1)Теорема Бернштейна-Кантора

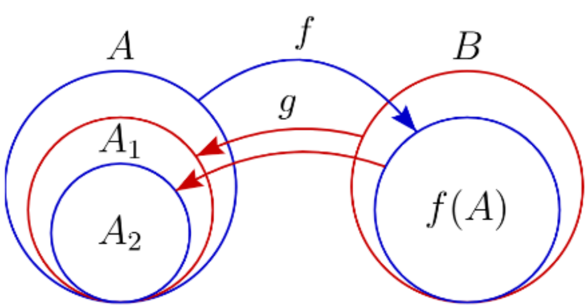
Теорема Бернштейна–Кантора

Биекция между множествами A и B существует тогда и только тогда, когда существуют инъекции из A в B и из B в A.

- Доказательство:
  - необходимость очевидна, так как биекция — частный случай инъекции
  - достаточность на следующем слайде
- Пример: отрезок $[0,1]$ и интервал $(0,1)$ равномощны
  - выберем α, β так, что $0 < \alpha < \beta < 1$
  - линейная функция $f(x) = \beta x + \alpha(1-x)$ — биекция $[0,1]$ на $[\alpha,\beta] \subseteq (0,1)$ и $(0,1)$ на $(\alpha,\beta) \subseteq [0,1]$
  - биекцию между $[0,1]$ и $(0,1)$ построить немного сложнее; в частности, она не может быть непрерывной функцией (почему?)

Доказательство теоремы Бернштейна–Кантора

Пусть $f : A \to B$ и $g : B \to A$ — инъекции; обозначим $A_1 = g(B)$, $A_2 = g(f(A))$:



g — биекция B на A_1
$\phi = f \circ g$ — биекция A на A_2

Так как B равномощно A_1, достаточно построить биекцию A на A_1

- Положим $C_0 = A_1 \backslash A_2$, $C_n = \phi(C_{n-1})$ для всех $n \in \mathbb{N}$, $C = \bigcup_{n=0}^{\infty} C_i$
- Определим функцию $\psi : A \to A$ условием $\psi(a) = \begin{cases} a, & a \in C \\ \phi(a), & a \notin C \end{cases}$
- $\psi(A) \subseteq A_1$ по определениям A_2, ϕ и C; докажем, что ψ — биекция A на A_1
- достаточно доказать, что любой элемент A_1 имеет единственный ψ-прообраз
  - пусть $c \in C$; тогда c — единственный ψ-прообраз c, принадлежащий C
    - если $a \notin C$ — ψ-прообраз $c \Rightarrow a = \phi^{-1}(c) \Rightarrow c \in C_i$, $i \geqslant 1$
    $\Rightarrow a \in C_{i-1} \subseteq C \Rightarrow$ противоречие $\Rightarrow c$ — единственный ψ-прообраз c
  - пусть $c \in A_1 \backslash C$; тогда у c нет ψ-прообразов в C
    - $c \in A_2$, т.е. имеет ψ-прообраз $\phi^{-1}(c)$ (единственный ввиду инъективности ϕ) $\square$

2)Вторая лемма о частных решениях

Вторая лемма о частных решениях

Пусть характеристический многочлен $\chi(x)$ рекуррентного соотношения $f(n) = a_1 f(n-1) + \dots + a_k f(n-k)$ имеет корень λ кратности не менее $m+1$. Тогда функция $f(n) = n^m \lambda^n$ является решением данного соотношения.

Доказательство:

- При $m = 0$ доказано ранее (лемма о частных решениях); далее $m > 0$
  - ⋆ λ является корнем первых m производных многочлена $\chi(x)$
  - ⋆ умножение многочлена на x не меняет кратности его ненулевых корней
  - ⋆ если многочлены $p_1(x)$ и $p_2(x)$ имеют общий корень λ кратности m_1 и m_2 соответственно, то у $p_1(n) \pm p_2(n)$ есть корень λ кратности $\min\{m_1, m_2\}$

$\Rightarrow$ λ является корнем многочленов

1. $x^n - a_1 x^{n-1} - \dots - a_k x^{n-k}$
2. $x^{n+1} - a_1 x^n - \dots - a_k x^{n-k+1}$
3. $(n+1)x^n - a_1 n x^{n-1} - \dots - a_k(n-k+1)x^{n-k}$ (производная многочлена 2)
4. $nx^n - a_1(n-1)x^{n-1} - \dots - a_k(n-k)x^{n-k}$ (вычли 1 из 3)

⋆ λ обращает многочлен 4 в ноль $\Rightarrow$ $n\lambda^n$ — решение нашего соотношения

⋆ умножим многочлен 4 на x, возьмем производную и вычтем многочлен 4:

$$n^2 x^n - a_1(n-1)^2 x^{n-1} - \dots - a_k(n-k)^2 x^{n-k}$$

$\Rightarrow$ $n^2\lambda^n$ — решение нашего соотношения

- Повторяя m раз, получаем решения $n\lambda^n, n^2\lambda^n, \dots, n^m\lambda^n$ $\square$

3)Переход к системе линейных уравнений и возведению матрицы в степень

Переход к системе линейных уравнений

Для компактности записи, пусть $f_n = f(n)$; запишем систему линейных уравнений

$$\begin{cases} f_n &= a_1 f_{n-1} + \dots + a_k f_{n-k} \\ f_{n-1} &= f_{n-1} \\ \cdots &= \cdots \\ f_{n-k+1} &= f_{n-k+1} \end{cases}$$

в матричном виде:

$$\begin{bmatrix} f_n \\ f_{n-1} \\ f_{n-2} \\ \vdots \\ f_{n-k+1} \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & \dots & a_{k-1} & a_k \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix} \begin{bmatrix} f_{n-1} \\ f_{n-2} \\ f_{n-3} \\ \vdots \\ f_{n-k} \end{bmatrix}$$

- Пусть $\vec{f_n} = (f_{n+k-1}, \dots, f_n)^\perp$, A — матрица системы

$\Rightarrow$ $\vec{f_n} = A\vec{f}_{n-1}$ для любого $n \geqslant 1$

$\Rightarrow$ $\vec{f_n} = A^n \vec{f_0}$ ($\vec{f_0}$ — вектор начальных значений функции f)

★ Задача: найти выражение для последней компоненты вектора, являющегося произведением степени известной матрицы на известный вектор

- степени матрицы A вычисляются через жорданову матрицу $J = TAT^{-1}$

4)Лемма о степени жордановой клетки

Жордановы матрицы

- Жорданова клетка — это матрица вида $J = \begin{bmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ 0 & 0 & \lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \lambda \end{bmatrix}$
  - ⋆ $J[i,i] = \lambda$ для всех i и некоторого $\lambda \in \mathbb{C}$; $J[i,i+1] = 1$; $J[i,j] = 0$ иначе
- Жорданова матрица — это блочно-диагональная матрица $J = \begin{bmatrix} \boxed{J_1} & & & 0 \\ & \boxed{J_2} & & \\ & & \ddots & \\ 0 & & & \boxed{J_r} \end{bmatrix}$,

  где все матрицы J_i — жордановы клетки (возможно, разных размеров)

★ Теорема Жордана: для любой матрицы $A \in \mathbb{C}^{k \times k}$ существует такая обратимая матрица T, что матрица $J = TAT^{-1}$ — жорданова

★ Равенство $A = T^{-1}JT$ можно использовать для возведения A в степень:
$A^n = (T^{-1}JT)^n = T^{-1}J^nT$

$\Rightarrow$ Достаточно уметь возводить в степень жордановы матрицы

Лемма о степени жордановой клетки

Пусть J — жорданова клетка размера t с числом λ. Тогда $J^n[i,j] = \binom{n}{j-i}\lambda^{n+i-j}$.
(Полагаем $\binom{n}{x} = 0$ при $x < 0$ и $x > n$.)

⋆ Лемма утверждает, что $J^n = \begin{bmatrix} \lambda^n & n\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & \dots & \binom{n}{t-1}\lambda^{n-t+1} \\ 0 & \lambda^n & n\lambda^{n-1} & \dots & \binom{n}{t-2}\lambda^{n-t+2} \\ 0 & 0 & \lambda^n & \dots & \binom{n}{t-3}\lambda^{n-t+3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \lambda^n \end{bmatrix}$

Доказательство по индукции: база ($n = 1$) очевидна; шаг индукции:

$$J^{n+1}[i,j] = \sum_{k=1}^{t} J^n[i,k] \cdot J[k,j] = J^n[i,j-1] + J^n[i,j] \cdot \lambda =$$
$$\binom{n}{j-1-i}\lambda^{n+i-j+1} + \binom{n}{j-i}\lambda^{n+i-j+1} = \binom{n+1}{j-i}\lambda^{n+1+i-j} \quad \square$$

Следствие: Для жордановой матрицы выполняется $J^n = \begin{bmatrix} \boxed{J_1^n} & & & 0 \\ & \boxed{J_2^n} & & \\ & & \ddots & \\ 0 & & & \boxed{J_r^n} \end{bmatrix}$

5)Лемма о характеристических многочленах

Лемма о характеристических многочленах

$|\lambda E - A| = \chi(\lambda)$

Доказательство: разложим определитель по первой строке (красный множитель — знак слагаемого, синий — определитель подматрицы в столбцах $1, \ldots, i-1$)

$$|\lambda E - A| = \begin{vmatrix} \lambda - a_1 & -a_2 & \ldots & -a_{k-1} & -a_k \\ -1 & \lambda & \ldots & 0 & 0 \\ 0 & -1 & \ldots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & -1 & \lambda \end{vmatrix} =$$

$$(\lambda - a_1)\lambda^{k-1} + \sum_{i=2}^{k} (-1)^{i+1}(-a_i)(-1)^{i-1}\lambda^{k-i} = \lambda^k - a_1\lambda^{k-1} - \cdots - a_{k-1}\lambda - a_k \quad \square$$

6)Теорема в общем случае

Общее решение

Теорема об общем решении (для произвольных корней)

Пусть характеристический многочлен рекуррентного соотношения $f(n) = a_1 f(n-1) + \cdots + a_k f(n-k)$ имеет s различных корней $\lambda_1, \ldots, \lambda_s \in \mathbb{C}$ с кратностями $m_1, \ldots, m_s$ соответственно, $m_1 + \cdots + m_s = k$. Тогда общее решение этого соотношения над $\mathbb{C}$ имеет вид

$$f(n) = (C_1 + \ldots + C_{m_1} n^{m_1 - 1})\lambda_1^n + \ldots + (C_{m_1 + \ldots + m_{s-1} + 1} + \ldots + C_k n^{m_s - 1})\lambda_s^n,$$

где константы $C_1, \ldots, C_k$ пробегают множество $\mathbb{C}$.

- По второй лемме о частных решениях мы знаем k специальных решений
  - вида $n^j \lambda_i^n$, где $i = 1, \ldots, s$; $j = 0, \ldots, m_i - 1$
- Теорема утверждает, что эти решения образуют базис пространства решений
  - которое имеет размерность k
- Доказать линейную независимость специальных решений, как в случае простых корней, не получится

★ Чтобы доказать теорему, мы покажем методами линейной алгебры, что любое решение является линейной комбинацией специальных решений

Собираем все вместе

- $A = \begin{bmatrix} a_1 & a_2 & \dots & a_{k-1} & a_k \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}$, $\vec{f}_n = A^n \vec{f}_0$

⋆ $A^n = T^{-1} J^n T$, J — жорданова

  ⋆ теорема Жордана

⋆ На диагонали матрицы J стоят корни $\chi(x)$ — числа $\lambda_1(m_1 \text{ раз}), \dots, \lambda_s(m_s \text{ раз})$

  ⋆ лемма о характеристических многочленах + подобие A и J

⋆ Размер жордановой клетки в J с числом λ_i не превосходит m_i $(i = 1, \dots, s)$

⋆ Ненулевые элементы J^n являются произведениями полиномов на экспоненты:

  ⋆ по лемме о степенях жордановой матрицы,
  $\binom{n}{j-i}\lambda^{n+i-j} = \frac{\lambda^{i-j}}{(j-i)!} n(n-1)\cdots(n+i-j+1)\lambda^n = p(n)\lambda^n$

⋆ Матрицы T и T^{-1}, как и вектор $\vec{f}_0$, не зависят от n

⇒ Элементы матрицы $T^{-1}J^nT = A^n$ и вектора $\vec{f}_n = A^n\vec{f}_0$ — линейные комбинации произведений вида $p(n)\lambda^n$

Пример ⟹

Собираем все вместе (2)

Пример: пусть $J = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \mu \end{bmatrix}$, $T[i,j] = t_{ij}$, $T^{-1}[i,j] = \tau_{ij}$; тогда

$$J^n = \begin{bmatrix} \lambda^n & \frac{n}{\lambda}\lambda^n & 0 \\ 0 & \lambda^n & 0 \\ 0 & 0 & \mu^n \end{bmatrix}, \; J^nT = \begin{bmatrix} (t_{11} + \frac{t_{21}}{\lambda}n)\lambda^n & (t_{12} + \frac{t_{22}}{\lambda}n)\lambda^n & (t_{13} + \frac{t_{23}}{\lambda}n)\lambda^n \\ t_{21}\lambda^n & t_{22}\lambda^n & t_{23}\lambda^n \\ t_{31}\mu^n & t_{32}\mu^n & t_{33}\mu^n \end{bmatrix},$$

$$T^{-1}J^nT = \begin{bmatrix} (\tau_{11}t_{11} + \tau_{12}t_{21} + \frac{\tau_{11}t_{21}}{\lambda}n)\lambda^n + \tau_{13}t_{31}\mu^n & (\dots) & (\dots) \\ (\tau_{21}t_{21} + \tau_{22}t_{21} + \frac{\tau_{21}t_{21}}{\lambda}n)\lambda^n + \tau_{23}t_{32}\mu^n & (\dots) & (\dots) \\ (\tau_{31}t_{21} + \tau_{32}t_{21} + \frac{\tau_{31}t_{21}}{\lambda}n)\lambda^n + \tau_{33}t_{33}\mu^n & (\dots) & (\dots) \end{bmatrix}$$

⋆ Любая функция, удовлетворяющая соотношению $f(n) = a_1 f(n-1) + \dots + a_k f(n-k)$, имеет вид $f(n) = p_1(n)\lambda_1^n + \dots + p_s(n)\lambda_s^n$, где $p_i(n)$ — многочлен степени не выше $m_i - 1$, $i = 1, \dots, s$

⇒ $f(n)$ является линейной комбинацией специальных решений $\lambda_1^n, \dots, n^{m_1-1}\lambda_1^n, \dots, \lambda_s^n, \dots, n^{m_s-1}\lambda_s^n$,

что и требовалось доказать □

7)Асимптотика n-го простого числа

Учимся считать: n-е простое число

Пусть $\pi(n)$ — количество простых чисел, не превосходящих n

★ Одна из важнейших комбинаторных теорем утверждает, что $\pi(n) \sim \frac{n}{\ln n}$

  ★ более точно, $\pi(n) = \frac{n}{\ln n} + O\left(\frac{n}{\ln^2 n}\right)$

- Задача: найти асимптотическую формулу для n-го простого числа
- Решение: пусть $p = p(n)$ — n-е простое число, тогда $\pi(p) = n$

  $\Rightarrow$ $n = \frac{p}{\ln p} + O\left(\frac{p}{\ln^2 p}\right)$

  ⋆ надо решить это «уравнение» относительно p

  - $O\left(\frac{p}{\ln^2 p}\right) = o\left(\frac{p}{\ln p}\right) \Rightarrow \frac{p}{\ln p} = O(n)$

  $\Rightarrow$ $O\left(\frac{p}{\ln^2 p}\right) = O\left(\frac{n}{\ln p}\right) = O\left(\frac{n}{\ln n}\right)$ (т.к. $p > n$)

  $\Rightarrow$ $\frac{p}{\ln p} = n + O\left(\frac{n}{\ln n}\right) = n\left(1 + O\left(\frac{1}{\ln n}\right)\right) \Rightarrow p = n \ln p\left(1 + O\left(\frac{1}{\ln n}\right)\right)$

  ⋆ надо избавиться от $\ln p$ справа; логарифмируем обе части

  - $\ln p = \ln n + \ln\ln p + O\left(\frac{1}{\ln n}\right)$

  $\Rightarrow$ $p < n^2$ для больших $n \Rightarrow \ln p < 2\ln n \Rightarrow \ln\ln p < \ln\ln n + O(1)$

  $\Rightarrow$ $\ln p = \ln n + \ln\ln n + O(1)$

  $\Rightarrow$ $p = n(\ln n + \ln\ln n + O(1))\left(1 + O\left(\frac{1}{\ln n}\right)\right) = n\ln n + n\ln\ln n + O(n)$ □

! Начав с более точной формулы $\pi(n) = \frac{n}{\ln n} + \frac{n}{\ln^2 n} + O\left(\frac{n}{\ln^3 n}\right)$, выведите более точное приближение для p

8)Уточнение формулы Стирлинга

Учимся считать: уточнение формулы Стирлинга

Мы знаем формулу Стирлинга в виде $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$

- Более точные варианты:
  - ⋆ $n! = \left(1 + O\left(\frac{1}{n}\right)\right)\sqrt{2\pi n}\left(\frac{n}{e}\right)^n$
  - ⋆ $n! = \left(1 + \frac{a}{n} + O(n^{-2})\right)\sqrt{2\pi n}\left(\frac{n}{e}\right)^n$
  - ⋆ $n! = \left(1 + \frac{a}{n} + \frac{b}{n^2} + O(n^{-3})\right)\sqrt{2\pi n}\left(\frac{n}{e}\right)^n \qquad (1)$
  - ...
- Задача: уточнить формулу Стирлинга, найдя константу a
- Метод: шевеление (малое возмущение) формулы (1)
  - $n! = n(n-1)!$
  - $(n-1)! = \left(1 + \frac{a}{n-1} + \frac{b}{(n-1)^2} + O((n-1)^{-3})\right)\sqrt{2\pi(n-1)}\left(\frac{n-1}{e}\right)^{n-1}$
  - ⋆ заметим, что $\frac{n-1}{n} = 1 - n^{-1}$; $\frac{n}{n-1} = (1-n^{-1})^{-1} = 1 + \frac{1}{n} + \frac{1}{n^2} + \cdots \Rightarrow$
  - $\frac{a}{n-1} = \frac{a}{n} \cdot \frac{n}{n-1} = \frac{a}{n} + \frac{a}{n^2} + O(n^{-3})$
  - $\frac{b}{(n-1)^2} = \frac{b}{n^2} + O(n^{-3})$
  - $O((n-1)^{-3}) = O(n^{-3})$
  - $\sqrt{2\pi(n-1)} = \sqrt{2\pi n}(1-n^{-1})^{1/2} = \sqrt{2\pi n}\left(1 - \frac{1}{2n} - \frac{1}{8n^2} + O(n^{-3})\right)$
    - формула Тейлора $(1+x)^\alpha = 1 + \alpha x + \frac{\alpha(\alpha-1)}{2}x^2 + O(x^3)$ при $x = -\frac{1}{n}$, $\alpha = \frac{1}{2}$
- Имеем
  - $(n-1)! = \left(1 + \frac{a}{n} + \frac{a+b}{n^2} + O(n^{-3})\right)\left(1 - \frac{1}{2n} - \frac{1}{8n^2} + O(n^{-3})\right)\sqrt{2\pi n}\left(\frac{n-1}{e}\right)^{n-1}$

Уточнение формулы Стирлинга (2)

$(n-1)! = \left(1 + \frac{a}{n} + \frac{a+b}{n^2} + O(n^{-3})\right)\left(1 - \frac{1}{2n} - \frac{1}{8n^2} + O(n^{-3})\right)\sqrt{2\pi n}\left(\frac{n-1}{e}\right)^{n-1}$

- Оценим $(n-1)^{n-1}$:
  - $(n-1)^{n-1} = n^{n-1}(1-n^{-1})^{n-1} = n^{n-1}(1-n^{-1})^n(1+n^{-1}+n^{-2}+O(n^{-3}))$
  - $(1-n^{-1})^n = e^{n\cdot\ln(1-n^{-1})} =$ [Тейлор]
    $= e^{n\left(-\frac{1}{n}-\frac{1}{2n^2}-\frac{1}{3n^3}+O\left(\frac{1}{n^4}\right)\right)} = e^{-1-\frac{1}{2n}-\frac{1}{3n^2}+O\left(\frac{1}{n^3}\right)} =$ [Тейлор]
    $= e^{-1}\left(1 - \frac{1}{2n} + \frac{1}{8n^2} + O(n^{-3})\right)\left(1 - \frac{1}{3n^2} + O(n^{-3})\right)\left(1 + O(n^{-3})\right)$
    $= e^{-1}\left(1 - \frac{1}{2n} - \frac{5}{24n^2} + O(n^{-3})\right)$
- Перемножим все скобки вида $1 + o(1)$:

$$\left(1 + \frac{a}{n} + \frac{a+b}{n^2} + O(n^{-3})\right)\left(1 - \frac{1}{2n} - \frac{1}{8n^2} + O(n^{-3})\right)\left(1 + \frac{1}{n} + \frac{1}{n^2} + O(n^{-3})\right)\cdot$$
$$\left(1 - \frac{1}{2n} - \frac{5}{24n^2} + O(n^{-3})\right) = \left(1 + \frac{a}{n} + \frac{a+b-1/12}{n^2} + O(n^{-3})\right)$$

- В итоге,
  - $n! = n(n-1)! = n\left(1 + \frac{a}{n} + \frac{a+b-1/12}{n^2} + O(n^{-3})\right)\sqrt{2\pi n}\left(\frac{n}{e}\right)^{n-1}\cdot\frac{1}{e} =$
    $= \left(1 + \frac{a}{n} + \frac{a+b-1/12}{n^2} + O(n^{-3})\right)\sqrt{2\pi n}\left(\frac{n}{e}\right)^n \qquad (2)$
- Коэффициенты (2) равны коэффициентам исходной формулы Стирлинга (1)
  $\Rightarrow a + b - \frac{1}{12} = b \Rightarrow a = \frac{1}{12}$

★ выражение $\left(1 + \frac{1}{12n}\right)\sqrt{2\pi n}\left(\frac{n}{e}\right)^n$ дает очень хорошее приближение для n!

9)Теорема Оре

Теорема Оре

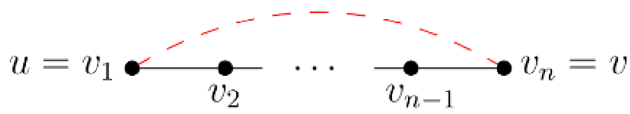
Пусть G — обыкновенный граф с n вершинами, $n > 2$. Если $\deg(u) + \deg(v) \geqslant n$ для любых двух несмежных вершин u и v графа G, то граф G гамильтонов.

Доказательство: от противного

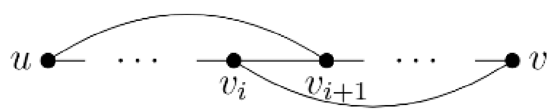
- пусть существует граф G, удовлетворяющий всем условиям теоремы и не являющийся гамильтоновым
- ★ если возможно, добавим к G новое ребро так, чтобы граф остался негамильтоновым
- ★ новый граф тоже удовлетворяет всем условиям теоремы
- будем повторять данную процедуру, пока это возможно
- в какой-то момент получим граф G', который удовлетворяет всем условиям теоремы и является максимальным негамильтоновым
  - превращается в гамильтонов при добавлении любого ребра
  - существование такого G' следует из того, что полный граф гамильтонов
- получим противоречие, построив гамильтонов цикл в G' $\Longrightarrow$

Доказательство теоремы Оре (окончание)

- Пусть u и v — произвольные несмежные вершины графа G'
- ⋆ В G' нет гамильтонова цикла, но при добавлении ребра (u, v) появится
  - $\Rightarrow$ в G' есть гамильтонов (u, v)-путь:



- Пусть $S = \{i \mid u \text{ смежна с } v_{i+1}\}$ и $T = \{i \mid v \text{ смежна с } v_i\}$
  - ⋆ $|S| = \deg(u)$, $|T| = \deg(v)$
  - $\Rightarrow$ $|S| + |T| \geqslant n$ по условию теоремы
  - элементы множеств S и T являются числами 1 до $n-1$
  - $\Rightarrow$ $S \cap T \neq \varnothing$
  - пусть $i \in S \cap T \Rightarrow$ в G' есть ребра (u, v_{i+1}) и (v_i, v):



$\Rightarrow$ В графе G' есть гамильтонов цикл
  - $u \to v_2 \to \cdots \to v_i \to v \to v_{n-1} \to \cdots \to v_{i+1} \to u$
- Требуемое противоречие получено

10)Теорема Клини

- Детерминированный конечный автомат (ДКА) — это пятерка $\mathcal{A} = (Q, \Sigma, \delta, s, T)$:
  - Q — непустое конечное множество состояний автомата
  - Σ — алфавит автомата (непустое конечное множество)
  - $\delta : Q \times \Sigma \to Q$ — функция переходов
  - $s \in Q$ — начальное (стартовое) состояние
  - $T \subseteq Q$ — множество конечных (терминальных) состояний

- НКА — это пятерка $\mathcal{A} = (Q, \Sigma, \delta, S, T)$, где $\delta \subseteq Q \times \Sigma \times Q$ — множество переходов
- ⋆ иногда δ удобно записывать как функцию $\delta : Q \times \Sigma \to 2^Q$
- $\delta(q, a)$ — множество вершин, в которые из q ведет ребро с меткой a
  - ⋆ $\delta(q, a)$ может быть пустым
- доопределим функцию δ:
- ⋆ $\delta(q, w)$ — множество вершин, в которые из q ведет маршрут, помеченный w
- ⋆ $\delta(P, w)$, где $P \subseteq Q$, — множество вершин, в которые ведет маршрут, помеченный w и начинающийся в вершине из P

- Пусть $\Sigma = \{a_1, \ldots, a_n\}$
- Язык $L \subseteq \Sigma^*$ — регулярный, если он может быть получен применением конечного числа операций объединения, умножения и итерации к языкам $\varnothing, \{\lambda\}, \{a_1\}, \ldots, \{a_n\}$
  - операции $\cup, \cdot, {}^*$ также называются регулярными
- Можно взять замыкание любого множества языков $\mathbf{L} \subseteq 2^{\Sigma^*}$ относительно регулярных операций

★ Множество $\mathbf{R} \subset 2^{\Sigma^*}$ всех регулярных языков над Σ совпадает с замыканием множества всех конечных языков над Σ относительно регулярных операций

- Обычный способ записи регулярных языков — регулярные выражения:
  - символы $\varnothing, \lambda, a \in \Sigma$ являются регулярными выражениями
  - r, s — регулярные выражения $\Rightarrow$ $(r)|(s)$, $(r) \cdot (s)$, $(r)^*$ — регулярные выражения
  - других регулярных выражений нет
    - ⋆ $|$ — стандартный символ для перечисления альтернатив (соответствует операции $\cup$)
    - ⋆ иногда вместо $|$ пишут $+$

Теорема Клини

Язык регулярен тогда и только тогда, когда он распознается некоторым конечным автоматом.

Теорема Рабина–Скотта

Для любого НКА существует ДКА, распознающий тот же самый язык.

Регулярные языки распознаются автоматами

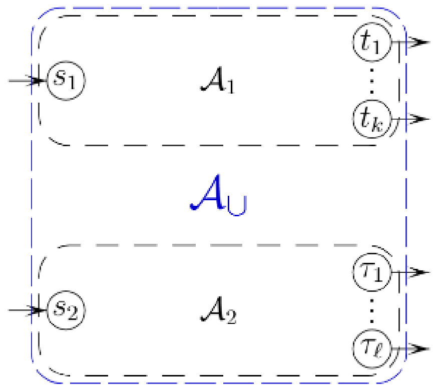
Докажем, что любой регулярный язык распознается конечным автоматом

- ⋆ теорема Рабина–Скотта дает использовать ДКА и НКА вперемешку

План:

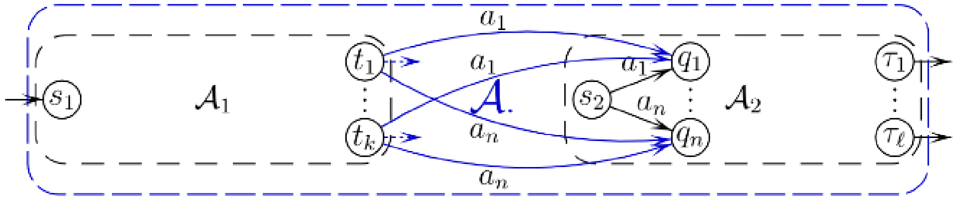
1. построить автоматы, распознающие языки $\varnothing, \{\lambda\}, \{a\}$
   - ! постройте самостоятельно
2. по ДКА $\mathcal{A}_1 = (Q_1, \Sigma, \delta_1, s_1, T_1)$ и $\mathcal{A}_2 = (Q_2, \Sigma, \delta_2, s_2, T_2)$ построить автоматы, распознающие языки
   - $L(\mathcal{A}_1) \cup L(\mathcal{A}_2)$
   - $L(\mathcal{A}_1) \cdot L(\mathcal{A}_2)$
   - $(L(\mathcal{A}_1))^*$

$$\mathcal{A}_\cup = (Q_1 \cup Q_2, \Sigma, \delta_1 \cup \delta_2, \{s_1, s_2\}, T_1 \cup T_2)$$
$$L(\mathcal{A}_\cup) = L(\mathcal{A}_1) \cup L(\mathcal{A}_2)$$



Регулярные языки распознаются автоматами (2)

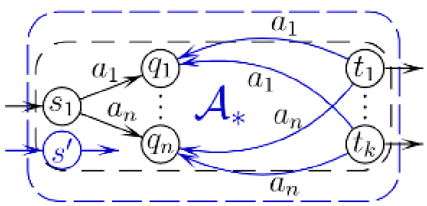
$\mathcal{A}_\cdot = (Q_1 \cup Q_2, \Sigma, \delta, \{s_1\}, T_2)$ при $\lambda \notin L_2$,
$\mathcal{A}_\cdot = (Q_1 \cup Q_2, \Sigma, \delta, \{s_1\}, T_1 \cup T_2)$ при $\lambda \in L_2$,
где $\delta = \delta_1 \cup \delta_2 \cup \{(t, a, q) \mid t \in T_1, q \in Q_2, (s_2, a, q) \in \delta_2\}$
$L(\mathcal{A}_\cdot) = L(\mathcal{A}_1) \cdot L(\mathcal{A}_2)$



$\mathcal{A}_* = (Q_1 \cup \{s'\}, \Sigma, \delta', \{s_1, s'\}, T \cup \{s'\})$, где
$\delta' = \delta_1 \cup \{(t, a, q) \mid t \in T, q \in Q_1, (s_1, a, q) \in \delta\}$

- s' нужно только для распознавания λ

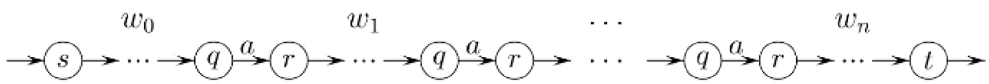
$L(\mathcal{A}_*) = (L(\mathcal{A}_1))^*$



Регулярность автоматных языков

- Пусть $\mathcal{A} = (Q, \Sigma, \delta, s, T)$ — автомат; докажем, что $L(\mathcal{A}) \in \mathbf{R}$ индукцией по $|\delta|$
  База индукции: $|\delta| = 0$
  - $L(\mathcal{A}) = \{\lambda\} \in \mathbf{R}$ при $s \in T$ и $L(\mathcal{A}) = \varnothing \in \mathbf{R}$ при $s \notin T$

  Шаг индукции: $|\delta| = k$
  - по предположению индукции, языки, распознаваемые автоматами с менее чем k переходами (ребрами), регулярны
  - возьмем произвольный переход $(q, a, r) \in \delta$, пусть $\delta' = \delta \setminus \{(q, a, r)\}$; положим
    $\mathcal{A}_0 = (Q, \Sigma, \delta', s, T)$
    $\mathcal{A}_1 = (Q, \Sigma, \delta', s, \{q\})$
    $\mathcal{A}_2 = (Q, \Sigma, \delta', r, \{q\})$
    $\mathcal{A}_3 = (Q, \Sigma, \delta', r, T)$
  - ⋆ языки $L(\mathcal{A}_0), L(\mathcal{A}_1), L(\mathcal{A}_2), L(\mathcal{A}_3)$ регулярны по предположению индукции
- Докажем, что $L(\mathcal{A}) = L(\mathcal{A}_0) \cup L(\mathcal{A}_1)a(L(\mathcal{A}_2)a)^*L(\mathcal{A}_3)$
  - пусть $w \in L(\mathcal{A})$ помечает (s, t)-маршрут W в $\mathcal{A}$, $t \in T$
  - ⋆ если $(q, a, r) \notin W$, то $w \in L(\mathcal{A}_0)$
  - ⋆ если $(q, a, r) \in W$, то $w = w_0 a w_1 \ldots a w_n$, где a отмечают все случаи использования перехода (q, a, r):



  $\Rightarrow$ $w_0 \in L(\mathcal{A}_1)$, $w_1, \ldots, w_{n-1} \in L(\mathcal{A}_2)$, $w_n \in L(\mathcal{A}_3)$ $\Rightarrow$ $w \in L(\mathcal{A}_1)a(L(\mathcal{A}_2)a)^*L(\mathcal{A}_3)$
  $\Rightarrow$ $w \in L(\mathcal{A}_0) \cup L(\mathcal{A}_1)a(L(\mathcal{A}_2)a)^*L(\mathcal{A}_3)$
  - $L(\mathcal{A}_0) \subseteq L(\mathcal{A})$ — очевидно
  - $w \in L(\mathcal{A}_1)a(L(\mathcal{A}_2)a)^*L(\mathcal{A}_3)$ $\Rightarrow$ $w = w_0 a w_1 \ldots a w_n$ как на рисунке $\Rightarrow$ $w \in L(\mathcal{A})$ $\square$

11)Теорема о полноте

Метод резолюций:

- формулы, которыми оперирует метод — это клозы (элементарные дизъюнкции)
- клоз рассматривается как множество литералов
  - порядок литералов не важен, повторяющиеся литералы стираются
- единственное правило вывода — правило резолюций:
  - если есть клозы вида $x \vee C$ и $\bar{x} \vee D$ (x — переменная), дописать клоз $C \vee D$
  - ⋆ клоз, содержащий пару литералов $\{y, \bar{y}\}$, не дописывается
  - если C и D — пустые множества литералов, дописывается пустой клоз $\square$
- аксиом нет
- условия — все клозы КНФ, поданной на вход метода
- цель — получить пустой клоз

Теорема о полноте

Теорема о полноте метода резолюций

КНФ $F = C_1 \wedge \cdots \wedge C_k$ является противоречием $\Leftrightarrow$ существует доказательство методом резолюций с условиями $C_1, \ldots, C_k$ и заключением $\square$.

Доказательство достаточности:

- рассмотрим доказательство методом резолюций с заключением $\square$
- каждая формула является либо условием, либо получено по правилу резолюций из каких-то предыдущих формул
  - а значит, является следствием конъюнкции этих формул согласно лемме
- отношение «быть следствием» транзитивно
- любая формула вида $C_{i_1} \wedge \cdots \wedge C_{i_j}$ является следствием F

$\Rightarrow$ любая формула в доказательстве является следствием F

⋆ пустой клоз является следствием формулы $x \wedge \bar{x}$, а значит, задает константу 0

$\Rightarrow$ 0 — следствие $F \Rightarrow F$ — противоречие $\square$

Комментарий:

⋆ мы доказали корректность метода: если существует доказательство, содержащее пустой клоз, то заданная КНФ действительно является противоречием

⋆ обратная импликация доказывает полноту метода: если КНФ — противоречие, то это можно доказать методом резолюций

Доказательство необходимости

- Проведем индукцию по числу n переменных в F
- База индукции: $n = 1$
  - F — противоречие $\Rightarrow$ F содержит клозы x и $\bar{x}$
  - $\Rightarrow$ по правилу резолюций из x и $\bar{x}$ выводится пустой клоз
- Шаг индукции:
  - пусть $F = F(x_1, \ldots, x_n)$, $S = \{C_1, \ldots, C_k\}$
  - считаем, что клоз не может содержать одновременно x_i и $\bar{x}_i$
    - если такой клоз есть, он задает константу 1 и может быть удален из F
  - построим два множества клозов, S^+ и S^-:
  - $S^+ = \{C \in S \mid \text{ в } C \text{ нет переменной } x_n\} \cup \{C \mid (C \vee x_n) \in S\}$
  - $S^- = \{C \in S \mid \text{ в } C \text{ нет переменной } x_n\} \cup \{C \mid (C \vee \bar{x}_n) \in S\}$
  - ⋆ докажем, что КНФ $F^+ = \bigwedge_{C \in S^+} C$ является противоречием:
  - пусть существует набор значений $b_1, \ldots, b_{n-1}$ такой, что $F^+_{|b_1,\ldots,b_{n-1}} = 1$
  - рассмотрим значения всех клозов из множества S на наборе $b_1, \ldots, b_{n-1}, 0$:
    - если клоз C не содержит переменную x_n, то $C_{|b_1,\ldots,b_{n-1},0} = C_{|b_1,\ldots,b_{n-1}} = 1$
    - если клоз имеет вид $C \vee x_n$, то $(C \vee x_n)_{|b_1,\ldots,b_{n-1},0} = C_{|b_1,\ldots,b_{n-1}} = 1$
    - клоз вида $C \vee \bar{x}_n$ превращается в 1 за счет значения $b_n = 0$
  - $\Rightarrow$ $F_{|b_1,\ldots,b_{n-1},0} = 1$, что невозможно, так как F — противоречие
  - ⋆ аналогично, $F^- = \bigwedge_{C \in S^-} C$ является противоречием
    - к гипотетическому набору, выполняющему F^-, надо добавить $b_n = 1$
  - ⋆ по предположению индукции, из каждого из множеств S^+, S^- можно вывести пустой клоз

$\Longrightarrow$

Шаг индукции — окончание

- Рассмотрим вывод пустого клоза из множества S^+
  - если в выводе участвовали только клозы из S, то из S выводим пустой клоз
  - пусть в выводе участвовал хотя бы один клоз $C \in S^+ \setminus S$; тогда $(C \vee x_n) \in S$
  - $\Rightarrow$ построим вывод из S, заменив в выводе из S^+ каждый клоз из $S^+ \setminus S$ на соответствующий клоз из S
  - $\Rightarrow$ во всех следствиях из таких клозов добавится литерал x_n
  - $\Rightarrow$ из S выводится клоз x_n
- ⋆ аналогично, из вывода пустого клоза из S^- получим вывод клоза $\bar{x}_n$ из S
  - $\Rightarrow$ из клозов x_n и $\bar{x}_n$ получим пустой клоз $\square$

Комментарий:

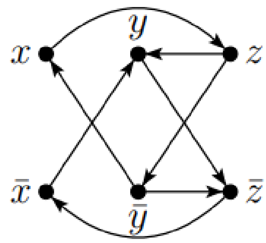
- ⋆ искать доказательства методом резолюций может компьютер
  - существуют различные стратегии оптимизации поиска вывода
- ⋆ на более общем варианте метода резолюций (для формул логики первого порядка) основан язык Пролог

12)Решение 2-SAT

2-выполнимость

- КНФ, в которой каждый клоз состоит из двух литералов, называется 2-КНФ
- ⋆ Задача SAT с 2-КНФ называется 2-выполнимость (2-SAT)
- ★ Формула $l_1 \vee l_2$, где l_1 и l_2 — литералы, эквивалентна $\bar{l}_1 \to l_2$ и $\bar{l}_2 \to l_1$
- Пусть дана 2-КНФ F; построим по ней орграф $G(F)$ (граф импликаций):
  - вершины — литералы из F
  - каждому клозу $l_1 \vee l_2$ сопоставлены ребра $(\bar{l}_1, l_2)$ и $(\bar{l}_2, l_1)$
- Эквивалентная формулировка 2-SAT на языке графа импликаций:
  - ★ существует ли раскраска ϕ графа импликаций в цвета $\{0, 1\}$ такая, что
    - (i) $\phi(l) \neq \phi(\bar{l})$ для любой вершины l и
    - (ii) $\phi(l_2) \geqslant \phi(l_1)$ для любого ребра (l_1, l_2)?
  - ϕ с указанными свойствами будем называть булевой раскраской
  - ◇ по транзитивности, если l_2 достижима из l_1, то $\phi(l_2) \geqslant \phi(l_1)$

Пример: $F = (x \vee y) \wedge (\bar{y} \vee \bar{z}) \wedge (\bar{x} \vee z) \wedge (\bar{z} \vee y)$



граф импликаций $G(F)$:

Лемма

Существует булева раскраска орграфа $G(F) \Leftrightarrow$ не существует переменной x, для которой вершины x и $\bar{x}$ взаимно достижимы в $G(F)$.

- Доказательство необходимости:
  - существование такой переменной x влечет $\phi(x) = \phi(\bar{x})$ согласно ($\diamond$), что нарушает первое условие для булевой раскраски $\square$
- Доказательство достаточности:
  - разобьем $G(F)$ на компоненты сильной связности
  - отношение достижимости компонент — отношение порядка, дополним его до линейного порядка $\leqslant$
    - т.е. выполним топологическую сортировку компонент
  - по условию, вершины x и $\bar{x}$ лежат в разных компонентах для любой переменной x

  $\Rightarrow$ положим $\phi(x) = 1$ ($\phi(x) = 0$), если $\mathrm{comp}(x) > \mathrm{comp}(\bar{x})$ ($\mathrm{comp}(x) < \mathrm{comp}(\bar{x})$)
    - все вершины любой компоненты имеют один цвет

  $\Rightarrow$ $\phi(x) \neq \phi(\bar{x})$ для всех x, условие (i) выполнено
  - пусть существует ребро (l_1, l_2) такое, что $\phi(l_1) = 1, \phi(l_2) = 0$

  $\Rightarrow$ существует ребро $(\bar{l}_2, \bar{l}_1)$, $\phi(\bar{l}_2) = 1, \phi(\bar{l}_1) = 0$

  $\Rightarrow$ $\mathrm{comp}(l_1) < \mathrm{comp}(l_2)$ и $\mathrm{comp}(\bar{l}_2) < \mathrm{comp}(\bar{l}_1)$
  - из нашего определения ϕ следует $\mathrm{comp}(\bar{l}_1) < \mathrm{comp}(l_1)$ и $\mathrm{comp}(l_2) < \mathrm{comp}(\bar{l}_2)$

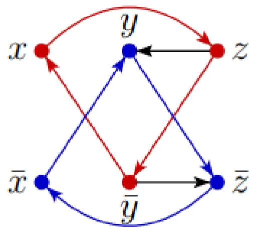
  $\Rightarrow$ противоречие с тем, что $\leqslant$ — порядок

  $\Rightarrow$ $\phi(l_2) \geqslant \phi(l_1)$ для любого ребра (l_1, l_2), условие (ii) выполнено $\square$

2-выполнимость (3)

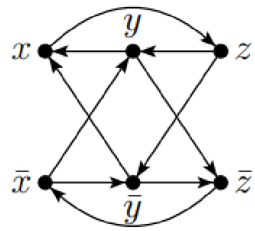
Примеры:

$F = (x \vee y) \wedge (\bar{y} \vee \bar{z}) \wedge (\bar{x} \vee z) \wedge (\bar{z} \vee y)$ выполнима:



В графе $G(F)$ две компоненты,
красные вершины красим в 0, синие — в 1

$F' = F \wedge (x \vee \bar{y})$ невыполнима:



В графе $G(F')$ единственная компонента,
ее нельзя раскрасить

Теорема

Задача 2-SAT может быть решена за время $O(\ell)$, где ℓ — число клозов в формуле.

- Доказательство:
  - построим по формуле F граф $G(F)$, в нем 2ℓ ребер
  - найдем компоненты сильной связности и отсортируем их топологически
    - например, и алгоритм Косараю, и алгоритм Тарьяна ищут компоненты за линейное от числа ребер время и выдают их в топологически отсортированном виде
  - если $\text{comp}(x) = \text{comp}(\bar{x})$ для какой-нибудь вершины x, возвращаем 0
  - иначе выполняем булеву раскраску $G(F)$ и возвращаем полученные значения
  - все шаги требуют времени $O(\ell)$ □