, 00000000001111100111,
11100000000000011111, 00000111000000011111, 00000000001110011111

**Bound:** $A(19, 4, 8) \geq 4698$
**Construction:** Shortening the $(20, 7830, 4, 8)$ code in coordinate 1

**Bound:** $A(21, 4, 6) \geq 2880$
**Generators of** $G$**:**
(1 2)(4 5)(7 8)(10 11)(13 14)(16 17)(19 20),
(1 10 4)(2 12 5 3 11 6)(7 13 16)(8 15 17 9 14 18)(20 21),
(1 5 18)(2 6 16)(3 4 17)(7 8 9)(10 20 15)(11 21 13)(12 19 14)
**Order of** $G$**:** 126
**Orbit representatives:**
110110110000000000000, 011100111000000000000,
001111010100000000000, 010101110100000000000,
111000011100000000000, 100011011100000000000,
100100111100000000000, 110110000110000000000,
101100100110000000000, 110000110110000000000,
111100100000100000000, 110101010000100000000,
001011110000100000000, 100011100100100000000,
010011010100100000000, 001100110100100000000,
010110100010100000000, 011100010010100000000,
100100101010100000000, 100010010110100000000,
001001010110100000000, 010001001110100000000,
001010100011100000000, 100001010011100000000,
010100010100110000000, 101000001100110000000,
010100001010100100000, 100100001100010100000,
010001001100010100000
**Additional codewords:**
000100100100100100100, 000010010010010010010,
000001001001001001001

**Bound:** $A(22,6,6) \geq 343$
**Generators of** $G$**:**
(2 9 6)(3 20 14)(4 16 15)(7 10 11)(8 17 12)(19 22 21),
(2 9)(3 20)(4 16)(5 13)(7 10)(8 21)(12 19)(17 22)
**Order of** $G$**:** 6
**Orbit representatives:**
0100000000010000111010, 0010010000010000011100,
0100001000000100101100, 0001000100010100001100,
1010001000011000001000, 0000011001010100001000,
1010000101000100001000, 0100000010110010001000,
1001000110000010001000, 1000100100001001001000,
0010011100000001001000, 0101000000000011101000,
0000001001001010101000, 0010010000100100101000,
0000000110001100101000, 0011100000001000101000,
1000000010010001101000, 0000001111100000001000,
1100000001100000101000, 1010001000100101000000,
0010000100011011000000, 0111000001000100100000,
1000010000100110010000, 0011010011100000000000,
1010100000001100000100, 1101010001000010000000,
1100001100100010000000, 0001000000110001011000,
0001011000011010000000, 0000010000010011110000,
0001010101000000101000, 0110000100001000011000,
0000101101000101000000, 0010000110100110000000,
0101100110000100000000, 0011000001010010001000,
0110000000111100000000, 1011010000001010000000,
0000100000011010011000, 0010110101010000000000,
0000010110010101000000, 1100000111010000000000,
0000100110111000000000, 1010100010010010000000,
0010100100100001010000, 1010010001000000110000,
0110101010100000000000, 0100101100010000001000,
0100010000011001001000, 1011000100101000000000,
0011000000000111000100, 0000000000111000101100,
0001100011001010000000, 1000000100110000001010,
0010001000010110010000, 1100010100001100000000,
1001001100010001000000, 0100110010001000010000,
1000101001101000000000, 0100001101000000110000,
0111100000010001000000, 0101010000100000110000,
1000000100011000110000, 0001011001000001010000,
0010001000101000110000, 0010001001010001100000,
0100000000001110110000, 0011101100000010000000,
0000000100100010111000, 0110010000000101010000,
0100010110000000001100, 0000011010000000111000,
0000000100000001101110

**Additional codewords:**
100100000000010110100000, 100100000000000100111000,
100000010000000010010110, 100000000000101010100001

**Bound:** $A(24,4,5) \geq 1920$
**Generators of** $G$**:**
(1 8 13 19 2 7 14 20)(3 6 21 23 4 5 22 24)(9 12 16 18 10 11 15 17),
(1 16 8 4)(2 15 7 3)(5 23 6 24)(9 20 21 14)(10 19 22 13)(11 12)(17 18)
**Order of** $G$**:** 96
**Orbit representatives:**
101011001000000000000000, 111000101000000000000000,
100101011000000000000000, 100001101100000000000000,
010011100010000000000000, 010101010010000000000000,
000011011010000000000000, 000101100110000000000000,
110001100000100000000000, 010110010000100000000000,
101001010000100000000000, 011010001000100000000000,
010001011000100000000000, 100010010100100000000000,
010100001000110000000000, 010110001000001000000000,
110000011000001000000000, 110010000100001000000000,
010100100100001000000000, 000000101101001000000000,
100001000100101000000000, 011000000100001100000000

**Bound:** $A(24,6,9) \geq 3080$
**Generators of** $G$**:**
(1 12 13)(2 11 14)(3 10 8)(4 9 7)(5 19 21)(6 20 22)(15 24 17)(16 23 18),
(1 11 16 14 18 5 2 12 15 13 17 6)(3 9 23 22 7 20 4 10 24 21 8 19)
**Order of** $G$**:** 1320
**Orbit representatives:**
101100111101100000000000, 011110011011100000000000,
011011101010010010000000

**Bound:** $A(24,6,11) \geq 5376$
**Generators of** $G$**:**
(4 8 13)(5 9 14)(6 7 15)(16 22 20)(17 23 21)(18 24 19),
(1 7 23)(2 8 24)(3 9 22)(4 6 5)(10 19 17)(11 20 18)(12 21 16)(13 15 14)
**Order of** $G$**:** 504
**Orbit representatives:**
111110011110110000000000, 001111101111100100000000,
110011110111001100000000, 111101001101011100000000,
101101110011011100000000, 110101001111100100100000,
110101110001110100100000, 111100010110101100100000,

0011100110111101100100000, 1011011000011011110100000,
1110011010011001001001100, 1011010101010101001001100,
0100011011101101001001100, 0110110100110011001001100

**Bound:** $A(24, 6, 12) \geq 5558$
**Generators of** $G$**:**
(1 22 16)(2 23 17)(3 24 18)(7 12 15)(8 10 13)(9 11 14),
(1 2 3)(4 5 6)(7 8 9)(10 11 12)(13 14 15)(16 17 18)(19 20 21)(22 23 24),
(1 24 2 22 3 23)(4 7 5 8 6 9)(10 15 11 13 12 14)(16 19 17 20 18 21),
(1 10 22 8 13 20 16)(2 11 23 9 14 21 17)(3 12 24 7 15 19 18)
**Order of** $G$**:** 504
**Orbit representatives:**
000111111111111000000000, 111111110010101000000000,
111011110101101100000000, 110101101011101110000000,
110101101101110100100000, 011010111101110100100000,
011101110011110100100000, 110101110111001100100000,
001001111111011100100000, 100011110011111100100000,
101101110101110010100000, 011100111101010101000000,
110100111101011010100000, 111001111001100100100100,
101010011111100100100100, 100101011110110100100100,
101101010101011100100100, 100110101011011100100100,
001010111010111100100100

**Bound:** $A(25, 4, 5) \geq 2380$
**Generators of** $G$**:**
(6 8 10 7 9)(11 15 14 13 12)(16 17 18 19 20)(21 24 22 25 23),
(1 2 3 4 5)(6 10 9 8 7)(11 13 15 12 14)(21 24 22 25 23),
(1 6 13 19 24)(2 7 14 20 25)(3 8 15 16 21)(4 9 11 17 22)(5 10 12 18 23)
**Order of** $G$**:** 125
**Orbit representatives:**
1111100000000000000000000, 1000011100100000000000000,
0110010000110000000000000, 0001010100110000000000000,
0101010000101000000000000, 0010011000101000000000000,
0101110000000001000000000, 1000111000000001000000000,
0001011010000001000000000, 1001100000100001000000000,
0010110000100001000000000, 1100001000100001000000000,
1010000010100001000000000, 1000000101100001000000000,
0100000010110001000000000, 0010000001101001000000000,
1000010100000001100000000, 0100100000100001100000000,
1000010000100001000010000, 0010001000001001000010000

**Bound:** $A(25, 6, 10) \geq 6600$
**Generators of** $G$**:**
(2 12 17 15 19 6 3 13 16 14 18 7)(4 10 24 23 8 21 5 11 25 22 9 20),
(2 21 12)(3 20 13)(4 18 14)(5 19 15)(6 11 9)(7 10 8)(16 25 23)(17 24 22)
**Order of** $G$**:** 1320
**Orbit representatives:**
1101111010110100000000000, 0101011011011110000000000,
1011110100101100010000000, 0101110111010010010000000,
0110110010101100110000000

**Bound:** $A(27, 4, 5) \geq 3456$
**Generators of** $G$**:**
(1 23 18)(2 24 16)(3 22 17)(4 26 12)(5 27 10)(6 25 11)(7 20 15)(8 21 13)(9 19 14),
(1 3 2)(4 6 5)(7 9 8)(10 12 11)(13 15 14)(16 18 17)(19 21 20)(22 24 23)(25 27 26),
(1 7 4)(2 8 5)(3 9 6)(10 16 13)(11 17 14)(12 18 15)(19 25 22)(20 26 23)(21 27 24)
**Order of** $G$**:** 27
**Orbit representatives:**
100000000111000000100000000, 001010000100100000100000000,
000001010100100000100000000, 000011100000100000100000000,
010000010000110000100000000, 001000000101010000100000000,
000001100100010000100000000, 000010010100010000100000000,
001100000000011000100000000, 000010001000101000100000000,
100000000001101000100000000, 001000100001001000100000000,
000011000010001000100000000, 000001001110000000100000000,
000000001001001100100000000, 010000000000101100100000000,
010000000001010100100000000, 000100100000100100100000000,
000010010000100100100000000, 001100000001000100100000000,
000000100101000100100000000, 010100000001000100100000000,
000001100010000100100000000, 100000011110000000000000000,
001000000100110000100000000, 010001010001100000000000000,
000100010001110000000000000, 000100100001001100000000000,
001001000011000000100000000, 000100100010110000000000000,
000000001010100001100000000, 100010000100110000000000000,
000000100001111000000000000, 001100000000100001100000000,
110000000110010000000000000, 100001000100001100000000000,
110011000100000000000000000, 000010001010000100100000000,
100000010011100000000000000, 010000000011001000100000000,
000010010000001010100000000, 000010010011000000100000000,
100000100110100000000000000, 101000000101010000000000000,
010001001010100000000000000, 000010001110100000000000000,
000100000100100010100000000, 000000110001000010100000000,
101001000110000000000000000, 000110101100000000000000000,

001000011100100000000000000, 001000001010001100000000000,
000000100000011100100000000, 100100000100010000100000000,
000101000000010001100000000, 100101001100000000000000000,
110000000010011000000000000, 000111010100000000000000000,
000101000110100000000000000, 010001001000000001100000000,
010000001000011000100000000, 000100000010001001100000000,
000000110010100001000000000, 101000000001110000000000000,
011011100000000000000000000, 110100100100000000000000000,
010000000101000001100000000, 010010100000000010100000000,
001001010010100000000000000, 000000101101100000000000000,
000000010001000101100000000, 000000010001101100000000000,
110000000000000110100000000, 100011000001100000000000000,
000100000010010110000000000, 001000000100000101100000000,
001000100100000010100000000, 001010000011100000000000000,
001000100100110000000000000, 000100000000000111100000000,
001000000100011100000000000, 110000000000100001100000000,
010000000010010001100000000, 000000010000010011100000000,
010001010110000000000000000, 000000001100010001100000000,
100001000001000001100000000, 010010010000000001100000000,
000100110100100000000000000, 101000010000000001100000000,
010001100100100000000000000, 000100011000000001100000000,
000100010110000000100000000, 000100100100001000100000000,
000011000100000001100000000, 001000010010001000100000000,
001010000010000001100000000, 011000011100000000000000000,
000100100001000001100000000, 100000000010110000100000000,
010001000100001000100000000, 100000100000010001100000000,
000110000010100000100000000, 000000001010010010100000000,
110010000010100000000000000, 000001010000001001100000000,
100000000010000101100000000, 100001000100000010100000000,
000000110000101000100000000, 101000000001000010100000000,
000000101000000101100000000, 001000000000001011100000000,
000000100000100011100000000, 000001000010000011100000000,
100000001100000100100000000, 011000000010000010100000000,
100010000000000011100000000, 101000000000010100100000000,
001011000000000010100000000, 010100000101100000000000000,
100000100010000010100000000, 010001000001000010100000000,
000000010010100010100000000, 010000001000100010100000000,
000110000000010010100000000, 000000001100001010100000000,
010100000000001010100000000, 000000010100000110100000000

**Bound:** $A(26, 4, 5) \geq 2816$
**Construction:** Shortening the $(27, 3456, 4, 5)$ code in coordinate 1

## References

[1] Brouwer, A. E. Bounds for binary constant weight codes. Online tables available at https://www.win.tue.nl/~aeb/codes/Andw.html

[2] Brouwer, A. E., Etzion, T. (2011). Some new distance-4 constant weight codes. Adv. Math. Commun. 5, 417–424.

[3] Brouwer, A. E., Shearer, J. B., Sloane, N. J. A., Smith, W. D. (1990). A new table of constant weight codes. IEEE Trans. Inform. Theory 36, 1334–1380.

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

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

[6] Laaksonen, A., Östergård, P. R. J. (2017). Constructing error-correcting binary codes using transitive permutation groups. Discrete Appl. Math. 233, 65–70.

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