Об оптимизации алгоритма Бухбергера

С.В. Агиевич

НИИ прикладных проблем математики
и информатики Белгосуниверситета

МаБИТ-2011

13 октября 2011 г.

1. Системы уравнений

Умножение «столбиком» двоичных слов-как-чисел:

$$
\begin{array}{cccccc}
 & & & x_3 & x_2 & x_1 \\
\times & & & & & \\
 & & & & x_5 & x_4 \\
\hline
 & & & x_3x_4 & x_2x_4 & x_1x_4 \\
+ & & & & & \\
 & & x_3x_5 & x_2x_5 & x_1x_5 & \\
\hline
 & x_{10} & x_9 & x_8 & x_7 & x_6
\end{array}
$$

Абстрактная система (многочлены над $\mathbb{F}_2$, неявно $= 0$):

$$
\begin{aligned}
& x_6 + x_1x_4, \\
& x_7 + x_2x_4 + x_1x_5, \\
& x_8 + x_3x_4 + x_2x_5 + x_1x_2x_4x_5, \\
& x_9 + x_3x_5 + x_2x_4x_5(x_1 + x_3 + x_1x_3), \\
& x_{10} + x_3x_5(1 + x_9), \\
& x_i^2 + x_i, \quad i = 1, \ldots, 10.
\end{aligned}
$$

Задача 3×2**-факторизации** $a = a_5a_4a_3a_2a_1$:

добавить многочлены $x_{5+i} + a_i$

2. Базисы Грёбнера

$P = K[x_1, \ldots, x_n]$	кольцо многочленов над полем K
$<$	мономиальный порядок
$\mathtt{LM}(f)$	старший моном $f \in P \setminus \{0\}$ относительно $<$
$\mathtt{LT}(f)$	старший член f

$G \subset P$ — **базис Грёбнера** идеала $I \subseteq P$, если

$\forall f \in I \setminus \{0\}$ найдется $g \in G$: $\mathtt{LM}(g) \mid \mathtt{LM}(f)$.

Применение. Если многочлены $F \subset P$ имеют единственный общий корень $(x_1, \ldots, x_n) = (a_1, \ldots, a_n)$, то G содержит многочлены $x_i - a_i$, $i = 1, \ldots, n$.

3. 3×2-факторизация

3×2-факторизация нечетных: $a = a_5 a_4 a_3 a_2 1$

Базис Грёбнера (порядок `grlex`):

```
{
  x1 + 1,
  x4 + 1,
  x6 + 1,
  x7 + x5 + x2,
  x8 + x3,
  x3 x5 + x2 x5 + x9,
  x2 x9 + x2 x5 + x10,
  x3 x9 + x2 x5 + x10 + x9,
  x5 x9 + x9,
  x2 x10 + x10,
  x3 x10 + x10,
  x5 x10 + x10,
  x9 x10
}
```

Анализ: $x_9 x_{10} = 0 \Rightarrow$

числа 25 (11001) 27 (11011), 29 (11101), 31 (11111) не могут быть 3×2-факторизованы

4. Алгоритм Бухбергера: критерий

$G = \{g_1, \ldots, g_r\} \subset I \subseteq P$

Деление f **на** G: исключение мономов, которые делятся на $\mathtt{LM}(g_i)$

$f \xrightarrow{G} g$, если $f = g_1 h_1 + \ldots + g_r h_r + g$, где

1) $\mathtt{LM}(g_i h_i) \leq \mathtt{LM}(f)$ для $h_i \neq 0$,

2) остаток g не содержит мономов, которые делятся на $\mathtt{LM}(g_i)$

Остаток зависит от порядка делителей и определен неоднозначно!

Однозначный остаток: $\bar{f}^G$ (зафиксирован порядок делителей)

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

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

Критерий. G — базис Грёбнера $\Leftrightarrow$ $S(g_i, g_j) \xrightarrow{G} 0$ для всех пар (g_i, g_j).

5. Алгоритм Бухбергера: основной алгоритм

Алгоритм Бухбергера

Вход: $F \subset P$, порядок $<$.

Выход: $G \subset P$ — базис Грёбнера идеала $\langle F \rangle$ относительно $<$.

Вспомогательные алгоритмы: `Update`.

Шаги:

1. $G \leftarrow \varnothing$, $B \leftarrow \varnothing$, $B^* \leftarrow \varnothing$.
2. Для всех $f \in F$:
   (a) $g \leftarrow \overline{f}^G$;
   (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.

6. Алгоритм Бухбергера: обновление

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).

7. Алгоритм Бухбергера: оптимизация

Критические пары: элементы B (обработать) и B^* (обработаны)

Основная трудоемкость: вычисление остатков $\overline{S(g_i, g_j)}^G$

В большинстве случаев остатки оказываются нулевыми!

Задача: оптимизировать `Update`, указав правила исключения неинформативных к.п. без вычисления остатков

8. Оптимизированное обновление

Алгоритм UpdateEx (оптимизированное 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) т.ч. $\mathtt{LM}(h) \not| \mathtt{LM}(f)$ 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).

9. Алгоритм UpdateEx: первый критерий Бухбергера

Пара без зацепления: (f, g) т.ч. $[\mathtt{LM}(f), \mathtt{LM}(g)] = \mathtt{LM}(f) \cdot \mathtt{LM}(g)$

Первый критерий Бухбергера:
$S(f, g) \overset{\{f,g\}}{\to} 0 \Rightarrow$ пару (f, g) можно исключить

10. Алгоритм UpdateEx: критерии GMI

Тройка многочленов: g_i, g_j, g_k (добавляются в G друг за другом)

Тройка S-многочленов:

$$t_{ij}S(g_i, g_j) - t_{ik}S(g_i, g_k) + t_{jk}S(g_j, g_k) = 0, \qquad (\star)$$

где $t_{uv} = \frac{[\mathtt{LM}(g_i),\mathtt{LM}(g_j),\mathtt{LM}(g_k)]}{[\mathtt{LM}(g_u),\mathtt{LM}(g_v)]}$.

Критерии GMI (Gebauer — Möller Installation):
1. Если некоторый из мономов t_{ij}, t_{ik} или t_{jk} равняется 1, то соответствующую к.п. следует исключить в пользу двух других.
2. Если сразу несколько мономов равняются 1, то в первую очередь исключается к.п. на «новых» многочленах (сначала $S(g_j, g_k)$, затем $S(g_i, g_k)$ и наконец $S(g_i, g_j)$).

Старые лучше новых?

11. Алгоритм UpdateEx: минимальная система к.п.

Теорема (неформально). Если в критериях GMI исключать в первую очередь к.п. на «старых» многочленах, то в результате будет получена минимальная система к.п.

Новые лучше старых!

Близкий результат (только для однородных систем с градуированным мономиальным порядком):

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

12. Алгоритм `UpdateEx`: использование B^*

Если

$$S(g_i, g_j) - t_{ik} S(g_i, g_k) + t_{jk} S(g_j, g_k) = 0,$$

то (g_i, g_j) должна быть исключена в пользу (g_i, g_k) и (g_j, g_k)

Но пара (g_i, g_j) может быть уже обработана (переведена в B^*)!

Критерии B^*:

1. Если $t_{ik} = 1$ и $(g_i, g_j) \in B^*$, то (g_i, g_k) можно исключить.
2. Если $t_{jk} = 1$, $t_{ik} \neq 1$ и $(g_i, g_j) \in B^*$, то (g_j, g_k) можно исключить.

13. Алгоритм UpdateEx: r-пары

r-пара: (f, g) т.ч. $\mathtt{LM}(g) \mid \mathtt{LM}(f)$

Критерий r-пар:
$S(f,g) = f - \frac{\mathtt{LM}(f)}{\mathtt{LT}(g)} g \Rightarrow$
$f \xrightarrow{\{S(f,g),g\}} 0 \Rightarrow$ f можно исключить из G в пользу g и (f, g)

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`.

Критерий r-пар несовместим с критериями GMI!

14. Эксперименты

Системы:

название	n	$\lvert G\rvert$	min / max	пояснение
`belt` (grlex)	16	660	3/4	полиномиальное описание подстановки на $\mathbb{F}_2^8$, заданной в стандарте шифрования СТБ 34.101.31
`belt` (grevlex)	16	471	3/4	
`commute3` (grlex)	18	926	2/5	полиномиальное описание пар обратимых коммутируемых матриц порядка 3 над $\mathbb{F}_2$
`commute3` (grevlex)	18	757	2/5	

Эксперименты: программная библиотека `GF2` (C++, шаблоны)

Результаты:

Система	`UpdateGMI`		`UpdateEx`		`UpdateGMI`/ `UpdateEx`
	к.п.	редукции к 0	к.п.	редукции к 0	
`belt` (grlex)	16262	12382 (76.1%)	15090	11210 (74.3%)	1.07
`belt` (grevlex)	16842	14729 (87.5%)	15856	13772 (86.9%)	1.06
`commute3` (grlex)	21433	18131 (84.6%)	19131	15943 (83.1%)	1.12
`commute3` (grevlex)	24604	20225 (82.2%)	22306	17743 (79.5%)	1.10