International Journal of Pure and Applied Mathematics
Volume 71 No. 4 2011, 595-608

GROEBNER BASES FOR QUATERNARY CODES

Robert Leppert[1], Mehwish Saleemi[2], Karl-Heinz Zimmermann[3] §
Institute of Computer Technology (E-13)
Hamburg University of Technology
Schwarzenbergstr. 95E, Hamburg, 21073, GERMANY

Abstract: A linear code can be described by a binomial ideal in a polynomial ring, given as the sum of a toric ideal and a nonprime ideal. A Groebner basis for such an ideal can be read off from a systematic generator matrix for the corresponding code. In this paper, an analogue result will be presented for quaternary codes.

AMS Subject Classification: 13P10, 94B05
Key Words: linear code, binomial ideal, polynomial ring, toric ideal, nonprime ideal, Groebner basis, quaternary codes

1. Introduction

In order to protect digital data signals send through a noise channel, error-correcting codes add redundancy to the information that allows to detect and correct errors which may have occured during transmission. In algebraic coding theory codes are described using algebraic structures and are studied in regard to key properties like number of codewords, number of detectable or correctable errors, or complexity of encoding and decoding [18, 19]. For example, a well-studied class of codes are the linear codes which are subspaces of an ambient vector space over a finite field. The most prominent linear codes are the cyclic codes and the Reed Muller codes, which facilitate encoding and decoding.

Around 1970 several binary nonlinear codes were constructed like the Kerdock, Preperata and Goethals codes [14, 17, 19, 21]. Kerdock and Preparata codes exist for all lengths $n = 4^l \geq 16$. At length 16, they coincide giving

Received: April 13, 2011

§Correspondence author

the Nordstrom-Robinson code [20]. These codes prominently contain about as many codewords as any known linear code with the same length and error correction capability. It was known early that Kerdock and Preparata codes are dual in the combinatorial sense that the weight distribution of one is the MacWilliams transform of the weight distribution of the other [19]. In 1994, Hammons et al. [16] accomplished a breakthrough when they showed that these nonlinear codes are binary image of $\mathbb{Z}_4$-linear codes under the Gray map and these $\mathbb{Z}_4$-analogues given as extended cyclic codes over $\mathbb{Z}_4$ are duals in the algebraic sense.

Groebner basis theory and algorithms were originally devised by Buchberger to solve fundamental problems in commutative algebra [5, 6], and have since become a powerful and widely used tool in algebraic geometry and commutative algebra to handle a large variety of problems which can be represented by multivariate polynomials [9, 10, 11, 22, 25].

Recently, binary linear codes were linked to binomial ideals [4]. In [23, 24] it has been shown that a linear code can be described by a binomial ideal given as the sum of a toric ideal and a nonprime ideal and that the reduced Groebner basis of this ideal (with respect to a lexicographic order) can be read off from the systematic generator matrix of the code. The calculations can be carried out in a polynomial ring over an algebraically closed field of characteristic 0 which provides the most comfortable situation in commutative algebra and algebraic geometry.

This paper strongly builds on these results and extends them to quaternary codes. It will be shown that a minimal Groebner basis of a quaternary code can be read off from its generator matrix and further calculations lead to the reduced Groebner basis.

2. Quaternary and Binary Codes

A quaternary code $\mathcal{C}$ of length n is an additive subgroup of $\mathbb{Z}_4^n$. An inner product on $\mathbb{Z}_4^n$ is defined by $\boldsymbol{a}\cdot\boldsymbol{b} = a_1b_1 + \cdots + a_nb_n \pmod 4$ and then the notions of dual code, self-orthogonal code ($\mathcal{C} \subseteq \mathcal{C}^\perp$), and self-dual code ($\mathcal{C} = \mathcal{C}^\perp$) are defined as usual. An element $\boldsymbol{c}$ of $\mathcal{C}$ is called a codeword and written as a row vector. The support of $\boldsymbol{c}$ consists of the coordinates at which it has nonzero entries, $\mathrm{supp}(\boldsymbol{c}) = \{i \mid c_i \neq 0\}$.

Two quaternary codes of the same length that differ only by a permutation of coordinates are called permutation-equivalent. Any quaternary code is permutation-equivalent to a quaternary code $\mathcal{C}$ with generator matrix of the

shape

$$\boldsymbol{G} = \begin{pmatrix} \boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{0} & 2\boldsymbol{I}_{k_2} & 2\boldsymbol{C} \end{pmatrix}, \tag{1}$$

where $\boldsymbol{A}$ and $\boldsymbol{C}$ are $\mathbb{Z}_2$-matrices, $\boldsymbol{B}$ is a $\mathbb{Z}_4$-matrix, and $\boldsymbol{I}_k$ is the $k \times k$ identity matrix. Thus the code is an elementary abelian group of type $4^{k_1}2^{k_2}$ having $2^{2k_1+k_2}$ codewords. Quaternary codes can be considered as $\mathbb{Z}_4$-modules. A quaternary code of type $4^{k_1}2^{k_2}$ is a free $\mathbb{Z}_4$-module if and only if $k_2 = 0$.

If a quaternary code $\mathcal{C}$ has generator matrix (1), then the dual code $\mathcal{C}^{\perp}$ is of type $4^{n-k_1-k_2}2^{k_2}$ and has generator matrix

$$\boldsymbol{H} = \begin{pmatrix} -\boldsymbol{B}^T - \boldsymbol{C}^T\boldsymbol{A}^T & \boldsymbol{C}^T & \boldsymbol{I}_{n-k_1-k_2} \\ 2\boldsymbol{A}^T & 2\boldsymbol{I}_{k_2} & \boldsymbol{0} \end{pmatrix}. \tag{2}$$

Define two maps from $\mathbb{Z}_4$ to $\mathbb{Z}_2$ as follows,

a	$\beta(a)$	$\gamma(a)$
0	0	0
1	0	1
2	1	1
3	1	0

These maps can be extended componentwise to maps from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^n$. Using these maps, define the Gray map $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ as

$$\phi(\boldsymbol{a}) = (\beta(\boldsymbol{a}), \gamma(\boldsymbol{a})), \quad \boldsymbol{a} \in \mathbb{Z}_4^n. \tag{3}$$

Define the Lee weights of 0, 1, 2, 3 in $\mathbb{Z}_4$ as 0, 1, 2, 1, respectively, and the weight $\mathrm{wt}_L(\boldsymbol{a})$ of $\boldsymbol{a} \in \mathbb{Z}_4^n$ as the integral sum of the Lee weights of its components. This weight function provides a distance d_L on $\mathbb{Z}_4^n$ called the Lee metric. The Gray map is an isometry from $\mathbb{Z}_4^n$ equipped with the Lee distance to $\mathbb{Z}_2^{2n}$ equipped with the Hamming distance [16]. The image of a quaternary code $\mathcal{C}$ under the Gray map ϕ is generally a nonlinear binary code $C = \phi(\mathcal{C})$ of length $2n$. A binary code C is called $\mathbb{Z}_4$-linear if its coordinates can be permuted in a way that it is the image of a quaternary code $\mathcal{C}$ under the Gray map.

The Kerdock and Preparata codes can be described as extended cyclic codes over $\mathbb{Z}_4$. To see this, let $h_2(X) \in \mathbb{Z}_2[X]$ be a primitive irreducible polynomial of degree m. There is a unique monic polynomial $h(X) \in \mathbb{Z}_4[X]$ of degree m so that $h(X) \equiv h_2(X) \pmod 2$ and $h(X)$ divides $X^n - 1 \pmod 4$, where

$n = 2^m - 1$. The polynomial $h(X)$ is a primitive basic irreducible polynomial and may be found by Graeffe's method [26].

Let $g(X)$ be the reciprocal polynomial to $(X^n-1)/[(X-1)h(X)]$. The cyclic code generated by $g(X)$, extended by an overall parity check, is a quaternary code $\mathcal{K}$ of length 2^m. This code is a free $\mathbb{Z}_4$-module of type 4^{m+1}. More specifically, write $g(X) = \sum_{i=0}^{l} g_i X^i$, where $l = 2^m - m - 2$, and put $g_\infty = -\sum_{i=0}^{l} g_i$. The code $\mathcal{K}$ has the generator matrix

$$\begin{pmatrix} g_\infty & g_0 & g_1 & \dots & g_l & 0 & \dots & 0 \\ g_\infty & 0 & g_0 & \dots & g_{l-1} & g_l & \dots & 0 \\ . & . & . & & . & . & & . \\ g_\infty & 0 & 0 & \dots & g_0 & g_1 & \dots & g_l \end{pmatrix}. \tag{4}$$

For $m \geq 3$ odd, the associated binary code $K = \phi(\mathcal{K})$ is the Kerdock code of length 2^{m+1} with 2^{2m+2} codewords and minimal distance $2^m - 2^{(m-1)/2}$ [16, 17].

The cyclic code generated by $h(X)$, extended by an overall parity check, is a quaternary code $\mathcal{P}$ that is dual to the code $\mathcal{K}$. This code is a free $\mathbb{Z}_4$-module of type 4^{2^m-m-1}. For $m \geq 3$ odd, the corresponding binary code $P = \phi(\mathcal{P})$ is the Preparata code of length 2^{m+1} with 2^k codewords, where $k = 2^{m+1} - 2m - 2$, and minimal distance 6. Note that Preparata's original code is a variant of this code with essentially the same properties [16, 21].

In the case of $m = 3$, both the Kerdock code and the Preparata code coincide; this code is known as the Nordstrom-Robinson code.

Example 2.1. Let $m = 3$. Take the polynomial $h_2(X) = X^3 + X + 1$. Then $h(X) = X^3 + 2X^2 + X - 1$ and $g(X) = h(X)$. The cyclic code generated by $h(X)$, extended by an overall parity check, is the octacode $\mathcal{O}$ given by the generator matrix

$$\begin{pmatrix} 1 & 3 & 1 & 2 & 1 & 0 & 0 & 0 \\ 1 & 0 & 3 & 1 & 2 & 1 & 0 & 0 \\ 1 & 0 & 0 & 3 & 1 & 2 & 1 & 0 \\ 1 & 0 & 0 & 0 & 3 & 1 & 2 & 1 \end{pmatrix}. \tag{5}$$

The octacode is a free $\mathbb{Z}_4$-module of type 4^4 and can be characterized as the unique self-dual quaternary code of length 8 and minimal Lee weight 6. The binary image of the octacode under the Gray map is the Nordstrom-Robinson code [20]. This code is nonlinear and can be characterized as the unique binary code of length 16, minimal distance 6, containing 256 words. Note that the best linear binary code of length 16 and minimal distance 6 has only 128 words [15].

3. Gröbner Bases and Linear Codes

Throughout this paper let $\mathbb{K}$ be a field. For each integral vector $\boldsymbol{a} \in \mathbb{N}_0^n$, the product $\boldsymbol{X}^{\boldsymbol{a}} = X_1^{a_1} \dots X_n^{a_n}$ in the unknowns $X_1, \dots X_n$ over $\mathbb{K}$ is called a monomial. A polynomial $f = \sum_a c_a \boldsymbol{X}^{\boldsymbol{a}}$ is a finite linear combination of monomial; the nonzero summands $c_a \boldsymbol{X}^{\boldsymbol{a}}$ are called terms. The set of all polynomials in $X_1, \dots X_n$ over $\mathbb{K}$ is a commutative ring denoted as $\mathbb{K}[\boldsymbol{X}] = \mathbb{K}[X_1, \dots X_n]$.

A monomial ordering on $\mathbb{K}[\boldsymbol{X}]$ is a relation $\prec$ on the set of monomials in $\mathbb{K}[\boldsymbol{X}]$, or equivalently, on the exponent vectors in $\mathbb{N}_0^n$ such that (i) $\prec$ is a total order, (ii) $\boldsymbol{0} = (0, \dots, 0)$ is the unique minimal element, and (iii) $\boldsymbol{a} \prec \boldsymbol{b}$ implies $\boldsymbol{a}+\boldsymbol{c} \prec \boldsymbol{b}+\boldsymbol{c}$ for all $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{N}_0^n$. A familiar example is the purely lexicographic order, i.e., $\boldsymbol{a} \prec_{lex} \boldsymbol{b}$ if and only if in $\boldsymbol{a} - \boldsymbol{b} \in \mathbb{Z}^n$ the leftmost nonzero entry is negative. Given a monomial order $\prec$ on $\mathbb{K}[\boldsymbol{X}]$, each polynomial $f \in \mathbb{K}[\boldsymbol{X}]$ has a unique largest monomial. The corresponding term is called the initial term of f and denoted by $\mathrm{in}_\prec(f)$. The initial terms of all polynomials in an ideal I of $\mathbb{K}[\boldsymbol{X}]$ generate the so-called initial ideal of I given by $\mathrm{in}_\prec(I) = \langle \mathrm{in}_\prec(f) \mid f \in I \rangle$.

Fix a monomial order $\prec$ on $\mathbb{K}[\boldsymbol{X}]$ and take a finite subset $\mathcal{G}_\prec$ of an ideal I in $\mathbb{K}[\boldsymbol{X}]$. If the initial term of any polynomial in I is divisible by the initial term of some polynomial in $\mathcal{G}_\prec$, the set $\mathcal{G}_\prec$ is a called a Groebner basis for I. A Groebner basis for I is called minimal if and only if all its elements are monic, i.e. have the leading coefficient of 1, and no initial term of one element is divisible by the initial term of another one. If even no term of one element is divisible by any initial term of another element, the basis is called reduced. Each ideal has a unique reduced Groebner basis.

Let $\mathcal{F} = \{f_1, \dots, f_s\}$ be an ordered set of polynomials. Each polynomial $f \in \mathbb{K}[\boldsymbol{X}]$ can be written as a unique linear combination of these polynomials by using the multivariate division algorithm in the form

$$f = \sum_{i=1}^{s} h_i f_i + r, \tag{6}$$

where $h_1, \dots, h_s, r \in \mathbb{K}[\boldsymbol{X}]$, $\mathrm{in}_\prec(h_i f_i) \preceq \mathrm{in}_\prec(f)$ if $h_i f_i \neq 0$ and either $r = 0$ or r is a sum of terms none of which is divisible by any of $\mathrm{in}_\prec(f_i)$, $1 \leq i \leq s$. The polynomial r is the remainder of f on division by $\mathcal{F}$ and is denoted by $r = \mathrm{rem}(f, \mathcal{F})$. The division can be accomplished by the following recursion: If the leading term of f is divisible by any of the initial terms $\mathrm{in}_\prec(f_i)$, then let $\mathrm{rem}(f, \mathcal{F}) = \mathrm{rem}(f - \frac{\mathrm{in}_\prec(f)}{\mathrm{in}_\prec(f_i)} f_i, \mathcal{F})$, where i smallest. Otherwise, that part is placed into the remainder: $\mathrm{rem}(f, \mathcal{F}) = \mathrm{in}_\prec(f) + \mathrm{rem}(f - \mathrm{in}_\prec(f), \mathcal{F})$. The algorithm terminates since in both cases the initial term of f decreases.

For any polynomial $f \in \mathbb{K}[\boldsymbol{X}]$, the difference $f - \mathrm{rem}(f, \mathcal{F})$ lies in the ideal $\langle F \rangle$ generated by $\mathcal{F}$. In particular, if $\mathcal{G}$ is a Groebner basis for an ideal I in $\mathbb{K}[\boldsymbol{X}]$, the ideal generated by $\mathcal{G}$ coincides with I and for each polynomial f in $\mathbb{K}[\boldsymbol{X}]$, f lies in I if and only if $\mathrm{rem}(f, \mathcal{G}) = 0$.

A minimal Groebner basis $\mathcal{G}$ for an ideal I in $\mathbb{K}[\boldsymbol{X}]$ can be transformed into the reduced one by the following algorithm: Take a monomial of an element $g \in \mathcal{G}$ that is divisable by the initial term of another element of $\mathcal{G}$. Then form $\mathcal{G}' = (\mathcal{G} \setminus \{g\}) \cup \{g'\}$, where $g' = \mathrm{rem}(g, \mathcal{G} \setminus \{g\})$. The set $\mathcal{G}'$ is also a minimal Groebner basis for I and repeating this step will eventually lead to the reduced basis.

A Groebner basis for an ideal I in $\mathbb{K}[\boldsymbol{X}]$ and a monomial order $\prec$ on $\mathbb{K}[\boldsymbol{X}]$ can be computed by Buchberger's algorithm. It begins with an arbitrary generating set for I and calculates in each step new elements of I by using expressions which guarantee to cancel leading terms and in this way eventually reveal other leading terms. These new elements are S-polynomials of polynomials f and g defined as

$$S(f,g) = \frac{\boldsymbol{X}^{\boldsymbol{u}}}{\mathrm{in}_{\succ}(f)} \cdot f - \frac{\boldsymbol{X}^{\boldsymbol{u}}}{\mathrm{in}_{\succ}(g)} \cdot g, \tag{7}$$

where $\boldsymbol{X}^{\boldsymbol{u}}$ is the least common multiple of the leading monomials of f and g. Buchberger's S-criterion says that a set of polynomials $\mathcal{G} = \{g_1, \ldots, g_s\}$ in $\mathbb{K}[\boldsymbol{X}]$ is a Groebner basis for the ideal $I = \langle g_1, \ldots, g_s \rangle$ if and only if the remainder on division of $S(g_i, g_j)$ by $\mathcal{G}$ is 0 for all $1 \leq i < j \leq s$. More details on Groebner bases can be found in [1, 2, 7, 9].

Toric varieties provide an good source of examples in algebraic geometry in order to test hypothesis for general theories. Affine toric varieties arise from toric ideals in polynomial rings [3, 13].

A binomial in the 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. Given a monomial order $\prec$ on $\mathbb{K}[\boldsymbol{X}]$. Each reduced Groebner basis of a binomial ideal I in $\mathbb{K}[\boldsymbol{X}]$ with respect to $\prec$ consists of binomials. Indeed, if there is a binomial generating set for I, then the new elements produced by a step in Buchberger's algorithm are also binomials [12].

Let $\boldsymbol{A} = (\boldsymbol{a}_1 \ldots \boldsymbol{a}_n) \in \mathbb{N}_0^{m \times n}$ be an integer matrix with columns $\boldsymbol{a}_i$, $1 \leq i \leq n$. Take the columns as exponent vectors for a collection of monomials $m_i = \boldsymbol{Y}^{\boldsymbol{a}_i}$ in the polynomial ring $\mathbb{K}[\boldsymbol{Y}] = \mathbb{K}[Y_1, \ldots, Y_m]$. The toric ideal associated with $\boldsymbol{A}$, denoted by $I_{\boldsymbol{A}}$, is given by the kernel of the $\mathbb{K}$-algebra homomorphism $\phi : \mathbb{K}[\boldsymbol{X}] \to \mathbb{K}[\boldsymbol{Y}] : \ X_i \mapsto m_i$, $1 \leq i \leq n$. This ideal is prime because it is defined as the kernel of a morphism into an integral domain. To see that this

ideal is also binomial, consider the extended homomorphism $\psi : \mathbb{K}[\boldsymbol{X}, \boldsymbol{Y}] \to \mathbb{K}[\boldsymbol{Y}] : X_i \mapsto m_i$, $1 \leq i \leq n$, and $Y_j \mapsto Y_j$, $1 \leq j \leq m$, for which the kernel can be directly given as the ideal $J = \langle X_i - m_i \mid 1 \leq i \leq n \rangle$. The ideal J is binomial and Groebner basis theory tells that any Groebner basis for J consists of binomials, too. Furthermore, if $\mathcal{G}_J$ is Groebner basis for J then by the elimination property $\mathcal{G}_{I_{\boldsymbol{A}}} = \mathcal{G}_J \cap \mathbb{K}[\boldsymbol{X}]$ is a Groebner basis for the ideal $I_{\boldsymbol{A}} = J \cap \mathbb{K}[\boldsymbol{X}]$ with respect to a lexicographic order in which each Y_i is larger than any X_i. Moreover, the ideal $I_{\boldsymbol{A}}$ is generated by binomials as follows:

$$I_{\boldsymbol{A}} = \langle \boldsymbol{X}^{\boldsymbol{u}} - \boldsymbol{X}^{\boldsymbol{v}} \mid \boldsymbol{A}\boldsymbol{u} = \boldsymbol{A}\boldsymbol{v}, \boldsymbol{u}, \boldsymbol{v} \in \mathbb{N}_0^n \rangle \,. \tag{8}$$

Indeed, each binomial $\boldsymbol{X}^{\boldsymbol{u}} - \boldsymbol{X}^{\boldsymbol{v}}$ with $\boldsymbol{A}\boldsymbol{u} = \boldsymbol{A}\boldsymbol{v}$ lies in $I_{\mathcal{A}}$, since $\phi(\boldsymbol{X}^{\boldsymbol{u}}) = \boldsymbol{Y}^{\boldsymbol{A}\boldsymbol{u}}$. Conversely, suppose there are elements in $I_{\boldsymbol{A}}$ which cannot be written as $\mathbb{K}$-linear combinations of binomials. Take a monomial order $\prec$ on $\mathbb{K}[\boldsymbol{X}]$ and choose a monic element $f \in I_{\boldsymbol{A}}$ with this property such that its leading monomial $\boldsymbol{X}^{\boldsymbol{u}}$ is minimal with respect to $\prec$. The expansion $\phi(f) = f(Y^{\boldsymbol{a}_1}, \ldots, Y^{\boldsymbol{a}_n})$ gives zero and thus the term $\boldsymbol{Y}^{\boldsymbol{A}\boldsymbol{u}}$ must cancel. Thus there is another monomial $\boldsymbol{X}^{\boldsymbol{v}}$ in f such that $\boldsymbol{v} \prec \boldsymbol{u}$ and $\boldsymbol{A}\boldsymbol{v} = \boldsymbol{A}\boldsymbol{u}$. The polynomial $g = f - \boldsymbol{X}^{\boldsymbol{u}} + \boldsymbol{X}^{\boldsymbol{v}}$ lies in $I_{\boldsymbol{A}}$ and by hypothesis cannot be written as an $\mathbb{K}$-linear combination of binomials. But $\mathrm{in}_{\prec}(g) \prec \mathrm{in}_{\prec}(f)$ contradicting the assumption. The claim follows. Furthermore, the generators $\boldsymbol{X}^{\boldsymbol{u}} - \boldsymbol{X}^{\boldsymbol{v}}$ of the ideal $I_{\boldsymbol{A}}$ can be chosen to be pure, i.e. $\gcd(\boldsymbol{X}^{\boldsymbol{u}}, \boldsymbol{X}^{\boldsymbol{v}}) = 1$.

Let $p \geq 2$ be an integer. The toric ideal $I_{\boldsymbol{A}}$ gets associated with the binomial ideal

$$I_{\boldsymbol{A},p} = I_{\boldsymbol{A}} + \langle X_i^p - 1 \mid 1 \leq i \leq n \rangle \tag{9}$$

This ideal is not toric, because it is not prime as the polynomials $X_i^p - 1$, $1 \leq i \leq n$, are reducible. By [24], this ideal can be written as

$$\begin{aligned} I_{\boldsymbol{A},p} \;=\; & \langle \boldsymbol{X}^{\boldsymbol{u}} - \boldsymbol{X}^{\boldsymbol{v}} \mid \boldsymbol{A}\boldsymbol{u} \equiv \boldsymbol{A}\boldsymbol{v} \bmod p, \boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}_p^n, \boldsymbol{X}^{\boldsymbol{u}} - \boldsymbol{X}^{\boldsymbol{v}} \;\text{ pure} \rangle \\ & + \langle X_i^p - 1 \mid 1 \leq i \leq n \rangle \,. \end{aligned} \tag{10}$$

This allows to study quaternary codes in the framework of polynomial rings and Groebner bases.

4. Groebner Bases for Quaternary Codes

Let $\mathcal{C}$ be a quaternary code whose parity check matrix $\boldsymbol{H}$ is given by (2). Choose $\boldsymbol{A}$ to be an integral matrix such that $\boldsymbol{H} = \boldsymbol{A} \otimes_{\mathbb{Z}} \mathbb{Z}_4$ and consider the binomial

ideal

$$I_{\boldsymbol{A},4} = I_{\boldsymbol{A}} + \langle X_i^4 - 1 \,|\, 1 \le i \le n \rangle. \tag{11}$$

Recall that for each codeword $\boldsymbol{c}$ in $\mathcal{C}$, $\boldsymbol{c}\boldsymbol{H}^t = 0$. But any codeword $\boldsymbol{c}$ can be written as $\boldsymbol{c} = \boldsymbol{c}_+ - \boldsymbol{c}_-$, where $\boldsymbol{c}_+$ and $\boldsymbol{c}_-$ are elements of $\mathbb{Z}_4^n$ with disjoint support. Thus $\boldsymbol{c}_+\boldsymbol{H}^t = \boldsymbol{c}_-\boldsymbol{H}^t$ and hence the pure binomial $\boldsymbol{X}^{\boldsymbol{c}_+} - \boldsymbol{X}^{\boldsymbol{c}_-}$ lies in the ideal $I_{\mathcal{A},4}$. In view of (10), this ideal is equivalent to

$$I_{\mathcal{C}} = \langle \boldsymbol{X}^{\boldsymbol{c}_+} - \boldsymbol{X}^{\boldsymbol{c}_-} \,|\, \boldsymbol{c}_+ - \boldsymbol{c}_- \in \mathcal{C} \rangle + \langle X_i^4 - 1 \,|\, 1 \le i \le n \rangle, \tag{12}$$

which is called the ideal associated with the code $\mathcal{C}$ [4, 23].

Each binomial of the form $\boldsymbol{X}^{\boldsymbol{c}_+} - \boldsymbol{X}^{\boldsymbol{c}_-}$ in $I_{\mathcal{C}}$ is equivalent to the binomial $\boldsymbol{X}^{\boldsymbol{c}_+ - \boldsymbol{c}_-} - 1$ modulo $I_{\mathcal{C}}$. Indeed, if $X_i^k Y - Z$ lies in $I_{\mathcal{C}}$, $1 \le i \le n$, $1 \le k \le 3$, then $Y - X_i^{4-k} Z = X_i^{4-k}(X_i^k Y - Z) - Y(X_i^4 - 1)$ is in $I_{\mathcal{C}}$ as well.

In the following, let $\mathcal{C}$ be a quaternary code whose generator matrix is given by (1). Let $\boldsymbol{a}_i$, $\boldsymbol{b}_i$, and $\boldsymbol{c}_j$ be the length-n vectors containing the rows of the submatrices $-\boldsymbol{A}$, $-\boldsymbol{B}$, and $-\boldsymbol{C}$, respectively. That is,

$$\boldsymbol{a}_i = (0, \ldots, 0, -g_{i,k_1+1}, \ldots, -g_{i,k_1+k_2}, 0, \ldots, 0),\ 1 \le i \le k_1, \tag{13}$$

$$\boldsymbol{b}_i = (0, \ldots, 0, -g_{i,k_1+k_2+1}, \ldots, -g_{i,n}),\ 1 \le i \le k_1, \tag{14}$$

$$\boldsymbol{c}_j = (0, \ldots, 0, -g_{j,k_1+k_2+1}, \ldots, -g_{j,n}),\ k_1 + 1 \le j \le n, \tag{15}$$

where entries are considered to be elements of $\mathbb{Z}_4$.

Theorem 4.1. *Take the lexicographic order on the polynomial ring $\mathbb{K}[\boldsymbol{X}]$ such that $X_1 \succ \ldots \succ X_n$. Then the ideal $I_{\mathcal{C}}$ has the minimal Groebner basis*

$$\begin{aligned} \mathcal{G} \;=\; & \{X_i - \boldsymbol{X}^{\boldsymbol{a}_i}\boldsymbol{X}^{\boldsymbol{b}_i} \mid 1 \le i \le k_1\} \\ & \cup \{X_i^2 - \boldsymbol{X}^{2\boldsymbol{c}_i} \mid k_1 + 1 \le i \le k_1 + k_2\} \\ & \cup \{X_i^4 - 1 \mid k_1 + k_2 + 1 \le i \le n\}. \end{aligned} \tag{16}$$

Proof: The elements of $\mathcal{G}$ lie in the ideal $I_{\mathcal{C}}$ by definition.

Conversely, claim that the generators of $I_{\mathcal{C}}$ lie in the ideal generated by $\mathcal{G}$. First, the binomial $X_i^4 - 1$, $1 \le i \le k_1$ can be reduced to $\boldsymbol{X}^{4\boldsymbol{a}_i}\boldsymbol{X}^{4\boldsymbol{b}_i} - 1$ using the binomials $X_i - \boldsymbol{X}^{\boldsymbol{a}_i}\boldsymbol{X}^{\boldsymbol{b}_i}$ in $\mathcal{G}$. Let $a_{ij} \neq 0$, i.e. $a_{ij} = 3$, for some $k_1 + 1 \le j \le k_1 + k_2$. Let j be minimal with this property. Then $\boldsymbol{X}^{4\boldsymbol{a}_i} = X_j^{4a_{ij}}\boldsymbol{X}^{4\boldsymbol{a}'_i}$ and so

$$\begin{aligned} & \mathrm{rem}(\boldsymbol{X}^{4\boldsymbol{a_i}}\boldsymbol{X}^{4\boldsymbol{b_i}} - 1, \mathcal{G}) = \\ & \quad = \mathrm{rem}(X_j^{4a_{ij}}\boldsymbol{X}^{4\boldsymbol{a'_i}}\boldsymbol{X}^{4\boldsymbol{b_i}} - 1 - X_j^{4a_{ij}-2}\boldsymbol{X}^{4\boldsymbol{a'_i}}\boldsymbol{X}^{4\boldsymbol{b_i}}(X_j^2 - \boldsymbol{X}^{2\boldsymbol{c_j}}), \mathcal{G}) \end{aligned}$$

$$= \quad \mathrm{rem}(X_j^{4a_{ij}-2}\boldsymbol{X}^{4\boldsymbol{a_i'}}\boldsymbol{X}^{4\boldsymbol{b_i}+2\boldsymbol{c_j}}-1,\mathcal{G}).$$

Further reductions by using the binomials $X_j^2-\boldsymbol{X}^{2\boldsymbol{c_j}}$ in $\mathcal{G}$ lead to

$$\mathrm{rem}(\boldsymbol{X}^{4\boldsymbol{a_i'}}\boldsymbol{X}^{4\boldsymbol{b_i}+4\,a_{ij}\,\boldsymbol{c_j}}-1,\mathcal{G})$$

and then to

$$\mathrm{rem}(\boldsymbol{X}^{4\boldsymbol{b_i}+\sum_{j=k_1+1}^{k_1+k_2}4\,a_{ij}\,\boldsymbol{c_j}}-1,\mathcal{G}).$$

The occuring exponents are zero modulo 4 and thus the binomial can further be reduced by X_i^4-1, $k_1+k_2+1\le i\le n$, to zero .

Second, X_i^4-1, $k_1+1\le i\le k_1+k_2$ can be reduced to $\boldsymbol{X}^{4\boldsymbol{c_i}}-1$ using the binomials $X_i^2-\boldsymbol{X}^{2\boldsymbol{c_i}}$ in $\mathcal{G}$. The latter polynomial reduces to zero as in the first case.

Third, let $\boldsymbol{X}^{\boldsymbol{w_+}}-\boldsymbol{X}^{\boldsymbol{w_-}}$ be an element of $I_{\mathcal{C}}$ with $\boldsymbol{w_+}-\boldsymbol{w_-}\in\mathcal{C}$. Consider its equivalent binomial $\boldsymbol{X}^{\boldsymbol{w}}-1$. The corresponding codeword $\boldsymbol{w}=\boldsymbol{w_+}-\boldsymbol{w_-}\in\mathbb{Z}_4^n$ is encoded by an information vector of the form $\boldsymbol{u}=(\boldsymbol{u_1},\boldsymbol{u_2})$, where $\boldsymbol{u_1}\in\mathbb{Z}_4^{k_1}$ and $\boldsymbol{u_2}\in\mathbb{Z}_2^{k_2}$. Thus

$$\boldsymbol{w}=\boldsymbol{u}\,\boldsymbol{G}=(\boldsymbol{u_1},\ \boldsymbol{u_1}\boldsymbol{A}+2\,\boldsymbol{u_2},\ \boldsymbol{u_1}\boldsymbol{B}+\boldsymbol{u_2}2\boldsymbol{C}).$$

Stepwise reduction using the binomials $X_i-\boldsymbol{X}^{\boldsymbol{a_i}}\boldsymbol{X}^{\boldsymbol{b_i}}$ in $\mathcal{G}$ leads to the binomial $\boldsymbol{X}^{\boldsymbol{w'}}-1$, where

$$\begin{aligned}\boldsymbol{w'} &= (\boldsymbol{0},\ \boldsymbol{u_1}\boldsymbol{A}+2\,\boldsymbol{u_2}+\boldsymbol{u_1}(-\boldsymbol{A}),\ \boldsymbol{u_1}\boldsymbol{B}+\boldsymbol{u_2}\,2\boldsymbol{C}+\boldsymbol{u_1}(-\boldsymbol{B}))\\ &= (\boldsymbol{0},\ 2\,\boldsymbol{u_2},\ \boldsymbol{u_2}\,2\boldsymbol{C}).\end{aligned}$$

This binomial, in turn, can be reduced to the binomial $\boldsymbol{X}^{\boldsymbol{w''}}-1$, where

$$\boldsymbol{w''}=(\boldsymbol{0},\ \boldsymbol{0},\ \boldsymbol{u_2}\,2\boldsymbol{C}+\boldsymbol{u_2}(-2\boldsymbol{C})),$$

by using the binomials $X_i^2-\boldsymbol{X}^{2\boldsymbol{c_i}}$ in $\mathcal{G}$. This proves the claim.

Next, claim that $\mathcal{G}$ is a Groebner basis for $I_{\mathcal{C}}$. Indeed, Buchberger's S-criterion leads to six cases: First, let $1\le i<j\le k_1$. Then

$$S(X_i-\boldsymbol{X}^{\boldsymbol{a_i}}\boldsymbol{X}^{\boldsymbol{b_i}},X_j-\boldsymbol{X}^{\boldsymbol{a_j}}\boldsymbol{X}^{\boldsymbol{b_j}})=X_i\boldsymbol{X}^{\boldsymbol{a_j}}\boldsymbol{X}^{\boldsymbol{b_j}}-X_j\boldsymbol{X}^{\boldsymbol{a_i}}\boldsymbol{X}^{\boldsymbol{b_i}},$$

which is divided by $\mathcal{G}$ as follows:

$$\begin{aligned}&\mathrm{rem}(X_i\boldsymbol{X}^{\boldsymbol{a_j}}\boldsymbol{X}^{\boldsymbol{b_j}}-X_j\boldsymbol{X}^{\boldsymbol{a_i}}\boldsymbol{X}^{\boldsymbol{b_i}},\mathcal{G})\\ &=\mathrm{rem}(X_i\boldsymbol{X}^{\boldsymbol{a_j}}\boldsymbol{X}^{\boldsymbol{b_j}}-X_j\boldsymbol{X}^{\boldsymbol{a_i}}\boldsymbol{X}^{\boldsymbol{b_i}}-\boldsymbol{X}^{\boldsymbol{a_j}}\boldsymbol{X}^{\boldsymbol{b_j}}(X_i-\boldsymbol{X}^{\boldsymbol{a_i}}\boldsymbol{X}^{\boldsymbol{b_i}}),\mathcal{G})\end{aligned}$$

$$= \mathrm{rem}(-X_j \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}} + \boldsymbol{X}^{\boldsymbol{a_i}+\boldsymbol{a_j}} \boldsymbol{X}^{\boldsymbol{b_i}+\boldsymbol{b_j}}, \mathcal{G})$$
$$= \mathrm{rem}(-X_j \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}} + \boldsymbol{X}^{\boldsymbol{a_i}+\boldsymbol{a_j}} \boldsymbol{X}^{\boldsymbol{b_i}+\boldsymbol{b_j}} + \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}} (X_j - \boldsymbol{X}^{\boldsymbol{a_j}} \boldsymbol{X}^{\boldsymbol{b_j}}), \mathcal{G}) = 0.$$

Second, let $k_1 + 1 \leq i < j \leq k_1 + k_2$. Then

$$S(X_i^2 - \boldsymbol{X}^{2\boldsymbol{c_i}}, X_j^2 - \boldsymbol{X}^{2\boldsymbol{c_j}}) = X_i^2 \boldsymbol{X}^{2\boldsymbol{c_j}} - X_j^2 \boldsymbol{X}^{2\boldsymbol{c_i}}.$$

Its remainder modulo $\mathcal{G}$ is

$$\begin{aligned}
&\mathrm{rem}(X_i^2 \boldsymbol{X}^{2\boldsymbol{c_j}} - X_j^2 \boldsymbol{X}^{2\boldsymbol{c_i}}, \mathcal{G}) \\
&= \mathrm{rem}(X_i^2 \boldsymbol{X}^{2\boldsymbol{c_j}} - X_j^2 \boldsymbol{X}^{2\boldsymbol{c_i}} - \boldsymbol{X}^{2\boldsymbol{c_j}} (X_i^2 - \boldsymbol{X}^{2\boldsymbol{c_i}}), \mathcal{G}) \\
&= \mathrm{rem}(-X_j^2 \boldsymbol{X}^{2\boldsymbol{c_i}} + \boldsymbol{X}^{2\boldsymbol{c_i}+2\boldsymbol{c_j}}, \mathcal{G}) \\
&= \mathrm{rem}(-X_j^2 \boldsymbol{X}^{2\boldsymbol{c_i}} + \boldsymbol{X}^{2\boldsymbol{c_i}+2\boldsymbol{c_j}} + \boldsymbol{X}^{2\boldsymbol{c_i}} (X_j^2 - \boldsymbol{X}^{2\boldsymbol{c_j}}), \mathcal{G}) = 0.
\end{aligned}$$

Third, let $k_1 + k_2 + 1 \leq i < j \leq n$. Then

$$S(X_i^4 - 1, X_j^4 - 1) = X_i^4 - X_j^4 = (X_i^4 - 1) - (X_j^4 - 1),$$

whose reduction modulo $\mathcal{G}$ gives

$$\begin{aligned}
&\mathrm{rem}((X_i^4 - 1) - (X_j^4 - 1), \mathcal{G}) = \\
&\quad = \quad \mathrm{rem}((X_i^4 - 1) - (X_j^4 - 1) - 1 \cdot (X_i^4 - 1), \mathcal{G}) \\
&\quad = \quad \mathrm{rem}(-(X_j^4 - 1), \mathcal{G}) \\
&\quad = \quad \mathrm{rem}(-(X_j^4 - 1) - (-1) \cdot (X_j^4 - 1), \mathcal{G}) = 0.
\end{aligned}$$

Fourth, let $1 \leq i \leq k_1$ and $k_1 + 1 \leq j \leq k_1 + k_2$. Then

$$S(X_i - \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}}, X_j^2 - \boldsymbol{X}^{2\boldsymbol{c_j}}) = X_i \boldsymbol{X}^{2\boldsymbol{c_j}} - X_j^2 \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}},$$

whose division into $\mathcal{G}$ yields

$$\begin{aligned}
&\mathrm{rem}(X_i \boldsymbol{X}^{2\boldsymbol{c_j}} - X_j^2 \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}}, \mathcal{G}) \\
&= \mathrm{rem}(X_i \boldsymbol{X}^{2\boldsymbol{c_j}} - X_j^2 \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}} - \boldsymbol{X}^{2\boldsymbol{c_j}} (X_i - \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}}), \mathcal{G}) \\
&= \mathrm{rem}(-X_j^2 \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}} + \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}+2\boldsymbol{c_j}}, \mathcal{G}) \\
&= \mathrm{rem}(-X_j^2 \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}} + \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}+2\boldsymbol{c_j}} + \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}} (X_j^2 - \boldsymbol{X}^{2\boldsymbol{c_j}}), \mathcal{G}) = 0.
\end{aligned}$$

Fifth, let $1 \leq i \leq k_1$ and $k_1 + k_2 + 1 \leq j \leq n$. Then

$$S(X_i - \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}}, X_j^4 - 1) = X_i - X_j^4 \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}},$$

which is reduced by $\mathcal{G}$ as follows:

$$\begin{aligned}
&\operatorname{rem}(X_i - X_j^4 \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}}, \mathcal{G}) \\
&= \operatorname{rem}(X_i - X_j^4 \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}} - (X_i - \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}}), \mathcal{G}) \\
&= \operatorname{rem}(-X_j^4 \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}} + \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}}, \mathcal{G}) \\
&= \operatorname{rem}(-X_j^4 \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}} + \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}} - \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}} (X_j^4 - 1), \mathcal{G}) = 0.
\end{aligned}$$

Sixth, let $k_1 + 1 \le i \le k_1 + k_2$ and $k_1 + k_2 + 1 \le j \le n$. Then

$$S(X_i^2 - \boldsymbol{X}^{2\boldsymbol{c_i}}, X_j^4 - 1) = X_i^2 - X_j^4 \boldsymbol{X}^{2\boldsymbol{c_i}},$$

which provides the following remainder modulo $\mathcal{G}$:

$$\begin{aligned}
&\operatorname{rem}(X_i^2 - X_j^4 \boldsymbol{X}^{2\boldsymbol{c_i}}, \mathcal{G}) \\
&= \operatorname{rem}(X_i^2 - X_j^4 \boldsymbol{X}^{2\boldsymbol{c_i}} - (X_i^2 - \boldsymbol{X}^{2\boldsymbol{c_i}}), \mathcal{G}) \\
&= \operatorname{rem}(-X_j^4 \boldsymbol{X}^{2\boldsymbol{c_i}} + \boldsymbol{X}^{2\boldsymbol{c_i}}, \mathcal{G}) \\
&= \operatorname{rem}(-X_j^4 \boldsymbol{X}^{2\boldsymbol{c_i}} + \boldsymbol{X}^{2\boldsymbol{c_i}} + \boldsymbol{X}^{2\boldsymbol{c_i}} (X_j^4 - 1), \mathcal{G}) = 0.
\end{aligned}$$

This proves the claim. Finally, it is clear that the Groebner basis $\mathcal{G}$ is minimal. □

The Groebner basis $\mathcal{G}$ for $I_{\mathcal{C}}$ is generally not reduced. Indeed, if the submatrix $\boldsymbol{A}$ is nonzero, then the standard monomial $\boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}}$, $1 \le i \le k_1$, is divisible by the initial term of the basis element $X_j^2 - \boldsymbol{X}^{2\boldsymbol{c_j}}$, $k_1 + 1 \le j \le k_1 + k_2$, whenever there is an entry 1 in $\boldsymbol{A}$ and thus $a_{ij} = -g_{ij} = 3$.

Corollary 4.1. *By the above lexicographic order on $\mathbb{K}[\boldsymbol{X}]$, the reduced Groebner basis for $I_{\mathcal{C}}$ is*

$$\begin{aligned}
\mathcal{G} \;=\; & \big\{ X_i - \boldsymbol{X}^{(-\boldsymbol{a_i})} \boldsymbol{X}^{\boldsymbol{b_i} + \sum_{j=k_1+1}^{k_1+k_2} (-a_{ij})\, 2\boldsymbol{c_j}} \mid 1 \le i \le k_1 \big\} \\
& \cup \{ X_i^2 - \boldsymbol{X}^{2\boldsymbol{c_i}} \mid k_1 + 1 \le i \le k_1 + k_2 \} \\
& \cup \{ X_i^4 - 1 \mid k_1 + k_2 + 1 \le i \le n \},
\end{aligned} \tag{17}$$

where the exponents are elements of the set $\{0, 1, 2, 3\}$.

Proof: Note that the vector $-\boldsymbol{a}_i$ corresponds to the row of the $\mathbb{Z}_2$-matrix $\boldsymbol{A}$ with entries from $\mathbb{Z}_2$, compared to the vector $\boldsymbol{a}_i$ with entries from $\{0, 3\}$. Take an initially reducible binomial $X_i - \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}}$ and let j be minimal so that $a_{ij} = 3$. Put $\boldsymbol{X}^{\boldsymbol{a_i}} = X_j^2 \boldsymbol{X}^{\boldsymbol{a_i'}}$. This binomial can be reduced as follows:

$$\operatorname{rem}(X_i - \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}}, \mathcal{G} \setminus \{ X_i - \boldsymbol{X}^{\boldsymbol{a_i}} \boldsymbol{X}^{\boldsymbol{b_i}} \})$$

$$
\begin{aligned}
&= X_i + \mathrm{rem}(-\boldsymbol{X^{a_i}X^{b_i}}, \mathcal{G} \setminus \{X_i - \boldsymbol{X^{a_i}X^{b_i}}\}) \\
&= X_i + \mathrm{rem}(-\boldsymbol{X^{a_i}X^{b_i}} + \boldsymbol{X^{a'_i}X^{b_i}}(X_j^2 - \boldsymbol{X^{2c_j}}), \mathcal{G} \setminus \{X_i - \boldsymbol{X^{a_i}X^{b_i}}\}) \\
&= X_i + \mathrm{rem}(-\boldsymbol{X^{a'_i}X^{b_i+2c_j}}, \mathcal{G} \setminus \{X_i - \boldsymbol{X^{a_i}X^{b_i}}\}).
\end{aligned}
$$

Further reductions lead to

$$
X_i - \boldsymbol{X^{(-a_i)}X^{b_i+\sum_{j=k_1+1}^{k_1+k_2}(-a_{ij})\,2c_j}},
$$

where the exponent $\sum_{j=k_1+1}^{k_1+k_2}(-a_{ij})\,2\boldsymbol{c_j}$ can be reduced modulo 4 by the binomials $X_i^4 - 1$, $k_1 + k_2 + 1 \le i \le n$. This proves the assertion. □

Example 4.2. The octacode $\mathcal{O}$ has the systematic generator matrx

$$
\begin{pmatrix}
1 & 0 & 0 & 0 & 3 & 1 & 2 & 1 \\
0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\
0 & 0 & 1 & 0 & 3 & 3 & 3 & 2 \\
0 & 0 & 0 & 1 & 2 & 3 & 1 & 1
\end{pmatrix}.
$$

Using the lexicographic order on $\mathbb{Q}[X_1, \ldots, X_8]$ with $X_1 \succ \ldots \succ X_n$, the ideal $I_{\mathcal{O}}$ has the reduced Groebner basis given by the elements

$$
\begin{array}{ll}
X_1 - X_5^1X_6^3X_7^2X_8^3, & X_5^4 - 1, \\
X_2 - X_5^3X_6^2X_7^1X_8^3, & X_6^4 - 1, \\
X_3 - X_5^1X_6^1X_7^1X_8^2, & X_7^4 - 1, \\
X_4 - X_5^2X_6^1X_7^3X_8^3, & X_8^4 - 1.
\end{array}
$$

Example 4.3. Consider the quaternary code $\mathcal{C}$ given by the systematic generator matrix

$$
\begin{pmatrix}
1 & 0 & 1 & 0 & 3 & 1 \\
0 & 1 & 1 & 1 & 2 & 0 \\
0 & 0 & 2 & 0 & 2 & 0 \\
0 & 0 & 0 & 2 & 2 & 2
\end{pmatrix}.
$$

Using the lexicographic order on $\mathbb{Q}[X_1, \ldots, X_6]$ with $X_1 \succ \ldots \succ X_6$, the ideal $I_{\mathcal{C}}$ has the minimal Groebner basis

$$
\{X_1 - X_3^3X_5^1X_6^3,\ X_2 - X_3^3X_4^3X_5^2,\ X_3^2 - X_5^2,\ X_4^2 - X_5^2X_6^2,\ X_5^4 - 1,\ X_6^4 - 1\}.
$$

The first two elements can be further reduced providing the reduced Groebner basis

$$
\{X_1 - X_3^1X_5^3X_6^3,\ X_2 - X_3^1X_4^1X_5^2X_6^2,\ X_3^2 - X_5^2,\ X_4^2 - X_5^2X_6^2,\ X_5^4 - 1,\ X_6^4 - 1\}.
$$

This construction of Groebner bases can be extended to $\mathbb{Z}_{p^m}$-codes, where p is prime and $m \ge 1$, by making use of the block structure of the generator matrix.

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* (German), PhD Thesis, Univ. of Innsbruck (1965).

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

[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. 10th 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] J.M. Goethals, Two dual families of nonlinear binary codes, *Electron. Lett.*, **10** (1974), 471-472

[15] M. Grassl, http://www.codetables.de (2010).

[16] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Sole, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory*, **40** (1994), 301-319.

[17] A.M. Kerdock, A class of low-rate nonlinear binary codes, *Inform. Control*, **20** (1972), 182-187.

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

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

[20] A.W. Nordstrom, J.P. Robinson, An optimal nonlinear code, *Inform. Control*, **11** (1967), 613-616.

[21] F.P. Preparata, A class of optimum nonlinear double-error correcting codes, *Inform. Control*, **13** (1968), 378-400.

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

[23] M. Saleemi, K.-H. Zimmermann, Linear codes as binomial ideals, *Int. J. Pure Appl. Math.*, **61** (2010), 147-156.

[24] M. Saleemi, K.-H. Zimmermann, Groebner bases for linear codes, *Int. J. Pure Appl. Math.*, **62** (2010), 481-491.

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

[26] Z.-X. Wan, *Quaternary Codes*, World Scientific, Singapore (1997).