




## Explicit Gröbner Basis of the Ideal of Vanishing Polynomials over $\mathbb{Z}_2 \times \mathbb{Z}_2$

### $\mathbb{Z}_2 \times \mathbb{Z}_2$ Üzerinde Sıfırlanan Polinomların İdealinin Açık Gröbner Tabanı

Abdullah Çağman 

Ağrı İbrahim Çeçen University Faculty of Science and Letters Department of Mathematics, Ağrı, Turkey

#### Abstract

Vanishing polynomials form an ideal of polynomial ring over the coefficient ring. In this paper, we give some vanishing polynomials of the polynomial ring  $\mathbb{Z}_m \times \mathbb{Z}_l[x_1, x_2, \dots, x_n]$  where  $(m, l) \neq 1$  and an explicit minimal strong Gröbner basis of the ideal of vanishing polynomials of the ring  $\mathbb{Z}_2 \times \mathbb{Z}_2[x]$ . Our proof is based fully on a combinatorial way.

**Keywords:** Gröbner basis, Polynomial ring, Vanishing Ideal, Vanishing polynomial

#### Öz

Sıfırlanan polinomlar, katsayı halkası üzerinde tanımlanan polinom halkalarının bir idealini oluştururlar. Bu makalede  $(m, l) \neq 1$  olmak üzere  $\mathbb{Z}_m \times \mathbb{Z}_l[x_1, x_2, \dots, x_n]$  polinom halkasının bazı sıfırlanan polinomlarını ve  $\mathbb{Z}_2 \times \mathbb{Z}_2[x]$  halkasının sıfırlanan polinomlarının idealinin açık minimal güçlü Gröbner tabanını vereceğiz. İspatımız tamamen kombinasyonel yöntemeye dayalı olacaktır.

**Anahtar Kelimeler:** Gröbner tabanı, Polinom halkası, Sıfırlanan ideal, Sıfırlanan polinom

### 1. Introduction

Although the notion of Gröbner basis firstly handled with the current name by Buchberger in his PhD thesis (Buchberger 1965), in 1927, Macaulay had been used this idea in his famous paper (Macaulay 1927).

When Buchberger was studying Gröbner basis for polynomial rings in his thesis at the same time Hironaka suggested the standart basis idea which is a remarkable method for solving the important problem of algebraic geometry “resolution of singularities of algebraic varieties” (Hironaka 1964). Though the statements Gröbner basis and standart basis are actually express the same things, Gröbner basis is come into prominence for the contribution to the computer algebra.

After the efforts of Buchberger and Hironaka in the 1960s, Gröbner basis did not see sufficiently interest about twenty years. But, in the middle of 1980s, the software Macaulay designed by David Bayer and Michael Stillman became a groundbreaking development for the Gröbner basis studies (Grayson and Stillman 2016). This computer algebra system

is still in progress and used in several works about the Gröbner basis.

The concept of Gröbner basis has been had many applications in different areas of mathematics. Solution of integer programming problem (Conti and Traverso 1991), graph theory (de Loera 1995), toric ideal theory serving as a bridge between the monomial ideal theory and the theory of triangulations of convex polytopes (Sturmfels 1996) and finding Markov basis in a statistical model (Aoki et al. 2010) are some examples of these applications.

In general, the interests of Gröbner basis are centered upon the field as a coefficient ring. The main reason for this is applications of Gröbner basis for arbitrary rings are very constraint. But, in recent years, several works with different coefficient rings have accelerated. For example, when proving correctness of data paths in system on chip design, usage of Gröbner basis in polynomial rings over has led to emergence of many works in this direction (Greuel et al. 2011), (Greuel et al. 2008), (Shekhar et al. 2005), (Wienand et al. 2008).

Let  $R$  be an arbitrary coefficient ring with finite elements. The polynomial  $p \in R[x_1, x_2, \dots, x_n]$  is called vanishing if the image of all elements of  $R^n$  is zero under this polynomial.

\*Corresponding Author: [acagman@agri.edu.tr](mailto:acagman@agri.edu.tr)

All vanishing polynomials form an ideal  $I$  which is called vanishing ideal. In this paper, our aim is to present an explicit Gröbner basis for the vanishing ideal  $I \subset \mathbb{Z}_2 \times \mathbb{Z}_2[x]$ .

This paper is organized as follows: Section 2 is devoted to some necessary notions about the polynomial rings and Gröbner basis. In the last section, we give some vanishing polynomials of the polynomial ring  $\mathbb{Z}_m \times \mathbb{Z}_l[x_1, x_2, \dots, x_n]$  where  $(m, l) \neq 1$  and the Gröbner basis of vanishing ideal  $I$  of polynomial ring with univariate over  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .

## 2. Materials and Methods

Let  $R$  be a commutative Noetherian ring with unity and  $R[x_1, x_2, \dots, x_n]$  a polynomial ring over  $R$  where  $n \geq 1$ . Let  $x^{\alpha_i} = x_1^{\alpha_{i1}} x_2^{\alpha_{i2}} \dots x_n^{\alpha_{in}}$  be a monomial,  $f = a_0 x^{\alpha_0} + a_1 x^{\alpha_1} + \dots + a_i x^{\alpha_i}$  a polynomial in  $R[x_1, x_2, \dots, x_n]$  where  $>$  being a monomial ordering,  $x^{\alpha_0} > x^{\alpha_1} > \dots > x^{\alpha_i}$ . We use the following notation:

- $Lt(f) = a_0 x^{\alpha_0}$  leading term of  $f$
- $Lp(f) = x^{\alpha_0}$  leading power product of  $f$
- $Lc(f) = a_0$  leading coefficient of  $f$
- $L(X) = \langle Lt(f) : f \in X \rangle$  leading term ideal of  $X$

**Definition 2.1.** Let  $R$  be a ring and  $I$  an ideal of polynomial ring  $R[x_1, x_2, \dots, x_n]$ .  $G = \{g_1, g_2, \dots, g_t\}$  consisting of nonzero polynomials is a Gröbner basis of  $I$  if  $G \subset I$  and  $L(G) = L(I)$ .

**Definition 2.2.** Let  $G = \{g_1, g_2, \dots, g_t\}$  be a Gröbner basis of an ideal  $I$ . If  $Lc(g_i) = 1$  for all  $i \in \{1, 2, \dots, t\}$  and  $Lp(g_i)$  does not divide  $Lp(g_j)$  for  $i \neq j$  then  $G$  is said to be a minimal Gröbner basis.

**Example 2.3.** Let  $f_1 = y + x, f_2 = x \in \mathbb{Q}[x, y]$ , and let us use the lex term order with  $y > x$ . Then  $\{f_1, f_2\}$  is a minimal Gröbner basis for the ideal  $I = \langle y^2 + yx + x^2, y + x, y \rangle$ .

**Definition 2.4.** Let  $G = \{g_1, g_2, \dots, g_t\}$  be a set consisting of nonzero polynomials in  $R[x_1, x_2, \dots, x_n]$ . If there is an  $i \in \{1, 2, \dots, t\}$  in which  $Lt(g_i)$  divides  $Lt(f)$  for all  $f \in I = \langle g_1, g_2, \dots, g_t \rangle$ , then  $G$  is said to be a strong Gröbner basis for  $I$ . Additionally, if  $Lt(g_i)$  does not divide  $Lt(g_j)$  for  $i \neq j$ , then  $G$  is said to be a minimal strong Gröbner basis.

## 3. Results

**Definition 3.1.** For  $f \in R[x_1, x_2, \dots, x_n]$ , let we define a new function  $f^*: R^n \rightarrow R$  in which  $f^*(a_1, a_2, \dots, a_n) = f(a_1, a_2, \dots, a_n)$ . If  $f$  is identically zero then  $f$  is called a vanishing polynomial. The set  $I = \{f \in R[x_1, x_2, \dots, x_n] : f \text{ is an ideal of } R[x_1, x_2, \dots, x_n]\}$  which is called vanishing ideal.

An explicit minimal strong Gröbner basis has been obtained for vanishing ideal of  $R[x_1, x_2, \dots, x_n]$  where  $R = \mathbb{Z}_m$  ( $m \geq 2$ ) in (Greuel et al. 2011). In this paper, we determine some vanishing polynomials in  $R[x_1, x_2, \dots, x_n]$  where  $R = \mathbb{Z}_m \times \mathbb{Z}_l$  ( $(m, l) \neq 1$ ) and give a minimal strong Gröbner basis for the vanishing ideal of  $\mathbb{Z}_2 \times \mathbb{Z}_2[x]$ .

**Lemma 3.2.** Consider the polynomial ring  $R[x_1, x_2, \dots, x_n]$  where  $R = \mathbb{Z}_m \times \mathbb{Z}_l$ . The polynomials,

$$p(k, t) = (m/2, l/2)x_1^{k_1}(x_1^{t_1} + 1) \dots x_n^{k_n}(x_n^{t_n} + 1) \text{ for } m \text{ and } l \text{ even}$$

$$p(k, t) = (0, l/2)x_1^{k_1}(x_1^{t_1} + 1) \dots x_n^{k_n}(x_n^{t_n} + 1) \text{ for } m \text{ odd and } l \text{ even}$$

$$p(k, t) = (m/2, 0)x_1^{k_1}(x_1^{t_1} + 1) \dots x_n^{k_n}(x_n^{t_n} + 1) \text{ for } m \text{ even and } l \text{ odd}$$

are vanishing polynomials.

**Proof.** Let we consider the case  $m$  and  $l$  are both even. We make our proof by induction on  $n$ .  $p(k, t) = (m/2, l/2)(x_1^{k_1}(x_1^{t_1} + 1))$  for  $n = 1$ . If we write any element of  $\mathbb{Z}_m \times \mathbb{Z}_l$ , say  $(a, b)$ , in the statement  $x_1^{k_1}(x_1^{t_1} + 1)$  then we come across the element  $(a^{k_1}(a^{t_1} + 1), b^{k_1}(b^{t_1} + 1))$ . If  $a$  is even then all of its powers are also even and so  $a^{k_1}(a^{t_1} + 1)$  is even, otherwise its powers are odd but  $a^{k_1}(a^{t_1} + 1)$  is still even. Likewise, due to the fact that  $b^{k_1}(b^{t_1} + 1)$  is even for all case, these statements are simplify with 2. Therefore, the value of  $(m/2, l/2)(x_1^{k_1}(x_1^{t_1} + 1))$  for the element  $(a, b)$  of  $\mathbb{Z}_m \times \mathbb{Z}_l$  is being zero. So, this indicates that  $p(k, t)$  is a vanishing polynomial.

Assume that the statement is true for  $n = d$ . That is,  $p(k, t) = (m/2, l/2)x_1^{k_1}(x_1^{t_1} + 1)x_2^{k_2}(x_2^{t_2} + 1) \dots x_d^{k_d}(x_d^{t_d} + 1)$  are vanishing polynomials. For  $n = d+1$ ,  $p(k, t) = (m/2, l/2)x_1^{k_1}(x_1^{t_1} + 1) \dots x_{d+1}^{k_{d+1}}(x_{d+1}^{t_{d+1}} + 1)$  and because of the value of  $(m/2, l/2)x_{d+1}^{k_{d+1}}(x_{d+1}^{t_{d+1}} + 1)$  is zero for all  $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_l$ ,  $p(k, t)$  is a vanishing polynomial for  $n = d+1$ . Thus,  $p(k, t)$  is a vanishing polynomial for the case  $m$  and  $l$  are both even.

The proof can be done in a similar way for the other cases.

**Theorem 3.3.** Let  $p(k, t)$  be a polynomial like in the Lemma 3.2 for polynomial ring  $\mathbb{Z}_2 \times \mathbb{Z}_2[x]$ . That is,  $p(k, t) = x^{k_1}(x^{t_1} + 1)$ . Then,  $G = \{x(x+1)\}$  is a minimal strong Gröbner basis for the vanishing ideal  $I$  of  $\mathbb{Z}_2 \times \mathbb{Z}_2[x]$ .

**Proof.** First of all, it is easily seen that there is no vanishing polynomial type  $ax+b$  in  $\mathbb{Z}_2 \times \mathbb{Z}_2[x]$ . Now we show that  $L(I) = L(G)$ . From the Lemma 3.2, one can see that  $G \subset I$  and so  $L(G) \subset L(I)$ . For the inverse inclusion let  $f \in L(I)$

be arbitrary. Then, there exist some  $n \geq 1$ ,  $t_i \in \mathbb{Z}_2 \times \mathbb{Z}_2[x]$  and  $f_i \in I(1 \leq i \leq n)$  such that

$$f = \sum_{i=1}^n t_i Lt(f_i).$$

If we assume that  $Lt(f_i) = a_i x^{k_i}$  then

$$f = \sum_{i=1}^n t_i Lt(f_i) = \sum_{i=1}^n t_i a_i x^{k_i} = \sum_{i=1}^n t_i a_i x^{k_i-2} x^2 = \sum_{i=1}^n t_i a_i x^{k_i-2} Lt(x(x+1)).$$

Thus,  $f \in L(G)$  and so  $L(I) \subset L(G)$  (note that  $k_i - 2$  is not negative since there is no vanishing polynomial degree one). This shows that  $L(I) = L(G)$ .

It is clear that  $G$  is a minimal strong Gröbner basis.

#### 4. Discussion

Since the division is troubled in rings except for fields, Gröbner basis works are progressing slowly in polynomial rings over any ring. In this paper, we give the Gröbner basis for the vanishing ideal over the coefficient ring  $\mathbb{Z}_2 \times \mathbb{Z}_2$ . The latter case is giving the Gröbner basis for the vanishing ideal of  $\mathbb{Z}_m \times \mathbb{Z}_l[x_1, x_2, \dots, x_n]$  where  $(m, l) \neq 1$ .

#### 5. References

- Aoki, S., Hibi, T., Ohsugi, H., Takemura, A. 2010.** Markov basis and Gröbner basis of Segre–Veronese configuration for testing independence in group-wise selections. *Ann. Inst. Stat. Math.*, 62: 299–321.
- Buchberger, B. 1965.** An algorithm for finding the bases elements of the residue class ring modulo a zero dimensional polynomial ideal, PhD thesis, Univ. of Innsbruck (Austria), 36 pp.
- Conti, P., Traverso, C. 1991.** Buchberger algorithm and integer programming, In: Mattson, H., Mora, T., Rao, T. [eds.], Applied Algebra Algebraic Algorithms and Error Correcting Codes. Lecture Notes in Computer Science, Springer, Berlin, vol. 539, pp. 130-139.
- De Loera, Jesús A. 1995.** Gröbner bases and graph colorings. *Beiträge Algebra Geom.*, 1995: 36 (1): 89-96.
- Grayson, DR., Stillman, ME. 01 August 2016.** Macaulay 2, a software system for research in algebraic geometry. <http://www.math.uiuc.edu/Macaulay2/>
- Greuel, GM., Seelisch, F., Wienand, O. 2011.** The Gröbner basis of the ideal of vanishing polynomials. *J. Symbolic Comput.*, 46: 561-570.
- Greuel, GM., Wedler, M., Wienand, O., Brickenstein, M., Dreyer, A. 2008.** New developments in the theory of Groebner bases and applications to formal verification. *J. Pure Appl. Algebra*, 213(8): 1612-1635.
- Hironaka, H. 1964.** Resolution of singularities of an algebraic variety over a field of characteristic zero. *Ann. Math.*, 79: 109–203.
- Macaulay, F.S. 1927.** Some properties of enumeration in the theory of modular systems. *Proc. London Math. Soc.*, 26: 531-555.
- Shekhar, N., Kalla, P., Enescu, F., Gopalakrishnan, S. 2005.** Equivalence verification of polynomial datapaths with fixed-size bitvectors using finite ring algebra. *In the proceedings of the 2005 IEEE/ACM International Conference on Computer Aided Design*, pp: 291–296.
- Sturmfels, B. 1996.** Gröbner Bases and Convex Polytopes, Amer. Math. Soc., Providence, 162 pp.
- Wienand, O., Wedler, M., Stoffel, D., Kunz, W., Greuel, GM. 2008.** An algebraic approach for proving data correctness in arithmetic data paths. *In the proceedings of the 20th International Conference on Computer Aided Verification*, pp: 473–486.