university of groningen

faculty of mathematics
and natural sciences

Automorphism groups of cyclic codes

A.R.F. Everts

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$$

$$(12)(56)$$

$$(15)$$

Bachelor Thesis in Mathematics

August 28, 2009

Automorphism groups of cyclic codes

Summary

Codes are used to store and send information. In this thesis we discuss binary codes, which can be seen as subsets of $\mathbb{F}_2^n$. Permuting the coordinates of a code results in an equivalent code, which shares a lot of the same properties with the original code. The automorphism group of a binary code consists of all permutations that map a code back to itself. An automorphism group of a code gives information about the structure of the code, but it is difficult to determine.

In this thesis we prove that the automorphism group of the Hamming code of length $n = 2^m - 1$ is isomorphic to $GL(m, 2)$. Next, we consider some transitive subgroups of S_n and discuss whether they can occur as an automorphism group of a cyclic code of length n. We also give an application of automorphism groups to the minimum weight of a code. In the last chapter, we use coding theory to prove a theorem about permutation groups.

Bachelor Thesis in Mathematics

Author: A.R.F. Everts
Supervisor: Prof. dr. J. Top

Date: August 28, 2009

Institute of Mathematics and Computing Science
P.O. Box 407
9700 AK Groningen
The Netherlands

Contents

Chapter 1

Introduction

To send information you can encode it into a sequence of symbols, for example braille, morse, or smoke signals. Sometimes it is important that the message is unreadable for outsiders, which is when encryption comes into play. In coding theory, however, it is not about the secrecy but about the correctness of a received message, since some parts might get changed during the transportation of the message. For this reason, there are often more symbols sent than strictly needed. This way you can notice small errors and sometimes even correct them. Codes that have this last property are called *error-correcting* codes. An example is the Reed-Solomon code. This code is used on music CDs to correct reading errors[1].

Mixing the coordinates of a code C will give a new code, which shares a lot of the same properties with the original code. Some of these permutations map the code back to itself, that is, every code word in C is mapped to a (possibly different) code word in C. For binary codes, these permutations form the automorphism group of the code. This group gives some information about the structure of the code. However, even though you can find it with a brute force method, it is not easy to determine this automorphism group.

It has already been established that every finite group is isomorphic to the automorphism group of some perfect binary code[9]. In this thesis we will consider the automorphism groups of cyclic binary codes. After an introduction to coding theory and automorphism groups, we will prove that the automorphism group of the Hamming code of length $n = 2^m - 1$ is isomorphic to $GL(m, 2)$. Then we will see some subgroups of S_n that can be found as the automorphism group of a cyclic code and some that can not. Furthermore, we give an application of automorphism groups to the minimum weight of a code. In the last chapter, we use coding theory to prove a theorem about permutation groups.

Chapter 2

Introduction to coding theory

In coding theory, a code C is a non-empty subset of a vectorspace V over a finite field K. V exists of all possible vectors of length n with symbols from K. When a vector $a = (a_0, a_1, \ldots, a_{n-1})$ is contained in C we call it a code word. The symbols $a_0, \ldots, a_{n-1}$ are referred to as the coefficients of a. Only binary codes are discussed in this thesis, although there are more general forms of the codes that we discuss. So from now on, V is equal to $\mathbb{F}_2^n$. In other words, a code word is a sequence of zeros and ones.

In the next paragraph, we will introduce some basic definitions and theorems of coding theory. For a more extensive explanation, the reader can refer to [1], [2] or [8].

2.1 Definitions

The *Hamming distance* $d_H(a, b)$ between two code words a and b is defined as the number of coefficients for which two code words differ. For example, the Hamming distance between $(0, 1, 1, 1)$ and $(1, 0, 1, 1)$ is equal to 2. The *weight* w of a code word a is the number of nonzero coefficients of a.

The *minimum Hamming distance* d of a code C is defined as:

$$d = \min\{d_H(a, b) : a, b \in C \ \& \ a \neq b\}.$$

The bigger the minimum distance, the better a code can detect errors. A code with minimum distance d can detect errors that involve up to $d - 1$ bits and can correct errors involving up to $(d - 1)/2$ bits.

A code C is *linear* if C is a k-dimensional subspace of $\mathbb{F}_2^n$, and is referred to as a $[n, k]$-code. This means that the sum of two code words from C is also a code word in C. Since C is a subspace, there exists a basis $\{v_1, v_2, \ldots, v_k\}$ for C such that each code word a in C can be written uniquely as $a = \alpha_1 v_1 + \ldots + \alpha_k v_k$, with $\alpha_i \in \mathbb{F}_2$. These linear independent vectors form the rows of the $k \times n$ *generator matrix* M. A vector $v \in \mathbb{F}_2^n$ is a code word of C if and only if there exists a row vector $\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{F}_2^k$ such that $\alpha M = \alpha_1 v_1 + \ldots + \alpha_k v_k = v$.

The *weight distribution* of a linear code is the sequence of numbers

$$A_t = \#\{a \in C \mid w(a) = t\},$$

where each A_t gives the number of codewords a in C that have weight t, with t ranging from 0 to n. These A_t are the coefficients of the bivariate polynomial

$$W(C; x, y) = \sum_{w=0}^{n} A_w x^w y^{n-w},$$

which is called the *weight enumerator*.

On $\mathbb{F}_2^n$ exists the symmetric bilinear form $\langle \cdot, \cdot \rangle$, which maps two code words $a = (a_0, \ldots, a_{n-1})$ and $b = (b_0, \ldots, b_{n-1})$ from $\mathbb{F}_2^n \times \mathbb{F}_2^n$ to an element of $\mathbb{F}_2$:

$$\langle a, b \rangle := \sum_{i=0}^{n-1} a_i b_i \bmod 2.$$

Now we can define the dual code $C^\perp$ of a $[n, k]$-code C:

$$C^\perp = \{b \in \mathbb{F}_2^n : \forall a \in C, \langle a, b \rangle = 0\}.$$

This dual code is a $[n, n-k]$ code, and it is linear, even when C is not. When C is linear, then it holds that $(C^\perp)^\perp = C$. With the *MacWilliams identity*[8], we can find the weight enumerator of the dual of the code:

$$W(C^\perp; x, y) = \frac{1}{\mid C \mid} W(C; y - x, y + x).$$

A *cyclic* code is a linear code with the property that for every $a = (a_0, a_1, \ldots, a_{n-1}) \in C$ the word $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ is also a code word of C. A cyclic code can be seen as an ideal in $\mathbb{F}_2[x]/(x^n - 1)$, as explained in the next theorem, which is based on theorems 2.1.3 and 2.1.4 in [1].

Theorem 1. *Every cyclic $[n, k]$-code $C \subset \mathbb{F}_2^n$ is isomorpic to an ideal $\hat{C}$ in $\mathbb{F}_2[x]/(x^n - 1)$, with $\hat{C} = (f)$ for a certain* generator polynomial *$f \in \mathbb{F}_2[x]$ with $f(x)|x^n - 1$ and $deg(f) = n - k$.*

A code word $a = (a_0, \ldots, a_{n-1}) \in C$ corresponds to the polynomial $g(x) = a_0 + a_1 x_1 + \ldots + a_{n-1} x^{n-1}$ in $\hat{C}$. We see that multiplying $g(x)$ with x corresponds to shifting the coefficients of a cyclic to the right. Both representations of a cyclic code will be used in this thesis.

The dual code of a cyclic code is also cyclic, so it has a generator polynomial $h(x)$. This $h(x)$ satisfies $h^*(x)f(x) = x^n - 1$, where $h^*(x) = x^{deg(h)} h(1/x)$ is the *reciprocal polynomial* of $h(x)$, see for a proof pages 11-13 of [1].

2.2 Examples of codes

1. The *zero code*, consisting only of the zero word $(0, 0, \ldots, 0)$, has by definition dimension 0 and minimum distance n.

2. The code $\mathbb{F}_2^n$ consists of all possible binary vectors of length n and is the dual of the code from example 2.2.1. It has dimension n, but the minimum weight is only 1.

3. The *repetition code*, $\mathbb{F}_2 \cdot (1, 1, \ldots, 1)$, has dimension 1, but the minimum distance is n.

4. The *even weight code* consists of all words in F_2^n with an even number of ones, so the minimum weight is 2. This code is the dual of the repetition code, so therefore it has dimension $n - 1$.

5. A code can be extended by adding a *parity bit*. This bit is equal to 1 if the sum of the other bits is odd, otherwise it is 0. So every code word of this extended code is of even weight, hence the extended code is a subcode of an even weight code.

6. A *block repetition code* is a cyclic code with a generator $f(x)$ that can be written as $f(x) = (1+x^l+x^{2l}+\ldots+x^{n-l})h(x)$ with $h(x)|x^l-1$, $l|n$ and $l < n$. Each code word exists of n/l identical blocks of length l, hence the minimum distance is at least n/l. The dimension is equal to $l - deg(h)$, which is smaller than $\frac{1}{2}n$.

2.3 Hamming code

In 1950, Richard Hamming published a code that is nowadays known as the Hamming code. This code can detect errors that involve up to 2 bits and correct errors that involve 1 bit. There are Hamming codes of different lengths, but the Hamming code of length 7 is the most wellknown. For $m \geq 1$ we construct the general Hamming code of length $n = 2^m - 1$ as follows.

Consider $G = \mathbb{F}_{2^m}^*$, this is a cyclic group [5], so there exists a $\alpha \in G$ such that $G = \langle\alpha\rangle$. Consider the minimum polynomial f of α over $\mathbb{F}_2$, which has degree m. The Hamming code H of length $n = 2^m - 1$ is a subset of $\{h \in \mathbb{F}_2[x] : \ deg(h) \leq n-1\}$ and is defined as follows[1]:

$$H = (f) = \{gf \ : \ g \in \mathbb{F}_2[x] \ \& \ deg(g) \leq n-m-1\}.$$

We see that the dimension of the Hamming code is $n - m$. There are many equivalent ways to define the Hamming-code:

$$\begin{aligned} H &= \{h \in \mathbb{F}_2[x] : \ f|h \ \& \ deg(h) \leq n-1\} \\ H &= \{h \in \mathbb{F}_2[x] : \ h(\alpha) = 0 \ \& \ deg(h) \leq n-1\} \\ H &= \{(a_0, \ldots, a_{n-1}) \in \mathbb{F}_2^n : \ a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} = 0\} \end{aligned}$$

You can also view the Hamming code as a subset of the group ring $\mathbb{F}_2[G]$. An element $a \in \mathbb{F}_2[G]$ is equal to a formal sum: $a = a_0g_0 + \ldots + a_{n-1}g_{n-1}$, with $g_i = \alpha^i$ for $i = 0, 1, \ldots, n-1$. We can now define:

$$H = \{x \in \mathbb{F}_2[G] : \ \sum_{i=0}^{n-1} a_i g_i = 0\},$$

where the sum on the right side is a normal sum.

The Hamming code can be extended by adding a parity bit to it. This *extended Hamming code*, $\tilde{H}$, can be seen as a subset of $\mathbb{F}_2[\mathbb{F}_{2^m}]$, wherein an element g is given by the formal sum $a_0 g_0 + \ldots + a_n g_n$, with $g_i = \alpha^i$ for $i = 0, 1, \ldots, n-1$ and $g_n = 0$:

$$\tilde{H} = \{y \in \mathbb{F}_2[\mathbb{F}_{2^m}] : \sum_{i=0}^{n} a_i = 0 \ \& \ \sum_{i=0}^{n} a_i g_i = 0\}.$$

2.4 BCH codes

Cyclic codes can also be described by the zeros of the generator polynomial. For the BCH codes, we choose these zeros in such a way that we have a lower bound for the minimum distance. These codes were invented independently by R.C. Bose and D.K. Ray-Chaudhuri in 1960 and by A. Hocquenghem in 1959[10]. The *BCH* codes are well-known for their good error-correcting properties when the code is not too long.

Definition 1. Let α be such that $\mathbb{F}_{2^m}^* = \langle \alpha \rangle$ and take $2 \leq \delta \leq n$, $m \geq 1$ and $0 \leq b \leq n$. Let $m_i(x)$ be the minimal polynomial of α^i over $\mathbb{F}_2$. Let $g(x)$ be the monic polynomial of lowest degree over $\mathbb{F}_2$ that has $\alpha^b, \ldots, \alpha^{b+\delta-2}$ among its zeros, that is,

$$g(x) = \operatorname{lcm}(m_b(x), \ldots, m_{b+\delta-2}(x)).$$

The $BCH(m, \delta, b)$ code of length $n = 2^m - 1$ is the code generated by $g(x)$. When $b = 1$, the $BCH(m, \delta, 1)$ code is called a *narrow sense BCH* code.

It is a well-known theorem that the minimum distance of the $BCH(m, \delta, b)$ code is at least δ, which is refered to as the *designed distance*, see theorem 8.1.1 in [10]. The actual minimum distance can be greater than δ.

The generator polynomial of $BCH(m, 2, 1)$ is equal to the minimal polynomial $h(x)$ of α over $\mathbb{F}_2$, so this code is equal to the Hamming code. With the Frobenius homomorphism we find that $h(\alpha^2) = h(\alpha)^2 = 0$, so α^2 is automatically a zero of $h(x)$ too. Hence, the $BCH(m, 3, 1)$ code is also equal to the Hamming code, and we conclude that the Hamming code has a minimum distance of at least 3.

Like the Hamming code, you can view a $BCH(m, \delta, 1)$ code as a subset of the group ring $\mathbb{F}_2[G]$ with $G = \mathbb{F}_{2^m}^*$. For example, for $\delta = 4$, the $BCH(m, 4, 1)$ code is given by

$$BCH(m, 4, 1) = \{x = \sum_{i=0}^{n-1} a_i \alpha^i \in \mathbb{F}_2[G] : \sum_{i=0}^{n-1} a_i \alpha^i = 0 \ \& \ \sum_{i=0}^{n-1} a_i \alpha^{3i} = 0\}.$$

Because $\delta = 4$, we know that the minimum distance is at least 4. Again with the Frobenius homomorphism, we find that α^4 is also a zero of the generator polynomial of this code. So this code is equal to the $BCH(m, 5, 1)$ code, and thus the minimum distance is at least 5.

Chapter 3

The automorphism group of a code

Let C be a binary code of length n. Mixing the coordinates of the code gives a new code, which shares many of the same properties with C, like the minimum weight and the weight enumerator. Some of these permutations of coordinates send C into itself: all code words of C are mapped to (possibly different) code words in C. These permutations together form the *automorphism group* of C, denoted by $Aut(C)$:

$$Aut(C) = \{\pi \in S_n : \pi(C) = C\}.$$

This is a subgroup of S_n, with composition of functions as operation and the identity function as the identity element.

In this thesis, we denote with (ij) the permutation that permutes the coefficients a_i and a_j of a $a = (a_0, a_1, \ldots, a_{n-1}) \in C$. So, unlike what is common in algebra, the numbers $0, 1, \ldots, n-1$ can occur in the representation of a permutation. For a code word $a = (a_0, \ldots, a_{n-1})$ and a permutation π, we define $\pi(a)$ as

$$\pi(a) = (a_{\pi(0)}, a_{\pi(1)}, \ldots, a_{\pi(n-1)}).$$

3.1 Examples

1. The automorphism groups of $\mathbb{F}_2^n$, the even weight code, the repetition code and the zero code are equal to S_n. For each of these codes, it is easy to see that each permutation $\pi \in S_n$ maps a code word again to a code word.

2. Let C be a code of length n, with n prime. If $Aut(C)$ contains a 2-cycle τ and a n-cycle σ, then $Aut(C)$ is equal to S_n. In theorem 6 we will see that this means that C is one of the codes mentioned in example 3.1.1.

   Proof. By renaming the coefficients we can say without loss of generality that $\tau = (01)$. Since n is prime, all powers σ^i of σ, with $1 \leq i \leq n-1$, are again n-cycles. So there is a power i of σ such that $\sigma^i = (01\ldots)$. By renaming the rest of the coordinates, we can say that $\sigma = (01\ldots n-1)$. Since $Aut(C)$ is a group, it also contains $\sigma\tau\sigma^{-1} = (12)$, $\sigma(12)\sigma^{-1} = (23)$, ..., $(n-2, n-1)$. These 2-cycles generate S_n.[7] □

For n not prime this does not necessarily hold. For example, consider the block repetition code generated by $1 + x^4$ in $\mathbb{F}_2[x]/(x^8 - 1)$. The automorphism group of this code contains (04) and (01 . . . 7), but not the permutation (01), so it does not contain all of S_n.

3. For a linear code C, it holds that C and $C^\perp$ have the same automorphism group.

   Proof. Let $\pi \in Aut(C)$. For a code word $b \in C^\perp$ holds $\langle b, a\rangle = \sum_{i=0}^{n-1} a_i b_i = 0$ for all $a \in C$, so also

   $$\langle \pi(b), \pi(a)\rangle = \sum_{i=0}^{n-1} a_{\pi(i)} b_{\pi(i)} = \sum_{i=0}^{n-1} a_i b_i = 0,$$

   for all a in C. Since $\pi(C) = C$, this means that $\pi(b)$ is perpendicular to every $a \in C$. So $\pi(b)$ is an element of $C^\perp$, hence $Aut(C) \subset Aut(C^\perp)$.

   Since C is linear, it holds that $(C^\perp)^\perp = C$, hence $Aut(C^\perp) \subset Aut((C^\perp)^\perp) = Aut(C)$. So $Aut(C) = Aut(C^\perp)$. □

4. The automorphism group of the linear code $C = \{(0000), (1100), (0011), (1111)\}$ consists of 8 elements[10]:

   $$Aut(C) = \{id, (01), (23), (01)(23), (02)(13), (03)(12), (0213), (0312)\}.$$

5. A permutation τ maps a code C to an equivalent code $\hat{C}$, and the automorphism group of $\hat{C}$ is equal to

   $$Aut(\hat{C}) = \{\tau\pi\tau^{-1} \ : \ \pi \in Aut(C)\}.$$

Chapter 4

The map ϕ

Consider a linear $[n,k]$-code C with generator matrix M and a permutation $\pi \in Aut(C)$. For every basis vector v_i of C, $\pi(v_i)$ can be expressed as a linear combination of the basis vectors of C:

$$\pi(v_i) = b_{i1}v_1 + b_{i2}v_2 + \ldots + b_{ik}v_k.$$

These b_{ij} together form the invertible $k \times k$ matrix B_π. The generator matrix of the code $\pi(C)$ is given by $B_\pi M$. The permutation π can be seen as a linear map from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ that permutes the basis vectors. Let A_π be the transpose of the $n \times n$ permutation matrix that belongs to this map. So A_π mixes the columns of M in the same way as π does, hence A_π satisfies $B_\pi M = MA_\pi$.

The map ϕ maps a permutation $\pi \in Aut(C)$ to the inverse of the matrix $B_\pi \in GL(k,2)$:

$$\phi(\pi) = B_\pi^{-1}. \tag{4.1}$$

For every $\pi_1, \pi_2 \in Aut(C)$ it holds that $A_{\pi_1 \circ \pi_2} = A_{\pi_2}A_{\pi_1}$. So

$$MA_{\pi_1 \circ \pi_2} = MA_{\pi_2}A_{\pi_1} = B_{\pi_2}MA_{\pi_1} = B_{\pi_2}B_{\pi_1}M,$$

and hence

$$\phi(\pi_1 \circ \pi_2) = (B_{\pi_2}B_{\pi_1})^{-1} = B_{\pi_1}^{-1}B_{\pi_2}^{-1} = \phi(\pi_1)\phi(\pi_2).$$

So the map ϕ is a group homomorphism. If ϕ is injective, then the automorphism group of the code C is isomorphic to a subgroup of $GL(k,2)$.

4.1 Injectivity of ϕ

We want to know for which codes the map ϕ is injective. We will prove that for cyclic codes this is the case if and only if the code is not a block repetition code, see theorem 2.

Consider a linear code C for which ϕ is not injective. This means that there is a $\pi \in Aut(C)$, $\pi \neq id$, with the property that $\phi(\pi) = I_k$, so $\pi(a) = a$ for every code word a in C. Suppose that this π puts the coordinate i on place j. Then, for every a, the coefficients a_i and a_j have to be equal, since $\pi(a) = a$. Hence the $(i+1)$-th and $(j+1)$-th columns of the generator matrix are equal. This means that the 2-cycle (ij) is contained in $Ker(C)$. We summarize this in the next lemma.

Lemma 1. *Let C be a linear code. If the map ϕ is not injective for C, then there is a 2-cycle (ij) in $Ker(\phi)$. This means that at least two columns of the generator matrix of C are equal.*

Now we will look at the injectivity of ϕ for cyclic codes.

Lemma 2. *Let C be a cyclic $[n,k]$-code and let σ be the n-cycle $(01\dots n-1)$. If the map ϕ from $Aut(C)$ to $GL(k,2)$ is not injective, then there is a $d \in \{1,\dots,n-1\}$ with $d|n$ such that σ^d is contained in $Ker(\phi)$.*

Proof. From lemma 1 we know that if ϕ is not injective, then there is a 2-cycle $(i, i+a)$ in $Ker(\phi)$. So for every $g(x) = b_0 + b_1x + \dots + b_{n-1}x^{n-1}$ in C it holds that $b_i = b_{i+a}$. Since C is cyclic, also $\sigma^{i-j}(g)$ is a code word of C for every j, so its i-th and $(i+a)$-th coefficients have to be equal. This means $b_j = b_{(j+a) \ mod \ n}$ for every $g(x)$ in C and $j = 0, 1, \dots, n-1$.

The permutation σ^a maps a $g(x) \in C$ to

$$\begin{aligned} x^a g(x) &= b_0x^a + b_1x^{a+1} + \ldots + b_{n-1}x^{n-1+a} \bmod x^n - 1 \\ &= b_{n-a} + \dots + b_{n-1}x^{a-1} + b_0x^a + b_1x^{a+1} + \ldots + b_{n-a-1}x^{n-1} \bmod x^n - 1 \\ &= g(x). \end{aligned}$$

We see that $\sigma^a(g) = g$, so σ^a is contained in $Ker(\phi)$.

Let $d = gcd(a,n)$, then there are $q, r \in \mathbb{Z}$ such that $d = qa + rn$ and thus

$$\sigma^d = \sigma^{qa+rn} = (\sigma^a)^q(\sigma^n)^r = (\sigma^a)^q.$$

So σ^d is in $Ker(\phi)$, and d satisfies $1 \le d \le a < n$ and $d|n$. This proves the lemma. □

Lemma 3. *Let C be a cyclic $[n,k]$-code with generator $f(x)$ and let σ be the n-cycle $(01\dots n-1)$. $Ker(\phi)$ contains σ^l for a l that satisfies $0 < l < n$ and $l|n$, if and only if $f(x)$ can be written as*

$$f(x) = \sum_{i=0}^{m-1} (x^l)^i g(x),$$

with $g(x)|x^l - 1$, $n = ml$ and $m \ge 2$.

Proof. (⇒) Suppose $f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$. If $\sigma^l \in Ker(\phi)$, then

$$f = x^l f = x^{2l} f = \ldots = x^{(m-1)l} f.$$

Consequently

$$\begin{aligned} a_0 &= a_l = a_{2l} = \ldots = a_{(m-1)l}, \\ a_1 &= a_{l+1} = a_{2l+1} = \ldots = a_{(m-1)l+1}, \\ \dots & \\ a_{l-1} &= a_{2l-1} = a_{3l-1} = \ldots = a_{n-1}. \end{aligned}$$

Now, define $g(x) = a_0 + a_1x + \ldots a_{l-1}x^{l-1}$, then $f(x) = (1 + x^l + \ldots + x^{(m-1)l})g(x)$. Since

$$f(x)|x^n - 1 = (1 + x^l + \ldots + x^{n-l})(x^l - 1)$$

we see that $g(x)|x^l - 1$, as we wanted.

($\Leftarrow$) Let $f = (1 + x^l + x^{2l} + \ldots + x^{(m-1)l})g$ with $g(x)|x^l - 1$. Then it holds that

$$x^l f(x) = (x^l + x^{2l} + \ldots + x^{(m-1)l} + 1)g(x) = f(x).$$

Every $k(x) \in C$ can be written as $k(x) = f(x)h(x)$ for some $h(x)$. We see that $x^l k(x) = x^l f(x)h(x) = f(x)h(x) = k(x)$, hence σ^l is contained in the kernel of the map ϕ. □

When we combine these two lemmas, we get the following important result.

Theorem 2. *Let C be a cyclic $[n, k]$-code. Then $\phi : Aut(C) \to GL(k, 2)$ is not injective if and only if C is a block repetition code.*

So we now know that the automorphism group of a code C is isomorphic to a subgroup of $GL(k, 2)$ if C is not a block repetition code. Curiously, in paragraph 8.5 of *The Theory of Error-Correcting Codes* of MacWilliams and Sloane (see [8]), this possibility of the code being a block repetition code is left out. Lemma 12 on page 231 states *"The permutation of coordinate places represented by the $n \times n$ matrix A is in $Aut(C)$ if and only if $KM = MA$ for some invertible $k \times k$ matrix K"*. A remark at the bottom of the page says *"By Lemma 12, the automorphism group of a binary linear code of dimension k is isomorphic to a subgroup of $GL(k, 2)$"*. However, we now know that this is not true for block repetition codes, since different permutations can result in the same matrix. So probably this is a flaw in this text.

When we define

$$N := \{\pi \in Aut(C) : \pi(a) = a \text{ for all } a \in C\},$$

then N is exactly the kernel of ϕ. So there is always a map from $Aut(C)/N$ to $GL(k, 2)$ that is injective.

4.2 Application to Hamming and BCH codes

With theorem 2, we can prove the following lemma.

Lemma 4. *The map ϕ is injective for the Hamming code of length $n = 2^m - 1$, for $m \geq 3$.*

Proof. For these values of m it holds that $m < \frac{1}{2}n$, thus $dim(H) = n - m > \frac{1}{2}n$. Consequently, H can not be a block repetition code, see example 2.2.6. From theorem 2 it follows that ϕ is injective for H. □

The next theorem proves that the map ϕ is also injective for the dual of the Hamming code and the dual of other narrow sense BCH codes.

Theorem 3. *The map ϕ is injective for the dual code of a narrow sense $BCH(m, \delta, 1)$ code of length $n = 2^m - 1$, $m \geq 2$.*

Proof. Let α be again such that $\mathbb{F}_{2^m}^* = \langle\alpha\rangle$. The generator polynomial $h(x)$ of $BCH(m, \delta, 1)$ is the polynomial of lowest degree over $\mathbb{F}_2$ that has $\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$ among its zeros. Let $g(x)$ be the generator polynomial of $BCH^{\perp}$, which satisfies $g^*(x)h(x) = x^n - 1$.

Suppose that ϕ is not injective for $BCH^{\perp}$. Then $BCH^{\perp}$ is a block repetition code, so there exist $l, p \in \mathbb{Z}$ with $n = pl$ and $p \geq 2$, and a $f(x)$ with $f(x)|x^l - 1$ such that

$$g(x) = (1 + x^l + x^{2l} + \ldots + x^{n-l})f(x).$$

The reciprocal of $g(x)$ is given by

$$\begin{aligned} g(x)^* &= (1 + x^l + x^{2l} + \ldots + x^{n-l})^* f^*(x) \\ &= (1 + x^l + x^{2l} + \ldots + x^{n-l}) f^*(x). \end{aligned}$$

So we see that $1 + x^l + \ldots + x^{n-l} | g^*(x)$. Furthermore, α is a zero of $1 + x^l + \ldots + x^{n-l}$:

$$1 + \alpha^l + \ldots + \alpha^{n-l} = (\alpha^n - 1)/(\alpha^l - 1) = 0,$$

since α is a primitive n-th root of unity and l is a proper divisor of n. So α is a zero of both $h(x)$ and $g^*(x)$, hence α is a multiple zero of $x^n - 1$. However, for odd n, $x^n - 1$ has only single roots:

$$gcd(x^n - 1, \frac{d}{dx}(x^n - 1)) = gcd(x^n - 1, x^{n-1}) = 1.$$

This leads to a contradiction, hence ϕ is injective for $BCH(m, \delta, 1)^{\perp}$. □

When δ is large enough, a BCH code is equal to the repetition code. This means that ϕ is not always injective for a $BCH(m, \delta, 1)$ code, although it is for its dual. We will show that ϕ is also surjective for the dual of the Hamming code, which leads to the following theorem.

Theorem 4. *The automorphism group of the Hamming code H of length $n = 2^m - 1$ is isomorphic to $GL(m, 2)$.*

Proof. To prove this, we consider $H^{\perp}$, since the automorphism group of a code is equal to the automorphism group of the dual code.

Theorem 3 tells us that ϕ is injective for $H^{\perp}$ for $m \geq 3$. For $m = 2$, $H^{\perp}$ is equal to the even weight code of length 3, for which ϕ is injective too. Also for the trivial case that $m = 1$ it holds that ϕ is injective for $H^{\perp}$.

The dimension of $H^{\perp}$ is m, so there is a basis $v_1, \ldots, v_m$ for $H^{\perp}$, which form the rows of the $m \times n$ generator matrix M. Let $p_0, \ldots, p_{n-1}$ be the n columns of the generator matrix. Since ϕ is injective, we know from lemma 1 that the $n = 2^m - 1$ vectors p_i are all different. Moreover, they are all not equal to zero, because $H^{\perp}$ is cyclic and not equal to the zero code. So $p_0, \ldots, p_{n-1}$ are exactly all the nonzero vectors of $\mathbb{F}_2^m$.

For every matrix $K \in GL(k, 2)$, the rows of $K^{-1}M$ give a new basis for $H^{\perp}$, so $K^{-1}M$ is also a generator matrix for $H^{\perp}$. Hence, the columns of $K^{-1}M$ need to be exactly all the nonzero vectors of $\mathbb{F}_2^m$. So mixing the columns of $K^{-1}M$ in the right way gives M. Thus there is a permutation matrix A for this permutation, which satisfies $K^{-1}M = MA$.

So for every $K \in GL(k,2)$ there is an automorphism π of $H^\perp$ for which $\phi(\pi) = K$. This means that the map ϕ is not only injective, but also surjective for $H^\perp$ and we can conclude

$$Aut(H) = Aut(H^\perp) \cong GL(k,2).$$

□

An alternative definition[11] of the Hamming code is the following: the Hamming code is the dual of a code with a generator matrix with all nonzero vectors of $\mathbb{F}_2^m$ as its columns. With the proof above, we can see that this defines an equivalent code of the Hamming code that we defined.

The map ϕ is injective for the cyclic code $H^\perp$, so $H^\perp$ is not a block repetition code. Consequently, the generator polynomial $g(x)$ of $H^\perp$ and its $n-1$ cyclic shifts $x^i g(x)$, $1 \leq i \leq n-1$, are all different. Since $H^\perp$ is m-dimensional, it has $2^m = n+1$ code words: the zero word and the n cyclic shifts of the generator polynomial. So all the nonzero code words have the same weight. Because the columns of the generator matrix of $H^\perp$ are exactly all the nonzero vectors of $\mathbb{F}_2^m$, we know that there are $\frac{n+1}{2} = 2^{m-1}$ columns with a 1 on the first position, hence this weight is equal to 2^{m-1}. So the weight enumerator of $H^\perp$ is equal to:

$$W(H^\perp; x, y) = y^n + nx^{2^{m-1}} y^{2^{m-1}-1} = y^n + nx^{(n+1)/2} y^{(n-1)/2}.$$

With the MacWilliams identity we find the weight enumerator of the Hamming code H:

$$\begin{aligned} W(H; x, y) &= \frac{1}{\mid H^\perp \mid} W(H^\perp; y-x, y+x) \\ &= \frac{1}{n+1}\left((y+x)^n + n(y-x)^{(n+1)/2}(y+x)^{(n-1)/2}\right). \end{aligned} \tag{4.2}$$

If we fill in $y = 1$ in (4.2) we get

$$\begin{aligned} W(H; x, 1) &= \frac{1}{n+1}\left((1+x)^n + n(1-x)^{(n+1)/2}(1+x)^{(n-1)/2}\right) \\ &= \frac{1}{n+1}\left(\sum_{k=0}^{n}\binom{n}{k}x^k + n\left[\sum_{k=0}^{\frac{n+1}{2}}\binom{\frac{n+1}{2}}{k}(-1)^k x^k\right]\left[\sum_{l=0}^{\frac{n-1}{2}}\binom{\frac{n-1}{2}}{l}x^l\right]\right). \end{aligned}$$

Since the Hamming code of length $n = 2^m - 1$ is equal to the $BCH(m,3,1)$ code, the minimum weight is at least 3. This means that the coefficients in front of x and x^2 are zero, which can also be verified by direct calculation. The coefficient in front of x^3 turns out to be equal to $\frac{1}{6}n(n-1)$, so the Hamming code contains code words of weight 3. Thus the minimum weight of a Hamming code of length $n = 2^m - 1$ is 3. The rather lengthy calculations can be found on page 25 and 26 of [1].

Chapter 5

Transitive subgroups

A subgroup G of S_n is *transitive* if for every i and j in $\{0, 1, \ldots, n-1\}$ there is a permutation $\pi \in G$ for which $\pi(i) = j$. For a cyclic code, the n-cycle $\sigma = (01 \ldots n-1)$ is an element of $Aut(C)$, so for every $i, j \in \{0, 1, \ldots, n-1\}$ it holds that $\sigma^{j-i}(i) = j$. Hence, the automorphism group of a cyclic code is transitive.

The next lemma describes a consequence of an automorphism group having a transitive subgroup. This lemma and the subsequent theorem are based on theorem 4.3.14 and corollary 4.3.15 of [10]. This theorem leads to an useful application of automorphism groups, which is stated in corollary 1: if the automorphism group of the extended code $\tilde{C}$ of a code C is transitive, then the original code C has odd minimum weight.

Lemma 5. *Let B be the matrix having as rows all code words of a code C. If the automorphism group of C is transitive, then all columns of B have the same number of ones. In other words, on each coordinate position of the code occurs equally often a 1.*

Proof. For every j in $\{0, 1, \ldots, n-1\}$, there is a permutation π_j in $Aut(C)$ with $\pi_j(0) = j$. Let A_{π_j} be the associated $n \times n$ permutation matrix. Since this permutation is an automorphism of C, the matrix BA_{π_j} has the same rows as B, but perhaps in different order. This means that the first column of BA_{π_j}, which is equal to the $(j+1)$-th column of B, has the same number of ones as the first column of B. Since this holds for every j, all columns of B must have the same number of ones. □

Although $Aut(C)$ is transitive for a cyclic code C, this does not hold in general for the extended code $\tilde{C}$.

Theorem 5. *Let C be a code of length n, with $A_i = \#\{a \in C | w(a) = i\}$, and $\tilde{C}$ the extended code of length $N = n + 1$. If the extended code $\tilde{C}$ has a transitive automorphism group, then*

$$A_{2j-1} = 2jA_{2j}/(N - 2j) \qquad \textit{for all } j.$$

Proof. Let $\tilde{A}_i$ be the number of code words in $\tilde{C}$ that have weight i. Since the extended code only has code words of even weight, $\tilde{A}_{2j}$ is equal to $A_{2j} + A_{2j-1}$. So the total weight of all the words of weight $2j$ in $\tilde{C}$ is $2j\tilde{A}_{2j} = 2j(A_{2j-1} + A_{2j})$. By lemma 5, this total weight has to be distributed evenly among the N positions of the extended code. So for each position there are $2j\tilde{A}_{2j}/N$ code words with a 1 on that position. This also holds for the position of the parity bit: there are $2j\tilde{A}_{2j}/N$ code words in $\tilde{C}$ for which the parity bit is equal to 1. So there are also $2j\tilde{A}_{2j}/N$ code words in C with weight $2j-1$:

$$A_{2j-1} = 2j\tilde{A}_{2j}/N = 2j(A_{2j-1} + A_{2j})/N.$$

From this we easily deduce $A_{2j-1} = 2jA_{2j}/(N-2j)$. □

Corollary 1. *Let $\tilde{C}$ be the extended code of a code C. If the automorphism group of $\tilde{C}$ contains a transitive subgroup, then C has odd minimum weight.*

Proof. From theorem 5 we see that $A_{2j} \neq 0$ implies $A_{2j-1} \neq 0$, so the minimum weight of C is odd. □

Now we want to apply this theorem to the Hamming code and other narrow sense BCH codes, although we already know that the minimum distance of the Hamming code is 3. This means that we have to show that the automorphism group of the extended code of a $BCH(m, \delta, 1)$ code has a transitive subgroup. In the next lemma we see that it even has a *doubly transitive* subgroup: for every $i, j, k, l \in 0, 1, \ldots, 2^m - 1$ with $i \neq k$ and $j \neq l$, there is a permutation π with $\pi(i) = j$ and $\pi(k) = l$.

Lemma 6. *Let $\tilde{B}$ be the extended $BCH(m, \delta, 1)$ code of length $N = n + 1 = 2^m$. Every isomorphism $\gamma : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m} : x \mapsto ax + b$, with $a \neq 0$ and $a, b \in \mathbb{F}_{2^m}$, provides an element of $Aut(\tilde{B})$.*

Proof. $\mathbb{F}_{2^m}$ is a field and $a \neq 0$, so the linear map γ has an inverse and hence it is indeed an isomorphism. Let α be again such that $\mathbb{F}^*_{2^m} = \langle \alpha \rangle$. We can see the $BCH(m, \delta, 1)$ code B as a subset of the group ring $\mathbb{F}_2[G]$, with $G = \mathbb{F}^*_{2^m}$ and $g_k = \alpha^k$ for $0 \leq k \leq n-1$:

$$B = \left\{ \sum_{k=0}^{n-1} c_k g_k \in \mathbb{F}_2[G] : \sum_{k=0}^{n-1} c_k g_k = \ldots = \sum_{k=0}^{n-1} c_k g_k^{\delta-1} = 0 \right\}$$

with a formal sum on the left and normal sums on the right. Likewise, define $W = \mathbb{F}_{2^m}$ with $w_k = \alpha^k$ for $0 \leq i \leq n-1$ and $w_n = 0$, so we can see $\tilde{B}$ as the set

$$\tilde{B} = \left\{ \sum_{k=0}^{n} c_k w_k \in \mathbb{F}_2[W] : \sum_{k=0}^{n} c_k = \sum_{k=0}^{n} c_k w_k = \ldots = \sum_{k=0}^{n} c_k w_k^{\delta-1} = 0 \right\}.$$

The map γ maps a $y = \sum_{k=0}^{n} c_k w_k$ in $\tilde{B}$ to

$$\gamma(y) = \gamma(\sum_{k=0}^{n} c_k w_k) = \sum_{k=0}^{n} c_k \gamma(w_k).$$

Since it is an isomorphism, we see that γ permutes the coefficients of y. We want to know if y is again an element of $\tilde{B}$. That means that for every $i \in \{0, 1, \ldots, \delta - 1\}$ it must hold that $\sum_{k=0}^{n} c_k(aw_k+b)^i = 0$. For $i=0$ this is clear, and for $1 \leq i \leq \delta - 1$ it holds that

$$\begin{aligned}\sum_{k=0}^{n} c_k(aw_k+b)^i &= \sum_{k=0}^{n} c_k \left(\sum_{j=0}^{i} \binom{i}{j} a^{i-j} w_k^{i-j} b^i \right) \\ &= \sum_{j=0}^{i} a^{i-j} b^i \binom{i}{j} \underbrace{\sum_{k=0}^{n} c_k w_k^{i-j}}_{=0} = 0.\end{aligned}$$

So we see that $\gamma(y)$ is again an element of $\tilde{B}$ and hence γ provides an element of $Aut(\tilde{B})$. □

We can see that these maps form together a doubly transitive subgroup of $Aut(\tilde{B})$, because for every $i,j,k,l \in \{0,1,\ldots,n\}$ with $i \neq k$ and $j \neq l$, there is a map γ with $\gamma(w_i) = w_j$ and $\gamma(w_k) = w_l$, namely the map whose graph is the line between the points (w_i, w_j) and (w_k, w_l). The automorphism group of $\tilde{B}$ is thereby transitive, and with corollary 1, we conclude that B has odd mimimum weight. The fact that $Aut(\tilde{B})$ is even doubly transitive is not used here.

Chapter 6

Automorphism groups of cyclic codes

In this chapter we will try to say something general about the automorphism groups of cyclic codes. We will discuss whether some specific subgroups of S_n occur as the automorphism group of a cyclic code of length n. In section 6.1 we present a table that lists all orders of automorphism groups that occur for cyclic codes of length $n \leq 15$. We will first have a look at S_n.

$\mathbf{S_n}$

Theorem 6. *The automorphism group of a linear code C of length n is equal to S_n if and only if C is one of the following codes: the zero code, $\mathbb{F}_2^n$, the repetition code or the even weight code.*

Proof. ($\Leftarrow$) We already saw in example 3.1.1 that for each of these codes, the automorphism group is equal to S_n.

($\Rightarrow$) Suppose C contains a code word a, that has at least one 1 and one 0, so the weight $w(a)$ satisfies $1 \leq w(a) \leq n-1$. Suppose that there is a 1 on place i and a 0 on place j. Since the automorphism group is equal to S_n, $\tau = (ij)$ is an element of $Aut(C)$. So $\tau(a)$ is contained in C, and also $a + \tau(a)$, which has weight 2. From this code word $a + \tau(a)$, we can make each code word of even weight with an appropiate permutation from S_n. So the even weight code is contained in C, and hence C is the even weight code of dimension $n-1$ or it is equal to $\mathbb{F}_2^n$. If C has no such code word a, then C is the zero code or the repetition code. □

This theorem holds for linear codes in general. However, when a linear code C has S_n as its automorphism group, then $Aut(C)$ contains the n-cycle $\sigma = (01 \ldots n-1)$ and hence the code turns out to be cyclic.

$\mathbb{Z}/\mathbf{n}\mathbb{Z}$

For a cyclic code C, the permutation group generated by σ is contained in $Aut(C)$, so

$$Aut(C) \supset \langle \sigma \rangle \cong \mathbb{Z}/n\mathbb{Z}.$$

Furthermore, if n is odd, then the permutation λ which maps i to $2i$ mod n is contained in $Aut(C)$, since for each $f(x)$ in a cyclic binary code C it holds that $f(x)^2 = f(x^2)$. For example, for $n = 7$ this permutation λ is given by $(0)(124)(365)$. Since for $n \geq 3$ it holds that $\lambda(0) = 0$ and $\lambda(1) = 2$, λ is not contained in the permutation group generated by σ. This means that for odd $n \geq 3$, the automorphism group of a cyclic code is not equal to $\langle \sigma \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

For even n, we do not have such a criterion.

$\mathbf{D_n}$

The dihedral group D_n is the group of symmetries of a regular polygon with n vertices. D_n consists of $2n$ elements and is generated by a rotation $\sigma = (01 \ldots n-1)$ and a reflection ρ that maps coordinate i to $n - 1 - i$. When $D_n \subset Aut(C)$ for a code C of length n, C is cyclic, so we can see σ and ρ as automorphisms of $\mathbb{F}_2[x]/(x^n - 1)$:

$$\sigma : f(x) \to xf(x)$$

$$\rho : f(x) \to x^{n-1} f(\frac{1}{x}).$$

Let $g(x)$ be the generator polynomial of C, then $g^*(x) = x^{deg(g)} g(1/x)$ must be an element of C too. Hence $(g^*) \subset C = (g)$, and because g and g^* have the same degree, it follows that $g(x) = g^*(x)$. So we can conclude that if $D_n \subset Aut(C)$, then the generator polynomial has to be equal to its reciprocal.

For odd $n \geq 5$, λ is not contained in D_n, since it mixes the vertices of the polygon in the wrong way. So for odd $n \geq 5$, there is no cyclic code C of length n with $Aut(C) = D_n$.

For $n = 4$, the dihedral group D_4 occurs as the automorphism group of the cyclic code of length 4 generated by $1 + x^2$. For even $n \geq 6$ we do not know if D_n occurs as the automorphism group of a cyclic code.

$\mathbf{A_n}$

The following theorem states that the automorphism group of a code is never equal to A_n, for $n \geq 2$. Notice that this does not only hold for cyclic but also for general linear codes.

Theorem 7. *There is no linear code C of length $n \geq 2$ with A_n as its automorphism group.*

Proof. $n = 2$. A_2 is equal to $\{id\}$, but every linear code in $\mathbb{F}_2^n$ has S_2 as automorphism group, and $S_2 \neq A_2$.

$n \geq 3$. Suppose there is a code C which has A_n as automorphism group. From theorem 6 we know that this code is not equal to the zero code or the repetition code, since A_n is not equal to S_n for $n \geq 3$. So there is a code word $c = (c_0, c_1, \ldots, c_{n-1})$ with at least one 1 and one 0, so there are i and j for which $c_i = 1$ and $c_j = 0$. For a k with $i \neq k \neq j$ it holds that $\mu = (ijk)$ is an element of A_n. Hence $d = \mu(c) + c$ is a code word of C. This code word d has weight 2, no matter what the value of c_k is. Let d_l and d_m denote the coefficients of d that are 1.

Now we claim that (lm) is contained in $Aut(C)$. If the coefficients a_l and a_m of every code word a in C are equal, then this is obvious. Suppose there is a code word a in C with a 0 and 1 on these places. Switching those coefficients is the same as adding d to a, which results in a code word of C. We conclude that (lm) is an element of $Aut(C)$. This leads to a contradiction, since (lm) is an odd permutation. So there is no linear code C of length $n \geq 2$ with $Aut(C) = A_n$. □

6.1 Table for $n \leq 15$

We computed the automorphism groups that appear for cyclic codes of length $n \leq 15$, by considering all divisors of $x^n - 1$. The results can be found in table 6.1, which was made using the online Magma Calculator[4]. The codes that are generated by 0, 1, $1 + x$ or $1+x+\cdots+x^{n-1}$ are not included in the table, because they all have S_n as automorphism group and appear for each n. For $n \in \{1, 2, 3, 5, 11, 13\}$, these are exactly all cyclic codes that occur.

Furthermore, since a code and its dual have the same automorphism group, we only look at codes of which the degree of the generator polynomial is lower than or equal to $\frac{1}{2}n$. Moreover, the reciprocal of a generator polynomial that is already in the list is left out, since an isomorphism between the automorphism groups is given by a conjugation.

The following lines of code show how Magma can be used to factorize $x^7 - 1$ and compute the automorphism group of the Hamming code generated by $x^3 + x + 1$. The automorphism groups of the other codes in table 6.1 were computed in the same way.

```
> P<x> := PolynomialRing(FiniteField(2));
> F:=Factorization(x^7-1);
> F;
[
    <x + 1, 1>,
    <x^3 + x + 1, 1>,
    <x^3 + x^2 + 1, 1>
]
> Hamming:=CyclicCode(7,F[2][1]);
> AutomorphismGroup(Hamming);
Permutation group acting on a set of cardinality 7
Order = 168 = 2^3 * 3 * 7
    (3, 6)(5, 7)
    (1, 3)(4, 5)
    (2, 3)(4, 7)
    (3, 7)(5, 6)
```

n	Generator	|Aut(C)|
4	x^2+1	8
6	x^2+1	72
	x^2+x+1	48
	x^3+1	48
7	x^3+x+1	168
8	x^2+1	1152
	x^3+x^2+x+1	384
	x^4+1	384
9	x^2+x+1	1296
	x^3+1	1296
10	x^2+1	28800
	$x^4+x^3+x^2+x+1$	3840
	x^5+1	3840
12	x^2+1	1036800
	x^2+x+1	82944
	x^3+1	82944
	x^3+x^2+x+1	31104
	x^4+1	31104
	x^4+x^2+1	4608
	x^4+x^3+x+1	3072
	$x^5+x^3+x^2+1$	2304
	$x^5+x^4+x^3+x^2+x+1$	46080
	$x^6+x^5+x^4+x^3+x^2+x+1$	144
	x^6+1	46080
	$x^6+x^5+x^3+x+1$	144
14	x^2+1	50803200
	x^3+x+1	21504
	$x^4+x^3+x^2+1$	21504
	x^5+x^2+x+1	2688
	x^6+x^2+1	56448
	$x^6+x^5+x^4+x^3+x^2+x+1$	645120
	$x^7+x^6++x^3+x^2+x+1$	56448
	x^7+1	645120
15	x^2+x+1	10368000
	x^4+x+1	20160
	$x^4+x^3+x^2+x+1$	933120
	$x^5+x^4+x^2+1$	20160
	x^5+1	933120
	$x^6+x^5+x^4+x^3+1$	360
	$x^6+x^4+x^3+x^2+1$	720
	x^7+x^3+x+1	360
	$x^7+x^6+x^5+x^2+x+1$	720

Table 6.1: A list of the orders of the automorphism groups of cyclic codes C of length $n \leq 15$. Trivial, equivalent and dual codes are left out.

When two automorphism groups have the same cardinality in table 6.1, it turns out that these groups are equal or conjugate. We see there are not so many different automorphism groups for cyclic codes of short lengths. However, the orders are quite big. For $n \geq 5$, the automorphism groups have more than $2n$ elements, so we see that D_n and $\mathbb{Z}/n\mathbb{Z}$ do not occur for cyclic codes of length $5 \leq n \leq 15$.

We notice that for all codes in the table, the order of $Aut(C)$ is even. For codes of even length n, this is not surprising, since σ has even order in this case. However, for odd n, we can not yet find an explanation.

For $n = 7$ we know that the code generated by $1 + x + x^3$ is the Hamming code, so its automorphism group is isomorphic to $GL(3, 2)$, which has indeed 168 elements. The Hamming code of length $n = 15$ is generated by $x^4 + x + 1$, so the corresponding automorphism group is isomorphic to $GL(4, 2)$, which has 20160 elements.

We do not see a code in the table that contradicts the following: if a code has a generator $f(x)$ of odd weight, so $f(1) \neq 0$, then $Aut(C)$ is equal to the automorphism group of the even subcode $\hat{C}$, which is generated by $(1 + x)f(x)$. The inclusion that $Aut(C) \subset Aut(\hat{C})$ is not so hard to prove: a permutation $\pi \in Aut(C)$ conserves the weight of a code word, so $\pi(\hat{C}) = \hat{C}$, and hence $\pi \in Aut(\hat{C})$.

Chapter 7

Application to permutation groups

In this last chapter, we use the notation of permutations as is common in algebra: the representation of an element of S_n can contain the numbers 1 to n.

We know that every permutation can be written as a product of 2-cycles, even as a product of 2-cycles of the form $(y, y+1)$. So the 2-cycle (12) and the n-cycle $\sigma = (123 \dots n)$ generate S_n. However, for a general 2-cycle $\tau = (1a)$ it does not hold that σ and τ generate all of S_n. For example, the permutation group with (15) and $(123 \dots 8)$ as generators, has only 64 elements[4], while S_8 contains $8! = 40320$ elements. With coding theory we can prove the following theorem about permutation groups.

Theorem 8. *Let $\tau = (1a)$ and $\sigma = (12 \dots n)$ be permutations in S_n, with $2 \leq a \leq n$. If $gcd(a-1, n) \neq 1$, then $\langle \sigma, \tau \rangle$ is not equal to S_n.*

Proof. Suppose $gcd(a-1, n) \neq 1$. Let c, d and e be such that $d = gcd(a-1, n)$, $n = de$ and $a - 1 = cd$. Consider the polynomial $f(x) = 1 + x + \dots + x^{e-1}$, then $f(x)|x^e - 1$. So we know that

$$g(x) = f(x^d) = 1 + x^d + x^{2d} + \dots + x^{(e-1)d}$$

is a divisor of $x^{de} - 1 = x^n - 1$.

The code C_1 of length e, generated by $f(x)$, is the repetition code of length e. This means that for every code word $v = v_0 + \dots + v_{e-1}x^{e-1}$ in C_1 it holds that all the coefficients are equal.

The block repetition code C_2, generated by $g(x)$, is cyclic and d-dimensional. Every code word exists of e identical blocks of length d. For every code word $b = b_0 + \dots + b_{n-1}x^{n-1}$ in C_2 it holds that $b_0 = b_d = b_{2d} = \dots = b_{cd} = b_{a-1}$. It follows that the permutation $(1a)$ is contained in $Aut(C_2)$. Since $1 < d < n$, this code C_2 is not equal to the repetition code, $\mathbb{F}_2^n$ or the even weight code. So by theorem 6, the automorphism group of C_2 is not equal to S_n. Since $\langle \sigma, \tau \rangle$ is a subgroup of $Aut(C_2)$, this proves that $\langle \sigma, \tau \rangle \neq S_n$. □

This theorem can be seen as a special case of the main theorem of the note *Symmetric and Alternating Groups Generated by a Full Cycle and Another Element* by D. Heath, I.M. Isaacs, J. Kiltinen and J. Sklar[6]. This theorem is cited below, where $\rho_n = (12 \dots n)$ and $g(\sigma)$ is defined as the greatest common divisor of the integers $\sigma(i) - i$ for $1 \leq i \leq k$, for a permutation $\sigma \in S_k$.

Theorem 9. *Let $\sigma \in S_k$, and write $G_n = \langle \sigma, \rho_n \rangle$, where $n \geq 2k-1$. If $g(\sigma)$ and n are relatively prime, then G_n is either A_n or S_n. In particular, if $g(\sigma) = 1$, then G_n is A_n or S_n for all $n \geq 2k-1$.*

The restriction to $n \geq 2k-1$ is not a problem. Let $\sigma = (1a)$ with $gcd(a-1, n) = 1$. If $a \leq \frac{1}{2}n+1$ then $n > 2a-1$, and we can apply theorem 9. Since $(1a)$ is an odd permutation, we conclude that $\langle \sigma, \rho_n \rangle = S_n$. When $a > \frac{1}{2}n + 1$, we can choose

$$\tilde{\sigma} = \rho_n^{-(a-1)} \sigma \rho_n^{a-1} = (1, k),$$

with $k = n - a + 2$, since $\langle \tilde{\sigma}, \rho_n \rangle = \langle \sigma, \rho_n \rangle$. It holds that $n > 2k - 2$ and

$$gcd(k-1, n) = gcd(n - (a-1), n) = gcd(a-1, n) = 1,$$

so we can apply theorem 9 to $\tilde{\sigma}$. This means that theorem 8 is indeed a special case of theorem 9.

Chapter 8

Conclusion

Automorphism groups of codes give information about the structure of the code, although it is not easy to determine them. We proved that the automorphism group of the Hamming code of length $n = 2^m - 1$ is isomorphic to $GL(m, 2)$.

This fact has already been established, and some articles (for example [3]) refer for it to the book *The Theory of Error-Correcting Codes* of F.J. MacWilliams and N.J.A. Sloane[8]. We pointed out a flaw in a remark on page 231 of this text and corrected it by giving exactly all counter examples: the block repetition codes. However, since the Hamming code is not a block repetition code for $m \geq 3$, the remark was true in this case.

We described two applications of automorphism groups. The first application is stated in corollary 1: if the automorphism group of the extended code $\tilde{C}$ of a code C has a transitive subgroup, then C has odd minimum weight. This can be applied to the Hamming code of length $n = 2^m - 1$ and other narrow sense BCH codes. The second application is theorem 8, which says that a 2-cycle $(1a)$ and the n-cycle $(12 \ldots n)$ do not generate S_n if $gcd(a-1, n) \neq 1$. We proved this using block repetition codes.

Further we discussed whether some subgroups of S_n can occur as the automorphism group of a cyclic code of length n, namely S_n, A_n, D_n and $\mathbb{Z}/n\mathbb{Z}$. The symmetric group S_n occurs only for linear codes that are equal to the zero code, the repetition code, the even weight code and $\mathbb{F}_2^n$, which are all cyclic codes. For $n \geq 2$, the alternating group A_n never occurs as automorphism group of a cyclic code of length n. For odd $n \geq 3$, both D_n and $\mathbb{Z}/n\mathbb{Z}$ do not occur as automorphism groups for a cyclic code, but for even n we do not have such results.

We made a complete list of the orders of $Aut(C)$ that occur for cyclic codes C of length $n \leq 15$, using Magma[4]. We see that these orders are all even numbers, which we can explain for even n, but not yet for odd n.

For even n, we do not know if there are cyclic $[n, k]$-codes that have D_n as automorphism group, apart from D_4 that occurs as automorphism group of the [4,2]-code generated by $f(x) = x^2 + 1$. Perhaps further research can approach this problem by considering the automorphism groups of the so called $[u|u + v]$-codes, as in theorem 5.2.5 of [13]. Maybe this can give additional conditions for the cyclic codes of even length and their automorphism groups.

Bibliography

[1] M. Berkenbosch, G. van der Heiden, R. Kuik & J. Top, *Dictaat Coderingstheorie*, Rijksuniversiteit Groningen, 1998

[2] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill Book Company, New York, 1968

[3] R. Bienert & B. Klopsch, *Automorphism Groups of Cyclic Codes*, Journal of Algebraic Combinatorics, 2007

[4] W. Bosma, J. Cannon & C. Playoust, *Online Magma Calculator*, Consulted in August 2009, `http://magma.maths.usyd.edu.au/calc/`

[5] B. van Geemen, H.W. Lenstra & F. Oort, *Collegedictaat Algebra: Ringen, Lichamen*, Rijksuniversiteit Groningen, 1997

[6] D. Heath, I.M. Isaacs, J. Kiltinen & J. Sklar, *Symmetric and Alternating Groups Generated by a Full Cycle and Another Element*, The American Mathematical Monthly, v.116 n.5, May 2009

[7] N. Jacobson, *Basic Algebra I*, W.H. Freeman, San Francisco, 1974: page 260

[8] F.J. MacWilliams & N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, Amsterdam, 1977

[9] K.T. Phelps, *Every Finite Group is the Automorphism Group of Some Perfect Code*, Journal of Combinatorial Theory Series A, v.43 n.1,p.45-51, september 1986

[10] S. Roman, *Coding and Information Theory*, Springer, New York, 1992

[11] H. van Tilborg, *Error-correcting Codes - a first course*, Studentlitteratur, Lund, 1997

[12] J. Top, *Collegedictaat Algebra: Groepen*, Rijksuniversiteit Groningen, 2003

[13] E.J.H. Brandenburg, *Finding the Minimal Distance of Cyclic Self-Dual Codes*, Bachelor Thesis, Rijksuniversiteit Groningen, 2009