Avancées sur un problème d'isomorphisme de polynômes et pinceaux de formes quadratiques

G. Macario-Rat[1], **J. Plût**[2], H. Gilbert[3]

[1]Orange Labs, gilles.macario-rat@orange.fr

[2]ANSSI, jerome.plut@ssi.gouv.fr

[3]ANSSI, henri.gilbert@ssi.gouv.fr

2014-01-31

Isomorphisme de polynômes à un secret

On fixe un corps k et l'algèbre $k[x_1, \ldots, x_n]$ des polynômes en n variables.

Definition (Familles de polynômes isomorphes)

Deux familles de polynômes $(a_1, \ldots, a_m)$ et $(b_1, \ldots, b_m)$ sont *isomorphes* si elles sont reliées par un changement de variables linéaire bijectif s :

$$a_i(x_1, \ldots, x_n) = b_i(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)).$$

Application cryptographique : protocole d'identification de [Patarin 1996]. Les familles a, b sont publiques, et s est le secret. Pour prouver la connaissance de s :

- le prouveur construit un changement de variables linéaire aléatoire t et divulgue $c = a \circ t$;
- le vérifieur demande aléatoirement un isomorphisme entre c et a, ou entre c et b.

Paramètres du problème IP1S

m	Nombre de polynômes	(1 ou 2)
n	Nombre de variables	(grand)
d	Degré des polynômes	(2 ou 3)
k	Corps de base	Caractéristique ?

- Le problème IP1S est plus facile (surdéterminé) avec plus de deux polynômes.
- La taille de la clé publique dépend du nombre de polynômes et de leur degré.
- La complexité des attaques dépend du nombre de variables.

Nous considérons le cas de **deux polynômes homogènes quadratiques** sur un corps de **toute caractéristique**.

Algorithmes précédents

- [Bouillaguet, Faugère, Fouque, Perret 2011] : transforment le problème en un système quadratique + linéaire surdéterminé.
  - Résolvent expérimentalement (Gröbner) en temps $\widetilde{O}(n^6)$.
  - Cassent toutes les tailles de paramètres proposées par [Patarin 1996] pour le cas quadratique.

q	n
2	16
2^4	6
2	32

- Ce travail : utilise des théorèmes de structure sur les (paires de) formes quadratiques pour les ramener à une forme canonique.
  - Utilise essentiellement de l'algèbre linéaire ou polynomiale (pas de base de Gröbner).
  - Traitement spécifique pour la caractéristique 2.

IP1S quadratique : le cas $m = 1$

Cas stupide : **un seul** polynôme.

- Le cas $m = 1$ correspond à calculer un isomorphisme entre deux formes quadratiques en n variables.
- À une forme quadratique q, on associe la *forme polaire* b définie par

$$b(x, y) = q(x + y) - q(x) - q(y).$$

- C'est une forme bilinéaire symétrique, reliée à q par l'*équation de polarité* :

$$2\,q(x) = b(x, x).$$

- Si $2 \neq 0$ dans K, les formes quadratiques sont en bijection avec les formes bilinéaires symétriques. Toute forme quadratique régulière est isométrique à une forme diagonale $(1, \ldots, 1)$ ou $(1, \ldots, 1, \delta)$, où δ n'est pas un carré.

Pinceaux de formes bilinéaires

Cas de **deux** polynômes (a_∞, a_0)

- Un *pinceau bilinéaire* est une droite projective dans l'espace des formes bilinéaires :

$$\lambda \longmapsto b_\lambda = b_0 + \lambda b_\infty. \tag{1}$$

  Il est dit

  dégénéré si, pour tout λ, $\det b_\lambda = 0$;

  régulier si l'une des formes (par exemple b_∞) est régulière (= inversible).

- Tout pinceau est la somme directe d'un pinceau non-dégénéré et d'un pinceau nul.
- On peut supposer que le pinceau non-dégénéré est régulier (quitte à procéder à une (petite) extension des scalaires).

Isomorphisme de pinceaux réguliers bilinéaires

- Soit $b_\lambda = b_\infty \lambda + b_0 = b_\infty(\lambda + m_b)$ un pinceau bilinéaire régulier ; $m_b = b_\infty^{-1} b_0$ est l'*endomorphisme caractéristique* de b.
- Un isomorphisme entre (a_λ) et (b_λ) est une application linéaire bijective s telle que ${}^t s \cdot a_\lambda \cdot s = b_\lambda$, soit encore

$$ {}^t s \cdot a_\infty \cdot s = b_\infty \qquad \text{et} \qquad s^{-1} \cdot m_a \cdot s = m_b. $$

- Si (a_λ) et (b_λ) sont isomorphes, alors quitte à effectuer un changement de base sur b, on peut supposer $m_a = m_b$.
- Le problème IP1S devient :

$$ {}^t s \cdot a_\infty \cdot s = b_\infty \qquad \text{et} \qquad s \text{ commute avec } m, $$

où a_∞, b_∞, $a_\infty m$, $b_\infty m$ sont symétriques.

Isomorphisme de pinceaux bilinéaires : le cas cyclique

L'endomorphisme m est *cyclique* si son polynôme minimal est égal à son polynôme caractéristique. Dans ce cas :

- Le commutant de m est réduit à l'algèbre de polynômes $k[m]$.
- Puisque $a_\infty\, m = {}^t m\, a_\infty$, toute s commutant à a_∞ vérifie la même relation $a_\infty\, s = s\, a_\infty$.
- L'équation de IP1S ${}^t s\, a_\infty\, s = b_\infty$ se simplifie en $a_\infty\, s^2 = b_\infty$.
- Il suffit de calculer une racine carrée de $a_\infty^{-1} b_\infty$ dans l'algèbre $k[m]$, ce qui est facile si k est fini.

IP1S cyclique en caractéristique impaire

Théorème (Résolution de IP1S cyclique en caractéristique impaire)

Soient k un corps fini de caractéristique impaire et (a_λ), (b_λ) deux pinceaux de formes quadratiques de dimension n sur k, isomorphes et cycliques. Il est possible de calculer un isomorphisme entre (a_λ) et (b_λ) en $\widetilde{O}(n^3)$ opérations dans k.

- Remplacer b par b' telle que $m = m_b = m_{b'}$.
- Calculer et factoriser le polynôme mimimal de m.
- Calculer les racines carrées de $a_\infty^{-1} b_\infty$ dans les corps résiduels de $k[m]$.
- Relever (Hensel) aux localisations de $k[m]$.
- Recoller (restes chinois).

De plus, on connaît le nombre de solutions.

Expérimentalement (instances aléatoires)

q	n	t (s)	% cyclic
3	80	5	87
3	128	34	88
3^{10}	32	15	100

q	n	t (s)	% cyclic
5	20	0.07	95
5	32	0.28	95
5	80	7	95

q	n	t (s)	% cyclic
7^6	32	11	100
65537	8	0.04	100
65537	20	1	100

- Opteron 850 2.2 GHz, 32 GB RAM.
- MAGMA version 2.13-15.

Formes quadratiques en caractéristique deux

- Si $2 = 0$ dans k, l'identité de polarité devient $b(x, x) = 0$: la forme polaire est une forme bilinéaire **alternée**.
- L'application de polarité n'est plus une bijection entre les formes quadratiques et bilinéaires.
- En général, on peut écrire une forme quadratique comme somme directe

$$\underbrace{(\text{forme quadratique régulière})}_{\text{dimension paire}} \quad \oplus \quad (\text{somme de carrés}).$$

- La somme de carrés est facile (semi-linéaire). On travaille donc sur les formes quadratiques régulières.
- On décrit tous les isomorphismes entre les pinceaux polaires, et on cherche à résoudre les équations données par leur action sur les coefficients diagonaux.

Pinceaux de formes bilinéaires alternées

Tout pinceau de formes bilinéaires alternées admet une base dans laquelle il a pour matrice

$$A_\infty = \begin{pmatrix} 0 & T \\ T & 0 \end{pmatrix}, \quad A_0 = \begin{pmatrix} 0 & TM \\ TM & 0 \end{pmatrix},$$

où T est une matrice inversible telle que T et TM soient symétriques.

- L'endomorphisme M est le *Pfaffien* de (A_λ). La matrice T ne dépend que de M.
- Si deux pinceaux (A_λ), (B_λ) sont isomorphes, on peut supposer que leurs pinceaux polaires sont égaux et de la forme ci-dessus.
- Le pinceau est dit *cyclique* si M est cyclique.

Automorphismes des pinceaux alternés

Théorème (Structure du groupe orthogonal)

Le groupe d'automorphismes d'un pinceau de formes bilinéaires alternées cyclique est engendré par les matrices

$$G_1(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \quad G_2(x) = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix},$$
$$G_3(x) = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}, \quad G_4 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

pour $x \in k[M]$.

Plus précisément, on a une décomposition LU : tout automorphisme (positif) est de la forme

$$G_2(y)G_3(u)G_1(x)$$

pour $x, y \in k[M]$ et $u \in k[M]^\times$.

Localisation du problème

- Quitte à factoriser le polynôme minimal de M, on suppose qu'il est de la forme f_0^d, où f_0 est irréductible.
- Dans ce cas, la matrice M est semblable à la matrice $\begin{pmatrix} M_0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & \\ & & & 1 \\ 0 & & & M_0 \end{pmatrix}$, où M_0 est la matrice compagnon de f_0.
- En général : extension des scalaires au corps $k[M_0]$. Pour simplifier : on présente uniquement le cas où $f_0 = 1$ (et donc M_0 est la matrice (0)). Dans ce cas, T est la matrice anti-identité.

Représentation algébrique de la diagonale

Pour toute matrice $A = (a_{i,j})$ de taille $d \times d$, on note

$$\psi(A) = \sum a_{i,i} M^{i-1} \quad \in R = k[M]/M^d.$$

La restriction de ψ aux matrices diagonales les met en bijection avec l'algèbre $R = k[M]$.

Action du groupe orthogonal sur les coefficients diagonaux

- Soient A une matrice diagonale, $x = \sum x_i M^i \in k[M]$, et $A' = {}^t\!xAx$. Alors :
$$\psi(A') \;=\; \varphi(x)\,\psi(A) \;=\; (\sum x_i^2 M^i)\psi(A).$$
- Soit $\theta(x) = \psi(TX)$; alors
$$\theta(x) = \psi(TX) = \sum x_{d-1-2i} M^{d-1-i}.$$

Action du groupe orthogonal sur les coefficients diagonaux

Le problème IP1S se ramène à : étant données M et T, classifier les matrices de la forme

$$\begin{pmatrix} A_1 & T \\ 0 & A_2 \end{pmatrix}, \begin{pmatrix} A_3 & TM \\ 0 & A_4 \end{pmatrix}$$

où les A_i sont des matrices diagonales.

Théorème

Soit $\alpha_i = \psi(A_i)$. L'action des matrices $G_1(x)$, $G_2(x)$, $G_3(x)$ sur les coefficients diagonaux est donnée par :

$$\begin{aligned}
G_1(x): &\quad \alpha_2 \longleftarrow \alpha_2 + \varphi(x)\,\alpha_1 + \theta(x), \quad \alpha_1 \longleftarrow \alpha_1;\\
G_2(x): &\quad \alpha_1 \longleftarrow \alpha_1 + \varphi(x)\,\alpha_2 + \theta(x), \quad \alpha_2 \longleftarrow \alpha_2;\\
G_3(x): &\quad \alpha_1 \longleftarrow \varphi(x)\,\alpha_1, \quad \alpha_2 \longleftarrow \varphi(x^{-1})\,\alpha_2;\\
G_4: &\quad \alpha_1 \leftrightarrow \alpha_2.
\end{aligned}$$

Équations locales pour IP1S

Soit $s = G_2(x)\, G_3(\varphi^{-1}(u^{-1}))\, G_1(y)$ une application orthogonale (positive). Le problème IP1S se ramène au système de **quatre équations semi-linéaires** en x, y, u :

$$
\begin{aligned}
u\alpha_1' &= \alpha_1 + \alpha_2\varphi(x) + \theta(x),\\
u\alpha_2 &= \alpha_2' + \alpha_1'\varphi(y) + \theta(y),\\
u\alpha_3' &= \alpha_3 + \alpha_4\varphi(x) + \theta(M\,x),\\
u\alpha_4 &= \alpha_4' + \alpha_3'\varphi(y) + \theta(M\,y).
\end{aligned}
$$

Résolution locale de IP1S

On peut éliminer u pour se ramener à un système en les deux inconnues x et z :

$$\begin{cases} \alpha\varphi(z) + \theta(z) = C, \\ \alpha\gamma\varphi(x) + \beta\theta(x) + \theta(Mx) = C', \\ \gamma\theta(x) + \beta\theta(z) + \theta(Mz) = C''. \end{cases}$$

- φ est bijective et conserve la valuation dans $k[M]$; θ est une application (presque) contractante.
- Si $\alpha\gamma (= \alpha_1\alpha_4 + \alpha_2\alpha_3)$ est inversible dans $k[M]$, le théorème du point fixe permet de résoudre le système en $O(d)$ étapes.
- Dans le cas général : en étudiant des équations de la forme $M^e\varphi(x) = a\,\theta(x) + b$, on peut résoudre en $O(d)$ étapes.

Résolution de IP1S cyclique en caractéristique deux

Théorème (IP1S cyclique en caractéristique 2)

Soient k un corps binaire et (A_λ), (B_λ) deux pinceaux de formes quadratiques sur k^n, isomorphes et cycliques. Il est possible de calculer un isomorphisme entre (A_λ) et (B_λ) en au plus $\widetilde{O}(n^3)$ opérations dans k.

- Calculer et factoriser les polynômes caractéristiques.
- Décomposition primaire des deux pinceaux.
- Résolution des équations locales (théorème de point fixe).
- Assemblage (restes chinois).

De plus, il est raisonnable de compter les solutions du problème.

Expérimentalement (instances aléatoires

q	n	t (s)	% cyclic
2	32	0.07	96
2	128	2	95
2	256	33	94
2^4	32	0.3	100
2^7	32	0.5	100

(Note : en général, le déterminant $\alpha_1\alpha_4 + \alpha_2\alpha_3$ est inversible dans $k[M]$, et la résolution locale est dominée par le théorème du point fixe).

Conclusion

Dans le cas cyclique :

- Preuve de la polynomialité de IP1S en toute caractéristique.
- Complexité dominée par l'algèbre linéaire et polynomiale.
- Utilise la classification des formes quadratiques.

Travail récent :

- Cas non-cyclique (caractéristique impaire).
- IP2S.

Restent à faire :

- Le cas non-cyclique en caractéristique 2.
- Le cas de $m \geqslant 3$ formes quadratiques.
- Les équations cubiques...