Computer Science Journal of Moldova, vol.**20**, no.3(60), 2012

Gröbner Basis Approach to Some Combinatorial Problems

Victor Ufnarovski

Abstract

We consider several simple combinatorial problems and discuss different ways to express them using polynomial equations and try to describe the Gröbner basis of the corresponding ideals. The main instruments are complete symmetric polynomials that help to express different conditions in rather compact way.

Keywords: Gröbner basis, zero-dimensional ideal, finite configuration, complete symmetric polynomials.

1 Introduction

As far as it was found that Gröbner basis is a nice instrument to solve polynomial systems of equations, there appear many ideas how to translate problems that do not look as suitable object for the Gröbner basis approach to non-trivial system of equations. A classical example is graph coloring (see [1], where many other interesting problems can be found). In this article we want to consider some elementary instruments that can be applied for easy combinatorial problems. The main of them is the complete symmetric polynomial.

2 How to describe a finite set?

Let us try Gröbner basis approach to some combinatorial problems in order to understand when such approach can be useful.

We start from a magic square of size m. It can be described as $m \times m$ matrix, elements of which are different integers between 1 and m^2 and

©2012 by V. Ufnarovski

such that the sums in every row, column and two main diagonals are the same. The sum conditions are nothing else than linear equations, thus the only difficulty is to express the conditions that all elements belong to the given finite set A and are different. Let us try to express this condition in equations as well.

If $A = \{a_1, a_2, \ldots, a_n\}$ is an arbitrary finite set of different numbers, then the condition $x \in A$ is trivially expressed as the equation $p_A(x) = 0$, where

$$p_A(x) = (x - a_1)(x - a_2) \cdots (x - a_n) = x^n + A_1 x^{n-1} + ... + A_n.$$

Note that the coefficients A_k are (up to sign $(-1)^k$) elementary symmetric polynomials in $a_1, \ldots, a_n$.

If y is another element from A then, of course, $p(y) = 0$, but to express the condition $y \neq x$ we need the equation $p_2(x, y) = 0$, where

$$p_2(x, y) = \frac{p(x) - p(y)}{x - y}.$$

This already allows us to write all necessary equations for the magic square, but we prefer a shorter way to express that $\{x_1, \ldots, x_n\}$ is the set A.

Theorem 1. *The conditions*

$$\sum x_i^k = \sum a_i^k, k = 1, \ldots n.$$

are equivalent to condition that all x_i are different and belong to A.

Proof. Obviously we have the similar equality for the elementary symmetric polynomials and therefore x_i are all different solutions of the equation $p_A(x) = 0$. ■

For example, it is easy now to find all magic squares of size 3 :

x_1	x_2	x_3
x_4	x_5	x_6
x_7	x_8	x_9

Simply write

$$x_1 + \cdots + x_9 = 1 + 2 + \cdots + 9,$$
$$x_1^2 + \cdots + x_9^2 = 1^2 + 2^2 + \cdots + 9^2,$$
$$\cdots$$
$$x_1^9 + \cdots + x_9^9 = 1^9 + 2^9 + \cdots + 9^9,$$

add all sum equations

$$x_1 + x_2 + x_3 = x_4 + x_5 + x_6 = x_7 + x_8 + x_9 = x_1 + x_4 + x_7 =$$

$$x_2 + x_5 + x_8 = x_3 + x_6 + x_9 = x_1 + x_5 + x_9 = x_3 + x_5 + x_7$$

and start Gröbner basis calculations! Here is the result.

$$[{x_9}^4 - 20\,{x_9}^3 + 140\,{x_9}^2 - 400\,x_9 + 384,$$
$${x_8}^2 + 2\,x_8x_9 + 2\,{x_9}^2 - 20\,x_8 - 30\,x_9 + 115,$$
$$x_7 + x_8 + x_9 - 15, x_6 + x_8 + 2\,x_9 - 20, x_5 - 5, x_4 - x_8 - 2\,x_9 + 10,$$
$$x_3 - x_8 - x_9 + 5, x_2 + x_8 - 10, x_1 + x_9 - 10].$$

We see that we have four choices for x_9 and two for x_8 – the rest is determined uniquely. Note that $x_5 = 5$ in any magic square.

When returning to general case note that in fact some a_i could be equal – the equations still describe the set A but in this case with the multiplicities.

The next step is to obtain the Gröbner basis for the ideal I, generated by the polynomials $\sum_i x_i^k - \sum_i a_i^k$. It is not an easy task for computer for large n, thus the following result can replace the calculations.

Let $h_i(x_1, \ldots, x_k) = \sum_{|\alpha_1 + \cdots \alpha_k| = i} x_1^{\alpha_1} \cdots x_k^{\alpha_k}$ be complete symmetric functions in k variables. We put additionally $A_0 = h_0 = 1$.

Theorem 2. *The set*

$$g_k(x_1, \ldots, x_k) = \sum_{i=0}^{n-k+1} A_i h_{n+1-k-i}(x_1, \ldots, x_k)$$

for $k = 1, \ldots, n$ describes the reduced Gröbner basis of the ideal I in the lexicographical ordering $x_n > x_{n-1} > \cdots > x_1$.

Proof. First we need to show that $g_k = 0$ is valid in $K[x_1, \ldots, x_n]/I$. As usual, the easiest way to prove is to use the generating function. If we rewrite the evident equality

$$(1-tx_1)\cdots(1-tx_n) = (1-ta_1)\cdots(1-ta_n) = 1+A_1t+A_2t^2+\cdots+A_nt^n$$

as

$$(1+h_1(x_1,\ldots,x_k)t+h_2(x_1,\ldots,x_k)t^2+\cdots)(1+A_1t+A_2t^2+\cdots+A_nt^n) =$$

$$\frac{1}{(1-tx_1)\cdots(1-tx_k)}(1+A_1t+A_2t^2\cdots+A_nt^n) = (1-tx_{k+1})\cdots(1-tx_n)$$

then the coefficient with t^{n+1-k} is $g_k(x_1, \ldots, x_k)$ at the beginning and zero at the end.

Second, note that the leading monomial of g_k is x_k^{n+1-k} which gives $n!$ different solutions for the system of equations $g_k = 0, k = 1, \ldots, n$. Thus this set should be a minimal Gröbner basis and it is easy to check that this Gröbner basis is reduced as well. ■

For $n = 3$ we have

$$g_1(x_1) = x_1^3 - (a_1 + a_2 + a_3)x_1^2 + (a_1a_2 + a_1a_3 + a_2a_3)x_1 - a_1a_2a_3,$$

$$g_2(x_1, x_2) = x_1^2+x_1x_2+x_2^2-(a_1+a_2+a_3)(x_1+x_2)+a_1a_2+a_1a_3+a_2a_3 =$$

$$x_2^2 - (a_1 + a_2 + a_3 - x_1)x_2 + (a_1a_2 + a_1a_3 + a_2a_3 - (a_1 + a_2 + a_3)x_1 + x_1^2),$$

$$g_3(x_1, x_2, x_3) = x_1+x_2+x_3-(a_1+a_2+a_3) = x_3-(a_1+a_2+a_3-x_1-x_2).$$

Note that if we take the elements g_k with $k \geq l$ we get the reduced Gröbner basis for the ideal I_l, generated by polynomials $\sum_i x_i^k - \sum_i a_i^k$ with $k \leq l$. This follows from the fact that the terms of higher degrees do not influence the reduction process. Naturally, $I_1 = I$ but for $l > 1$ we have infinitely many solutions of the corresponding system.

More interesting are the remaining equations.

Theorem 3. *The condition that m different numbers $x_1, \ldots, x_m$ belong to A is expressed as a system of equations:*

$$g_k(x_1, \cdots, x_k) = 0, \ k = 1, \ldots, m.$$

Proof. We already know that the conditions are valid. It remains to note that the equations have $n(n-1)\cdots(n-m+1)$ solutions and this exactly the number of ways to choose m ordered elements from n. ■

Note that for $m = 2$ we get our familiar conditions $p_A(x_1) = 0$, $p_2(x_1, x_2) = 0$, but we do not need the condition $p_A(x_2) = 0$, which follows from them. More generally it follows from the proof that the polynomials g_k form the reduced Gröbner basis of the corresponding ideal.

If some a_i are equal, the theorem is still valid if we allow the equality of x_i up to multiplicity (e.g. if $x_i = x_j = x_k = a$, then a should appear at least three times in A). For example, if $a_1 = a_2 = 0$, $a_3 = a_4 = 1$, then our equation is $x^4-2x^3+x^2 = 0$ and the condition that $x_1, x_2, x_3 \in A$ looks as

$$x_1^4-2x_1^3+x_1^2 = 0, x_1^3+x_1^2x_2+x_1x_2^2+x_2^3-2(x_1^2+x_1x_2+x_2^2)+(x_1+x_2) = 0,$$

$$x_1^2 + x_1x_2 + x_1x_3 + x_2^2 + x_2x_3 + x_3^2 - 2(x_1 + x_2 + x_3) + 1 = 0.$$

The last equation does not allow $x_1 = x_2 = x_3 = 0$, but $x_1 = x_2 = 0$, $x_3 = 1$ is a perfect solution.

If $A = \{0, 1, \ldots, n-1\}$ then a standard way to simplify the equations (see [1]) is to replace this set by $B = \{1, \varepsilon, \ldots, \varepsilon^{n-1}\}$ with $\varepsilon^n = 1$. In this case $g_1(x_1) = x_1^n - 1$ and $g_k(x_1, \ldots, x_k) = h_k(x_1, \ldots, x_k)$ for $k > 1$.

If the size of A is not too large the equations are rather robust – we can easily create bounds δ_k such that if all $|g_k| < \delta_k$, then $|x_i - a_j| < \varepsilon$ for some j. Thus the equations have some practical applications. For large A the number of terms makes this approach impractical and the equations from Theorem 1 are probably more convenient.

It would be interesting to understand how to obtain the intersections. If B is another finite set we can create the similar equations. Together two systems of equations describe the intersection $A \bigcap B$, but it is rather unclear how these two Gröbner bases cooperate to form the Gröbner basis , which describes $A \bigcap B$. Understanding this probably could open new ways to optimize Gröbner basis calculations.

One possible application of this approach is sudoku. The experiments on sudoku examples show that the computations are much less efficient than direct combinatorial searching of the solution. Again, we need the correct interpretation of the elimination process to improve the efficiency of Gröbner basis approach.

Another remark. As we will see later, it is possible to express even more difficult conditions, e.g. $x > y$. One way to do it is to write that $x-y$ belongs to the known finite set S of differences, thus $p_S(x-y) = 0$. But what is the Gröbner basis interpretation of transitivity law:

$$x > y, y > z \Rightarrow x > z?$$

Why such trivial things are so difficult to obtain?

3 Points on the plane

Suppose now that we have a set S consisting of n different points (a_j, b_j) in the plane and want to describe the conditions that m given points $P_k = (x_k, y_k)$ belong to S. The simplest case is when we deal with real numbers. Then it is sufficient to introduce complex numbers $w_j = a_j + ib_j$ and use Theorem 3 to get necessary equations in the complex form. Of course, using their real and imaginary parts we can get the equations in the real form as well. For example, to describe that P_1, P_2 are different and belong to the set $(0,0), (0,1), (1,0), (1,1)$ we introduce first four complex numbers $w_1 = 0$, $w_2 = 1$, $w_3 = i$, $w_4 = 1 + i$. The corresponding equation having w_i as roots is

$$w^4 - (2 + 2\,i)\,w^3 + 3\,iw^2 + (1 - i)\,w = 0.$$

Thus the equations

$$z_1{}^4 - (2 + 2\,i)\,z_1{}^3 + 3\,iw^2 + (1 - i)\,z_1 = 0,$$

$$z_1{}^3 + z_1{}^2 z_2 + z_1 z_2{}^2 + z_2{}^3 - (2 + 2\,i)\left(z_1{}^2 + z_1 z_2 + z_2{}^2\right) +$$

$$+3\,i\,(z_1 + z_2) + 1 - i = 0$$

describe the situation. Converting this to real equations does not look attractive, as we already can see in the case of the first equation:

$$x_1{}^4-6\,x_1{}^2y_1{}^2+y_1{}^4-2\,x_1{}^3+6\,x_1{}^2y_1+6\,x_1y_1{}^2-2\,y_1{}^3-6\,x_1y_1+x_1+y_1=0,$$

$$6x_1y_1{}^2-6x_1{}^2y_1+y_1-2x_1{}^3-4x_1y_1{}^3+2y_1{}^3-x_1+3x_1{}^2+4x_1{}^3y_1-3y_1{}^2=0.$$

The situation is more difficult when the numbers are not real. Nevertheless in the generic case we can also find some approach, though not so obvious. As in the previous section we can easy describe the conditions that $x_1,\dots,x_m$ belong to $A=\{a_1,\dots,a_n\}$ and similarly that $y_1,\dots,y_m$ belong to $B=\{b_1,\dots,b_n\}$. The trouble is to coordinate the choices. In the generic case we have an easy solution: because all the numbers a_i+b_j are different, all that we need to say is that the numbers x_k+y_k belong to the set $C=\{a_1+b_1,a_2+b_2,\dots,a_n+b_n\}$ and we can express this according to the previous section.

We illustrate this in the following case. Suppose that the set S consists of two different points $(a,b),(c,d)$ with the "generic" coordinates. We need to describe the conditions that two given points (x,y) and (z,t) belong to S and are different. We use Theorem 1 to describe the corresponding elements in the ideal shorter. Here the first line describes the condition that coordinates belong to A and B and the last ones that $x+y$ and $z+t$ belong to C:

$$\begin{gathered}\left\{x^2+z^2-a^2-c^2,x+z-a-c,\ y^2+t^2-b^2-d^2,y+t-b-d,\right.\\ x+y+z+t-a-b-c-d,x^2+2\,xy+y^2+z^2+2\,zt\\ \left.+t^2-a^2-2\,ab-b^2-c^2-2\,cd-d^2\right\}.\end{gathered}$$

We can easily obtain Gröbner basis using the generic condition:

$$\begin{gathered}[t^2+(-b-d)\,t+bd,(-d+b)\,z+(c-a)\,t-cb+ad,\\ y+t-b-d,(-d+b)\,x+(-c+a)\,t-ab+cd].\end{gathered}$$

Note that this is a Gröbner basis so long as $b\neq d$.

In the case $b=d$ the Gröbner basis is different:

$$[t-d,z^2+(-a-c)\,z+ac,y-d,x+z-a-c],$$

but this is obviously not a generic case.

4 Small combinatorial problem

In this section we want to so consider very small combinatorial example to illustrate some ways to translate other conditions on the Gröbner basis language.

The problem is to find a word, consisting of 5 different letters A, B, C, D, E and satisfying the following conditions:

1. Exactly one consonant is written between two vowels.
2. Every vowel is placed on an odd place.
3. The letter C is placed before D, which itself is placed before A.
4. The letter B is placed before E.
5. The number of letters between C and E is odd.

No one condition looks as an equation, but we want to find the equations that equivalently describe the problem.

First of all we have a permutation of letters, which means that we can suppose that every letter has some value – its place in the word. From the first section we know how to describe this shortly:

$$A^k + B^k + C^k + D^k + E^k = 1^k + 2^k + 3^k + 4^5 + 5^k$$

for $k = 1, \ldots 5$.

The first condition now can be expressed as

$$|A - E| = 2 \Leftrightarrow (A - E)^2 = 2^2.$$

The second condition we could express using Theorem 3, but if we note that it is equivalent with the condition that the third letter is a vowel, we get a trivial equation $(A - 3)(E - 3) = 0$.

How to express the condition $D > C$ as an equation? A possible way is to say that $D - C$ belongs to the set $\{1, 2, 3, 4\}$ and this is an equation. Similarly we express the remaining conditions (note that the last one means that $|C - E| = 2$ or $|C - E| = 4$.)

Now we are ready to start Maple session to implement this. The only difficulty is that the letter D is reserved in Maple and we replace it by T. To see the result directly we use the command *solve*, that (with the help of Gröbner basis) finds the solution of the system. The last two lines we need to print our nice result using the found substitution.

$> S := \{X - T + B, Y - T + C, Z - A + T,$
$A + B + C + T + E - (1 + 2 + 3 + 4) - 5,$
$A^2 + B^2 + C^2 + T^2 + E^2 - 1^2 - 2^2 - 3^2 - 4^2 - 5^2,$
$A^3 + B^3 + C^3 + T^3 + E^3 - 1^3 - 2^3 - 3^3 - 4^3 - 5^3,$
$A^4 + B^4 + C^4 + T^4 + E^4 - 1^4 - 2^4 - 3^4 - 4^4 - 5^4,$
$A^5 + B^5 + C^5 + T^5 + E^5 - 1^5 - 2^5 - 3^5 - 4^5 - 5^5,$
$expand((A-3)*(E-3)), expand((C-E+2)^2*(C-E+4)^2),$
$expand((Y-1)*(Y-2)*(Y-3)), expand((Z-1)*(Z-2)*(Z-3)),$
$expand((X-1)*(X-2)*(X-3)*(X-4)), expand((A-E)^2-4)\}:$
$> R := solve(S);$

$$R := \{A = 5, B = 2, C = 1, E = 3, T = 4, X = 2, Y = 3, Z = 1\}$$

> f := (x, y) − > subs(R, x) < subs(R, y):
> sort([A, B, C, T, E], f);

$$[C, B, E, T, A]$$

References

[1] W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, Amer Mathematical Society, 1994,

Victor Ufnarovski

Received June 11, 2012

Centre for Mathematical Sciences, Mathematics,
Lund University, LTH
P.O. Box 118, SE-22100, Lund, Sweden
E–mail: *ufn@maths.lth.se*