Минимальный базис модуля сизигий старших членов

А.В. Шокуров <shok@ispras.ru>

Институт системного программирования им. В.П. Иванникова РАН, 109004, Россия, г. Москва, ул. А. Солженицына, д. 25

Аннотация. Системы полиномиальных уравнений – один из наиболее универсальных математических объектов. Почти все задачи криптографического анализа можно свести к поиску решений систем полиномиальных уравнений. Соответствующее направление исследований принято называть алгебраическим криптоанализом. С точки зрения вычислительной сложности, системы полиномиальных уравнений охватывают весь диапазон возможных вариантов, от алгоритмической неразрешимости диофантовых уравнений до хорошо известных эффективных методов решения линейных систем. Метод Бухбергера приводит систему алгебраических уравнений к системе специального вида, определяемой базисом Гребнера исходной системы уравнений, позволяющему использовать исключение зависимых переменных. Фундаментом определения базиса Гребнера является допустимое упорядочение на множестве термов. Множество допустимых упорядочений на множестве термов бесконечно и даже континуально. Наиболее трудоемким этапом при нахождении базиса Гребнера с помощью алгоритма Бухбергера является доказательство приводимости к нулю всех S-многочленов. Известно, что достаточно провести такую проверку только для любого подмножества таких многочленов, представляющих систему образующих K[X]-модуля S-многочленов. Возникает естественная задача нахождения такой минимальной системы образующих. Существование такой системы образующих следует из теоремы Накаямы. Предложен алгоритм построения такого базиса для любого упорядочения.

Ключевые слова: кольцо многочленов; поле; идеал; сизигия; базис Гребнера; алгоритм Бухбергера; допустимый порядок

DOI: 10.15514/ISPRAS-2018-30(6)-16

Для цитирования: Шокуров А.В. Минимальный базис модуля сизигий старших членов. Труды ИСП РАН, том 30, вып. 6, 2018 г., стр. 293-304. DOI: 10.15514/ISPRAS-2018-30(6)-16

1. Основные определения и обозначения

Пусть K – поле и $K[x_1,\dots,x_n]$ – кольцо многочленов от независимых переменных $X=\{x_1,\dots,x_n\}$. Термом на переменных X будем называть выражения вида $x_1^{m_1}\dots x_n^{m_n}$, где $m_1,\dots,m_n$ – неотрицательные целые числа. Для термов в дальнейшем будем использовать обозначение $x_1^{m_1}\dots x_n^{m_n}=x^{\omega}$, где

$\omega=(m_1,\dots,m_n)\in\mathbb{Z}_+^n$. Множество всех термов на множестве переменных X обозначим через $T\langle X\rangle$. Множество всех термов является коммутативным моноидом относительно умножения. Заметим, что каждый многочлен $f\in[x_1,\dots,x_n]$ представим в виде

$$f=\sum_{t\in T\langle X\rangle}\alpha_t\,t,\alpha_t\in K, \qquad (1)$$

причем только конечное число коэффициентов $\alpha_t\neq 0$. Обозначим через $T_f\langle X\rangle$ множество ненулевых термов многочлена f

$$T_f\langle X\rangle=\{t\in T\langle X\rangle|\alpha_t\neq 0\},$$

причем только конечное число коэффициентов $\alpha_t\neq 0$. Обозначим через $T_f\langle X\rangle$ множество ненулевых термов многочлена f

$$T_f\langle X\rangle=\{t\in T\langle X\rangle|\alpha_t\neq 0\}.$$

Определение 1.1. Допустимым порядком на множестве термов $T\langle X\rangle$ называется линейный порядок $\prec$, удовлетворяющий свойствам

$$\forall t,t_1,t_2\in T\langle X\rangle\ \mathrm{t}_1\prec\mathrm{t}_2\Rightarrow\mathrm{tt}_1\prec\mathrm{tt}_2,$$
$$\forall t\in T\langle X\rangle\ \mathrm{t}\neq 1\Rightarrow 1\prec\mathrm{t}.$$

Фиксируем допустимый порядок на $T\langle X\rangle$. Отметим, что множество термов вполне упорядочено относительно $\prec$.

Определение 1.2. Старшим термом многочлена f называется максимальный элемент множества $T_f\langle X\rangle$. Старший терм многочлена f будем обозначать через $\mathrm{HT}(f)$.

Определение 1.3. Старшим мономом многочлена f, заданного формулой ([1]) называется моном $\alpha_t t$, где t – его старший терм. Старший моном многочлена f будем обозначать через $\mathrm{HM}(f)$.

Определение 1.4. Базисом Гребнера идеала I называется его конечный базис G, удовлетворяющий условию

$$\forall f\in I\exists g\in G\mathrm{HM}(g)|\mathrm{HM}(f).$$

Определение 1.5. Пусть $f,h\in K[X]$ и G – конечное подмножество в $K[X]$. Будем говорить, что существует простая монотонная редукция f к h по модулю G, если $\mathrm{HM}(g)\prec\mathrm{HM}(f)$ и для некоторых $g,\mu_g\in K[X]$ выполняется равенство $h=f-\mu_g g$. Простую монотонную редукцию f к h по модулю G будем обозначать через $f\to_G h$. Если имеется последовательность простых монотонных редукций

$$f\to_G h_1\ \to_G\dots\to_G\ h_k,$$

будем говорить что имеется монотонная редукция f к h по модулю G и записывать ее формулой $f\to_{G^*}h$, где $h=h_k$.

Определение 1.6. Пусть $f\to_{G^*}h$ и из $f\to_{G^*}h$ следует, что $h=h_1$. В этом случае будем говорить, что (монотонная) редукция $f\to_{G^*}h$ является полной, а f приводится к нормальной форме h по модулю множества G, и записывать формулой $f\to_{G^*}\underline{h}$.

Напомним определение операции $S(f,g)$ для многочленов $f,g \in K[X]$. Введем обозначение

$$u_{f,g} = \frac{\text{НМ}(g)}{\text{НОД}(\text{НТ}(f),\text{НТ}(g))} \qquad (2).$$

Тогда $S(f,g) = u_{f,g}f - u_{g,f}g \in K[X]$.

Пусть $G = \{g_1, \dots, g_m\}$. Алгоритм нахождения базиса Гребнера основан на следующем критерии Бухбергера [1].

Теорема 1. Конечное множество $G \subset K[X]$ является базисом Гребнера идеала $I \subset K[X]$, порожденного множеством G, тогда и только тогда, когда

$$\forall f,g \in G \;\; S(f,g) \to_{G^*} 0.$$

В действительности нет необходимости проверять условие (2) на всех парах (g_i, g_j). Достаточно проверить его только для пар, S-операции на которых порождают S-операции для остальных пар [2].

Теорема 2. Пусть $H \subset G \times G$ такое подмножество, что выполнено

$$\forall 1 \le i < j \le m \forall (1 \le k < l \le m | (g_k, g_l) \in H) \exists f_{k,l} | S(g_i, g_j) = \sum_{(g_k,g_l)\in H} f_{k,l}\, S(g_k, g_l).$$

Тогда

$$(\forall (g_k, g_l) \in H \; S(g_k, g_l) \to_{G^*} 0) \Rightarrow \; \forall 1 \le i < j \le m \; S(g_i, g_j) \to_{G^*} 0.$$

Наиболее трудоемкой процедурой в алгоритме Бухбергера является проверка выполнения условий $S(g_i, g_j) \to_{G^*} 0$. Теорема 2 позволяет сократить число таких проверок. Однако чтобы воспользоваться этим критерием, необходимо уметь находить соответствующие множества H. Алгебраическое решение этой задачи без вычисления S-операций проведено в данной работе.

2. Сизигии старших членов

Пусть $\{f_1, \dots, f_m\}$ – базис идеала I. Рассмотрим свободный $K[X]$-модуль с выделенным базисом $e_1, \dots, e_m$, соответствующим базису идеала $I = (f_1, \dots, f_m)$.

Определение 2.1. Пусть $F = (f_1, \dots, f_m) \in K[X]^m$. Сизигией старших членов $\boldsymbol{F}$ называется такой $S = (h_1, \dots, h_m) \in K[X]^m$, что

$$\sum_{i=1}^{m} h_i HM(f_i) = 0.$$

Множество всех сизигий (старших членов) F будем обозначать $\mathcal{S}(F)$.

Согласно определению 2.1 выполняется включение $\mathcal{S}(F) \subset K[X]^m$. Рассматривая $K[X]^m$ как $K[X]$-модуль, получаем представление $S = \sum_{i=1}^m h_i\, e_i$, где $e_i, i = 1, \dots, m$, – стандартный $K[X]$-базис в $K[X]^m$. Очевидно, $\mathcal{S}(F)$ является подмодулем $K[X]$-модуля $K[X]^m$. Определение S-операции может быть записано с использованием сизигий в виде скалярного произведения

$$S(f_i, f_j) = S_{f_i,f_j} \cdot F, \qquad (3)$$

где $S(f_i, f_j) = u_{f_i,f_j}e_i - u_{f_j,f_i}e_j \in \mathcal{S}(F)$. Сизигии $S(f_i, f_j)$ называются критическими.

Определение 2.2. Сизигия $S \in \mathcal{S}(F)$ называется однородной степени $\omega \in \mathbb{Z}_+^{\boldsymbol{n}}$, если

$$S = (c_1 x_1^{\omega}, \dots, c_m x_m^{\omega}) = \sum_{i=1}^{m} c_i \, \mathrm{x}^{\boldsymbol{\omega}_i} e_i, \omega_i \in \mathbb{Z}_+^n, \qquad (4)$$

где $c_i \in K$ и $HT(x^{\omega_i} f_i) = x^{\omega}$ при $c_i \neq 0$. Положим также по определению $\deg e_i = HT(f_i)$.

Определение 2.3. Выражения вида te_i, где $t \in T\langle X\rangle$ и $i = 1, \dots, m$, называются термами в $K[X]$-модуле $K[X]^m$. Множество термов в $K[X]$-модуле $K[X]^m$ обозначим через $T\langle X\rangle\langle e_1, \dots, e_m\rangle$.

Лемма 1. Порядок на множестве термов в $K[X]$-модуле $K[X]^m$, заданный формулой

$$te_i < st_j \iff \Big(tHT(f_i) \prec sHT(f_j) \vee \Big(tHT(f_i) = sHT(f_j) \wedge HT(f_i) \succ HT(f_j)\Big)\Big),$$

является линейным и допустимым, т.е.

$$\forall t_1, t_2, t_3 \in T\langle X\rangle \; t_1 e_i < t_2 e_j \Rightarrow t_3 t_1 e_i < t_3 t_2 e_j,$$
$$\forall V \subset T\langle X\rangle\langle e_1, \dots, e_m\rangle \exists v \in V : \forall v' \in Vv \neq v' \Rightarrow v < v'.$$

Доказательство. Следует непосредственно из свойств линейности и допустимости порядка $\prec$ на множестве термов $T\langle X\rangle$.

Определение 2.4. Старшим термом сизигии $S = (h_1, \dots, h_m)$ называется наибольший из ненулевых термов $HT(h_i)e_i$. Соответственно, минимальным термом сизигии называется наименьший из ненулевых термов $HT(h_i)e_i$. Старший терм обозначим через $HT(S)$, а младший – $LT(S)$.

В силу определения 2.2 для однородной сизигии S для всех $i = 1, \dots, m$ выполняется равенство $dS = \omega_i + de_i$. В частности сизигии S_{f_i,f_j} из формулы (3) являются однородными и $dS_{f_i,f_j} = du_{f_i,f_j} + de_i = du_{f_j,f_i} + de_j$.

Лемма 2. Сизигии $\mathcal{S}(F)$ допускают единственное представление в виде суммы однородных сизигий.

Доказательство. Пусть $S = (h_1, \dots, h_m) \in \mathcal{S}(F)$. Для каждого $\omega \in \mathbb{Z}_+^{\boldsymbol{n}}$ определим $h_{i,\omega}$ как слагаемое многочлена h_i, для которого $deg(h_{i,\omega}f_i) = \omega$. Тогда согласно определению сизигии $S_\omega = (h_{1,\omega}, \dots, h_{m,\omega})$ также является сизигией и выполняется соотношение $S = \sum_{\omega\in\mathbb{Z}_+^n} S_\omega$. Единственность такого представления очевидна.

Лемма 3. Любая однородная сизигия S представима в виде суммы $S = \sum_{1\le i<j\le m} g_{i,j}\, S_{f_i,f_j}$, где $g_{i,j}$ – однородные многочлены, причем $g_{i,j} = 0$ при $dS \neq d(g_{i,j}S_{f_i,f_j})$. Иными словами, критические сизигии составляют базис модуля сизигий.

Доказательство. Пусть утверждение леммы неверно. Пусть □ – подмодуль модуля сизигий $F = \mathcal{S}(F)$, порожденный всеми критическими сизигиями. В множестве сизигий $F \setminus$□ выберем элемент S с минимальным старшим термом. Пусть $t^{\omega_i} e_i$ – ее старший терм и $a_i t^{\omega_i} e_i$ – соответствующий старший моном. Тогда по определению сизигии у нее имеется меньший ненулевой терм вида $t^{\omega_j} e_j$, для которого выполняется равенство $t^{\omega_j} HT(f_j) = t^{\omega_i} HT(f_i)$. Тогда $t_i^{\omega} e_i - t_j^{\omega} e_j = t^{\alpha} S_{f_i,f_j}$, сизигия $S - a S_{f_i,f_j}$ неразложима по критическим сизигиям, а ее старший терм меньше $t_i^{\omega} e_i$, что противоречит выбору сизигии S.

Из леммы 2 следует, что модуль сизигий старших членов является однородным модулем с фильтрацией, определяемой множеством $\mathbb{Z}_+^n$ относительно однородного кольца многочленов $K[X]$ с той же фильтрацией. Такое однородное кольцо многочленов является локальным – его единственным максимальным однородным идеалом является идеал $(x_1, \dots, x_n)$. Следовательно к модулю сизигий старших членов применима следующая лемма Накаямы [3].

Лемма 4. Пусть A – локальное кольцо и □ – его (единственный) максимальный идеал, M – конечнопорожденный A-модуль и пусть $\varphi: M \to M/$□M – гомоморфизм факторизации. Элементы $m_1, \dots, m_s$ порождают модуль M тогда и только тогда, когда их образы $\varphi(m_1), \dots, \varphi(m_s)$ порождают фактормодуль $M/$□M.

Определение 2.5. Базис $L \subset \mathcal{S}(F)$ в модуле сизигий $\mathcal{S}(F)$ называется минимальным, если любое его собственное подмножество не является базисом модуля сизигий.

Поскольку $K[X]/$□$M = K$, и, следовательно, фактормодуль $M/$□M является векторным пространством над K, получаем

Следствие 1. Число элементов минимального базиса модуля сизигий $\mathcal{S}(F)$ является его инвариантом.

Теперь из леммы 3 и следствия 1 вытекает

Следствие 2. Существует минимальный базис модуля сизигий $\mathcal{S}(F)$, состоящий из критических сизигий. Число элементов такого базиса не зависит от его выбора.

Далее предложен алгоритм нахождения такого минимального базиса. Заметим, что предложенный в работе алгоритм нахождения такого базиса не является полным. Доказательство неприводимости множества элементов Σ^* неточное, рассуждение о дальнейшем повторе выполняемой там процедуры по индукции является неполным и некорректным. По тем же причинам некорректно доказательство по индукции минимальности базиса Σ^{**}.

3. Разложимые сизигии

Введем несколько обозначений. Напомним, что $F = (f_1, \dots, f_m) \in K[X]^m$ Положим $T(F) = \{\tau_1, \dots, \tau_m\}$, где $\tau_i = HT(f_i)$. Поскольку K – поле, то без ограничения общности можно считать, что где $HM(f_i) = \tau_i$. Также, не

ограничивая общность, можно считать, что $\tau_i \prec \tau_j$ при $i < j$. При $i < j$ положим $S_{f_i,f_j} = \alpha_{i,j} e_i + \beta_{i,j} e_j$. Обозначим множество критических сизигий для F через Σ. Согласно лемме 2 множество Σ является однородным базисом $K[X]$-модуля $\mathcal{S}(F)$. Введем обозначение

$$\Sigma_\omega = \{s \in \Sigma | ds \prec \omega\}, \omega \in \mathbb{Z}_+^n$$

Определение 3.1. Однородная сизигия s степени $\omega \in \mathbb{Z}_+^n$ называется разложимой, если выполняется соотношение

$$s = \sum_{\sigma \in \Sigma_\omega} c_\sigma \, t_\sigma \sigma, \omega = d(t_\sigma \sigma), t_\sigma \in T(K[X]), c_\sigma \in K.$$

Непосредственно из определения 3.1 следует

Лемма 5. Сумма разложимых однородных сизигий одинаковой степени разложима.

Из определения 3.1. и леммы 5 следует

Лемма 6. Пусть Σ_0^ω – подмножество множества всех разложимых критических сизигий размерности $\omega \in \mathbb{Z}_+^n$, $\Sigma'_\omega = \Sigma_\omega \cup \Sigma_0^\omega$, s – однородная сизигия размерности ω и

$$s = \sum_{\sigma \in \Sigma'_\omega} c_\sigma \, t_\sigma \sigma, \qquad \omega = d(t_\sigma \sigma), \qquad t_\sigma \in T(K[X]), \qquad c_\sigma \in K. \qquad (5)$$

Тогда сизигия s – разложима.

В дальнейшем количество ненулевых элементов c_σ в разложении (5) будем называть длиной этого разложения.

Лемма 7. Пусть заданы число k, подмножество $L = \{l_1, \dots, l_p\}$ в $\{1, \dots, m\} \setminus \{k\}$, $\omega \in \mathbb{Z}_+^n$ и такая однородная сизигия s размерности ω

$$s = \sum_{i \in L} a_i \, t_i S_{f_i,f_k}, \qquad t_i \in T(K[X]), \qquad deg(t_i S_{f_i,f_k}) = \omega,$$

что $a_i \neq 0$ при $i \in L$ и $\sum_{i \in L} a_i = 0$. Тогда имеется разложение

$$\mathrm{s} = \sum_{i=1}^{p-1} \left(\sum_{j=1}^{i} a_{l_j} \right) \mathrm{u_i} \mathrm{S}_{\mathrm{f_{l_i}},\mathrm{f_{l_{i+1}}}}, \ \mathrm{u_i} \in \mathrm{T(K[X])}.$$

Согласно определению критических сизигий имеем

$$S_{f_i,f_j} = u_{i,j} e_{f_i} - u_{j,i} e_{f_j},$$

причем $\mathbf{deg}\, \boldsymbol{S_{f_i,f_j}} = \mathbf{deg}\, \boldsymbol{u_{i,j}} + \mathbf{deg}\, \boldsymbol{e_{f_i}} = \mathbf{deg}\, \boldsymbol{u_{j,i}} + \mathbf{deg}\, \boldsymbol{e_{f_j}}, \boldsymbol{u_{i,j}}, \boldsymbol{u_{j,i}} \in \boldsymbol{T(K[X])}$.

По условию леммы для всех $i \in L$ выполняются равенства $\deg t_i + \deg u_{k,i} + \deg e_{f_k} = \omega$ и, следовательно, для всех пар $i, j \in L, i \neq j$

$$\mathrm{t_i} S_{f_i,f_k} - \mathrm{t_j} S_{f_j,f_k} = \mathrm{t_i}\left(\mathrm{u_{i,k}} \mathrm{e_{f_i}} - \mathrm{u_{k,i}} \mathrm{e_{f_k}}\right) - \mathrm{t_j}\left(\mathrm{u_{j,k}} \mathrm{e_{f_j}} - \mathrm{u_{k,j}} \mathrm{e_{f_k}}\right) =$$

$$\left(\mathrm{t_i u_{i,k} e_{f_i}} - \mathrm{t_j u_{j,k} e_{f_i}}\right) + \left(\mathrm{t_j u_{k,j}} - \mathrm{t_{iu_{k,i}}}\right)\mathrm{e_{f_k}} = \mathrm{t_i u_{i,k} e_{f_i}} - \mathrm{t_j u_{j,k} e_{f_j}} =$$
$$t_{i,j} S_{f_i,f_j}, \text{ где } t_{i,j} = x^{\omega - \deg S_{f_i,f_j}}.$$

Следовательно,

$$\mathrm{s} = \sum_{i\in L} a_i t_i S_{f_i,f_k} = \sum_{i=1}^{p-1} \left(\sum_{j=1}^{i} a_{l_j}\right)\left(t_{l_i} S_{\mathrm{f_{l_i}},f_{l_k}} - t_{l_{i+1}} S_{\mathrm{f_{l_{i+1}}},f_{l_k}}\right) =$$
$$\sum_{i=1}^{p-1}\left(\sum_{j=1}^{i} a_{l_j}\right) t_{l_i,l_{i+1}} \mathrm{S_{f_{l_i},f_{l_{i+1}}}}.$$

Лемма 8. Множество неразложимых критических сизигий Σ^* получается с помощью следующего алгоритма:

Шаг 1. $\boldsymbol{S \coloneqq \Sigma}$.

Шаг 2. Найти сизигию $s \in S$, представимую в виде $s = t_u u + t_v v$, где $\forall w \in \{u, v\} \subset \Sigma$ выполняется $t_w \in T(K[X])$ и либо $\deg t_w > 1$, либо $\deg t_w = 1$ и $w \notin S$.

Шаг 3. Если сизигия s найдена, то $S \coloneqq S \setminus \{s\}$ и перейти к шагу 2.

Шаг 4. $\Sigma^* \coloneqq S$.

Доказательство. Без ограничения общности можно считать, что $\deg HT(f_1) \prec \deg HT(f_2) \prec \cdots \prec \deg HT(f_m)$. Определим порядок $<$ на Σ формулой:

$$\sigma_1 < \sigma_2 \Leftrightarrow (HT(\sigma_1) < HT(\sigma_2) \vee \left(HT(\sigma_1) = HT(\sigma_2) \wedge LT(\sigma_1) < LT(\sigma_2)\right)).$$

Согласно лемме 3.1 все исключаемые сизигии разложимы. Достаточно проверить, что будут исключены все разложимые сизигии. Пусть это не так. Выберем в множестве Σ^* разложимую сизигию S_{f_i,f_j} наименьшей степени ω, минимальную относительно порядка $<$. Из ее возможных разложений вида (5), для которых $\Sigma_0^{\omega}=\Sigma^{\omega} \setminus \Sigma^*$, выберем разложение наименьшей длины. В этом разложении выберем максимальное относительно порядка $<$ ненулевое слагаемое $c_{\sigma_0} t_{\sigma_0} \sigma_0$, где $\sigma_0 = S_{f_k,f_l}$ и $k > l$ [1]. Тогда $j \le k$.

При $i < j$ положим $S_{f_i,f_j} = \alpha_{i,j} e_i + \beta_{i,j} e_j$.

Пусть $j = k > l$. Тогда из равенства (5) и леммы 7 следует, что $S_{f_i,f_j} = t_{\sigma_0} S_{f_i,f_j} + t_2 S_{f_i,f_l} = t_2 S_{f_i,f_l} - t_{\sigma_0}$.Если $t_2 \ne 1$, то сизигия S_{f_i,f_j} должна быть удалена на шаге 3 и, следовательно, не принадлежит Σ^*. Пусть $t_2 = 1$, тогда

[1] В этом месте доказательства неразложимости сизигий из Σ^* в работе [4] делается неправильное предположение о существовании слагаемого в правой части представления сизигии, старший член которой совпадает со старшим членом разложимой сизигии S_{f_i,f_j}

$S_{f_i,f_l} = S_{f_i,f_j} + t_{\sigma_0}$. Тогда, поскольку $i < j$ и $l < j$, то $S_{f_i,f_l} < S_{f_i,f_j}$ и имеется разложение

$$S_{f_i,f_l} = \left(c_{\sigma_0} - 1\right) t_{\sigma_0} + \sum_{\sigma\in\Sigma'_{\omega},\sigma\ne\sigma_0} c_\sigma\, t_\sigma \sigma,$$

что противоречит свойству минимальности сизигии S_{f_i,f_j}.

Следовательно, $k > j > i$. Положим

$$\boldsymbol{\Sigma}_\omega(\sigma_0) = \left\{\sigma \in \boldsymbol{\Sigma}'_\omega \;\middle|\; HT(t_\sigma) = t_{\sigma_0} t_0 e_k, c_\sigma \ne 0\right\}.$$

Из соотношения (5) и неравенства $k > j > i$ следует, что

$$\sum_{S_{f_l,f_k}\in\Sigma_\omega(\sigma_0)|k>l} c_{S_{f_l,f_k}}\, \mathrm{t}_{f_l,f_k} \alpha_{l,k} e_k = 0.$$

Поэтому

$$\sum_{S_{f_l,f_k}\in\Sigma_\omega(\sigma_0)|k>l} c_{S_{f_l,f_k}} = 0.$$

Тогда к разложению

$$\sum_{S_{f_l,f_k}\in\Sigma'_\omega|k>l} c_{S_{f_l,f_k}}\, \mathrm{t}_{f_l,f_k} S_{f_l,f_k} \qquad (7)$$

применима лемма 7, позволяющая получить новое разложение

$$\sum_{S_{f_l,f_k}\in\Sigma_\omega(\sigma_0)|k>l} \mathrm{c}_{S_{f_l,f_k}}\, \mathrm{t}_{f_l,f_k} S_{f_l,f_k} = \sum_{S_{f_i,f_k}\in\Sigma'^{\omega}|i<k,j<k} d_{S_{f_l,f_k}}\, \mathrm{t}_{S_{f_i,f_j}} S_{f_i,f_j}, \qquad (8)$$

имеющее меньшее число ненулевых слагаемых. Поэтому, заменяя слагаемые вида (7) в разложении (5) с помощью формулы (8), получаем новое разложение сизигии s, имеющее меньшее число слагаемых, что противоречит выбору этой сизигии и ее разложения.

Из леммы 8 следует, что $\Sigma_d = \Sigma \setminus \Sigma^*$ – множество всех разложимых критических сизигий, а из алгоритма построения Σ^* вытекает, что Σ^* является базисом пространства сизигий $S(G)$. При доказательстве леммы 8 был также определен порядок $<$ на множестве критических сизигий.

Лемма 9. Простая редукция относительно множества Σ_d и порядка $<$ на множестве критических сизигий преобразует элемент $\sigma \in \Sigma^*$ в $\sigma' \in \Sigma^*$.

Доказательство. Пусть $\boldsymbol{\sigma \to_{\Sigma_d} \sigma'}$. Тогда $\sigma' \in \Sigma$ и выполняется равенство $\sigma' = \sigma - \sigma_1$, где $\sigma_1 \in \Sigma_d$. Пусть $\sigma' \in \Sigma_d$. Тогда $\sigma = \sigma' + \sigma_1 \in \Sigma_d$, что противоречит условию $\sigma \in \Sigma^* = \Sigma \setminus \Sigma_d$. Следовательно, $\sigma' \in \Sigma^*$.

Поэтому определена полная редукция сизигий из множества Σ^* относительно множества разложимых сизигий Σ_d, задающая отображение $\Sigma^* \to \Sigma^*$. Образ этого отображения обозначим через Σ^{**}. Относительно этого множества справедлива

Лемма 10. Множество Σ^{**} является базисом $K[X]$-модуля сизигий $S(F)$, и при

выполнении соотношения

$$\sum_{\mathbf{\sigma}\in\mathbf{\Sigma}^{**}} \mathrm{a}_{\mathbf{\sigma}}\mathbf{\sigma} = \sum_{\sigma\in\Sigma_d} p_\sigma, \quad \textit{где}\ \mathbf{\Sigma}^{**} = \{\mathbf{\sigma}\in\mathbf{\Sigma}^{**} \mid \deg\mathbf{\sigma} = \mathbf{\omega}\}, \mathrm{a}_{\mathbf{\sigma}}\in \mathrm{K}, \qquad (9)$$

всегда

$$\sum_{\sigma\in\Sigma_d} p_\sigma\,\sigma = 0.$$

Доказательство. Пусть это не так. Среди разложений вида (9) выберем соотношение, с ненулевой правой частью минимальной длины. Без ограничения общности можно считать, что $\deg(p_\sigma\sigma) = \omega$ и p_σ – мономы. Высотой критической сизигии $\sigma = \alpha e_f + \beta e_g$ будем называть e_f, если $f \succ g$, или e_g в противном случае. Высоту сизигии σ обозначим через $\mathrm{V}(\sigma)$. Положим

$$L = \{\sigma\in\Sigma_d | p_\sigma \neq 0\},$$
$$e = \max_{\sigma\in\mathrm{L}} \mathrm{V}(\sigma),$$

и

$$L_0 = \{\sigma\in L | \mathrm{V}(\sigma) = e\}.$$

Тогда из определения Σ^{**}следует, что

$$\forall \alpha e_f + \beta e_g \in \Sigma^{**} \forall \tau\in L\ e_f \neq e, e_g \neq e.$$

Поэтому из условия (9) следует, что $\sum_{\sigma\in L_0} p_\sigma \mathrm{HT}\sigma = 0$ и, следовательно, воспользовавшись леммой 7 для разложения

$$s = \sum_{\sigma\in L_0} p_\sigma\,\sigma,$$

получим разложение

$$s = \sum_{\sigma\in L_1} q_\sigma\,\sigma, \text{ где } L_1 \subset \Sigma_d,$$

меньшей длины. Поэтому имеется соотношение вида (9) с правой частью меньшей длины.

Для любого $L\subset\Sigma^*$ определен максимальный элемент в L. Обозначим этот элемент через $M(L)$.

Лемма 11. Пусть Σ^{***} – результат следующего алгоритма:

Шаг 1. $S^{***} \coloneqq \emptyset, T \coloneqq \mathbf{\Sigma}^{**}$.

Шаг 2. Пусть σ – нормальная форма (см. определение 1.6) элемента $M(T)$ относительно множества $T \setminus \{M(T)\}$.

Шаг 3. Если $\sigma \neq 0$, то $S^{***} \coloneqq S^{***} \cup \{\sigma\}$.

Шаг 4. $T \coloneqq T \setminus \{M(T)\}$.

Шаг 5. Если $T \neq \emptyset$ перейти к шагу 2.

Шаг 6. $\Sigma^{***} \coloneqq S^{***}$.

Тогда Σ^{***} является минимальным базисом $K[X]$-модуля сизигий $\mathcal{S}(F)$.

Доказательство. Каждый раз на шаге 4 данного алгоритма множество сизигий $S^{***}\cup T$ является базисом $K[X]$-модуля сизигий $\mathcal{S}(F)$. Поэтому достаточно

доказать минимальность базиса Σ^{***}.

Пусть $\Sigma^{***} = \{s_1, \dots, s_k\}$. В силу леммы Накаямы достаточно проверить линейную независимость элементов Σ^{***}, т.е. проверить, что любая однородная линейная комбинация элементов из Σ^{***}, неразложима. Пусть это не так. В силу леммы 10 это означает, что имеется нетривиальная линейная комбинация элементов из Σ^{***}, равная нулю

$$\sum_{i=1}^{k} \alpha_i\, s_i = 0, \alpha_i \in K. \qquad (10)$$

Пусть e – старший терм этого разложения. Тогда этот терм является одновременно старшим термов по крайней мере двух слагаемых разложения (10). Без ограничения общности можно считать, что этими слагаемыми являются $\alpha_1 s_1$ и $\alpha_2 s_2$, что невозможно виду шага 2 алгоритма, поскольку этот старший член должен исчезнуть при приведении к нормальной форме. Следовательно, согласно лемме Накаямы Σ^{***} является минимальным базисом.

Список литературы

[1]. Gebauer R., Moller H.M. On an Instalation of Buchberger's Algorithm. Journal of Symbolic Computation, no. 6, 1987, pp. 257-286..

[2]. Caboara M., Kreuzer M., Robbiano L. Efficiently computing minimal sets of critical pairs, Journal of Symbolic Computation, No. 38, 2004, pp. 1169-1190.

[3]. Ленг С.. Алгебра. Москва, Мир, 1968.

[4]. Агиевич С.В. Усовершенствованый алгоритм Бухбергера. Труды Института математики НАН Беларуси, том 20, no. 1, 2012, стр. 3-13.

[5]. Buchberger B. Grobner Bases: An Algorithmic Method in Polynomial Ideal. In Multidimensional Systems Theory and Applications, 1985, pp. 184-232.

Minimal basis of the syzygies module of leading terms

A.V. Sokurov <shok@ispras.ru>

Ivannikov Institute for System Programming of the Russian Academy of Sciences, 25, Alexander Solzhenitsyn st., Moscow, 109004, Russia

Abstract. Systems of polynomial equations are one of the most universal mathematical objects. Almost all the problems of cryptographic analysis can be reduced to finding solutions to systems of polynomial equations. The corresponding direction of research is called algebraic cryptanalysis. In terms of computational complexity, systems of polynomial equations cover the entire range of possible options, from algorithmic insolubility of Diophantine equations to well-known efficient methods for solving linear systems. The method of Buchberger [5] brings a system of algebraic equations to the system of a special type defined by the Gröbner original system of equations, allowing the use of the exception of the dependent variables. The basis for determining the Groebner basis is the permissible ordering on the set of terms. The set of admissible orderings on the set of terms is infinite and even continuum. The most time-consuming step in finding the Groebner basis using the Buchberger algorithm is to prove that all S-polynomials representing a system of generators of K[X]-module S-polynomials. There is a natural problem of finding such a minimal system of generators. The existence of such a

system of generators follows from Nakayama's theorem. An algorithm for constructing such a basis for any ordering is proposed.

Keywords: polynomial ring; field; ideal; syzygy; Groebner basis; Buchberger algorithm; admissible order

DOI: 10.15514/ISPRAS-2018-30(6)-16

For citation: Sokurov A.V. Minimal basis of the syzygies module of leading terms. Trudy ISP RAN/Proc. ISP RAS, vol. 30, issue 6, 2018, pp. 293-304 (in Russian). DOI: 10.15514/ISPRAS-2018-30(6)-16

References

[1]. Gebauer R., Moller H.M. On an Instalation of Buchberger's Algorithm. Journal of Symbolic Computation, no. 6, 1987, pp. 257-286.
[2]. Caboara M., Kreuzer M., Robbiano L. Efficiently computing minimal sets of critical pairs. Journal of Symbolic Computation, no. 38, 2004, pp. 1169-1190.
[3]. Lang S. Algebra. Addison-Wesley Publishing Company Reading, 1965.
[4]. Agievich S. V. Improved Buchberger algorithm. Proceedings of the Institute of Mathematics, National Academy of Sciences of Belarus, vol. 20, issue 1, 2012, pp. 3-13 (in Russian).
[5]. Buchberger B. Grobner Bases: An Algorithmic Method in Polynomial Ideal. In Multidimensional Systems Theory and Applications, 1985, pp. 184-232.