International Journal of Pure and Applied Mathematics

Volume 73 No. 4 2011, 435-442

GROEBNER BASES FOR LINEAR CODES OVER GF(4)

Mehwish Saleemi[1], Karl-Heinz Zimmermann[2 §]

[1,2]Hamburg University of Technology
Hamburg, 21071, GERMANY

Abstract: A linear code over a prime field 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 of the corresponding code. In this paper, a similar result will be presented for linear codes over GF(4). To this end, the extented alphabet GF(4) is dealt with by enlarging the polynomial ring.

AMS Subject Classification: 13P10, 94B30
Key Words: Groebner basis, linear code, binomial ideal, polynomial ring, toric ideal, nonprime ideal

1. Introduction

Data signals sent over a noisy channel are protected against errors during transmission by adding redundancy. In algebraic coding theory, codes have an underlying algebraic structure and are studied with respect to key properties like number of codewords, number of detectable or correctable errors, and complexity of encoding and decoding. A well-investigated class of codes are the linear codes which are subspaces of an ambient vector space over a finite field [13, 14].

Groebner basis theory and algorithms have been originally devised by Buchberger in order to solve fundamental problems in commutative algebra [5, 6], Since then, Groebner bases have 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 [10, 11, 12, 15, 19].

Received: June 10, 2011

[§]Correspondence author

Recently, binary linear codes were linked to binomial ideals [4]. In [16, 17, 18] it has been shown that a linear code over a prime field GF(p) or local ring $\mathbb{Z}_{p^m}$ 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. However, the results do not directly carry over to linear codes over a finite extension field, since the representation of a code as an ideal heavily depends on the underlying alphabet.

This paper establishes an analogous result for linear codes over GF(4). However, in contrast to the case of linear codes over a prime field, the alphabet GF(4) needs special attention by enlarging polynomial ring.

For more details on the required background, we refer to the literature: Groebner bases [1, 2, 10, 11, 15, 19], toric ideals [3], and linear codes [13, 14].

2. Linear Codes over GF(4) and Groebner Bases

Let $\mathrm{GF}(4) = \{0, 1, \alpha, \alpha^2 = \alpha + 1\}$ be the Galois field with four elements. Let $\mathcal{C}$ be a linear code of length n and dimension k over GF(4) with systematic generator matrix $\boldsymbol{G} = (g_{ij}) = (\boldsymbol{I} \mid \boldsymbol{A})$, i.e., $\mathcal{C} = \{\boldsymbol{uG} \mid \boldsymbol{u} \in \mathrm{GF}(4)^k\}$, $\boldsymbol{I}$ is the $k \times k$ identity matrix, and $\boldsymbol{A}$ is a $k \times (n-k)$ matrix over GF(4). Note that there is an isomorphism $\phi : \mathrm{GF}(4) \to \mathbb{Z}_2 \times \mathbb{Z}_2$ of abelian groups, where $\phi(0) = (0, 0)$, $\phi(1) = (1, 0)$, $\phi(\alpha) = (0, 1)$, and $\phi(\alpha^2) = (1, 1)$.

In view of the polynomial ring $\mathbb{K}[\boldsymbol{Z}] = \mathbb{K}[\{Z_i^{(k,l)} \mid 1 \leq i \leq n, 0 \leq k, l \leq 1\}]$, associate with each vector $\boldsymbol{c} = (c_1, \ldots, c_n) \in \mathrm{GF}(4)^n$ the monomial

$$\boldsymbol{Z}^{\boldsymbol{c}} = Z_1^{\phi(c_1)} \cdots Z_n^{\phi(c_n)}. \tag{1}$$

Put $Z_i^{(0,0)} = 1$, $Z_i^{(1,0)} = X_i$, $Z_i^{(0,1)} = Y_i$, and $Z_i^{(1,1)} = X_i Y_i$, $1 \leq i \leq n$. In this way, each monomial $\boldsymbol{Z}^{\boldsymbol{c}}$ becomes an element of the polynomial ring $\mathbb{K}[\boldsymbol{X}, \boldsymbol{Y}] = \mathbb{K}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$, e.g.,

$$\boldsymbol{Z}^{(0,1,\alpha,\alpha^2,1,\alpha,0)} = X_2 Y_3 X_4 Y_4 X_5 Y_6.$$

The ideal in the polynomial ring $\mathbb{K}[\boldsymbol{X}, \boldsymbol{Y}]$ associated to the code $\mathcal{C}$ is defined as

$$I_{\mathcal{C}} \;=\; \langle \boldsymbol{Z}^{\boldsymbol{c}_+} - \boldsymbol{Z}^{\boldsymbol{c}_-} \mid \boldsymbol{c}_+ - \boldsymbol{c}_- \in \mathcal{C} \rangle + \langle X_i^2 - 1, Y_i^2 - 1 \mid 1 \leq i \leq n \rangle. \tag{2}$$

Note that each binomial of the form $\boldsymbol{Z}^{\boldsymbol{c}_+} - \boldsymbol{Z}^{\boldsymbol{c}_-}$ in $I_{\mathcal{C}}$ is equivalent to the binomial $\boldsymbol{Z}^{\boldsymbol{c}_+ - \boldsymbol{c}_-} - 1$ modulo $I_{\mathcal{C}}$. Indeed, if $X_iY - Z$ lies in $I_{\mathcal{C}}$, then $Y - X_iZ = X_i(X_iY - Z) - Y(X_i^2 - 1)$ is also in $I_{\mathcal{C}}$; similarly, if $Y_iX - Z$ belongs to $I_{\mathcal{C}}$, then $X - Y_iZ = Y_i(Y_iX - Z) - X(Y_i^2 - 1)$ lies in $I_{\mathcal{C}}$, $1 \leq i \leq n$.

In the following, let $\boldsymbol{a}_i$ denote the length-n vector containing the i-th row of the submatrix $\boldsymbol{A}$; that is,

$$\boldsymbol{a}_i = (0, \ldots, 0, g_{i,k+1}, \ldots, g_{i,n}), \quad 1 \leq i \leq k. \tag{3}$$

Subsequently, take the lexicographic order on the polynomial ring $\mathbb{K}[\boldsymbol{X}, \boldsymbol{Y}]$ such that

$$X_1 \succ \ldots \succ X_k \succ Y_1 \succ \ldots \succ Y_k \succ X_{k+1} \succ \ldots \succ X_n \succ Y_{k+1} \succ \ldots \succ Y_n. \tag{4}$$

Theorem 1. *In view of the monomial order (4), the ideal $I_{\mathcal{C}}$ has the reduced Groebner basis*

$$\begin{aligned} \mathcal{G} \;=\; & \{X_i - \boldsymbol{Z}^{\boldsymbol{a}_i},\, Y_i - \boldsymbol{Z}^{\alpha\cdot\boldsymbol{a}_i} \mid 1 \leq i \leq k\} \\ & \cup \{X_i^2 - 1,\, Y_i^2 - 1 \mid k+1 \leq i \leq n\}. \end{aligned} \tag{5}$$

Proof. Claim that the elements of $\mathcal{G}$ lie in the ideal $I_{\mathcal{C}}$. Indeed, the binomials $X_i - \boldsymbol{Z}^{\boldsymbol{a}_i}$ and $Y_i - \boldsymbol{Z}^{\alpha\cdot\boldsymbol{a}_i}$, $1 \leq i \leq k$, correspond to the rows of the matrices $\boldsymbol{G}$ and $\alpha\boldsymbol{G}$, respectively. This proves the claim.

Conversely, claim that the generators of $I_{\mathcal{C}}$ lie in the ideal generated by $\mathcal{G}$. To see this, first consider the binomial $X_i^2 - 1$, $1 \leq i \leq k$, which can be reduced modulo $\mathcal{G}$ as follows:

$$\begin{aligned} \mathrm{rem}(X_i^2 - 1, \mathcal{G}) &= \mathrm{rem}(X_i^2 - 1 - X_i(X_i - \boldsymbol{Z}^{\boldsymbol{a}_i}), \mathcal{G}) = \mathrm{rem}(X_i\boldsymbol{Z}^{\boldsymbol{a}_i} - 1, \mathcal{G}) \\ &= \mathrm{rem}(X_i\boldsymbol{Z}^{\boldsymbol{a}_i} - 1 - \boldsymbol{Z}^{\boldsymbol{a}_i}(X_i - \boldsymbol{Z}^{\boldsymbol{a}_i}), \mathcal{G}) \\ &= \mathrm{rem}((\boldsymbol{Z}^{\boldsymbol{a}_i})^2 - 1, \mathcal{G}). \end{aligned} \tag{6}$$

The occuring exponents are even and thus further reduction by the binomials $X_j^2 - 1$ and $Y_j^2 - 1$, $k+1 \leq j \leq n$, leads to zero.

Second, in a similar way, the binomials $Y_i^2 - 1$, $1 \leq i \leq k$, can be reduced modulo $\mathcal{G}$ to the binomial $(\boldsymbol{Z}^{\alpha\boldsymbol{a}_i})^2 - 1$ and then further to zero.

Third, consider the generators of the code $\mathcal{C}$ given by the rows of the matrix $\boldsymbol{G}$. For this, let $\boldsymbol{e}_i$ denote the i-th unit vector, i.e., $\boldsymbol{e}_i$ is the vector with a 1 in the i-th component and zeros elsewhere, $1 \leq i \leq n$. First, the binomial $\boldsymbol{Z}^{\boldsymbol{c}} - 1$ corresponding to the generator $\boldsymbol{c} = \boldsymbol{e}_i + \boldsymbol{a}_i$, $1 \leq i \leq k$, reduces modulo $\mathcal{G}$ as follows:

$$\mathrm{rem}(\boldsymbol{Z}^{\boldsymbol{e}_i + \boldsymbol{a}_i} - 1, \mathcal{G}) \;=\; \mathrm{rem}(X_i\boldsymbol{Z}^{\boldsymbol{a}_i} - 1 - \boldsymbol{Z}^{\boldsymbol{a}_i}(X_i - \boldsymbol{Z}^{\boldsymbol{a}_i}), \mathcal{G})$$

$$= \quad \mathrm{rem}((\boldsymbol{Z}^{\boldsymbol{a}_i})^2 - 1, \mathcal{G}). \tag{7}$$

Second, the binomial $\boldsymbol{Z}^{\boldsymbol{c}} - 1$ associated with the scalar multiple $\boldsymbol{c} = \alpha(\boldsymbol{e}_i + \boldsymbol{a}_i)$, $1 \leq i \leq k$, gets reduced mod $\mathcal{G}$ in the following way:

$$\begin{aligned} \mathrm{rem}(\boldsymbol{Z}^{\alpha(\boldsymbol{e}_i+\boldsymbol{a}_i)} - 1, \mathcal{G}) &= \mathrm{rem}(Y_i \boldsymbol{Z}^{\alpha\boldsymbol{a}_i} - 1 - \boldsymbol{Z}^{\alpha\boldsymbol{a}_i}(Y_i - \boldsymbol{Z}^{\alpha\boldsymbol{a}_i}), \mathcal{G}) \\ &= \mathrm{rem}((\boldsymbol{Z}^{\alpha\boldsymbol{a}_i})^2 - 1, \mathcal{G}). \end{aligned} \tag{8}$$

Third, the binomial $\boldsymbol{Z}^{\boldsymbol{c}} - 1$ related to the scalar multiple $\boldsymbol{c} = \alpha^2(\boldsymbol{e}_i + \boldsymbol{a}_i)$, $1 \leq i \leq k$, is reduced as follows:

$$\begin{aligned} &\mathrm{rem}(\boldsymbol{Z}^{\alpha^2(\boldsymbol{e}_i+\boldsymbol{a}_i)} - 1, \mathcal{G}) = \\ &= \mathrm{rem}(X_i Y_i \boldsymbol{Z}^{\alpha^2\boldsymbol{a}_i} - 1 - Y_i \boldsymbol{Z}^{\alpha^2\boldsymbol{a}_i}(X_i - \boldsymbol{Z}^{\boldsymbol{a}_i}), \mathcal{G}) \\ &= \mathrm{rem}(Y_i \boldsymbol{Z}^{\boldsymbol{a}_i} \boldsymbol{Z}^{\alpha^2\boldsymbol{a}_i} - 1, \mathcal{G}) \\ &= \mathrm{rem}(Y_i \boldsymbol{Z}^{\boldsymbol{a}_i} \boldsymbol{Z}^{\alpha^2\boldsymbol{a}_i} - 1 - \boldsymbol{Z}^{\boldsymbol{a}_i} \boldsymbol{Z}^{\alpha^2\boldsymbol{a}_i}(Y_i - \boldsymbol{Z}^{\alpha\boldsymbol{a}_i}), \mathcal{G}) \\ &= \mathrm{rem}(\boldsymbol{Z}^{\boldsymbol{a}_i} \boldsymbol{Z}^{\alpha\boldsymbol{a}_i} \boldsymbol{Z}^{\alpha^2\boldsymbol{a}_i} - 1, \mathcal{G}), \end{aligned} \tag{9}$$

where the last binomial is equal to

$$\prod_{\substack{j=k+1 \\ a_{i,j}\neq 0}}^{n} X_j^2 Y_j^2 - 1. \tag{10}$$

More generally, let $\boldsymbol{Z}^{\boldsymbol{c}_+} - \boldsymbol{Z}^{\boldsymbol{c}_-}$ be an element of $I_{\mathcal{C}}$ with $\boldsymbol{c}_+ - \boldsymbol{c}_- \in \mathcal{C}$. By the remarks prior to the theorem and the fact that the binomials $X_i^2 - 1$ and $Y_i^2 - 1$ reduce to zero modulo $\mathcal{G}$, it is sufficient to consider the equivalent binomial $\boldsymbol{Z}^{\boldsymbol{c}} - 1$, where $\boldsymbol{c} = \boldsymbol{c}_+ - \boldsymbol{c}_- \in \mathcal{C}$. Successive reduction of this binomial by using (7) to (9) leads to a binomial of the form $X_{k+1}^{d_{k+1}} Y_{k+1}^{e_{k+1}} \cdots X_n^{d_n} Y_n^{e_n} - 1$, whose exponents $d_{k+1}, e_{k+1}, \ldots, d_n, e_n$ are even. This binomial can in turn be reduced to zero by the binomials $X_i^2 - 1$ and $Y_i^2 - 1$, $k+1 \leq i \leq n$, proving the claim. Hence, the ideal generated by $\mathcal{G}$ equals the ideal $I_{\mathcal{C}}$ of the code $\mathcal{C}$.

Next, claim that $\mathcal{G}$ is a Groebner basis for $I_{\mathcal{C}}$. Indeed, Buchberger's S-criterion leads to the following cases: First, let $1 \leq i < j \leq k$. The S-polynomial

$$S(X_i - \boldsymbol{Z}^{\boldsymbol{a}_i}, X_j - \boldsymbol{Z}^{\boldsymbol{a}_j}) = X_i \boldsymbol{Z}^{\boldsymbol{a}_j} - X_j \boldsymbol{Z}^{\boldsymbol{a}_i}$$

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

$$\begin{aligned} &\mathrm{rem}(X_i \boldsymbol{Z}^{\boldsymbol{a}_j} - X_j \boldsymbol{Z}^{\boldsymbol{a}_i}, \mathcal{G}) = \\ &= \mathrm{rem}(X_i \boldsymbol{Z}^{\boldsymbol{a}_j} - X_j \boldsymbol{Z}^{\boldsymbol{a}_i} - \boldsymbol{Z}^{\boldsymbol{a}_j}(X_i - \boldsymbol{Z}^{\boldsymbol{a}_i}), \mathcal{G}) \end{aligned}$$

$$\begin{aligned}
&= \mathrm{rem}(-X_j\boldsymbol{Z}^{\boldsymbol{a}_i} + \boldsymbol{Z}^{\boldsymbol{a}_j}\boldsymbol{Z}^{\boldsymbol{a}_i}, \mathcal{G}) \\
&= \mathrm{rem}(-X_j\boldsymbol{Z}^{\boldsymbol{a}_i} + \boldsymbol{Z}^{\boldsymbol{a}_j}\boldsymbol{Z}^{\boldsymbol{a}_i} + \boldsymbol{Z}^{\boldsymbol{a}_i}(X_j - \boldsymbol{Z}^{\boldsymbol{a}_j}), \mathcal{G}) \\
&= \mathrm{rem}(\boldsymbol{Z}^{\boldsymbol{a}_j}\boldsymbol{Z}^{\boldsymbol{a}_i} - \boldsymbol{Z}^{\boldsymbol{a}_i}\boldsymbol{Z}^{\boldsymbol{a}_j}, \mathcal{G}) = 0.
\end{aligned}$$

Second, let $1 \leq i, j \leq k$. The S-polynomial

$$S(X_i - \boldsymbol{Z}^{\boldsymbol{a}_i}, Y_j - \boldsymbol{Z}^{\alpha\boldsymbol{a}_j}) = X_i\boldsymbol{Z}^{\alpha\boldsymbol{a}_j} - Y_j\boldsymbol{Z}^{\boldsymbol{a}_i}$$

reduces modulo $\mathcal{G}$ as follows:

$$\begin{aligned}
&\mathrm{rem}(X_i\boldsymbol{Z}^{\alpha\boldsymbol{a}_j} - Y_j\boldsymbol{Z}^{\boldsymbol{a}_i}, \mathcal{G}) = \\
&= \mathrm{rem}(X_i\boldsymbol{Z}^{\alpha\boldsymbol{a}_j} - Y_j\boldsymbol{Z}^{\boldsymbol{a}_i} - \boldsymbol{Z}^{\alpha\boldsymbol{a}_j}(X_i - \boldsymbol{Z}^{\boldsymbol{a}_i}), \mathcal{G}) \\
&= \mathrm{rem}(-Y_j\boldsymbol{Z}^{\boldsymbol{a}_i} + \boldsymbol{Z}^{\alpha\boldsymbol{a}_j}\boldsymbol{Z}^{\boldsymbol{a}_i}, \mathcal{G}) \\
&= \mathrm{rem}(-Y_j\boldsymbol{Z}^{\boldsymbol{a}_i} + \boldsymbol{Z}^{\alpha\boldsymbol{a}_j}\boldsymbol{Z}^{\boldsymbol{a}_i} + \boldsymbol{Z}^{\boldsymbol{a}_i}(Y_j - \boldsymbol{Z}^{\alpha\boldsymbol{a}_j}), \mathcal{G}) \\
&= \mathrm{rem}(\boldsymbol{Z}^{\alpha\boldsymbol{a}_j}\boldsymbol{Z}^{\boldsymbol{a}_i} - \boldsymbol{Z}^{\boldsymbol{a}_i}\boldsymbol{Z}^{\alpha\boldsymbol{a}_j}, \mathcal{G}) = 0.
\end{aligned}$$

Third, let $1 \leq i \leq k$ and $k+1 \leq j \leq n$. The S-polynomial

$$S(X_i - \boldsymbol{Z}^{\boldsymbol{a}_i}, X_j^2 - 1) = X_i - X_j^2\boldsymbol{Z}^{\boldsymbol{a}_i}$$

is reduced mod $\mathcal{G}$ in the following way:

$$\begin{aligned}
&\mathrm{rem}(X_i - X_j^2\boldsymbol{Z}^{\boldsymbol{a}_i}, \mathcal{G}) = \\
&= \mathrm{rem}(X_i - X_j^2\boldsymbol{Z}^{\boldsymbol{a}_i} - (X_i - \boldsymbol{Z}^{\boldsymbol{a}_i}), \mathcal{G}) \\
&= \mathrm{rem}(-X_j^2\boldsymbol{Z}^{\boldsymbol{a}_i} + \boldsymbol{Z}^{\boldsymbol{a}_i}, \mathcal{G}) \\
&= \mathrm{rem}(-X_j^2\boldsymbol{Z}^{\boldsymbol{a}_i} + \boldsymbol{Z}^{\boldsymbol{a}_i} + \boldsymbol{Z}^{\boldsymbol{a}_i}(X_j^2 - 1), \mathcal{G}) \\
&= \mathrm{rem}(\boldsymbol{Z}^{\boldsymbol{a}_i} - \boldsymbol{Z}^{\boldsymbol{a}_i}, \mathcal{G}) = 0.
\end{aligned}$$

Fourth, let $1 \leq i \leq k$ and $k+1 \leq j \leq n$. The S-polynomial

$$S(X_i - \boldsymbol{Z}^{\boldsymbol{a}_i}, Y_j^2 - 1) = X_i - Y_j^2\boldsymbol{Z}^{\boldsymbol{a}_i}$$

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

$$\begin{aligned}
&\mathrm{rem}(X_i - Y_j^2\boldsymbol{Z}^{\boldsymbol{a}_i}, \mathcal{G}) = \\
&= \mathrm{rem}(X_i - Y_j^2\boldsymbol{Z}^{\boldsymbol{a}_i} - (X_i - \boldsymbol{Z}^{\boldsymbol{a}_i}), \mathcal{G}) \\
&= \mathrm{rem}(-Y_j^2\boldsymbol{Z}^{\boldsymbol{a}_i} + \boldsymbol{Z}^{\boldsymbol{a}_i}, \mathcal{G}) \\
&= \mathrm{rem}(-Y_j^2\boldsymbol{Z}^{\boldsymbol{a}_i} + \boldsymbol{Z}^{\boldsymbol{a}_i} + \boldsymbol{Z}^{\boldsymbol{a}_i}(Y_j^2 - 1), \mathcal{G}) \\
&= \mathrm{rem}(\boldsymbol{Z}^{\boldsymbol{a}_i} - \boldsymbol{Z}^{\boldsymbol{a}_i}, \mathcal{G}) = 0.
\end{aligned}$$

Fifth, let $1 \leq i < j \leq k$. The S-polynomial

$$S(Y_i - \boldsymbol{Z}^{\alpha \boldsymbol{a}_i}, Y_j - \boldsymbol{Z}^{\alpha \boldsymbol{a}_j}) = Y_i \boldsymbol{Z}^{\alpha \boldsymbol{a}_j} - Y_j \boldsymbol{Z}^{\alpha \boldsymbol{a}_i}$$

gets reduced to zero mod $\mathcal{G}$ analogously to the first case.

Sixth, let $1 \leq i \leq k$ and $k+1 \leq j \leq n$. The S-polynomial

$$S(Y_i - \boldsymbol{Z}^{\alpha \boldsymbol{a}_i}, X_j^2 - 1) = Y_i - X_j^2 \boldsymbol{Z}^{\alpha \boldsymbol{a}_i}$$

gets divided into $\mathcal{G}$ as follows:

$$\begin{aligned} &\operatorname{rem}(Y_i - X_j^2 \boldsymbol{Z}^{\alpha \boldsymbol{a}_i}, \mathcal{G}) = \\ &= \operatorname{rem}(Y_i - X_j^2 \boldsymbol{Z}^{\alpha \boldsymbol{a}_i} - (Y_i - \boldsymbol{Z}^{\alpha \boldsymbol{a}_i}), \mathcal{G}) \\ &= \operatorname{rem}(-X_j^2 \boldsymbol{Z}^{\alpha \boldsymbol{a}_i} + \boldsymbol{Z}^{\alpha \boldsymbol{a}_i}, \mathcal{G}) \\ &= \operatorname{rem}(-X_j^2 \boldsymbol{Z}^{\alpha \boldsymbol{a}_i} + \boldsymbol{Z}^{\alpha \boldsymbol{a}_i} + \boldsymbol{Z}^{\alpha \boldsymbol{a}_i}(X_j^2 - 1), \mathcal{G}) \\ &= \operatorname{rem}(\boldsymbol{Z}^{\alpha \boldsymbol{a}_i} - \boldsymbol{Z}^{\alpha \boldsymbol{a}_i}, \mathcal{G}) = 0. \end{aligned}$$

Seventh, let $1 \leq i \leq k$ and $k+1 \leq j \leq n$. The S-polynomial

$$S(Y_i - \boldsymbol{Z}^{\alpha \boldsymbol{a}_i}, Y_j^2 - 1) = Y_i - Y_j^2 \boldsymbol{Z}^{\alpha \boldsymbol{a}_i}$$

is reduced to zero mod $\mathcal{G}$ similarly to the third case.

Eighth, let $k+1 \leq i < j \leq n$. Then

$$S(X_i^2 - 1, X_j^2 - 1) = X_i^2 - X_j^2 = (X_i^2 - 1) - (X_j^2 - 1).$$

Nineth, let $k+1 \leq i, j \leq n$. Then

$$S(X_i^2 - 1, Y_j^2 - 1) = X_i^2 - Y_j^2 = (X_i^2 - 1) - (Y_j^2 - 1).$$

Tenth, let $k+1 \leq i < j \leq n$. Then

$$S(Y_i^2 - 1, Y_j^2 - 1) = Y_i^2 - Y_j^2 = (Y_i^2 - 1) - (Y_j^2 - 1).$$

In the last three cases, the S-polynomials are linear combinations of elements lying in $\mathcal{G}$ and thus get divided by $\mathcal{G}$ to zero. This establishes the claim. Finally, it is clear that the basis $\mathcal{G}$ is reduced. Hence, the result follows. □

Example 1. The *hexacode* [8] is a linear code $\mathcal{H}$ of length 6 and dimension 3 over GF(4) given as

$$\mathcal{H} = \{(a, b, c, f(1), f(\alpha), f(\alpha^2)) \mid f(x) = ax^2 + bx + c, a, b, c \in \mathrm{GF}(4)\}. \quad (11)$$

This code has 64 codewords: 45 codewords of Hamming weight 4, 18 codewords of weight 6, and the zero word. By (11), a systematic generator matrix for the hexacode is the following:

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

By Theorem 1, the reduced Groebner basis for the associated ideal $I_{\mathcal{H}}$ with respect to the lexicgraphic order (4) has the following elements:

$$\begin{array}{ll} X_1 - X_4X_5Y_5Y_6, & X_4^2 - 1, \\ X_2 - X_4X_5X_6Y_6, & X_5^2 - 1, \\ X_3 - X_4X_5X_6, & X_6^2 - 1, \\ Y_1 - Y_4X_5X_6Y_6, & Y_4^2 - 1, \\ Y_2 - Y_4X_5Y_5X_6, & Y_5^2 - 1, \\ Y_3 - Y_4Y_5Y_6, & Y_6^2 - 1. \end{array}$$

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] J.H. Conway, N.J.A. Sloane, *Sphere Packings, Lattices and Groups,* Springer, New York (1998).

[9] 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.

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

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

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

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

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

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

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

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

[18] R. Leppert, M. Saleemi, K.-H. Zimmermann, Groebner bases for quaternary codes, *Int. J. Pure Appl. Math.*, to appear.

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