Communications to SIMAI Congress,
ISSN 1827-9015, Vol. 1 (2006)

DOI: 10.1685/CSC06038

LINEAR ALGEBRA AND CIRCUITS

Gaetana Restuccia
Department of Mathematics, University of Messina
C.da Papardo, salita Sperone, 31, 98166 Messina, Italy
grest@dipmat.unime.it

Vito Carfì
Department of Mathematics,University of Messina
C.da Papardo, salita Sperone, 31, 98166 Messina, Italy
vicarfi@tin.it

We give an introduction to the kinds of problems we will be interested in throughout this work. A familiar special case in the theory of systems of linear equations is the row reduction of matrices of the systems.
Let k be any field (e.g. the rational number $\mathbb{Q}$, the real number $\mathbb{R}$, the complex number $\mathbb{C}$). We consider polynomials $f(X_1, \ldots, X_n)$ in n variables with coefficients in k. Such polynomials are finite sums of terms of the type $aX_1^{\alpha_1} \cdots X_n^{\alpha_n}$, where $a \in k$ and $\beta_i \in \mathbb{N}$, $i = 1, \ldots, n$. We call $X_1^{\alpha_1} \cdots X_n^{\beta_n}$ a power product. Let $k[X_1, \ldots, X_n]$ be the set of all polynomials in n variables with coefficients in the field k. $k[X_1, \ldots, X_n]$ is a commutative ring with respect to the usual operations of addition and multiplication of polynomials. Moreover $k[X_1, \ldots, X_n]$ is a k-vector space with basis the set $\prod$ of all power products $\prod = \{X_1^{\alpha_1} \cdots X_n^{\alpha_n}, \alpha_i \in \mathbb{N}, i = 1, \ldots, n\}$.
Consider the system $f_1 = 0, \ldots, f_m = 0$ (1), where each f_i is a linear polynomial. In this case the algorithmic method to resolve (1) is the well-known row reduction which changes the system (1) to row echelon form.

Example 0.1. *Let $f_1 = X_1 - 2X_2 + X_3$ and $f_2 = 2X_1 - X_2 + 2X_3$ be linear polynomials in $k[X_1, X_2, X_3]$. We consider the ideal $I = (f_1, f_2)$ and the algebraic variety $V(I) \in k^3$, that is, the set of solutions of the system*

$$\begin{cases} X_1 - 2X_2 + X_3 = 0 \\ 2X_1 - X_2 + 3X_3 = 0 \end{cases} \qquad (*)$$

We apply row reduction on the matrix associated with the system

$$\begin{pmatrix} 1 & -2 & 1 \\ 2 & -1 & 3 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & -2 & 1 \\ 0 & 3 & 1 \end{pmatrix}$$

Licensed under the Creative Commons Attribution Noncommercial No Derivatives

The last matrix is in row echelon form. The solutions of the system (*) are the same as those of the system

$$\begin{cases} X_1 - 2X_2 + X_3 = 0 \\ 3X_2 + X_3 = 0 \end{cases}.$$

but, in this case, they can be easily obtained parametrically as:

$$X_1 = -\frac{5}{3}X_3, \quad X_2 = -\frac{1}{3}X_3.$$

The row reduction process is, in fact, a method to change a generating set for the ideal $I = (f_1, f_2)$ into another generating set.
The general ingredients that we extract from the examples can be used for the general situation of non-linear polynomials.
The notion of circuit plays a crucial rule in the above process. This notion comes from matroid theory, but it is very important in the research of an universal Gröbner basis for the ideal I, the vanishing ideal of $k[X_1, \ldots, X_n]$ of a $(n-m)$- dimensional vector subspace of k^n.
We give some definitions:
Let V be an $(n-m)$- dimensional vector subspace of k^n and let I be its vanishing ideal in the ring $k[X_1, \ldots, X_n]$, generated by m linear forms $f_1, \ldots, f_m$, $f_i = \sum_{j=1}^{n} a_{ij}X_j$, $i = 1, \ldots, m$.

Definition 0.2. *Let $f \in I$ be a non-zero linear form.$f = \sum_{i=1}^{n} a_i X_i$ is a circuit if $supp(f) = \{i : a_i \neq 0\}$ is minimal with respect to inclusion.*

There are at most $\binom{n}{m-1}$ circuits, since if I is generated by linear forms, the Buchberger algorithm is equivalent to Gaussian elimination on the coefficients matrix.

Proposition 0.3. *Let I be the vanishing ideal in $k[X_1, \ldots, X_n]$ of a $(n-m)$- dimensional vector space. Then every reduced Groöbner basis consists of m circuits.*

Theorem 0.4. [1], *chap.*2
Let I be an ideal of $k[X_1, \ldots, X_n]$ generated by linear forms. The set of circuits in I is a minimal universal Gröbner basis for I.

1 Linear forms with coefficients in a ring

Now consider any commutative, noetherian, ring R with unit element.
Consider the ring $S = R[Y_1, \ldots, Y_n]$, where $Y_1, \ldots, Y_n$ are indeterminates on R and m elements $f_1, \ldots, f_m \in S$ that are linear in the $Y_i's$ variables.
$f_i = \sum_{j=1}^{n} a_{ij}Y_j$, $i = 1, \ldots, m$, $a_{ij} \in R$.
Let $J = (f_1, \ldots, f_m)$ be the vanishing ideal of these forms in S. The ideal J is known and it appears as the presentation ideal of the symmetric algebra $Sym_R(M)$ of a module M that is the cokernel of the map $0 \to R^m \xrightarrow{f} R^n$, where f is represented by the matrix (a_{ij}). (In fact, we can obtain the ideal J, as a presentation ideal of the

symmetric algebra of a vector space.)
However the linear forms have coefficients in the ring R, not in the field k(linear algebra).
The aim of our research is to give:

1. A definition of circuit in this context.

2. If $R = k[X_1, \ldots, X_s]$, to prove that if J is an ideal generated by linear forms of $R[Y_1, \ldots, Y_n]$ that are circuits, then this set is a minimal universal Gröbner basis of J.

Consider the presentation of $Sym_R(M)$

$$Sym_R(M) = R[Y_1, \ldots, Y_n]/J.$$

Let $<$ be a monomial order on the monomials of $R[Y_1, \ldots, Y_n]$ in the variables Y_i such that

$$Y_1 < Y_2 < \cdots < Y_n.$$

We call $<$ an admissible order.
With respect to this term order, if $f = \sum a_\alpha \underline{Y}^\alpha$, $\underline{Y}^\alpha = Y_1^{\alpha_1} \cdots Y_n^{\alpha_n}$, $\underline{\alpha} \in \mathbb{N}^n$, we put $\text{in}_< f = a_\alpha \underline{Y}^\alpha$, where $\underline{Y}^\alpha$ is the largest monomial in f such that $a_\alpha \neq 0$.
If we assign degree 1 to each variable Y_i and degree 0 to the elements of R, we have the following facts:

1) J is a graded ideal

2) The natural epimorphism $S \to Sym_R(M)$ is a graded homomorphism of graded algebras on R, S is a graded ring and $Sym_R(M)$ is a graded algebra.

Definition 1.1. *The ideal $(f_1, \ldots, f_n)$ is generated by circuits if*

$$in_< J = (I_1 Y_1, I_2 Y_2, \ldots, I_n Y_n),$$

where $I_1, \ldots I_n$ are ideals generated by elements of R.

If $R = k[X_1, \ldots, X_s]$ we can use the Gröbner bases theory and Buchberger's algorithm to compute $\text{in}_< J$.
$Sym_R(M) = k[X_1, \ldots, X_s, Y_1, \ldots, Y_n]/J$. We can introduce a term order on $S = k[X_1, \ldots, X_s, Y_1, \ldots, Y_n]$, such that $Y_1 < Y_2 < \cdots < Y_n$ and $X_i < Y_i$ for any i.
For example $X_1 < X_2 < \cdots < X_s < Y_1 < Y_2 < \cdots < Y_n$ is such a term order.
If G is a Gröbner basis for $J \subset k[X_1, \ldots, X_s, Y_1, \ldots, Y_n]$, we have $\text{in}_< J = (\text{in}_< G) = (\text{in}_< f, f \in J)$ and if the elements of G are linear in the $Y_i s$, it follows that $f_1, \ldots, f_n$ is generated by circuits.

Example 1.2. *For $s = n$, let J be the ideal of S generated by the 2-minors of the matrix*

$$\begin{pmatrix} X_1 & X_2 & \cdots & X_n \\ Y_1 & Y_2 & \cdots & Y_n \end{pmatrix}$$

Then $in_< J = (I_1 Y_1, \ldots, I_n Y_n) = ((X_1)Y_2, (X_1, X_2)Y_3, \ldots, (X_1, X_2, \ldots X_{n-1})Y_n)$ and J is generated by circuits. The set $G = \{X_1 Y_2 - X_2 Y_1, X_1 Y_3 - X_3 Y_1, \ldots, X_{n-1} Y_n - X_n Y_{n-1}\}$ is a minimal universal Groebner basis for J.

Remark 1.3. *If $R = k[X_1, \ldots, X_s]$, from the theory of Gröbner basis, if $f_1, \ldots, f_n$ is generated by circuits with respect to any admissible term order $<$, then $f_1, \ldots, f_n$ is generated by circuits for another admissible term order, too.*

Project: To give criteria to study systems of equations of S, linear in the variables Y_i.

REFERENCES

1. G. Restuccia, Symmetric Algebras of finitely generated graded modules and s-sequences, *Rendiconti del Politecnico di Torino*, (2005)(to appear)

2. B. Sturmfels, Groebner bases and convex polytopes, *Amer. Math. Soc.*, (1996)

3. D. Eisenbud, Commutative Algebra with a vieux toward algebraic geometry *Springer- Verlag*, (1994)