International Journal of Pure and Applied Mathematics
Volume 61 No. 2 2010, 147-156

LINEAR CODES AS BINOMIAL IDEALS

Mehwish Saleemi[1], Karl-Heinz Zimmermann[2] §
[1,2]Institute of Computer Technology (E-13)
Hamburg University of Technology
Schwarzenbergstr. 95 E, Hamburg, 21071, GERMANY
[1]e-mail: chughtai@tuhh.de
[2]e-mail: k.zimmermann@tuhh.de

Abstract: Recently, binary linear codes were associated with binomial ideals. We show that each linear code can be described by a binomial ideal given as the sum of a toric ideal and a non-prime ideal. We compute the Hilbert polynomials of the projective subschemes corresponding to the binomial ideal of a code and its toric subideal. Moreover, we study the minimal generators and Groebner bases of the binomial ideals of a linear code. The situation turns out to be quite similar to the case of toric ideals. For the binomial ideals of binary linear codes, the Graver bases, the universal Groebner bases, and the set of circuits are essentially equal.

AMS Subject Classification: 13P10, 94B05
Key Words: commutative polynomial rings, binomial ideals, projective subschemes, Groebner bases, Graver bases

1. Introduction

Error-correcting codes are used to protect digital data against the errors that occur during transmission through a communication channel, see [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

Received: February 22, 2010
§Correspondence author

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, a lot of research was devoted to cyclic codes that form a class of linear codes allowing both easier determination of their 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. Recently, the application of Groebner basis computations to the study of linear codes became an active field of research [10], [18], [17]. 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 related to the code, see [4].

Originally, the method of Groebner bases was introduced by Buchberger for the algorithmic solution of some of the fundamental problems in commutative algebra [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 [1], [2], [9], [19].

In this paper, we show that each linear code can be described by a binomial ideal which is given as the sum of a toric ideal and a non-prime ideal. We compute the Hilbert polynomials of the projective subschemes which correspond to the binomial ideal of a code and its toric subideal. Moreover, we study the minimal generators and Groebner bases of the binomial ideals of a linear code. The situation turns out to be quite similar to the case of toric ideals. For the binomial ideals of binary linear codes, the Graver bases, the universal Groebner bases, and the set of circuits are essentially equal.

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.

Given a term order $\prec$, each non-zero polynomial $f \in \mathbb{K}[\boldsymbol{X}]$ has a unique *initial monomial*, 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 monomials of its elements,

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

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 monomials in $\mathcal{G}_\prec$,

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

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. For Groebner basics the reader may consult, [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, [12]. Toric ideals naturally arise in various fields of applied mathematics, [11], [19].

Toric ideals often emerge in the following setting, [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

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

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

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

This is the *toric ideal associated to* $\boldsymbol{A}$ and is denoted by $I_{\boldsymbol{A}}$ (see [3], [19]). 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,

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

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 [3, 19]

$$J = \langle X_j - m_j \mid 1 \leq j \leq n \rangle.$$

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 ordering 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

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

This ideal is not toric, since it is not prime as the polynomials $X_i^p - 1$, $1 \leq i \leq n$, are reducible. In order to study this ideal, we consider the *saturation* of an ideal I in $\mathbb{K}[\boldsymbol{X}]$, given as

$$\overline{I} = \{ f \in \mathbb{K}[\boldsymbol{X}] \mid X_i^m \cdot f \in I \text{ for some } m \text{ and all } i \}.$$

Clearly, $\overline{I}$ is an ideal and we have $I \subseteq \overline{I}$ and $\overline{\overline{I}} = \overline{I}$. For instance, if $I = \langle f \cdot X_1, \ldots, f \cdot X_n \rangle$, then $\bar{I} = \langle f \rangle$. For notational simplicity write $\underline{p-1} = \{0, 1, \ldots, p-1\}$.

Proposition 2.1. *Let $\mathbb{K}$ be a field, let p be a prime, and let $\boldsymbol{A}$ be a $d \times n$ matrix with non-negative integral entries. The ideal $I_{\boldsymbol{A},p}$ in $\mathbb{K}[\boldsymbol{X}]$ equals the ideal*

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

Proof. First, let $\boldsymbol{X}^{\boldsymbol{u}} - \boldsymbol{X}^{\boldsymbol{v}}$ be a pure binomial in $I_{\boldsymbol{A},p}$, where $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{N}_0^n$ such

that $\boldsymbol{Au} = \boldsymbol{Av}$. Write $\boldsymbol{u} = \boldsymbol{u}_1 p + \boldsymbol{u}_2$ and $\boldsymbol{v} = \boldsymbol{v}_1 p + \boldsymbol{v}_2$, where $\boldsymbol{u}_1, \boldsymbol{v}_1 \in \mathbb{N}_0^n$ and $\boldsymbol{u}_2, \boldsymbol{v}_2 \in \underline{p-1}^n$. We have

$$\boldsymbol{X}^{\boldsymbol{u}} - \boldsymbol{X}^{\boldsymbol{v}} = \boldsymbol{X}^{(\boldsymbol{u}_1+\boldsymbol{v}_1)p}(\boldsymbol{X}^{\boldsymbol{u}_2} - \boldsymbol{X}^{\boldsymbol{v}_2}) - \boldsymbol{X}^{\boldsymbol{u}}(\boldsymbol{X}^{\boldsymbol{v}_1 p} - 1) + \boldsymbol{X}^{\boldsymbol{v}}(\boldsymbol{X}^{\boldsymbol{u}_1 p} - 1).$$

Claim that the right-hand side lies in $J_{\boldsymbol{A},p}$. Indeed, we have

$$X_i^p X_j^p - 1 = (X_i^p - 1)(X_j^p - 1) + (X_i^p - 1) + (X_j^p - 1), \quad 1 \le i, j \le n.$$

Thus for each $\boldsymbol{w} \in \mathbb{N}_0^n$, $\boldsymbol{X}^{\boldsymbol{w}p} - 1$ lies in $\langle X_i^p - 1 \mid 1 \le i \le n\rangle$ and hence in $J_{\boldsymbol{A},p}$. Moreover, $\boldsymbol{Au} = \boldsymbol{Av}$ and $\gcd(\boldsymbol{X}^{\boldsymbol{u}}, \boldsymbol{X}^{\boldsymbol{v}}) = 1$ imply that $\boldsymbol{Au}_2 \equiv \boldsymbol{Av}_2 \mod p$ and $\gcd(\boldsymbol{X}^{\boldsymbol{u}_2}, \boldsymbol{X}^{\boldsymbol{v}_2}) = 1$. This shows that $\boldsymbol{X}^{\boldsymbol{u}} - \boldsymbol{X}^{\boldsymbol{v}} \in J_{\boldsymbol{A},p}$. The claim is proved.

Second, let $\boldsymbol{X}^{\boldsymbol{u}_2} - \boldsymbol{X}^{\boldsymbol{v}_2}$ be a pure binomial in $J_{\boldsymbol{A},p}$, where $\boldsymbol{Au}_2 \equiv \boldsymbol{Av}_2 \mod p$ and $\boldsymbol{u}_2, \boldsymbol{v}_2 \in \underline{p-1}^n$. By definition, there are $\boldsymbol{u}_1, \boldsymbol{v}_1 \in \mathbb{N}_0^n$ such that $\boldsymbol{u} = \boldsymbol{u}_1 p + \boldsymbol{u}_2$, $\boldsymbol{v} = \boldsymbol{v}_1 p + \boldsymbol{v}_2$, and $\boldsymbol{Au} = \boldsymbol{Av}$. Moreover, we have $\gcd(\boldsymbol{X}^{\boldsymbol{u}}, \boldsymbol{X}^{\boldsymbol{v}}) = 1$. It follows that

$$\boldsymbol{X}^{(\boldsymbol{u}_1+\boldsymbol{v}_1)p}(\boldsymbol{X}^{\boldsymbol{u}_2} - \boldsymbol{X}^{\boldsymbol{v}_2}) = (\boldsymbol{X}^{\boldsymbol{u}} - \boldsymbol{X}^{\boldsymbol{v}}) + \boldsymbol{X}^{\boldsymbol{u}}(\boldsymbol{X}^{\boldsymbol{v}_1 p} - 1) - \boldsymbol{X}^{\boldsymbol{v}}(\boldsymbol{X}^{\boldsymbol{u}_1 p} - 1)$$

lies in $I_{\boldsymbol{A},p}$ and hence $\boldsymbol{X}^{\boldsymbol{u}_2} - \boldsymbol{X}^{\boldsymbol{v}_2}$ belongs to the saturation of $I_{\boldsymbol{A},p}$.

Thus we have proved that $I_{\boldsymbol{A},p} \subseteq J_{\boldsymbol{A},p} \subseteq \overline{I_{\boldsymbol{A},p}}$. Let $f \in \overline{I_{\boldsymbol{A},p}}$. Then $X_i^m \cdot f \in I_{\boldsymbol{A},p}$ for some $m \ge 1$, $1 \le i \le n$. But the binomials $X_i^p - 1$, $1 \le i \le n$, show that all variables X_i are invertible modulo $I_{\boldsymbol{A},p}$; i.e., if $X_i \cdot f \in I_{\boldsymbol{A},p}$ then $f = X_i^p \cdot f - (X_i^p - 1) \cdot f \in I_{\boldsymbol{A},p}$, $1 \le i \le n$. Thus $f \in I_{\boldsymbol{A},p}$ and hence $I_{\boldsymbol{A},p} = \overline{I_{\boldsymbol{A},p}}$. The result follows. □

Example 2.2. Take the matrix

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

The toric ideal $I_{\boldsymbol{A}}$ in $\mathbb{F}_2[\boldsymbol{X}]$ has the reduced Groebner basis $\{X_1X_2+X_4, X_1X_3+X_5, X_1X_6 + X_2X_5, X_1X_7 + X_4X_5, X_2X_3 + X_6, X_2X_5 + X_4X_5, X_2X_7 + X_4X_6, X_3X_4+X_7, X_3X_7+X_5X_6, X_4X_5X_6+X_7^2\}$. On the other hand, the ideal $I_{\boldsymbol{A},2}$ in $\mathbb{F}_2[\boldsymbol{X}]$ has the reduced Groebner basis $\{X_1+X_2X_4, X_2+X_3X_6, X_3+X_4X_7, X_4+X_5X_6, X_5^2+1, X_6^2+1, X_7^2+1\}$.

Let $\mathbb{K}$ be an algebraically closed field. Take a toric ideal $I = I_{\boldsymbol{A}}$ in $\mathbb{K}[X_1, \ldots, X_n]$ and consider its homogenization I^h in $\mathbb{K}[\boldsymbol{X}_0] = \mathbb{K}[X_0, X_1, \ldots, X_n]$. The ideal I^h is binomial (see [12]) and defines the projective subscheme $X = \operatorname{Proj} \mathbb{K}[\boldsymbol{X}_0]/I^h$ of $\mathbb{P}^n$ given by the set of all homogeneous prime ideals $\wp \subset \mathbb{K}[\boldsymbol{X}_0]/I^h$ that do not contain the irrelevant ideal $\langle X_0, \ldots, X_n\rangle$, see [15]. By a linear change of coordinates we can assume that no component of X lies in the hypersurface $H_i = \{X_i^p = X_0^p\}$, $1 \le i \le n$. Then there is an exact sequence of

graded vector spaces over $\mathbb{K}$,

$$0 \longrightarrow \mathbb{K}[\boldsymbol{X}_0]/I^h \stackrel{\cdot(X_i^p - X_0^p)}{\longrightarrow} \mathbb{K}[\boldsymbol{X}_0]/I^h \longrightarrow \mathbb{K}[\boldsymbol{X}_0]/(I^h + \langle X_i^p - X_0^p\rangle) \longrightarrow 0.$$

Taking the d-th graded part of this sequence, we obtain

$$h_{X\cap H_i}(d) = h_X(d) - h_X(d-p), \quad d \gg 0.$$

By iterating this argument, we arrive at

$$h_{X\cap\bigcap_i H_i}(d) = \sum_{j=0}^{n}(-1)^j\binom{n}{j}h_X(d-jp), \quad d \gg 0.$$

The same equation holds for the corresponding Hilbert polynomial $\chi_X \in \mathbb{Z}[d]$ when $d \gg 0$.

Proposition 2.3. *If no component of the projective subscheme* $X = \mathrm{Proj}\mathbb{K}[\boldsymbol{X}_0]/I^h_{\boldsymbol{A}}$ *lies in the hypersurfaces* $H_i = \{X_i^p = X_0^p\}$, $1 \le i \le n$, *then the Hilbert polynomial of the projective subscheme* $X' = \mathrm{Proj}\,\mathbb{K}[\boldsymbol{X}_0]/I^h_{\boldsymbol{A},p}$ *of* $\mathbb{P}^n$ *is given by*

$$\chi_{X'}(d) = \sum_{j=0}^{n}(-1)^j\binom{n}{j}\chi_X(d-jp), \quad d \gg 0.$$

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 $k \le n$ and $\mathcal{C} = \psi(\mathbb{F}_p^k)$. There is a $n \times k$ matrix $\boldsymbol{G}$, called *generator matrix*, such that $\mathcal{C} = \{\boldsymbol{G}\boldsymbol{a} \mid \boldsymbol{a} \in \mathbb{F}_p^k\}$. Moreover, there is an $(n-k) \times n$ matrix $\boldsymbol{H}$, called *parity-check matrix*, such that $\boldsymbol{H}\boldsymbol{c} = \boldsymbol{0}$ if and only if $\boldsymbol{c} \in \mathcal{C}$. The elements of $\mathcal{C}$ are called *codewords*. Define the *support* of a codeword $\boldsymbol{u} \in \mathcal{C}$ as the set $\mathrm{supp}(\boldsymbol{u}) = \{i \mid u_i \ne 0\}$ of non-zero coordinates [16].

Let $\mathcal{C}$ be a linear code of length n and dimension k over $\mathbb{F}_p$. Define the *ideal associated with* $\mathcal{C}$ as

$$I_{\mathcal{C}} = \langle \boldsymbol{X}^{\boldsymbol{u}} - \boldsymbol{X}^{\boldsymbol{v}} \mid \boldsymbol{u} - \boldsymbol{v} \in \mathcal{C}\rangle + \langle X_i^p - 1 \mid 1 \le i \le n\rangle,$$

where each vector $\boldsymbol{u} \in \mathbb{F}_p^n$ is considered as integral vector in the monomial $\boldsymbol{X}^{\boldsymbol{u}}$. For the binary case, the ideal $I_{\mathcal{C}}$ was defined in [4]. If $\boldsymbol{H}$ denotes a parity check matrix of $\mathcal{C}$, then the condition $\boldsymbol{u} - \boldsymbol{v} \in \mathcal{C}$ is equivalent to $\boldsymbol{H}\boldsymbol{u} = \boldsymbol{H}\boldsymbol{v}$. Thus by Proposition 2.1, we obtain

$$I_{\mathcal{C}} = I_{\boldsymbol{A}} + \langle X_i^p - 1 \mid 1 \le i \le n\rangle,$$

where $\boldsymbol{A}$ is an integral $(n-k)\times n$ matrix such that $\boldsymbol{H} = \boldsymbol{A} \otimes_{\mathbb{Z}} \mathbb{F}_p$.

Our objective is to understand the minimal generators and Groebner bases of the binomial ideal $I_{\mathcal{C}}$. We will see that the results are quite similar to the case of toric ideals, see [19].

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

$$Y - X_i^{p-j} Z = X_i^{p-j}(X_i^j Y - Z) - Y(X_i^p - 1) \in I_{\boldsymbol{A},p}.$$

We frequently switch back and forth between codewords $\boldsymbol{u}$ in $\mathcal{C}$ and associated binomials $\boldsymbol{X}^{\boldsymbol{u}^+} - \boldsymbol{X}^{\boldsymbol{u}^-}$ in $I_{\mathcal{C}}$.

A binomial $\boldsymbol{X}^{\boldsymbol{u}^+} - \boldsymbol{X}^{\boldsymbol{u}^-}$ in an ideal I of $\mathbb{K}[\boldsymbol{X}]$ is called *primitive* if there is no other binomial $\boldsymbol{X}^{\boldsymbol{v}^+} - \boldsymbol{X}^{\boldsymbol{v}^-}$ in I such that $\boldsymbol{X}^{\boldsymbol{v}^+}$ divides $\boldsymbol{X}^{\boldsymbol{u}^+}$ and $\boldsymbol{X}^{\boldsymbol{v}^-}$ divides $\boldsymbol{X}^{\boldsymbol{u}^-}$. The set of all primitive binomials in I is called the *Graver basis* of I, see [19].

Proposition 3.1. *The Graver basis of the ideal $I_{\mathcal{C}}$ is given by the binomials $X_i^p - 1$, $1 \le i \le n$, and all pure and primitive binomials in $I_{\boldsymbol{A}}$ of the form $\boldsymbol{X}^{\boldsymbol{u}^+} - \boldsymbol{X}^{\boldsymbol{u}^-}$, where $\boldsymbol{u} \in \mathcal{C}$.*

Proof. Each primitive binomial in $I_{\mathcal{C}}$ is pure since all variables X_i, $1 \le i \le n$, are invertible modulo $I_{\mathcal{C}}$.

Let $\boldsymbol{X}^{\boldsymbol{v}^+} - \boldsymbol{X}^{\boldsymbol{v}^-}$ be a pure binomial in $I_{\mathcal{C}}$. Write $\boldsymbol{v}^+ = \boldsymbol{v}_1 p + \boldsymbol{u}^+$ and $\boldsymbol{v}^- = \boldsymbol{v}_2 p + \boldsymbol{u}^-$, where $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathbb{N}_0^n$ and $\boldsymbol{u}^+, \boldsymbol{u}^- \in \underline{p-1}^n$. If $\boldsymbol{u}^+ = \boldsymbol{0} = \boldsymbol{u}^-$ then $\boldsymbol{X}^{\boldsymbol{v}^+} - \boldsymbol{X}^{\boldsymbol{v}^-}$ is divisible by some $X_i^p - 1$, $1 \le i \le n$. Otherwise, $\boldsymbol{X}^{\boldsymbol{u}^+}$ divides $\boldsymbol{X}^{\boldsymbol{v}^+}$ and $\boldsymbol{X}^{\boldsymbol{u}^-}$ divides $\boldsymbol{X}^{\boldsymbol{v}^-}$. But by Proposition 2.1, $\boldsymbol{X}^{\boldsymbol{u}^+} - \boldsymbol{X}^{\boldsymbol{u}^-}$ lies in $I_{\mathcal{C}}$ and so $\boldsymbol{u} \in \mathcal{C}$. The result follows. □

Proposition 3.2. *For every term order $\prec$, the reduced Groebner basis $\mathcal{G}_\prec$ of $I_{\mathcal{C}}$ consists of pure and primitive binomials of the form $X_i^p - 1$, $1 \le i \le n$, and $\boldsymbol{X}^{\boldsymbol{u}^+} - \boldsymbol{X}^{\boldsymbol{u}^-}$, where $\boldsymbol{u} \in \mathcal{C}$.*

Proof. Claim that $\mathcal{G}_\prec$ consists of pure binomials. Indeed, by Proposition 2.1, the ideal $I_{\mathcal{C}}$ is generated by a finite set of binomials. Apply the Buchberger algorithm to this set. In each step, the new polynomials produced are binomials, too. Thus the resulting Groebner basis consists of binomials. These binomials are pure, since the variables X_i are invertible modulo $I_{\mathcal{C}}$, $1 \le i \le n$.

Claim that each binomial $\boldsymbol{X}^{\boldsymbol{u}^+} - \boldsymbol{X}^{\boldsymbol{u}^-}$ in $\mathcal{G}_\prec$ is primitive. Indeed, let $\boldsymbol{u}^+ \succ \boldsymbol{u}^-$. Then $\boldsymbol{X}^{\boldsymbol{u}^+}$ is a minimal generator in the initial ideal of $I_\mathcal{C}$ and $\boldsymbol{X}^{\boldsymbol{u}^-}$ is a standard monomial. Suppose $\boldsymbol{X}^{\boldsymbol{u}^+} - \boldsymbol{X}^{\boldsymbol{u}^-}$ is not primitive. Take a vector $\boldsymbol{v}$ in $\mathcal{C}$ different from $\boldsymbol{u}$ such that $\boldsymbol{X}^{\boldsymbol{v}^+}$ divides $\boldsymbol{X}^{\boldsymbol{u}^+}$ and $\boldsymbol{X}^{\boldsymbol{v}^-}$ divides $\boldsymbol{X}^{\boldsymbol{u}^-}$. If $\boldsymbol{v}^+ \succ \boldsymbol{v}^-$, then $\boldsymbol{X}^{\boldsymbol{u}^+}$ is not a minimal generator, a contradiction. If $\boldsymbol{v}^+ \prec \boldsymbol{v}^-$, then $\boldsymbol{X}^{\boldsymbol{v}^-}$ is an initial monomial and so $\boldsymbol{X}^{\boldsymbol{u}^-}$ is not standard, a contradiction.

The result now follows from Proposition 3.1. □

The *universal Groebner basis* of an ideal I in $\mathbb{K}[\boldsymbol{X}]$ is the union of all reduced Groebner bases $\mathcal{G}_\prec$ of I as $\prec$ runs over all term orders. Since any ideal has only finitely many distinct initial ideals, the universal Groebner basis of an ideal is a finite set of binomials, see [9], [19]. Proposition 3.2 shows that the universal Groebner basis of $I_\mathcal{C}$ lies in the Graver basis of $I_\mathcal{C}$.

A non-zero codeword $\boldsymbol{u}$ in $\mathcal{C}$ is called a *circuit* if the support of $\boldsymbol{u}$ is minimal with respect to inclusion and the coordinate values of $\boldsymbol{u}$ are relatively prime.

Proposition 3.3. *All circuits in $\mathcal{C}$ lie in the universal Groebner basis of $I_\mathcal{C}$.*

Proof. Let $\boldsymbol{u}$ be a circuit in $\mathcal{C}$. Fix an elimination term order $\prec$ such that all variables X_i, where $u_i = 0$, are larger than the variables X_j, where $u_j \neq 0$, and write $\boldsymbol{u} = \boldsymbol{u}^+ - \boldsymbol{u}^-$ such that $\boldsymbol{u}^+ \succ \boldsymbol{u}^-$. Claim that $\boldsymbol{X}^{\boldsymbol{u}^+} - \boldsymbol{X}^{\boldsymbol{u}^-}$ appears in the reduced Groebner basis $\mathcal{G}_\prec$ of $I_\mathcal{C}$. Indeed, let $\boldsymbol{v}$ be a non-zero vector in $\mathcal{C}$ such that $\boldsymbol{v}^+ \succ \boldsymbol{v}^-$ and $\boldsymbol{X}^{\boldsymbol{v}^+}$ divides $\boldsymbol{X}^{\boldsymbol{u}^+}$. Then $\mathrm{supp}(\boldsymbol{v}^+) \subset \mathrm{supp}(\boldsymbol{u})$ and by the choice of the term order, $\mathrm{supp}(\boldsymbol{v}^-) \subset \mathrm{supp}(\boldsymbol{u})$. Hence $\mathrm{supp}(\boldsymbol{v}) \subset \mathrm{supp}(\boldsymbol{u})$. Since $\boldsymbol{u}$ is a circuit, it follows that $\boldsymbol{v}$ must be a multiple of $\boldsymbol{u}$. But $\boldsymbol{X}^{\boldsymbol{v}^+}$ divides $\boldsymbol{X}^{\boldsymbol{u}^+}$ and so $\boldsymbol{u} = \boldsymbol{v}$. □

Given two vectors $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_p^n$. We say that $\boldsymbol{u}$ is *conformal to* $\boldsymbol{v}$ if $\mathrm{supp}(\boldsymbol{u}) \subset \mathrm{supp}(\boldsymbol{v})$.

Proposition 3.4. *Each codeword $\boldsymbol{v}$ in $\mathcal{C}$ can be written as a linear combination of circuits each of which conformal to $\boldsymbol{v}$.*

Proof. Let d denote the minimum Hamming distance of $\mathcal{C}$. We proceed by induction on n. If $n = d$, then the assertion is clear. Suppose $n \geq d + 1$ and let $\boldsymbol{v}$ be a non-circuit in $\mathcal{C}$. We may assume that $\mathrm{supp}(\boldsymbol{v}) = \{1, \ldots, n\}$, since otherwise we may delete redundant columns in $\boldsymbol{H}$ and, by induction hypothesis, write $\boldsymbol{v}$ as a conformal linear combination of circuits. Take a circuit $\boldsymbol{u}$ in $\mathcal{C}$. By construction, $\boldsymbol{u}$ is conformal to $\boldsymbol{v}$. Among all non-zero coordinate ratios

v_i/u_i let λ denote the minimum. Then $\boldsymbol{v} - \lambda\boldsymbol{u}$ is conformal to $\boldsymbol{v}$ and has zero ith coordinate for some i, $1 \leq i \leq n$. By induction, the vector $\boldsymbol{v} - \lambda\boldsymbol{u}$ can be written as a linear combination of circuits each of which conformal to $\boldsymbol{v}$. Now the identity $\boldsymbol{v} = \lambda\boldsymbol{u} + (\boldsymbol{v} - \lambda\boldsymbol{u})$ provides the assertion. □

Theorem 3.5. *If $\mathcal{C}$ is a binary linear code, then the set of circuits in $\mathcal{C}$ equals the subset of the Graver basis of $\mathcal{C}$ consisting of the binomials $\boldsymbol{X}^{\boldsymbol{u}^+} - \boldsymbol{X}^{\boldsymbol{u}^-}$, where $\boldsymbol{u} \in \mathcal{C}$.*

Proof. Let $\boldsymbol{X}^{\boldsymbol{v}^+} - \boldsymbol{X}^{\boldsymbol{v}^-}$ be an element in the Graver basis of $I_{\mathcal{C}}$, where $\boldsymbol{v} \in \mathcal{C}$. By Proposition 3.4, there is a circuit $\boldsymbol{u}$ that is conformal to $\boldsymbol{v}$; that is, we can write $\boldsymbol{X}^{\boldsymbol{u}^+} - \boldsymbol{X}^{\boldsymbol{u}^-}$ such that $\text{supp}(\boldsymbol{u}^+) \subseteq \text{supp}(\boldsymbol{v}^+)$ and $\text{supp}(\boldsymbol{u}^-) \subseteq \text{supp}(\boldsymbol{v}^-)$. By hypothesis, the involved monomials are square-free and so $\boldsymbol{X}^{\boldsymbol{u}^+}$ divides $\boldsymbol{X}^{\boldsymbol{v}^+}$ and $\boldsymbol{X}^{\boldsymbol{u}^-}$ divides $\boldsymbol{X}^{\boldsymbol{v}^-}$. But $\boldsymbol{X}^{\boldsymbol{v}^+} - \boldsymbol{X}^{\boldsymbol{v}^-}$ is primitive and so $\boldsymbol{v} = \boldsymbol{u}$. The reverse inclusion follows from Propositions 3.2 and 3.3. □

Example 3.6. The binary linear code $\mathcal{C}$ given by the ideal $I_{\boldsymbol{A},2}$ in Example 2.2 is the $[7, 4, 3]$ Hamming code [14, 16]. The circuits (minimum weight vectors) of the code are 1101000, 1010100, 1000011, 0110010, 0100101, 0011001, 0001110. By Theorem 3.5, the circuits correspond to the Graver basis of the associated ideal $I_{\mathcal{C}}$: $X_1X_2X_4 - 1$, $X_1X_3X_5 - 1$, $X_1X_6X_7 - 1$, $X_2X_3X_6 - 1$, $X_2X_5X_7 - 1$, $X_3X_4X_7 - 1$, $X_4X_5X_6 - 1$, $X_i^2 + 1$, $1 \leq i \leq 7$.

References

[1] W. Adams, P. Loustaunau, *An Introduction to Groebner Bases*, Graduate Studies in Mathematics, AMS, 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*, PhD Thesis, Univ. of Insbruck (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, In: *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, 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] W. Fulton, *Introduction to Toric Varieties*, Princeton Univ. Press (1993).

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

[15] R. Hartshorne, *Algebraic Geometry*, Springer, Grad. Texts Math, **52** (1977).

[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.*, To Appear.

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