Лекція. Базиси Гребнера (1)

Багато фундаментальних задач математики, природничих та технічних наук можна сформулювати з точки зору систем нелінійних поліномів багатьох змінних. Базиси Гребнера забезпечують єдиний, потужний підхід до розв'язання подібних задач. Приклади включають рішення алгебраїчних систем рівнянь, символьну інтеграцію та рішення лінійних крайових задач (диференціальних рівнянь).

Цей метод успішно застосовується і в інших областях, включаючи доведення геометричних теорем, забарвлення графів та лінійну цілочисельну оптимізацію.

Базиси Гребнера також використовувались для вирішення задач у таких сферах, як побудова та аналіз нелінійних криптосистем, робототехніка, інженерія програмного забезпечення, знаходження генетичних зв'язків між видами та розгадування загадок судоку.

Усі системи комп'ютерні алгебри загального призначення, такі як Maple та Mathematica, забезпечують реалізацію базисів Гребнера.

Питання, які будуть розглянуті, містять:

(1) Що таке базиси Гребнера?

(2) Чому корисні базиси Гребнера?

(3) Як обчислюються базиси Гребнера?

Поняття базисів Гребнера було введено Бруно Бухбергером у 1965 р. Бухбергер назвав їх за іменем керівника своєї дисертації Вольфганга Гребнера.

Хоча деякі ідеї, що лежать в основі цієї роботи, передували його дисертації, Бухбергер був першим, хто представив систематичне трактування теми, включаючи обчислювальний алгоритм.

У 1997 році він отримав нагороду від Асоціації обчислювальної техніки (ACM), яка визначає важливість цього внеску в математику та комп'ютерні науки.

Базиси Гребнера надають спосіб перетворення множини F поліномів багатьох змінних у другу множину G, яка має певні властивості, яких F не має.

Наприклад, проблеми, які важко вирішити з точки зору F, стає порівняно легко вирішити за допомогою G. Більше того, алгоритм обчислення G з F досить простий для розуміння та досить простий у здійсненні.

Як приклад, припустимо, ми хочемо розв'язати наступну систему чотирьох нелінійних квадратичних рівнянь у трьома невідомими:

$$x\,y = 0, \qquad x^2 + y^2 = 1, \qquad z^2 - x^2 = 1, \qquad y^2 + z^2 = 2.$$

Базиси Гребнера працюють з поліномами замість рівнянь, тому система записується як список поліномів, які неявно прирівнюються до нуля. Ось як обчислити базиси Гребнера в Sympy.

```
>>> F = [ x*y, x**2 + y**2 - 1, z**2 - x**2 - 1, y**2 + z**2 - 2 ]
>>> F
```

$$\left[xy,\ x^2+y^2-1,\ -x^2+z^2-1,\ y^2+z^2-2\right]$$

```
>>> G = groebner(F, z, y, x, order='grevlex')
>>> print(G)
GroebnerBasis([x**3 - x, -x**2 + z**2 - 1, x**2
+ y**2 - 1, x*y], z, y, x, domain='ZZ',
order='grevlex')
```

Параметр order необхідний для обчислення базиса Гребнера стосовно певного лексикографічного впорядкування термів. Ось базис для одної і тієї ж множини F відносно іншого впорядкування.

```
>>> G = groebner(F, z, y, x, order='lex')
>>> print(G)
GroebnerBasis([-x**2 + z**2 - 1, x**2 + y**2 -
1, x*y, x**3 - x], z, y, x, domain='ZZ',
order='lex')
```

Який взаємозв'язок між базисом Гребнера G та вхідним базисом F? Основна властивість узагальнена наступною теоремою.

Теорема. Нехай $F = \{f_1, f_2, \dots f_s\}$ - вхідний базис (набір поліномів з дійсними або комплексними коефіцієнтами) і нехай $G = \{g_1, g_2, \dots g_t\}$ - вихід, або базис Гребнера (також набір поліномів).

Тоді дійсні і комплексні рішення двох систем F і G ідентичні, навіть аж до кратності рішень.

Отже, базис Гребнера спрощує набір поліномів, але насправді це не вирішує систему рівнянь. Однак зауважте, що обидві базис, обчислені вище, «перетворюють» систему, і її набагато простіше вирішити. Наприклад, перший поліном у G

```
>>> print(G[0])
x**3 - x
```

передбачає лише x, тому його можна вирішити безпосередньо

```
>>> solve(G[0], x)
```

$$[-1, 0, 1]$$

Що робити, якщо наша система рівнянь не має рішення? Дуже простий приклад - пара лінійних рівнянь

$$2x + 8y = 5; \quad x + 4y = 2.$$

Помноження другого рівняння на 2 і віднімання результату від першого дає 0 = 1. Це означає, що система рівнянь еквівалентна системі 1 = 0, яка не має розв’язків.

```
>>> F = [2*x + 8*y - 5, x + 4*y - 2]
```

```
>>> G = groebner(F)
>>> G
```

$$GroebnerBasis\left(\left(\mathrm{Poly}\left(1, x, y, domain = \mathbb{Z}\right)\right), (x,\ y)\right)$$

Взагалі система F має (редукований) базис Гребнера G = [1] тоді і лише тоді, коли відповідний набір рівнянь $\{f_1 = 0, f_2 = 0, \dots f_s = 0\}$ не має рішення.

Впорядкування мономів

Коли Sympy просять виконати обчислення базису Гребнера, потрібен спеціальний параметр. Два типи, з якими ми стикалися, - це lex та grevlex, і кожен з них бере аргумент, який є впорядкованим списком змінних. Розглянемо значення цього параметра і чому він важливий, коли ділимо поліноми.

Розглянемо наступний (випадково впорядкований) поліном двох змінних у розгорнутому вигляді,

$$x^2 + y^2 + 4\,x\,y^2 + 5\,x + 2 + 7\,x\,y.$$

Кожен із шести доданків називається мономом, і кожен моном виражається як постійний коефіцієнт, який помножений на добуток змінних, піднятим у певних ступенях. (Ступені самого постійного терма - всі нульові.)

Одне впорядкування термінів полягає в сортуванні їх у порядку зменшення за ступенем однієї зі змінних, наприклад, x,

$$x^2 > (4\,x\,y^2,\, 5\,x,\, 7\,x\,y) > (y^2,\, 2).$$

Є один терм ступеня 2 для x, три ступеня 1 і два ступеня 0.

Тепер для кожного набору термів одного ступеня для x ми сортуємо їх за низхідним ступенем y,

$$x^2 > 4\,x\,y^2 > 7\,x\,y > 5\,x > y^2 > 2$$

Щоб домогтися загального впорядкування всіх термів. Це називається **чисто лексикографічним порядком** і задається в Sympy автоматично.

```
>>> x**2 + y**2 + 4*x*y**2 + 5*x + 2 + 7*x*y
```

$$x^2 + 4xy^2 + 7xy + 5x + y^2 + 2$$

Якби була третя змінна z, ми б сортували всі доданки у кожному $x^i y^i$ за порядком їх зменшення в z.

Інший спосіб впорядкувати терми - це сортування їх спочатку у порядку зменшення за загальним ступенем,

$$4\,x\,y^2 > x^2 > 7\,x\,y > y^2 > 5\,x > 2.$$

Існує один терм ступеня 3, три ступеня 2, один ступеня 1 і один ступеня 0. Для кожного набору термів одного ступеня ми виконуємо сортування за лексикографічним порядком,

$$4\,x\,y^2 > (x^2,\, y^2,\, 7\,x\,y) > 5\,x > 2.$$

Це називається ступінчастим лексикографічним порядком і задається в Sympy як grlex.

$$x^2 + 4\,x\,y^2 + 7\,x\,y + 5\,x + y^2 + 2$$

Інтерес до базисів Гребнера мотивований тим, що вони мають "кращі" властивості, ніж інші системи поліномів. Залежно від того, які властивості представляють інтерес у конкретному контексті, обчислюється базис Гребнера даної системи з урахуванням конкретного впорядкування мономів.

Наприклад, лексикографічний порядок (lex) використовується найчастіше, оскільки він створює систему, яку легше вирішити методом, аналогічним елімінації Гаусса.

Ступінчасте лексикографічне впорядкування (grlex) використовується в таких застосуваннях, як приклад цілочисельне програмування в якому упорядкування загального ступеня монома важливіше, ніж послідовність показників у цьому мономі.

Ділення поліномів

$$\begin{array}{r|l} & 2\,x - 1 \\ \hline 3\,x^2 - x + 2 & 6\,x^3 - 5\,x^2 + 9\,x + 3 \\ & \underline{6\,x^3 - 2\,x^2 + 4\,x\phantom{{}+3}} \\ & \phantom{6\,x^3 - 2\,x^2 + {}}-3\,x^2 + 5\,x + 3 \\ & \phantom{6\,x^3 - 2\,x^2 + {}}\underline{-3\,x^2 + \,x - 2} \\ & \phantom{6\,x^3 - 2\,x^2 + {}}4\,x + 5 \end{array}$$

Приклад ділення

Спочатку спробуйте розділити f(x) = x^3 + 1 на g(x) = x + 1 з термами, розташованими у звичайному порядку. Ви повинні отримати частку q(x) = x^2 + x + 1 і залишок r = 0.

Потім оберніть терми в f і g і поділіть f (x) = 1 + x^3 на g (x) = 1 + x. Після трьох ітерацій процедури ми отримуємо таку ж частку та решту, що й раніше.

Тепер змінимо дільник на g (x) = x-1 і поділимо f на g з термами у звичайному порядку. Ви повинні отримати частку q (x) = x^2 + x + 1 і залишок r = 2.

Нарешті, переставте доданки f і g і поділіть f (x) = 1 + x^3 на g (x) = -1 + x.

Частка виглядає як $q(x) = -1-x-x^2-2x^3-2x^4-2x^5-\ldots,$ але ітерації тривають далі!

Щоразу, коли два поліноми однієї змінної діляться, а їхні терми, розташовані в порядку збільшення степеней, звичайна процедура ділення працює правильно, якщо залишок r = 0, але не закінчується, якщо $r \neq 0$.

Отже, для поліномів однієї змінної єдине можливе впорядування термів як для розділеного, так і для дільника

$$1 < x < x^2 < x^3 < \ldots .$$

Однак ситуація відрізняється для поліномів двох чи більше змінних, де можливе багато впорядкувань термів.

Обчислюючи базис Гребнера, потрібно буде розділити один поліном на набір з двох або більше поліномів.

Цей процес називається *загальним діленням*. (Іноді це називається множинним діленням.)

Припустимо, наприклад, ділимо поліном f на два поліноми [g1; g2]. Це дає частку q1 відносно g1, іншу частку q2 відносно g2 і остаточний залишок r, що задовольняє

$$f = q_1 \cdot g_1 + q_2 \cdot g_2 + r.$$

Приклад. Розділимо $f = x^2\,y + x\,y^2 + y^2$ на $[g_1, g_2] = [x\,y - 1, y^2 - 1],$ упорядковуючи терміни лексикографічно з x> y.

$$
\begin{array}{lll}
 & q_1 = x + y & \\
 & q_2 = 1 & \\
g_1 = x\,y - 1 & \overline{x^2y + x\,y^2 + y^2} & = f \\
g_2 = y^2 - 1 & x^2y - x & \\
 & \overline{x\,y^2 + x + y^2} & = f - x\,g_1 \\
 & x\,y^2 - y & \\
 & \overline{x + y^2 + y} & = f - (x + y)\,g_1 \\
 & y^2 + y \quad x \to r & \\
 & y^2 - 1 & \\
 & \overline{y + 1} & = f - (x + y)\,g_1 - g_2 \\
 & 0 \qquad y + 1 \to r & r = x + y + 1
\end{array}
$$

Ми виразили початковий поліном як

$$x^2y + x\,y^2 + y^2 = (x + y) \cdot (x\,y - 1) + 1 \cdot (y^2 - 1) + (x + y + 1).$$

```
procedure GeneralDivide(f;G)
{Вхід: Поліном, що ділиться f, поліноми дільники G = [g1; : : : ; gs]}
{Результат: Частка r, залишки [q1; : : : ; qs] }
    h := f {ініціалізувати поліном, що залишився}
    q1 := 0; : : : ; qs := 0 { ініціалізувати залишки до нуля }
    while h <> 0 do
        divoccurred := false
        for i := 1 to s while divoccurred = false do
            if LT(gi) ділить LT(h) then
                qi := qi + LT(h)/LT(gi) { додати терм до частки
            qi}
                h := h - LT(h)/LT(gi) * gi { відняти добуток від
            h}
                divoccurred := true
            end if
            if divoccurred = false then {LT(h) не має дільника }
                r := r + LT(h) { додати LT (h) до залишку }
                h := h + LT(h) {відняти LT(h) від того, що
            ділиться}
            end if
```

```
            end do
        return(r; [q1; : : : ; qs])
end procedure
```

Теорема. (Лінійні комбінації). Якщо $G = \{g_1, g_2, \dots g_s\}$ - це базис Гребнера, а f - поліном, тоді залишок, коли f ділиться на елементи G дорівнює нулю, remainder(f, G) = 0, якщо і тільки тоді, коли f може бути виражена (не однозначно) як лінійна комбінація базових елементів,

$$f = h_1 \cdot g_1 + h_2 \cdot g_2 + \ldots + h_s \cdot g_s,$$

де h_i певні поліноми.

S-поліноми

Питання, розглянуте в цьому розділі, полягає в тому, як, починаючи з набору поліномів F, ми можемо систематично (алгоритмічно) побудувати базис Гребнера G, еквівалентний F. Бухбергер вирішив цю проблему, визначивши певну лінійну комбінацію двох поліномів яку називають S-поліномом.

Теорема Бухбергера. Сукупність поліномів G - базис Гребнера тоді і тільки тоді, коли S-поліном будь-яких двох елементів G зводиться до нуля; тобто для всіх пар (gi; gj) в G,

$$\text{remainder}(\text{spoly}(g_1,\, g_2), G) = 0.$$

Що таку S-поліном

$$\text{spoly}(p,\, q) = \text{lcm}(\text{LT}(p),\, \text{LT}(q)) \left(\frac{p}{\text{LT}(p)} - \frac{q}{\text{LT}(q)} \right),$$

де LT позначає провідний терм полінома. Включення коефіцієнта lcm змушує скасувати терми LT в знаменниках.

Наприклад

$$p = 2\,x^2\,y + x\,y^4 \quad \text{та} \quad q = x^2 + y + 1,$$

$$\begin{aligned}\operatorname{spoly}(p,\,q) &= \operatorname{lcm}(2\,x^2\,y,\,x^2)\left(\frac{2\,x^2\,y + x\,y^4}{2\,x^2\,y} - \frac{x^2 + y + 1}{x^2}\right)\\ &= x\,y^4 - 2\,y^2 - 2\,y.\end{aligned}$$

Якщо взяти впорядкування grlex

$$\begin{aligned}\operatorname{spoly}(p,\,q) &= \operatorname{lcm}(x\,y^4,\,x^2)\left(\frac{2\,x^2\,y + x\,y^4}{x\,y^4} - \frac{x^2 + y + 1}{x^2}\right)\\ &= -y^5 + 2\,x^3\,y - y^4.\end{aligned}$$

Процедура побудови базиса Гребнера

procedure $Gröbner Basis(F)$
{Input: Set of polynomials F}
{Output: Gröbner basis G equivalent to F}
    $G := F$ {initialize G to F}
    $C := G \times G$ {form set of (unordered) critical pairs}
    while $C \neq \emptyset$ **do** {any critical pairs left?}
      Choose a pair (f, g) from C
      $C := C \setminus \{(f, g)\}$ {remove the pair from C}
      $h := \text{remainder}(\text{spoly}(f, g), G)$ {reduce the S-polynomial}
      if $h \neq 0$ **then** {spoly(f, g) does not reduce to 0}
        $C := C \cup (G \times \{h\})$ {add new pairs to C}
        $G := G \cup \{h\}$ {place h in G}
      end if
    end do
    return(G)
end procedure