Gröbner Bases

A Useful Tool in Algebra

Arnab Chakraborty

A common puzzle found in many elementary puzzle books asks the reader to pour out some specified amount of milk using two (or more) containers of fixed volumes. For instance, a typical version may read as follows.

Example 1 In a dairy shop there is a huge container holding milk, and only two jugs of 3 litre and 5 litre capacities. However, these are not graduated. When a customer comes with a container (of an unknown volume) to take 4 litres of milk, the salesman is at a loss as to how he can give 4 litres of milk using only those two jugs. Can you help the distressed salesman? □

I do not think that you will take much time to help the poor salesman, who is obviously not too bright at mathematics. The simple observation that 4 may be written as $2\times5-2\times3$ is enough to suggest that the salesman should pour 2 jugfuls of the bigger jug, and then take away 2 jugfuls of the other one. All this is pretty simple once we know that $4 = 2 \times 5 - 2 \times 3$. But how do you come to know of this in the first place? Mere inspection may not be enough, as one finds in the next example.

Example 2 Suppose you are given two jugs. They have volumes 4 litres, 6 litres. Suggest a method for giving 5 litres of milk to a customer. □

To solve this observe that you have only the following 'moves' in your arsenal: (Here J_4 denotes the 4 litre jug, while J_6 stands for the other one.)

1. J_4 to J_6
2. J_6 to J_4

Arnab Chakraborty did his BStat (Hons.) and MStat degrees from the Indian Statistical Institute (Calcutta). He is now a PhD student in the Department of Statistics at Stanford University, California. His research interest lies in areas of statistics and computational algebra. Apart from that he is also interested in playing the piano and wishes he could really play well.

3. J_4 to customer

4. J_6 to customer

5. Source to J_4

6. Source to J_6

But the jugs not being graduated, you can never perform any of the above moves halfway – you have to either fill up the container into which you are pouring, or you have to completely empty the one from which you are pouring. And this implies that whatever strategy you choose, at any stage the amount of milk in any of the containers must be of the form $6n + 4m$, where m and n can be any integers, positive, negative, or zero. This is because, the jugs being ungraduated, you have to move in steps of 6 or 4 only.

Thus example 2 cannot be solved, since any number of the form $6n + 4m$ has to be even, while 5 is an odd number. Our analysis has, nevertheless, led a very useful corollary. We state this result as a general fact below.

FACT : Suppose we have k ungraduated jugs of volumes $V_1, V_2,$ V_k litres. We assume that all the V_i's are integers. Then the only volumes of milk that we can measure out to a customer are of the form

$$n_1V_1 + n_2V_2 + \quad + n_kV_k,$$

where each n_i is an integer (positive, negative, or zero).

Do not worry if you find that, for some choices of $n_1,$ $, n_k,$ the volume turns out to be negative. Giving a negative volume of milk to the customer simply means taking that amount of milk *from* him.

We shall call these measurable volumes of milk as *ideal volumes*, and refer to the set of such volumes as an *ideal*. Thus each set of jugs gives rise to one ideal of measurable volumes. Before proceeding further, you will do well to acquaint yourself better with this new concept of ideals. And this is precisely what the following exercise will help you to do.

Exercise : Let $\mathcal{I}$ denote an ideal (for some set of jugs). Suppose that v and w are two members of $\mathcal{I}$ Do you think that $v - w$ and $v + w$ are also in $\mathcal{I}$? What about $53v$?

What we have done above is to observe that all the volumes of milk that one can possibly measure using a given set of jugs are of a special structure, and we have called their set an ideal. So, given an integer volume V we want to know whether it is a member of our ideal or not. If it is, then V must be of the form

$$V = n_1V_1 + \quad + n_kV_k.$$

If we can know the n_i's we at once know how to measure volume V using jugs of volumes $V_1, \quad V_k$.

More than two thousand years ago, this problem was solved by a famous Greek mathematician called Euclid. He made the following simple, yet brilliant, observation, which we present in modern terminology.

Euclid's Observation : If $\mathcal{I}$ is the ideal obtained for jugs of volumes $V_1, \quad V_k$, then an integer volume V of milk is in $\mathcal{I}$ if and only if the gcd of $V_1, \quad V_k$ divides V

If you want to see how Euclid proved this observation simply notice that any integer of the form $n_1V_1 + \quad + n_kV_k$ must be divisible by the gcd of V_i's. Conversely, we claim that the gcd of V_i's is itself of the form $n_1V_1 + \quad + n_kV_k$ for some integers $n_1, \quad , n_k$. Proving this is simple if you remember the long-division-like procedure of computing the gcd of two numbers.

Well, coming back to our puzzle, we observe that we have got a complete solution to it. We present it below.

Step 1: Compute the gcd (G, say) of the volumes $V_1, \quad V_k$. Express G as

$$G = n_1V_1 + \quad + n_kV_k$$

for suitable integers n_i.

Step 2: Check whether the desired volume(V,say) is divisible by this gcd. If not, then you cannot measure this volume. Otherwise, you can measure it.

Now, so far in our puzzle we have been talking about volumes of milk. However, even a layman can see that all that we have done actually works for any integer-valued quantity – irrespective of any physical interpretation that we may attach to it. Now, mathematicians go one step further. They are the sort of people who are always trying to stretch things as far as they can. Their motto seems to be 'If you have a key that fits one lock, then try it on another lock too'. Thus, when the mathematicians saw that replacing 'volume' by 'any integer-valued quantity' did not change the essence of the puzzle, they at once tried to replace the 'integers' as well just to see what happens! And something remarkable did happen, as we shall presently see.

The very first thing that they tried their hands on were polynomials. Now, to understand what they did you must recall that a polynomial is an expression of the form $a_0 + a_1x +$ $+ a_nx^n$,where the a_i's are any numbers. For instance, $3.5 - x + 1000.45x^2$ is a polynomial. You may be wondering why the mathematicians chose *polynomials* in place of integers. Well, their answer was 'Polynomials *behave like* integers'. They do have a point here, no doubt. After all, polynomials can be added just like integers and, just like integers, they can be multiplied as well. More specifically, all the following properties are true for both integers and polynomials.

Common Properties of Integers and Polynomials:

If a, b, c are either all integers or all polynomials, then

1. $(a + b) + c = a + (b + c)$, $(ab)c = a(bc)$
2. $a + b = b + a$
3. $a(b + c) = ab + ac$
4. $1 \times a = a$, $0 + a = a$
5. $ab = ba$

Clearly, if you note that the usual long division like algorithm (by the way, it is called Euclid's algorithm) for finding

gcd of integers may be directly adapted for polynomials, you can understand why our earlier algorithm works for polynomials also. Thus, given polynomials $f_1, \quad , f_k$ we define the *ideal generated by them* as the set $Ideal(f_1, \quad , f_k)$ of all polynomials of the form

$$g_1 f_1 + g_2 f_2 + \quad + g_k f_k,$$

where the g_i's are any polynomials. Our problem is to check whether some given polynomial f is in this ideal or not. Applying Euclid's algorithm we first compute the gcd, say h, of the f_i's and then check whether h divides f or not.

Now, once they saw that the method worked for polynomials, the mathematicians went one step further. They tried to work with polynomials in two variables (x and y, say). As you might have guessed already, these are objects like $1.3 + x - 45x^{12}y^3$. If we call an expression like $ax^m y^n$ (a is any nonzero number, m and n are nonnegative integers) a *monomial* then a polynomial in two variables is a sum[1] of monomials. Henceforth, we shall refer to polynomials in two variables as *2-polynomials.*

[1] Since a may be negative, difference is also included.

Suppose that from the space of all such 2-polynomials, we pick up k of them, $f_1, \quad , f_k$. As usual, their ideal is the set of all 2-polynomials of the form

$$g_1 f_1 + \quad + g_k f_k,$$

where the g_i's are any 2-polynomials. Our problem is to check whether some given 2-polynomial f is in this ideal or not.

And now comes the fix. Euclid's algorithm fails to be of any direct help here as the following example shows.

Example 3 Suppose $k = 2$, and f_1, f_2 are just x and y, respectively, and let us take $f = x$. If you want to follow Euclid's precept, you first try to compute the gcd of f_1 and f_2. But what do you *mean* by gcd here? The greatest common factor? You cannot measure 'greatness' for 2-polynomials. For ordinary polynomials we have the concept of degree, and can say that a polynomial with higher degree

is a 'greater' polynomial. But not so in presence of two variables. Which is greater, $x^2y + y^3$ or $y^2x + x^3$? So we have to define gcd here in a different way. We factor both f_1 and f_2 and bunch up as many common factors as possible to define gcd of f_1 and f_2. In our case the only common factor is 1. So $\gcd(f_1, f_2) = 1$. Obviously the Euclidean idea fails here, since this gcd itself lies outside the ideal set. □

The moral is that the use of gcd that we made for polynomials in one variable cannot be made for 2-polynomials. So we cannot possibly hope to check membership in an ideal simply by checking divisibility by some suitably chosen 2-polynomial as in the case of polynomials with a single variable. So what do we do?

We recall that the method for finding gcd was like a long division. Can we at least do long division with 2-polynomials? The answer is yes. First, we introduce an ordering among *monomials*. Given two *monomials* ax^my^n and bx^py^q, we shall say that the first one is 'bigger' (written as $ax^my^n \succ bx^py^q$) if $m > p$, or if $m = p$ and $n > q$. Note that the constants a, b (positive or negative) do not matter in this ordering [2].

Exercise: Which is bigger, $100x^3y$ or $2x^2y^{100}$? Which is the bigger monomial in the 2-polynomial $10x^3y - x^4$?

The biggest monomial in a 2-polynomial, f, will be called its *head monomial* denoted by $\mathrm{HM}(f)$. Now we shall see how to perform long division with 2-polynomials.

[2] This ordering is called the *lexicographic ordering* in the literature.

The long division algorithm for 2-polynomials is quite similar to that for polynomials in one variable. It is a stepwise procedure. At each step we subtract some suitable multiple of the divisor from the dividend, such that during the subtraction some term is completely knocked off from the dividend. The result of this subtraction serves as the dividend for the next step. When we cannot do this anymore we declare the final dividend as the remainder. The details are provided in the pseudo-code below.

Long division algorithm for 2-polynomials: Dividing

f by g:

Let $\mu = HM(g)$
Let $Divisor = g$
Let $Dividend = f$
Let $Quotient = 0$
While there is some monomial in $Dividend$ (divisible) by μ **do**
    Let $\hat{\mu}$ = a monomial in $Dividend$ such that μ divides $\hat{\mu}$.
    Let $m = \hat{\mu}/\mu$.
    Add m **to** $Quotient$.
    Replace $Dividend$ **by** $Dividend - m(Divisor)$.
Endwhile
Let $Remainder = Dividend$.

Figure 1 shows one implementation of the above algorithm.

This suggests one method of checking membership in an ideal. Why not divide f by all the f_i's simultaneously? This may be done as follows. At each step we choose some f_i, and carry out *one step* of long division using this f_i as the divisor. At the next step we divide the remainder by some f_j, and so on. We stop when we cannot do any more such divisions, and call the remainder at that last step the remainder of the overall process. To distinguish this process from the usual long division we shall henceforth call it a *polynomial reduction.*

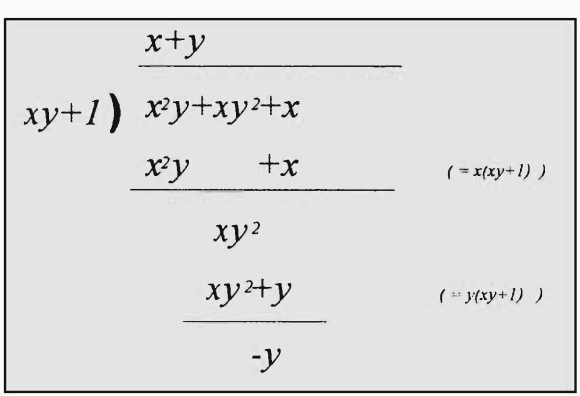

Figure 1. Long division of $f=x^2y+xy^2+x$ by $g=xy+1$.

It is clear that if the remainder vanishes, then f is in the ideal generated by the f_i's. It may also seem natural that the remainder must vanish when f is in the ideal generated by the f_i's. But, unfortunately, two problems prevent this from being so.

Problem 1: Depending on the choices of the f_i's at each step, the remainder may change.

Problem 2: Even if f is in the ideal, and even if you are determined to consider all the possible choices of f_i's at each step, you may still not obtain zero as a remainder.

Example 4 Let $k = 2, f_1 = xy, f_2 = xy + 1$. Then if we apply polynomial reduction to $f = xy$, we get remainder 0 if we use f_1 as divisor; however, we get remainder -1 if we use f_2 as divisor. Now try dividing $f = 1$. Clearly, the remainder is 1 itself. But $1\ (= f_2 - f_1)$ *is* in $Ideal(f_1, f_2)$. □

So here is a pretty fix. However, notice that the situation does not preclude the existence of *some choice* of the f_i's for which neither of the problems is present, but which generate the same ideal. If f_i's constitute one such choice, then obviously membership in the ideal may be easily checked by polynomial reduction as for polynomials with a single variable. In this case we shall call this nice set $\{f_1, \quad , f_k\}$ a *Gröbner basis* of the ideal. Too vague? Well, here is a rigorous version of the definition.

Definition : Given an ideal $\mathcal{I}$ of 2-polynomials, we shall call a *finite* set $\{f_1, \quad , f_k\}$ a *Gröbner basis* of $\mathcal{I}$ (with respect to lexicographic order) if

1. $\{f_1, \quad , f_k\}$ generates $\mathcal{I}$,
2. for any 2-polynomial f, if we do long division of f by the f_i's then the remainder is unique (irrespective of which f_i was used in which step),
3. if, further, $f \in \mathcal{I}$, then this unique remainder must be zero.

But before trying to find one such basis, let us look at a diagrammatic representation of polynomial reduction. Suppose that at some step we are going to divide g (which is possibly the remainder from the preceding step). So we choose some f_i such that $HM(f_i)$ divides some monomial in g, say,

$$m \times HM(f_i) = \text{ some monomial in } g,$$

where m is some monomial. Then the step consists of subtracting mf_i from g, leaving remainder $g - mf_i$, which serves as the dividend at the next step.

We shall represent the above by drawing an arrow from g to $g - mf_i$. In other words, an arrow from some 2-polynomial g to some 2-polynomial h implies that if at some step during polynomial reduction by $f_1, \ldots, f_k$ the 2-polynomial g comes as the dividend, then at the next step a possible candidate for the dividend is h. Of course, at some step more than one f_i may be eligible as a divisor. In such a case, more than one arrow emanates from g, each arrow corresponding to some choice of the divisor. Next, imagine all the 2-polynomials written down on a huge piece of paper. If we now draw all the possible arrows we shall get an arrow-diagram. A *portion* of such a diagram is shown in *Figure* 2.

The following observations are now in order.

Observations :

1. The diagram depends on the set $f_1, \ldots, f_k$. If you enlarge the set, more arrows will appear.

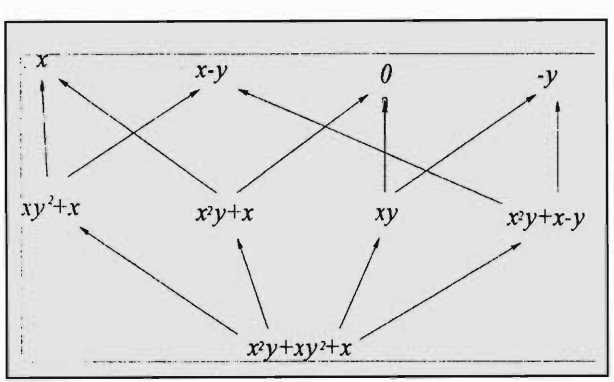

Figure 2. Each arrow represents one step of polynomial reduction. Here k=2, and $f_1 = xy$, $f_2 = xy+1$.

2. From some polynomials, no arrows come out. We shall call them *dead ends*. In the course of a polynomial reduction, once you come across such a polynomial you have to declare that as your remainder. Observe that at each step during the reduction we are knocking off one monomial from the dividend. Also, the new monomials that enter into the dividend during the step are all 'less than' the knocked off monomial. Since there are only finitely many monomials 'less than' any given monomial (check!), the reduction process must stop after some step. That is, *we must come to a dead end.*

3. Start from any polynomial f, go on following the arrows until you come to some dead end h. Then your path represents one implementation of the polynomial reduction of f by $f_1, \quad , f_k$ leaving remainder h. We shall denote such a path (along consecutive arrows) from f to h as $f \xrightarrow{*} h$.

4. If $f \xrightarrow{*} 0$ then for any 2-polynomial g we must have $gf \xrightarrow{*} 0$.

5. Suppose f is in $Ideal(f_1, \quad , f_k)$. Then there is a chain of arrows from f to 0, but possibly not all the arrows are correctly aligned [3]. We shall denote this by $f \xleftrightarrow{*} 0$.

[3] This may not seem obvious at first sight. However, its proof is not important for this article.

Next, we present a result which shows that actually the two problems mentioned above are not two distinct problems. If we can solve the first of them then the other one solves itself.

Result: Suppose that the 2-polynomials $g_1, \quad , g_k$ are chosen in such a way that for any 2-polynomial f the remainder upon polynomial reduction by g_i's is unique. Then for any f in $Ideal(g_1, \quad , g_k)$ this unique remainder must be zero.

Proof: Since f is in the ideal, by the last observation above,

$$f \xleftrightarrow{*} 0.$$

Now we claim that whenever two 2-polynomials f and g are such that $f \xleftrightarrow{*} g$ we always have some 2-polynomial h such that

$$f \xrightarrow{*} h,$$

and

$$g \xrightarrow{*} h.$$

If we can justify this claim then the result follows immediately (how?).

To justify the claim we use induction on l, the number of arrows in the $\overset{*}{\leftrightarrow}$ path between f and g. If $l = 0$, then $f = g$, and so $h = f$ is one choice for h. Suppose now that we have proved the result for $l = n$, for some $n \geq 0$. We shall prove it for $l = n + 1$, as well.

In *Figure* 3 the zigzag arrows denote the $\overset{*}{\leftrightarrow}$ path between f and g. It is of length $n + 1$. Let τ be the 2-polynomial just before g on this path. Then there is a path of length n between f and τ. Hence, by our assumption, there is some 2-polynomial α such that

$$f \xrightarrow{*} \alpha, \text{ and } \tau \xrightarrow{*} \alpha.$$

Now apply polynomial reduction to g. This takes you up a path along consecutive arrows until you come to some dead end (β, say, which is your remainder). Assume that $\tau \rightarrow g$, as shown in the figure. Then you have two paths (along consecutive arrows) starting from τ – one terminates at α, and the other at β. In view of observation 3 above, this means that you have two polynomial reductions of τ, one leaving remainder α, the other β. Due to the assumed uniqueness of remainders we must have $\alpha = \beta$, justifying

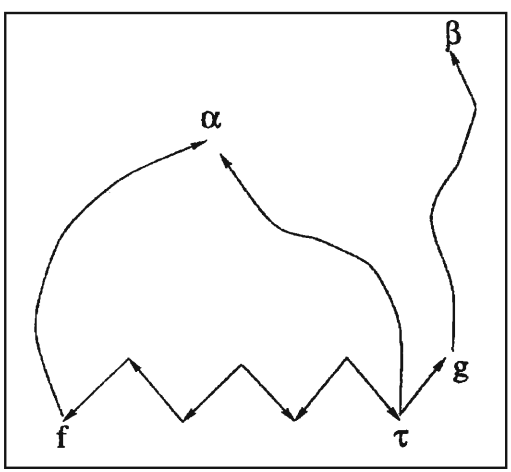

Figure 3. Here actually $\alpha=\beta$, since both are remainders of τ.

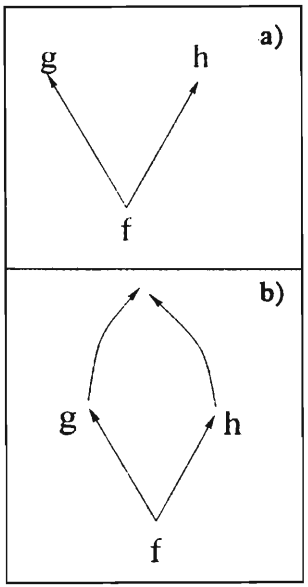

Figure 4. a) Non-combining branches. Here g, h do not lead to the same destination.
b) Recombining branches.

the claim for the case when $\tau \rightarrow g$. If $g \rightarrow \tau$ then the proof is obvious from the diagram once you reverse the direction of the arrow between τ and g. Simply go from g to α via τ. □

If you have understood the above argument then you may similarly try to prove the following result which we shall need later.

Result : If f and g are 2-polynomials such that $f - g \xrightarrow{*} 0$, then there must exist a 2-polynomial h such that

$$f \xrightarrow{*} h \text{ and } g \xrightarrow{*} h.$$

So our aim now is to get hold of g_i's such that

(i) $Ideal(g_1, \quad , g_l) = Ideal(f_1, \quad , f_k)$

(ii) the g_i's satisfy the condition of the above result.

If g_i's meet these conditions, then by the above result they must constitute a Gröbner basis. Note that in this case the arrow-diagram for the g_i's has the following property:

> Start from any point in the diagram, follow whichever path you like (along the arrows) until you come to a dead-end; you will find that you always come to the same dead-end irrespective of the path you have followed.

How can you get an arrow-diagram with this property? Of course, if the diagram has no branching at all, then the condition holds trivially. But, even if branching occurs, the property may still hold good, as we shall see below.

Consider the two branchings shown in *Figure* 4

In case (b) the branches have eventually recombined. Thus, both the branches eventually lead to the same destination. Clearly such a branching poses no problem. But in the other case the branches terminate *as separate branches.* Here the two branches lead to different dead-ends, a situation which

we wish to avoid. If only we could guarantee (by choosing the g_i's appropriately) that this latter type of branching is not present in the arrow-diagram, then we have achieved our aim of obtaining a Gröbner basis.

Let us take a closer look at the mechanism of branching. In the branching shown in *Figure* 5 two branches radiate from a root f.

From the very definition of the arrows we see that $f \rightarrow f_1$ means that there is some divisor g_1, say, and some monomial m_1 such that

$$m_1 HM(g_1) = \text{ some monomial in } f,$$

and

$$f_1 = f - m_1 g_1.$$

Similarly, for the other branch we have some divisor (g_2, say) and monomial m_2 such that

$$m_2 HM(g_2) = \text{ some monomial in } f,$$

and

$$f_2 = f - m_2 g_2.$$

By an earlier result we know that one *sufficient* condition for the branches to recombine is that

$$f_1 - f_2 \xrightarrow{*} 0.$$

i.e.,

$$m_2 g_2 - m_1 g_1 \xrightarrow{*} 0.$$

Now, if $HM(m_1 g_1) \succ HM(m_2 g_2)$, then subtract $-m_1 g_1$ from $m_2 g_2 - m_1 g_1$, and then subtract $m_2 g_2$ to arrive at remainder zero. Similarly you may reduce $m_2 g_2 - m_1 g_1$ to zero if $HM(m_2 g_2) \succ HM(m_1 g_1)$. So in either of these cases the branches do recombine.

Thus, we have narrowed down the source of non-unique remainders to those branches for which

$$HM(m_1 g_1) = HM(m_2 g_2).$$

Hence, if we choose $g_1, \quad , g_l$ such that

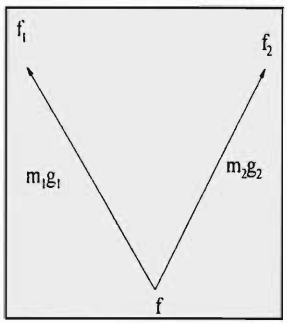

Figure 5. A close look at branching.

(i) $Ideal(g_1, \quad , g_l) = Ideal(f_1, \quad , f_k)$,

(ii) whenever for any two monomials m_1, m_2 we have $HM(m_1 g_1) = HM(m_2 g_2)$, we must also have $m_2 g_2 - m_1 g_1 \xrightarrow{*} 0$.

then $\{g_1, \quad , g_l\}$ is a Gröbner basis of our ideal.

Exercise : Let $HM(g_i) = a_i x^{p_i} y^{q_i}$, for $i = 1, 2$. Let $p = \text{Max}\{p_1, p_2\}$ and $q = \text{Max}\{q_1, q_2\}$. Define the monomial m as $x^p y^q$. Suppose that m_1, m_2 are two monomials such that $HM(m_1 g_1) = HM(m_2 g_2)$. Show that

1. $HM(m_1 g_1)$ is divisible by m,
2. if we put $\mu_i = \frac{1}{a_i} x^{p-p_i} y^{q-q_i}$, for $i = 1, 2$, then $m_1 g_1 - m_2 g_2$ is divisible by $\mu_1 g_1 - \mu_2 g_2$.

To keep the notations simple we shall call $\mu_1 g_1 - \mu_2 g_2$ defined above as $trouble\ (g_1, g_2)$. From the above exercise, and an earlier result, we immediately get the following important result [4].

[4] In the literature this result is known as *Buchberger's criterion.*

Result : Let $f_1, \quad , f_k$ be any set of 2-polynomials. Let $g_1, \quad , g_l$ be 2-polynomials chosen such that

(i) $Ideal(f_1, \quad , f_k) = Ideal(g_1, \quad , g_l)$,

(ii) for all $i, j = 1, \quad , l$ we have $trouble(g_i, g_j) \xrightarrow{*} 0$.

Then $g_1, \quad , g_l$ is a Gröbner basis of $Ideal(f_1, \quad , f_k)$.

The result gives us a *sufficient* condition for g_i's to be a Gröbner basis of $Ideal(f_1, \quad , f_k)$. But apparently it does not tell us whether for given f_i's such g_i's exist or not, and even if they exist, it does not seem to tell us how to find them. However, a careful second look at the result yields the following simple algorithm due to Buchberger to compute a Gröbner basis. The method starts by checking whether the set $\{f_1, \quad f_k\}$ itself is a Gröbner basis or not. To this end it picks some pair $\{i, j\}$, and computes $trouble(f_i, f_j)$. Then polynomial reduction is applied to it with divisor set

$\{f_1, \quad f_k\}$ to see if we get remainder zero. If so, then the pair poses no problem; otherwise, if we get a non-zero remainder (h, say) then we conclude that $\{f_1, \quad , f_k\}$ is not a Gröbner basis, but that $\{f_1, \quad , f_k, h\}$ may be one. So we apply the above method afresh to this latter set, and so on. When the process terminates, we obviously end up with a Gröbner basis. A somewhat nontrivial argument (omitted here) shows that the process always terminates after a *finite* number of steps.

Buchberger's Algorithm:

Input : 2-polynomials $f_1, \quad , f_k$.

Output : 2-polynomials $g_1, \quad , g_l$ constituting a Gröbner basis for *Ideal* $\{f_1, \quad , f_k\}$.

Notation : For any finite set A, let $\mathcal{D}(\mathcal{A})$ denote the set of all pairs of distinct elements of A.

Method :

Let $\mathcal{G} = \{f_1, \quad , f_k\}$.
Let $\mathcal{B} = \mathcal{D}(\mathcal{G})$.
While $\mathcal{B}$ is nonempty **do**
    Pick some pair $\{f, h\}$ from $\mathcal{B}$.
    Remove the pair from $\mathcal{B}$.
    Let $g = trouble(f, h)$.
    Apply polynomial reduction to g with divisor set $\mathcal{G}$.
    Let $h =$ remainder from this polynomial reduction.
    If $h \neq 0$ **then**
        Insert h into $\mathcal{G}$.
        Let $\mathcal{B} = \mathcal{D}(\mathcal{G})$.
    Endif
Endwhile

The elements of $\mathcal{G}$ are now the required $g_1, \quad , g_l$.

Finally let us take stock of what we have achieved so far. We have defined ideals for integers, polynomials in a single variable, and lastly, for 2-polynomials. The puzzle that we posed initially involved checking membership in an ideal for the integer case. We saw that Euclid's method pro-

vided a solution for that case, as well as for the case of polynomials in one variable. However, the method failed for 2-polynomials. Through our discussion we have got a different method which works for 2-polynomials. It essentially consists of two steps. Given 2-polynomials $f_1, \quad , f_k$, if we want to check whether some 2-polynomial f belongs to $Ideal(f_1, \quad , f_k)$, we first compute a Gröbner basis $\{g_1, \quad , g_l\}$ of this ideal. The second step is to apply polynomial reduction to f with this basis as the divisor set. f is in the ideal if and only if the remainder turns out to be zero.

But what does come out of it? Yes, it solves our original puzzle generalized for 2-polynomials alright, but *is that all*? No, it is not. Gröbner bases have lots of other applications in algebra. In particular, there is a fascinating subject called algebraic geometry [5], where Gröbner bases have become a very useful tool. There ideals may be interpreted as certain geometric objects. But that is quite another story. And you may wish to learn that yourself once you pick up the basic notions of abstract algebra.

[5] This subject deals with geometric objects from an algebraic viewpoint.

Suggested Reading

[1] **D Cox, J Little and D O'Shea, *Ideals, varieties and algorithms : An introduction to computational algebraic geometry and commutative algebra* (2nd edition), Springer, Undergraduate Texts in Mathematics, 1991.**

[2] **R K Shyamasundar, Introduction to Algorithms, *Resonance*, Vol. 1, No. 9, 1996. (This is the reference for the language used to describe the algorithms in the present article.)**

Address for Correspondence
Arnab Chakraborty
Department of Statistics
Stanford University
California, USA.

Not Abel to Solve

The quadratic was solved with ease.
The cubic and biquadratic did tease
but got done in the same year.
And then the quintic made it clear
that algebra developed by degrees!

B Sury