International Journal of Pure and Applied Mathematics
Volume 58 No. 1 2010, 1-9

GROEBNER BASES FOR A CLASS OF IDEALS IN COMMUTATIVE POLYNOMIAL RINGS

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

Abstract: We construct reduced Groebner bases for a certain class of ideals in commutative polynomial rings. A subclass of these ideals corresponds to the generalized Reed-Muller codes when considered in the quotient ring of the polynomial ring.

AMS Subject Classification: 13P10, 94B30
Key Words: commutative polynomial rings, ideals, Groebner bases, reduced Groebner bases, generalized Reed-Muller codes

1. Introduction

Originally, the method of Groebner bases was introduced by Bruno Buchberger for the algorithmic solution of some of the fundamental problems in commutative algebra [2], [3], and [4]. Today, Groebner bases provide a uniform approach to solving a wide range of problems expressed in terms of sets of multivariate polynomials such as the solvability and solving algebraic systems of equations, ideal and radial membership decision, effective computation in residue class rings modulo polynomial ideals, linear Diophantine equations with polynomial coefficients, algebraic relations among polynomials, implicitization, and inverse polynomial mappings [1], [5], [9], [11].

Received: October 25, 2009

§Correspondence author

The main additional ideas that contributed to the theory of Groebner bases that include Groebner bases can be constructed w.r.t. arbitrary admissible orderings and lexical orderings having the elimination property [13], Groebner bases that can be used for computing syzygies [14], Groebner bases that are universal [12], and Groebner bases that can be designed for desired orderings [8]. Moreover, there are numerous applications of Groebner bases for solving problems in various fields requiring ingenuous reductions that can be established by computations of Groebner bases [10].

Furthermore, the construction of Groebner bases for classes of ideals is of general interest [11]. In this paper, we provide reduced Groebner bases for a class of ideals in a commutative polynomial ring. A subclass of these ideals corresponds to the generalized Reed-Muller codes, when considered in a quotient ring of the polynomial ring. First, however, we provide a rapid summary of Groebner bases in the next section.

2. Polynomial Rings and Groebner Bases

We provide basic facts about polynomial rings and Groebner bases [1], [5], and [9]. For this, we consider the commutative polynomial ring $A = \mathbb{K}[x_1, \ldots, x_n]$ in n unknowns over a field $\mathbb{K}$. An element $x_1^{a_1} \cdots x_n^{a_n}$ in A is called a *monomial* and an element $cx_1^{a_1} \cdots x_n^{a_n}$ with $c \in \mathbb{K} \setminus \{0\}$ is called a *term*. The *degree* of a monomial $m = x_1^{a_1} \cdots x_n^{a_n}$ in A is $\deg(m) = a_1 + \ldots + a_n$. We write monomials in the form $\boldsymbol{x}^a = x_1^{a_1} \cdots x_n^{a_n}$, where $\boldsymbol{a} = (a_1, \ldots, a_n)$.

Let M denote the set of all monomials in A. A partial ordering $\prec$ on the set M is called *admissible* if it is a total ordering, $1 \prec m$ holds for any monomial $m \neq 1$, and the ordering is compatible with the multiplication of monomials; that is, for any pair of monomials m and m' in M, $m \prec m'$ implies $mn \prec m'n$ for any monomial n in M.

Let f be a non-zero polynomial in A and suppose $\prec$ is an admissible ordering of the monomials in A. Then f can be uniquely written as $f = c_1m_1 + \ldots + c_lm_l$ with monomials $m_1 \succ \ldots \succ m_l$ and $c_i \neq 0$, $1 \leq i \leq l$. Define the *support* of f to be $\mathrm{supp}(f) = \{m_i \mid 1 \leq i \leq l\}$, the *leading monomial* of f to be $\mathrm{lm}(f) = m_1$, the *leading term* of f to be $\mathrm{lt}(f) = c_1m_1$, the *leading coefficient* of f to be $\mathrm{lc}(f) = c_1$, and the *degree* of f to be $\deg(f) = \max\{\deg(m_i) \mid 1 \leq i \leq l\}$. It can be shown that any strictly decreasing sequence of monomials in an admissible ordering is finite. This allows to use induction over the set of polynomials in A with respect to their leading monomials.

The division algorithm for polynomials in A is based on an admissible ordering $\prec$ on the monomials in A and consists of successive reduction steps. Given a polynomial $f \in A$ and an ordered sequence $G = (g_1, \ldots, g_s)$ of polynomials in A. Define $\mathrm{rem}(f, (g_1, \ldots, g_s)) = \mathrm{rem}(f - h \cdot g_k, (g_1, \ldots, g_s))$, where k is the smallest index such that $\mathrm{lm}(g_k)$ divides $\mathrm{lm}(f)$ and $h \in A$ is chosen such that $\mathrm{lt}(f) = \mathrm{lt}(h \cdot g_k)$. If no $\mathrm{lm}(g_i)$ divides $\mathrm{lm}(f)$, define $\mathrm{rem}(f, (g_1, \ldots, g_s)) = \mathrm{lt}(f) + \mathrm{rem}(f - \mathrm{lt}(f), (g_1, \ldots, g_s))$. This reduction process is finite since in both cases the leading monomial of f drops.

For any polynomials $f, g \in A$, we have $f - \mathrm{rem}(f, (g_1, \ldots, g_s)) \in \langle g_1, \ldots, g_s \rangle$. In particular, if $\mathrm{rem}(f, (g_1, \ldots, g_s)) = 0$, then f belongs to the ideal $\langle g_1, \ldots, g_s \rangle$ in A generated by the polynomials $g_1, \ldots, g_s$.

Let I be an ideal in A. Define the ideal of leading monomials of I to be $\ell(I) = \langle \mathrm{lm}(f) \mid f \in I \rangle$. A set $\{g_1, \ldots, g_s\}$ of elements in I is called a *Groebner basis* for I if the ideal of leading monomials of I is given by $\langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s) \rangle$. It follows that if $\{g_1, \ldots, g_s\}$ is a Groebner basis for I then $I = \langle g_1, \ldots, g_s \rangle$. Each ideal in A possesses a Groebner basis and thus is finitely generated. Furthermore, it follows from the definitions that any permutation of a Groebner basis is also a Groebner basis.

Let $G = \{g_1, \ldots, g_s\}$ be a Groebner basis for the ideal $I = \langle g_1, \ldots, g_s \rangle$. Then for all polynomials $f, f' \in A$, we have $\mathrm{rem}(f, G) = \mathrm{rem}(f', G)$ if and only if $f - f' \in I$. In particular, $\mathrm{rem}(f, G) = 0$ if and only if $f \in I$. Since $f - \mathrm{rem}(f, G)$ lies in I, each element in the quotient ring A/I can be represented with a polynomial $\mathrm{rem}(f, G)$, which is given as a linear combination of monomials outside of $\ell(I)$. These monomials constitute a $\mathbb{K}$-basis for the residue ring A/I. Moreover, given a fixed admissible ordering, the polynomial $\mathrm{rem}(f, G)$ is uniquely defined and does not depend on the Groebner basis of I.

Groebner bases are not unique. However, each ideal I in A contains a reduced Groebner basis and that basis is unique. A Groebner basis $G = \{g_1, \ldots, g_s\}$ for the ideal $I = \langle g_1, \ldots, g_s \rangle$ in A is called *reduced* if the set G forms a minimal Groebner basis for I and no monomial in the support of a generator g_i is divisible by the leading monomial of another generator g_j, $i \neq j$. A Groebner basis $G = \{g_1, \ldots, g_s\}$ for the ideal $I = \langle g_1, \ldots, g_s \rangle$ in A is said to be *minimal* if each generator g_i is monic, $1 \leq i \leq s$, and the leading monomial of a generator g_i is not divisible by the leading monomial of another generator g_j, $i \neq j$.

There is a nice criterion for a set of polynomials to be a Groebner basis known as Buchberger's S-criterion. For this, let f and g be polynomials in A.

Define the *S-polynomial* of f and g as

$$S(f,g) = \frac{\mathrm{lcm}(\mathrm{lm}(f),\mathrm{lm}(g))}{\mathrm{lt}(f)} f - \frac{\mathrm{lcm}(\mathrm{lm}(f),\mathrm{lm}(g))}{\mathrm{lt}(g)} g,$$

where lcm denotes the least common multiple. The S-polynomial $S(f,g)$ cancels the initial terms of f and g according to the term ordering. *Buchberger's S-criterion* says that a set of monic polynomials $G = \{g_1, \ldots, g_s\}$ in A is a Groebner basis for the ideal $\langle g_1, \ldots, g_s \rangle$ if and only if $\mathrm{rem}(S(g_i, g_j), G) = 0$ for all $1 \leq i < j \leq s$.

3. Ideals and their Reduced Groebner Bases

Let $\mathbb{K}$ be a field and let $A = \mathbb{K}[x_1, \ldots, x_n]$ be a commutative polynomial ring over $\mathbb{K}$. Take a non-empty subset S of $\mathbb{N}_0^n$ and consider the ideal $I = I(S)$ generated by the set

$$\{\eta(\boldsymbol{a}) \mid \boldsymbol{a} \in S\}, \tag{1}$$

where

$$\eta(\boldsymbol{a}) = (x_1 - 1)^{a_1} \cdots (x_n - 1)^{a_n}, \quad a_1 \geq 0, \ldots, a_n \geq 0. \tag{2}$$

In particular, we have $\eta(\mathbf{0}) = 1$ and thus if S contains the n-tuple $\mathbf{0} = (0, \ldots, 0)$ then $I(S) = A$.

Let $M = M(S)$ be the set of n-tuples $\boldsymbol{a} \in S$ that are minimal with respect to the component-wise natural $\leq$-ordering. In particular, if $S = \mathbb{N}_0^n$ then $M(S) = \{\mathbf{0}\}$ and $I(S) = A$. If $S = \mathbb{N}_0^n \setminus \{\mathbf{0}\}$ then the set $M(S)$ consists of the unit vectors and the ideal $I(S)$ is generated by the terms $x_j - 1$, $1 \leq j \leq n$.

Theorem 1. *For any monomial ordering on A, the ideal I in A has the reduced Groebner basis*

$$G = \{\eta(\boldsymbol{a}) \mid \boldsymbol{a} \in M\}. \tag{3}$$

The ideal of leading terms of I equals $\langle \{\boldsymbol{x}^a \mid \boldsymbol{a} \in M\} \rangle$.

For the proof we need two assertions. To this end, for each non-empty subset S of $\mathbb{N}_0^n \setminus \{\mathbf{0}\}$ define

$$S' = \{(a_1, \ldots, a_j - 1, \ldots, a_n) \mid (a_1, \ldots, a_n) \in S, a_j > 0, 1 \leq j \leq n\}.$$

Then $M' = \{(a_1, \ldots, a_j - 1, \ldots, a_n) \mid (a_1, \ldots, a_n) \in M, a_j > 0, 1 \leq j \leq n\}$ is the corresponding set of minimal elements of S'. Finally, put $G' = \{\eta(\boldsymbol{a}) \mid \boldsymbol{a} \in M'\}$.

Observe that for each monomial ordering on $\mathbb{N}_0^n$, the leading monomial (and term) of $\eta(\boldsymbol{a})$, $\boldsymbol{a} \in \mathbb{N}_0^n$, equals $\boldsymbol{x}^a$. Indeed, each monomial in $\eta(\boldsymbol{a})$ is of the form

$\boldsymbol{x}^{\boldsymbol{b}}$ for some $\boldsymbol{b} \in \mathbb{N}_0^n$ with $\boldsymbol{b} \preceq \boldsymbol{a}$. Thus $\boldsymbol{a} = \boldsymbol{b} + \boldsymbol{c}$ for some $\boldsymbol{c} \in \mathbb{N}_0^n$. But $\boldsymbol{0} \preceq \boldsymbol{c}$ and thus $\boldsymbol{b} \preceq \boldsymbol{b} + \boldsymbol{c} = \boldsymbol{a}$. The claim follows.

Lemma 1. *Given any monomial ordering on A, for each polynomial $f \in A$ and each variable x_j, $1 \leq j \leq n$, we have*

$$(x_j - 1)\mathrm{rem}(f, G') = \mathrm{rem}((x_j - 1)f, G).$$

Proof. Take a monomial ordering $\prec$ on A. First, suppose there is a generator $g \in G'$ such that $\mathrm{lm}(f)$ is divisible by $\mathrm{lm}(g)$. Then $\mathrm{rem}(f, G') = \mathrm{rem}(f - g' \cdot g, G')$ for some monomial $g' \in A$ and so $\mathrm{lm}((x_j - 1)f)$ is divisible by $\mathrm{lm}((x_j - 1)g)$. But $(x_j - 1)g \in G$ and thus $\mathrm{rem}((x_j - 1) \cdot f, G) = \mathrm{rem}((x_j - 1)[f - g'g], G)$. We may assume that the assertion holds for all polynomials f' with $f' \prec f$. But $f - g'g \prec f$ and thus $(x_j - 1)[f - g'g] \prec (x_j - 1)f$. Therefore, $\mathrm{rem}((x_j - 1)[f - g'g], G) = (x_j - 1)\mathrm{rem}(f - g'g, G') = (x_j - 1)\mathrm{rem}(f, G')$, as required.

Second, suppose there is no generator $g \in G'$ such that $\mathrm{lm}(f)$ is divisible by $\mathrm{lm}(g)$. Then there is no generator $g \in G'$ such that $\mathrm{lm}((x_j - 1)f)$ is divisible by $\mathrm{lm}((x_j - 1)g)$. Write $f = m + h$, where $m = \mathrm{lt}(f)$. Then $\mathrm{rem}(f, G') = \mathrm{lt}(f) + \mathrm{rem}(f - \mathrm{lt}(f), G') = m + \mathrm{rem}(h, G')$. Moreover, $\mathrm{rem}((x_j - 1)f, G) = \mathrm{lt}((x_j - 1)f) + \mathrm{rem}((x_j - 1)f - \mathrm{lt}((x_j - 1)f), G) = x_j m + \mathrm{rem}((x_j - 1)h - m, G)$.

First, suppose that the leading term of $(x_j - 1)h - m$ is $-m$. Thus $\mathrm{rem}((x_j - 1)h - m, G) = -m + \mathrm{rem}((x_j - 1)h - m - (-m), G) = -m + \mathrm{rem}((x_j - 1)h, G)$. We may assume that the assertion holds for all polynomials f' with $f' \prec f$. But $h \prec f$ and thus $\mathrm{rem}((x_j - 1)h, G) = (x_j - 1)\mathrm{rem}(h, G')$. It follows that $\mathrm{rem}((x_j - 1)f, G) = (x_j - 1)m + (x_j - 1)\mathrm{rem}(h, G') = (x_j - 1)[m + \mathrm{rem}(h, G')] = (x_j - 1)\mathrm{rem}(f, G')$, as required.

Second, assume that the leading term of $(x_j - 1)h - m$ is $x_j m'$, where $h = m' + h'$ and m' is the leading term of h. There are two cases.

First, suppose that there exists no generator $g \in G'$ such that $\mathrm{lm}(h) = m'$ is divisible by $\mathrm{lm}(g)$. Thus $\mathrm{rem}(h, G') = m' + \mathrm{rem}(h', G')$ and there is no generator $g \in G'$ such that $\mathrm{lm}((x_j - 1)h) = x_j m'$ is divisible by $\mathrm{lm}((x_j - 1)g)$. But $(x_j - 1)g \in G$ and thus $\mathrm{rem}((x_j - 1)h - m, G) = x_j m' + \mathrm{rem}((x_j - 1)h' - (m + m'), G)$. It follows that $\mathrm{rem}((x_j - 1)f, G) = x_j(m + m') + \mathrm{rem}((x_j - 1)h' - (m + m'), G)$. But there is no generator $g \in G'$ such that $\mathrm{lm}(g)$ divides m or m' and so there is no generator $g \in G$ with this property. It follows that $\mathrm{rem}((x_j - 1)f, G) = (x_j - 1)(m + m') + \mathrm{rem}((x_j - 1)h', G)$. On the other hand, $(x_j - 1)\mathrm{rem}(f, G') = (x_j - 1)(m + m') + (x_j - 1)\mathrm{rem}(h', G')$. Since $h' \prec f$, we obtain by induction, $(x_j - 1)\mathrm{rem}(h', G') = \mathrm{rem}((x_j - 1)h', G)$ and thus $\mathrm{rem}((x_j - 1)f, G) = (x_j - 1)(m + m') + \mathrm{rem}((x_j - 1)h', G)$, as required.

Second, assume that there is a generator $g \in G'$ such that $\mathrm{lm}(h) = m'$ is

divisible by $\mathrm{lm}(g)$. Then $\mathrm{rem}(f, G') = m + \mathrm{rem}(h, G') = m + \mathrm{rem}(h - g'g, G')$ for some $g' \in A$ and $\mathrm{lm}((x_j - 1)h) = x_j m'$ is divisible by $\mathrm{lm}((x_j - 1)g)$. But $(x_j - 1)g \in G$ and thus $\mathrm{rem}((x_j - 1)h, G) = \mathrm{rem}((x_j - 1)(h - g'g)), G) = (x_j - 1)\mathrm{rem}(h - g'g, G')$, where the last equation follows by induction, since $h - g'g \prec h$. Now $\mathrm{rem}((x_j - 1)f, G) = mx_j + \mathrm{rem}((x_j - 1)h - m, G) = mx_j + \mathrm{rem}((x_j - 1)(h - g'g) - m, G)$. But by hypothesis, there is no generator $g \in G'$ such that $\mathrm{lm}(g)$ divides m and so there is no generator $g \in G$ with this property. Thus the last term becomes $(x_j - 1)m + \mathrm{rem}((x_j - 1)(h - g'g), G)$. Since $h - g'g \prec h$, we obtain by induction the term $(x_j - 1)m + (x_j - 1)\mathrm{rem}((h - g'g), G')$, which equals $(x_j - 1)\mathrm{rem}(f, G')$, as claimed. □

Lemma 2. *Given any monomial ordering on A, let S be a non-empty subset of $\mathbb{N}_0^n \setminus \{\mathbf{0}\}$. For each polynomial $f \in I(S)$, $\mathrm{rem}(f, G') = 0$ implies $\mathrm{rem}(f, G) = 0$.*

Proof. Let $f \in I(S)$ such that $\mathrm{rem}(f, G') = 0$. First, suppose there is a generator $g' \in G'$ such that $\mathrm{lm}(f)$ is divisible by $\mathrm{lm}(g')$. Since $f \in I(S)$, we have that $\mathrm{lm}(f)$ is divisible by $\mathrm{lm}((x_j - 1)g')$ for some $1 \leq j \leq n$. But $g = (x_j - 1)g'$ lies in G and thus $\mathrm{rem}(f, G) = \mathrm{rem}(f - h'g, G) = \mathrm{rem}(f - [h'(x_j - 1)]g', G') = \mathrm{rem}(f, G)$ for some polynomial $h' \in A$.

Second, assume that there is no generator $g' \in G'$ such that $\mathrm{lm}(g')$ divides $\mathrm{lm}(f)$. Then there is no generator $g \in G$ such that $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$. Thus we obtain $\mathrm{rem}(f, G') = \mathrm{lt}(f) + \mathrm{rem}(f - \mathrm{lt}(f), G') = \mathrm{rem}(f, G)$.

Therefore, we can mimic the division of f with respect to G by the division of f with respect to G'. □

We are now ready to prove Theorem 1.

Proof. Let S be a non-empty subset of $\mathbb{N}_0^n$. Claim that G provides a generating set of the ideal $I = I(S)$. Indeed, let $\boldsymbol{a} \in S$. There is a minimal element $\boldsymbol{b} \in M$ such that $\boldsymbol{b} \leq \boldsymbol{a}$. Then $\boldsymbol{a} = \boldsymbol{b} + \boldsymbol{c}$ for some $\boldsymbol{c} \in \mathbb{N}_0^n$ and thus $\eta(\boldsymbol{a}) = \eta(\boldsymbol{b}) \cdot \eta(\boldsymbol{c})$. The claim follows.

Claim that the ideal I is finitely generated. Indeed, by Dickson's Lemma [9], there is a finite set of vectors $\boldsymbol{s}^{(1)}, \ldots, \boldsymbol{s}^{(r)} \in S$ such that

$$S \subseteq (\boldsymbol{s}^{(1)} + \mathbb{N}_0^n) \cup \ldots \cup (\boldsymbol{s}^{(r)} + \mathbb{N}_0^n).$$

For each element $\boldsymbol{s} \in \boldsymbol{s}^{(i)} + \mathbb{N}_0^n$, $1 \leq i \leq r$, there is some $\boldsymbol{t} \in \mathbb{N}_0^n$ such that $\boldsymbol{s} = \boldsymbol{s}^{(i)} + \boldsymbol{t}$. Thus $\boldsymbol{s}^{(i)} \leq \boldsymbol{s}$ and hence the set of minimal elements of S is contained in the set $\{\boldsymbol{s}^{(1)}, \ldots, \boldsymbol{s}^{(r)}\}$. The claim follows.

Claim that G is a Groebner basis for $I = I(S)$. We need to show that in view of Buchberger's S-criterion, $\mathrm{rem}(S(g, h), G) = 0$ for all polynomials

$g, h \in G$. First, take a non-empty subset $S \subseteq \mathbb{N}_0^n$ such that $\mathbf{0} \in S$. Then $I(S) = A$, $M(S) = \{\mathbf{0}\}$ and $G = \{1\}$ is a Groebner basis for A.

Second, let S be a non-empty subset of $\mathbb{N}_0^n \setminus \{\mathbf{0}\}$. Let $\boldsymbol{a}, \boldsymbol{b} \in M(S)$ such that the generators $\eta(\boldsymbol{a})$ and $\eta(\boldsymbol{b})$ have a common factor $x_j - 1$, $1 \leq j \leq n$. By considering the set S', there exist $\boldsymbol{a}', \boldsymbol{b}' \in M(S')$ such that $\eta(\boldsymbol{a}) = (x_j - 1)\eta(\boldsymbol{a}')$ and $\eta(\boldsymbol{b}) = (x_j - 1)\eta(\boldsymbol{b}')$. By induction, we may assume that G' is a Groebner basis for $I(S')$. We have $S(\eta(\boldsymbol{a}), \eta(\boldsymbol{b})) = (x_j - 1)S(\eta(\boldsymbol{a}'), \eta(\boldsymbol{b}'))$. Thus by Lemma 1, $\mathrm{rem}(S(\eta(\boldsymbol{a}), \eta(\boldsymbol{b})), G) = (x_j - 1)\mathrm{rem}(S(\eta(\boldsymbol{a}'), \eta(\boldsymbol{b}')), G')$. By induction, we have $\mathrm{rem}(S(\eta(\boldsymbol{a}'), \eta(\boldsymbol{b}')), G') = 0$ and hence the assertion follows.

Let $\boldsymbol{a}, \boldsymbol{b} \in M(S)$ such that the generators $\eta(\boldsymbol{a})$ and $\eta(\boldsymbol{b})$ have no common factor. Assume that $a_u > 0$, $a_{u+1} = \ldots = a_n = 0$, $b_1 = \ldots = b_{v-1} = 0$, and $b_v > 0$, where $1 \leq u < v \leq n$. By considering the set S', the elements $\boldsymbol{a}' = (a_1, \ldots, a_u - 1, 0, \ldots, 0)$ and $\boldsymbol{b}' = (0, \ldots, 0, b_v - 1, \ldots, b_n)$ belong to the set $M' = M(S')$ of minimal elements of S'. We have

$$S(\eta(\boldsymbol{a}), \eta(\boldsymbol{b})) = g_u g_v S(\eta(\boldsymbol{a}'), \eta(\boldsymbol{b}')) + \prod_{i=1}^{u} g_i^{a_i} \cdot \eta(\boldsymbol{b}') - \prod_{i=v}^{n} g_i^{b_i} \cdot \eta(\boldsymbol{a}').$$

This polynomial lies in $I(S)$. Moreover, by induction, the polynomial on the right hand side reduces to zero modulo G'. Thus, by Lemma 2, the polynomial reduces to zero modulo G. The claim follows.

Claim that the Groebner basis G for I is minimal. Indeed, the elements of G are monic. Moreover, let $\eta(\boldsymbol{a})$ and $\eta(\boldsymbol{b})$ be distinct elements of G. If the leading term $\boldsymbol{x}^a$ of $\eta(\boldsymbol{a})$ would be a divisor of the leading term $\boldsymbol{x}^b$ of $\eta(\boldsymbol{b})$, then $\boldsymbol{a} \leq \boldsymbol{b}$ contradicting that $\boldsymbol{a}$ and $\boldsymbol{b}$ lie in M and thus are $\leq$-incompatible. The claim is proved.

Claim that the minimal Groebner basis G for I is reduced. Indeed, let $\eta(\boldsymbol{a})$ and $\eta(\boldsymbol{b})$ be distinct elements of G. Each monomial in the support of $\eta(\boldsymbol{a})$ is of the form $\boldsymbol{x}^c$ such that $\boldsymbol{c} \leq \boldsymbol{a}$. If the leading term $\boldsymbol{x}^b$ of $\eta(b)$ would divide $\boldsymbol{x}^c$ then $\boldsymbol{b} \leq \boldsymbol{c}$. But then $\boldsymbol{b} \leq \boldsymbol{a}$ contradicting that $\boldsymbol{a}$ and $\boldsymbol{b}$ are $\leq$-incompatible. The claim follows. □

Example 1. Consider the subset $S = \{(a_1, a_2) \mid (a_1 + 1)(a_2 + 1) \geq 14\}$ of $\mathbb{N}_0^2$. The corresponding set of minimial elements amounts to $M = \{(0, 13), (1, 6), (2, 4), (3, 3), (4, 2), (6, 1), (13, 0)\}$ and thus the ideal $I(S)$ in $\mathbb{K}[x_1, x_2]$ has the reduced Groebner basis $\{\eta(a_1, a_2) \mid (a_1, a_2) \in M\}$.

The augmentation mapping $\phi : \mathbb{K}[x_1, \ldots, x_n] \to \mathbb{K}$ given by $\sum_a c_a \boldsymbol{x}^a \mapsto \sum_a c_a$ is a $\mathbb{K}$-algebra epimorphism, whose kernel $J = \ker \phi$ is generated as an

ideal by the set $G_1 = \{x_i - 1 \mid 1 \leq i \leq n\}$. Each power J^k, $k \geq 0$, of the augmentation ideal J is then generated by the set $G_k = \{\eta(\boldsymbol{a}) \mid \sum_{i=1}^{n} a_i \geq k\}$. By Theorem 1, the ideal J^k in A has the reduced Groebner basis

$$G_k = \left\{ \eta(\boldsymbol{a}) \mid \sum_{i=1}^{n} a_i = k \right\}. \tag{4}$$

The ideals J^k amount to generalized Reed-Muller codes when considered in the quotient ring of $\mathbb{F}_p[x_1, \ldots, x_n]$ of the form $\mathbb{F}_p[x_1, \ldots, x_n]/\langle x_i^p - 1 \mid 1 \leq i \leq n \rangle$ [6], [7]. One advantage of representing ideals as codes over linear codes is that their extra structure (given by their Groebner bases) allows a very compact representation of the encoding function [10]. We will report on the coding properties of the ideals discussed in this work in a forthcoming paper.

References

[1] W. Adams, P. Loustaunau, *An Introduction to Groebner Bases*, Graduate Studies in Mathematics, AMS, Providence, RI, **3** (1994).

[2] 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 Insbruck (1965), In German.

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

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

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

[6] S.D. Berman, On the theory of group codes, *Kibernetika*, **3** (1967), 31-39.

[7] P. Charpin, Une généralisation de la construction de Berman des codes de Reed et Muller p-aires, *Comm. Algebra*, **16** (1988), 2231-2246.

[8] S. Collart, M. Kalkbrenner, D. Mall, Converting bases with a Groebner walk, *J. Symbolic Computation*, **24** (1997), 465-469.

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

[12] V. Weispfenning, Constructing universal Groebner bases, LNCS, Springer, New York, **365** (1989), 408-417.

[13] W. Trinks, Über Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen, *J. Number Theory*, **10** (1978), 475-488.

[14] G. Zacharias, *Generalized Groebner Bases in Commutative Polynomial Rings*, Bachelor Thesis, MIT (1978).