International Journal of Pure and Applied Mathematics
Volume 62 No. 4 2010, 481-491

GROEBNER BASES FOR LINEAR CODES

Mehwish Saleemi[1], Karl-Heinz Zimmermann[2 §]
[1,2]Institute of Computer Technology (E-13)
Hamburg University of Technology
Schwarzenbergstr. 95E, Hamburg, 21073, GERMANY
[1]e-mail: chughtai@tuhh.de
[2]e-mail: k.zimmermann@tuhh.de

Abstract: Each linear code can be described by a binomial ideal given as the sum of a toric ideal and a non-prime ideal. In this paper, we show that each such binomial ideal has a very natural reduced Groebner basis which can be easily constructed from a systematic generator matrix of the code.

AMS Subject Classification: 13P10, 94B05
Key Words: commutative polynomial ring, binomial ideal, Groebner basis, linear code, encoding, decoding

1. Introduction

Error-correcting codes are used to protect digital data against the errors that occur during transmission through a communication channel, see [15, 16]. There are two ways to construct error-correcting codes: algebraic coding and probabilistic coding. The construction of good codes by probabilistic methods turned out to be difficult, while R.W. Hamming showed how easy it is to devise algebraic codes by introducing a class of binary single-error-correcting codes whose performance can be easily estimated by the computation of a parameter called Hamming distance, see [14].

The main objects of study in algebraic coding are codes that are linear subspaces of finite-dimensional vector spaces over a finite field. In particular, research was mainly devoted to cyclic codes that form a class of linear codes

Received: June 30, 2010
§Correspondence author

allowing both easier determination of their decoding properties like minimum Hamming distance and low-complexity decoders. Cooper [8] used the polynomial description of cyclic codes in order to construct a decoder by Groebner basis computations. The "Cooper philosophy" was the first instance of applications to associate Groebner bases with linear codes. The application of Groebner basis computations to the study of linear codes became an active field of study (see [10, 17, 18]).

Recently, binomial ideals were associated with binary linear codes such that Groebner basis computations can be used for decoding and to solve several problems related to graphs associated with the code, see [4]. More generally, it was emphasized that linear codes can be described by binomial ideals each of which given as the sum of a toric ideal and a non-prime ideal. The Hilbert polynomials corresponding to the binomial ideal of a code and its toric subideal were described. Moreover, the minimal generators and Groebner bases of the binomial ideals of a code were studied. In particular, in the binary situation, the Graver bases, the universal Groebner bases, and the set of circuits of the binomial ideal turned out to be essentially equal, see [19].

Originally, the method of Groebner bases was introduced by Buchberger for the algorithmic solution of some of the fundamental problems in commutative algebra, see [5, 6]. Today, Groebner bases provide a uniform approach to solving a wide range of problems expressed in terms of sets of multivariate polynomials such as the solvability and solving algebraic systems of equations, ideal and radial membership decision, effective computation in residue class rings modulo polynomial ideals, linear Diophantine equations with polynomial coefficients, algebraic relations among polynomials, implicitization, and inverse polynomial mappings, see [1, 2, 9, 20].

In this paper, we show that the binomial ideal associated with a linear code has a very natural reduced Groebner basis which can be easily constructed from a systematic generator matrix of the code. Moreover, we illustrate that Groebner bases for linear codes provide a very compact representation of the encoding and decoding functions.

2. Binomial Ideals

Throughout this paper, $\mathbb{K}$ denotes a field and $\mathbb{K}[\boldsymbol{X}] = \mathbb{K}[X_1, \ldots, X_n]$ the commutative polynomial ring in n indeterminates over $\mathbb{K}$. Recall that a *term* in $\mathbb{K}[\boldsymbol{X}]$ is a scalar times a monomial. The *monomials* in $\mathbb{K}[\boldsymbol{X}]$ are denoted

by $\boldsymbol{X}^{\boldsymbol{u}} = X_1^{u_1} X_2^{u_2} \cdots X_n^{u_n}$ and are identified with the lattice points $\boldsymbol{u} = (u_1, \ldots, u_n) \in \mathbb{N}_0^n$, where $\mathbb{N}_0$ stands for the set of non-negative integers. The *degree* of a monomial $\boldsymbol{X}^{\boldsymbol{u}}$ is the sum $u_1 + \cdots + u_n$. A total order $\prec$ on $\mathbb{N}_0^n$ is a *term order* if the zero vector $\mathbf{0}$ is the unique minimal element, and $\boldsymbol{u} \prec \boldsymbol{v}$ implies $\boldsymbol{u} + \boldsymbol{w} \prec \boldsymbol{v} + \boldsymbol{w}$ for all $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \mathbb{N}_0^n$. Familiar term orders are the purely lexicographic order, the degree lexicographic order, and the degree reverse lexicographic order. Any strictly decreasing sequence of monomials in a term order is finite. This allows to use induction over the set of polynomials in $\mathbb{K}[\boldsymbol{X}]$ with respect to their leading monomials.

Given a term order $\prec$, each non-zero polynomial $f \in \mathbb{K}[\boldsymbol{X}]$ has a unique *initial term*, denoted by $\mathrm{in}_\prec(f)$, which is given by the largest involved monomial with respect to the term order. If I is an ideal in $\mathbb{K}[\boldsymbol{X}]$, then its *initial ideal* is the monomial ideal generated by the initial terms of its elements,

$$\mathrm{in}_\prec(I) = \langle \mathrm{in}_\prec(f) \mid f \in I \rangle. \tag{1}$$

The monomials that do not lie in the initial ideal $\mathrm{in}_\prec(I)$ are called *standard monomials*. A finite subset $\mathcal{G}_\prec$ of an ideal I in $\mathbb{K}[\boldsymbol{X}]$ is a *Groebner basis* of I with respect to $\prec$ if the initial ideal $\mathrm{in}_\prec(I)$ is generated by the set of initial terms in $\mathcal{G}_\prec$,

$$\mathrm{in}_\prec(I) = \langle \mathrm{in}_\prec(g) \mid g \in \mathcal{G}_\prec \rangle. \tag{2}$$

If no monomial in this generating set is redundant, then the Groebner basis is called *minimal*. It is called *reduced* if for any two distinct elements $g, h \in \mathcal{G}_\prec$, no term of h is divisible by $\mathrm{in}_\prec(g)$. The reduced Groebner basis is uniquely determined for an ideal and a term order provided that its elements are assumed to be monic.

A reduced Groebner basis for an ideal I and a term order $\prec$ can be obtained by the *Buchberger algorithm* that starts with any set of generators for I. It makes use of the *division algorithm* that rewrites each polynomial f modulo I uniquely as a $\mathbb{K}$-linear combination of standard monomials. Given a polynomial $f \in \mathbb{K}[\boldsymbol{X}]$ and an ordered sequence $\mathcal{G} = (g_1, \ldots, g_s)$ of polynomials in $\mathbb{K}[\boldsymbol{X}]$. Let $\mathrm{rem}(f, (g_1, \ldots, g_s)) = \mathrm{rem}(f - h \cdot g_k, (g_1, \ldots, g_s))$, where k is the smallest index such that $\mathrm{in}_\prec(g_k)$ divides $\mathrm{in}_\prec(f)$ and $h \in \mathbb{K}[\boldsymbol{X}]$ is chosen such that $\mathrm{in}_\prec(f) = \mathrm{in}_\prec(h \cdot g_k)$. If no $\mathrm{in}_\prec(g_i)$ divides $\mathrm{in}_\prec(f)$, define $\mathrm{rem}(f, (g_1, \ldots, g_s)) = \mathrm{in}_\prec(f) + \mathrm{rem}(f - \mathrm{in}_\prec(f), (g_1, \ldots, g_s))$. This reduction process is finite since in both cases the leading term of f drops.

For any polynomials $f, g \in \mathbb{K}[\boldsymbol{X}]$, we have

$$f - \mathrm{rem}(f, (g_1, \ldots, g_s)) \in \langle g_1, \ldots, g_s \rangle.$$

In particular, if $\mathrm{rem}(f, (g_1, \ldots, g_s)) = 0$, then f belongs to the ideal $\langle g_1, \ldots, g_s \rangle$

in $\mathbb{K}[\boldsymbol{X}]$ generated by the polynomials $g_1, \ldots, g_s$.

There is a nice criterion for a set of polynomials to be a Groebner basis known as Buchberger's S-criterion. For this, let f and g be polynomials in $\mathbb{K}[\boldsymbol{X}]$. Define the *S-polynomial* of f and g as

$$S(f,g) = \frac{\operatorname{lcm}(\operatorname{in}_\prec(f), \operatorname{in}_\prec(g))}{\operatorname{in}_\prec(f)} f - \frac{\operatorname{lcm}(\operatorname{in}_\prec(f), \operatorname{in}_\prec(g))}{\operatorname{in}_\prec(g)} g,$$

where lcm denotes the least common multiple. The S-polynomial $S(f,g)$ cancels the initial terms of f and g according to the term ordering. *Buchberger's S-criterion* says that a set of monic polynomials $G = \{g_1, \ldots, g_s\}$ in $\mathbb{K}[\boldsymbol{X}]$ is a Groebner basis for the ideal $\langle g_1, \ldots, g_s \rangle$ if and only if $\operatorname{rem}(S(g_i, g_j), G) = 0$ for all $1 \leq i < j \leq s$. For Groebner basics the reader may consult, see [1, 2, 7, 9].

A *binomial* in a polynomial ring $\mathbb{K}[\boldsymbol{X}]$ is a difference of two monomials, say $\boldsymbol{X}^{\boldsymbol{u}} - \boldsymbol{X}^{\boldsymbol{v}}$, where $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{N}_0^n$. A *binomial ideal* is an ideal in $\mathbb{K}[\boldsymbol{X}]$ that is generated by binomials. The class of binomial prime ideals is the same as the class of the toric ideals, see [12]. Toric ideals naturally arise in various fields of applied mathematics, see [11, 20].

Toric ideals often emerge in the following setting (see [3]): Let $\boldsymbol{A} = (a_{i,j})$ be a $d \times n$ matrix with non-negative integer entries. The columns of $\boldsymbol{A}$ give rise to a collection of monomials in the polynomial ring $\mathbb{K}[\boldsymbol{Y}] = \mathbb{K}[Y_1, \ldots, Y_d]$ defined as

$$m_j = Y_1^{a_{1,j}} \cdots Y_d^{a_{d,j}}, \quad 1 \leq j \leq n. \tag{3}$$

The ideal corresponding to the matrix $\boldsymbol{A}$ is the kernel of the $\mathbb{K}$-algebra homomorphism

$$\phi : \mathbb{K}[\boldsymbol{X}] \to \mathbb{K}[\boldsymbol{Y}] : X_j \mapsto m_j, \quad 1 \leq j \leq n. \tag{4}$$

This is the *toric ideal associated to* $\boldsymbol{A}$ and is denoted by $I_{\boldsymbol{A}}$ (see [3, 20]). The ideal $I_{\boldsymbol{A}}$ is prime since it is the kernel of a homomorphism into an integral domain. Moreover, it is generated by binomials,

$$I_{\boldsymbol{A}} = \langle \boldsymbol{X}^{\boldsymbol{u}} - \boldsymbol{X}^{\boldsymbol{v}} \mid \boldsymbol{A}\boldsymbol{u} = \boldsymbol{A}\boldsymbol{v}, \boldsymbol{u}, \boldsymbol{v} \in \mathbb{N}_0^n \rangle. \tag{5}$$

The generating binomials $\boldsymbol{X}^{\boldsymbol{u}} - \boldsymbol{X}^{\boldsymbol{v}}$ can be chosen to be *pure*; i.e., $\gcd(\boldsymbol{X}^{\boldsymbol{u}}, \boldsymbol{X}^{\boldsymbol{v}}) = 1$.

A Groebner basis for the ideal $I = I_{\boldsymbol{A}}$ can be computed in $\mathbb{K}[\boldsymbol{X}, \boldsymbol{Y}]$ from the ideal (see [3, 20])

$$J = \langle X_j - m_j \mid 1 \leq j \leq n \rangle. \tag{6}$$

For this, observe that $I = J \cap \mathbb{K}[\boldsymbol{X}]$. Moreover, since J is generated by binomials, Groebner basis theory implies that all the elements in any reduced Groebner basis for J are binomials, too. Suppose $\mathcal{G}$ is a Groebner basis for J

with respect to an elimination term order in which any monomial containing one of the Y_i is greater than any monomial containing only the X_j. Then I has the Groebner basis $\mathcal{G} \cap \mathbb{K}[\boldsymbol{X}]$ and so is also generated by binomials.

Let $\boldsymbol{A}$ be a $d \times n$ matrix with non-negative entries and let p be a prime. We associate with the toric ideal $I_{\boldsymbol{A}}$ in $\mathbb{K}[\boldsymbol{X}]$ the binomial ideal

$$I_{\boldsymbol{A},p} = I_{\boldsymbol{A}} + \langle X_i^p - 1 \mid 1 \leq i \leq n \rangle. \tag{7}$$

This ideal is not toric, since it is not prime as the polynomials $X_i^p - 1$, $1 \leq i \leq n$, are reducible. By [19], the binomial ideal $I_{\boldsymbol{A},p}$ in $\mathbb{K}[\boldsymbol{X}]$ can be written as

$$\begin{aligned} I_{\boldsymbol{A},p} \;=\; & \langle \boldsymbol{X}^{\boldsymbol{u}'} - \boldsymbol{X}^{\boldsymbol{v}'} \mid \boldsymbol{A}\boldsymbol{u}' \equiv \boldsymbol{A}\boldsymbol{v}' \mod p, \boldsymbol{u}', \boldsymbol{v}' \in \underline{p-1}^n, \gcd(\boldsymbol{X}^{\boldsymbol{u}'}, \boldsymbol{X}^{\boldsymbol{v}'}) = 1 \rangle \\ & + \langle X_i^p - 1 \mid 1 \leq i \leq n \rangle, \end{aligned} \tag{8}$$

where $\underline{p-1} = \{0, 1, \ldots, p-1\}$.

3. Linear Codes

Let $\mathbb{F}_p$ be the finite field with p elements. A *linear code* $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_p$ is the image of a one-to-one linear mapping $\psi : \mathbb{F}_p^k \to \mathbb{F}_p^n$. We have $k \leq n$ and $\mathcal{C} = \psi(\mathbb{F}_p^k)$. The code $\mathcal{C}$ is called an $[n, k]$ code. The elements of $\mathcal{C}$ are termed *codewords* and are written as row vectors. Define the *support* of a codeword $\boldsymbol{c} \in \mathcal{C}$ as the set $\mathrm{supp}(\boldsymbol{c}) = \{i \mid c_i \neq 0\}$ of non-zero coordinates.

A *generator matrix* $\boldsymbol{G}$ for an $[n, k]$ code $\mathcal{C}$ over $\mathbb{F}_p$ is a $k \times n$ matrix whose rows form a basis of $\mathcal{C}$; that is, $\mathcal{C} = \{\boldsymbol{a}\boldsymbol{G} \mid \boldsymbol{a} \in \mathbb{F}_p^k\}$. The code $\mathcal{C}$ is in *standard form* if it has a generator matrix that is in reduced echelon form $\boldsymbol{G} = (\boldsymbol{I}_k \mid \boldsymbol{M})$, where $\boldsymbol{I}_k$ is the $k \times k$ identity matrix; the encoding and the generator matrix are then called *systematic*. Each linear code is equivalent (by column permutations) to a linear code in standard form. If $\mathcal{C}$ is in standard form, then the first k symbols of a codeword are called *information symbols*. These can be chosen arbitrarily and then the remaining symbols, which are called *parity check symbols*, are determined.

If $\mathcal{C}$ is an $[n, k]$ code over $\mathbb{F}_p$, then the *dual code* $\mathcal{C}^\perp$ is given by all words $\boldsymbol{u} \in \mathbb{F}_p^n$ such that $\langle \boldsymbol{u}, \boldsymbol{c} \rangle = 0$ for each $\boldsymbol{c} \in \mathcal{C}$, where $\langle , \rangle$ denotes the ordinary inner product. The dual code $\mathcal{C}^\perp$ is an $[n, n-k]$ code. If $\boldsymbol{G} = (\boldsymbol{I}_k \mid \boldsymbol{M})$ is a generator matrix for $\mathcal{C}$, then $\boldsymbol{H} = \left(-\boldsymbol{M}^T \mid \boldsymbol{I}_{n-k}\right)$ is a generator matrix for $\mathcal{C}^\perp$. We have for each word $\boldsymbol{c} \in \mathbb{F}_p^n$, $\boldsymbol{c} \in \mathcal{C}$ if and only if $\boldsymbol{c}\boldsymbol{H}^T = \boldsymbol{0}$. The matrix $\boldsymbol{H}$ is termed a *parity check matrix* for $\mathcal{C}$ (see [15, 16]).

Let $\mathcal{C}$ be an $[n,k]$ code over $\mathbb{F}_p$. Define the *ideal associated with* $\mathcal{C}$ as

$$I_{\mathcal{C}} = \langle \boldsymbol{X}^{c} - \boldsymbol{X}^{c'} \mid \boldsymbol{c} - \boldsymbol{c}' \in \mathcal{C} \rangle + \langle X_i^p - 1 \mid 1 \leq i \leq n \rangle, \tag{9}$$

where each element $\boldsymbol{c} \in \mathbb{F}_p^n$ is considered as an integral vector in the monomial $\boldsymbol{X}^c$ (see [4, 19]). The binomial ideal $I_{\mathcal{C}}$ can be based on a toric ideal (see [19]). To see this, let $\boldsymbol{H}$ be a parity check matrix for $\mathcal{C}$ and take an integral $(n-k) \times n$ matrix $\boldsymbol{A}$ such that $\boldsymbol{H} = \boldsymbol{A} \otimes_{\mathbb{Z}} \mathbb{F}_p$. Then by (8), we obtain

$$I_{\mathcal{C}} = I_{\boldsymbol{A}} + \langle X_i^p - 1 \mid 1 \leq i \leq n \rangle. \tag{10}$$

Each codeword $\boldsymbol{c} \in \mathcal{C}$ can be written as $\boldsymbol{c} = \boldsymbol{c}^+ - \boldsymbol{c}^-$, where $\boldsymbol{c}^+$ and $\boldsymbol{c}^-$ are elements of $\mathbb{F}_p^n$ that have disjoint support. Since $\boldsymbol{c}\boldsymbol{H}^T = \boldsymbol{0}$, it follows that $\boldsymbol{c}^+\boldsymbol{H}^T = \boldsymbol{c}^-\boldsymbol{H}^T$ and so the binomial $\boldsymbol{X}^{c^+} - \boldsymbol{X}^{c^-}$ lies in $I_{\mathcal{C}}$. Note that the decomposition $\boldsymbol{c} = \boldsymbol{c}^+ - \boldsymbol{c}^-$ is not unique. Indeed, if $X_i^j Y - Z \in I_{\mathcal{C}}$ is a binomial, where $1 \leq i \leq n$ and $1 \leq j \leq p-1$, then

$$Y - X_i^{p-j} Z = X_i^{p-j}(X_i^j Y - Z) - Y(X_i^p - 1) \in I_{\mathcal{C}}. \tag{11}$$

It follows that each binomial $\boldsymbol{X}^c - \boldsymbol{X}^{c'}$ in $I_{\mathcal{C}}$ is equivalent to a binomial $\boldsymbol{X}^{c-c'} - 1$ modulo $I_{\mathcal{C}}$, where the element $\boldsymbol{c} - \boldsymbol{c}'$ is computed in $\mathbb{F}_q^n$. We frequently switch back and forth between codewords $\boldsymbol{c}$ in $\mathcal{C}$ and associated binomials $\boldsymbol{X}^{c^+} - \boldsymbol{X}^{c^-}$ in $I_{\mathcal{C}}$.

In the following, let $\mathcal{C}$ be an $[n,k]$ code over $\mathbb{F}_p$ given in standard form with generator matrix $\boldsymbol{G} = (g_{i,j}) = (\boldsymbol{I}_k \mid \boldsymbol{M})$ and parity check matrix $\boldsymbol{H} = \big(-\boldsymbol{M}^T \mid \boldsymbol{I}_{n-k}\big)$. Let $\boldsymbol{m}_i$ be the length-n vector containing the ith row of the matrix $-\boldsymbol{M}$, i.e., $\boldsymbol{m}_i = (0, \ldots, 0, -g_{i,k+1}, \ldots, -g_{i,n})$ over $\mathbb{F}_p$, $1 \leq i \leq k$; in the following, these vectors are considered as integral vectors with entries ≥ 0.

Theorem 3.1. *Take the lexicographic order on* $\mathbb{K}[\boldsymbol{X}]$ *with* $X_1 \succ \ldots \succ X_n$. *The binomial ideal* $I_{\mathcal{C}}$ *has the reduced Groebner basis*

$$\mathcal{G} = \{X_i - \boldsymbol{X}^{\boldsymbol{m}_i} \mid 1 \leq i \leq k\} \cup \{X_i^p - 1 \mid k+1 \leq i \leq n\}. \tag{12}$$

Proof. By definition, the elements of $\mathcal{G}$ lie in the ideal $I_{\mathcal{C}}$. Conversely, let $\boldsymbol{X}^c - \boldsymbol{X}^d$ be an element of $I_{\mathcal{C}}$ with $\boldsymbol{c} - \boldsymbol{d} \in \mathcal{C}$. The reduction of $\boldsymbol{X}^c - \boldsymbol{X}^d$ via $\mathcal{G}$ leads to the binomial $\boldsymbol{X}^{\boldsymbol{a}} - \boldsymbol{X}^{\boldsymbol{b}}$, where $\boldsymbol{a} = c_1\boldsymbol{m}_1 + \ldots + c_k\boldsymbol{m}_k + \boldsymbol{c}'$, $\boldsymbol{b} = d_1\boldsymbol{m}_1 + \ldots + d_k\boldsymbol{m}_k + \boldsymbol{d}'$, $\boldsymbol{c}' = (0, \ldots, 0, c_{k+1}, \ldots, c_n)$ and $\boldsymbol{d}' = (0, \ldots, 0, d_{k+1}, \ldots, d_n)$. In each step of the reduction, the resulting binomial $\boldsymbol{X}^{c'} - \boldsymbol{X}^{d'}$ satisfies $\boldsymbol{c}' - \boldsymbol{d}' \in \mathcal{C}$. But the vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ both have zeros at the positions 1 to k and so $\boldsymbol{a}\boldsymbol{H}^T = \boldsymbol{b}\boldsymbol{H}^T$ implies that $\boldsymbol{a} = \boldsymbol{b}$. Thus the binomial $\boldsymbol{X}^c - \boldsymbol{X}^d$ is reduced by $\mathcal{G}$ to 0.

Furthermore, the binomial $X_i^p - 1$, $1 \leq i \leq k$, is reduced by $\mathcal{G}$ (using $X_i - \boldsymbol{X}^{\boldsymbol{m}_i}$) to $\boldsymbol{X}^{p\boldsymbol{m}_i} - 1$ and this binomial in turn is reduced by $\mathcal{G}$ (using $X_{k+1}^p - 1, \ldots, X_n^p - 1$) to 0. It follows that $\mathcal{G}$ is a generating set of the ideal $I_{\mathcal{C}}$.

Finally, consider the S-polynomials of the elements in $\mathcal{G}$. First, let $1 \leq i < j \leq k$. We have $S(X_i - \boldsymbol{X}^{\boldsymbol{m}_i}, X_j - \boldsymbol{X}^{\boldsymbol{m}_j}) = X_i\boldsymbol{X}^{\boldsymbol{m}_j} - X_j\boldsymbol{X}^{\boldsymbol{m}_i}$. Division into $\mathcal{G}$ yields

$$\begin{aligned}
&\operatorname{rem}(X_i\boldsymbol{X}^{\boldsymbol{m}_j} - X_j\boldsymbol{X}^{\boldsymbol{m}_i}, \mathcal{G}) = \\
&\quad = \operatorname{rem}(X_i\boldsymbol{X}^{\boldsymbol{m}_j} - X_j\boldsymbol{X}^{\boldsymbol{m}_i} - \boldsymbol{X}^{\boldsymbol{m}_j}(X_i - \boldsymbol{X}^{\boldsymbol{m}_i}), \mathcal{G}) \\
&\quad = \operatorname{rem}(-X_j\boldsymbol{X}^{\boldsymbol{m}_i} + \boldsymbol{X}^{\boldsymbol{m}_j}\boldsymbol{X}^{\boldsymbol{m}_i}), \mathcal{G}) \\
&\quad = \operatorname{rem}(-X_j\boldsymbol{X}^{\boldsymbol{m}_i} + \boldsymbol{X}^{\boldsymbol{m}_j}\boldsymbol{X}^{\boldsymbol{m}_i} - (-\boldsymbol{X}^{\boldsymbol{m}_i})(X_j - \boldsymbol{X}^{\boldsymbol{m}_j}), \mathcal{G}) \\
&\quad = \operatorname{rem}(\boldsymbol{X}^{\boldsymbol{m}_j}\boldsymbol{X}^{\boldsymbol{m}_i} - \boldsymbol{X}^{\boldsymbol{m}_i}\boldsymbol{X}^{\boldsymbol{m}_j}, \mathcal{G}) = 0.
\end{aligned}$$

Second, let $k+1 \leq i < j \leq n$. We have $S(X_i^p - 1, X_j^p - 1) = X_i^p - X_j^p = (X_i^p - 1) - (X_j^p - 1)$ and thus the S-polynomial reduces to zero. Third, let $1 \leq i \leq k$ and $k+1 \leq j \leq n$. We have $S(X_i - \boldsymbol{X}^{\boldsymbol{m}_i}, X_j^p - 1) = X_i - X_j^p\boldsymbol{X}^{\boldsymbol{m}_i}$. Division into $\mathcal{G}$ provides

$$\begin{aligned}
\operatorname{rem}(X_i - X_j^p\boldsymbol{X}^{\boldsymbol{m}_i}, \mathcal{G}) &= \operatorname{rem}(X_i - X_j^p\boldsymbol{X}^{\boldsymbol{m}_i} - (X_i - \boldsymbol{X}^{\boldsymbol{m}_i}), \mathcal{G}) \\
&= \operatorname{rem}(-X_j^p\boldsymbol{X}^{\boldsymbol{m}_i} + \boldsymbol{X}^{\boldsymbol{m}_i}, \mathcal{G}) \\
&= \operatorname{rem}(-X_j^p\boldsymbol{X}^{\boldsymbol{m}_i} + \boldsymbol{X}^{\boldsymbol{m}_i} - (-\boldsymbol{X}^{\boldsymbol{m}_i})(X_j^p - 1), \mathcal{G}) = 0.
\end{aligned}$$

It follows that the set $\mathcal{G}$ is a Groebner basis for $I_{\mathcal{C}}$. Moreover, it is clear that the Groebner basis $\mathcal{G}$ is reduced. □

The reduced Groebner basis given above consists of pure and primitive binomials and thus is in accordance with [19, Proposition 3.2].

Example. The ternary Golay code $\mathcal{C}_{11}$ is an $[11, 6]$ code with minimum Hamming distance 5 and generator matrix $\boldsymbol{G}_{11} = (\boldsymbol{I}_6 \mid \boldsymbol{M})$ (see [13, 15, 16]), where

$$\boldsymbol{M} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 & 1 \\ 1 & 0 & 1 & 2 & 2 \\ 2 & 1 & 0 & 1 & 2 \\ 2 & 2 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \end{pmatrix}.$$

Take the lexicographic order with $X_1 \succ \ldots \succ X_{11}$, the corresponding ideal $I_{\mathcal{C}_{11}}$ in $\mathbb{Q}[\boldsymbol{X}]$ has the reduced Groebner basis given by the elements

$$\begin{array}{ll}
X_7^3 - 1, & X_1 - X_7^2X_8^2X_9^2X_{10}^2X_{11}^2, \\
X_8^3 - 1, & X_2 - X_8^2X_9X_{10}X_{11}^2, \\
X_9^3 - 1, & X_3 - X_7^2X_9^2X_{10}X_{11}, \\
X_{10}^3 - 1, & X_4 - X_7X_8^2X_{10}^2X_{11}, \\
X_{11}^3 - 1, & X_5 - X_7X_8X_9^2X_{11}^2, \\
 & X_6 - X_7^2X_8X_9X_{10}^2.
\end{array}$$

By Theorem 3.1, the binomial ideal $I_{\mathcal{C}}$ has the associated initial ideal

$$\mathrm{in}_{\prec}(I_{\mathcal{C}}) = \langle X_1, \ldots, X_k, X_{k+1}^p, \ldots, X_n^p \rangle. \tag{13}$$

An immediate consequence of Theorem 3.1 is a systematic encoding algorithm for linear codes using division with respect to a Groebner basis. Note that this procedure is a variant of the encoding method for multi-dimensional cyclic codes in which the codewords are represented as polynomials in a residue class ring (see [10]).

Proposition 3.2. *Let $\mathcal{C}$ be an $[n, k]$ code over $\mathbb{F}_p$, and let $\mathcal{G}$ be the reduced Groebner basis for $\mathcal{C}$ given in (12).*

— The information positions are given by the nonstandard monomials for $I_{\mathcal{C}}$ in which each X_i appears to a power of at most $p-1$, $1 \leq i \leq k$.

— The parity check positions are provided by the standard monomials for $I_{\mathcal{C}}$ in which each X_i appears to a power of at most $p-1$, $k+1 \leq i \leq n$.

— The following algorithm gives a systematic encoder E for the code $\mathcal{C}$: Take an information word $\boldsymbol{w} \in \mathbb{F}_p^k$ and put $\boldsymbol{X}^{\boldsymbol{w}} = X_1^{w_1} \cdots X_k^{w_k}$. Divide $\boldsymbol{X}^{\boldsymbol{w}}$ into $\mathcal{G}$ and form $E(\boldsymbol{w}) = (\boldsymbol{X}^{\boldsymbol{w}} - 1) - \mathrm{rem}(\boldsymbol{X}^{\boldsymbol{w}} - 1, \mathcal{G})$. This gives the corresponding codeword in $\mathcal{C}$.

Proof. The first two assertions are clear from the initial ideal of $I_{\mathcal{C}}$. Finally, let $\boldsymbol{w} \in \mathbb{F}_p^k$ be an information word. The division of $\boldsymbol{X}^{\boldsymbol{w}} - 1$ into the Groebner basis $\mathcal{G}$ gives

$$\begin{aligned} \mathrm{rem}(\boldsymbol{X}^{\boldsymbol{w}} - 1, \mathcal{G}) &= \mathrm{rem}(\boldsymbol{X}^{w_1\boldsymbol{m}_1 + \ldots + w_k\boldsymbol{m}_k} - 1, \mathcal{G}) \\ &= \boldsymbol{X}^{w_1\boldsymbol{m}_1 + \ldots + w_k\boldsymbol{m}_k} - 1, \end{aligned}$$

where the exponent in the last binomial $\boldsymbol{X}^{w_1\boldsymbol{m}_1 + \ldots + w_k\boldsymbol{m}_k} - 1$ is computed over $\mathbb{F}_p$. It follows that the remainder only involves parity check positions so that the information position are not changed in the process of computing the remainder. The encoded binomial

$$E(\boldsymbol{w}) = (\boldsymbol{X}^{\boldsymbol{w}} - 1) - \mathrm{rem}(\boldsymbol{X}^{\boldsymbol{w}} - 1, \mathcal{G}) = \boldsymbol{X}^{\boldsymbol{w}} - \boldsymbol{X}^{w_1\boldsymbol{m}_1 + \ldots + w_k\boldsymbol{m}_k}$$

is an element of the ideal $I_{\mathcal{C}}$ and represents the codeword $\boldsymbol{wG}$. Thus the reduction of $\boldsymbol{w}$ by the basis $\mathcal{G}$ mimicks the representation of $\boldsymbol{w}$ by a codeword in $\mathcal{C}$. As a result, E is a systematic encoding function for $\mathcal{C}$. □

A general method for decoding a linear code $\mathcal{C}$ is known as *syndrome decoding*, see [15, 16]. It is based on the obervation that if $\boldsymbol{c} \in \mathcal{C}$ is a codeword and some errors $\boldsymbol{e} \in \mathbb{F}_p^n$ are introduced on transmission of $\boldsymbol{c}$, then the received word will be $\boldsymbol{u} = \boldsymbol{c} + \boldsymbol{e}$. If $\boldsymbol{H}$ denotes a parity check matrix for $\mathcal{C}$, then $\boldsymbol{uH}^T = \boldsymbol{eH}^T$ and so $\boldsymbol{uH}^T$ only depends on the error. The possible values for $\boldsymbol{eH}^T \in \mathbb{F}_p^{n-k}$

are known as *syndromes* and are in one-to-one correspondence with the cosets of $\mathcal{C}$ in $\mathbb{F}_p^n$. Syndrome decoding is based on a table of p^{n-k} entries called *standard array* that is indexed by the possible values of the syndromes $\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^T$ and contains the vectors in the corresponding cosets with the smallest number of nonzero entries.

An immediate consequence of Theorem 3.1 is a decoding algorithm for linear codes using division with respect to a Groebner basis. This algorithm was given in slightly different form in [4].

Proposition 3.3. *Let $\mathcal{C}$ be an $[n,k]$ code over $\mathbb{F}_p$, and let $\mathcal{G}$ be the reduced Groebner basis for $\mathcal{C}$ given in (12). Suppose the code $\mathcal{C}$ is t-error-correcting. The following algorithm gives a decoder D for the code C: Given a received word $\boldsymbol{u} \in \mathbb{F}_p^n$. If the word given by $\operatorname{rem}(\boldsymbol{X}^{\boldsymbol{u}} - 1, \mathcal{G})$ has at most t nonzero entries, then form $D(\boldsymbol{u}) = (\boldsymbol{X}^{\boldsymbol{u}} - 1) - \operatorname{rem}(\boldsymbol{X}^{\boldsymbol{u}} - 1, \mathcal{G})$. This gives the codeword that is closest to the received word. Otherwise, the received word $\boldsymbol{u}$ contains more than t errors.*

Proof. Suppose $\boldsymbol{u}$ is the received word and no more than t errors occurred during transmission. Then the corresponding error vector has at most t nonzero entries and is uniquely determined. The binomial $D(\boldsymbol{u}) = (\boldsymbol{X}^{\boldsymbol{u}} - 1) - \operatorname{rem}(\boldsymbol{X}^{\boldsymbol{u}} - 1, \mathcal{G})$ is an element of $I_{\mathcal{C}}$ and so corresponds to a codeword in $\mathcal{C}$. If the word given by $\operatorname{rem}(\boldsymbol{X}^{\boldsymbol{u}} - 1, \mathcal{G})$ has at most t nonzero entries, then by uniqueness it corresponds to the error vector. □

In summary, the study of a linear code $\mathcal{C}$ by using the corresponding binomial ideal $I_{\mathcal{C}}$ provides an extra structure that allows a very compact representation of the encoding and decoding function. We only need to know a reduced Groebner basis for the ideal $I_{\mathcal{C}}$. In particular, syndrome decoding of an $[n,k]$ code by the standard array needs to maintain $O(p^{n-k})$ entries, while syndrome decoding by the Groebner basis (Proposition 3.3) requires to store only $O(n)$ entries.

References

[1] W. Adams, P. Loustaunau, *An Introduction to Groebner Bases*, AMS Lecture Series, Providence, RI, **3** (1994).

[2] T. Becker, V. Weispfenning, *Groebner Bases – A Computational Approach to Commutative Algebra*, Springer, New York (1998).

[3] A.M. Bigatti, L. Robbiano, Toric ideals, *Mathematica Contemporanea*, **21** (2001), 1-25.

[4] M. Borges-Quintana, M.A. Borges-Trenard, P. Fitzpatrick, E. Martinez-Moro, Groebner bases and combinatorics for binary codes, *AAECC*, **19** (2008), 393-411.

[5] B. Buchberger, *An Algorithm for Finding the Bases Elements of the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal*, Ph.D. Thesis, Univ. of Innsbruck (1965), In German.

[6] B. Buchberger, An algorithmical criterion for the solvability of algebraic systems of equations, *Aequationes Mathematicae*, **4** (1970), 374-384, In German.

[7] B. Buchberger, F. Winkler (Eds.), *Groebner Bases and Applications,* LMS Series, Cambridge University Press, London **251** (1998).

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

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

[10] D. Cox, J. Little, D. O'Shea, *Using Algebraic Geometry*, Springer, New York (1998).

[11] M. Drton, B. Sturmfels, S. Sullivan, *Lectures on Algebraic Statistics*, Birkhäuser, Basel (2009).

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

[13] M.J.E. Golay, Notes on digital coding, *Proc. IRE*, **37** (1949), 657.

[14] R.W. Hamming, Error detecting and error correcting codes, *Bell Syst. Tech. J.*, **29** (1950), 147-160.

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

[16] F.J. MacWilliams, N.J.A. Sloane, *Error Correcting Codes*, North Holland, New York (1977).

[17] M. Sala, T. Mora, L. Perret, S. Sakata, C. Traverso, *Groebner Bases, Coding, and Cryptography*, Springer, Berlin (2009).

[18] M. Saleemi, K.-H. Zimmermann, Groebner bases for a class of ideals in commutative polynomial rings, *Int. J. Pure Appl. Math.*, **58**, No. 1 (2010), 1-9.

[19] M. Saleemi, K.-H. Zimmermann, Linear codes as binomial ideals, *Int. J. Pure Appl. Math.*, **61**, No. 1 (2010), 147-156.

[20] B. Sturmfels, *Groebner Bases and Convex Polytopes*, AMS Lecture Series, Providence, RI, **8** (1996).