

Сигнатурные алгоритмы вычисления базисов Грёбнера для решения полиномиальных систем

Галкин Василий
`galkin-vv@yandex.ru`

Московский государственный университет
имени М.В. Ломоносова
Механико-математический факультет

Цели работы

Основная цель – создание теоретического фундамента для применения сигнатурных алгоритмов вычисления базиса Грёбнера к решению приближённых систем полиномиальных уравнений.

- ▶ Анализ сигнатурных алгоритмов
 - ▶ Определение свойств многочленов, выбираемых F5
 - ▶ Доказательство остановки F5
 - ▶ Формулировка простого аналога
- ▶ Применение к приближённым вычислениям
 - ▶ Строгая формулировка задачи приближённого решения системы
 - ▶ Классификация необратимых приближённых элементов
 - ▶ Вероятностный модулярный метод для определения класса необратимого элемента
 - ▶ Метод замены мономов переменными (TSV) для перемещения необратимых старших элементов

Сигнатурные алгоритмы

Сходства с алгоритмом Бухбергера

- ▶ Содержат очередь редуцируемых многочленов
- ▶ Каждый её элемент или отбрасывается правилами, или редуцируется

Вычисляют сигнатуру и используют её

- ▶ Разрешены только редукции, сохраняющие сигнатуры, с использованием удовлетворяющих критериям редукторов
- ▶ Правила отбрасывания элементов очереди анализируют сигнатуры

Сигнатурные алгоритмы – одни из наиболее эффективных для вычисления базиса Грёбнера.

Доказательство остановки сигнатурных алгоритмов

- ▶ F5 (J.-C. Faugère, 2002), F5B (Y. Sun, D. Wang, 2010), F5C (C. Eder, J. Perry, 2009)
 - ▶ остановка доказана только для регулярного случая
- ▶ G2V(S. Gao, Y. Guan, F. Volny IV, 2010), GVW(S. Gao, F. Volny IV, M. Wang, 2010)
 - ▶ по сравнению с F5 критерии отбрасывают меньше многочленов
 - ▶ остановка не доказана
- ▶ AP(A. Arri, J. Perry, 2011), TRB-MJ (L. Huang, 2010), SB (B. Roune, M. Stillman, 2012)
 - ▶ по сравнению с F5 позволяют использовать больше редукторов
 - ▶ сложное доказательство остановки, на основе редуцируемости всех S-пар, также применимое к GVW

Вопрос эффективности открыт, проблема остановки F5 актуальна

Свойства многочленов в F5

Критерии, применяемые алгоритмом F5, могут быть упрощены

- ▶ Свойства редуцируемых S-пар
 - ▶ Все редуцируемые алгоритмом S-пары имеют в качестве старшей части многочлен, однозначно определяемый как последний из полученных многочленов в некотором множестве.
 - ▶ Все редуцируемые алгоритмом S-пары имеют в качестве младшей части многочлен, однозначно определяемый как многочлен с минимальной по \prec «дробью» $\frac{S}{HM}$ в множестве потенциальных редукторов.
- ▶ Свойство используемого редуктора
 - ▶ Среди непустого множества потенциальных редукторов, сохраняющих сигнатуру, критерии алгоритма выберут ровно один – многочлен с минимальной по \prec «дробью» $\frac{S}{HM}$.

Следствие

Если существует редуктор, отбрасываемый критериями, то существует и не отбрасываемый критериями редуктор.

F5 останавливается

Определение

Цепь многочленов с сигнатурой: последовательность $\{h_i\}$, $\mathcal{S}(h_{i-1})|\mathcal{S}(h_i)$

Доказательство.



1. Если алгоритм не останавливается - он получит бесконечную цепь с возрастающим $\frac{\mathcal{S}}{\text{HM}}$
2. В бесконечной цепи найдутся $\text{HM}(h_i)|\text{HM}(h_j)$
3. h_i – сигнатурный редуктор для h_j
4. Если есть сигнатурный редуктор, то есть и сигнатурный редуктор, удовлетворяющий критериям
5. Это противоречит тому, что h_j не было редуцировано

Алгоритм SingleStepSignatureGroebner

$<_H$ – порядок на многочленах с сигнатурой,
сравнивающий дроби $\frac{S}{HM}$

Вход: многочлены $\{f_1, \dots, f_m\}$ с сигнатурами.

Переменные:

B – очередь многочленов, ожидающих анализа

R – промежуточный базис до определённой
сигнатуры, включающий сизигии

Результат:

R – базис Грёбнера идеала (f_1, \dots, f_m)

Код алгоритма

1. $B \leftarrow \{\text{входные многочлены } f_1, \dots, f_m \text{ с их сигнатурами}\}$
2. $R \leftarrow \{\text{известные сизигии, в частности тривиальные}\}$
3. **do while** $B \neq \emptyset$:
 - 3.1 $(\sigma, p') \leftarrow \text{элемент } B \text{ с } \prec\text{-минимальной сигнатурой}$
 - 3.2 $B \leftarrow B \setminus \{b \in B, S(b) = \sigma\}$
 - 3.3 $p \leftarrow \text{Сигнатурно_редуцировать } (\sigma, p') \text{ по } R$
 - 3.4 $R \leftarrow R \cup \{(\sigma, p)\}$
 - 3.5 **if** $p \neq 0$:
 - 3.5.1 **for** $\{r \in R \mid 0 \neq r <_H (\sigma, p)\}$: $B \leftarrow B \cup \{\frac{\text{LCM}(\text{HM}(r), \text{HM}(p))}{\text{HM}(r)} r\}$
 - 3.5.2 **for** $\{r \in R \mid r >_H (\sigma, p)\}$: $B \leftarrow B \cup \{\frac{\text{LCM}(\text{HM}(r), \text{HM}(p))}{\text{HM}(p)} (\sigma, p)\}$
 - 3.6 $B \leftarrow B \setminus \{b \in B \mid \exists r \in R r <_H b \text{ и есть делимость } S(r) \mid S(b)\}$

Доказательства остановки и корректности основаны на формулировках инвариантов для различных этапов

Алгоритмы вычисления базиса Грёбнера с приближёнными входными данными над \mathbb{R}

Вопрос о приближённом базисе Грёбнера в \mathbb{R} возникает из задачи решения полиномиальных систем, которые могут быть заданы приближённо

- ▶ Символические вычисления (исчерпывающий базис) – рост символических коэффициентов
- ▶ Вычисления над \mathbb{Q} – рост длины численных коэффициентов
- ▶ Вычисления с оценкой точности – проблемы нулей
 - ▶ Определение численными методами
 - ▶ Определение модулярными методами
 - ▶ Изменение порядка на мономах

Приближённые числа

Определения

Приближённым (комплексным) числом называется пара (a, ε) , $a \in \mathbb{C}$, $\varepsilon \in \mathbb{R}$

Специализацией приближённого числа a называется $a_0 \in \mathbb{C}$, $|a_0 - a| < \varepsilon$

Формализация задачи поиска базиса Грёбнера: ищем множество, содержащее решения при любых специализациях входных данных.

Операции с приближёнными числами

Сложение $(a_1, \varepsilon_1) + (a_2, \varepsilon_2) = (a_1 + a_2, \varepsilon_1 + \varepsilon_2)$

Умножение $(a_1, \varepsilon_1) \times (a_2, \varepsilon_2) = (a_1 a_2, \varepsilon_1 |a_2| + \varepsilon_2 |a_1| + \varepsilon_1 \varepsilon_2)$

Вычитание на основе сложения и умножения на -1:

$$(a_1, \varepsilon_1) - (a_2, \varepsilon_2) = (a_1 - a_2, \varepsilon_1 + \varepsilon_2)$$

Обращение определяется только для приближённых чисел, для которых 0 не является специализацией, что эквивалентно $|a| - \varepsilon > 0$:

$$\frac{1}{(a, \varepsilon)} = \left(\frac{1}{a}, \frac{\varepsilon}{|a| (|a| - \varepsilon)} \right)$$

Классификация необратимых приближённых элементов

Определения

символический ноль – при любой специализации входных данных соответствующие вычисления дают точный ноль.

ноль, индуцированный входными данными – некоторые, но не все, специализации дают точный ноль

ноль, внесённый вычислениями – не существует специализации, дающей точный ноль

Модулярный метод

- ▶ Вычислениями по произвольному модулю определяется предположительная комбинация входных элементов для элемента базиса
- ▶ Поиск аналога в приближённом случае сводится к решению линейной системы
- ▶ Тест на символический ноль при решении системы в приближённых числах
 - ▶ Точное – символические вычисления над \mathbb{Q} с заменой неточных входных значений на переменные
 - ▶ Вероятностное – модулярные вычисления в конечном поле с заменой неточных входных значений на произвольные элементы конечного поля

Расхождение между символическими и модулярными вычислениями

- ▶ \mathbb{Q} -многочлен тождественно обнуляется по выбранному модулю
 - ▶ Оценка на максимальный коэффициент для определения максимального числа простых чисел, на которые могут делиться все коэффициенты
- ▶ Модулярная специализация \mathbb{Q} -многочлена имеет корень
 - ▶ Оценка на максимальную степень, ограничивающая число корней

Итоговая оценка на модуль

Оценка предлагает диапазон простых чисел, в котором доля чисел, могущих привести к расхождению не более 2α .

- ▶ Начало диапазона $P_0 > \sqrt{\frac{R2^R V}{\alpha}}$.
- ▶ Количество простых чисел в диапазоне $N_p > \frac{R2^R \log_{P_0} 2Z_0}{\alpha}$

R – число строк в системе

V – количество приближённых коэффициентов во входных данных

Z_0 – максимальный числитель точного \mathbb{Q} -коэффициента во входных данных

Метод TSV

TSV (J.-C. Faugère, Y. Liang, 2011): Комбинирование алгоритмов нахождения базисов Грёбнера и приближённых вычислений. При получении старшего необратимого элемента в качестве коэффициента при $x_1^{i_1} \cdots x_m^{i_m}$:

- ▶ Добавляется новая переменная y' , младше всех остальных
- ▶ Для того, чтоб страшный член редуцировался, идеал расширяется $I^e = (I, x_1^{i_1} \cdots x_m^{i_m} - y')$
- ▶ В случае сигнатурных алгоритмов выполняется перезапуск с самого начала, поскольку сигнатура добавленного многочлена меньше текущей, а алгоритмы требуют обработки в порядке возрастания сигнатур для своей корректной работы

Применение TSV без перезапуска алгоритмов

Взвешенный порядок \prec_w на сигнатурах с параметром – вектором мономов $w = (w_1, \dots, w_m)$:

$$(t_1, i_1) \prec_w (t_2, i_2) \iff \begin{cases} t_1 w_{i_1} < t_2 w_{i_2} \\ t_1 w_{i_1} = t_2 w_{i_2}, i_1 < i_2 \end{cases}.$$

- ▶ Добавляется новая переменная y' , младше всех остальных
- ▶ Во входные данные вводится дополнительный многочлен $x_1^{j_1} \cdots x_m^{j_m} - y'$ для того, чтоб страшный член редуцировался
- ▶ Параметр весов сигнатур расширяется мономов w' , выбранным так, чтоб добавленный многочлен имел сигнатуру «точно перед текущей»
- ▶ Алгоритм продолжается без перезапуска





Использование результата TSV для решения системы

- ▶ Строится алгоритм SingleStepSignatureGroebner для \mathbb{C}
 - ▶ Модулярные вычисления для классификации нулей
 - ▶ Если необратимость устранить не удалось, применяется метод TSV
- ▶ На основе найденного базиса в расширенном TSV идеале многочленов I^e строится оператор нормальной формы $\phi : I \rightarrow I$ как композиция
 - ▶ Вложения $Id^e : I \rightarrow I^e$
 - ▶ Оператора нормальной формы в I^e - редукции по базису Грёбнера $\phi^e : I^e \rightarrow I^e$
 - ▶ Отображения $I^e \rightarrow I$, индуцируемого заменами
$$y' \mapsto x_1^{i_1} \cdots x_m^{i_m}$$
- ▶ Для решения полиномиальной системы применяется метод матриц действия, использующий лишь оператор нормальной формы ϕ .

Основные результаты

- ▶ Доказана остановка F5 [1, 2]
- ▶ Предложен алгоритм `SingleStepSignatureGroebner`, корректность и остановка которого доказаны без использования понятия S-пар [3, 4]
- ▶ Дана классификация необратимых приближённых элементов
- ▶ Построена методика применения сигнатурного алгоритма `SingleStepSignatureGroebner` для приближённых вычислений над \mathbb{C}

Публикации

-  Галкин В. В. Остановка Алгоритма F5 // Вестник МГУ. — 201?
-  Galkin V. Termination of Original F5 // ArXiv e-prints. — 2012. — March. — 1203.2402.
-  Галкин В. В. Простой итеративный алгоритм вычисления базисов Грёбнера, основанный на сигнатурах // Вестник МГУ. — 201?
-  Galkin V. Simple signature-based Groebner basis algorithm // ArXiv e-prints. — 2012. — May. — 1205.6050.

Пример символического нуля

Пример

$$\begin{array}{lll} \text{poly}(f_1) = & y^2z + a, & \mathcal{S}(f_1) = (1, 1) \\ \text{poly}(f_2) = & y^2z^2 + xz + 1, & \mathcal{S}(f_2) = (1, 2) \\ \text{poly}(f_3) = & y^3z + xy + 1, & \mathcal{S}(f_3) = (1, 3) \\ \text{poly}(f_4) = & \text{poly}(f_1) = y^2z + a, & \mathcal{S}(f_4) = (1, 1) \\ \text{poly}(f_5) = & \text{poly}(f_2) - z\text{poly}(f_4) = xz - az + 1, & \mathcal{S}(f_5) = (1, 2) \\ \text{poly}(f_6) = & \text{poly}(f_3) - y\text{poly}(f_4) = xy - ay + 1, & \mathcal{S}(f_6) = (1, 3) \\ \text{poly}(f_7) = & z\text{poly}(f_6) - y\text{poly}(f_5) = (a - a)yz + z - y, & \mathcal{S}(f_7) = (z, 3) \end{array}$$

Пример индуцированного или внесённого нуля

Пример

$$\text{poly}(f_1) = y^2z + z^2 + az, \quad \mathcal{S}(f_1) = (1, 1)$$

$$\text{poly}(f_2) = xyz, \quad \mathcal{S}(f_2) = (1, 2)$$

$$\text{poly}(f_3) = xy^2 + bx + 1, \quad \mathcal{S}(f_3) = (1, 3)$$

$$\text{poly}(f_4) = \text{poly}(f_1) = y^2z + z^2 + az, \quad \mathcal{S}(f_4) = (1, 1)$$

$$\text{poly}(f_5) = \text{poly}(f_2) = xyz, \quad \mathcal{S}(f_5) = (1, 2)$$

$$\text{poly}(f_6) = \text{poly}(f_3) = xy^2 + bx + 1, \quad \mathcal{S}(f_6) = (1, 3)$$

$$\text{poly}(f_7) = - (y\text{poly}(f_5) - x\text{poly}(f_4)) = xz^2 + axz, \quad \mathcal{S}(f_7) = (y, 2)$$

$$\begin{aligned} \text{poly}(f_8) &= (z\text{poly}(f_6) - x\text{poly}(f_4)) + \text{poly}(f_7) = \\ &= ((xy^2z + bxz + z) - (xy^2z + xz^2 + axz)) + xz^2 + axz = ((b-a)+a)xz + z, \\ \mathcal{S}(f_8) &= (z, 3) \end{aligned}$$