Journée maths Actuelles 2024

Autour des bases de Grobner

Résolution de système à plusieurs inconnues

1 Le cas de $k[x]$

Soit k un corps, disons $\mathbb{R}$ ou $\mathbb{C}$. On note $k[x]$ l 'anneau des polynômes en une variable.
Si on se donne une équation dans $k[x]$, on arrive dans certains cas à en trouver les solutions

1). Si $f = ax + b$, la solution est $x = -b/a$ si $a \neq 0$.

2). Si $f = ax^2 + bx + c$, on trouve une ou deux solutions dans $\mathbb{C}$ en utilisant la méthode du déterminant

3). Si f est de degré 3 ou 4, on peut encore trouver des solutions qui s'écrivent avec des racines, avec la méthode de Cardan pour le degré 3 et la méthode de Ferrari pour le degré 4.

4). À partir du degré 5, le théorème d'Abel Ruffini de 1824 nous apprend qu'en général les solutions d'une équation polynomiale ne peuvent pas toujours s'écrire à l'aide des opérations élémentaires et des racines.

Dans la suite, nous allons plutôt nous intéresser à la résolution de système. Continuons sur l'exemple de $k[x]$.

Exemple 1.1. Si on considère

$$\begin{cases} f(x) = & x^8 + 7x^5 + 3x + 1 \\ g(x) = & x \end{cases}$$

On peut facilement résoudre : on considère les racines de g, qui est juste 0, et on regarde si 0 est solution de f. Or $f(0) = 1$, donc le système ci-dessus n'a pas de solution.

Exemple 1.2. Si maintenant on considère

$$\begin{cases} f(x) = & 2x^4 + x^3 + 2x^2 + 5x + 2 \\ g(x) = & 4x^3 + 2x^2 + 2x + 1 \end{cases}$$

On pourrait résoudre par rapport à g puis évaluer en f, mais on peut également utiliser le fait que toute solution de f et g est également solution de toute combinaison linéaire de f et g.

$$\begin{aligned} g_1 = & \quad f - 1/2xg = x^2 + 9/2x + 2 \\ g_2 = & \quad g - 4xg_1 = -16x^2 - 6x + 1 \\ g_3 = & \quad g_1 + (1/16)g_2 = 33/8x + 33/16 \\ g_4 = & \quad g_2 + (16 * 8/33)xg_3 = 2x + 1 \end{aligned}$$

Donc toute solution du système est solution de $2x + 1$. D'ailleurs, si on regarde ce qu'on a fait précédemment, on a calculé le pgcd de f et g.

En particulier, les solutions du système f, g sont exactement les solutions du système donné par le pgcd de f et g. Cette propriété vient du fait que l'anneau $k[x]$ est principal (tout ses idéaux peuvent être engendré par un seul élément).

De manière plus générale , même dans le cas des systèmes on ne peut pas toujours les résoudre en calculant le pgcd, (par exemple si le système est redondant, c'est à dire constitué de f et d'un multiple de f ou si le pgcd est de haut degré) mais c'est une méthode qui permet souvent de simplifier le problème.

2 Le cas de deux variables

Contrairement au cas en une variable, une équation à deux variables (ou plus) possède en général une infinité de solutions (au moins dans $\mathbb{C}$ car dans $\mathbb{R}$ l'équation $x^2 + y^2 = 0$ ne possède qu'une solution). Un exemple est $f = y - x - 1$ qui donne une droite.

Si on a deux équations en deux variables, le nombre générique de solutions se restreint alors à un nombre fini de points.

Exemple 2.1. Supposons que se retrouve face au système suivant

$$\begin{cases} f(x,y) = & x^2 + 2xy + y^2 \\ g(x,y) = & xy + 2y^2 \end{cases}$$

On peut évidemment voir que la première équation est en réalité $(x+y)^2$ puis en calculer les solutions, mais supposons que l'on souhaite faire la méthode du cas à une variable, à savoir, faire diminuer le degré.

On se retrouve face à la question : quel est "le plus grand terme" de f ? et de g ? Ce qu'on appellera dans la suite le "terme dominant" de f (respectivement de g).

Une réponse à cette question réside dans le fait d'ordonner les monomes. Il faut donc choisir un ordre, et un bon !

Définition 2.2. Un ordre monomial est un ordre total sur l'ensemble des monômes d'un anneau de polynômes donné, compatible avec la multiplication, c'est-à-dire :

pour tout monôme w, si deux monômes u et v vérifient $u \leq v$, alors $uw \leq vw$.

Il existe plusieurs exemples d'ordre monomiaux. Voici quelques exemples classiques :

Exemple 2.3. L'ordre lexicographique : c'est l'ordre du dictionnaire. Dans l'anneau de polynôme $k[x,y]$, on choisit que $x > y$. Alors $x^{a_1}y^{b_1} > x^{a_2}y^{b_2}$ si et seulement si $a_1 > a_2$ ou si $a_1 = a_2$ et $b_1 > b_2$.

Exercice : Ordonner les monomes $x, xy, x^2y, xy^3, y, x^2$.
Réponse : $x^2y > x^2 > xy^3 > xy > x > y$

Exemple 2.4. L'ordre lexicographique gradué : c'est l'ordre lexicographique, mais on prend d'abord en compte le degré total. Dans l'anneau de polynôme $k[x,y]$, on choisit que $x > y$. Alors $x^{a_1}y^{b_1} > x^{a_2}y^{b_2}$ si et seulement si $a_1 + b_1 > a_2 + b_2$ ou si $(a_1 + b_1 = a_2 + b_2$ et $a_1 > a_2)$ ou si$(\ a_1 + b_1 = a_2 + b_2$, $a_1 = a_2$ et $b_1 > b_2)$.

Exercice : Ordonner les monomes $x, xy, x^2y, xy^3, y, x^2$.
Réponse : $xy^3 > x^2 * y > x^2 > x * y > x > y$

Prenons l'ordre lexicographique gradué et notre exemple.

$$\begin{cases} f(x,y) = & x^2 + 2xy + y^2 \\ g(x,y) = & xy + 2y^2 \end{cases}$$

Alors $\mathrm{lm}(f) = x^2$ et $\mathrm{lm}(g) = xy$. On se rend compte qu'on ne peut pas éliminer les termes en multipliant simplement par un scalaire. Par contre, on a $y\mathrm{lm}(f) - x\mathrm{lm}(g) = 0$.

On peut donc calculer $yf - xg = y^3$. Ici on peut arrêter le calcul car la seule solution possible est $y = 0$ et donc $x = 0$.

On peut cependant se demander si on aurait pu réduire encore y^3 car la puissance est plus grande que celle des termes dominants de f et g. Un tel algorithme de réduction existe et s'appelle la division multivariée. Néanmoins sur cet exemple, y^3 est déjà réduit.

Exemple 2.5. Exemple de réduction multivariée non triviale : calculons la réduction multivariée de x^3 par f et g. On calcule $x^3 - xf = -2x^2y - xy^2$, puis $-2x^2y - xy^2 + 2yf = 3xy^2 + 2y^3$. À partir de là, le terme de tête de f ne divise plus le terme de tête du reste.

On calcule alors modulo g : $3xy^2 + 2y^3 - 3yg = -4y^3$.

Et ici on s'arrête.

Sur l'exemple $< x^2 + 2xy + y^2, xy + 2y^2 >=< x^2 + 2xy + y^2, xy + 2y^2, y^3 >$, on se rend compte que contrairement au cas d'une seule variable, la nouvelle équation qu'on a fait apparaître y^3 n'est non seulement pas de degré plus petit, mais en plus ne permet pas d'éliminer une des équations précédentes. Pourtant, elle est plus "simple" dans le sens où elle ne fait apparaître qu'un seul monôme.

Remarque 2.6. L'exemple précédent fait cependant apparaître un cas de figure intéressant : par construction y^3 est bien dans l'idéal $< x^2 + 2xy + y^2, xy + 2y^2 >$. Par contre, si on applique la procédure de division multivariée, on se rend compte que le reste de y^3 par la division mutivariée de f et g ne donne pas 0.

La division multivariée ne donne pas forcément un critère d'appartenance à l'idéal !

Question : Comment décider si un polynôme appartient à un certain idéal (ou formulé autrement, comment décider si une équation polynomiale provient d'opérations élémentaires effectuées sur un système donné ?)

Dans la suite on va garder l'algorithme de division multivarié, et essayer de travailler sur ce qu'on appelle la "présentation de l'idéal". C'est-à-dire les équations dont on dispose qui décrivent le système d'équation.

Exemple 2.7. Si on regarde (encore) l'exemple $< x^2 + 2xy + y^2, xy + 2y^2 >$, on remarque que ce qui "fait" que la division multivariée n'arrive pas à 0, c'est qu'aucun des termes de tête de f ou de g ne divise y^3.

On est donc obligé de rajouter l'équation y^3 à notre système si on veut qu'il soit "plus lisible".

La question se pose ensuite : est-ce qu'on a tout le monde ? Peut-on faire apparaître de nouveaux monomes dominants ? Sur cet exemple il se trouve que non.

Pourquoi ? Une manière de faire apparaître de nouveaux termes dominants est de calculer ce qu'on appelle les S-polynômes.

En fait, on a déjà calculé un S-polynôme plus tôt sans le dire. Lorsqu'on a pris f et g et qu'on a essayé d'annuler leurs termes de tête.

Définition 2.8. Soit f et g deux polynômes de $k[x, y]$. On définit le S-polynôme de f et g de la manière suivante

$$S(f, g) = \frac{\text{lcm}(lt(f), lt(g))}{lt(f)} f - \frac{\text{lcm}(lt(f), lt(g))}{lt(g)} g$$

Exercice : Calculer le S-polynôme de $f = 2xy+y+x$ et $g = y^2+y$ pour l'ordre deglex. On a $f*y-2*x*g = -x * y + y^2$.

Si on continue l'exercice, ici on peut réduire le S-polynôme par rapport à f puis à g. $2(-x * y + y^2) = 2y^2 + y + x \mod(f)$, et $2y^2 + y + x = x - y \mod(g)$.

Donc le S-polynôme se réduit en $x - y$.

(Ici encore on remarque que ce calcul nous a mené vers un élément du système plus simple).

Exemple 2.9. Maintenant on sait que $< 2xy + y + x, y^2 + y >=< 2xy + y + x, y^2 + y, x - y >$. On peut se demander si en "tapant" le terme de tête de $x - y$ avec ceux de f et g on crée de nouveaux polynômes.

Si on calcule le S-polynôme de f et $x-y$ on trouve $f-2y*(x-y)=2*y^2+x+y$ qui se réduit en 0 par $f, g, x-y$.

On ne produit donc rien de nouveau.

Définition 2.10. Cette procédure qui consiste à prendre des polynômes d'un système d'équation et à faire taper les termes de tête pour en créer de nouveau, puis à continuer jusqu'à ce qu'on ne produise que des polynômes qui se réduisent à 0 est ce qu'on appelle l'**algorithme de Buchberger.** (1976)

Et la sortie qu'on obtient de cet algorithme est appelé une **base de Grobner**.

Une base de Grobner d'un système d'équations (d'un idéal) est grosso modo une présentation du système où on a exhibé de nouvelles équations, en général plus simples.

Les bases de Grobner ont de multiples propriétés, parmi celles-ci nous en citerons deux :

Proposition 2.11. 1). Si G est une base de Grobner d'un idéal I, alors on peut tester si $f \in I$ à l'aide d'un algorithme de division mutivariée.

2). Soit S un système d'équations qui admet une unique solution, alors la base de Grobner (minimale, réduite) est de la forme $G = \{x-a, y-b\}$.

Tout ce qui a été présenté dans le cas de deux variables s'étend pour des polynômes à $n \geq 2$ variables.

3 Cas d'application des bases de Grobner : Solver de Sudoku

Le but de cette partie est de déterminer des conditions polynomiales quant à la résolution du sudoku et d'en coder une résolution grâce aux bases de Grobner. [1]

3.1 Présentation du problème

On se propose d'écrire un algorithme de résolution de sudoku fondé sur des calculs de bases de Gröbner.

Le principe du sudoku est de remplir une matrice $M = (M_{i,j}) \in M_9(\mathbb{Z})$ par des chiffres de $[\![1,9]\!]$ tels que :

— sur chaque ligne, les neuf chiffres apparaissent (ou encore, les éléments de la ligne sont tous distincts) ;

— même contrainte sur chaque colonne ;

— chacune des 9 sous-matrices $(M_{i+3k_1, j+3k_2})_{i,j \in [\![1,3]\!]}$ pour $k_1, k_2 \in [\![0,2]\!]$ a tout ses coefficients distincts (les 9 chiffres apparaissent sur chacune de ces sous-matrices) ;

— de plus, les matrices que l'on regarde peuvent avoir déjà certains chiffres fixés.

Le principe de la résolution que nous proposons sera de déterminer une base de Gröbner de l'idéal des contraintes sur les coefficients, et ainsi, si cette idéal définit bien une unique solution, en réduisant $M_{i,j}$ modulo l'idéal de ces relations, on obtiendra la seule valeur possible pour ce coefficient. [2]

3.2 Contraintes

Contrainte 1.

Déterminer les équations correspondant aux contraintes "$M_{i,j}$ prend ses valeurs dans $[\![1,9]\!]$".

Indications. Penser au fait que $M_{i,j}$ doit annuler un certain polynôme $P \in k[X]$, et ainsi, écrire $P(M_{i,j}) = 0$. On prendra P unitaire et scindé à racines simples (bien choisies...).

1. Repris de `https://www.unilim.fr/pages_perso/tristan.vaccon/TPACGA.pdf`

2. La proposition suivante a l'avantage de bien fonctionner avec le calcul de bases de Gröbner de sage. Néanmoins, une autre présentation des contraintes est possible. En effet, pour avoir tout les termes sur une colonne distincts et égaux à un élément de $[\![1,9]\!]$, il suffit d'ajouter l'équation $\prod_{i=1}^{9}(X-m_{i,j}) - \prod_{i=1}^{9}(X-i) = 0$, et de faire de même pour toutes les lignes, colonnes et sous-carrés. Hélas, cette méthode, pourtant très simple, produit un calcul de base de Gröbner bien trop compliqué pour sage, et c'est la raison de la méthode proposée dans cette partie.

Contrainte 2.

Déterminer les équations correspondant à la contrainte "tous les éléments d'une même colonne sont distincts".

Indications. $Q(X,Y) = \frac{P(X)-P(Y)}{X-Y} \in k[X,Y]$ est bien un polynôme. De plus, $Q(X,Y)$ n'est pas divisible par $X-Y$. Il suffit de poser $X=Y$, on a $Q(X,X) = P'(X)$ qui est non nul dès que P est non constant. Ainsi, si $M_{i,j}, M_{i',j'} \in k$ sont tels que $Q(M_{i,j}, M_{i',j'}) = 0$, $P(M_{i,j}) = 0$, $P(M_{i',j'}) = 0$, alors nécessairement, $M_{i,j} \neq M_{i',j'}$ puisque sinon, $Q(M_{i,j}, M_{i,j}) = P'(M_{i,j}) \neq 0$ puique P est à racines simples.

Les contraintes à regarder sont donc les $Q(M_{i,j}, M_{i',j'})$ pour i, j, i', j' bien choisis.

Contrainte 3.

Faire de même pour les lignes et les sous-matrices $3 * 3$ correspondant aux contraintes sur les 9 carrés.

Contrainte 4.

On suppose que la valeur de $M_{i,j}$ est fixé dans le sudoku de départ à $a_{i,j} \in [\![1,9]\!]$. Quelle est la contrainte polynomiale sur $M_{i,j}$ correspondante à ajouter à notre liste de contraintes ?

3.3 Résolution

On suppose qu'une grille de sudoku est donnée par une matrice $M = (m_{i,j})$ ayant ses coefficients déjà fixés dans $[\![1,9]\!]$ et les autres, non encore connus, mis à zéro. On suppose qu'il existe une seule solution à ce sudoku.

Comment connaître la valeur que doit prendre $m_{i,j}$? Que se passe-t-il si la grille proposée n'a pas de solutions ?

Indications. On sait quelles sont les contraintes (polynomiales) à appliquer à $M_{i,j}$...

Appliquer ce qui précède à la grille suivante en écrivant une procédure **SudokuSolve** prenant en entrée une matrice à coefficients dans $[\![0,9]\!]$ et renvoyant la solution si elle existe et est unique, et un message d'erreur approprié sinon :

		8	4				3	
				1		8		4
					7			1
7		1	2			4	8	
8			6		1			
	2	6			8	5		7
2			3					
9		3		2				
4	8				5	2		

4 Cas d'application des bases de Grobner : cryptographie

4.1 HFE

1). 1988 : MATSUMOTO-IMAI on fait une trap sur MQ (appelé C^*)

2). 1995 : attaque de PATARIN

3). 1996 : HFE, PATARIN répare C^*

On note $\varphi\colon \mathbb{F}_{q^n} \to (\mathbb{F}_q)^n$ une bijection (qui préserve la structure de F_q espace vectoriel).
Soit

$$\begin{array}{rccc} P\colon & \mathbb{F}_{q^n} & \to & \mathbb{F}_{q^n} \\ & X & \mapsto & \sum_{i=0}^{r} \lambda_i X^i \end{array}$$

où $\lambda_i \in \mathbb{F}_{q^n}$ et r sont fixés.
On choisit deux bijections affines sur $(\mathbb{F}_q)^n$.

$$\begin{array}{rccc} S\colon & (\mathbb{F}_q)^n & \to & (\mathbb{F}_q)^n \\ & x & \mapsto & Ax+v \end{array}$$

La fonction S est bijective dès que A est inversible, et A est à coefficients dans $\mathbb{F}_q$.
Soit T une autre bijection affine $(\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$.
La trappe pour MQ est le triplet P, S, T.

MQ : On va considérer la composition $T \circ P \circ S$.

1). Soit $x = (x_1, \cdots, x_n) \in \mathbb{F}_q^n$ un message de base.

2). On applique S : $S(x)$

3). On applique P : $P(\varphi^{-1}(S(x)))$

4). Puis on applique T : $T(\varphi(P(\varphi^{-1}(S(x)))))$.

Chiffrement : $T(P(S(x)))$.
Déchiffrement :

1). Calcul des c tels que $T^{-1}(c) = P(S(x))$.

2). Calcul des racines de $P - T^{-1}(c)$ (notées $y_1, \cdots, y_k$). (Calcul que l'on peut faire avec Berlekamp)

3). Calcul de $S^{-1}(y_1), \cdots, S^{-1}(y_k)$, le message clair est dans cette liste.

Pour savoir quel est le bon clair, on rajoute une entête connue : $\_KEY\_|\_\_\_128\_\_\_$
Pour que $T(P(S(x)))$ soit MQ, il faut que les équations quand elles passent dans P deviennent quadratiques. Pour cela on prend P de la forme

$$P = \sum_{0 \le i \le j \le r} \lambda_{i,j} X^{q^i+q^j} + \sum_{0 \le i \le r} \mu_i X^{q^i}$$

Si $X \in \mathbb{F}_{q^n}$, on peut l'écrire sous la forme $X = x_1 + x_2\alpha + \cdots + x_n\alpha^{n-1}$ avec $\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha]$ et $x_i \in \mathbb{F}_q$. En particulier, on a $x_1^q = x_1$, et donc

$$\begin{array}{rcc} X^{q^i+q^j} = & & (x_1 + x_2\alpha + \cdots + x_n\alpha^{n-1})^{q^i+q^j} \\ = & & (x_1 + x_2\alpha + \cdots + x_n\alpha^{n-1})^{q^i}(x_1 + x_2\alpha + \cdots + x_n\alpha^{n-1})^{q^j} \\ = & & (x_1 + x_2\alpha^{q^i} + \cdots + x_n(\alpha^{n-1})^{q^i})(x_1 + x_2\alpha^{q^j} + \cdots + x_n(\alpha^{n-1})^{q^j}) \end{array}$$

Comme les $(\alpha^\ell)^{q^i}$) s'expriment de nouveau en fonction des α^l, on déduit de l'écriture $X^{q^i+q^j}$ est un polynôme de degré 2 en fonction des x_k. De même X^{q^i} est un polynôme de degré 1 en fonction des x_k.

Sous l'hypothèse que la composition par S et T rend le système HFE indiscernable d'un système aléatoire, alors attaquer HFE revient à résoudre le système MQ.

$$\begin{cases} f_1(x_1, \cdots, x_n) & = y_1 \\ \cdots & \\ f_m(x_1, \cdots, x_n) & = y_m \end{cases}$$

Il s'agit donc de calculer une base de Grobner de $f_1 - y_1, f_2 - y_2, \cdots, f_m - y_m$.

Si $m = n$ dans $\mathbb{F}_2$, le dsol a, en général, une structure en escalier (montant) (en fonction de n). (CF thèse de Magali Bardet).

Pour HFE, la structure des équations fait que le dsol reste constant à partir d'un certain moment (Faugère 1998, Joux 2002).

En 1999 : Kipris-Shamir, attaque algébrique contre HFE via Minrank

Voir

- thèse Courtois pour NP-complétude de Minrank

- réparations de HFE : HFE$^-$1, HFE OV, UOV, Rainbow (3eme round du NIST avant une attaque avec Minrank, W BENLLENS 2022)

5 Polycracker

On va décrire un cryptosystème générique, basé sur la difficulté à trouver la solution d'un système polynomial. On se fixe $\mathbb{K}$ un corps fini. On suppose que Bob veut envoyer un message m à Alice. Alice choisit un vecteur aléatoire $a = (a_1, \cdots, a_n) \in \mathbb{K}^n$ (sa clef secrète) puis $s \geq 1$ et des polynômes aléatoires $f_1, \cdots, f_s \in K[X]$. Elle calcule alors les polynômes $g_i = f_i - f(a_1, \cdots, a_s)$ pour tout $i = 1, \cdots, s$. Les polynômes $(g_1, \cdots, g_s)$ serviront à Alice de clef publique.

Chiffrement et déchiffrement : Bob choisit des polynômes aléatoires $(h_1, \cdots, h_s) \in K[X]$ et envoie à Alice le message codé $c = m + h_1 g_1 + h_2 g_2 + \cdots + h_s g_s$. Afin de déchiffrer le message, Alice évalue c en $a_1, \cdots, a_n$, et obtient le message original m.

1). On se place ici dans $\mathbb{K} = \mathbb{F}_2$. Alice choisit $n = 2$, $a = (1, 0)$, et $f_1 = x^3 + xy + y$, $f_2 = x^2 + xy^3 + xy^2$.

   1). Quels sont les polynômes g que va utiliser Alice comme clef publique ?

   2). Si Bob choisit $h_1 = x$ et $h_2 = y + 1$ et veut envoyer comme message $m = 1$, quel message enverra-t-il à Alice ?

2). En remarquant qu'on peut retrouver le message m si on arrive à trouver le z tels que $c - z \in \langle g_1, \cdots, g_s \rangle$, proposer une attaque de Polly Cracker basé sur le calcul de base de Gröbner. Pourquoi n'y a-t-il qu'un tel z ?

3). On suppose que la clef publique d'Alice est composées des polynômes $g_1 = y+1$ et $g_2 = x^2+xy^2+y^3+1$. Bob lui envoie le polynôme $c = x^3 + x^2y + xy^4 + x + y^5 + y^4 + y^3 + y$. Sachant que le système utilisé est Polly Cracker sur $\mathbb{F}_2$, retrouver le message de Bob (l'élément de $\mathbb{F}_2$ qui a été envoyé).

Solution

1). Si on calcule la base de Grobner de l'idéal engendré $(g_1, \cdots, g_s)$ et ensuite on calcule la réduction de c modulo cette base de Gröbner et cette réduction donne l'entier $z = m$ que l'on cherche.

2). On calcule le S-polynôme de g_1 et g_2, $S = g_1 x^2 + y g_2 = x^2 + xy^3 + y^4 + y$. On vérifie que la division mutivariée de S par g_1, g_2 donne 0, donc (g_1, g_2) est déjà une base de Gröbner. On calcule ensuite la réduction de c modulo cette base de Gröbner, ce qui revient à transformer tous les x^2 en $xy^2 + y^3 + 1$ et tous les y en 1. On trouve $c = 0$ modulo l'idéal engendré par (g_1, g_2). Donc $c = 0$.