Усовершенствованный алгоритм Бухбергера

С. В. Агиевич
Научно-исследовательский институт прикладных проблем математики и информатики
Белорусский государственный университет
пр. Независимости 4, 220030 Минск, Беларусь
agievich@bsu.by

Аннотация

Предлагается усовершенствованный алгоритм Бухбергера, в котором учтены известные и использованы новые критерии исключения критических пар. Новые критерии основаны на построении минимальной системы образующих модуля, который порождается критическими сизигиями.

1 Алгоритм Бухбергера

Пусть K — поле, $P = K[x_1, \dots, x_n]$ — кольцо многочленов от переменных $x_1, \dots, x_n$ над полем K, T — множество мономов от этих переменных, $<$ — допустимый мономиальный порядок на T (подробнее см. [1]). Для ненулевого $f \in P$ пишем: $\mathtt{LM}(f)$ — старший (относительно порядка $<$) моном f, $\mathtt{LC}(f)$ — коэффициент при старшем мономе, $\mathtt{LT}(f) = \mathtt{LC}(f) \cdot \mathtt{LM}(f)$ — старший член.

Пусть $G = \{g_1, \dots, g_r\}$ — система ненулевых многочленов P. Если f содержит член ct, $c \in K$, $t \in T$, который делится на некоторый $\mathtt{LM}(g_i)$, то мы можем исключить данный член, заменив f на $f - cg_it/\mathtt{LT}(g_i)$. Последовательно исключая самые старшие подходящие члены f, мы в конце концов получим представление $f = h_1g_1 + \dots + h_rg_r + g$, где $h_i \in P$, $\mathtt{LM}(h_ig_i) \leq \mathtt{LM}(f)$ и в g нет членов, которые делятся на $\mathtt{LM}(g_i)$. Многочлен g является остатком от деления f на G, что записывается как $f \xrightarrow{G} g$.

Остаток g определен, вообще говоря, неоднозначно, поскольку на шагах деления $f \leftarrow f - cg_it/\mathtt{LT}(g_i)$ могут встретиться сразу несколько делителей g_i таких, что $\mathtt{LM}(g_i) \mid t$. В таких случаях будем отдавать предпочтение многочлену g_i с минимальным индексом i, а соответствующий данной цепочке делений остаток обозначать через $\bar{f}^G$. Для пустой системы G полагаем $\bar{f}^G = f$.

Пусть I — идеал кольца P. Система G называется *базисом Грёбнера* I, если для любого ненулевого $f \in I$ найдется $g_i \in G$ такой, что $\mathtt{LM}(g_i) \mid \mathtt{LM}(f)$. Эквивалентно, G — базис Грёбнера, если остаток от деления f на G всегда нулевой, независимо от порядка делителей.

Базисы Грёбнера обладают рядом замечательных свойств, что делает их нахождение важным при решении многих задач теории кодирования, теории инвариантов, криптографии и других математических дисциплин. В частности, с помощью базисов Грёбнера можно описывать решения систем полиномиальных уравнений.

Для нахождения базисов Грёбнера используется алгоритм Бухбергера, который основан на следующем критерии: G — базис Грёбнера тогда и только тогда, когда $S(g_i, g_j) \xrightarrow{G} 0$ для любых $g_i, g_j \in G$. Здесь $S(g_i, g_j)$ — так называемый *S-многочлен* пары (g_i, g_j):

$$S(g_i, g_j) = \frac{[\mathtt{LM}(g_i), \mathtt{LM}(g_j)]}{\mathtt{LT}(g_i)} g_i - \frac{[\mathtt{LM}(g_i), \mathtt{LM}(g_j)]}{\mathtt{LT}(g_j)} g_j,$$

$[\mathtt{LM}(g_i), \mathtt{LM}(g_j)]$ — н.о.к. мономов $\mathtt{LM}(g_i)$ и $\mathtt{LM}(g_j)$.

Алгоритм Бухбергера

Вход: $F \subset P$, порядок $<$.
Выход: $G \subset P$ — базис Грёбнера идеала $\langle F \rangle$ относительно порядка $<$.
Вспомогательные алгоритмы: `Update`.
Шаги:

1. $G \leftarrow \varnothing$, $B \leftarrow \varnothing$, $B^* \leftarrow \varnothing$.
2. Для всех $f \in F$:
   (a) $g \leftarrow \bar{f}^G$;
   (b) если $g \neq 0$, то $(G, B) \leftarrow \texttt{Update}(G, B, B^*, g)$.
3. Пока $B \neq \varnothing$:
   (a) выбрать $(g_i, g_j) \in B$,
   (b) $B \leftarrow B \setminus \{(g_i, g_j)\}$, $B^* \leftarrow B^* \cup \{(g_i, g_j)\}$;
   (c) $g \leftarrow \overline{S(g_i, g_j)}^G$;
   (d) если $g \neq 0$, то $(G, B) \leftarrow \texttt{Update}(G, B, B^*, g)$.
4. Возвратить G.

Алгоритм Update (обновление в алгоритме Бухбергера)

Вход: $G \subset P$, $B \subset P \times P$, $B^* \subset P \times P$, $g \in P \setminus \{0\}$.
Выход: обновленные G и B.
Шаги:

1. $G \leftarrow G \cup \{g\}$.
2. $B \leftarrow B \cup \{(f, g) \colon f \in G\}$.
3. Возвратить (G, B).

Элементы множества B в алгоритме Бухбергера принято называть *критическими парами*. Критические пары определяют S-многочлены $S(g_i, g_j)$, по которым, в свою очередь, вычисляются остатки g. Обработанные критические пары переносятся из B в B^*. Множество B^*, пока избыточное, будет использоваться в предлагаемом далее усовершенствовании алгоритма.

Нахождение остатков является самым трудоемким шагом алгоритма Бухбергера. С другой стороны, вычислительные эксперименты показывают, что большинство остатков оказываются нулевыми, т. е. бесполезными. Для того, чтобы избежать бесполезных вычислений, усовершенствованные редакции алгоритма Бухбергера снабжаются дополнительными механизмами исключения некоторых критических пар. Данные механизмы основаны на том, что только по старшим мономам многочленов g_i и g_j можно сделать вывод $S(g_i, g_j) \xrightarrow{H} 0$, где H — множество многочленов, которые содержатся в G или будут включены в G на следующих шагах алгоритма Бухбергера. Указанный вывод позволяет исключить пару (g_i, g_j) из B, даже не выполняя деление.

Известны следующие механизмы исключения критических пар: исключение по критериям Бухбергера [1], исключение r-пар [2], исключение по критериям Гебауэра — Мюллера [4], построение минимальной системы образующих модуля сизигий старших мономов G [3]. В качестве примера, первый критерий Бухбергера позволяет исключить пару (g_i, g_j), у которой нет зацепления (старших мономов), т. е. старшие мономы взаимно просты: $[\mathtt{LM}(g_i), \mathtt{LM}(g_j)] = \mathtt{LM}(g_i) \cdot \mathtt{LM}(g_j)$. Для такой пары $S(g_i, g_j) \overset{\{g_i,g_j\}}{\to} 0$.

Нами предлагается усовершенствованный алгоритм Бухбергера, в котором явно или косвенно использованы все перечисленные механизмы исключения критических пар. Усовершенствование состоит в замене алгоритма `Update` на алгоритм `UpdateEx`:

Алгоритм UpdateEx (усовершенствованное обновление)

Вход: $G \subset P$, $B \subset P \times P$, $B^* \subset P \times P$, $g \in P \setminus \{0\}$.
Выход: обновленные G и B.
Шаги:

1. Исключить из B пары (f, h) такие, что $\mathtt{LM}(h) \not| \, \mathtt{LM}(f)$ и $\mathtt{LM}(g) \mid [\mathtt{LM}(f), \mathtt{LM}(h)]$.
2. Для всех $f \in G$: если $\mathtt{LM}(g) \mid \mathtt{LM}(f)$, то $G \leftarrow G \setminus \{f\}$, $B \leftarrow B \cup \{(f, g)\}$.
3. $R \leftarrow \{(f, g) \colon f \in G\}$.
4. Для всех пар $(f, g) \in R$ с зацеплением: если найдется другая пара $(h, g) \in R$, для которой
   1) $[\mathtt{LM}(h), \mathtt{LM}(g)] \mid [\mathtt{LM}(f), \mathtt{LM}(g)]$,
   2) $\mathtt{LM}(g) \not| [\mathtt{LM}(f), \mathtt{LM}(h)]$ или $\mathtt{LM}(g) \mid [\mathtt{LM}(f), \mathtt{LM}(h)]$ и $B^* \cap \{(f, h), (h, f)\} \neq \varnothing$,

   то исключить (f, g) из R.
5. Исключить из R пары без зацепления.
6. $G \leftarrow G \cup \{g\}$.
7. $B \leftarrow B \cup R$.
8. Возвратить (G, B).

В разделе 4 мы объясним принципы, заложенные в основу алгоритма `UpdateEx`, и обоснуем корректность замены `Update` на `UpdateEx`. Мы докажем следующий результат:

Предложение 1. Замена в алгоритме Бухбергера вспомогательного алгоритма `Update` на `UpdateEx` корректна.

Предварительно в разделах 2, 3 мы получим вспомогательные результаты, которые касаются алгебраических структур, построенным по старшим мономам многочленов G. Отметим, что в `UpdateEx` используется информация только об этих старших мономах.

На сегодняшний день лучшим среди алгоритмов обновления критических пар, в которых используется информация только о $\mathtt{LM}(G)$, признается (см. например [5]) алгоритм с условным название `UpdateGMI`, основанный на критериях из работы [4] и первом критерии Бухбергера. Нами проведены вычислительные эксперименты по сравнению `UpdateGMI` с `UpdateEx`. В экспериментах обрабатывались системы над полем из двух элементов. Установлено, что для систем общего вида (не являющихся сильно структурированными) при использовании `UpdateEx` требуется обрабатывать на 6-12% меньше пар, чем при использовании `UpdateGMI`.

2 Сизигии старших мономов

Вернемся к системе многочленов $G = \{g_1, \dots, g_r\}$, которая используется в алгоритме Бухбергера. Старший член g_i обозначим через t_i, а коэффициент при старшем члене — через c_i. Пусть $[t_i, t_j]$ — н.о.к. t_i и t_j,

$$t_{ij} = \frac{[t_i, t_j]}{t_i}, \quad t_{ji} = \frac{[t_i, t_j]}{t_j}.$$

Набор $s = (s_1, \dots, s_r) \in P^r$ называется *сизигией* старших мономов G, если $\sum_{i=1}^{r} s_i \,\mathtt{LM}(g_i) = 0$. Множество всех сизигий обозначим через M.

Сизигию $s = (s_1, \dots, s_r)$ удобно записывать в виде $\sum s_i e_i$, где $\{e_1, \dots, e_r\}$ — стандартный базис P^r. Так S-многочлену $S(g_i, g_j)$ соответствует сизигия

$$\sigma_{ij} = \frac{t_{ij}}{c_i} e_i - \frac{t_{ji}}{c_j} e_j.$$

Такие сизигии называются *критическими*. Везде далее при записи σ_{ij} считаем, что $i < j$. Пусть $\Sigma = \{\sigma_{ij} \colon 1 \le i < j \le r\}$.

Выражения te_i, $t \in T$, $1 \le i \le r$, называются *маркированными мономами*. Пусть $T\langle e_1, \dots, e_r\rangle$ — множество всех таких мономов. Распространим порядок $<$ на множество $T\langle e_1, \dots, e_r\rangle$: $te_i \le t'e_j$, если $tt_i < t't_j$ (сравнение в T) или $tt_i = t't_j$ и $i \le j$. Для маркированных мономов определено отношение делимости: $te_i \mid t'e_j$, если $i = j$ и $t \mid t'$.

Сизигию $s = \sum s_i e_i$ можно рассматривать как линейную комбинацию (над K) маркированных мономов. Как и в случае многочленов, $\mathtt{LM}(s)$ — старший маркированный моном s.

Уровнем маркированного монома $m = te_i$ назовем произведение $\tau(m) = tt_i$. Уровнем сизигии назовем максимальный уровень входящих в нее маркированных мономов. Сизигия однородна, если она является суммой маркированных мономов одного уровня. Понятно, что критические сизигии — однородны. Понятно также, что всякую сизигию можно представить в виде суммы однородных компонент.

Множество M является P-модулем. Базисом Грёбнера данного модуля относительно порядка $<$ на $T\langle e_1, \dots, e_r\rangle$ называется система $s_1, \dots, s_n \in M$, которая обладает следующим свойством: для любого $s \in M$ найдется индекс $i \in \{1, \dots, n\}$ такой, что $\mathtt{LM}(s_i) \mid \mathtt{LM}(s)$. Известно, что Σ является базисом Грёбнера M (см. например [3]).

Далее нам потребуется использовать связи между тройками критических сизигий σ_{ij}, σ_{ik} и σ_{jk} $(i < j < k)$. Предположим, что $t_k \mid [t_i, t_j]$ и, следовательно, $[t_i, t_k] \mid [t_i, t_j]$ и $[t_j, t_k] \mid [t_i, t_j]$. Пусть

$$t = \frac{[t_i, t_j]}{[t_i, t_k]}, \quad t' = \frac{[t_i, t_j]}{[t_j, t_k]}.$$

Тогда $t_{ij} = t_{ik}t$, $t_{ji} = t_{jk}t'$, $t_{ki}t = t_{kj}t'$ и

$$\begin{aligned}\sigma_{ij} &= \left(\frac{t_{ik}t}{c_i} e_i - \frac{t_{ji}}{c_j} e_j\right) + \frac{t_{ki}t}{c_k} e_k - \frac{t_{ki}t}{c_k} e_k = \\ &= -t\left(\frac{t_{ki}}{c_k} e_k - \frac{t_{ik}}{c_i} e_i\right) + \left(\frac{t_{ki}t}{c_k} e_k - \frac{t_{ji}}{c_j} e_j\right) = t'\sigma_{kj} - t\sigma_{ki}.\end{aligned}$$

Полученное равенство является следствием того, что $t_k \mid [t_i, t_j]$. Равенство получено при ограничениях $k < i < j$, но его можно распространить и на другие варианты расположения индекса k относительно индексов i и j:

$$\begin{aligned}\sigma_{ij} &= t\sigma_{ik} + t'\sigma_{kj} \quad i < k < j, \\ \sigma_{ij} &= t\sigma_{ik} - t'\sigma_{jk} \quad i < j < k.\end{aligned}$$

Равенства такого типа будем записывать в виде

$$s = \pm t_u u \pm t_v v, \qquad s, u, v \in \Sigma, \quad t_u, t_v \in T.$$

3 Минимальная система образующих модуля сизигий

В этом разделе мы определим алгоритм построения минимальной (по числу элементов) системы образующих модуля M. Минимальная система определяет правила исключения критических пар на шагах алгоритма Бухбергера. При этом исключается максимальное количество пар, какое только можно исключить по информации о старших мономах входящих в них многочленов.

Для $S \subseteq M$ через S_t, $S_{<t}$, $S_{\leq t}$ будем обозначать подмножества S, составленные из сизигий уровня t, $< t$, $\leq t$ соответственно. Будем говорить, что сизигия $s \in M \setminus \{0\}$ *разложима*, если найдется представление

$$s = \sum_{u \in M_{<\tau(s)}} f_u u, \quad f_u \in P. \tag{1}$$

Если представления (1) не существует, то s — *неразложима*. Нулевая сизигия считается разложимой.

Поскольку Σ — базис Грёбнера, ненулевые u в правой части (1) можно представить в виде

$$u = \sum_{\sigma \in \Sigma_{\leq \tau(u)}} g_\sigma \sigma, \quad g_\sigma \in P.$$

Поэтому представление (1) можно заменить на представление

$$s = \sum_{\sigma \in \Sigma_{<\tau(s)}} h_\sigma \sigma, \quad h_\sigma \in P. \tag{2}$$

Исключим из M все сизигии, удовлетворяющие (1) или (2) и обозначим оставшееся множество через M^*. Пусть $\Sigma^* = \Sigma \cap M^*$ — множество неразложимых критических сизигий.

Предложение 2. Множество Σ^* можно построить с помощью следующего алгоритма:

1. $S \leftarrow \Sigma$.
2. Найти сизигию $s \in S$, которая представляется в виде $s = \pm t_u u \pm t_v v$, где для $w \in \{u, v\}$: $w \in \Sigma$, $t_w \in T$, причем либо $t_w \neq 1$, либо $t_w = 1$ и $w \notin S$.
3. Если искомая сизигия s найдена, то $S \leftarrow S \setminus \{s\}$ и возвратиться к шагу 2.
4. Возвратить S.

Доказательство. Во-первых, докажем, что на шаге 3 действительно исключаются сизигии $s \notin \Sigma^*$. Первая исключаемая сизигия имеет вид $s = \pm t_u u \pm t_v v$, где $t_u, t_v \neq 1$ и, следовательно, $\tau(u) < \tau(s)$ и $\tau(v) < \tau(s)$. Поэтому s соответствует (1) и не принадлежит Σ^*. Каждая следующая исключаемая сизигия является суммой слагаемых $\pm t_w w$, где

- либо $t_w \neq 1$ и, следовательно, $\tau(w) < \tau(s)$;
- либо $t_w = 1$ и $w \notin S$, т. е. w представляется слагаемыми уровня $< \tau(w) = \tau(s)$.

В обоих случаях $s \notin \Sigma^*$.

Во-вторых, докажем, что на шаге 3 будут исключены все сизигии $s \notin \Sigma^*$. Такие сизигии можно представить в виде

$$s = \sum_{\sigma \in \Sigma_{<\tau(s)}} \alpha_\sigma t_\sigma \sigma,$$

где $\alpha_\sigma \in K$, $t_\sigma \in T$ и для $\alpha_\sigma \neq 0$ уровень $\tau(s) = t_\sigma \tau(\sigma)$.

Среди слагаемых в правой части найдется $\alpha_u t_u u$ такое, что $\alpha_u \neq 0$ и старшие мономы s и $t_u u$ совпадают. Это значит, что $s - t_u u = \pm t_v v$ для некоторых $t_v \in T$ и $v \in \Sigma$.

Если $t_v \neq 1$, то сизигия s будет исключена из S, так как представляется в виде $t_u u \pm t_v v$ при $t_u, t_v \neq 1$.

Если $t_v = 1$, то s будет исключена при условии, что v будет исключена. Но

$$v = \mp(\alpha_u - 1)t_u u \mp \sum_{\substack{\sigma \in \Sigma_{<\tau(v)} \\ \sigma \neq u}} \alpha_\sigma t_\sigma \sigma.$$

В соответствии с данным представлением сизигия $v \notin \Sigma^*$ и ее можно обработать также, как и s. Важно, что $v < s$. Можно продолжить индуктивные рассуждения и в конце концов доказать, что v будет исключена алгоритмом и, следовательно, s также будет исключена.□

Предложение 3. $\langle \Sigma^* \rangle = M$.

Доказательство. Множество Σ^* получается из Σ применением алгоритма из предыдущего предложения. Алгоритм работает так, что для текущего S исключается сизигия $s \in S$, которая представляется сизигиями меньших уровней. Это значит, что при исключении каждой s выполняется $s \in \langle S \setminus \{s\} \rangle$ и, следовательно, $\langle S \rangle = \langle S \setminus \{s\} \rangle$. Поскольку первоначально $S = \Sigma$ и $\langle \Sigma \rangle = M$, получаем нужный результат. □

Хотя Σ^* состоит только из неразложимых сизигий, разложимыми могут быть их линейные комбинации. В следующем предложении определен алгоритм, который устраняет линейно избыточные элементы Σ^*.

Предложение 4. Пусть Σ^{**} — результат работы следующего алгоритма:

1. $S \leftarrow \Sigma^*$.
2. Найти сизигию $s \in S$, которая представляется в виде $s = \pm u \pm t_v v$, где $u \in S$, $t_v \in T$, $v \in \Sigma$, причем либо $t_v \neq 1$, либо $t_v = 1$ и $v \in S$.
3. Если искомая сизигия s найдена, то $S \leftarrow S \setminus \{s\}$ и возвратиться к шагу 2.
4. Возвратить S.

Тогда всякая нетривиальная линейная комбинация элементов Σ^{**} является неразложимой.

Доказательство. Пусть $\Sigma^* = \{s_1, s_2, \ldots, s_n\}$ и для некоторых не равных одновременно нулю $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ линейная комбинация $\sum_{i=1}^n \alpha_i s_i$ разложима, т. е. совпадает с сизигией $w \notin M^*$.

Пусть, не нарушая общности, $s_1 = \max_{i:\, \alpha_i \neq 0} s_i$. Старший моном s_1 совпадает со старшим мономом некоторой сизигии $u = s_i$ или, если это не так, со старшим мономом сизигии $t_v v$, $t_v \neq 1$, $v \in \Sigma$, которая входит в разложение w.

В первом случае $s_1 - u = \pm t_v v$ для некоторых $t_v \in T$ и $v \in \Sigma$. При этом либо сизигия $s_1 - u$ разложима, либо $t_v = 1$, $v \in \Sigma^*$ и разложима нулевая сизигия $s_1 - u \mp v$.

Во втором случае $s_1 - t_v v = \pm t_u u$, где $t_u \in T$, $u \in \Sigma$. Сизигия $s_1 = \pm t_u u + t_v v$ неразложима. Поэтому $t_u = 1$ и $u \in \Sigma^*$.

В обоих случаях будет найдена разложимая линейная комбинация $s_1 \pm u$ или $s_1 \pm u \pm v$, в которой $u, v \in \Sigma^*$ и $u, v < s_1$. Домножим найденную линейную комбинацию на α_1 и вычтем ее из первоначальной комбинации $\sum_{i=1}^n \alpha_i s_i$. Получим линейную комбинацию элементов Σ^*, которая снова является разложимой и в которой максимальная сизигия меньше s_1.

Новую линейную комбинацию можно обработать также, как первоначальную. Рассуждения можно продолжить и установить, что всякая разложимая линейная комбинация является линейной комбинацией базовых разложимых комбинаций вида $s \pm u$ или $s \pm u \pm v$.

Поскольку алгоритм построения Σ^{**} исключает хотя бы один элемент во всякой базовой комбинации, исходная линейная комбинация, составленная только из элементов Σ^{**}, не может существовать. Это и требовалось доказать. □

Множество Σ^{**} определено, вообще говоря, неоднозначно, в зависимости от выбора подходящих элементов s на шаге 2. Тем не менее, при любом порядке выбора s справедлив следующий результат.

Предложение 5. Множество Σ^{**} является минимальной системой образующих M.

Доказательство. Множество Σ^{**} получается из Σ^* применением алгоритма из предыдущего предложения. Алгоритм работает так, что для текущего S исключается сизигия $s \in S$, которая вхожит в разложимую линейную комбинацию. Это значит, что при исключении каждой s выполняется $s \in \langle S \setminus \{s\}\rangle$ и $\langle S\rangle = \langle S \setminus \{s\}\rangle$. Первоначально $S = \Sigma^*$, причем $\langle \Sigma^*\rangle = M$. Поэтому Σ^{**} является системой образующих M.

Докажем, что Σ^{**} является минимальной системой образующих. Пусть $\Sigma^{**} = \{s_1, s_2, \ldots, s_n\}$ и пусть $\{b_1, b_2, \ldots, b_m\}$ — еще одна система образующих. Предположим, что $m < n$.

Элементы s_i выражаются через b_j:

$$s_i = \sum_{j=1}^{m} \beta_{ij} b_j + \sum_{j=1}^{m} h_{ij} b_j, \quad i = 1, \ldots, n,$$

где $\beta_{ij} \in K$, $h_{ij} \in P$, причем ненулевые h_{ij} не имеют свободных членов.

Поскольку $m < n$, существуют не равные одновременно нулю $\alpha_1, \ldots, \alpha_n \in K$ такие, что

$$\sum_{i=1}^{n} \alpha_i s_i = \sum_{i=1}^{n} \alpha_i h_{ij} b_i.$$

Пусть t — максимальный уровень s_i, для которых $\alpha_i \neq 0$. Выделим в левой и правой частях предыдущего соотношения сизигии уровня t:

$$\sum_{\alpha_i \neq 0, \tau(s_i) = t} \alpha_i s_i = \sum_{\alpha_i \neq 0, \tau(t_i \pi) = t} \alpha_i t_i b_i(\pi),$$

где $b_i(\pi)$ — однородная часть (уровня π) сизигии b_i, $t_i \in T \cup \{0\}$, причем $t_i \neq 1$ (в силу того, что h_{ij} не содержат свободных членов).

Но полученное равенство означает, что среди элементов Σ^{**} имеется линейное соотношение, что противоречит предложению 4. □

При выполнении алгоритма Бухбергера критические сизигии добавляются порциями $\{\sigma_{ik} \colon 1 \leq i < k\}$, $k = 2, 3, \ldots, r$. Адаптируем алгоритмы предложений 2, 4 с учетом данной специфики. Будем писать $t \mid_{\neq} t'$, если t является собственным делителем t'.

Предложение 6. Следующий алгоритм возвращает минимальную систему образующих M:

1. $S \leftarrow \Sigma$.
2. Для $k = 2, \ldots, r$ выполнить:
   (a) исключить из S сизигии σ_{ij} такие, что $i, j < k$ и $t_k \mid [t_i, t_j]$;
   (b) исключить из S сизигии σ_{jk}, для которых найдется $\sigma_{ik} \in S$ со свойствами: $[t_i, t_k] \mid_{\neq} [t_j, t_k]$, $t_k \not| [t_i, t_j]$;
   (c) исключить из S сизигии σ_{ik}, для которых найдется $\sigma_{jk} \in S$ со свойствами: $i < j$, $[t_i, t_k] = [t_j, t_k]$, $t_k \not| [t_i, t_j]$.
3. Возвратить S.

Доказательство. Пусть $i < j < k$ и $\gamma = [t_i, t_j, t_k]$. Для сизигий σ_{ij}, σ_{ik} и σ_{jk} справедливо соотношение

$$\gamma_{jk}\sigma_{jk} - \gamma_{ik}\sigma_{ik} + \gamma_{ij}\sigma_{ij} = 0,$$

где

$$\gamma_{ij} = \frac{\gamma}{\tau(\sigma_{ij})},\ \gamma_{ik} = \frac{\gamma}{\tau(\sigma_{ik})},\ \gamma_{jk} = \frac{\gamma}{\tau(\sigma_{jk})}.$$

Если некоторый из мономов γ_{ij}, γ_{ik} или γ_{jk} равняется 1, то соответствующая сизигия может быть исключена на шагах алгоритмов предложений 2, 4.

Может оказаться так, что сразу несколько мономов равняются 1. Анализируемый алгоритм работает так, что в таких случаях исключается меньшая сизигия. Конкретнее,

a) если $t_k \mid [t_i, t_j]$, то $\gamma_{ij} = 1$ и на шаге 2a исключается сизигия σ_{ij};

b) если $t_k \not| [t_i, t_j]$, $[t_i, t_k] \mid_{\neq} [t_j, t_k]$, то $\gamma_{jk} = 1$, $\gamma_{ij} \neq 1$, $\gamma_{ik} \neq 1$ и на шаге 2b исключается сизигия σ_{jk};

c) если $t_k \not| [t_i, t_j]$, $[t_i, t_k] = [t_j, t_k]$, то $\gamma_{ik} = 1$, $\gamma_{ij} \neq 1$ и на шаге 2c исключается сизигия σ_{ik}.

Алгоритм исключит все разложимые сизигии. Действительно, пусть σ_{jk} — разложимая сизигия, т. е.

$$\sigma_{jk} = \sum_{u \in \Sigma_{<\tau(\sigma_{jk})}} \alpha_u t_u u.$$

Среди u с ненулевыми α_u найдется сизигия, которая содержит маркированный моном te_k. Это либо сизигия вида σ_{ik}, либо сизигия вида σ_{kl}. В обоих случаях уровень сизигии делит уровень $\tau(\sigma_{jk})$, не совпадая с ним. В первом случае σ_{jk} будет исключена на шаге 2b. Во втором случае $t_l \mid [t_j, t_k]$ и σ_{jk} будет исключена на шаге 2a.

Для неразложимых сизигий выполняются все исключения алгоритма, определенного в предложении 4. Действительно, если некоторая из линейных комбинаций $\sigma_{ij} + \sigma_{ik}$, $\sigma_{ij} - \sigma_{jk}$ или $\sigma_{ij} - \sigma_{jk} + \sigma_{ik}$ разложима, то алгоритм исключит сизигию σ_{ij} на шаге 2a. Если разложима линейная комбинация $\sigma_{jk} - \sigma_{ik}$, то алгоритм исключит сизигию σ_{ik} на шаге 2c.

Применяя предложение 5, получаем нужный результат. □

Вернемся к правилам исключения сизигий σ_{ij}, σ_{ik}, σ_{jk}, описанным в доказательстве. В работе [4] предложены похожие правила. Отличие состоит в том, что при совпадении с 1 сразу нескольких мономов γ_{ij}, γ_{ik}, γ_{jk} исключается не меньшая, а большая из соответствующих сизигий. Как показано в [3], правила исключения [4] в общем случае не позволяют построить минимальную систему образующих M. Для того, чтобы построить минимальную систему, сохранив эти правила, в [3] предложено использовать не только текущее множество S (в терминах алгоритма предложения 6), но и ранее исключенные неразложимые сизигии.

Отметим, что предложенные в [3] алгоритмы построения минимальной системы образующих M имеют ограничения: многочлены G должны быть однородными, порядок на T должен быть градуированным. Алгоритм предложения 6 годится для общего случая.

4 Обоснование алгоритма `UpdateEx`

Перейдем к доказательству предложения 1. Определим промежуточные между `Update` и `UpdateEx` алгоритмы `Update1`, `Update2`, `Update3` и обоснуем корректность переходов между алгоритмами.

Пусть $S \subseteq \Sigma$ — некоторая система образующих модуля M. Тогда любую сизигию $\sigma_{ij} \in \Sigma$ можно выразить через сизигии из S:

$$\sigma_{ij} = \sum_{\sigma_{kl} \in S} h_{kl}\sigma_{kl}, \quad h_{kl} \in P.$$

Такие же выражения справедливы для соответствующих S-многочленов:

$$S(g_i, g_j) = \sum_{\sigma_{kl} \in S} h_{kl} S(g_k, g_l).$$

Поэтому если $S(g_k, g_l) \xrightarrow{G} 0$ для всех $\sigma_{kl} \in S$, то $S(g_i, g_j) \xrightarrow{G} 0$ для всех $\sigma_{ij} \in \Sigma$, т.е. система G является базисом Грёбнера.

Сказанное означает, что на шагах алгоритма Бухбергера можно проверять не все критические пары, а только те пары, которые в совокупности задают минимальную систему образующих. Для исключения критических пар можно воспользоваться алгоритмом предложения 6 и получить следующую модификацию алгоритма `Update`:

Алгоритм Update1

---

1. Исключить из B пары (f, h) такие, что $\mathtt{LM}(g) \mid [\mathtt{LM}(f), \mathtt{LM}(h)]$.
2. $R \leftarrow \{(f, g) \colon f \in G\}$.
3. Для всех пар $(f, g) \in R$: если найдется другая пара $(h, g) \in R$, для которой
   1) $[\mathtt{LM}(h), \mathtt{LM}(g)] \mid [\mathtt{LM}(f), \mathtt{LM}(g)]$,
   2) $[\mathtt{LM}(h), \mathtt{LM}(g)] \neq [\mathtt{LM}(f), \mathtt{LM}(g)]$ или $[\mathtt{LM}(h), \mathtt{LM}(g)] = [\mathtt{LM}(f), \mathtt{LM}(g)]$ и f добавлен в G позже h,
   3) $\mathtt{LM}(g) \not| [\mathtt{LM}(f), \mathtt{LM}(h)]$,

   то исключить (f, g) из R.
4. $G \leftarrow G \cup \{g\}$.
5. $B \leftarrow B \cup R$.
6. Возвратить (G, B).

Рассмотрим шаг 3 полученного алгоритма. Предположим, что $[\mathtt{LM}(h), \mathtt{LM}(g)] = [\mathtt{LM}(f), \mathtt{LM}(g)]$. Тогда исключение (h, g) вместо (f, g) не повлияет на дальнейшее выполнение алгоритма Бухбергера. Действительно, в дальнейшем исключение (h, g) или исключение из-за нее других пар будет выполняться в зависимости только от $[\mathtt{LM}(h), \mathtt{LM}(g)]$, т. е. при тех же условиях, что и для (f, g). Выбирая между (f, g) или (h, g), будем исключать в первую очередь пары с зацеплением. Пары без зацепления исключим после окончания шага 3.

В итоге получим следующий алгоритм:

Алгоритм Update2

---

1. Исключить из B пары (f, h) такие, что $\mathtt{LM}(g) \mid [\mathtt{LM}(f), \mathtt{LM}(h)]$.
2. $R \leftarrow \{(f, g) \colon f \in G\}$.
3. Для всех пар $(f, g) \in R$ с зацеплением: если найдется другая пара $(h, g) \in R$, для которой
   1) $[\mathtt{LM}(h), \mathtt{LM}(g)] \mid [\mathtt{LM}(f), \mathtt{LM}(g)]$,
   2) $\mathtt{LM}(g) \not| [\mathtt{LM}(f), \mathtt{LM}(h)]$,

   то исключить (f, g) из R.
4. Исключить из R пары без зацепления.

5. $G \leftarrow G \cup \{g\}$.

6. $B \leftarrow B \cup R$.

7. Возвратить (G, B).

Рассмотрим шаг 2 полученного алгоритма. Следуя [2], предположим, что множество R содержит пары (f, g) такие, что $\mathtt{LM}(g) \mid LM(f)$. Для этих пар (назовем их *r-парами*) выполняется

$$S(f, g) = f - \frac{\mathtt{LM}(f)}{\mathtt{LT}(g)} g.$$

Следовательно, $f \xrightarrow{\{S(f,g),g\}} 0$ и многочлен f можно исключить из G в пользу многочлена g и r-пары (f, g).

При обработке g пары с многочленом f будут исключены на шаге 1, поскольку выполняется условие $\mathtt{LM}(g) \mid [\mathtt{LM}(f), \mathtt{LM}(h)]$. Если при дальнейшей работе алгоритма Бухбергера будет исключена и пара (f, g), то информация о f будет потеряна. Поэтому на шаге 1 следует запретить исключение r-пар.

Окончательно получаем следующую модификацию алгоритма `Update2`:

Алгоритм Update3

---

1. Исключить из B пары (f, h) такие, что $\mathtt{LM}(h) \not| \, \mathtt{LM}(f)$ и $\mathtt{LM}(g) \mid [\mathtt{LM}(f), \mathtt{LM}(h)]$.

2. Для всех $f \in G$: если $\mathtt{LM}(g) \mid \mathtt{LM}(f)$, то $G \leftarrow G \setminus \{f\}$, $B \leftarrow B \cup \{(f, g)\}$.

3. $R \leftarrow \{(f, g) \colon f \in G\}$.

4. Для всех пар $(f, g) \in R$ с зацеплением: если найдется другая пара $(h, g) \in R$, для которой

   1) $[\mathtt{LM}(h), \mathtt{LM}(g)] \mid [\mathtt{LM}(f), \mathtt{LM}(g)]$,
   2) $\mathtt{LM}(g) \not| [\mathtt{LM}(f), \mathtt{LM}(h)]$,

   то исключить (f, g) из R.

5. Исключить из R пары без зацепления.

6. $G \leftarrow G \cup \{g\}$.

7. $B \leftarrow B \cup R$.

8. Возвратить (G, B).

Отметим, что исключение многочлена f упрощает систему G и тем самым ускоряет нахождение остатков на шагах 2a и 3c алгоритма Бухбергера. Кроме этого, уменьшается количество критических пар, обрабатываемых в алгоритмах обновления. Отметим также, что исключение f при обработке r-пар соответствует правилам исключения критических пар, заданным в предложении 6, но может противоречить правилам из работы [4].

Хотя алгоритм `Update3` основан на алгоритме построения минимальной системы образующих модуля сизигий, при выполнении алоритма Бухбергера могут быть обработаны критические пары, которые не относятся к минимальной системе. Дело в том, что пары исключаются из B не только в алгоритме `Update3`, но и на шаге 3b алгоритма Бухбергера. Поэтому пара (f, h), которая должна быть исключена из B на шаге 1 алгоритма `Update3`, может быть уже обработана, т. е. перемещена из B в B^*.

Тем не менее, обработанную пару (f, h) все равно можно использовать. Пусть на шаге 3 алгоритма `Update3` выполняется: $[\mathtt{LM}(h), \mathtt{LM}(g)] \mid [\mathtt{LM}(f), \mathtt{LM}(g)]$ и $\mathtt{LM}(g) \mid [\mathtt{LM}(f), \mathtt{LM}(h)]$. Тогда

$$S(f,h) - S(f,g) + \frac{[\mathtt{LM}(f), \mathtt{LM}(g), \mathtt{LM}(h)]}{[\mathtt{LM}(h), \mathtt{LM}(g)]} S(h,g) = 0$$

и пару (f, h) можно исключить в пользу (f, g) и (h, g), либо пару (f, g) можно исключить в пользу (f, h) и (h, g). В алгоритме `Update3` может быть исключена только пара (f, h). Однако, если (f, h) уже обработана, т. е. $S(f, h) \xrightarrow{G} 0$ для текущей системы G, то (f, g) можно исключить в пользу (h, g). Добавляя это дополнительное исключение в `Update3`, получаем окончательный алгоритм `UpdateEx`.

Список литературы

[1] **Кокс Д., Литтл Дж., О'Ши Д.** Идеалы, многообразия и алгоритмы. М.: Мир, 2000.

[2] **Boulier F.** A new criterion to avoid useless critical pairs in Buchberger's algorithm // Technical report LIFL 2001-07, avail. at: `http://www.lifl.fr/~boulier/PUBLICATIONS/LIFL2001-07.ps.gz`.

[3] **Caboara M., Kreuzer M., Robbiano L.** Efficiently computing minimal sets of critical pairs // Journal of Symbolic Computation. — 2004. — Vol. 38. — № 4. — P. 1169–1190.

[4] **Gebauer R., Möller H. M.** On an Installation of Buchberger's Algorithm // Journal of Symbolic Computation. — 1987. — № 6. — P. 257–286.

[5] **Mora T.** Solving Polynomial Equation Systems II. Macaulay's Paradigm and Gröbner Theory. Cambridge University Press, 2005.