International Journal of Pure and Applied Mathematics
Volume 91 No. 2 2014, 155-167
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v91i2.2
ijpam.eu

GRÖBNER BASES FOR PERFECT BINARY LINEAR CODES

Natalia Dück[1 §], Karl-Heinz Zimmermann[2]
[1,2]Hamburg University of Technology
21073 Hamburg, GERMANY

Abstract: There is a deep connection between linear codes and combinatorial designs. Combinatorial designs can give rise to linear codes and vice versa. In particular, perfect codes always hold combinatorial designs. Recently, linear codes have been associated to binomial ideals by the so-called code ideal which completely describes the code. It will be shown that for a perfect binary linear code, the codewords of minimum Hamming weight are in one-to-one correspondence with the elements of a reduced Gröbner basis for the code ideal with respect to any graded order.

AMS Subject Classification: 13P10, 94B05, 51E10
Key Words: Gröbner basis, linear code, perfect code, Steiner system, minimum distance

1. Introduction

Digital data are exposed to disturbances when transmitted through a noisy channel and thus errors can occur. Error-correcting codes provide an instrument to detect and correct such errors by adding redundancy. The construction of these codes and the study of their key properties such as the number of codewords and the error-correcting capabilities are an active field of research, see [12, 19].

Received: April 17, 2013

[§]Correspondence author

The first connection between linear codes and Gröbner bases was given by the "Cooper philosophy“, see [8]. Originating from commutative algebra, Gröbner bases provide a uniform approach to tackling a wide range of problems such as solving algebraic systems of equations, ideal membership decision, and effective computation in residue class rings modulo polynomial ideals, see [1, 5, 9, 17].

A different connection between linear codes and ideals in polynomial rings was presented in [6]. Here the authors introduced an ideal associated to a binary linear code and proved that a Gröbner basis can be used for determining the minimum distance.

Thereafter, this approach was generalized to linear codes over prime fields in [15, 16]. In particular, it has been shown that a linear code can be described by a binomial ideal over any field whose reduced Gröbner basis with respect to the lexicographic order can easily be constructed from a systematic generator matrix. In some applications, however, it is advantageous to have a Gröbner basis with respect to a graded order.

There is a deep connection between linear codes and combinatorial designs [4]. In particular, coding theory can be applied to the classification of designs and the Assmus-Mattson theorem allows to uncover designs from linear codes [2, 13]. Conversely, designs give rise to linear codes and can also become a handy tool in proving properties of codes, see [3, 14].

In this paper, it will be shown that for each perfect binary linear code the reduced Gröbner basis for the corresponding code ideal with respect to any graded order has a nice structure in the sense that the minimum weight codewords correspond one-to-one with the elements of the Gröbner basis. This is proved by exploiting a connection between codes and combinatorial designs. Furthermore, in the general situation it will be proved that the reduced Gröbner basis for the code ideal of a binary linear code will contain an element of minimum Hamming weight and so will reveal the minimum distance of the code. Although this result is not essentially new (see [6]), we regard it as worth mentioning since it is proved in a more direct manner.

This paper is organized as follows. In the next two sections, linear codes, Steiner systems, Gröbner bases, binomial ideals, and code ideals are introduced. The Section 4 contains the main result about the structure of the reduced Gröbner basis for perfect binary codes with respect to any graded monomial order. The Section 5 provides a new proof of the fact that the reduced Gröbner basis for the code ideal of a binary linear code with respect to any graded order contains an element of minimum Hamming weight.

2. Linear Codes and Combinatorial Designs

Throughout this paper, denote by $\mathbb{K}$ an arbitrary field and by $\mathbb{N}_0$ the set of non-negative integers.

Let $\mathbb{F}$ be a finite field and let n and k be positive integers with $n \geq k$. A *linear code* of length n and dimension k over $\mathbb{F}$ is the image $\mathcal{C}$ of a one-to-one linear mapping $\phi : \mathbb{F}^k \to \mathbb{F}^n$, i.e., $\mathcal{C} = \{\phi(a) \mid a \in \mathbb{F}^k\}$. Such a code is denoted as an $[n, k]$ code and its elements are called *codewords*. In algebraic coding, the codewords are always written as row vectors.

The *support* of a vector $x \in \mathbb{F}^n$, denoted by $\mathrm{supp}(x)$, is a subset of $\underline{n} = \{1, \ldots, n\}$ consisting of all indices $i \in \underline{n}$ such that $x_i \neq 0$, and the *Hamming weight*, denoted by $\mathrm{wt}(x)$, is the number of non-zero components and so equals the cardinality of the codeword's support. Note that for a binary code, each codeword is completely determined by its support. The *Hamming distance* between two vectors $x, y \in \mathbb{F}^n$, written $\mathrm{dist}(x, y)$, is the number of positions at which they differ and so is given by $\mathrm{dist}(x, y) = \mathrm{wt}(x - y)$. The Hamming distance defines a metric on $\mathbb{F}^n$.

An important invariant of a linear code $\mathcal{C}$ is its *minimum distance*, written $d_H(\mathcal{C})$, which is the minimum value of the Hamming distances over all pairs of distinct codewords. For a linear code, the minimum distance equals the *minimum weight*, which is the minimum value of the Hamming weights over all non-zero codewords.

A linear code of length n, dimension k, and minimum distance d is called an $[n, k, d]$ code. Suppose the minimum distance of the code is $d = 2e + 1$ for some non-negative integer e. Consider the balls of radius e around the codewords, i.e., $B_e(x) = \{y \in \mathbb{F}^n \mid \mathrm{dist}(x, y) \leq e\}$. Balls around distinct codewords are disjoint and cover part of the ambient space $\mathbb{F}^n$. It follows that the code can detect $2e$ errors and correct e errors, see [12, 19]. In particular, if the balls around the codewords cover the whole ambient space, i.e.,

$$\mathbb{F}^n = \bigcup_{c \in \mathcal{C}} B_e(c),$$

the code is said to satisfy the *sphere-packing bound* and is called a *perfect code*. Prominent examples of perfect linear codes are the one-error correcting Hamming codes and the binary and ternary Golay codes, see [18].

Finally, a specific class of combinatorial block designs will be introduced, see [4]. A *Steiner system* is an n-element set S together with a collection of k-element subsets of S, called *blocks*, such that every t-element subset of S is contained in exactly one block. A block design with this property is denoted by $S(t, k, n)$. Perfect binary codes always hold designs. Indeed, the above considerations show that if $\mathcal{C}$ is a perfect binary linear code of length n and minimum distance d, the set of supports of all codewords with minimum weight d naturally forms a Steiner system $S(e+1, d, n)$, where $e = (d-1)/2$, see [14, Thm. 4.4.5]. For instance, the binary Golay code is a $[23, 12, 7]$ perfect code whose codewords of minimal Hamming weight form an $S(4, 7, 23)$ design, see [12, 19].

3. Binomial Ideals and Gröbner Bases

Let $\mathbb{K}[\mathbf{x}] = \mathbb{K}[x_1, \ldots, x_n]$ be the polynomial ring in n variables and denote the *monomials* by $\mathbf{x}^{\mathbf{u}} = x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}$, where $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{N}_0^n$. The *total degree* of a monomial $\mathbf{x}^{\mathbf{u}}$ is given by the sum $u_1 + \ldots + u_n$. A *monomial order* on $\mathbb{K}[\mathbf{x}]$ is a relation $\succ$ on the set of monomials in $\mathbb{K}[\mathbf{x}]$ satisfying: (1) $\succ$ is a total ordering, (2) the monomial $\mathbf{x}^{\mathbf{0}} = 1$ is the unique minimal element, and (3) $\mathbf{x}^{\mathbf{u}} \succ \mathbf{x}^{\mathbf{v}}$ implies $\mathbf{x}^{\mathbf{u}}\mathbf{x}^{\mathbf{w}} \succ \mathbf{x}^{\mathbf{v}}\mathbf{x}^{\mathbf{w}}$ for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{N}_0^n$. A *graded order* is a monomial order which orders first by the total degree. Familiar monomial orders are the lexicographic order, the degree lexicographic order, and the degree reverse lexicographic order.

Given a monomial order $\succ$ on $\mathbb{K}[\mathbf{x}]$, each non-zero polynomial $f \in \mathbb{K}[\mathbf{x}]$ has a unique *leading term*, denoted by $\mathrm{lt}_\succ(f)$ or simply $\mathrm{lt}(f)$, which is given by the largest involved term. The coefficient and the monomial of the leading term are called the *leading coefficient* and the *leading monomial*, respectively. Monomial orders are required to introduce the generalized division algorithm. For a fixed monomial order and an ordered s-tuple of polynomials $F = (f_1, \ldots, f_s)$ in $\mathbb{K}[\mathbf{x}]$, each polynomial $f \in \mathbb{K}[\mathbf{x}]$ can be written as

$$f = \sum_{i=1}^{s} a_i f_i + r, \tag{1}$$

where $a_1, \ldots, a_s \in \mathbb{K}[\mathbf{x}]$ with $\mathrm{lt}(f) \succeq \mathrm{lt}(a_i f_i)$ if $a_i \neq 0$ for $1 \leq i \leq s$, and $r = 0$ or r is a linear combination of monomials, none of which is divisible by the leading term of any of the polynomials f_i. The polynomial r is called the *remainder* of f on division by F and one says that f is *reduced* to r by F, see [9].

If I is an ideal in $\mathbb{K}[\mathbf{x}]$ and $\succ$ is a monomial order on $\mathbb{K}[\mathbf{x}]$, its *leading ideal* is the monomial ideal generated by the leading monomials of its elements,

$$\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(f) \mid f \in I \rangle. \tag{2}$$

A finite subset $\mathcal{G}$ of an ideal I in $\mathbb{K}[\mathbf{x}]$ is a *Gröbner basis* for I with respect to $\succ$ if the leading ideal of I is generated by the set of leading monomials in $\mathcal{G}$; i.e.,

$$\langle \mathrm{lt}(I)\rangle = \langle \mathrm{lt}(g) \mid g \in \mathcal{G}\rangle. \tag{3}$$

A Gröbner basis is *minimal* if no monomial in the basis is redundant, and it is *reduced* if for any two distinct elements $g, h \in \mathcal{G}$, no term of h is divisible by $\mathrm{lt}(g)$. A reduced Gröbner basis is uniquely determined provided that the generators are monic.

A Gröbner basis for an ideal I in $\mathbb{K}[\mathbf{x}]$ with respect to a monomial order $\succ$ on $\mathbb{K}[\mathbf{x}]$ can be calculated by *Buchberger's algorithm.* A sufficient criterion for a set of polynomials to be a Gröbner basis is given by *Buchberger's S-criterion.* Define the *S-polynomial* of two polynomials f and g in $\mathbb{K}[\mathbf{x}]$ as

$$S(f,g) = \frac{\mathbf{x}^\gamma}{\mathrm{lt}(f)} f - \frac{\mathbf{x}^\gamma}{\mathrm{lt}(g)} g, \tag{4}$$

where $\mathbf{x}^\gamma$ is the least common multiple of the leadings monomials of f and g. Then a finite set of polynomials $\mathcal{G}$ is a Gröbner basis for I if and only if the S-polynomial of any two polynomials in $\mathcal{G}$ is reduced to zero by $\mathcal{G}$, see [1, 5, 9].

A *binomial* is a polynomial given by the difference of two monomials and a *binomial ideal* is an ideal generated by binomials. A Gröbner basis of such an ideal always consists of binomials, see [11]. The following result will become useful in the main section.

Lemma 1. *Let $f = \mathbf{x}^\alpha - \mathbf{x}^\beta$ and $g = \mathbf{x}^\gamma - \mathbf{x}^\delta$ be two binomials in $\mathbb{K}[\mathbf{x}]$ whose respective leading terms $\mathbf{x}^\alpha$ and $\mathbf{x}^\gamma$ are relatively prime. Then the S-polynomial $S(f,g)$ is reduced to zero on division by the pair (f,g).*

Proof. Since $\mathbf{x}^\alpha$ and $\mathbf{x}^\gamma$ do not have a proper common divisor the S-polynomial $S(f,g) = \mathbf{x}^{\alpha+\delta} - \mathbf{x}^{\beta+\gamma}$ can be written as

$$\mathbf{x}^{\alpha+\delta} - \mathbf{x}^{\beta+\gamma} = \mathbf{x}^\delta\left(\mathbf{x}^\alpha - \mathbf{x}^\beta\right) - \mathbf{x}^\beta\left(\mathbf{x}^\gamma - \mathbf{x}^\delta\right) = \mathbf{x}^\delta \cdot f - \mathbf{x}^\gamma \cdot g. \qquad \square$$

Note that this result actually holds for arbitrary polynomials with possibly more than two terms.

For a given $[n,k]$ code $\mathcal{C}$ over a field $\mathbb{F}_p$ with p elements, define the associated *code ideal* as (see [6, 7, 16])

$$I_{\mathcal{C}} = \left\langle \mathbf{x}^c - \mathbf{x}^{c'} \mid c - c' \in \mathcal{C}\right\rangle + I_p(\mathbf{x}), \tag{5}$$

where

$$I_p(\mathbf{x}) = \langle x_i^p - 1 \,|\, 1 \leq i \leq n \rangle \,. \tag{6}$$

Note that $I_p(\mathbf{x})$ allows to view the exponents of the monomials as vectors in $\mathbb{F}_p^n$. In this way, the codewords are encoded by the exponents and not by the coefficients as in the "Cooper Philosophy", see [8]. Thus the code ideal $I_{\mathcal{C}}$ can be considered as a subset of $\mathbb{K}[\mathbf{x}]$ for any field $\mathbb{K}$. A binomial $\mathbf{x}^c - \mathbf{x}^{c'}$ as in (5) is said to be associated to the codeword $c - c'$. It can be shown that the S-polynomial of two binomials corresponding to codewords yields a binomial which is also associated to a codeword, and that every binomial in a Gröbner bases for $I_{\mathcal{C}}$ is associated to a codeword in $\mathcal{C}$.

4. Gröbner Bases for Perfect Binary Codes

The reduced Gröbner basis for the code ideal (5) with respect to the lexicographical order can directly be read off from a standard generator matrix of the code, see [16]. The lexicographical order is of importance in elimination theory. For several applications, however, it is advantageous to have a graded order instead of a lexicographical one such as for the homogenization of ideals and the computation of affine Hilbert functions. In particular in the context of binary codes, a graded order is required in many applications, see [6, 7]. Motivated by this, we examine the structure of Gröbner bases with respect to a graded order for the special class of perfect codes.

Lemma 2. *Let $\mathcal{C}$ be a perfect binary linear code with odd minimum distance. Then every codeword of $\mathcal{C}$ can be written as a sum of minimum weight codewords.*

Proof. Write $d = 2e + 1$ for the minimum distance of $\mathcal{C}$. The assertion will be proved using induction on the Hamming weight. A codeword with minimum weight d has this property.

Therefore, let $c \in \mathcal{C}$ be a codeword with Hamming weight $w > d$ and support $\{i_1, \ldots, i_w\}$. Since the codewords of minimum Hamming weight form a Steiner system $S(e + 1, d, n)$, there is a codeword c' of minimal Hamming weight and support $\{i_1, i_2, \ldots, i_{e+1}, j_1, \ldots, j_{d-(e+1)}\}$. Thus the codeword $c - c'$ has Hamming weight $\mathrm{wt}(c-c') \leq w-(e+1)+d-(e+1) = w-1$. By induction, $c - c'$ can be written as a sum of minimum weight codewords and so c can be expressed in the same way. □

Let $c \in \mathcal{C}$ be a non-zero codeword. If c has odd Hamming weight, write $c = c^+ - c^-$, where c^+ and c^- have disjoint support and $|\text{supp}(c^+)| = |\text{supp}(c^-)| + 1$. Otherwise, write $c = c^+ - c^-$, where c^+ and c^- have disjoint support and $|\text{supp}(c^+)| = |\text{supp}(c^-)|$. Note that for any non-zero codeword c of odd Hamming weight and any graded monomial order, the binomial $\mathbf{x}^{c^+} - \mathbf{x}^{c^-}$ has leading term $\mathbf{x}^{c^+}$.

Theorem 3. *Let $I_\mathcal{C}$ be the code ideal of a perfect binary $[n, k, d]$ code $\mathcal{C}$ with odd minimum distance. A reduced Gröbner basis for the ideal $I_\mathcal{C}$ with respect to any graded monomial order is given by the following set of polynomials,*

$$\mathcal{G} = \left\{ \mathbf{x}^{c^+} - \mathbf{x}^{c^-} \mid c = c^+ - c^- \in \mathcal{C}, wt(c) = d \right\} \cup \left\{ x_i^2 - 1 \mid 1 \leq i \leq n \right\}. \tag{7}$$

Proof. Let $d = 2e + 1$ denote the minimum distance of $\mathcal{C}$. For any set $J \subseteq \underline{n}$, write $\mathbf{x}_J = \prod_{i \in J} x_i$. In particular, for $J = \emptyset$, $\mathbf{x}_J = 1$ and for $J = \underline{n}$, $\mathbf{x}_J = x_1 \cdots x_n$.

First, claim that the set $\mathcal{G}$ generates the ideal $I_\mathcal{C}$. Indeed, observe first that if a binomial $\mathbf{x}^{c-c'} - 1$ is contained in the ideal $I_\mathcal{C}$, then $\mathbf{x}^{c'}(\mathbf{x}^{c-c'} - 1) = \mathbf{x}^c - \mathbf{x}^{c'} \bmod I_2(\mathbf{x})$ will also be in there. Therefore, we only need to show that for each codeword $c - c' \in \mathcal{C}$, the binomial $\mathbf{x}^{c-c'} - 1$ is generated by the binomials in $\mathcal{G}$. For this, note that in view of Prop. 2, each codeword can be written as a sum of codewords of minimum Hamming weight. To this end, let $c = \sum_{i=1}^s c_i$ be such a sum. Claim that

$$\mathbf{x}^c - 1 = \sum_{k=1}^{s} \sum_{\substack{A \subseteq \underline{s} \\ |A| = k}} \prod_{i \in A} (\mathbf{x}^{c_i} - 1) \bmod I_2(\mathbf{x}). \tag{8}$$

Indeed, we only need to consider the monomial $\mathbf{x}^{c_{j_1} + \cdots + c_{j_m}}$ on the right hand side of this equation. For $m = 0$, the monomial $\mathbf{x}^0 = 1$ appears in $\binom{s}{k}$ sets with cardinality k and coefficient $(-1)^k$, $1 \leq k \leq s$. Thus, the monomial 1 has the coefficient

$$\sum_{k=1}^{s} \binom{s}{k} (-1)^k = (1 - 1)^s - 1 = -1.$$

For $0 < m < s$, the monomial $\mathbf{x}^{c_{j_1} + \cdots + c_{j_m}}$ appears in $\binom{s-m}{k}$ sets with cardinality $m + k$ and coefficient $(-1)^k$, $0 \leq k \leq s - m$, and so has the coefficient

$$\sum_{k=0}^{s-m} \binom{s-m}{k} (-1)^k = (1 - 1)^{s-m} = 0.$$

The monomial $\mathbf{x}^{c_1+\cdots+c_s} = \mathbf{x}^c$ appears in exactly one subset, which has cardinality s and coefficient 1. This establishes the above equation and proves the first part.

Second, claim that the set $\mathcal{G}$ satisfies Buchberger's criterion. Indeed, it has to be checked that the S-polynomial of each pair of binomials in $\mathcal{G}$ gets reduced to zero. However, due to Lemma 1 only those pairs need to be considered whose leading terms have a proper common divisor. Three cases can occur:

1. Consider two binomials corresponding to the same codeword with support $\{i_1, i_2, \ldots, i_{e+1}, \ldots, i_{2e+1}\}$ and let $1 \leq s \leq e+1$. Put
$$f = \mathbf{x}_{\{i_1,i_2,\ldots,i_s,i_{s+1},\ldots,i_{e+1}\}} - \mathbf{x}_{\{i_{e+2},\ldots,i_{2e+1}\}}$$
and
$$g = \mathbf{x}_{\{i_1,i_2,\ldots,i_s,i_{e+2},\ldots,i_{2e+2-s}\}} - \mathbf{x}_{\{i_{s+1},\ldots,i_{e+1},i_{2e+3-s},\ldots,i_{2e+1}\}}.$$
Then the monomial with support $\{i_1, i_2, \ldots, i_s\}$ is the greatest common divisor of the leading terms of f and g and so gives
$$\begin{aligned} &S(f,g) = \\ &\quad \left((\mathbf{x}_{\{i_{s+1},\ldots,i_{e+1}\}})^2 - (\mathbf{x}_{\{i_{e+2},\ldots,i_{2e+2-s}\}})^2\right) \mathbf{x}_{\{i_{2e+3-s},\ldots,i_{2e+1}\}}. \end{aligned}$$
This binomial gets reduced to zero by the elements of $I_2(\mathbf{x})$.

2. Take a binomial associated to a codeword with support $\{i_1,\ldots,i_{2e+1}\}$ and a binomial from $I_2(\mathbf{x})$, say $x_{i_1}^2 - 1$, such that they have a proper common divisor. Then
$$\begin{aligned} S(\mathbf{x}_{\{i_1,i_2,\ldots,i_{e+1}\}} - \mathbf{x}_{\{i_{e+2},\ldots,i_{2e+1}\}}, x_{i_1}^2 - 1) &= \\ \mathbf{x}_{\{i_2,\ldots,i_{e+1}\}} - \mathbf{x}_{\{i_1,i_{e+2},\ldots,i_{2e+1}\}}&. \end{aligned}$$
This binomial corresponds to the same codeword up to a sign change and so is being reduced to zero.

3. Pick two binomials corresponding to different minimum weight codewords with respective supports J and K, whose intersection has cardinality $s \geq 1$; the case $s = 0$ is covered by Lemma, see 1. Since the codewords of minimum Hamming weight form a Steiner system $S(e+1, d, n)$, it follows that $s < e+1$. Thus we may assume that
$$J = \{1, \ldots, s, i_1, i_2, \ldots, i_{d-s}\} \text{ and } K = \{1, \ldots, s, j_1, j_2, \ldots, j_{d-s}\},$$

where $\{i_1, i_2, \ldots, i_{d-s}\} \cap \{j_1, j_2, \ldots, j_{d-s}\} = \emptyset$. Put

$$f = \mathbf{x}_{\{1,\ldots,s,i_1,i_2,\ldots,i_{e+1-s}\}} - \mathbf{x}_{\{i_{e+2-s},\ldots,i_{d-s}\}}$$

and

$$g = \mathbf{x}_{\{1,\ldots,s,j_1,j_2,\ldots,j_{e+1-s}\}} - \mathbf{x}_{\{j_{e+2-s},\ldots,j_{d-s}\}}.$$

Then

$$S(f,g) = \mathbf{x}_{\{i_1,\ldots,i_{e+1-s},j_{e+2-s},\ldots,j_{d-s}\}} - \mathbf{x}_{\{j_1,\ldots,j_{e+1-s},i_{e+2-s},\ldots,i_{d-s}\}}.$$

Note that both monomials in $S(f,g)$ have total degree $d-s$.

Two cases can occur. First, let $d-s = e+1$, i.e., $s = e$. Since the codewords of minimum Hamming weight form a Steiner system $S(e+1, d, n)$, there are minimum weight codewords with respective supports

$$\{i_1, i_2, \ldots, i_{e+1-s}, j_{e+2-s}, \ldots, j_{e+1}, s_1, s_2, \ldots, s_e\}$$

and

$$\{j_1, j_2, \ldots, j_{e+1-s}, i_{e+2-s}, \ldots, i_{e+1}, t_1, t_2, \ldots, t_e\}.$$

By adding these two codewords and the two codewords which have respective supports J and K, one obtains a non-zero codeword with support

$$\{s_1, s_2, \ldots, s_e, t_1, t_2, \ldots, t_e\}$$

and Hamming weight $2e < d$ contradicting the assumption that the minimum distance is d. Thus $\{s_1, s_2, \ldots, s_e\} = \{t_1, t_2, \ldots, t_e\}$ and hence the S-polynomial gets reduced to zero.

Second, let $d-s \neq e+1$ and so $s < e$. Take the S-polynomial $h^{(0)} = S(f,g)$ and reduce it by the binomials used in the first case, i.e., the binomials corresponding to codewords with supports

$$\{i_1, i_2, \ldots, i_{e+1-s}, j_{e+2-s}, \ldots, j_{e+1}, s_{11}, s_{12}, \ldots, s_{1e}\}$$

and

$$\{j_1, j_2, \ldots, j_{e+1-s}, i_{e+2-s}, \ldots, i_{e+1}, t_{11}, t_{12}, \ldots, t_{1e}\}.$$

This gives the binomial

$$h^{(1)} = \mathbf{x}_{\{j_{e+2},\ldots,j_{d-s},s_{11},\ldots,s_{1e}\}} - \mathbf{x}_{\{i_{e+2},\ldots,i_{d-s},t_{11},\ldots,t_{1e}\}}.$$

Note that both monomials in this binomial have total degree $d-s-1$. This process can be repeated until the monomials in the resulting binomial have total degree $e+1$ which happens after $m = e - s$ steps. In the kth step, a binomial of the form

$$h^{(k)} = \mathbf{x}_{\{a_1,\ldots,a_{e+1},\ldots,a_{d-s-k}\}} - \mathbf{x}_{\{b_1,\ldots,b_{e+1},\ldots,b_{d-s-k}\}}$$

is reduced to the binomial

$$h^{(k+1)} = \mathbf{x}_{\{a_{e+2},\ldots,a_{d-s-k},s_{k1},\ldots,s_{ke}\}} - \mathbf{x}_{\{b_{e+2},\ldots,b_{d-s-k},t_{k1},\ldots,t_{ke}\}}$$

using binomials corresponding to minimum weight codewords with supports

$$\{a_1,\ldots,a_{e+1},s_{k1},s_{k2},\ldots,s_{ke}\} \text{ and } \{b_1,\ldots,b_{e+1},t_{k1},t_{k2},\ldots,t_{ke}\}.$$

The binomial $h^{(m)}$ obtained in the last step has the shape

$$\mathbf{x}_{\{a_1,\ldots,a_{e+1}\}} - \mathbf{x}_{\{b_1,\ldots,b_{e+1}\}}.$$

Then the first case applies and the binomial gets reduced to zero.

This proves the second part and the assertion is established. □

Example 1. The binary $[23, 12, 7]$ Golay code is a perfect linear code with 253 codewords of minimum weight 7 [12, 19]. In view of Thm. 3, the reduced Gröbner basis for its code ideal with respect to any graded order consists of $253 \cdot \binom{7}{4} + 23 = 8878$ binomials. Indeed, this has been confirmed by computations with the computer algebra system `Singular`, see [10].

The class of known perfect binary linear codes is rather small consisting of the trivial codes, the repetition codes, the Hamming codes, and the Golay code, see [19].

5. Minimum Weight Codewords and Gröbner Bases

For non-perfect linear codes it cannot be guaranteed that all minimum weight codewords appear in the reduced Gröbner basis for the associated code ideal. However, we have the following result which can also be found in [6, Prop. 5]. Our proof is more straightforward.

Proposition 4. *Let $\mathcal{C}$ be a binary linear code and let $\mathcal{G}$ be the reduced Gröbner basis for the code ideal $I_{\mathcal{C}}$ with respect to any graded monomial order. Then $\mathcal{G}$ contains a binomial that corresponds to a codeword of $\mathcal{C}$ with minimum Hamming weight.*

Proof. Let $d = 2e + 1$ (or $d = 2e + 2$) denote the minimum distance of $\mathcal{C}$ and let $\mathcal{G}$ be the reduced Gröbner basis for the code ideal $I_{\mathcal{C}}$ with respect to any graded monomial order. Divide any codeword $c \in \mathcal{C}$ of minimum Hamming weight by $\mathcal{G}$. Claim that this reduction process will terminate only if $\mathcal{G}$ contains a codeword of minimum Hamming weight.

Indeed, using the notation as in the proof of Thm. 3, take $f = \mathbf{x}^{c^+} - \mathbf{x}^{c^-} \in I_{\mathcal{C}}$. Then f must be reduced to zero by $\mathcal{G}$. Note that as $I_{\mathcal{C}}$ is a binomial ideal the reduced Gröbner basis $\mathcal{G}$ consists of binomials. Denote by $g_i \in \mathcal{G}$ the binomial used in the ith step of the reduction process.

In the first step, the leading term of g_1 must divide $\mathbf{x}^{c^+}$. It follows that $\mathrm{lt}(g_1) = \mathbf{x}^{c^+}$. Otherwise, g_1 would correspond to a codeword with Hamming weight less than $2e+1 = d$ (or $2e+2 = d$), since by the graded order the second monomial of g_1 has degree equal to or less than that of the leading monomial. Therefore, $g_1 = \mathbf{x}^{c^+} - \mathbf{x}^{\alpha_1}$ for some α_1 with Hamming weight $\leq e + 1$.

If d is even, then α_1 must be of Hamming weight $e + 1$ and then g_1 corresponds to minimum weight codeword.

If d is odd and α_1 has Hamming weight $< e + 1$, then g_1 will correspond to a codeword of minimum Hamming weight and we are done. Otherwise, α_1 has Hamming weight $e + 1$ and the reduction step is repeated using the bionomial $g_2 = \mathbf{x}^{\alpha_1} - \mathbf{x}^{\alpha_2} \in \mathcal{G}$ such that the Hamming weight of α_2 is $\leq e + 1$. But the reduction process must terminate and so there must be an element $g_i = \mathbf{x}^{\alpha_{i-1}} - \mathbf{x}^{\alpha_i} \in \mathcal{G}$ such that the Hamming weight of α_i is e. Hence, the binomial g_i corresponds to a codeword with minimum Hamming weight. □

This result provides a direct method to calculate the minimum distance of a binary linear code that requires computing the reduced Gröbner basis for the associated code ideal with respect to some graded order, and then to search for a binomial in the Gröbner basis, not lying in the subideal $I_2(\mathbf{x})$, whose number of appearing indeterminates is minimal. This binomial will correspond to a codeword of minimum Hamming weight. The performance of this method heavily depends on the efficiency to compute a Gröbner basis. Nevertheless, the underlying structure allows several improvements. The algorithm given in [6] is adapted to this particular setting.

Finally, there is no direct generalization to perfect non-binary codes. The reason is that in the binary case the Hamming weight of a codeword equals the total degree of each binomial associated with the codeword. In the non-binary case, however, a binomial of minimal total degree is not necessarily a codeword of minimal Hamming weight since the Hamming weight only counts the number of non-zero positions.

References

[1] W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, American Mathematical Society, 1994.

[2] E.F. Assmus, Jr, On the Reed-Muller Codes, *Discrete Math.*, **106** (1992).

[3] E.F. Assmus, Jr., J.D. Key, *Designs and Their Codes*, Cambridge University Press, 1994.

[4] E.F. Assmus, Jr., J.D. Key, Codes and finite geometries, In: *Handbook of Coding Theory*, North-Holland, Elsevier, 1998.

[5] T. Becker, V. Weispfenning, *Gröbner Bases – A Computational Approach to Commutative Algebra*, Springer, 1998.

[6] M. Borges-Quintana, M.A. Borges-Trenard, P. Fitzpatrick, E. Martinez-Moro, Gröbner bases and combinatorics for binary codes, *AAECC*, **19**, No. 5 (2008), 393-411.

[7] M. Borges-Quintana, M.A. Borges-Trenard, I. Marquez-Corbella, E. Martinez-Moro, An algebraic view to gradient descent decoding, *IEEE Information Theory Workshop (ITW)* (2010), 1-4.

[8] A. B. Cooper, Towards a new method of decoding algebraic codes using Gröbner bases, *Transactions 10-th Army Conf. Appl. Math. Comp.*, **93** (1992), 293-297.

[9] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer, 1996.

[10] G.-M. Pfister, G. Schönemann, H. Decker, W. Greuel, *Singular 3-1-5 — A Computer Algebra System for Polynomial Computations* (2012), http://www.singular.uni-kl.de.

[11] D. Eisenbud, B. Sturmfels, Binomial ideals, *Duke Mathemtical Journal*, **84** (1996), 89-133.

[12] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, 1988.

[13] V. Pless, Symmetry codes over GF(3) and new 5-designs, *Journal of Combinatorial Theory* (1972), 119-142.

[14] Steven Roman, *Coding and Information Theory*, Springer, 1992.

[15] M. Saleemi, K.-H. Zimmermann, Gröbner bases for linear codes, *International Journal of Pure and Applied Mathematics*, **62** (2010), 481-491.

[16] M. Saleemi, K.-H. Zimmermann, Linear codes as binomial ideals, *International Journal of Pure and Applied Mathematics*, **61** (2010), 147-156.

[17] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, American Mathematical Society, 1996.

[18] J.H. van Lint, A survey of perfect codes, *Rocky Mountain Journal of Mathematics*, **5** (1975), 199-224.

[19] J.H. van Lint, *Introduction to Coding Theory*, Springer, Berlin, 1999.