International Journal of Pure and Applied Mathematics
Volume 98 No. 4 2015, 419-441
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v98i4.2

GRAVER BASES AND NIVERSAL GRÖBNER BASES FOR LINEAR CODES

Natalia Dück[1], Karl-Heinz Zimmermann[2] §
[1,2]Hamburg University of Technology
21071 Hamburg, GERMANY

Abstract: A linear code over a finite field can be associated with two binomial ideals. In this paper, algorithms for computing their Graver bases and universal Gröbner bases are given.

AMS Subject Classification: 13P10, 94B05
Key Words: Gröbner basis, Graver basis, universal Gröbner basis, linear code

1. Introduction

Gröbner bases have originally been introduced by Buchberger for the algorithmic solution of some fundamental problems in commutative algebra [6]. They have turned out to be a crucial concept for further advance in the field of computer algebra [1, 2, 8, 11].

Linear codes with their additional algebraic properties, on the other hand, form an important subclass of error-correcting codes. Their relevance is well established in the field of coding theory [12, 20].

Recently, it has been emphasized that linear codes over finite fields can be described by binomial ideals given as a sum of a toric ideal and a non-prime ideal [4, 5, 15]. In this way, a direct link between the two prospering subjects of linear codes and Gröbner bases has been provided. In the binary case, this correspondence holds important information about the code like its minimum distance and its minimal support codewords, and allows a new decoding

Received: May 8, 2014

§Correspondence author

method [4, 13]. This has led to new insight into the algebraic structure of linear codes and using the rich theory of toric ideals [13, 9]. Central to all these applications is the computation of reduced Gröber bases.

In this paper, we will address the problem of computing the Graver basis and the universal Gröbner basis for both binomial ideals associated to a linear code. The essential ideas stem from [18] for the toric case and from [13] which only considers the modular case.

This paper is organized as follows. Section 2 introduces the required notions and definitions. Section 3 shows how both ideals associated to linear codes can be computed from certain toric ideals by substitution of variables. Section 4 provides a method for computing the Graver bases for code ideals. Section 5 describes a procedure for calculating the universal Gröbner basis from the Graver basis for a code ideal.

2. Preliminaries

This section will introduce the necessary concepts from commutative algebra and algebraic coding. We assume familiarity with the basic definitions and notions of monomial orders and Gröbner bases as introduced in [1, 7].

2.1. Universal Gröbner Bases and Graver Bases

Let $\mathbb{K}[\mathbf{x}] = \mathbb{K}[x_1, \ldots, x_n]$ be the commutative polynomial ring in n indeterminates over a field $\mathbb{K}$ and let *monomials* in $\mathbb{K}[\mathbf{x}]$ be denoted by $\mathbf{x}^u = x_1^{u_1} \cdots x_n^{u_n}$, where $u = (u_1, \ldots, u_n) \in \mathbb{N}_0^n$.

For a given ideal $I \subset \mathbb{K}[\mathbf{x}]$ and a monomial order $\succ$ on $\mathbb{N}_0^n$, the *leading ideal* of I w.r.t. $\succ$ is denoted by $\mathrm{lt}_\succ(I)$ and the reduced Gröbner basis for I w.r.t. $\succ$ is designated by $\mathcal{G}_\succ(I)$. For a given ideal I only finitely many different reduced Gröbner bases exist, and their union is called the *universal Gröbner basis* for I denoted by $\mathcal{U}(I)$ [17, 18, 21].

If two different monomial orders $\succ$ and $\succ'$ on $\mathbb{N}_0^n$ have the same leading ideal $\mathrm{lt}_\succ(I) = \mathrm{lt}_{\succ'}(I)$, then the reduced Gröbner bases are also the same $\mathcal{G}_\succ(I) = \mathcal{G}_{\succ'}(I)$ [10]. This result can be further generalized by introducing the notion of *weight vectors*. For any $\omega \in \mathbb{R}^n$ and any polynomial $f = \sum c_i \mathbf{x}^{u_i} \in \mathbb{K}[\mathbf{x}]$, define the *initial form* $\mathrm{lt}_\omega(f)$ of f to be the sum of all terms $c_i \mathbf{x}^{u_i}$ in f such that the inner product $\omega \cdot u_i$ is maximal, and for an ideal I define its *leading ideal associated to* ω as

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

Note that unlike to the leading ideal w.r.t. a monomial order this ideal is not necessarily generated by monomials. For a non-negative weight vector $\omega \in \mathbb{R}^n_+$ and a monomial order $\succ$ on $\mathbb{N}^n_0$, a new term order $\succ_\omega$ is defined by ordering monomials first by their ω-degree and breaking ties using $\succ$,

$$\mathbf{x}^a \succ_\omega \mathbf{x}^b \quad :\Longleftrightarrow \quad a \cdot \omega > b \cdot \omega \ \vee \ (a \cdot \omega = b \cdot \omega \ \wedge \ \mathbf{x}^a \succ \mathbf{x}^b). \tag{2}$$

For any non-negative weight vector $w \in \mathbb{R}^n_+$ and any monomial order $\succ$ on $\mathbb{N}^n_0$, $\mathrm{lt}_w(I) = \mathrm{lt}_\succ(I)$ if and only if $\mathrm{lt}_w(g) = \mathrm{lt}_\succ(g)$ for all $g \in \mathcal{G}_\succ(I)$ [10, Lemma 2.10]

A *binomial* in $\mathbb{K}[\mathbf{x}]$ is a polynomial consisting of two terms, i.e., a binomial is of the form $c_u\mathbf{x}^u - c_v\mathbf{x}^v$, where $u, v \in \mathbb{N}^n_0$ and $c_u, c_v \in \mathbb{K}$ are non-zero. A binomial is *pure* if the involved monomials are relatively prime. All binomials considered here will be pure and henceforth the prefix pure will be omitted. A *binomial ideal* is an ideal generated by binomials.

A binomial $\mathbf{x}^u - \mathbf{x}^v$ in a binomial ideal I is *primitive* if there is no other binomial $\mathbf{x}^{u'} - \mathbf{x}^{v'}$ in I such that $\mathbf{x}^{u'}$ divides $\mathbf{x}^u$ and $\mathbf{x}^{v'}$ divides $\mathbf{x}^v$. The set of all primitive binomials in I is called the *Graver basis* for I and is denoted by $\mathrm{Gr}(I)$. The universal Gröbner basis for a binomial ideal I is always a subset of the Graver basis, $\mathcal{U}(I) \subseteq \mathrm{Gr}(I)$ [18].

Toric ideals form a specific class of binomial ideals [3]. Affine toric ideals can be introduced by integer matrices [18]. For an integer $d \times n$ matrix A, the *toric ideal* associated to A is defined as

$$I_A = \langle \mathbf{x}^u - \mathbf{x}^v \mid Au = Av,\ u, v \in \mathbb{N}^n_0 \rangle\,. \tag{3}$$

Note that each vector $u \in \mathbb{Z}^n$ can be uniquely written as $u = u^+ - u^-$ where u^+, u^- have disjoint support and their entries are non-negative. For instance, the vector $u = (1, -2, 0)$ splits into $u^+ = (1, 0, 0)$ and $u^- = (0, 2, 0)$. In this way, the toric ideal I_A can be expressed as

$$I_A = \left\langle \mathbf{x}^{u^+} - \mathbf{x}^{u^-} \mid u \in \ker_{\mathbb{Z}}(A) \right\rangle. \tag{4}$$

2.2. Linear Codes and Binomials Ideals

Let $\mathbb{F}_q$ denote the finite field with q elements where q is a prime power. In what follows, whenever we write $q = p^r$, p shall be a prime and r a non-negative integer. A *linear code* $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_q$ is the image of a one-to-one linear mapping from $\mathbb{F}_q^k$ to $\mathbb{F}_q^n$. Such a code $\mathcal{C}$ is called an $[n, k]$ code whose elements are called *codewords*, which are always written as row vectors [12, 20].

A *generator matrix* for an $[n,k]$ code $\mathcal{C}$ is a $k \times n$ matrix G over $\mathbb{F}_q$ whose rows form a basis for $\mathcal{C}$, and a *parity check matrix* H is an $(n-k) \times n$ matrix over $\mathbb{F}_q$ such that a word $c \in \mathbb{F}_q^n$ belongs to $\mathcal{C}$ if and only if $cH^T = \mathbf{0}$.

The *support* of a word $u \in \mathbb{F}_q^n$, denoted by $\mathrm{supp}(u)$, is the set of coordinates $i \in \{1, \ldots, n\}$ such that $u_i \neq 0$.

Let $\mathcal{C}$ be an $[n,k]$ code over the finite field $\mathbb{F}_q$, where $q = p^r$ is a prime power. Two binomial ideals can be associated to this code.

First, the *ordinary code ideal* associated to $\mathcal{C}$ is an ideal in the polynomial ring $\mathbb{K}[\mathbf{x}] = \mathbb{K}[x_{11}, \ldots, x_{1r}, x_{21} \ldots, x_{nr}]$ given as a sum of binomial ideals [5, 15],

$$I(\mathcal{C}) = I'(\mathcal{C}) + I_p, \tag{5}$$

where

$$I'(\mathcal{C}) = \langle \mathbf{x}^c - \mathbf{x}^{c'} \mid c - c' \in \mathcal{C} \rangle \tag{6}$$

and

$$I_p = \left\langle x_{ij}^p - 1 \mid 1 \leq i \leq n,\ 1 \leq j \leq r \right\rangle. \tag{7}$$

Note that the components of the word $c \in \mathbb{F}_q^n$ in the exponent of the monomial $\mathbf{x}^c$ are replaced by their canonical integer representations using the vector space isomorphism between $\mathbb{F}_q$ and $\mathbb{F}_p^r$.

The binomial $\mathbf{x}^u - \mathbf{x}^{u'}$ in the code ideal is said to *correspond* to the codeword $u - u'$. In contrast to the integral case, however, different binomials may correspond to the same codeword. For example, the word $(1,1,0)$ in $\mathbb{F}_2^3$ can be written as $(1,1,0) = (0,1,0) - (1,0,0)$ or $(1,1,0) = (1,0,0) - (0,1,0)$.

In order to define the second binomial ideal associated to $\mathcal{C}$, let α be a primitive element of $\mathbb{F}_q$ and define the *crossing map*

$$\blacktriangle : \mathbb{F}_q^n \to \mathbb{Z}^{n(q-1)}$$

by

$$\mathbf{a} = (a_1, \ldots, a_n) = (\alpha^{j_1}, \ldots, \alpha^{j_n}) \mapsto (\mathbf{e}_{j_1}, \ldots, \mathbf{e}_{j_n}),$$

where $\mathbf{e}_i$ is the ith unit vector of length $q-1$, $1 \leq i \leq q-1$, and each zero coordinate is mapped to the zero vector of length $q-1$. For instance, consider the field $\mathbb{F}_4 = \{0, \alpha, \alpha^2 = \alpha + 1, \alpha^3 = 1\}$ and $n = 2$. The crossing map $\blacktriangle : \mathbb{F}_q^2 \to \mathbb{Z}^6$ assigns $(\alpha, 1)$ to 100001, $(0,0)$ to 000000, and $(\alpha^2, 0)$ to 010000.

The associated mapping

$$\blacktriangledown : \mathbb{Z}^{n(q-1)} \to \mathbb{F}_q^n$$

is given as

$$(j_{1,1},\ldots,j_{1,q-1},j_{2,1},\ldots,j_{n,q-1}) \mapsto \left(\sum_{i=1}^{q-1} j_{1,i}\alpha^i,\ldots,\sum_{i=1}^{q-1} j_{n,i}\alpha^i\right).$$

This map is the right inverse of $\blacktriangle$, since $\blacktriangledown \circ \blacktriangle$ is the identity on $\mathbb{Z}^{n(q-1)}$.

Second, the *generalized code ideal* associated to the code $\mathcal{C}$ is an ideal in the larger polynomial ring $\mathbb{K}[\mathbf{x}] = \mathbb{K}[\mathbf{x}_1,\ldots,\mathbf{x}_n]$, where $\mathbf{x}_j = (x_{j1},\ldots,x_{j,q-1})$ for $1 \le j \le n$, given as [14]

$$I_+(\mathcal{C}) = \left\langle \mathbf{x}^{\blacktriangle a} - \mathbf{x}^{\blacktriangle b} \mid a - b \in \mathcal{C} \right\rangle. \tag{8}$$

A generating set for the code ideal $I_+(\mathcal{C})$ will contain both a generating set of the associated linear code as well as their scalar multiples and an encoding of the additive structure of the field $\mathbb{F}_q$ [14, 16]. The latter can be given by the ideal I_q in $\mathbb{K}[\mathbf{x}]$ generated by the set

$$\bigcup_{i=1}^{n} \left(\{x_{iu}x_{iv} - x_{iw} \mid \alpha^u + \alpha^v = \alpha^w\} \cup \{x_{iu}x_{iv} - 1 \mid \alpha^u + \alpha^v = 0\}\right). \tag{9}$$

In the following, we write $\mathcal{U}(\mathcal{C}) = \mathcal{U}(I(\mathcal{C}))$ and $\mathcal{U}_+(\mathcal{C}) = \mathcal{U}(I_+(\mathcal{C}))$ for the universal Gröbner basis for $I(\mathcal{C})$ and $I_+(\mathcal{C})$, respectively, and $\mathrm{Gr}(\mathcal{C}) = \mathrm{Gr}(I(\mathcal{C}))$ and $\mathrm{Gr}_+(\mathcal{C}) = \mathrm{Gr}(I_+(\mathcal{C}))$ for the Graver basis for $I(\mathcal{C})$ and $I_+(\mathcal{C})$, respectively.

For a binary linear code both, the generalized code ideal and the code ideal are equal. In general, the code ideal is an elimination ideal of the generalized code ideal. To see this, let $\mathcal{C}$ be an $[n,k]$ code over $\mathbb{F}_q$. For any natural number $s \le q-1$ and for indices $1 \le i_1 < i_2 < \cdots < i_s \le q-1$ denote by $\underline{\mathbf{x}}_{i_1,i_2,\ldots,i_s}$ the variables

$$x_{1i_1},\ldots,x_{1i_s},x_{2i_1},\ldots,x_{ni_1},\ldots,x_{nis}.$$

The generalized code ideal belongs to the ring $\mathbb{K}[\mathbf{x}] = \mathbb{K}[x_{11},\ldots,x_{n,p-1}]$ whereas the ordinary code ideal can be considered to belong to the ring $\mathbb{K}[\underline{\mathbf{x}}_{i_1,\ldots,i_r}] \subset \mathbb{K}[\mathbf{x}]$ for certain indices $i_1,\ldots,i_r$,

$$I(\mathcal{C}) = \left\langle \underline{\mathbf{x}}^a_{i_1,\ldots,i_r} - \underline{\mathbf{x}}^b_{i_1,\ldots,i_r} \,|a - b \in \mathcal{C} \right\rangle. \tag{10}$$

Proposition 1. *Let $\mathcal{C}$ be an $[n,k]$ code over $\mathbb{F}_q$. The code ideal $I(\mathcal{C})$ as defined in Eq. (10) is an elimination ideal of the ideal $I_+(\mathcal{C})$. More precisely, for any choice of r indices $1 \le i_1 < \cdots < i_r \le q-1$ such that $\alpha^{i_1},\ldots,\alpha^{i_r}$ are linearly independent in $\mathbb{F}_p^r$ holds*

$$I(\mathcal{C}) = I_+(\mathcal{C}) \cap \mathbb{K}[\underline{\mathbf{x}}_{i_1,i_2\ldots,i_r}].$$

Proof. Let $\underline{\mathbf{x}}^a_{i_1,\ldots,i_r} - \underline{\mathbf{x}}^b_{i_1,\ldots,i_r} \in I(\mathcal{C})$, i.e., $a - b \in \mathcal{C}$. For $1 \le i \le n$, let $(a_{i1}, \ldots, a_{ir})$ be the vector in $\mathbb{F}_p^r$ corresponding to the ith component of a and analogously for b. Then $\underline{\mathbf{x}}^a_{i_1,\ldots,i_r} - \underline{\mathbf{x}}^b_{i_1,\ldots,i_r} = \mathbf{x}^{a'} - \mathbf{x}^{b'}$, where $a' = (a_{11}\mathbf{e}_{i_1} + \cdots + a_{1r}\mathbf{e}_{i_r}, \ldots, a_{n1}\mathbf{e}_{i_1} + \cdots + a_{nr}\mathbf{e}_{i_1})$ and analogously for b'. Furthermore, $\blacktriangledown(a' - b') = a - b \in \mathcal{C}$ and so, $\underline{\mathbf{x}}^a_{i_1,\ldots,i_r} - \underline{\mathbf{x}}^b_{i_1,\ldots,i_r} \in I_+(\mathcal{C}) \cap \mathbb{K}[\underline{\mathbf{x}}_{i_1,\ldots,i_r}]$.

Conversely, let $\mathbf{x}^a - \mathbf{x}^b$ be a binomial in $I_+(\mathcal{C}) \cap \mathbb{K}[\underline{\mathbf{x}}_{i_1,\ldots,i_r}]$. Clearly, $a - b$ must be of the form $((a_{11} - b_{11})\mathbf{e}_{i_1} + \cdots + (a_{1r} - b_{1r})\mathbf{e}_{i_r}, \ldots, (a_{n1} - b_{n1})\mathbf{e}_{i_1} + \cdots + (a_{nr} - b_{nr})\mathbf{e}_{i_1}))$ with $\blacktriangledown(a - b) = a - b \in \mathcal{C}$. And the result follows. □

3. Code Ideals From Toric Ideals

In this section, the generalized code ideal $I_+(\mathcal{C})$ will be related to a toric ideal. Such a connection has already been established for the ordinary code ideal $I(\mathcal{C})$ in the case of a prime field [13, Remark 1 and Proposition 3.1]. To see this, define for any prime number p and any $m \times n$ matrix A over $\mathbb{F}_p$ the extended $m \times (n + m)$ integer matrix

$$A(p) = \left(\begin{array}{c|c} \triangle A & pI_m \end{array} \right) \tag{11}$$

where $\triangle A$ is an $m \times n$ integer matrix such that $A = \triangle A \otimes_{\mathbb{Z}} \mathbb{F}_p$.

Proposition 2. *[13, Remark 1 and Proposition 3.1] The ordinary code ideal $I(\mathcal{C})$ associated to an $[n, k]$ code $\mathcal{C}$ over $\mathbb{F}_p$ with parity check matrix H is given by*

$$I(\mathcal{C}) = \left\{ f(\mathbf{x}, \mathbf{1}) \mid f \in I_{H(p)} \right\} \subset \mathbb{K}[\mathbf{x}], \tag{12}$$

where $\mathbf{1}$ is the all-1 vector of length $n-k$ and $I_{H(p)}$ is the toric ideal in $\mathbb{K}[\mathbf{x}, \mathbf{y}] = \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_{n-k}]$ associated to the integer matrix $H(p)$.

This result can be extended to linear codes over any finite field. For this, take the finite field $\mathbb{F}_q$ with $q = p^r$ and an $\mathbb{F}_p$-basis $B = \{b_1, \ldots, b_r\}$ of $\mathbb{F}_q$. For any matrix $H \in \mathbb{F}_q^{m \times n}$ with row vectors $h_1, \ldots, h_m$ define the extended matrix

$$H' = \begin{pmatrix} b_1 h_1 \\ \vdots \\ b_r h_1 \\ \vdots \\ b_1 h_m \\ \vdots \\ b_r h_m \end{pmatrix} \in \mathbb{F}_q^{rm \times n}$$

given by multiplying the row vectors of H with the elements from the basis B. Replace each entry by its row representation in $\mathbb{F}_p^r$ according to the basis B and denote the resulting matrix by $H_e \in \mathbb{F}_p^{mr\times nr}$. Finally, the matrix H_e is associated to the $mr \times nr + mr$ integer matrix

$$H(q) = \left(\begin{array}{c|c} \triangle H_e & pI_{mr} \end{array} \right), \tag{13}$$

where $\triangle H_e$ is an $mr \times nr$ integer matrix such that $\triangle H_e \otimes_{\mathbb{Z}} \mathbb{F}_p = H_e$.

Example 3.3. Consider the following 2×4 matrix over the finite field $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = \alpha + 1\}$,

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

In view of the basis $B = \{1, \alpha\}$, we obtain

$$H' = \begin{pmatrix} \alpha & 0 & 1 & 0 \\ \alpha^2 & 0 & \alpha & 0 \\ \alpha^2 & \alpha & 0 & 1 \\ 1 & \alpha^2 & 0 & \alpha \end{pmatrix}$$

and

$$H_e = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

giving the integer matrix $H(4) = (\triangle H_e \,|\, 2I_4)$. ♢

Proposition 4. *The ordinary code ideal $I(\mathcal{C})$ associated to an $[n, k]$ code $\mathcal{C}$ over $\mathbb{F}_q$ with parity check matrix $H \in \mathbb{F}_q^{n-k\times n}$ is given by*

$$I(\mathcal{C}) = \left\{ f(\mathbf{x}, \mathbf{1}) \,\middle|\, f \in I_{H(q)} \right\}, \tag{14}$$

where $\mathbf{1}$ is the all-one vector of length $(n-k)r$ and $I_{H(q)}$ is the toric ideal in the ring $\mathbb{K}[\mathbf{x}, \mathbf{y}] = \mathbb{K}[x_{11}, \ldots, x_{nr}, y_1, \ldots, y_{(n-k)r}]$ associated to the integer matrix $H(q)$.

Proof. The code ideal $I(\mathcal{C})$ is generated by binomials and so it is sufficient to consider only binomials. The ideal $I_{H(q)}$ is toric and for all $a, b \in \mathbb{Z}^{nr}$ and $a', b' \in \mathbb{Z}^{(n-k)r}$, the following holds

$$\mathbf{x}^a\mathbf{y}^{a'} - \mathbf{x}^b\mathbf{y}^{b'} \in I_{H(q)} \quad \Longleftrightarrow \quad \triangle H_e(a-b)^{\mathbf{T}} \equiv \mathbf{0} \bmod p.$$

By passing from $\triangle H_e$ to $\triangle H_e \otimes_{\mathbb{Z}} \mathbb{F}_p = H_e$ and from $a-b \in \mathbb{Z}^{nr}$ to $a-b \mod p \in \mathbb{F}_p^{nr}$, $a-b$ belongs to $\ker(H_e)$ if and only if $\mathbf{x}^a\mathbf{y}^{a'} - \mathbf{x}^b\mathbf{y}^{b'} \in I_{H(q)}$. But the kernels $\ker(H_e)$ and $\ker(H)$ are isomorphic under the $\mathbb{F}_p$-isomorphism between $\mathbb{F}_p^r$ and $\mathbb{F}_q$ and hence the result follows. □

A similar result holds for the generalized code ideals. To see this, let α denote a fixed primitive element of the finite field $\mathbb{F}_q$ and let $B = \{b_1, \ldots, b_r\}$ be an $\mathbb{F}_p$-basis for $\mathbb{F}_q$. For any matrix $H \in \mathbb{F}_q^{m\times n}$ with columns $h_1, \ldots, h_n$ define the extended matrix

$$H' = \left(\begin{array}{c|c|c|c|c|c} \alpha h_1 & \alpha^2 h_1 & \ldots & \alpha^{q-1} h_1 & \alpha h_2 & \ldots & \alpha^{q-1} h_n \end{array} \right) \in \mathbb{F}_q^{m\times n(q-1)}.$$

Replace each entry by its column representation in $\mathbb{F}_p^r$ acoording to the basis B and denote the resulting matrix by $H_{+,e} \in \mathbb{F}_p^{mr\times n(q-1)}$. Finally, the matrix $H_{+,e}$ is associated with the integer $mr \times n(q-1) + mr$ matrix

$$H_+(q) = \left(\begin{array}{c|c} \triangle H_{+,e} & pI_{rm} \end{array} \right), \tag{15}$$

where $\triangle H_{+,e}$ is an $mr \times n(q-1)$ integer matrix such that $\triangle H_{+,e} \otimes_{\mathbb{Z}} \mathbb{F}_p = H_{+,e}$.

Example 3.5. Consider the following 2×3 matrix over the finite field $\mathbb{F}_9$ with primitive element α satisfying $\alpha^2 + \alpha + 2 = 0$,

$$H = \begin{pmatrix} \alpha^2 & \alpha & 0 \\ 0 & 0 & \alpha^6 \end{pmatrix}.$$

In view of the basis $B = \{1, \alpha\}$, the extended matrix is

$$H' = \left(\begin{array}{c|c|c} H_1' & H_2' & H_3' \end{array} \right)$$

where

$$H_1' = \begin{pmatrix} \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha & \alpha^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$
$$H_2' = \begin{pmatrix} \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$
$$H_3' = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \alpha^7 & \alpha^8 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{pmatrix},$$

and

$$H_{+,e} = \left(\begin{array}{c|c|c} H_{1,+,e} & H_{2,+,e} & H_{3,+,e} \end{array} \right),$$

where

$$H_{1,+,e} = \begin{pmatrix} 2 & 2 & 0 & 2 & 1 & 1 & 0 & 1 \\ 2 & 0 & 2 & 1 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$H_{2,+,e} = \begin{pmatrix} 1 & 2 & 2 & 0 & 2 & 1 & 1 & 0 \\ 2 & 2 & 0 & 2 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$H_{3,+,e} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 2 & 2 & 0 & 2 \\ 1 & 0 & 1 & 2 & 2 & 0 & 2 & 1 \end{pmatrix},$$

giving the integer matrix $H_+(9) = (\triangle H_e \,|\, 3I_4)$. ♢

Proposition 6. *The generalized code ideal $I_+(\mathcal{C})$ associated to an $[n,k]$ code $\mathcal{C}$ over $\mathbb{F}_q$ with parity check matrix H is given by*

$$I_+(\mathcal{C}) = \left\{ f(\mathbf{x},\mathbf{1}) \mid f \in I_{H_+(q)} \right\}, \tag{16}$$

where $\mathbf{1}$ is the all-one vector of length $(n-k)r$ and $I_{H_+(q)}$ is the toric ideal in the ring $\mathbb{K}[\mathbf{x},\mathbf{y}] = \mathbb{K}[x_{11},\ldots,x_{n,q-1},y_1,\ldots,y_{(n-k)r}]$ associated to the integer matrix $H_+(q)$.

Proof. The code ideal $I_+(\mathcal{C})$ is generated by binomials and so it is sufficient to consider only binomials. Let $a,a',b,b' \in \mathbb{Z}^{n(q-1)}$. Writing

$$a-b = (c_{11},\ldots,c_{1,q-1},c_{21},\ldots,c_{2,q-1},\ldots,c_{n,q-1}) = (\mathbf{c}_1,\ldots,\mathbf{c}_n)$$

gives

$$\mathbf{x}^a\mathbf{y}^{a'} - \mathbf{x}^b\mathbf{y}^{b'} \in I_{H_+(q)} \quad \Longleftrightarrow \quad \triangle H_{+,e}(\mathbf{c}_1,\ldots,\mathbf{c}_n)^{\mathbf{T}} \equiv \mathbf{0} \bmod p.$$

Identifying the entries c_{ij}'s with their images under the canonical mapping $\mathbb{Z} \to \mathbb{F}_p$ shows that $\triangle H_{+,e}(\mathbf{c}_1,\ldots,\mathbf{c}_n)^{\mathbf{T}} \equiv \mathbf{0} \bmod p$ holds if and only if for all $0 \le s \le r-1$ and $1 \le i \le n-k$,

$$\sum_{j=1}^{n} \left(\pi_s\left(\alpha h_{ij}\right) c_{j1} + \ldots + \pi_s\left(\alpha^{q-1} h_{ij}\right) c_{j,q-1} \right) = 0 \quad \text{over } \mathbb{F}_p,$$

where $\pi_j : \mathbb{F}_q \to \mathbb{F}_p : \sum_{i=1}^{r} a_i b_i \mapsto a_j$ denotes the projection onto the jth component according to the basis B. On the other hand, $H\blacktriangledown(\mathbf{c}_1, \ldots, \mathbf{c}_n)^{\mathbf{T}} = \mathbf{0}$ if and only if for all $1 \leq i \leq n-k$,

$$0 = \sum_{j=1}^{n} h_{ij} \left(\sum_{\ell=1}^{q-1} c_{j\ell} \alpha^{\ell} \right) = \sum_{j=1}^{n} \left((h_{ij}\alpha)\, c_{j1} + \cdots + \left(h_{ij}\alpha^{q-1}\right) c_{j,q-1} \right) \qquad \text{over } \mathbb{F}_q.$$

Applying the projections π_s, $1 \leq s \leq r$ provides the equivalence between both formulae. □

Example 3.7. Take the $[3, 2]$ code $\mathcal{C}$ over $\mathbb{F}_4$ with parity check matrix

$$H = \begin{pmatrix} \alpha & \alpha^3 & \alpha^2 \end{pmatrix},$$

where α is a primitive element of $\mathbb{F}_4$ satisfying $\alpha^2 + \alpha + 1 = 0$. In view of the F_2-basis $B = \{1, \alpha\}$, we obtain the matrix

$$H_+(4) = \left(\begin{array}{cccccccc|cc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 2 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 2 \end{array} \right).$$

The reduced Gröbner basis for the toric ideal $I_{H_+(4)}$ w.r.t. the lexicographic ordering consists of the binomials

$$\begin{array}{lll} x_{11} - x_{33}, & x_{12} - x_{31}, & x_{13} - x_{32}, \\ x_{21} - x_{32}, & x_{22} - x_{33}, & x_{23} - x_{31}, \\ x_{31}^2 - y_2, & x_{31}x_{32} - x_{33}, & x_{31}x_{33} - x_{32}y_2, \\ x_{31}y_1 - x_{32}x_{33}, & x_{32}^2 - y_1, & x_{33}^2 - y_1y_2. \end{array}$$

The substitution $\mathbf{y} \mapsto \mathbf{1}$ and a further Gröber basis computation lead to the reduced Gröbner basis for the generalized code ideal $I_+(\mathcal{C})$,

$$\left\{ \begin{array}{lllll} x_{11} - x_{33}, & x_{12} - x_{32}x_{33}, & x_{13} - x_{32}, & x_{21} - x_{32}, & x_{22} - x_{33}, \\ x_{23} - x_{32}x_{33}, & x_{31} - x_{32}x_{33}, & x_{32}^2 - 1, & x_{33}^2 - 1 & \end{array} \right\}.$$

♢

4. Computing the Graver Basis

The Graver basis for the ordinary code ideal associated to a linear code over a finite prime field can be computed as an elimination ideal of the $\mathbb{Z}$-kernel of the matrix [13, Remark 3]

$$\begin{pmatrix} \triangle H & \mathbf{0} & pI_m \\ I_n & I_n & \mathbf{0} \end{pmatrix} \in \mathbb{Z}^{(m+n)\times(2n+m)}, \tag{17}$$

where $\triangle H$ gives rise to the parity check matrix $H = \triangle H \otimes_{\mathbb{Z}} \mathbb{F}_p$ of the code. In this section, a uniform method for computing the Graver basis for the ordinary and the generalized code ideal will be developed.

4.1. Generalization of Lawrence Liftings

For each $m\times n$ integer matrix $\triangle H$, let $H = \triangle H \otimes_{\mathbb{Z}} \mathbb{F}_p$ and define the *p-Lawrence lifting* of $\triangle H$ as the $(m+n)\times(2n+m)$ integer matrix

$$\Lambda(H)_p = \begin{pmatrix} \triangle H & \mathbf{0} & pI_m \\ I_n & I_n & \mathbf{0} \end{pmatrix}. \tag{18}$$

Consider the toric ideal $I_{\Lambda(H)_p}$ in the ring $\mathbb{K}[\mathbf{x},\mathbf{y},\mathbf{z}]$ where $\mathbf{x} = (x_1,\ldots,x_n)$, $\mathbf{y} = (y_1,\ldots,y_n)$ and $\mathbf{z} = (z_1,\ldots,z_m)$, and define the ideal $I_{\Lambda(H)}$ in $\mathbb{K}[\mathbf{x},\mathbf{y}]$ as

$$I_{\Lambda(H)} = \left\{ g(\mathbf{x},\mathbf{y},\mathbf{1}) \,\middle|\, g \in I_{\Lambda(H)_p} \right\}. \tag{19}$$

Proposition 8. *The ideal $I_{\Lambda(H)}$ is binomial and all pure binomials in $I_{\Lambda(H)}$ are of the form $\mathbf{x}^u\mathbf{y}^v - \mathbf{x}^v\mathbf{y}^u$, where $u - v \in \ker(H)$.*

Proof. Let $\{g_1,\ldots,g_k\}$ be a generating set for $I_{\Lambda(H)_p}$. Then by definition, $\{g'_1,\ldots,g'_k\}$, where $g'_i(\mathbf{x},\mathbf{y}) = g_i(\mathbf{x},\mathbf{y},\mathbf{1})$ for $1 \le i \le k$, is a generating set for $I_{\Lambda(H)}$. Since $I_{\Lambda(H)_p}$ is generated by binomials, so is $I_{\Lambda(H)}$.

In view of the second assertion, take a binomial $\mathbf{x}^{u^+}\mathbf{y}^{v^+} - \mathbf{x}^{u^-}\mathbf{y}^{v^-}$ in $\mathbb{K}[\mathbf{x},\mathbf{y}]$. Then

$$\begin{aligned} \mathbf{x}^{u^+}\mathbf{y}^{v^+} - \mathbf{x}^{u^-}\mathbf{y}^{v^-} \in I_{\Lambda(H)} &\Leftrightarrow \exists c \in \mathbb{Z}^m : (u^+ - u^-, v^+ - v^-, c) \in \ker\left(\Lambda(H)_p\right) \\ &\Leftrightarrow u^+ - u^- \in \ker(H) \wedge u^+ - u^- = v^- - v^+ \\ &\Leftrightarrow u^+ - u^- \in \ker(H) \wedge u^+ = v^- \wedge u^- = v^+. \end{aligned}$$

This gives the result. □

Proposition 9. *For each binomial ideal I in $\mathbb{K}[\mathbf{x},\mathbf{y}]$ in which every binomial is of the form $\mathbf{x}^a\mathbf{y}^b - \mathbf{x}^b\mathbf{y}^a$, the Graver basis, the universal Gröbner basis and every reduced Gröbner basis coincide.*

Proof. The Graver basis is a Gröbner basis w.r.t. any monomial order since it contains the universal Gröbner basis. Claim that it is also the reduced Gröbner basis w.r.t. an arbitrary monomial order. Indeed, suppose there are binomials $\mathbf{x}^a\mathbf{y}^b - \mathbf{x}^b\mathbf{y}^a$ and $\mathbf{x}^c\mathbf{y}^d - \mathbf{x}^d\mathbf{y}^c$ in $\mathrm{Gr}(I)$, where $\mathbf{x}^a\mathbf{y}^b$ and $\mathbf{x}^c\mathbf{y}^d$ are the respective leading terms. If $\mathbf{x}^a\mathbf{y}^b$ divides $\mathbf{x}^c\mathbf{y}^d$, then $\mathbf{x}^b\mathbf{y}^a$ divides $\mathbf{x}^d\mathbf{y}^c$ contradicting the primitiveness of $\mathbf{x}^a\mathbf{y}^b - \mathbf{x}^b\mathbf{y}^a$. By the same argument, the non-leading term in a primitive binomial is not divisible by the leading term of another primitive binomial. This proves the claim. By the inclusions the result follows. □

4.2. Application to Code Ideals

In this section, we provide algorithms to establish the Graver bases for both code ideals.

First, we consider ordinary code ideals.

Proposition 10. *Let $\mathcal{C}$ be an $[n,k]$ code over $\mathbb{F}_q$ with parity check matrix H, and let $\mathcal{G}$ be the reduced Gröbner basis for the ideal $I_{\Lambda(H_e)}$ w.r.t. any monomial order. Then the Graver basis for the ordinary code ideal $I(\mathcal{C})$ is given by*

$$Gr\,(\mathcal{C}) = \{\mathbf{x}^u - \mathbf{x}^v \,|\mathbf{x}^u\mathbf{y}^v - \mathbf{x}^v\mathbf{y}^u \in \mathcal{G}\}\,. \tag{20}$$

Proof. By Prop. 4 and 8, the binomial $\mathbf{x}^u - \mathbf{x}^v$ belongs to $I(\mathcal{C})$ if and only if the binomial $\mathbf{x}^u\mathbf{y}^v - \mathbf{x}^v\mathbf{y}^u$ belongs to $I_{\Lambda(H_e)}$. It follows that the binomial $\mathbf{x}^u - \mathbf{x}^v$ is primitive for $I(\mathcal{C})$ if and only if the binomial $\mathbf{x}^u\mathbf{y}^v - \mathbf{x}^v\mathbf{y}^u$ is primitive for $I_{\Lambda(H_e)}$, i.e.,

$$\mathrm{Gr}\,(\mathcal{C}) = \left\{\mathbf{x}^u - \mathbf{x}^v \,\middle|\, \mathbf{x}^u\mathbf{y}^v - \mathbf{x}^v\mathbf{y}^u \in \mathrm{Gr}\left(I_{\Lambda(H_e)}\right)\right\}.$$

Moreover, by Prop. 9, every reduced Gröbner basis for $I_{\Lambda(H_e)}$ und the Graver basis coincide and in particular, $\mathcal{G} = \mathrm{Gr}\left(I_{\Lambda(H_e)}\right)$. The assertion follows. □

This result gives rise an algorithm which computes the Graver basis for the ordinary code ideal (Alg. 1). It makes use of the following macros:

- `triangleHe`(H, B) applied to an $m \times n$ matrix H over $\mathbb{F}_q$ and a basis B for the $\mathbb{F}_p$-space $\mathbb{F}_q$ returns the $mr \times nr$ integer matrix $\triangle H_e$ constructed from the matrix H according to (13).

Algorithm 1 Computation of the Graver basis for the ordinary code ideal

Input: Finite field $\mathbb{F}_q$ with prime power $q = p^r$ and $\mathbb{F}_p$-basis B for $\mathbb{F}_q$, and an $(n-k) \times n$ matrix H over $\mathbb{F}_q$.

Output: Graver basis for the code ideal $I(\mathcal{C})$ associated to the $[n,k]$ code $\mathcal{C}$ over $\mathbb{F}_p$ with parity check matrix H.

1: $I \leftarrow \texttt{toricIdeal}(\Lambda(H)_p, nr, nr, (n-k)r)$;
2: $I_{\Lambda(H)} \leftarrow \texttt{substitute}(I, \mathbf{z} \to \mathbf{1})$;
3: $G \leftarrow \texttt{groebnerBasis}(I_{\Lambda(H)}, \succ)$;
4: **return** $\mathrm{Gr}(\mathcal{C}) \leftarrow \texttt{substitute}(G, \mathbf{y} \to \mathbf{1})$

- $\texttt{pLawrenceLift}(M)$ applied to an integer matrix M and a prime number p returns its p-Lawrence lifting.
- $\texttt{toricIdeal}(M, m, n, o)$ applied to an integer matrix M and non-negative integers m, n, o returns a generating set for the toric ideal associated to M in $\mathbb{K}[\mathbf{x}, \mathbf{y}, \mathbf{z}]$ with $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$ having the respective lengths m, n, o.
- $\texttt{substitute}(S, \mathbf{v} \to \mathbf{1})$ applied to a set of polynomials S and a sequence of variables $\mathbf{v}$ returns the set of polynomials from S where the variables in $\mathbf{v}$ are substituted by 1.
- $\texttt{groebnerBasis}(I, \succ)$ applied to a set of polynomials I and a monomial order $\succ$ returns the reduced Gröbner basis for I w.r.t. $\succ$.

Example 4.11. Consider the $[3,2]$ code $\mathcal{C}$ over the field $\mathbb{F}_3$ with parity check matrix

$$H = \begin{pmatrix} 1 & 2 & 1 \end{pmatrix}.$$

Note that $\triangle H_e = \begin{pmatrix} 1 & 2 & 1 \end{pmatrix}$ and so the 3-Lawrence lifting of the matrix $\triangle H_e$ is

$$\Lambda(H_e)_3 = \left(\begin{array}{ccc|ccc|c} 1 & 2 & 1 & 0 & 0 & 0 & 3 \\ \hline & I_3 & & & I_3 & & \mathbf{0} \end{array}\right).$$

Computing the reduced Gröbner basis for the toric ideal $I_{\Lambda(H_e)_3}$ in the polynomial ring $\mathbb{F}_2[x_1, x_2, x_3, y_1, y_2, y_3, z]$ w.r.t. the grevlex order and substituting $z \mapsto 1$ yields a generating set for the ideal $I_{\Lambda(H_e)}$,

$$\{x_3^3 + y_3^3,\ x_2^3 + y_2^3,\ x_2x_3 + y_2y_3,\ x_1^3 + y_1^3,\ x_1x_3^2 + y_1y_3^2,$$

$$x_1^2x_3 + y_1^2y_3,\ x_1x_2 + y_1y_2,\ x_3y_2^2 + x_2^2y_3,\ x_3^2y_2 + x_2y_3^2,$$
$$x_3y_1 + x_1y_3,\ x_1^2y_2 + x_2y_1^2,\ x_1y_2^2 + x_2^2y_1,\ x_1x_3y_2 + x_2y_1y_3\big\}$$

which is also the reduced Gröbner basis w.r.t. the same monomial order. Moreover, the substitution $\mathbf{y} \mapsto \mathbf{1}$ yields the Graver basis for the code $\mathcal{C}$,

$$\mathrm{Gr}\,(\mathcal{C}) = \big\{x_3^3 + 1,\ x_2^3 + 1,\ x_2x_3 + 1,\ x_1^3 + 1,\ x_1x_3^2 + 1,\ x_1^2x_3 + 1,\ x_1x_2 + 1,$$
$$x_3 + x_2^2,\ x_3^2 + x_2,\ x_3 + x_1,\ x_1^2 + x_2,\ x_1 + x_2^2,\ x_1x_3 + x_2\big\}.$$

♢

Second, consider generalized code ideals.

Proposition 12. *Let $\mathcal{C}$ be an $[n,k]$ code over $\mathbb{F}_q$ with parity check matrix H, and let $\mathcal{G}$ be the reduced Gröbner basis for the ideal $I_{\Lambda(H_{+,e})}$ w.r.t. any monomial order. Then the Graver basis for the generalized code ideal $I_+(\mathcal{C})$ associated to the code $\mathcal{C}$ is given by*

$$Gr_+\,(\mathcal{C}) = \{\mathbf{x}^u - \mathbf{x}^v \,|\mathbf{x}^u\mathbf{y}^v - \mathbf{x}^v\mathbf{y}^u \in \mathcal{G}\}\,. \tag{21}$$

The proof is similar to that of Prop. 10 using the Prop. 8, 6, and 9.

This assertion provides an algorithm for computing the Graver basis for a generalized code ideal (Alg. 2).

It will make use of the additional macro:

- `triangleHe+`(H, B) applied to an $m \times n$ matrix H over a finite field $\mathbb{F}_q$ and a $\mathbb{F}_p$-basis B for for $\mathbb{F}_q$ returns the integer $mr \times n(q-1)$ matrix $\triangle H_{+,e}$ obtained from the matrix H according to (15).

Example 4.13. (Ex. 7 cont'd) The 2-Lawrence lifting of the matrix $\triangle H_{+,e}$ gives the matrix

$$\Lambda\,(H_{+,e})_2 = \left(\begin{array}{ccc|ccc|ccc|c|cc} 1&0&1&1&1&0&0&1&1&\mathbf{0}&2&0\\ 1&1&0&0&1&1&1&0&1&\mathbf{0}&0&2\\ \hline \multicolumn{9}{c|}{\multirow{2}{*}{I_9}} & \multirow{2}{*}{I_9} & \multicolumn{2}{c}{\multirow{2}{*}{$\mathbf{0}\ \ \mathbf{0}$}}\\ \multicolumn{9}{c|}{} & & \multicolumn{2}{c}{} \end{array}\right).$$

Using this matrix the Graver basis for $I_+(\mathcal{C})$ can be computed by Alg. 2. This basis consists of 135 binomials. ♢

Algorithm 2 Computation of the Graver basis for the generalized code ideal

Input: Finite field $\mathbb{F}_q$ with prime power $q = p^r$, an $\mathbb{F}_p$-basis B for $\mathbb{F}_q$ and a primitive element α, and an $(n-k) \times n$ matrix H over $\mathbb{F}_q$.

Output: Graver basis for the generalized code ideal $I_+(\mathcal{C})$ associated to the $[n,k]$ code $\mathcal{C}$ over $\mathbb{F}_q$ with parity check matrix H.

1: $\triangle He+ \leftarrow$ `triangleHe+`(H, B);
2: $\Lambda(H)_p \leftarrow$ `pLawrenceLift`$(\triangle He, p)$;
3: $I \leftarrow$ `toricIdeal`$(\Lambda(H)_p, n(q-1), n(q-1), (n-k)r)$;
4: $I_{\Lambda(H)} \leftarrow$ `substitute`$(I, \mathbf{z} \to \mathbf{1})$;
5: $G \leftarrow$ `groebnerBasis`$(I_{\Lambda(H)}, \succ)$;
6: **return** $\mathrm{Gr}(\mathcal{C}) \leftarrow$ `substitute`$(G, \mathbf{y} \to \mathbf{1})$

5. Computing the Universal Gröbner Basis

In this section, the universal Gröbner basis for a generalized code ideal will be established from the Graver basis. The results are equally applicable to ordinary code ideals.

Lemma 14. *Let I be a binomial ideal in $\mathbb{K}[\mathbf{x}]$ and let $\mathbf{x}^u - \mathbf{x}^{u'}$ be a binomial in I. If there is a binomial $\mathbf{x}^v - \mathbf{x}^{v'} \in I$ such that both monomials $\mathbf{x}^v$ and $\mathbf{x}^{v'}$ divide either $\mathbf{x}^u$ or $\mathbf{x}^{u'}$, then $\mathbf{x}^u - \mathbf{x}^{u'}$ does not belong to any reduced Gröbner basis for the ideal I.*

Proof. Let $\succ$ be any monomial order on $\mathbb{K}[\mathbf{x}]$, let $\mathbf{x}^u$ be the leading term of the binomial $\mathbf{x}^u - \mathbf{x}^{u'}$, and $\mathbf{x}^v - \mathbf{x}^{v'}$ be a binomial in I with leading monomial $\mathbf{x}^v$.

First, assume that both terms in $\mathbf{x}^v - \mathbf{x}^{v'}$ divide $\mathbf{x}^u$. But as both divide the monomial $\mathbf{x}^u$, $\mathbf{x}^u - \mathbf{x}^{u'}$ cannot belong to the reduced Gröbner basis w.r.t. $\succ$.

Second, assume that both terms in $\mathbf{x}^v - \mathbf{x}^{v'}$ divide $\mathbf{x}^{u'}$. This contradicts $\mathbf{x}^{u'}$ being a standard monomial. □

Example 5.15. (Ex. 11 cont'd) The Graver basis for the linear code $\mathcal{C}$ over $\mathbb{F}_3$ with parity check matrix $H = (1\,2\,1)$ is given by

$$\mathrm{Gr}\,(\mathcal{C}) = \big\{x_3^3+1,\ x_2^3+1,\ x_2x_3+1,\ x_1^3+1,\ x_1x_3^2+1,\ x_1^2x_3+1,\ x_1x_2+1,\\ x_3+x_2^2,\ x_3^2+x_2,\ x_3+x_1,\ x_1^2+x_2,\ x_1+x_2^2,\ x_1x_3+x_2\big\}.$$

By Lemma 14, $x_1x_3+x_2$ does not belong to the universal Gröbner basis because both terms of the primitive binomial x_1+x_3 divide x_1x_3. In fact, it can be shown that $\mathcal{U}(\mathcal{C}) = \mathrm{Gr}(\mathcal{C}) \setminus \{x_1x_3+x_2\}$. ♢

Proposition 16. *The universal Gröbner basis for the generalized code ideal associated to a linear code over a finite field with characteristic two consists of exactly those primitive binomials whose involved terms are both unequal to* 1 *with the exception of the binomials of the form* $x_{ij}^2 - 1$.

Proof. Let $\mathcal{C}$ be an $[n, k]$ code over a field $\mathbb{F}_q$ with characteristic 2. Note that all primitive binomials in the generalized code ideal $I_+(\mathcal{C})$ are squarefree since $x_{ij}^2 - 1 \in I_+(\mathcal{C})$ for all $1 \leq i \leq n$ and $1 \leq j \leq q-1$,

First, claim that no primitive binomial with one term equal to 1 belongs to the universal Gröbner basis. Indeed, let $\mathbf{x}^c - 1 \in I_+(\mathcal{C})$ be a primitive binomial with $\deg(\mathbf{x}^c) > 1$. Since $\mathbf{x}^c \neq 1$, we can write $\mathbf{x}^c = x_{ij}\mathbf{x}^{c'}$ for some i, j and $c' \neq \mathbf{0}$. Then $x_{ij}(\mathbf{x}^c - 1) \equiv \mathbf{x}^{c'} - x_{ij} \bmod x_{ij}^2 - 1$ and thus $\mathbf{x}^{c'} - x_{ij}$ belongs to $I_+(\mathcal{C})$. Since $\mathbf{x}^{c'}$ and x_{ij} are both proper factors of $\mathbf{x}^c$, the binomial $\mathbf{x}^c - 1$ cannot belong to the universal Gröbner basis by Lemma 14.

Second, claim that any primitive binomial whose involved terms are both unequal to 1 belongs to the universal Gröbner basis. Indeed, let $\mathbf{x}^u - \mathbf{x}^{u'} \in I_+(\mathcal{C})$ be a primitive binomial with $u, u' \neq \mathbf{0}$, and put $s = \deg(\mathbf{x}^u)$ and $t = \deg(\mathbf{x}^{u'})$, and assume that $s \geq t$ (according to Prop. 23 it is sufficient to show that either $\mathbf{x}^u - \mathbf{x}^{u'}$ or $\mathbf{x}^u - \mathbf{x}^{u'}$ belongs to the universal Gröbner basis).

Assume that this binomial does not belong to the universal Gröbner basis and therefore not to any reduced Gröbner basis. Let $\succ$ be a monomial order with the property that

$$\{x_{ij} \mid ij \notin \operatorname{supp}(u) \cup \operatorname{supp}(u')\} \succ \{x_{ij} \mid ij \in \operatorname{supp}(u) \cup \operatorname{supp}(u')\}$$

and the monomials in $\{x_{ij} \mid ij \in \operatorname{supp}(u) \cup \operatorname{supp}(u')\}$ are compared by their ω-degree, where $\omega_{ij} = 1$ for $ij \in \operatorname{supp}(u)$ and $\omega_{ij} = \frac{s-1}{t}$ for $ij \in \operatorname{supp}(u')$. In view of this order, $\mathbf{x}^u \succ \mathbf{x}^{u'}$ because $u \cdot \omega = s > s - 1 = \frac{s-1}{t} t = u' \cdot \omega$.

Since the considered binomial lies in the ideal $I_+(\mathcal{C})$ it must be reduced to zero on division by the reduced Gröbner basis $\mathcal{G}_\succ(I_+(\mathcal{C}))$ It follows that there must be a pure binomial $\mathbf{x}^v - \mathbf{x}^{v'} \in \mathcal{G}_\succ(I_+(\mathcal{C}))$ with leading term $\mathbf{x}^v$ such that $\mathbf{x}^v$ divides $\mathbf{x}^u$.

We have $\operatorname{supp}(v) \cap \operatorname{supp}(v') = \emptyset$, $\operatorname{supp}(v) \subset \operatorname{supp}(u)$, and by the chosen monomial order, $\operatorname{supp}(v') \subseteq \operatorname{supp}(u) \cup \operatorname{supp}(u')$. However, $\operatorname{supp}(v') \not\subset \operatorname{supp}(u')$ since this would contradict the primitiveness of the binomial $\mathbf{x}^u - \mathbf{x}^{u'}$. Moreover, $\operatorname{supp}(v') \not\subset \operatorname{supp}(u)$ since otherwise the binomial $\mathbf{x}^{v+v'} - 1 \equiv \mathbf{x}^{v'}(\mathbf{x}^v - \mathbf{x}^{v'}) \bmod I_q$ would contradict the primitiveness. In other words, the monomial $\mathbf{x}^{v'}$ must involve variables from both $\mathbf{x}^u$ and $\mathbf{x}^{u'}$.

Claim that $\operatorname{supp}(v) \cup \operatorname{supp}(v') = \operatorname{supp}(u) \cup \operatorname{supp}(u')$. Indeed, write $\mathbf{x}^{v'}$ as a product of monomials $\mathbf{x}^{u_1}$ and $\mathbf{x}^{u_2}$ such that $\operatorname{supp}(u_1) \subset \operatorname{supp}(u)$ and

$\mathrm{supp}(u_2) \subset \mathrm{supp}(u')$. Then $\mathbf{x}^{u_1}(\mathbf{x}^v - \mathbf{x}^{u_1+u_2}) \equiv \mathbf{x}^{u_1+v} - \mathbf{x}^{u_2} \bmod I_q$ belongs to $I_+(\mathcal{C})$, where $\mathbf{x}^{u_1+v}$ divides $\mathbf{x}^u$ and $\mathbf{x}^{u_2}$ divides $\mathbf{x}^{u'}$. Since the binomial $\mathbf{x}^u - \mathbf{x}^{u'}$ is primitive, it follows that $\mathbf{x}^{u_1+v} = \mathbf{x}^u$ and $\mathbf{x}^{u_2} = \mathbf{x}^{u'}$. This proves the claim.

Summing up, $\mathbf{x}^v - \mathbf{x}^{v'} = \mathbf{x}^{u_1} - \mathbf{x}^{u_2}\mathbf{x}^{u'}$ where $\mathbf{x}^{u_1}\mathbf{x}^{u_2} = \mathbf{x}^u$ and $u_1, u_2 \neq \mathbf{0}$. Since $\deg(\mathbf{x}^u) = s$ there must be an integer $i \geq 1$ such that $\deg(\mathbf{x}^{u_1}) = s - i$ and $\deg(\mathbf{x}^{u_2}) = i$. Then

$$u_1 \cdot \omega = s - i < s \leq s - 1 + i = u' \cdot \omega + u_2 \cdot \omega = (u' + u_2) \cdot \omega.$$

shows that $\mathrm{lt}_\succ(\mathbf{x}^v - \mathbf{x}^{v'}) = \mathbf{x}^{v'}$, a contradiction. Hence, the binomial $\mathbf{x}^u - \mathbf{x}^{u'}$ belongs to the universal Gröbner basis. □

For linear codes over a finite field with characteristic 2, Prop. 16 provides an easy way to obtain the universal Gröbner from the Graver basis.

Example 5.17. (Ex. 13 cont'd) The Graver basis consists of 135 binomials. Removing all binomials with one involved term equal to 1 gives the universal Gröbner basis consisting of 99 binomials. ♢

For linear codes over a finite field with characteristic > 2 a method similar to that in [18] for toric ideals can be applied in order to compute the universal Gröbner basis from the Graver basis.

To this end, for a given non-negative weight vector $\omega \in \mathbb{R}_+^{n(q-1)}$ and an ideal I, denote by $\mathcal{G}_\omega(I)$ the reduced Gröbner basis for I w.r.t. $\succ_\omega$, where $\succ$ is some tie breaking monomial order.

For any elements $u, u' \in \mathbb{N}_0^{n(q-1)}$ define the cone

$$C[u, u'] = \left\{\omega \in \mathbb{R}_+^{n(q-1)} \mid \omega \cdot u > \omega \cdot u' \ \wedge\ \mathbf{x}^u - \mathbf{x}^{u'} \in \mathcal{G}_\omega(I_+(\mathcal{C}))\right\}. \qquad (22)$$

This cone is essentially the same as in [18]. In this setting, however, the cone is restricted to the positive orthant.

Lemma 18. *[18, Proposition 1.11] For any monomial order $\succ$ and any ideal I in $\mathbb{K}[\mathbf{x}]$, there exists a non-negative integer vector $\omega \in \mathbb{N}^{n(q-1)}$ such that $lt_\omega(I) = lt_\succ(I)$.*

Proposition 19. *The primitive binomial $\mathbf{x}^u - \mathbf{x}^{u'} \in I_+(\mathcal{C})$ belongs to the universal Gröbner basis of $I_+(\mathcal{C})$ if and only if the cone $C[u, u']$ is non-empty.*

Proof. If the cone $C[u, u']$ is non-empty, then by definition $\mathbf{x}^u - \mathbf{x}^{u'} \in \mathcal{U}_+(\mathcal{C})$.

Conversely, assume that $\mathbf{x}^u - \mathbf{x}^{u'}$ belongs to the universal Gröbner basis of $I_+(\mathcal{C})$. Then there is a monomial order $\succ$ such that $\mathbf{x}^u - \mathbf{x}^{u'} \in \mathcal{G}_\succ(I_+(\mathcal{C}))$

with $\mathbf{x}^u$ being the leading monomial and thus $\mathbf{x}^{u'}$ being a standard monomial. By Lemma 18, there is a weight vector $\omega \in \mathbb{R}_+^{n(q-1)}$ such that $\mathrm{lt}_\omega(I_+(\mathcal{C})) = \mathrm{lt}_\succ(I_+(\mathcal{C}))$. Therefore, $\mathbf{x}^u \in \mathrm{lt}_\omega(I_+(\mathcal{C}))$. Moreover, $\mathbf{x}^u - \mathbf{x}^{u'} \notin \mathrm{lt}_\omega(I_+(\mathcal{C}))$ because otherwise

$$\mathbf{x}^u - \left(\mathbf{x}^u - \mathbf{x}^{u'}\right) = \mathbf{x}^{u'} \in \mathrm{lt}_\omega(I_+(\mathcal{C})) = \mathrm{lt}_\succ(I_+(\mathcal{C}))$$

contradicting the fact that $\mathbf{x}^{u'}$ is a standard monomial. This implies that $\omega \cdot u > \omega \cdot u'$ and thus that $C[u, u']$ is non-empty. □

Given an $[n, k]$ code $\mathcal{C}$ over $\mathbb{F}_q$ and a vector $u \in \mathbb{N}_0^{n(q-1)}$. Define

$$\mathrm{Co}(u) = \mathrm{Co}(u, \mathcal{C}) = \left\{ v \in \mathbb{N}_0^{n(q-1)} \,|\, \blacktriangledown u - \blacktriangledown v \in \mathcal{C} \right\} \tag{23}$$

and

$$\mathcal{M}(u) = \left\{ \omega \in \mathbb{R}_+^{n(q-1)} \,|\, \omega \cdot u < \omega \cdot v \; \forall v \in \mathrm{Co}(u) \setminus \{u\} \right\}. \tag{24}$$

Lemma 20. *[18, Lemma 7.4] For $u, u' \in \mathbb{N}_0^{n(q-1)}$,*

$$C[u, u'] = \mathcal{M}(u') \cap \bigcap_{ij \in supp(u)} \mathcal{M}(u - \mathbf{e}_{ij}). \tag{25}$$

A proof is given in [18]. The set $\mathcal{M}(v)$ and thus the cone $C[u, u']$ can be computed from the Graver basis [18]. To see this, note that $\omega \in \mathcal{M}(u)$ implies that $\mathbf{x}^u \notin \mathrm{lt}_\omega(I_+(\mathcal{C}))$. Moreover,

$$\mathrm{lt}_\omega(I_+(\mathcal{C})) = \langle \mathrm{lt}_\omega(f) \mid f \in \mathrm{Gr}_+(\mathcal{C}) \rangle \,. \tag{26}$$

It follows that a monomial $\mathbf{x}^u$ does not belong to the leading ideal $\mathrm{lt}_\omega(I_+(\mathcal{C}))$ if and only if for each primitive binomial $\mathbf{x}^v - \mathbf{x}^{v'}$ in $I_+(\mathcal{C})$ such that $\mathbf{x}^v$ divides $\mathbf{x}^u$, $\mathrm{lt}_\omega(\mathbf{x}^v - \mathbf{x}^{v'}) \neq \mathbf{x}^v$, which is equivalent to $\omega \cdot v \leq \omega \cdot v'$. But as the set $\mathcal{M}(u)$ is open, it can be described by all such strict inequalities. This yields an alternative description of the set $\mathcal{M}(v)$,

$$\mathcal{M}(v) = \left\{ \omega \in \mathbb{R}_+^{n(q-1)} \,\middle|\, \forall \mathbf{x}^u - \mathbf{x}^{u'} \in \mathrm{Gr}_+(\mathcal{C}) \text{ s.t. } \mathbf{x}^u \,|\, \mathbf{x}^v : \left[\omega \cdot u' > \omega \cdot u\right] \right\}. \tag{27}$$

Similar to [18, Corollary 7.9, Proof of Theorem 7.8] it will be shown that if $\mathbf{x}^u - \mathbf{x}^{u'}$ belongs to the universal Gröbner basis for $I_+(\mathcal{C})$, then so does $\mathbf{x}^{u'} - \mathbf{x}^u$. Although this is true for toric ideals and binomial ideals associated to integer lattices [18, 19], it does not hold for binomial ideals in general as demonstrated in the following

Example 5.21. Take the binomial ideal $I = \langle x^2 - xy, y^2 - xy \rangle$ in $\mathbb{K}[x, y]$. The reduced Gröbner basis w.r.t. the lex order with $x \succ y$ is given by the set $\{xy - y^2, x^2 - y^2\}$. Thus $xy - y^2$ belongs to the universal Gröbner basis for I. Suppose $y^2 - xy$ also belongs to the universal Gröbner basis and therefore to some reduced Gröbner basis $\mathcal{G}_\succ(I)$ with $y^2 \succ xy$. Pick any weight vector $\omega = (\omega_1, \omega_2) \in \mathbb{R}^2_+$ that represents the order $\succ$. Clearly, $\omega_2 > \omega_1$ and thus $xy \succ x^2$. But as $xy - x^2 \in I$, the monomial xy cannot be standard contradicting the assumption that $y^2 - xy$ belongs to any reduced Gröbner basis. ♢

Lemma 22. *A primitive binomial $\mathbf{x}^u - \mathbf{x}^{u'}$ in the generalized code ideal $I_+(\mathcal{C})$ with $u, u' \neq \mathbf{0}$ belongs to the universal Gröbner basis if there is a non-negative vector $\omega \in \mathbb{R}^{n(q-1)}_+$ such that*

$$\omega \cdot u' \leq \omega \cdot u < \omega \cdot v \quad \text{for all } v \in Co(u) \setminus \{u, u'\}.$$

Proof. Assume that such a vector $\omega \in \mathbb{R}^{n(q-1)}_+$ exists. Claim that $\omega \in \bigcap_{ij \in \mathrm{supp}(u)} \mathcal{M}(u - \mathbf{e}_{ij})$, i.e., each proper factor of the monomial $\mathbf{x}^u$ is standard w.r.t. the weight vector ω. Indeed, if $\omega \notin \mathcal{M}(u - \mathbf{e}_{ij})$ for some $ij \in \mathrm{supp}(u)$, then there is an element $v \in \mathrm{Co}(u - \mathbf{e}_{ij}) \setminus \{u - \mathbf{e}_{ij}\}$ such that $\omega \cdot (u - \mathbf{e}_{ij}) \geq \omega \cdot v$. Thus $\omega \cdot (v + \mathbf{e}_{ij}) \leq \omega \cdot u$ with $v + \mathbf{e}_{ij} \in \mathrm{Co}(u) \setminus \{u\}$. By hypothesis, $v + \mathbf{e}_{ij} = u'$ contradicting the assumption that the binomial $\mathbf{x}^u - \mathbf{x}^{u'}$ is pure and so not primitive. This proves the claim.

First, consider the case $\omega \cdot u' < \omega \cdot u$. Then the definition, $\omega \in \mathcal{M}(u')$ and the result follows from Prop. 19 and Lemma 20.

Second, consider the case $\omega \cdot u' = \omega \cdot u$. Let $\succ$ be any monomial order such that $\{x_{ij} \,|ij \in \mathrm{supp}(u)\} \succ \{x_{ij} \,|ij \in \mathrm{supp}(u')\}$. Therefore, $\mathbf{x}^u \succ_\omega \mathbf{x}^{u'}$ and since every proper factor of $\mathbf{x}^u$ is standard, we see that this monomial is actually a minimal generator in $\mathrm{lt}_{\succ_\omega}(I_+(\mathcal{C}))$. Moreover, $\mathbf{x}^{u'}$ is a standard monomial w.r.t. $\succ_\omega$ because $\omega \cdot u' < \omega \cdot v$ for all $v \in \mathrm{Co}(u) \setminus \{u, u'\}$. This shows that $\mathbf{x}^u - \mathbf{x}^{u'} \in \mathcal{G}_\omega(I_+(\mathcal{C}))$. □

Proposition 23. *If a binomial $\mathbf{x}^u - \mathbf{x}^{u'}$ with $u, u' \neq \mathbf{0}$ belongs to the universal Gröbner basis for the generalized code ideal $I_+(\mathcal{C})$, then the binomial $\mathbf{x}^{u'} - \mathbf{x}^u$ also belongs to the universal Gröbner basis.*

Proof. Assume that $\mathbf{x}^u - \mathbf{x}^{u'}$ belongs to the universal Gröbner basis with leading term $\mathbf{x}^u$. This binomial is pure, primitive, and there is a monomial order $\succ$ such that $\mathbf{x}^u - \mathbf{x}^{u'} \in \mathcal{G}_\succ(I_+(\mathcal{C}))$ and $\mathrm{lt}_\succ(\mathbf{x}^u - \mathbf{x}^{u'}) = \mathbf{x}^u$.

By Lemma 18, there is a weight vector $\omega \in \mathbb{R}^{n(q-1)}_+$ that represents the order $\succ$. Suppose all coordinates of ω are strictly positive (otherwise ω can be replaced by a nearby vector from the same Gröbner cone). Then $\omega \cdot u > \omega \cdot u'$.

Define the weight vector $\omega' \in \mathbb{R}_+^{n(q-1)}$ as follows: Put $\omega'_{ij} = 0$ for $ij \in \operatorname{supp}(u)$ and $\omega'_{ij} = \omega_{ij}$ otherwise. Then $0 = \omega' \cdot u < \omega' \cdot u'$. Define another weight vector

$$\omega'' = (\omega \cdot (u - u'))\omega' - (\omega' \cdot (u - u'))\omega.$$

This vector is non-negative since $\omega' \cdot (u - u')$ is a negative scalar and $\omega \cdot (u - u')$ is a positive scalar. By definition, $\omega'' \cdot (u - u') = 0$ and so $\omega'' \cdot u = \omega'' \cdot u'$.

Claim that $\omega'' \cdot u < \omega'' \cdot v$ for all $v \in \operatorname{Co}(u) \setminus \{u, u'\}$. Indeed, first let $\omega \cdot v < \omega \cdot u$. Then the binomial $\mathbf{x}^u - \mathbf{x}^v \in I_+(\mathcal{C})$ has leading term $\mathbf{x}^u$. We conclude that $\operatorname{supp}(u)$ and $\operatorname{supp}(v)$ are disjoint because otherwise $\mathbf{x}^u$ would have a proper factor that belongs to $\operatorname{lt}_\succ(I_+(\mathcal{C}))$. This implies $\omega' \cdot v = \omega \cdot v$. Furthermore, $\omega \cdot v > \omega \cdot u'$ since $\mathbf{x}^{u'}$ is a standard monomial. Hence,

$$\omega'' \cdot v = \big((\omega - \omega') \cdot (u - u')\big)\,(\omega \cdot v) > \big((\omega - \omega') \cdot (u - u')\big)\,(\omega \cdot u') = \omega'' \cdot u' = \omega'' \cdot u.$$

Second, let $\omega \cdot v \geq \omega \cdot u$. Then

$$\begin{aligned} \omega'' \cdot v &= (\omega \cdot (u - u'))(\omega' \cdot v) - (\omega' \cdot (u - u'))(\omega \cdot v) \\ &\geq (\omega \cdot (u - u'))(\omega' \cdot v) - (\omega' \cdot (u - u'))(\omega \cdot u) \\ &> -(\omega' \cdot (u - u'))(\omega \cdot u) = \omega'' \cdot u. \end{aligned}$$

This proves the claim. In particular, $\omega'' \cdot u = \omega'' \cdot u' < \omega'' \cdot v$ for all $v \in \operatorname{Co}(u) \setminus \{u, u'\}$ and hence by Lemma 22, $\mathbf{x}^{u'} - \mathbf{x}^u \in \mathcal{U}_+(\mathcal{C})$. □

Finally, a method for computing the universal Gröbner basis for a code ideal from its Graver basis is given (Alg. 3). This procedure is similar to that for toric ideals [18, Algorithm 7.6]. Its correctness follows from Prop. 19, Lemma 20 and Eq. (27). The proposed algorithm makes use of the following subroutines:

- `swap`(a, b) applied to variables a and b swaps the contents of these variables.
- $\mathbf{x}^u \mid \mathbf{x}^v$ applied to monomials $\mathbf{x}^u$ and $\mathbf{x}^v$ returns 1 if the monomial $\mathbf{x}^u$ divides the monomial $\mathbf{x}^v$ and 0 otherwise.
- `addRow`(A, a) applied to an integer $m \times n$ matrix A and an integer row vector a of length m returns the extended matrix A by adding the row a.
- `break` quits the current `for`-loop.
- `empty`(A) applied to an integer $m \times n$ matrix A returns 1 if the open cone defined by $\{\omega \in \mathbb{R}_+^n \mid A\omega > 0\}$ is empty and 0 otherwise.

The run-time of the algorithm depends on the size of the Graver basis and is in the worst-case $O\left(|\operatorname{Gr}_+(\mathcal{C})|^2\right)$.

Algorithm 3 Computation of the universal Gröbner basis

Input: Graver basis $\mathrm{Gr}_+(\mathcal{C})$
Output: Universal Gröbner basis $\mathcal{U}_+(\mathcal{C})$

$\mathcal{U}_+(\mathcal{C}) \leftarrow \mathrm{Gr}_+(\mathcal{C})$;
$A \leftarrow [\,]$;
for all $\mathbf{x}^u - \mathbf{x}^{u'} \in \mathrm{Gr}_+(\mathcal{C})$ **do**
  if $|\mathrm{supp}(u')| < |\mathrm{supp}(u)|$ **then**
    $\mathtt{swap}(u, u')$;
  end if
  for all $\mathbf{x}^v - \mathbf{x}^{v'} \in \mathrm{Gr}_+(\mathcal{C})$ **do**
    $a_{11} \leftarrow \mathbf{x}^v \mid \mathbf{x}^u$;
    $a_{12} \leftarrow \mathbf{x}^v \mid \mathbf{x}^{u'}$;
    $a_{21} \leftarrow \mathbf{x}^{v'} \mid \mathbf{x}^u$;
    $a_{22} \leftarrow \mathbf{x}^{v'} \mid \mathbf{x}^{u'}$;
    if $(a_{11} \wedge a_{12}) \vee (a_{21} \wedge a_{22})$ **then**
      $\mathcal{U}_+(\mathcal{C}) \leftarrow \mathcal{U}_+(\mathcal{C}) \setminus \{\mathbf{x}^u - \mathbf{x}^{u'}\}$;
      `break`;
    end if
    for all $ij \in \mathrm{supp}(u)$ **do**
      if $\mathbf{x}^v \mid \mathbf{x}^{u-\mathbf{e}_{ij}}$ **then**
        $A \leftarrow \mathtt{addRow}(A, v' - v)$;
      else if $\mathbf{x}^{v'} \mid \mathbf{x}^{u-\mathbf{e}_{ij}}$ **then**
        $A \leftarrow \mathtt{addRow}(A, v - v')$;
      end if
    end for
    if a_{12} **then**
      $A \leftarrow \mathtt{addRow}(A, v' - v)$;
    else if a_{22} **then**
      $A \leftarrow \mathtt{addRow}(A, v - v')$;
    end if
  end for
  if $\mathtt{empty}(A)$ **then**
    $\mathcal{U}_+(\mathcal{C}) \leftarrow \mathcal{U}_+(\mathcal{C}) \setminus \{\mathbf{x}^u - \mathbf{x}^{u'}\}$;
  end if
end for
return $\mathcal{U}_+(\mathcal{C})$

References

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

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

[3] A.M. Bigatti and L. Robbiano, Toric ideals, *Mathematica Contemporanea*, **21**, (2001), 125.

[4] M. Borges-Quintana, M.A. Borges-Trenard, P. Fitzpatrick, and E. Martinez-Moro, Gröbner bases and combinatorics for binary codes, *AAECC*, **19**, No. 5 (2008), 393411.

[5] M. Borges-Quintana, M.A. Borges-Trenard, and E. Martinez- Moro, On a Gröbner bases structure associated to linear codes, *J. of Discret. Math. Sci. and Cryptogr.*, **10**, No. 2 (2007), 151191.

[6] B. Buchberger, *An Algorithm for Finding the Bases Elements of the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal*, PhD thesis, University of Innsbruck (1965).

[7] D. Cox, J. Little, and D. OShea, *Ideals, Varieties, and Algorithms*, Springer (1996).

[8] D. Cox, J. Little, and D. OShea, *Using Algebraic Geometry*, Springer (1998).

[9] N. Dück and K.-H. Zimmermann, Universal Gröbner Bases for Binary Linear Codes, *IJPAM*, **86**, No. 2 (2013),345358.

[10] K. Fukuda, A. N. Jensen, and R. R. Thomas, Computing Gröbner fans, *Math. Comput.*, **76** No. 260 (2007), 21892212.

[11] G.-M. Greuel and G. Pfister, *A Singular Introduction to Commutative Algebra*, Springer, Berlin (2002).

[12] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, New York (1977).

[13] I. Marquez-Corbella and E. Martinez-Moro, Algebraic structure of the minimal support codewords set of some linear codes. *Adv. in Math. of Commun.*, **5**, (2011), 233244.

[14] I. Marquez-Corbella, E. Martinez-Moro, and E. Suarez-Canedo, On the ideal associated to a linear code, *Adv. in Math. of Commun.*, submitted (2012).

[15] M. Saleemi and K.-H. Zimmermann, Linear codes as binomial ideals, *IJPAM*, **61**, No. 2 (2010), 147156.

[16] M. Saleemi and K.-H. Zimmermann, Gröbner bases for linear codes over GF(4), *IJPAM*, **73**, No. 4 (2011), 435442.

[17] N. Schwartz, Stability of Gröbner bases, *Journal of Pure and Applied Algebra*, **53**, No. 12 (1988), 171 186.

[18] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, American Mathematical Society, USA (1996).

[19] B. Sturmfels, R. Weismantel, and G. M. Ziegler, Gröbner Bases of Lattices, Corner Polyhedra, and Integer Programming. *Beitrge zur Algebra und Geometrie*, **36**, No. 2 (1995), 281298.

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

[21] V. Weispfenning, Constructing Universal Gröbner bases, *AAECC*, **356** (1987), 408417.