有限域上置换正交系的算法判别

陆佩忠
(中国科学院系统科学研究所, 北京 100080)

摘要 将有限域上置换正交组化成仿射代数之间的同态, 然后利用 Gr└bner 基理论给出置换正交组的算法判别.

关键词 置换多项式 正交系 代数族 Gr└bner 基

本文将在密码中有重要应用的置换正交组转化成代数族之间的多项式映射, 进而转化成仿射代数间的同态, 从而利用约化 Gr└bner 基得到置换正交组的简明的判别准则.

有限域上的置换多项式(简记为 PP (Permutation polynomial)) 和相应的正交组(简记为 OS(Orthogonal system)) 在密码学和组合数学中有重要的应用, 因而有丰富的研究内容[1, 2]. 然而要判别一个多项式是否是一个 PP 和判别一组多元多项式是否是一个 OS, 除了穷尽代入计算外尚无更好的方法. 现将定义和已有的结果简叙如下, 以方便使用和对比. 设 $q = p^e$, p 是素数, $F_q[x_1, \cdots, x_n]$ 是 F_q 上多变元多项式环, 设整数 $n > 1$, $1 \leqslant k \leqslant n$, 称 $F_q[x_1, \cdots, x_n]$ 中的 k 个多项式 $f_1(x_1, \cdots, x_n), \cdots, f_k(x_1, \cdots, x_n)$ 是一正交系, 如果对任 $(b_1, \cdots, b_k) \in F_q^k$, 方程组

$$\begin{aligned} f_1(x_1, \cdots, x_n) &= b_1, \\ &\vdots \\ f_k(x_1, \cdots, x_n) &= b_k \end{aligned} \tag{1}$$

恰有 q^{n-k} 个解. 此时, 当 $k = 1$ 时, 称 n 变元多项式 $f(x_1, \cdots, x_n)$ 是 n 变元置换多项式. 对正交系的判别有如下的结果:

定理 1 (Hermite-Dickson 判别, 参见文献[1], Thm. 7.6, Thm. 7.41) 多元多项式组 $f_1, \cdots, f_n \in F_q[x_1, \cdots, x_n]$ 是正交系当且仅当如下两条件满足:

( ) 剩余多项式

$$f_1^{q-1} \cdots f_n^{q-1} \bmod (x_1^q - x_1, \cdots, x_n^q - x_n)$$

的 $x_1^{q-1} \cdots x_n^{q-1}$ 项系数 $\neq 0$;

( ) 剩余多项式

$$f_1^{t_1} \cdots f_n^{t_n} \bmod (x_1^q - x_1, \cdots, x_n^q - x_n)$$

的 $x_1^{q-1} \cdots x_n^{q-1}$ 项系数是 0, 对任意 $0 \leqslant t_i \leqslant q-1$, $0 \leqslant i \leqslant n$, 且 t_i 不全为 $q-1$ 和不全为 $t_i \neq 0 \pmod p$.

注意: ( ) Hermite 判别法只适合于 $k = n$ 的正交系. 对 $1 \leqslant k < n$ 的多项式组, 给出类似的 Hermite 判别, 这是一个未解决的问题, 见 Mullen[2] 文中的 Open 问题 1, 2. ( ) 该判别法需要几乎穷尽 q^n 次个多项式的乘积剩余, 显然是很复杂的, 特别是当 q 很大时, 但好处是算法中无需存储. 如果根据定义直接进行 q^n 次验证, 显然速度更快, 但需要 q^k 个字长 $(n-k)\log_2 q$ 的存储器.

本文首先将研究 PP 和 OS 问题转化成研究代数几何中代数族之间的映射, 由代数几何基本知识知, 该问题等价于研究仿射代数的同态. 为此, 本文利用 Gr$\ddot{o}$bner 基研究该同态的同态核、同态象, 从而得到 OS 的简洁可行的判别准则.

1 代数族映射与 Gr$\ddot{o}$bner 基

设 $\bar{k} \supseteq k = F_q$ 是 F_q 的代数封闭域, 则易知

$$k^n = V_{\bar{k}}(x_1^q - x_1, \cdots, x_n^q - x_n) = \{(a_1, \cdots, a_n) \in \bar{k}^n \mid a_i^q - a_i = 0,\ 0 \leqslant i \leqslant n\},$$

因而 F_q^n 是一个代数族. 设 $V \subseteq \bar{k}^n$, $W \subseteq \bar{k}^m$ 是两个代数族, 映射 α

$$\alpha: V \to W$$

$$(a_1, \cdots, a_n) \mapsto (f_1(a_1, \cdots, a_n), \cdots, f_m(a_1, \cdots, a_n)),$$

这里 $f_1, \cdots, f_m \in k[x_1, \cdots, x_n]$. 这时称 α 为代数族的多项式映射. 设 V 是 $\bar{k}^n$ 的子集, 记

$$I(V) = \{f(x_1, \cdots, x_n) \in k[x_1, \cdots, x_n] \mid f(a_1, \cdots, a_n) = 0,$$
$$\text{对任意}(a_1, \cdots, a_n) \in V\}.$$

由代数几何知识知:

引理 1 代数族多项式映射 α 可引导出仿射 k 代数间的同态

$$\alpha^*: k[y_1, \cdots, y_m]/I(W) \to k[x_1, \cdots, x_n]/I(V),$$
$$y_i + I(W) \mapsto f_i + I(V),$$

且 α 是映上的当且仅当 α^* 是单同态. α 是单射的当且仅当 α^* 是满同态. α 是多项式双射当且仅当 α^* 是 k 代数同构. 而且仿射 k 代数间的任一同态 α^* 必是由代数族间的多项式映射 α 导出.

证明由文献[4] 中 p. 239 命题 8 便知, 故略.

设 I, J 分别是 $k[x_1, \cdots, x_n]$ 和 $k[y_1, \cdots, y_m]$ 的理想, $f_1, \cdots, f_m$ 是 $k[x_1, \cdots, x_n]$ 的 m 个多项式, 且有 $J = \langle g_1, \cdots, g_t \rangle$ 和关系 $g_i(f_1, \cdots, f_m) \in I$, 则可定义如下的 k 代数同态

$$\phi: k[y_1, \cdots, y_m]/J \to k[x_1, \cdots, x_n]/I,$$
$$y_i + J \mapsto f_i + I,$$

设 $K = \langle I, y_1 - f_1, \cdots, y_m - f_m \rangle$ 是 $k[y_1, \cdots, y_m, x_1, \cdots, x_n]$ 中的理想, 设 "$<$" 是该多项式环的单项上消去序, 且 $Y < X$. 设 G 是 K 在该序下的约化 Gr$\ddot{o}$bner 基, 则有如下结论:

引理 2) $\ker(\phi) = \langle G \cap k[y_1, \cdots, y_m] (\mathrm{mod} J) \rangle$;

) $img(\phi) = \left\{ f + I \in k[x_1, \cdots, x_n]/I \mid \exists\, h \in k[y_1, \cdots, y_m],\ f \xrightarrow{G}_+ h \right\}$;

) ϕ 是映上当且仅当对 $i = 1, \cdots, n$, 存在 $g_i = x_i - h_i \in G$, 这里 $h_i \in k[y_1, \cdots, y_m]$.

证明参见文献[3] 中定理 2. 4. 10.

引理 3 $I(F_q^n) = \langle x_1^q - x_1, \cdots, x_n^q - x_n \rangle$.

证 显然只要证明 $I(F_q^n) \subset \langle x_1^q - x_1, \cdots, x_n^q - x_n \rangle$. 设"$<$"是字典序且 $x_1 < \cdots < x_n$, 则显然 $\{x_1^q - x_1, \cdots, x_n^q - x_n\}$ 是理想 $\langle x_1^q - x_1, \cdots, x_n^q - x_n \rangle$ 的 Gr$\ddot{o}$bner 基. 若 $f \in I(F_q^n)$, 现欲证 $f \in \langle x_1^q - x_1, \cdots, x_n^q - x_n \rangle$, 即 $f \xrightarrow{G}_+ 0$. 故设 f 已被 G 约成标准型, 即 $\deg_{x_i} f < q$, $i = 1, \cdots, n$. 现对 n 作归纳法. 当 $n = 1$ 时, 由于 $x_1^q - x_1$ 无重根, 故结论成立. 设 $n - 1$ 时成立. 将 f 写成

$$f = f_0 + f_1 x_n + \cdots + f_t x_n^t,$$

其中 $f_t \neq 0$, $0 \leqslant t < q$, $f_i \in F_q[x_1, \cdots, x_{n-1}]$, 对任意 $(a_1, \cdots, a_{n-1}) \in F_q^{n-1}$ 取定, 则 $f(a_1, \cdots, a_{n-1}, x_n) \in I(F_q) = \langle x_n^q - x_n \rangle$, 此时 $f(a_1, \cdots, a_{n-1}, x_n)$ 已约化, 故 $f(a_1, \cdots, a_{n-1}, x_n) = 0$, 所以 $f_i(a_1, \cdots, a_{n-1}) = 0$, 由于 $f_i \bmod(\langle x_1^q - x_1, \cdots, x_{n-1}^q - x_{n-1} \rangle)$ 也已约化, 由归纳假设知 $f_i = 0$, $i = 1, \cdots, t$, 从而 $f = 0$.

定理 2 设 $\alpha = (f_1, \cdots, f_n)$, 其中 $f_i \in F_q[x_1, \cdots, x_n]$, G 是 $F_q[x_1, \cdots, x_n, y_1, \cdots, y_n]$ 中的理想 $\langle y_i - f_i, x_i^q - x_i \mid i = 1, \cdots, n \rangle$ 在序 $y < x$ 下的约化 Gröbner 基. 则 α 是一个多项式正交系当且仅当 $G = \{x_1 - h_1, \cdots, x_n - h_n\}$, 这里 $h_i \in F_q[y_1, \cdots, y_n]$.

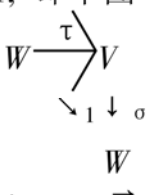
注 1 当 $\alpha = (f_1, \cdots, f_n)$ 是多项式正交系时, $(h_1, \cdots, h_n)$ 恰好是逆多项式正交系.

$$f_i(h_1, \cdots, h_n) = y_i, \quad i = 1, \cdots, n,$$

$$h_i(f_1, \cdots, f_n) = x_i, \quad i = 1, \cdots, n.$$

2 利用相伴内射判别正交系

设 $W \subseteq k^n$, $V \subseteq k^m$ 是两个代数族. 若 $\sigma: V \to W$ 是代数族之间的映上的多项式映射, 则存在多项式单射 $\tau: W \to V$, 使得 $\sigma \cdot \tau = 1$, 即下图可交换:



设 $V = F_q^n$, $W = F_q^m$, 给定多项式映射 $\sigma: V \to W$, 令:

$$\Gamma_\sigma = \{\tau: W \to V \mid \sigma \cdot \tau = 1\},$$

则称 Γ_σ 是与 σ 相伴的单射集. 设 σ 是一个多项式映射, 且

$$\sigma = (f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)).$$

定理 3 σ 是多项式正交系当且仅当 $|\Gamma_\sigma| = q^{(n-m)q^m}$.

证 对任 $a \in W$, $a = (a_0, \cdots, a_{m-1})$, $a_i \in F_q$. 把 a 看成是一个 q 进制的整数. 设

$$M_a = \{b \in V \mid \sigma(b) = a\},$$

$n_a = |M_a|$, 则

$$V = \bigcup_{a=1}^{q^m} M_a,$$

且当 $a \neq b$ 时, $M_a \cap M_b = \emptyset$. 故有等式

$$\sum_{a=1}^{q^m} n_a = q^n. \tag{2}$$

对映射 τ, 欲使 $\sigma \cdot \tau = 1$ 当且仅当对任 $a \in W$, $\tau(a) \in M_a$. 故

$$|\Gamma_\sigma| = n_1 \cdots n_{q^m}. \tag{3}$$

当 σ 是 OS 时, $n_1 = \cdots = n_{q^m} = q^{n-m}$, 故由式(3)知 $|\Gamma_\sigma| = q^{(n-m)q^m}$.

反之, 若 $|\Gamma_\sigma| = q^{(n-m)q^m}$, 则

$$\begin{cases} \sum_{a=1}^{q^m} n_a = q^n, \\ |\Gamma_\sigma| = n_1 \cdots n_{q^m} = q^{(n-m)q^m}, \end{cases}$$

由几何平均不等式和算术平均不等式达到极值的条件知: $n_1 = \cdots = n_{q^m} = q^{n-m}$. 所以 σ 是一个 OS, 证毕.

设 $K_V = k[x_1, \cdots, x_n]/I(V)$, $K_W = k[y_1, \cdots, y_m]/I(W)$ 分别是代数族 V, W 对应的仿射 k 代数. $\tau^*: K_V \to K_W$, $\sigma^*: K_W \to K_V$, 是 k 代数同态. 设 $\mathrm{Hom}(K_V, K_W)$ 是 k 代数同态集.

$$\Gamma_{\sigma^*} = \{\tau^* \in \mathrm{Hom}(K_V, K_W) \mid \tau^* \cdot \sigma^* = 1\},$$

称 Γ_{σ^*} 是 σ^* 的相伴代数同态单射集. Γ_{σ^*} 是使下图交换的代数同态集:

$$\begin{array}{ccc} K_W & \xrightarrow{\sigma^*} & K_V \\ & \searrow_1 \downarrow \tau^* & \\ & & K_W \end{array}$$

推论 1 σ 是 OS 当且仅当其相伴代数同态单射集的阶 $|\Gamma_{\sigma^*}| = q^{(n-m)q^m}$.

3 算法判别

下面, 根据定理 2 给出置换正交系的判别算法, 为此, 先简要介绍 Gröbner 基理论, 详细内容参见文献[3].

在 $k[x_1, \cdots, x_n]$ 的单项集合上定义一个项序"<", 例如字典全序: $1 < x_1 < \cdots < x_n < x_1^2 < x_1x_2 < \cdots < x_n^2 < x_1^3 < \cdots$. 这样对于 $f \in k[x_1, \cdots, x_n]$, f 可表示成

$$f = a_1X^{\alpha_1} + a_2X^{\alpha_2} + \cdots + a_rX^{\alpha_r},$$

其中 $0 \neq a_i \in k$, $X^{\alpha_i} = x_1^{e_{i1}} \cdots x_n^{e_{in}}$, 整数 $e_i \geqslant 0$, 且 $X^{\alpha_1} > X^{\alpha_2} > \cdots > X^{\alpha_r}$.

定义 1 $lp(f) = X^{\alpha_1}$ 是 f 的首项积; $lc(f) = a_1$ 是 f 的首项系数; $lt(f) = a_1X^{\alpha_1}$ 是 f 的首项.

如果 G 是 $k[x_1, \cdots, x_n]$ 的子集, 记 $lt(G) = \{lt(g) \mid g \in G\}$. 设 I 是环 $k[x_1, \cdots, x_n]$ 的理想, 令 $Lt(I) = \langle lt(f) \mid f \in I \rangle$ 为 I 中多项式的首项在 $k[x_1, \cdots, x_n]$ 中生成的理想.

定义 2 设 I 是 $k[x_1, \cdots, x_n]$ 的理想, G 是 I 的子集. 如果 $\langle lt(G) \rangle = Lt(I)$, 则称 G 是 I 的 Gröbner 基.

定义 3 设 $0 \neq f, g \in k[x_1, \cdots, x_n]$, $L = \mathrm{lcm}(lp(f), lp(g))$, 则多项式

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

称之为 f 和 g 的 S 多项式.

计算 $k[X]$ 的每个理想的 Gröbner 基的关键步骤是消项. 给定 $k[x_1, \cdots, x_n]$ 中的任意两个多项式 f, h 和一个非全零多项式集合 $F = \{f_1, \cdots, f_t\}$, 如果 $h = f - (c_1X_1f_1 + \cdots + c_tX_tf_t)$, 其中 $c_i \in k$, X_i 是幂积项, 满足 $lp(f) = X_ilp(f_i)$, $lp(h) < lp(f)$, 则记为 $f \xrightarrow{F} h$. 如果存在 $h_i \in k[x_1, \cdots, x_n]$, $i = 1, \cdots, s$, 使得 $f \xrightarrow{F} h_1 \xrightarrow{F} \cdots \xrightarrow{F} h_s \xrightarrow{F} h$, 则记为 $f \xrightarrow{F}_+ h$.

下面给出判别一组多项式是否是 OS 的算法, 在算法中要用到的项序"<"是 $k[y_1, \cdots, y_n, x_1, \cdots, x_n]$ 的单项子集上的全字典项序, 且使得 $y_1 < \cdots < y_n < x_1 < \cdots < x_n$.

算法 1 判别多项式组是正交系的 Gröbner 基算法.

输入: $F=\{f_1, \cdots, f_n\}\subset k[x_1, \cdots, x_n]$.

输出: 判别 F 是 OS 与否.

初始化: $G:=\{y_1-f_1, \cdots, y_n-f_n, x_1^q-x_1, \cdots, x_n^q-x_n\}$, OS:= false,

$$\mathscr{G}=\{\{f, g\}\mid f, g\in G, \text{且} f\neq g\}.$$

WHILE $\mathscr{G}\neq\emptyset$ DO.

任取$\{f, g\}\in\mathscr{G}$,

$\mathscr{G}\leftarrow\mathscr{G}\setminus\{\{f, g\}\}$,

$S(f, h)\xrightarrow{G}_+ h$, 使得 h 约化.

IF $h\neq 0$ THEN,

$$\mathscr{G}=\mathscr{G}\cup\{\{u, h\}\mid u\in G\},$$

$$G:=G\cup\{h\}.$$

IF $x_i\in lt(G)$, $i=1, \cdots, n$ THEN OS:= true,

RETURN OS.

致谢 感谢导师刘木兰教授的鼓励和支持.

参 考 文 献

1 Lidl R, Niederreiter H. Finite Fields, London: Addison_Wesley Publishing Company, 1983

2 Mullen G L. Permutation polynomials over finite fields. In: Lecture Notes in Pure and Applied Mathematics, Vol 141, 1993. 131~ 151

3 Adams W W, Loustaunau P. An Introduction to Gröbner Bases. New York: American Mathematical Society, 1994

4 Cox D, Little J, O'Shea D. Ideals, Varieties and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra, New York: Springer_Verlag, 1992

(1997-03-27 收稿, 1998-02-26 收修改稿)

$Y_C\Omega_{2n}$是易项

赵希顺 王 驹④

(南京大学数学系, 南京 210093; ④中国科学院软件研究所, 北京 100080)

摘要 证明了如下结果: 对任意的 $n\geqslant 1$, $Y_C\Omega_{2n}$是易项, 即对任 λ项 M, $\lambda\beta+Y_C\Omega_{2n}=M$ 是协调的. 其中 Y_C 是 Curry 不动点组合子, $\Omega_{2n}=\omega_{2n}\omega_{2n}$, $\omega_{2n}=\lambda x.\, xx\cdots x$($\lambda x$ 之后 x 有 $2n$ 次出现). 从而, 部分证明了 Jacopini 提出的如下问题: 对任意的 $n\geqslant 2$, $Y_C\Omega_n$是易项.

关键词 $\lambda\beta$ 演算 Kuper 定理 易项

一项 Z 是易项如果对任意的闭项 Y 有 Con($\lambda\beta+Z=Y$) 成立, 即 $\lambda\beta+Z=Y$ 是协调的. 易项的概念由 Jacopini 于 1975 年首先引入, 他证明了 $\Omega\equiv(\lambda x.\, xx)(\lambda x.\, xx)$ 是易项, 之后有