齐次 F5 算法的简单终止性证明

潘森杉* 胡予濮 王保仓
(西安电子科技大学综合业务网国家重点实验室 西安 710071)

摘 要：自从F5算法提出以来，出现了一批基于标签的Gröbner基算法，它们使用了不同的选择策略且减少冗余多项式的准则也各不相同。为了满足正确终止性，这些算法的策略和准则必须满足一些一般的规律。根据这些规律，该文提出了一个框架，使大多数算法成为该框架的实例。随后，利用重写基的性质，得到了框架的简单正确终止证明。为了得到F5算法的简单证明，该文对F5算法的约化操作进行合理的化简。特别地，对于齐次F5算法，证明了其复杂的选择策略等价于按模序选择。这样，齐次F5算法就能看成框架的一个特例，从而得到了F5算法的简单证明。

关键词：密码学；Gröbner 基；标签；F5 算法；终止证明
中图分类号： TP309 **文献标识码**： A **文章编号**：1009-5896(2015)08-1989-05
DOI: 10.11999/JEIT141601

Simpler Termination Proof on Homogeneous F5 Algorithm

Pan Sen-shan Hu Yu-pu Wang Bao-cang
(*State Key Laboratory of Integrated Service Networks*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: Since the F5 algorithm is proposed, a bunch of signature-based Gröbner basis algorithms appear. They use different selection strategies to get the basis gradually and use different criteria to discard redundant polynomials as many as possible. The strategies and criteria should satisfy some general rules for correct termination. Based on these rules, a framework which include many algorithms as instances is proposed. Using the property of rewrite basis, a simple proof of the correct termination of the framework is obtained. For the simple proof of the F5 algorithm, the reduction process is simplified. In particular, for homogeneous F5 algorithm, its complicated selection strategy is proved equivalent to selecting polynomials with respect to module order. In this way, the F5 algorithm can be seen as an instance of the framework and has a rather short proof.

Key words: Cryptography; Gröbner basis; Signature; F5 algorithm; Termination proof

1 引言

Gröbner基与求解多元多项式系统密切相关。这一工具已应用于很多场景，例如编码理论、密码学乃至物理、生物等自然科学领域。Buchberger于1965年提出了第1个Gröbner基求解算法[1]。Faugère提出了基于线性代数的F4算法[2]和基于标签的F5算法[3]。尽管在文献[3]中，F5算法的正确终止证明是错误的，但F5算法仍是当今最高效的Gröbner基求解算法之一。其巧妙地利用标签去消除冗余的计算。运用这个想法，最近几年学者们提出了其它基于标签的算法：Arri-Perry(AP)[4],Gao-Guan-Volny(G^2V)[5], Gao-Volny-Wang(GVW)[6] 和 Gao-Volny-Wang-Huang-Stroomer(GVWHS)[7]。它们都使用了Buchberger风格，但它们似乎又与F5算法截然不同。2011年，文献[8]给出了F5算法的正确性证明，并把其终止性证明留作一个公开问题。这一公开问题在文献[9]中也被认为是困难的。本文作者在文献[10]中给出了齐次F5的终止性证明，但其设计的框架只适用于增量型算法，不具有一般性。通过把算法的准则改写成二元序关系，文献[11]给出了一个一般算法的简单证明。然而，它没有解决F5的终止性问题。为了满足正确终止性，这些算法的策略和准则必须满足一些一般的规律。根据这些规律，本文给出了基于标签算法的一般框架，使得这些算法都被包含入框架之中。严格地说，这一框架不是一个算法，因其部分操作没有具体确定。本文研究这一框架的正确性和终止性，从理论上给出了一个简单证明。这就意味着，上述F5类算法的正确性和终止性都同时得到了证明。也就是说，对于任意的多项式组，这一类算法都能在有限的时间内算出正确的

2014-06-23 收到，2015-04-24 改回，2015-06-08 网络优先出版
国家自然科学基金(61173151, 61173152)资助课题
*通信作者：潘森杉 pansenshan@gmail.com

Gröbner基。只要遵循框架的基本要求，设计出来的算法都正确。这一结论对于指导设计更高效Gröbner基求解算法来说是非常重要的。与文献[10]的证明相比，本文利用重写基的性质，极大化简了证明过程。为了得到F5算法的简单证明，本文对F5算法的约化操作进行合理的化简。特别地，对于齐次F5算法，本文证明了其复杂的选择策略等价于按模序选择。这样，齐次F5算法就能看成框架的一个特例，从而得到了F5算法的简单证明。

2 预备知识

令 $\mathcal{R}=\mathcal{K}[x_1,x_2,\cdots,x_n]$ 为域 $\mathcal{K}$ 上的 n 变量多项式环，$\mathcal{M}$ 为单项式 $\left\{\prod_{i=1}^{n}x_i^{a_i}\mid a_i\in\mathcal{N}\right\}$。$\le$ 记为 $\mathcal{M}$ 上的可允许单项式序，那么 $\mathcal{R}$ 上的任意非零多项式 p 就能唯一地表示成有序单项式组合：$p=\sum_{a\in A}c_ax^a$，其中 $c_a\in\mathcal{K}\setminus\{0\}$，$x^a\in\mathcal{M}$，$A$ 为 $\mathcal{N}^n$ 上的一个有限集。$\mathrm{HM}(p)$（相应地，$\mathrm{HT}(p)$，$\mathrm{HC}(p)$）叫做 p 关于 $\le$ 的首单项式(相应地，首项，首项系数)。若两个多项式 p 和 q 使得 $\mathrm{HM}(p)\le\mathrm{HM}(q)$，则 $p\le q$。p 的次数记为 $\deg(p)$，若 $p\ne0$ 其次数为 $\max\left\{\sum_{i=1}^{n}a_i|a\in A\right\}$，否则为−1。

令 $\mathcal{I}$ 为集合 $F=\{f_1,f_2,\cdots,f_d\}\in\mathcal{R}$ 生成的理想，即 $\mathcal{I}=\{u_1f_1+u_2f_2+\cdots+u_df_d\mid u_1,u_2,\cdots,u_d\in\mathcal{R}\}$。考虑映射 $\phi:\mathcal{R}^d\to\mathcal{I}$ 使得 $\sum_{i=1}^{d}u_i\boldsymbol{e}_i\mapsto\sum_{i=1}^{d}u_if_i$，其中 $\boldsymbol{e}_i$ 是 $\mathcal{R}^d$ 的第 i 个单位向量使得自由 $\mathcal{R}$-模 $\mathcal{R}^d$ 由集合 $E=\{\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_d\}$ 生成。本文在 $\mathcal{M}_d=\{m\boldsymbol{e}_i\mid m\in\mathcal{M},i\in[1,d]\}$ 上定义一个模序 $\le_s$ 与 $\le$ 适配}(见文献[10]和文献[12])：$m\le t\Rightarrow m\boldsymbol{e}_i\le_s t\boldsymbol{e}_i$。如果不产生歧义，$\le_s$ 简记为 $\le$。$L=\{(\max\{\mathrm{HM}(u_i)\boldsymbol{e}_i,\le\},p)\mid\phi(u)=p\in\mathcal{I}\}$ 被叫作 ℓ-多项式(即，标签-多项式)的集合，其中 $\max\{\mathrm{HM}(u_i)\boldsymbol{e}_i,\le\}$ 表示选取关于序 $\le$ 最大的 $\mathrm{HM}(u_i)\boldsymbol{e}_i$，$\boldsymbol{u}=\sum_{i=1}^{d}u_i\boldsymbol{e}_i\in\mathcal{R}^d$。令 $\alpha=(\boldsymbol{s},p)\in L^*$，其中 $L^*=L\setminus(\boldsymbol{0},0)$，第 1 部分 $\boldsymbol{s}=\max\{\mathrm{HM}(u_i)\boldsymbol{e}_i,\le\}$ 叫做 α 的标签，记为 $\mathrm{S}(\alpha)$，第 2 部分 $p=\mathrm{poly}(\alpha)$ 是其多项式部分。不失一般性，本文假定 $\mathrm{poly}(\alpha)$ 总是首一的。同样，定义 α 的首单项式为 $\mathrm{HM}(\alpha)=\mathrm{HM}(p)$，次数为 $\deg(\alpha)=\deg(p)$。如果 $\mathrm{S}(\alpha)=t\boldsymbol{e}_j$，就把 $\mathrm{idx}(\alpha)=j$ 记为其索引，$\deg(\mathrm{S}(\alpha))=\deg(t)$。s-次数(见文献[13])定义为 $\deg_s(\alpha)=\deg(\mathrm{S}(\alpha))+\deg(f_{\mathrm{idx}(\alpha)})$。子集 $\mathrm{Syz}=\{(\boldsymbol{s},0)\in L^*\}$ 叫做 L 的合冲子模，$\mathrm{NS}=L\setminus\mathrm{Syz}$ 被叫作非合冲多项式集。令 $(\boldsymbol{s}_1,p_1)$ 和 $(\boldsymbol{s}_2,p_2)$ 为 NS 中的两个非合冲 ℓ-多项式。由形如 $(p_2\boldsymbol{s}_1-p_1\boldsymbol{s}_2,0)$ 的合冲生成的模叫做主合冲子模 PS。

一个 ℓ-多项式 $\alpha\in L$ 是可预测的，如果一个 Gröbner 基算法已经找到一个合冲 $\delta\in\mathrm{Syz}$ 使得 $\mathrm{S}(\delta)\mid\mathrm{S}(\alpha)$。算法应当避免计算这样的 α，因此其被称为冗余的。

$\alpha\in\mathrm{NS}$ 被称为是关于 $B\subset L^*$ 首可约的，若存在一个 ℓ-多项式 $\beta\in B$ 满足下列条件之一，

(1) $\mathrm{HM}(t\beta)=\mathrm{HM}(\alpha)$ 且 $\mathrm{S}(t\beta)<\mathrm{S}(\alpha)$；

(2) $\mathrm{S}(t\beta)=\mathrm{S}(\alpha)$ 且 $\mathrm{HM}(t\beta)<\mathrm{HM}(\alpha)$；

(3) $\mathrm{HM}(t\beta)=\mathrm{HM}(\alpha)$ 且 $\mathrm{S}(t\beta)=\mathrm{S}(\alpha)$，$t\in\mathcal{M}$。

否则，α 关于 B 首不可约。

$\alpha-t\beta$ 这一操作叫做 S-约化（对应地，M-约化，超首约化)，若满足条件(1) (对应地，条件(2)，条件(3))。条件(1)中，β 和 $t\beta$ 分别被称为 S-约化子和乘性 S-约化子。有时 $t\beta$ 也简称为 S-约化子。令 γ 为用 α 去 S-约化 $t\beta$ 的结果，这一过程可表示成 $\alpha\xrightarrow[B]{}\gamma$。$\xrightarrow[B]{*}$ 是 $\xrightarrow[B]{}$ 的自反传递闭包，即反复执行约化操作直到得到一个 S-不可约的 ℓ-多项式。若不考虑标签的大小关系，这样的约化叫做 c-约化。

由文献[4]和文献[10]的结论可得到如下的性质。

引理 1 令 α 为 NS 中的非合冲元。α 是可以被 L^* 来 M-约化的，当且仅当它是可以被 L^* 来 S-约化的。

推论 1[11] 令 $\alpha,\beta\in L^*$ 使 $\mathrm{S}(\alpha)=\mathrm{S}(\beta)$ 且它们非合冲。若 α 和 β 都 S-不可约，则 $\mathrm{HM}(\alpha)=\mathrm{HM}(\beta)$。

由文献[13]可知，若 $\alpha\in\mathrm{NS}$ 是齐次的，则 $\deg(\alpha)=\deg_s(\alpha)$，否则 $\deg(\alpha)\le\deg_s(\alpha)$。

若 α 是 S-不可约的且 $\deg(\alpha)<\deg_s(\alpha)$，则称其为一个突变（原始定义见文献[14])。如果输入多项式是齐次的，那么 NS 中是不存在突变的。

一个集合 $G\subset L$ 叫做模 L 的 S-Gröbner 基，如果任意的非合冲 $\alpha\in\mathrm{NS}$ 能够被 G 首约化。

由引理 1 可知，$\mathcal{I}$ 中的每个非零多项式可以被 $\mathcal{I}$ 的 Gröbner 基 $\{\mathrm{poly}(\alpha)\mid\alpha\in G,\mathrm{poly}(\alpha)\ne0\}$ 约化。因此 S-Gröbner 基实际上是文献[4]的一个术语，它是文献[8]中“强 Gröbner 基”的精简版。由上述定义可知，合冲 ℓ-多项式不是 S-Gröbner 基的必要组成部分。本文说两个 ℓ-多项式 α 和 β 等价，如果 $\mathrm{S}(\alpha)=\mathrm{S}(\beta)$ 且 $\mathrm{HM}(\alpha)=\mathrm{HM}(\beta)$。显然，所有的非合冲首不可约 ℓ-多项式组成具有最少个数的 S-Gröbner 基。文献[4]，文献[9]和文献[10]指出，非合冲不可约 ℓ-多项式只有有限多个(不计等价)。

本文引入文献[11]中定义在 G 上的关于重写准则的概念。一个 ℓ-多项式 $\alpha\in G$ 是标签 $\boldsymbol{s}$ 的重写子，如果 α 是 G 中使得 $\mathrm{S}(t\alpha)=\boldsymbol{s}$ 的 $\preceq$-最大元素，其中 $t\in\mathcal{M}$，$\preceq$ 为 G 上一个线性序(称为重写序)。与文献

[11]相比，这里对$\preceq$没有过多的限制：它只要是G上的线性序即可。有时本文也把$t\alpha$叫做$\boldsymbol{s}$的重写子。$m\beta \in \mathcal{M}\times G$是可重写的，如果$\mathrm{S}(m\beta)$的重写子是$\alpha \neq \beta$。

令$\alpha,\beta \in \mathrm{NS}$且定义$C_{\alpha\beta}$为最小公倍数$\mathrm{lcm}(\mathrm{HM}(\alpha),\mathrm{HM}(\beta))$。令$m_\alpha = C_{\alpha\beta}/(\mathrm{HM}(\alpha))$且$m_\beta = C_{\alpha\beta}/(\mathrm{HM}(\beta))$。令$\mathrm{r}(\alpha) > \mathrm{r}(\beta)$，其中操作$\mathrm{r}(\alpha) = \mathrm{S}(\alpha)/\mathrm{HM}(\alpha)$在文献[11]中被叫做$\alpha$的(标签-首项)比，且模序$\leq$的定义延拓到Laurent多项式环$\mathcal{K}[x_1,x_2,\cdots,x_n,x_1^{-1},x_2^{-1},\cdots,x_n^{-1}]$上。$m_\alpha\alpha$在文献[6]中被称为$\alpha$和$\beta$的J-对。$(\alpha,\beta)$叫做c-对，$\deg(C_{\alpha\beta})$叫做c-对$(\alpha,\beta)$的(全)次数。$\mathrm{r}(\alpha) > \mathrm{r}(\beta)$时，$\deg_s(m_\alpha\alpha)$叫做c-对的s-次数。

3　框架伪代码

不失一般性，假设$\boldsymbol{e}_1 < \boldsymbol{e}_2 < \cdots < \boldsymbol{e}_d$，且输入多项式$\{f_1,f_2,\cdots,f_d\}$之间互相约化不会产生零多项式。

框架的伪代码示于表1，其中，$\mathrm{sort}(F,\leq)$(相应地，$\min(F,\leq)$)表示按序“$\leq$”排列(相应地，按序“$\leq$”选取)集合F中的元素，J- pair(γ,β)表示生成γ和β的J-对。

注意到，该框架有意不给出代码第7行两个准则的具体操作，目的是使框架能包含不同版本的合冲准则和重写准则。有些算法的准则不能完全去掉可重写或可预测的J-对。假设在某轮循环中，选出的$t\alpha$可重写或可预测，即使它通过了这两个准则，本文后续的正确终止证明是不受影响的。

本文的算法1框架比文献[9]的算法更简单且更有一般性，主要体现在以下两方面。

(1)该框架是非递增的，但它可以涵盖递增算法，只要把模序设置为索引兼容的(即这个模序最先比较两个标签的索引)。

(2)尽管选择策略在代码第5行已经给定，但它仍可以模拟文献[9]中先选次数最低J-对的策略，只要把单项式序设置成次数兼容的(即这个序最先比较两个元素的次数)。详细的模拟见第4节。

表1 框架伪代码

(1)输入：一组多项式$F = \{f_1,f_2,\cdots,f_d\} \in \mathcal{R}$
(2)输出：理想$\mathcal{I} = < f_1,\cdots,f_d >$的Gröbner基
(3)初始化：$F \leftarrow \mathrm{sort}(\{f_1,\cdots,f_d\},\leq), \lambda_i = (\boldsymbol{e}_i, f_i),\ i \in [1,d]$其中$\boldsymbol{e}_1 < \boldsymbol{e}_2 < \cdots < \boldsymbol{e}_d$
　$G \leftarrow \varnothing$
　$P \leftarrow \{\lambda_i |\ i \in [1,d]\}$
(4) **while** $P \neq \varnothing$ **do**
(5)　　$t\alpha \leftarrow \min(P,\leq_s)$
(6)　　$P \leftarrow P \setminus \{t\alpha\}$
(7)　　**if** $t\alpha$通过合冲准则和重写准则 **then**
(8)　　$t\alpha \xrightarrow[G]{*} \beta$
(9)　　$G \leftarrow G \cup \beta$
(10)　　**if** $\mathrm{poly}(\beta) \neq 0$ **then**
(11)　　$P \leftarrow P \cup \{\text{J- pair}(\gamma,\beta) |\ \forall \gamma \in G \setminus \mathrm{Syz}, \gamma \neq \beta\}$
(12)　　**end if**
(13)　　**end if**
(14) **end while**
(15) **return** $\{\mathrm{poly}(\gamma) |\ \gamma \in G\}$

4　正确终止性证明

首先，本文引入文献[11]中关于重写基的一些术语。G是标签$\boldsymbol{s}$的重写基，如果$\boldsymbol{s}$的重写子$t\alpha \in \mathcal{M}\times G$不是S-可约化的。对于所有小于$\boldsymbol{s}$的标签$\boldsymbol{s}'$，如果$G$是标签$\boldsymbol{s}'$的重写基，那么$G$被称为直到$\boldsymbol{s}$的重写基(记为$G^{\mathrm{re}}_{<\boldsymbol{s}}$)。$\ell$-多项式集$L_{<\boldsymbol{s}}$的S-Gröbner基也可以记为$G^{\mathrm{sig}}_{<\boldsymbol{s}}$。记号$G^{\mathrm{re}}_{<\boldsymbol{s}}$和$G^{\mathrm{sig}}_{<\boldsymbol{s}}$有类似的定义。

引理2　令G为$G^{\mathrm{sig}}_{<\boldsymbol{s}}$，如果$\alpha$是首不可约$\ell$-多项式且$\mathrm{S}(\alpha) < s$，则$G$中有另一$\ell$-多项式与$\alpha$等价。

证明　令$t\beta$为标签$\mathrm{S}(\alpha)$的重写子。我们有$\mathrm{S}(t\beta) = \mathrm{S}(\alpha)$是首不可约标签，且$t\beta$不是S-可约化的。由推论1可知，$\mathrm{HM}(t\beta) = \mathrm{HM}(\alpha)$。$t\beta$一定是超首不可约的，即$t = 1$，否则就与$\alpha$是首不可约的事实矛盾。所以$\beta \in G$是等价于$\alpha$的。　　证毕

推论2　如果G是$G^{\mathrm{re}}_{<\boldsymbol{s}}$，则$G$也是$G^{\mathrm{sig}}_{<\boldsymbol{s}}$。

证明　反证假设G不是$G^{\mathrm{sig}}_{<\boldsymbol{s}}$。因为模序$\leq$为一良序，令$\alpha \in L$为具有极小标签的S-不可约$\ell$-多项式使得$G$中没有与$\alpha$等价的$\ell$-多项式。当然，$\mathrm{S}(\alpha) < \boldsymbol{s}$成立。令$t\beta$为标签$\mathrm{S}(\alpha)$的重写子。根据重写基的定义，$\mathrm{S}(t\beta) = \mathrm{S}(\alpha)$是一个S-不可约标签且$t\beta$不是S-可约的。甚至，$t = 1$，否则与标签$\mathrm{S}(t\beta)$不可约矛盾。根据推论1，$\beta$与$\alpha$等价且$\beta \in G$，这与假设矛盾。

由于非合冲不可约ℓ-多项式只有有限多个(不计等价)，β与α等价，导致矛盾。　　证毕

引理3　令$\alpha \in \mathrm{NS}$为首不可约的。在执行有限步后，假设框架已正确算出直到首不可约标签$\mathrm{S}(\alpha)$的重写基(即，$G = G^{\mathrm{re}}_{<\mathrm{S}(\alpha)}$)。在继续执行有限步后，$G$将变为$G^{\mathrm{re}}_{\leq\mathrm{S}(\alpha)}$。

证明　下面考虑$\mathrm{S}(\alpha)$的两种情况。

若$\mathrm{S}(\alpha) = \boldsymbol{e}_i$，框架初始化后，$P$中就有一个标签为$\mathrm{S}(\alpha)$的J-对，并且它能通过两个准则。

若$\mathrm{S}(\alpha) \neq \boldsymbol{e}_i$，对于所有的$i \in [1,d]$，那么就存在重写子$t\beta$，其标签为$\mathrm{S}(\alpha)$。因为$t\beta$可以被$\alpha$来M-约化，由引理1可知，$t\beta$是S-可约的。由于$t\beta$既不可重写又不可预测，它将通过两个准则。

如果有J-对其标签为$\boldsymbol{s} < \mathrm{S}(\alpha)$，那么这个J-对

的标签是首不可约的。由选择策略和下面引理可知，标签为 $\mathrm{S}(\alpha)$ 的 J-对将在有限步后被选出，并且被 S-约化成等价于 α 的首不可约 ℓ-多项式。 证毕

与文献[10]的证明方法相似，下面将用 Huang 的思想来构造向量 $\boldsymbol{N}_P^w$，从而证明终止问题。

引理 4 在有限步循环之后，假设框架已经算出 S-Gröbner 基，那么该框架将会在继续执行有限步后终止。

证明 当然，此时 P 中的 J-对和 G 中的 ℓ-多项式是有限的。由于合冲 ℓ-多项式不能生成新的 J-对，证明着眼于非合冲 ℓ-多项式。G 中所有非合冲 ℓ-多项式记为 $\{G(k_1),G(k_2),\cdots,G(k_w)\}$。定义 NS 上的序 $\preceq_p$ 为 $\alpha\preceq_p\beta$ 当且仅当 $r(\beta)\le r(\alpha)$，则有一个作用在集合 $\{1,2,\cdots,w\}$ 上的置换 ζ，使得 $G(k_{\zeta(1)})\succeq G(k_{\zeta(2)})\succeq\cdots\succeq G(k_{\zeta(w)})$，因为 $\preceq_p$ 是一良序。P 中所有的 J-对可以被记入一个向量 $\boldsymbol{N}_P^w=(n_1,n_2,\cdots,n_w)\in\mathcal{N}^w:n_j$ 表示 $\preceq_p$-等价于某个 $G(k_{\zeta(j)}),j\in[1,w]$ 的 J-对个数。

执行完伪代码第 6 行后，令 γ 为 P 中选出的 J-对，其必 $\preceq_p$-等价于某个 $G(k_{\zeta(j)})$。这轮循环过后，出现以下两种情况。

框架将不生成新的 J-对。那么，向量 $\boldsymbol{N}_P^w$ 将变成 $(n_1,n_2,\cdots,n_{j-1},n_j-1,n_{j+1},n_{j+2},\cdots,n_w)$。

框架将生成新的 J-对。这意味着 γ 将通过两个准则，并被约为非合冲 ℓ-多项式，记为 β。由于我们已经得到了 S-Gröbner 基，β 必 $\preceq_p$-等价于某个 $G(k_{\zeta(j+i)})$，其中 $i\in[1,w-j]$。由 β 和 G 中另一 ℓ-多项式生成的 J-对将不会 $\preceq_p$ 大于 β，$\boldsymbol{N}_P^w$ 将变成 $(n_1,n_2,\cdots,n_{j-1},n_j-1,n_{j+1},n_{j+2},\cdots,n_w)+\boldsymbol{a}$。
其中 $\boldsymbol{a}$ 为 w 维向量使得 $a_v=0,v\in[1,j+i),a_v\ge0,v\in[j+i,w]$。

因此，$\boldsymbol{N}_P^w$ 将关于字典序减小，框架将在有限步内终止，因为字典序在 $\mathcal{N}^w$ 上是良基的。 证毕

下面将用归纳法证明，框架能在有限步后正确终止。这里不考虑合冲 ℓ-多项式是因为这类多项式不能生成新的 J-对。框架的正确性取决于是否能够计算出所有的首不可约 ℓ-多项式。

定理 1 对于 $\mathcal{R}$ 上任意的有限集 $F=\{f_1,f_2,\cdots,f_d\}$，框架能够正确终止。

证明 对 L 上的首不可约 ℓ-多项式进行归纳。因为 $\boldsymbol{e}_1<\boldsymbol{e}_2<\cdots<\boldsymbol{e}_d$ 为首不可约标签，起始步 $G=G_{<\boldsymbol{e}_1}^{\mathrm{re}}$。归纳步由引理 3 和推论 2 保证，因为首不可约 ℓ-多项式是有限的，在有限步循环后，框架就计算出 S-Gröbner 基。再由引理 4 可知，框架能有限步终止。 证毕

5 化简

在 F5 算法的约化过程中，需要检查每一个 S-约化子是否能通过两个准则，而不是像本文代码第 7 行那样，只检查被约化的 ℓ-多项式。本文把 F5 算法的约化操作叫做 F5-约化。文献[10]证明了“S-约化”与“F5-约化”是等价的，利用文献[11]的方法，本文给出一个极其简单的等价性证明。

引理 5 令 $\alpha\in L^*$ 且 G 为 $G_{<\mathrm{S}(\alpha)}^{\mathrm{re}}$。若 α 是 S-可约的，那么 α 也是 F5-可约的。

证明 令 $t\beta$ 为 α 的一个 S-约化子且其有最小的标签，其中 $\beta\in G$。显然，$t\beta$ 既不 S-可约也不可预测。由于 G 已经是标签 $\mathrm{S}(t\beta)$ 的重写基，标签 $\mathrm{S}(t\beta)$ 的重写子不可约，其记为令 $s\gamma$。更进一步，由推论 1 可知，$\mathrm{S}(s\gamma)=\mathrm{S}(t\beta)$ 且 $\mathrm{HM}(s\gamma)=\mathrm{HM}(t\beta)$。也就是说，$\alpha$ 能被 $\gamma\in G$ 来重写。 证毕

6 选择策略

注意到，本文给出的伪代码在每轮循环时，总是选择具有最小标签的 J-对来做约化，即按模序 $\le$ 选取。这与 GVW 算法的选取策略显然是相同的。更重要的是，下面的研究表明这种策略与文献[3]和文献[10]所用的策略是有相似性的。利用这一点，F5 算法就能被看成前文框架的一个特例，进而被证明正确终止。

回忆 F5 算法所用的模序为 $\le_{\mathrm{POT}}$（位置先于项）：$m\boldsymbol{e}_i\le_{\mathrm{POT}}t\boldsymbol{e}_j$，如果 $i<j$，或者 $i=j$，$m\le t$，其中 $m,t\in\mathcal{M}$。而 F5 算法的选取策略较复杂，因其每轮选出一个次数最小的 c-对的集合 P_d。但是，在 F5 算法的约化子函数中，每次约化所用的 ℓ-多项式都是确定的：在 P_d 中选择关于模序 $\le_{\mathrm{POT}}$ 最小的一个 J-对。令 $\alpha=(m\boldsymbol{e}_i,p)$ 和 $\beta=(t\boldsymbol{e}_j,q)$ 为两个 J-对，如果用二元序 $\le_{\mathrm{F5}}$ 来表示 F5 算法的约化策略，那么 $\alpha<_{\mathrm{F5}}\beta$ 可以写成

(1) $i<j$；
(2) $i=j$ 且 $\deg(p)<\deg(q)$；
(3) $i=j$，$\deg(p)=\deg(q)$ 且 $m<t$。

因为 F5 算法的输入是齐次多项式，由文献[13]可知，$\deg_s(\alpha)=\deg(\alpha)$，$\deg_s(\beta)=\deg(\beta)$。于是，$\le_{\mathrm{F5}}$ 可以表示成

(1) $i<j$；
(2) $i=j$ 且 $\deg(m)<\deg(t)$；
(3) $i=j$，$\deg(m)=\deg(t)$ 且 $m<t$。

因此，选择 J-对来约化时用的 $\le_{\mathrm{F5}}$ 序可以记为 $\le_{\mathrm{PDT}}$（位置先于次数先于项），而 F5 算法使用模序为 $\le_{\mathrm{POT}}$。当单项式序 $\le$ 不是次数兼容的时候(例如，$\le_{\mathrm{LEX}}$)，模序 $\le_{\mathrm{POT}}$ 与 $\le_{\mathrm{PDT}}$ 是不相同的。这里，读者可能会认为，本文的框架不能模拟 F5 算法的流程。事实上，对于齐次 F5 算法，下面的结果表明模序

$\le_{\mathrm{POT}}$与$\le_{\mathrm{PDT}}$的效果是相同的。

首先，关于单项式序$\le$，定义一次数兼容序$\le_d: m <_d t$若下面二者之一成立

(1) $\deg(m) < \deg(t)$；

(2) $\deg(m) = \deg(t)$且$m < t$。

可以看到，上文中的序$\le_{\mathrm{PDT}}$与$\le_d$是适配的。记HM'(相应地，S')为关于$\le_d$(相应地，$\le_{\mathrm{PDT}}$)的首单项式(相应地，标签)。本文得到关于这些序的一个有趣的结果。

命题　若$\alpha \in L$是一个齐次ℓ-多项式，则$\mathrm{HM}'(\alpha) = \mathrm{HM}(\alpha)$且$\mathrm{S}'(\alpha) = \mathrm{S}(\alpha)$。并且，若$\alpha, \beta \in L$是齐次的，则有

(1) $\mathrm{S}'(t\alpha) = \mathrm{S}(t\alpha)$且$\mathrm{HM}'(t\alpha) = \mathrm{HM}(t\alpha)$；

(2) 若$\deg(\mathrm{HM}(\alpha)) = \deg(\mathrm{HM}(\beta))$，则$\mathrm{S}'(\alpha+\beta) = \mathrm{S}(\alpha+\beta)$且$\mathrm{HM}'(\alpha+\beta) = \mathrm{HM}(\alpha+\beta)$。

由于F5算法生成新的ℓ-多项式的方法无非就是$t\alpha$和$\alpha+\beta$这两种，所以当算法的输入为齐次多项式时，$\le$和$\le_{\mathrm{POT}}$就是$\le_d$和$\le_{\mathrm{PDT}}$。也就是说，可以把齐次F5算法看成是使用了多项式序$\le_d$和模序$\le_{\mathrm{PDT}}$。从上文已知，F5算法在每次约化时都按$\le_{\mathrm{PDT}}$从小到大的顺序选取J-对。因此，F5算法的选择策略与本文的框架一致。对于合冲准则和重写准则，仿照文献[10]的方法，该框架也能准确地模拟F5的操作。由此可见，F5算法是框架的一个特例。

7　非齐次输入多项式

从前文的伪代码描述里可以看出，框架可以处理非齐多项式，但根据上一节讨论，框架不能模拟非齐F5算法的选择策略。因为此时，$\deg(\alpha) \le \deg_s(\alpha)$，选择次数为$d$的J-对不一定等同于选择s-次数为$d$的J-对。

所幸的是，可以把框架的选择策略替换成$\le_{\mathrm{F5}}$，改变后框架的证明与原始证明类似。这是因为，只有引理3的证明与选取策略相关。

引理 6　$\alpha \in \mathrm{NS}$为首不可约的。有限步之后，假设框架已算出直到首不可约标签$\mathrm{S}(\alpha)$的重写基(即，$G = G^{\mathrm{re}}_{<\mathrm{S}(\alpha)}$)。在有限轮循环之后，框架将从$P$中选出标签为$\mathrm{S}(\alpha)$的J-对，且其能通过合冲与重写准则。

证明　证明J-对的存在与引理3相同。与齐次输入的情况比，框架将处理一些由突变生成的额外的J-对。由于次数不超过$\deg(\alpha)$的ℓ-多项式的个数是有限的，在有限步循环后，满足条件的J-对将被选出，从而被约化成α。　　证毕

参 考 文 献

[1] Buchberger B. Ein algorithmus zum auffinden der basiselemente des restklassenrings nach einem nulldimensionalen polynomideal[D]. [Ph.D. dissertation], Universität Innsbruck, Austria, 1965.

[2] Faugère J C. A new efficient algorithm for computing Gröbner bases (F4)[J]. *Journal of Pure and Applied Algebra*, 1999, 139(1-3): 61–88.

[3] Faugère J C. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)[C]. Proceedings of the 27th International Symposium on Symbolic and Algebraic Computation, New York, USA, 2002: 75–83.

[4] Arri A and Perry J. The F5 criterion revised[J]. *Journal of Symbolic Computation,* 2011, 46(9): 1017–1029.

[5] Gao Shu-hong, Guan Yin-hua, and Volny F IV. A new incremental algorithm for computing Groebner bases[C]. Proceedings of the 35th International Symposium on Symbolic and Algebraic Computation, New York, USA, 2010: 13–19.

[6] Gao Shu-hong, Volny F, and Wang Ming-sheng. A new algorithm for computing Gröbner bases[OL]. http://www.math.clemson.edu/~sgao/papers/gvw_R130704.pdf, 2010.

[7] Volny F. New algorithms for computing Gröbner bases[D]. [Ph.D. dissertation], Clemson University, USA, 2011.

[8] Sun Yao and Wang Ding-kang. A generalized criterion for signature related Gröbner basis algorithms[C]. Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation, New York, USA, 2011: 337–344.

[9] Eder C and Perry J. Signature-based algorithms to compute Gröbner bases[C]. Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation, New York, USA, 2011: 99–106.

[10] Pan Sen-shan, Hu Yu-pu, and Wang Bao-cang. The termination of the F5 algorithm revisited[C]. Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation, New York, USA, 2013: 291–298.

[11] Eder C and Roune B H. Signature rewriting in Gröbner basis computation[C]. Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation, New York, USA, 2013: 331–338.

[12] Huang Lei. A new conception for computing Gröbner basis and its applications[OL]. http://arxiv.org/abs/1012.5425. 2010.

[13] Eder C. An analysis of inhomogeneous signature-based Gröbner basis computations[J]. *Journal of Symbolic Computation*, 2013, 59(0): 21–35.

[14] Ding Jin-tai, Cabarcas D, Schmidt D, *et al.*. Mutant Gröbner basis algorithm[C]. Proceedings of the 1st International Conference on Symbolic Computation and Cryptography, Beijing, China, 2008: 23–32.

潘森杉：　男，1986年生，博士生，研究方向为多变量公钥密码、Gröbner基.

胡予濮：　男，1955年生，博士，教授，博士生导师，研究方向为格公钥密码、流密码等.

王保仓：　男，1979年生，博士，副教授，硕士生导师，研究方向为格公钥密码、多变量密码等.