

Полиномиальные идеалы и комбинаторика диаграмм Юнга

Дмитрий Павлов
СПИИРАН, Санкт-Петербург

25 января 2013

Полиномиальные модели

Полиномиальная модель: $y = f(x_1, \dots, x_d) \in K[x_1, \dots, x_d]$
(K — конечное или бесконечное поле)

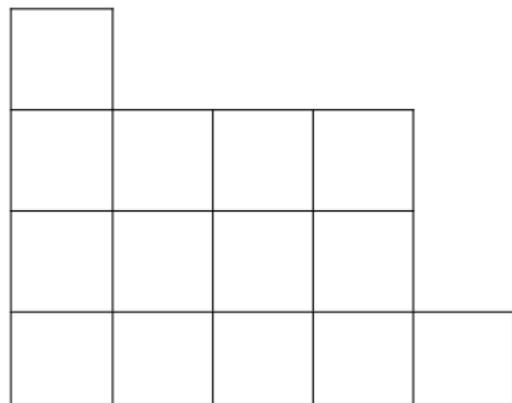
Полная полиномиальная модель: $x_i t \in \text{supp}(f) \Rightarrow t \in \text{supp}(f)$.

y^3				
y^2	xy^2	x^2y^2	x^3y^2	
y	xy	xy^2	xy^3	
1	x	x^2	x^3	x^4

Диаграммы Юнга

Отождествляем мономы (одночлены) с элементами $\mathbb{Z}_{\geq 0}^d$:
 $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_d^{\alpha_d} \sim (\alpha_1, \alpha_2, \dots, \alpha_d), \quad \alpha_i \in \mathbb{Z}, \alpha_i \geq 0.$

Диаграмма Юнга — конечное подмножество $\mathbb{Z}_{\geq 0}^d$, содержащее с каждым элементом все его делители.



Полная полиномиальная модель от d переменных \sim диаграмма Юнга в d -мерном пространстве.

Полиномиальные идеалы

Рассмотрим $\mathfrak{A} = \{f \in K[x_1, \dots, x_d] \mid f(p_i) = 0, p_i \in \mathcal{F} \subset K^d\}$

- ▶ $0 \in \mathfrak{A}$;
- ▶ если $f, g \in \mathfrak{A}$, то $f + g \in \mathfrak{A}$;
- ▶ если $f \in \mathfrak{A}$ и $h \in K[x_1, \dots, x_d]$, то $hf \in \mathfrak{A}$

\mathfrak{A} — полиномиальный идеал, обозначим $I(\mathcal{F})$

$$f(p_i) = f'(p_i), \forall p_i \in \mathcal{F} \Leftrightarrow f - f' \in I(\mathcal{F})$$

Класс вычетов g по модулю $I(\mathcal{F})$:

$$\{r \in K[x_1, \dots, x_d] : g = f + r, f \in I(\mathcal{F})\}.$$

Набор значений $\{y_i \in K \mid p_i \in \mathcal{F}\}$ определяет класс вычетов.

Размерность факторалгебры $K[x_1, \dots, x_d]/I(\mathcal{F})$ равна $|\mathcal{F}|$.

Идеал называется *нульмерным*, если его факторалгебра является конечнопорождённой. $I(\mathcal{F})$ нульмерен.

Базисы полиномиальных идеалов

Любой идеал \mathfrak{A} в $K[x_1, \dots, x_d]$ является конечнопорождённым:
 $\forall \mathfrak{A} \subset K[x_1, \dots, x_d] \quad \exists f_1, \dots, f_s \in K[x_1, \dots, x_d] : \mathfrak{A} = \langle f_1, \dots, f_k \rangle$
(Гильберт, 1890)

Набор образующих $\langle f_1, \dots, f_k \rangle$ называется *базисом*.

Базис в общем случае неоднозначен: $\langle x + y, x^2 \rangle = \langle x + y, y^2 \rangle$.

Некоторые базисы обладают полезными свойствами.

Мономиальные упорядочения и деление полиномов

Полное мономиальное упорядочение \succ на множестве мономов $\{x^\alpha = x_1^{\alpha_1} \dots x_d^{\alpha_d} : \alpha = (\alpha_1, \dots, \alpha_d) \in \mathbb{Z}_{\geq 0}^d\}$ называется *допустимым*, если:

- ▶ $\alpha \succ \mathbf{0}$ для любого $\alpha \neq \mathbf{0}$;
- ▶ Если $\alpha \succ \beta$, то $\alpha + \gamma \succ \beta + \gamma$ для любого $\gamma \in \mathbb{Z}_{\geq 0}^d$.

$\text{LM}_\succ(f)$ – старший моном полинома f по упорядочению \succ .

Деление полинома g на набор полиномов (f_1, \dots, f_s) :

$$g = \sum_{i=1}^s h_i f_i + r \quad h_i, r \in K[x_1, \dots, x_d]$$

$$\forall m \in \text{supp}(r), \forall i \in [1..s] \quad \nexists t \in \mathbb{Z}_{\geq 0}^d : m = \text{LM}(f_i)t$$

r однозначен и зависит от выбранного \succ .

Лексикографическое упорядочение (lex):

$$x_1 >_{\text{lex}} x_2 >_{\text{lex}} \dots >_{\text{lex}} x_d.$$

Базисы Грёбнера

$G \in \mathfrak{A}$ идеала \mathfrak{A} – базис Грёбнера \mathfrak{A} , если (Бухбергер, 1965):

$$\langle \{LM_{\succ}(g_i) : g_i \in G\} \rangle = \langle \{LM_{\succ}(f) : f \in \mathfrak{A}\} \rangle$$

Базис Грёбнера \mathfrak{A} является базисом \mathfrak{A} , зависит от \succ и неоднозначен.

Редуцированный базис Грёбнера $GB_{\succ}(\mathfrak{A}) \subset \mathfrak{A}$:

- ▶ Коэффициент при старшем члене любого полинома из $GB_{\succ}(\mathfrak{A})$ равен 1.
- ▶ Никакой моном никакого $g \in GB_{\succ}(\mathfrak{A})$ не принадлежит $\langle LM(GB_{\succ}(\mathfrak{A}) \setminus g) \rangle$

$GB_{\succ}(\mathfrak{A})$ однозначно определён в зависимости от \succ и \mathfrak{A} .

Важность базисов Грёбнера

При любом допустимом \succ :

- ▶ Алгоритм деления g на $GB_{\succ}(\mathfrak{A})$ гарантированно завершается
- ▶ Позволяет решить задачу принадлежности полинома идеалу (т.е. $r = 0$)
- ▶ Из $GB_{\succ}(\mathfrak{A})$ легко получить мономиальный базис факторалгебры \mathfrak{A}

При лексикографическом упорядочении ($GB_{\text{lex}}(\mathfrak{A})$):

- ▶ Символьно-численный метод решения систем полиномиальных уравнений
- ▶ Замена переменных в системах полиномиальных уравнений

Для некоторых задач нужны *все* базисы Грёбнера; их конечное число (Роббиано, 1985).

Алгоритмы вычисления базисов Грёбнера

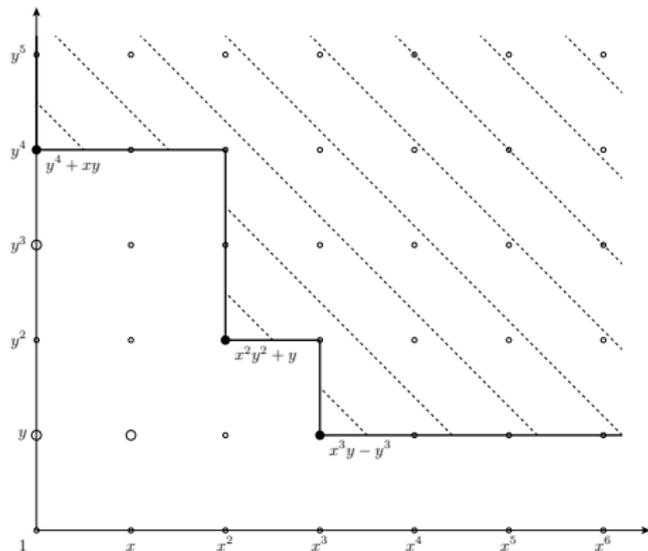
Задача относится к классу NP-Hard, т.е. не решается с помощью алгоритмов полиномиальной сложности.

- ▶ Алгоритм Бухбергера: вычисление $GB_{\succ}(\langle f_1, \dots, f_k \rangle)$
- ▶ Алгоритм Бухбергера-Мёллера: вычисление $GB_{\text{lex}}(I(\mathcal{F}))$
- ▶ Алгоритм FGLM: $GB_{\succ_1}(\mathcal{A}) \rightarrow GB_{\succ_2}(\mathcal{A})$ для нульмерного \mathcal{A}

Вычисление полного ансамбля базисов Грёбнера:

- ▶ Gröbner walk (Tran, 2000): $GB_{\succ_1}(\mathcal{A}) \rightarrow GB_{\succ_2}(\mathcal{A})$ для произвольного \mathcal{A} и «соседних» \succ_1 и \succ_2
- ▶ Реверсивный поиск (Avis, Fukuda, 1993) – алгоритм обхода графа, не требующий доп. памяти
- ▶ GFan (Jensen, 2007) – программный пакет для вычисления всех базисов Грёбнера произвольного \mathcal{A}

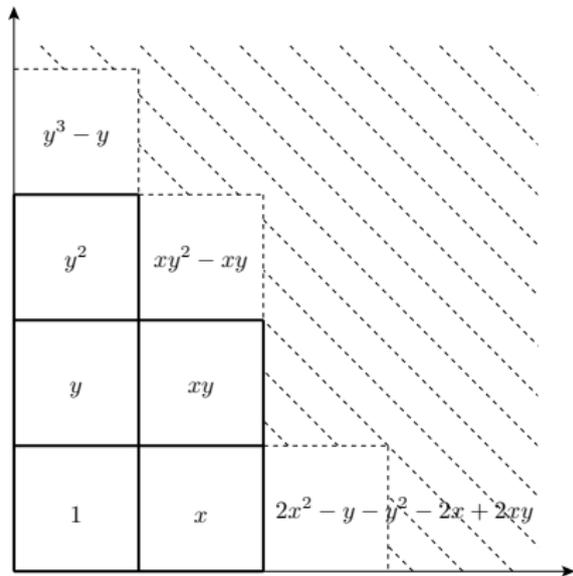
Факторалгебра ненульмерного идеала



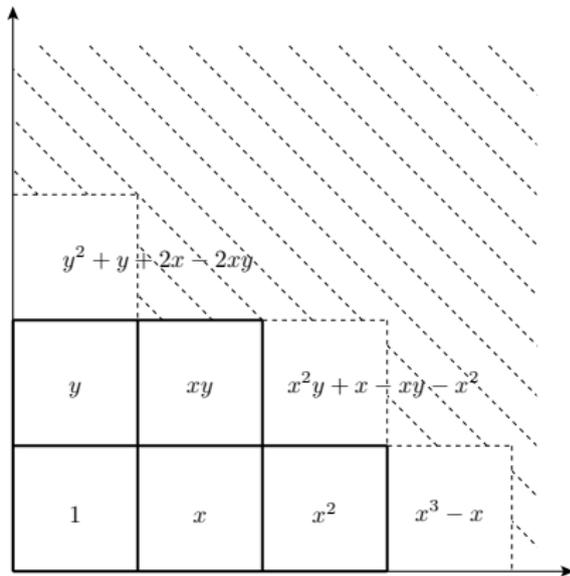
Факторалгебра идеала, заданного базисом $\{y^4 + xy, x^2y^2 + y, x^3y - y^3\}$, порождена мономами, лежащими под заштрихованной областью.

Факторалгебра нульмерного идеала \sim диаграмма Юнга

$$\mathcal{F} = \{(0, 0), (0, -1), (1, 0), (1, 1), (-1, 1)\}.$$



$G_{x>y}(\mathcal{F})$



$G_{y>x}(\mathcal{F})$

Все ли возможные мономиальные базисы факторалгебры можно получить из базисов Грёбнера?

Связь алгебраической статистики с нульмерными идеалами

Модель $y = f(x_1, \dots, x_d)$ с носителем $\text{supp}(y) = \{t_1, \dots, t_n\}$ *идентифицируема* планом $\mathcal{F} = \{p_1, \dots, p_n\}$, если $\text{rank}(\{F_{ij}\}_{n \times n}) = n$, где $F_{ij} = t_j(p_i)$.
 $\text{span}(\text{supp}(y))$ задаёт факторалгебру $I(\mathcal{F})$.

Прямая задача (Pistone, Wynn, 1996): каковы полные полиномиальные модели, идентифицируемые \mathcal{F} ?

Обратная задача (Caboara, Robbiano, 2001): дано $\mathcal{D} = (a_{1,1}, \dots, a_{1,r_1}) \times \dots \times (a_{d,1}, \dots, a_{d,r_d})$ (*полный экспериментальный план*), и $y = f(x_1, \dots, x_d)$. Найти все $\mathcal{F} \in \mathcal{D}$, идентифицирующие y .

Алгебраический веер, статистический веер (fan)

Алгебраический веер (algebraic fan, AF) – это множество полиномиальных моделей, полученных из всевозможных $GB_{\succ}(I(\mathcal{F}))$.

Если $GB_{\succ}(I(\mathcal{F})) = \{g_1, \dots, g_k\}$, то множество мономов

$$Y = \{t \mid t \neq LM_{\succ}(g_i)u, \forall i \in [1..k]\}$$

является диаграммой Юнга, линейно-независимой в $I(\mathcal{F})$.

$y = a_1 t_1 + \dots + a_{|Y|} t_{|Y|}$ является полной полиномиальной моделью.

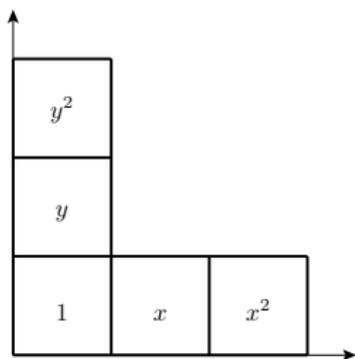
Статистический веер (statistical fan, SF) – это множество всех полных полиномиальных моделей, идентифицируемых \mathcal{F} .

$$AF \subseteq SF$$

Алгебраический веер \neq статистический веер

$$\mathcal{F} = \{(0, 0), (0, -1), (1, 0), (1, 1), (-1, 1)\}.$$

Рассмотрим $Y = \{1, x, y, x^2, y^2\}$.



$$F = \begin{pmatrix} 1 & x & y & x^2 & y^2 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 \end{pmatrix}$$

$\det(F) \neq 0 \Rightarrow Y \in \text{SF}$, однако $Y \notin \text{AF}$.

Нахождение статистического веера

Алгоритм (Васильев, Павлов, 2009) основан на рекурсивном переборе конечных полных множеств мономов (диаграмм Юнга), линейно-независимых в $I(\mathcal{F})$.

Основные принципы:

- ▶ Перебор диаграммы Юнга размера n
- ▶ Отбрасывание ветви перебора при получении линейно-зависимой комбинации мономов
- ▶ «Инкрементальный» метод Гаусса для проверки линейной зависимости
- ▶ Кэширование значений мономов $t_j(p_i)$
- ▶ Сохранение всех перебранных диаграмм, для избежания дублирования ветвей

Базисы Грёбнера в алгоритме не используются.

Псевдокод алгоритма

find-statistical-fan (\mathcal{F} , seq = {}, dimples = {1}, excluded = {}, $n = 0$, found = {}, $F = ()_{N \times n}$, $H = (0, \dots, 0)_{1 \times N}$)

for all $t \in \text{dimples}$

if $\exists x \in \text{excluded} : x|t$ **then**

continue

end if

$(F', n', \text{seq}') \leftarrow (F, n, \text{seq})$

$F \leftarrow F \cup (t(p_1), \dots, t(p_N))^T, p_i \in \mathcal{F}$

$n \leftarrow n + 1$

seq = seq + t

for $i \in \{1..N\}$ **do**

if $H_i > 0$ and $F_{in} \neq 0$ **then**

for $j \in \{1..N\}$ **do**

$F_{jn} \leftarrow F_{jn} - F_{jH_i} F_{in}$

end for

end if

end for

independent \leftarrow False

for $i \in \{1..N\}$ **do**

if $H_i = 0$ and $F_{in} \neq 0$ **then**

$H_i \leftarrow n$

for $j \in \{1..N\}$ **do**

$F_{jn} \leftarrow F_{jn} / F_{in}$

end for

for $k \in \{1..n\}$ **do**

for $j \in \{1..N\}$ **do**

$F_{jk} \leftarrow F_{jk} - F_{ik} F_{jn}$

end for

end for

 independent \leftarrow True

end if

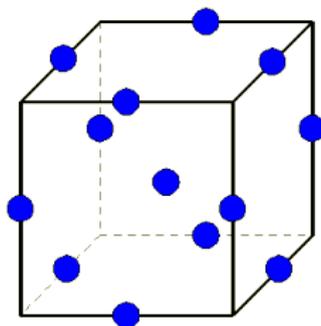
end for

Псевдокод алгоритма (окончание)

```
if not independent then  
  if seq  $\notin$  found then  
    yield seq  
    find-statistical-fan( $\mathcal{F}$ , seq', dimples  $\setminus$  t, excluded  $\cup$   
t, n', found  $\cup$  {seq}, F', H')  
  end if  
  else  
    newdimples  $\leftarrow$  update-dimples(t, dimples  $\setminus$  t)  
    find-statistical-fan( $\mathcal{F}$ , seq, newdimples, excluded, n,  
found, F, H)  
  end if  
  (F, n, seq)  $\leftarrow$  (F', n', seq')  
end for
```

Пример: экспериментальный план Бокса-Бенкена

$$\mathcal{F} = \{(0, \pm 1, \pm 1, \dots \pm 1),$$
$$(\pm 1, 0, \pm 1, \dots \pm 1),$$
$$\dots$$
$$(\pm 1, \pm 1, \pm 1, \dots 0),$$
$$(0, 0, 0, \dots 0)\}$$



При $d = 3$ GFan находит 12 базисов Грёбнера для $I(\mathcal{F})$.

Статистический веер –
на две модели больше алгебраического:

$$\{1, z, z^2, y, yz, y^2, y^2z, x, xz, xz^2, xy, x^2, x^2y\}$$

$$\{1, z, z^2, y, yz, yz^2, y^2, x, xz, xy, xy^2, x^2, x^2z\}$$

При $d = 4$, в алгебраическом веере 48 моделей, а в статистическом – 96.

Теория представлений

Таблица Юнга:

12					
5	7	13	14		
2	6	8	11		
1	3	4	9	10	

S_n — группа перестановок n элементов.

RSK-соответствие (Робинсон, 1938, Шенстед, 1961, Кнут, 1970): $w \in S_n \sim (P, Q)$ (перестановка \sim паре таблиц Юнга).

Модуль Шпехта (1935): S_n можно представить в виде группы линейных операторов на *таблоидах*. Диаграмма Юнга $\lambda \in \mathcal{Y}_n$ соответствует неприводимому представлению S_n . Размерность неприводимого представления $\dim \lambda$ равна количеству таблиц Юнга f^λ в этой диаграмме.

Быстрый подсчёт $\dim \lambda$: формула крюков

1					
5	3	2	1		
7	5	4	3	1	

Рис.: Длины «крюков»

$$\dim \lambda = \frac{n!}{\prod_{x \in Y(\lambda)} h(x)}$$

(Фрейм, Робинсон, Тролл, 1957)

Для $d > 2$ аналогичной формулы не известно.

Максимальная размерность неприводимого представления

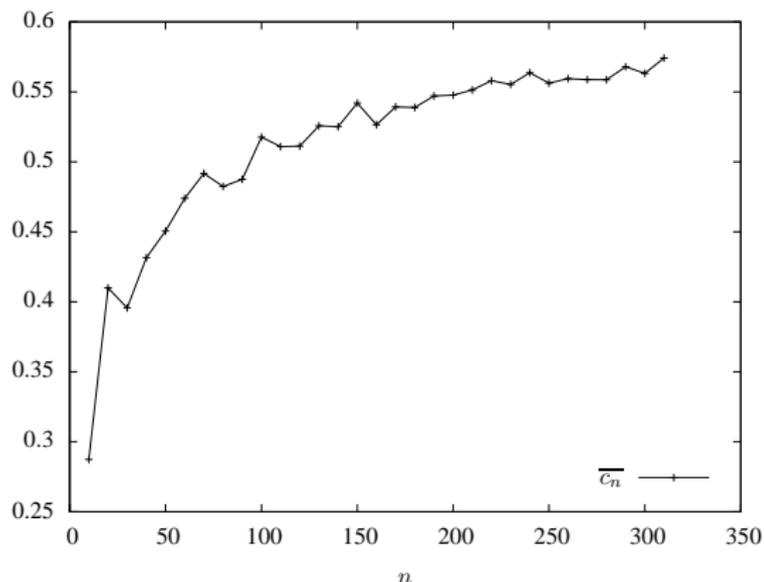
$$-\frac{c_1}{2} \leq \frac{1}{\sqrt{n}} \ln \left(\frac{\max_{\Lambda \in \hat{S}_n} \dim \Lambda}{\sqrt{n!}} \right) \leq -\frac{c_0}{2}$$

$$c_1 \approx 0.2313, \quad c_0 \approx 2.5651$$

(Вершик, Керов, 1985)

Существует ли $\lim_{n \rightarrow \infty} \frac{1}{\sqrt{n}} \ln \left(\frac{\max \dim \Lambda}{\sqrt{n!}} \right) = -\lim_{n \rightarrow \infty} c(n) = -c$?

Значения $c(n)$



Начиная с $n = 140$ значения приблизительные, из-за ограничения перебора.

Спасибо за внимание!