Groebner Bases and Its Applications

Rabia Deniz Genç, 18025053

Thesis Advisor: Assist. Prof. Dr. Eda YILDIZ

Department of Mathematics, Faculty of Arts and Sciences

Noetherian Ring

Definition. A commutative ring R is called *Noetherian* if each ideal in R is finitely generated.

Hilbert Basis Theorem. If R is a *Noetherian ring*, then so is $R[X]$.

Monomials

Definition.
A total order $>$ on the monomials of $R = k[x_1,...,x_n]$ is called a term order if
(a) $x^A > 1$, for every monomial $x^A \neq 1$ and
(b) If $x^A > x^B$, then for every monomial x^C, $x^{A+C} > x^{B+C}$.

There is only one term order on $k[x]$:
$x^d > x^{d-1} > x^{d-2} > ... > x > 1$

Definition. Let $f=\sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1,...,x_n]$ and let $>$ be a monomial order.
(i) The **multidegree** of f is multideg(f) = max$(\alpha\in\mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0)$ (the maximum is taken with respect to $>$).
(ii) The **leading coefficient** of f is LC(f)=$a_{multideg(f)}\in k$.
(iii) The **leading monomial** of f is LM$(f) = x^{multideg(f)}$ (with coefficient 1).
(iv) The **leading term** of f is LT(f) = LC$(f)\cdot$ LM(f).
(v) LCM$(x^\alpha, x^\beta) = x_1^{max(\alpha_1,\beta_1)} x_2^{max(\alpha_2,\beta_2)} x_3^{max(\alpha_3,\beta_3)} ... x_n^{max(\alpha_n,\beta_n)}$

Definition. An ideal $I\subset k[x_1,...,x_n]$ is said to be **monomial ideal** if there is a subset $A\subset \mathbb{Z}^n_{\geq 0}$ (possibly infinite) such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha\in A} h_\alpha x^\alpha$, where $h_\alpha\in k[x_1,\cdots,x_n]$. In this case, we write $I = \langle x^\alpha: \alpha\in A\rangle$.

Lemma. Let $I = \langle x^\alpha: \alpha\in A\rangle$ be a monomial ideal. Then a monomial x^β lies in I if and only x^β is divisible by x^α for some $\alpha\in A$.

Lemma. Let I be a monomial ideal, and let $f\in k[x_1,...,x_n]$. Then the following are equivalent:
i) $f\in I$.
ii) Every term of f lies in I.
iii) f is a k-linear combination of the monomials in I.

Corollary. Two monomial ideals are the same if and only if they contain the same monomials.

Dickson's Lemma. Let $I = \langle x^\alpha: \alpha\in A\rangle \subseteq k[x_1,\cdots,x_n]$ be a monomial ideal. Then I can be written in the form $I=\langle x^{\alpha(1)},\cdots,x^{\alpha(s)}\rangle$ where $\alpha(1),\cdots,\alpha(s)\in A$. In particular, I has a finite basis.

Definition. Let $I\subset k[x_1,...,x_n]$ be an ideal other than $\{0\}$.
i) We denote by LT(I) the set of leading terms of elements of I. Thus, LT$(I)=\{cx^\alpha$: there exists $f\in I$ with LT$(f) = cx^\alpha\}$.
ii) We denote by $\langle$LT$(I)\rangle$ the ideal generated by the elements of LT(I).

Proposition. Let $I\subset k[x_1,...,x_n]$ be an ideal.
i) $\langle$LT$(I)\rangle$ is a monomial ideal.
ii) There are $g_1,...,g_t\in I$ such that $\langle$LT$(I)\rangle = \langle$LT(g_1), ..., LT$(g_t)\rangle$.

Specific Orders

We use spesific orders while calculating Groebner Bases. It helps find the leading terms of polynomials for *S-polynomials*. The leading term depends on which specific order we choose.

The lexicographic order.
Let $\alpha = (\alpha_1,\alpha_2,...,\alpha_n)$ and $\beta = (\beta_1,\beta_2,...,\beta_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{lex} \beta$ if in the vector difference $\alpha-\beta \in \mathbb{Z}^n$, the leftmost nonzero entry is positive. We will write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.

The graded lexicographic order.
Let $\alpha = (\alpha_1,\alpha_2,...,\alpha_n)$ and $\beta = (\beta_1,\beta_2,...,\beta_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grlex} \beta$ if $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$ or $|\alpha| = |\beta|$ and $\alpha >_{lex} \beta$. We will write $x^\alpha >_{grlex} x^\beta$ if $\alpha >_{grlex} \beta$.

The graded reverse lexicographic order.
Let $\alpha = (\alpha_1,\alpha_2,...,\alpha_n)$ and $\beta = (\beta_1,\beta_2,...,\beta_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grevlex} \beta$ if
$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$ or $|\alpha| = |\beta|$ and the rightmost nonzero entry of $\alpha-\beta \in \mathbb{Z}^n$ is negative. We will write $x^\alpha >_{grevlex} x^\beta$ if $\alpha >_{grevlex} \beta$.

Example

1. Compare the vectors α_0= (2,1), α_1=(1,2), α_2=(1,0) and α_3=(0,3) in lexicographic order, graded lexicographic order and graded reverse lexicographic order.

First start by comparing vector α_0 with other vectors: $\alpha_0 >_{lex} \alpha_1$ since $\alpha_0-\alpha_1$= (1,−1), $\alpha_0 >_{lex} \alpha_2$ since $\alpha_0-\alpha_2$=(1,1), $\alpha_0 >_{lex} \alpha_3$ since $\alpha_0-\alpha_3$= (2,−2). If we compare vector α_1 with other vectors, we get the following results: $\alpha_1 >_{lex} \alpha_2$ since $\alpha_1-\alpha_2$= (0,2), $\alpha_1 >_{lex} \alpha_3$ since $\alpha_1-\alpha_3$= (1,−1). We continue with the vector α_2: $\alpha_2 >_{lex} \alpha_3$ since $\alpha_2-\alpha_3$= (1,−3).
Thus, we obtain the result $\alpha_0 >_{lex} \alpha_1 >_{lex} \alpha_2 >_{lex} \alpha_3$.

If we compare the vectors in graded lexicographic order, firstly we need to find $|\alpha_0|$, $|\alpha_1|$, $|\alpha_2|$, $|\alpha_3|$. If we calculate $|\alpha_i|$, we will reach these results: $|\alpha_0| = 3$, $|\alpha_1| = 3$, $|\alpha_2| = 1$, $|\alpha_3| = 3$. From here, it is observed that $\alpha_0 >_{grlex} \alpha_2$, $\alpha_1 >_{grlex} \alpha_2$, $\alpha_3 >_{grlex} \alpha_2$. Since both $|\alpha_0|$, $|\alpha_1|$ and $|\alpha_3|$ are equal to 3, we need to examine their lexicographic order. If we use the result above, we obtain $\alpha_0 >_{grlex} \alpha_1 >_{grlex} \alpha_3 >_{grlex} \alpha_2$.

If we compare the vectors in graded reverse lexicographic order, firstly we need to find $|\alpha_0|$, $|\alpha_1|$, $|\alpha_2|$, $|\alpha_3|$. If we utilize the above result, we get $\alpha_0 >_{grevlex} \alpha_2$, $\alpha_1 >_{grevlex} \alpha_2$, $\alpha_3 >_{grevlex} \alpha_2$. $|\alpha_0| = |\alpha_1|$ and $\alpha_0-\alpha_1 = (1,-1)$ since the rightmost non-zero entry of $\alpha_0-\alpha_1 \in \mathbb{Z}^n$ is negative, it implies that $\alpha_0 >_{grevlex} \alpha_1$. $|\alpha_0| = |\alpha_3|$ and $\alpha_0-\alpha_3 = (2,-2)$ since the rightmost non-zero entry of $\alpha_0-\alpha_3 \in \mathbb{Z}^n$ is negative, it implies that $\alpha_0 >_{grevlex} \alpha_3$. $|\alpha_1| = |\alpha_3|$ and $\alpha_1-\alpha_3 = (1,-1)$ since the rightmost non-zero entry of $\alpha_1-\alpha_3 \in \mathbb{Z}^n$ is negative, it implies that $\alpha_1 >_{grevlex} \alpha_3$. If we examine all these orderings, the result can be expressed graded reverse lexicographically as follows: $\alpha_0 >_{grevlex} \alpha_1 >_{grevlex} \alpha_3 >_{grevlex} \alpha_2$.

Example

2. In lexicographic order, graded lexicographic order and graded reverse lexicographic order, consider the polynomial $f = x^2y + xy^2 + x + y^3$ and $x>y$.

If we use the results from the above question, we obtain the following orderings:
$x^2y >_{lex} xy^2 >_{lex} x >_{lex} y^3$.
$x^2y >_{grlex} xy^2 >_{grlex} y^3 >_{grlex} x$.
$x^2y >_{grevlex} xy^2 >_{grevlex} y^3 >_{grevlex} x$.

S-Polynomials

Let f, g be monomials then

$$S(f,g) = \frac{LCM(LM(f),LM(g))}{LT(f)}.f - \frac{LCM(LM(f),LM(g))}{LT(g)}.g$$

Groebner Bases

Definition. Fix a monomial order. A finite subset $G=\{g_1,...,g_t\}$ of an ideal I is said to be a **Groebner basis** (or **standard basis**) if
$\langle$LT(g_1),...,LT$(g_t)\rangle=\langle$LT$(I)\rangle$.

Equivalently, but more informally, a set $\{g_1,..., g_t\}\subset I$ is a Groebner basis of I if and only if the leading term of any element of I is divisible by one of the LT(g_i)

Corollary. Fix a monomial order. Then every ideal $I\subset k[x_1,...,x_n]$ other than $\{0\}$ has a Groebner basis. Furthermore, any Groebner basis for an ideal I is a basis of I.

Proposition. Let $G=\{g_1,...,g_t\}$ be a Groebner basis for an ideal $I\subset k[x_1,...,x_n]$ and let $f\in k[x_1,...,x_n]$ Then there is a unique $r\in k[x_1,...,x_n]$ with the following two properties:
i) No term of r is divisible by any of LT(g_1),...,LT(g_t).
ii) There is $g\in I$ such that $f=g+r$.
In particular, r is the remainder on division of f by G no matter how the elements of G are listed when using the division algorithm.

Corollary. Let $G=\{g_t,...,g_t\}$ be a Groebner basis for an ideal $I\subset k[x_1,...,x_n]$ and let $f\in k[x_1,...,x_n]$. Then $f\in I$ if and only if the remainder on division of f by G is zero.

Definition. We will write $\overline{f}^F$ for the remainder on division of f by the ordered s-tuple $F=(f_1,...,f_s)$. If F is a Groebner basis for $(f_1,...,f_s)$ then we can regard F as a set (without any particular order) by **i)** No term of r is divisible by any of LT(g_1),...,LT(g_t) and **ii)** There is $g\in I$ such that $f=g+r$.

For instance, with $F = (x+y^3z,\ x^2y^2-z^2)\subset k[x,y,z]$, using the lexicographic order, we have
$\overline{x^3}^F = yz^3$
since the division algorithm yields $x^3 = x^2(x+y^3z) - yz(x^2y^2+z^2)+yz^3$.

Buchberger's Criterion

Let $I\subset K[X_1, \ldots, X_t]$ be a polynomial ideal with basis $G = \{g_1,...,g_t\}$. G is a Groebner basis for I if and only if for all pairs g_i and g_j for $i\neq j$ the remainder of the division of S(g_i,g_j) by G (listed in some order) equals zero.

Buchberger's Algorithm

Let $I=\langle f_1,...,f_s\rangle\neq\{0\}$ be a polynomial ideal. Then a Groebner basis for I can be constructed in a finite number of steps by the following algorithm:
Input: $F=(f_1,...,f_s)$
Output: a Groebner basis $G=(g_1,...,g_t)$ for I, with $F\subset G$
$G:=F$
REPEAT
  $G':=G$
  FOR each pair $\{p,q\}$. $p\neq q$ in G' DO
    $S:=\overline{S(p,q)}^{G'}$
    IF $S\neq 0$ THEN $G:=G\cup\{S\}$
UNTIL $G=G'$

Example

Consider the ring $k[x,y,z]$ with grlex order and $I=\langle f_1,f_2\rangle=\langle xz-y^2, x^3-z^2\rangle$. To determine whether I is a Groebner basis, we check $S(f_1,f_2)$.

To determine whether I is a Groebner basis, we check $S(f_1,f_2)$.
$S(f_1,f_2)=\frac{x^3z}{xz}f_1-\frac{x^3z}{x^3}f_2 = -x^2y^2+z^3$. $F=(f_1,f_2)$ is not a Groebner basis because $\overline{S(f_1,f_2)}^F = -x^2y^2+z^3$.
In order to obtain a Groebner basis, we should include that remainder in our generating set. As a result, F became (f_1,f_2,f_3) and since $S(f_1,f_2)=f_3$, $\overline{S(f_1,f_2)}^F=0$.
Thus, if $S(f_1,f_3)$ and $S(f_2,f_3)$ are equal to zero, F will indeed form a Groebner basis. Accordingly, let us compute $S(f_1,f_3)$ now.
$S(f_1,f_3)=\frac{x^2y^2z}{xz}f_1-\frac{x^2y^2z}{-x^2y}f_3 = -xy^4+z^4$, So, it follows that $\overline{S(f_1,f_3)}^F = -xy^4+z^4$. We must add $f_4=-xy^4+z^4$ to our generating set. If we let $F=(f_1,f_2,f_3,f_4)$ then we have $\overline{S(f_1,f_3)}^F=0$.
For all $1\leq i,j\leq 4$, $\overline{S(f_i,f_j)}^F$ should be equal to zero. Let us verify these.
$S(f_2,f_3)=\frac{x^3y^2}{x^3}f_2-\frac{x^3y^2}{-x^2y^2}f_3= xz^3-y^2z^2= y^2f_2+xf_3$, hence $\overline{S(f_2,f_3)}^F=0$.
$S(f_2,f_4)=\frac{x^3y^4}{x^3}f_2-\frac{x^3y^4}{-xy^4}f_4= x^2z^4-y^4z^2= y^4f_2-x^2f_4$. So $\overline{S(f_2,f_4)}^F=0$.
$S(f_1,f_4)=\frac{xy^4z}{xz}f_1-\frac{xy^4z}{-xy^4}f_4 =-y^6+z^5=f_5$. We must add $f_5=-y^6+z^5$ to our generating set. If we let $F=(f_1,f_2,f_3,f_4,f_5)$ then we have So $\overline{S(f_1,f_4)}^F=0$. For all $1\leq i,j\leq 5$, $\overline{S(f_i,f_j)}^F$ should be equal to zero. Let us verify these.
$S(f_2,f_5)=\frac{x^3y^6}{x^3}f_2-\frac{x^3y^6}{-y^6}f_5 = x^3z^5-y^6z^2= z^2f_5+z^5f_2$. So $\overline{S(f_2,f_5)}^F=0$.
$S(f_3,f_4)=\frac{x^2x^4}{-x^2y^2}f_3-\frac{x^2x^4}{-xy^4}f_4 = xz^4-y^2z^3= z^3f_1$. So $\overline{S(f_3,f_4)}^F=0$.
$S(f_3,f_5)=\frac{x^2y^6}{-x^2y^2}f_3-\frac{x^2y^6}{-y^6}f_5 = x^2z^5-y^4z^3= -x^2f_5-y^4f_3$. So $\overline{S(f_3,f_5)}^F=0$.
$S(f_1,f_5)=\frac{xy^6z}{xz}f_3-\frac{xy^6z}{-y^6}f_5 = -y^8+xz^6= z^5f_1+y^2f_5$. So $\overline{S(f_4,f_5)}^F=0$.
$S(f_4,f_5)=\frac{xy^6}{-xy^4}f_4-\frac{xy^6}{-y^6}f_5 = xz^5-y^2z^4= xf_5-y^2f_4$. So $\overline{S(f_4,f_5)}^F=0$.
$\overline{S(f_i,f_j)}^F=0$ for all $1\leq i,j\leq 5$, by Buchberger's Criterion it follows that a grlex Groebner basis I is given by $\{f_1,f_2,f_3,f_4,f_5\} = \{xz-y^2, x^3-z^2, -x^2y^2+z^3, -xy^4+z^4, -y^6+z^5\}$.

Minimal Groebner Bases

A minimal Groebner basis for a polynomial ideal I is a Groebner basis G for I such that:
i) LC(p)=1 for all $p\in G$,
ii) For all $p\in G$, LT$(p)\notin\langle$LT$(G-\{p\})\rangle$.

Reduced Groebner Bases

A reduced Groebner basis for a polynomial ideal I is a Groebner basis G for I such that:
i) LC(p)=1 for all $p\in G$,
ii) For all $p\in G$, no monomial of p lies in $\langle$LT$(G-\{p\})\rangle$.

Some Applications of Groebner Bases

Groebner bases, which is crucial in algebraic geometry, have applications in various fields, including computer-aided design, robotics, and cryptography. Used in Computer Algebra Systems, they enable symbolic computation. In coding theory, Groebner bases aid in constructing error-correcting codes. Their role extends to algebraic cryptanalysis, robotics problem-solving, invariant theory in physics and chemistry, and modeling biochemical reaction networks in biology. The historical evolution of Gröbner bases emphasizes their versatility in various applications across computer science, cryptography, engineering, and the sciences, highlighting their ongoing significance in contemporary research and the solution of practical problems. We can examine some applications of the Groebner bases in more detail in the following part.

The Ideal Membership Problem

If we combine Groebner bases with the division algorithm, we get the following ideal membership algorithm: given an ideal $I =\langle f_i,..., f_s\rangle$, we can decide whether a given polynomial f lies in I as follows. First, using an algorithm similar to Buchberger's Algorithm, find a Groebner basis $G=\{g_1,...,g_t\}$ for I. Then we get $f\in I$ if and only if $\overline{f}^G=0$.

Example. Let $I=\langle f_1,f_2\rangle=\langle x^2y^2+xz^3, yz^2\rangle\in\mathbb{C}[x,y,z]$ and use the grlex order. Let $f=xy^3z^5+y^3z^2+x^2y^2+xz^3$. We want to know if $f\in I$.
The generating set given is not a Groebner basis of I because LT(I) also contains polynomials such as LT$(S(f_1,f_2))$=LT$(xz^5)=xz^5$ that are not in the ideal $\langle$LT(f_1),LT$(f_2)\rangle=\langle x^2y^2, yz^2\rangle$. Therefore, when we start computing a Groebner basis for I, we obtain the following result:
$G=\{f_1,f_2,f_3\}=\{yz^2,\ xz^5,\ x^2y^2+xz^3\}$.
We may now test polynomials for membership in I. For example, dividing f above by G, we find $f=y^2f_1+y^3f_2+f_3$. Since the remainder is zero, we have $f\in I$.
For another example, consider $f=x^2+yz+1$. Even without completely computing the remainder on division by G, we can see from the form of the elements in G that $f\notin I$. The reason is that LT$(f)= x^2$ is clearly not in the ideal $\langle$LT(G)$\rangle=\langle yz^2,\ xz^5, x^2y^2\rangle$. Hence, $\overline{f}^G\neq 0$, so that $f\notin I$.
This last observation illustrates the way the properties of an ideal are revealed by the form of the elements of a Groebner basis.

The Problem of Solving Polynomial Equations

We will explore the application of the Groebner basis technique in solving systems of polynomial equations involving several variables.

Example. Consider the equations
$x^2+y^2+z^2=1$,
$z^2=y$,
$x=y$ in $\mathbb{C}^3$.
These equations define the ideal $I=\langle x^2+y^2+z^2-1, z^2-y, x-y\rangle\subset\mathbb{C}[x,y,z]$ and our goal is to determine all points in $\mathbf{V}(I)$. We can calculate $\mathbf{V}(I)$ using any basis of I. So let us see what happens when we use a Groebner Basis. We will compute a Groebner basis on I with respect to the grlex order. The basis is $G=\{g_1,g_2,g_3\}=\{\ 2z^4+z^2-1,\ y-z^2,\ x-z^2\}$. First, the polynomial g_1 depends only on z, hence, we get the result $z = \frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, i, -i$. Next, when these value of z is substituted into the equations g_2=0 ,g_3=0, we get $(\frac{1}{2},\ \frac{1}{2},\ \frac{-1}{\sqrt{2}})$, $(\frac{1}{2},\ \frac{1}{2},\ \frac{1}{\sqrt{2}})$, $(-1,\ -1,\ -i)$, $(-1,\ -1,\ i)$. Since $\mathbf{V}(I) = \mathbf{V}(g_1,g_2,g_3)$, we have found all solutions of the original equations.

Groebner Bases in Cryptography

Groebner bases have applications in cryptography, particularly in the field of algebraic cryptanalysis. One notable example is in the analysis of algebraic equations arising from certain cryptosystems. Consider a cryptographic system based on polynomial equations, such as a multivariate polynomial public-key cryptosystem.
For instance, consider a multivariate polynomial system used in a cryptosystem:

$$\begin{aligned} f_1(x_1,x_2,\cdots,x_n) &= 0\\ f_2(x_1,\ x_2,\cdots,x_n) &= 0\\ &\vdots\\ f_m(x_1,\ x_2,\cdots,\ x_n) &= 0 \end{aligned}$$

The provided equations likely characterize a process related to either encrypting information or generating cryptographic keys. In this system, x_1, ..., x_n represent the information we aim to retain, and we safeguard this information through the equation system f_i. The easier it is to solve for x_i's from the equation system, the more susceptible our information becomes to compromise, which is an undesirable outcome. Our desired scenario involves the equations being difficult to solve, ensuring the security of our private keys. In the encryption process, it is essential for the encryption stage to be efficient to ensure a fast algorithm. To achieve this, we utilize Groebner bases, as it expedites intermediate calculations in the process. Groebner bases serve as a mathematical tool to streamline and simplify the system of equations, thereby facilitating a clearer comprehension of their algebraic structure.

Groebner Bases in Coding Theory

Groebner bases have applications in Coding Theory, particularly in the study of error-correcting codes. One example is the use of Groebner bases to analyze and construct algebraic geometric codes.
Algebraic geometric codes are a class of error-correcting codes derived from algebraic varieties. Groebner bases play a crucial role in finding suitable generators for these codes.
Consider an example where you want to construct an algebraic geometric code for a specific algebraic variety defined by polynomial equations. The Groebner basis of these polynomials can be computed to obtain a set of polynomials that generate the same ideal. These polynomials can then be used as the basis for an algebraic geometric code.
For instance, suppose you have an algebraic variety defined by the polynomials:

$$\begin{aligned} f_1(x,y,z) &= x^2+y^2+z^2-1\\ f_2(x,y,z) &= x+y+z-2 \end{aligned}$$

The Groebner basis with respect to a certain monomial ordering might be:

$$\begin{aligned} g_1(x,y,z) &= x+y+z-2\\ g_2(x,y,z) &= z^2-2z+1 \end{aligned}$$

These polynomials can be used as generators for an algebraic geometric code associated with the algebraic variety defined by f_1 and f_2. The advantage of using g_1 and g_2 polynomials instead of f_1 and f_2 polynomials lies in the properties and simplifications provided by the Groebner basis. The Groebner bases, represented by g_1 and g_2, is often more simplified compared to the original set of polynomials f_1 and f_2. This simplification makes it easier to work with and analyze the algebraic structure of the code. In coding theory, these algebraic geometric codes have applications in providing efficient ways to detect and correct errors in data transmission or storage, making them an essential tool in modern communication systems.

References

[1] Bayer, D. A. (1982). The division algorithm and the Hilbert scheme. Harvard University.

[2] Boege, W., Gebauer, R., & Kredel, H. (1986). Some examples for solving systems of algebraic equations by calculating Groebner bases. Journal of Symbolic Computation, 2(1), 83-98.

[3] Cox, D., Little, J., & OShea, D. (2013). Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra. Springer Science & Business Media.

[4] Eisenbud, D. (2013). Commutative algebra: with a view toward algebraic geometry (Vol. 150). Springer Science & Business Media.

[5] Gianni, P., & Mora, T. (1987, June). Algebrric solution of systems of polynomirl equations using Groebher bases. In International Conference on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes (pp. 247-257). Berlin, Heidelberg: Springer Berlin Heidelberg.

[6] Hungerford, T. W. (2012). Algebra (Vol. 73). Springer Science & Business Media.

[7] Malik, D. S., Mordeson, J. N., &Sen, M. K. (1997). Fundamentals of abstract algebra. McGraw-Hill.

[8] Saleemi, M. (2012). Coding theory via Groebner bases (Doctoral dissertation, Technische Universität Hamburg).

[9] Sharp, R. Y. (2000). Steps in commutative algebra (No. 51). Cambridge university press.

[10] Van Der Waerden, B. L. (1975). On the sources of my book Moderne Algebra. Historia mathematica, 2(1), 31-40.

[11] Yang, K., Zhang, Q., Yuan, R., Yu, W., Yuan, J., & Wang, J. (2015). Selective harmonic elimination with Groebner bases and symmetric polynomials. IEEE transactions on Power Electronics, 31(4), 2742-2752.