Дискретные структуры

МФТИ, весна 2014

Александр Дайняк

www.dainiak.com

Одно обобщение деления многочленов

Утверждение.

Пусть $P \in \mathbb{F}[x_1, \dots, x_m]$ и $\tilde{P} \in \mathbb{F}[x_i]$ — произвольные ненулевые многочлены.

Тогда существуют $Q, R \in \mathbb{F}[x_1, \dots, x_m]$, такие, что

$$P = \tilde{P} \cdot Q + R,$$

и $\deg_{x_i} R < \deg_{x_i} \tilde{P}$.

Доказательство: во всех мономах P, куда x_i входит в степени больше $\deg_{x_i} R$, заменяем эту степень, выразив её через $\tilde{P}$.

По сути, это «деление столбиком», в котором мы рассматриваем P как многочлен от x_i с коэффициентами из $\mathbb{F}[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_m]$.

Пример

Пусть $P \coloneqq x_1^5 x_2^8 x_4 + x_1^2 + x_1 x_3$ и $\tilde{P} \coloneqq x_1^2 + 3x_1$. Тогда

$$P = x_1^3 x_2^8 x_4 \cdot \left(\tilde{P} - 3x_1\right) + \left(\tilde{P} - 3x_1\right) + x_1 x_3 =$$

$$= (x_1^3 x_2^8 x_4 + 1) \cdot \tilde{P} - 3x_1^4 x_2^8 x_4 - 3x_1 + x_1 x_3 =$$

$$= (x_1^3 x_2^8 x_4 + 1) \cdot \tilde{P} - 3x_1^2 x_2^8 x_4 \left(\tilde{P} - 3x_1\right) - 3x_1 + x_1 x_3 =$$

$$= (x_1^3 x_2^8 x_4 - 3x_1^2 x_2^8 x_4 + 1) \cdot \tilde{P} + 9x_1^3 x_2^8 x_4 - 3x_1 + x_1 x_3 =$$

$$= (\dots) \cdot \tilde{P} + 9x_1 x_2^8 x_4 \left(\tilde{P} - 3x_1\right) - 3x_1 + x_1 x_3 =$$

$$= (\dots) \cdot \tilde{P} - 27x_1^2 x_2^8 x_4 - 3x_1 + x_1 x_3 =$$

$$= (\dots) \cdot \tilde{P} - 27x_2^8 x_4 \left(\tilde{P} - 3x_1\right) - 3x_1 + x_1 x_3 =$$

$$= \underbrace{(\dots)}_{Q} \cdot \tilde{P} + \underbrace{81x_1 x_2^8 x_4 - 3x_1 + x_1 x_3}_{R}$$

Теорема Алона о нулях

Теорема.
Пусть $P \in \mathbb{F}[x_1, \ldots, x_m]$ — произвольный полином,
и пусть $x_1^{t_1} \cdot \ldots \cdot x_m^{t_m}$ — моном старшей степени, то есть $\sum_i t_i = \deg P$.

Пусть $S_1, \ldots, S_m \subseteq \mathbb{F}$ — произвольные множества, такие, что $|S_i| \geq t_i + 1$ для всех i.

Тогда найдутся такие $s_1 \in S_1, \ldots, s_m \in S_m,$ что

$$P(s_1, \ldots, s_m) \neq 0$$

Доказательство теоремы Алона

Доказательство: индукция по $\deg P$.

Если $\deg P = 1$, то P — линейная форма:

$$P(x_1, \dots, x_m) = c_0 + \sum_i c_i x_i$$

Если, например, $c_1 \neq 0$, то $|S_1| \geq 2$ и, как бы ни были фиксированы $x_2 \leftarrow s_2, \dots, x_m \leftarrow s_m$, уравнение $P(x_1, s_2, \dots, s_m) = 0$ имеет не более одного корня.

Значит, найдётся $s_1 \in S_1$, для которого $P(s_1, s_2, \dots, s_m) \neq 0$.

Доказательство теоремы Алона

Пусть $\deg P > 1$, и для многочленов меньшей степени утверждение теоремы выполнено.

Б.о.о. будем считать, что $t_1 > 0$.

Зафиксируем произвольное $s \in S_1$ и поделим с остатком P на $(x_1 - s)$:

$$P = (x_1 - s) \cdot Q + R,$$

где $Q \not\equiv 0$ и $\deg_{x_1} R < \deg_{x_1}(x_1 - s) = 1$, то есть R *не зависит от* x_1.

Доказательство теоремы Алона

$$P = (x_1 - s) \cdot Q + R,$$

где $Q \not\equiv 0$ и $\deg_{x_1} R < \deg_{x_1}(x_1 - s) = 1,$ т.е. R не зависит от x_1.

Если найдётся набор $s_2 \in S_2, \dots, s_m \in S_m$, такой, что $R(s_2, \dots, s_m) \neq 0,$ то

$$P(s, s_2, \dots, s_m) \neq 0,$$

что и требовалось.

Остаётся разобрать случай, когда

$$\forall s_2 \in S_2, \dots, \forall s_m \in S_m \quad R(s_2, \dots, s_m) = 0.$$

Доказательство теоремы Алона

$$P = (x_1 - s) \cdot Q + R$$

Т.к. в P один из мономов степени $\deg P$ имеет вид $x_1^{t_1} \cdot \ldots \cdot x_m^{t_m}$,

то в Q один из мономов степени $\deg Q$ имеет вид $x_1^{t_1-1} \cdot \ldots \cdot x_m^{t_m}$.

По предположению индукции, найдутся такие

$$s_1 \in S_1 \setminus \{s\}, \quad s_2 \in S_2, \quad \ldots, \quad s_m \in S_m,$$

для которых

$$Q(s_1, \ldots, s_m) \neq 0.$$

Для таких $s_1, \ldots, s_m$ получаем

$$P(s_1, \ldots, s_m) = (s_1 - s) \cdot Q(s_1, \ldots, s_m) \neq 0$$

Аддитивная комбинаторика

Аддитивная комбинаторика изучает свойства подмножеств натуральных чисел и абелевых групп при сложении.

Пусть $A, B \subseteq G$, где G — абелева группа.

Обозначим

$$A + B := \{a + b \mid a \in A, b \in B\}$$

Вопрос: как можно оценить $|A + B|$, если известны $|A|$ и $|B|$?

Пример простой оценки сверху:

$$|A + B| \leq \min\{|G|, |A| \cdot |B|\}$$

Теорема Коши—Давенпорта

Теорема (Cauchy, Davenport).
Если $A, B \subseteq \mathbb{Z}_p$, где p — простое число, то

$$|A + B| \geq \min\{p, |A| + |B| - 1\}$$

Доказательство:
Сначала рассмотрим лёгкий случай $|A| + |B| > p$.
Для любого $c \in \mathbb{Z}_p$ имеем

$$|A| + |c - B| = |A| + |B| > p$$

а значит $A \cap (c - B) \neq \emptyset$, и найдутся $a \in A$ и $b \in B$, такие, что $a = c - b$. Отсюда $c \in A + B$.

Т.к. c брался произвольным, получаем $A + B = \mathbb{Z}_p$.

Теорема Коши—Давенпорта

Пусть теперь $|A| + |B| \leq p$.

Допустим, что $|A + B| < |A| + |B| - 1$, и придём к противоречию.

По предположению, найдётся $C \subset \mathbb{Z}_p$, такое, что $|C| = |A| + |B| - 2$ и $A + B \subseteq C$.

Рассмотрим многочлен

$$P(x, y) \coloneqq \prod_{c \in C} (x + y - c) \in \mathbb{Z}_p[x, y]$$

Заметим, что $P(x, y) = 0$ для любых $x \in A, y \in B$.

Теорема Коши—Давенпорта

$$P(x,y) \coloneqq \prod_{c \in C} (x + y - c) \in \mathbb{Z}_p[x,y]$$

Раскрыв скобки в определении P, видим, что

$$\operatorname{coef}_{x^{|A|-1}y^{|B|-1}} P = \left(\frac{(|A|+|B|-2)!}{(|A|-1)!(|B|-1)!}\right) \bmod p \quad \neq 0$$

то есть моном $x^{|A|-1}y^{|B|-1}$ реально входит в многочлен.

По теореме Алона, найдутся $a \in A$ и $b \in B$, такие, что $P(a,b) \neq 0$.

Но такого не может быть по определению P.

Покрытие вершин куба гиперплоскостями

Вопрос: сколько плоскостей нужно, чтобы покрыть все, *кроме одной*, вершины куба?

Теорема (Алон, Фюреди).
Наименьшее число плоскостей, достаточное, чтобы покрыть все, кроме одной, вершины куба в $\mathbb{R}^n$, равно n.

Доказательство:

Б.о.о. будем считать, что у нас куб $\{0,1\}^n$, и что вершина, которую мы не покрываем $(0,0,\dots,0)$.

Покрытие вершин куба гиперплоскостями

Куб $\{0,1\}^n$, не покрываем вершину $(0,0,\ldots,0)$.

n плоскостей достаточно — например, такие:

- $x_1 - 1 = 0$
- $x_2 - 1 = 0$
- …
- $x_n - 1 = 0$

Сложная часть — доказать, что меньшим числом плоскостей не обойтись.
Докажем это от противного…

Покрытие вершин куба гиперплоскостями

Допустим, мы обошлись m плоскостями, $m < n$. Пусть их уравнения такие:

$$\langle \boldsymbol{a}_1, \boldsymbol{x} \rangle - b_1 = 0$$
$$\vdots$$
$$\langle \boldsymbol{a}_m, \boldsymbol{x} \rangle - b_m = 0$$

При этом $b_1, \dots, b_m \neq 0$, т.к. ни одна из плоскостей не должна покрывать точку $(0,0, \dots, 0)$.
Рассмотрим многочлен:

$$P(x_1, \dots, x_n) \coloneqq \prod_{j=1}^{m} \left(b_j - \langle \boldsymbol{a}_j, \boldsymbol{x} \rangle\right) - \left(\prod_{j=1}^{m} b_j\right) \cdot \left(\prod_{i=1}^{n} (1 - x_i)\right)$$

Имеем $\deg P = n$, и

$$\operatorname{coef}_{x_1 \cdot x_2 \cdot \dots \cdot x_n} P = (-1)^{n+1} \prod_{j=1}^{m} b_j \neq 0.$$

По теореме Алона, найдутся $\alpha_1 \in \{0,1\}, \dots, \alpha_n \in \{0,1\}$, для которых $P(\alpha_1, \dots, \alpha_n) \neq 0$.

Покрытие вершин куба гиперплоскостями

Допустим, мы обошлись m плоскостями:

$$\langle \boldsymbol{a}_1, \boldsymbol{x} \rangle - b_1 = 0$$
$$\vdots$$
$$\langle \boldsymbol{a}_m, \boldsymbol{x} \rangle - b_m = 0$$

По теореме Алона, найдётся точка из $\{0,1\}^n$, на которой многочлен

$$P(x_1, \dots, x_n) \coloneqq \prod_{j=1}^{m} \left(b_j - \langle \boldsymbol{a}_j, \boldsymbol{x} \rangle\right) - \left(\prod_{j=1}^{m} b_j\right) \cdot \left(\prod_{i=1}^{n} (1 - x_i)\right)$$

не равен нулю. Но это невозможно:

- $P(0, \dots, 0) = \prod_{j=1}^{m} \left(b_j\right) - \left(\prod_{j=1}^{m} b_j\right) \cdot \left(\prod_{i=1}^{n} 1\right) = 0$
- Для любой точки $(\alpha_1, \dots, \alpha_n) \in \{0,1\}^n \setminus \{(0, \dots, 0)\}$ имеем $P(\alpha_1, \dots, \alpha_n) = \prod_{j=1}^{m} (0) - \left(\prod_{j=1}^{m} b_j\right) \cdot 0 = 0$

Регулярные подграфы в регулярных графах

Общая постановка многих задач в теории графов:
в данном графе с известными свойствами выделить подграф
с требуемыми свойствами.

Например:

- В заданном графе найти максимальную клику
- В заданном несвязном графе найти компоненту связности
  с максимальным числом вершин.
- …

Регулярные подграфы в регулярных графах

Вопрос: во всяком ли k-регулярном графе существует $(k-1)$-регулярный подграф?

Известно следующее:

- Это так для $k \leq 3$ — *простое упражнение*.
- Это так для $k = 4$ — и это трудная теорема (В.А. Ташкинов ’1984)
- Это в общем случае не верно для $k \geq 6$

Регулярные подграфы в регулярных графах

Вопрос: во всяком ли k-регулярном графе существует k'-регулярный подграф ($k' < k$)?

Известно, например, что для любых нечётных k и k' ответ на вопрос положительный.

Если ослабить условие «строгой» регулярности и рассматривать «почти регулярные» графы (у которых степени вершин близки, но необязательно равны) — тоже можно доказать кое-что интересное…

Регулярные подграфы в регулярных графах

Теорема (Алон, Фридланд, Калаи).
Пусть p — простое число. Пусть $G = (V, E)$ — мультиграф (без петель), удовлетворяющий условиям

- $\Delta(G) \leq 2p - 1$,
- $\frac{1}{|V|} \sum_{v \in V} d(v) > 2p - 2$.

Тогда в G есть p-регулярный подграф.

Доказательство теоремы А—Ф—К

- $\Delta(G) \leq 2p-1, \quad$ и $\frac{1}{|V|}\sum_{v\in V} d(v) > 2p-2$

Каждому $e \in E$ сопоставим переменную x_e.

Рассмотрим многочлен от переменных $\{x_e\}_{e\in E}$ с коэффициентами в $\mathbb{Z}_p$:

$$P \coloneqq \prod_{v\in V}\left(1-\left(\sum_{e\in E:\, e\ni v} x_e\right)^{p-1}\right) - \prod_{e\in E}(1-x_e)$$

Доказательство теоремы А—Ф—К

- $\frac{1}{|V|}\sum_{v\in V} d(v) > 2p-2$

$$P \coloneqq \underbrace{\prod_{v\in V}\left(1-\left(\sum_{e\in E:\, e\ni v} x_e\right)^{p-1}\right)}_{Q} - \prod_{e\in E}(1-x_e)$$

Из условия, $2\cdot|E| = \sum_{v\in V} d(v) > (2p-2)\cdot|V|$, отсюда

$$\deg Q \le (p-1)\cdot|V| < |E|.$$

Следовательно, $\deg P = |E|$.

При этом, $\operatorname{coef}_{\prod_{e\in E} x_e} P = (-1)^{|E|+1} \neq 0.$

Доказательство теоремы А—Ф—К

$$P \coloneqq \prod_{v \in V} \left(1 - \left(\sum_{e \in E\colon e \ni v} x_e\right)^{p-1}\right) - \prod_{e \in E} (1 - x_e)$$

$\deg P = |E|$ и $\operatorname{coef}_{\prod_{e \in E} x_e} P = (-1)^{|E|+1} \neq 0.$

Значит, по теореме Алона, найдётся набор значений $\boldsymbol{\alpha} = (\alpha_e)_{e \in E} \in \{0,1\}^{|E|}$, такой, что $P(\boldsymbol{\alpha}) \neq 0$.

При этом для любого $v \in V$ имеем

$$\sum_{e \in E\colon e \ni v} \alpha_e \overset{p}{=} 0,$$

иначе, по малой теореме Ферма, получилось бы

$$\left(\sum_{e \in E\colon e \ni v} \alpha_e\right)^{p-1} \overset{p}{=} 1 \quad \Rightarrow \quad P(\boldsymbol{\alpha}) = 0 \qquad (\text{в } \mathbb{Z}_p).$$

Доказательство теоремы А—Ф—К

- $\Delta(G) \leq 2p - 1$
- $P \coloneqq \prod_{v \in V}(1 - (\sum_{e \in E:\, e \ni v} x_e)^{p-1}) - \prod_{e \in E}(1 - x_e)$

Нашли $\boldsymbol{\alpha} \in \{0,1\}^{|E|}$, т. ч. $P(\boldsymbol{\alpha}) \neq 0$, и $\forall v \in V$

$$\sum_{e \in E:\, e \ni v} \alpha_e \overset{p}{=} 0$$

Кроме того, видно, что $\boldsymbol{\alpha} \neq \mathbf{0}$. Взяв те рёбра G, для которых $\alpha_e = 1$, и все вершины G, получим непустой остовный подграф G'.

В подграфе G' степень каждой вершины v равна $\sum_{e \in E:\, e \ni v} \alpha_e \overset{p}{=} 0$, а значит, эта степень равна нулю либо p.

Доказательство теоремы А—Ф—К

По набору $\boldsymbol{\alpha}$ построили непустой остовный подграф G'.

В подграфе G' степень каждой вершины равна нулю или p.

Выбросив из G' вершины нулевой степени, получим искомый p-регулярный подграф.