Конспект лекций по курсу

ЛОГИЧЕСКИЕ И КОМБИНАТОРНЫЕ МЕТОДЫ АНАЛИЗА ДАННЫХ

группа 517 (1-й год магистратуры)
2019/20 уч. год

Лектор *С. И. Гуров*

2020

Оглавление

Глава 1

Информационный подход в распознавании образов

1.1 Информация по Хартли

Определение 1.1 (информация по Хартли[1]). Если Ω — конечное множество, то *информация* $I(\omega)$ *его элемента* $\omega \in \Omega$ есть величина

$$I(\omega) = \log \left|\Omega\right|.$$

Здесь и далее все логарифмы — по основанию 2 $\Rightarrow$ информация измеряется в *битах*. Ясно, что $\lceil I(\omega) \rceil$ есть число бит, необходимое для указания номера элемента ω в пронумерованном 1, 2, ... множестве Ω.

Если на Ω задано отношение эквивалентности $\sim$, то *информация* $I_\sim(\omega)$ *элемента* ω *по эквивалентности* ω есть

$$I_\sim(\omega) = \log \left|[\omega]_\sim\right|$$

Ясно, что у всех элементов, входящих в один класс эквивалентности информация по данной эквивалентности одинакова.

[1] Ральф Хартли (Ralph Vinton Lyon Hartley, 1888–1970) — американский исследователь области электроники; ввёл в 1928 г. логарифмическую меру информации, которая называется *хартлиевской*.

Утверждение 1.2. *Если* $N = |\Omega/\sim|$ *— число классов эквивалентности, то*

$$\sum_{\omega\in\Omega} 2^{-(I_\sim(\omega)+\log N)} = 1.$$

Доказательство. Пусть $\Omega/\sim = \{ W_1, \ldots, W_N \}$ и i-й класс эквивалентности описывается как $W_i = [\omega]_\sim$ для некоторого своего элемента ω. Тогда, переходя от суммирование по элементам к суммированию по классам эквивалентности и с учётом, $2^{-\log N} = 1/N$), получим

$$\sum_{\omega\in\Omega} 2^{-(I_\sim(\omega)+\log N)} = \frac{1}{N}\sum_{i=1}^{N} \big|W_i\big| \cdot 2^{-\log|W_i|} = \\ = \frac{1}{N}\sum_{i=1}^{N} 1 = 1.$$

□

Неравномерные коды. Пусть

- X — конечный алфавит, состоящий из $|X| = q$ произвольных букв;
- X^n — множество всех слов длины $n \geqslant 1$ над X, или *сообщений*;
- $\{0,1\}^+$ — множество всех конечных двоичных слов, *исключая* пустое; они будут являться *кодовыми словами.*

Для однозначности восстановления сообщений при приёме используют:

- кодовые слова одинаковой длины;

- разделитель между кодовыми словами;
- префексные коды.

Определение 1.3. *Неравномерным бинарным кодом* называют образ C инъективного отображения

$$\psi : X^n \to \{0,1\}^+, \quad \operatorname{Im}\psi = C,$$

определённого для каждого $n = 1, 2, \ldots$.

Образ $\psi(x)$ сообщения x называют *кодовым словом*.

Неравномерный код называется *префексным* или *дешифрируемым*, если $\psi(x)$ не является началом никакого слова $\psi(x')$ для всех $x' \neq x$.

Слова префексного кода можно записывать в строку непрерывно, поскольку данная строка однозначно разлагается на составляющие её кодовые слова.

Длину кодового слова $\psi(x)$ обозначим $l(x)$.

Утверждение 1.4 (неравенство Крафта, критерий существования существования префиксных кодов). *Для существования префиксного кода C необходимо и достаточно, чтобы*

$$\sum_{x \in C} 2^{-\ell(x)} \leqslant 1.$$

Пример 1.5. Для кода

$$C = \{\, C_1 = 01,\, C_2 = 10,\, C_3 = 110,\, C_4 = 001 \,\}$$

имеем $|C| = 4$, $\ell_1 = \ell_2 = 2$, $\ell_3 = \ell_4 = 3$ и

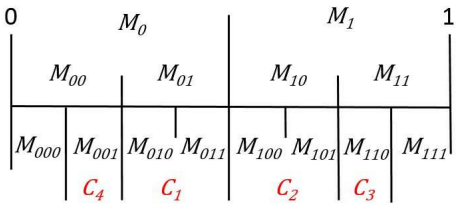
$$2 \cdot \frac{1}{4} + 2 \cdot \frac{1}{8} = \frac{6}{8} = \frac{3}{4} < 1.$$

Доказательство. Рассмотрим код C с длинами слов $\ell_1, \ldots, \ell_N$ и отрезок $[0,1]$ на числовой прямой. Далее

1) разделим его пополам, левую половину обозначим M_0, а правую — M_1;
2) поделим M_0 пополам и обозначим его левую половину M_{00}, а правую M_{01}; проделав то же самое с M_1, получим M_{10}, а левую M_{11};
3) и т. д., пока длина индекса j полученного отрезка M_j не станет равна $\max\{\ell_1, \ldots, \ell_N\}$;
4) сопоставим отрезок M_i кодовому слову $i \in C$; ясно, что длина отрезка M_i равна $2^{-\ell_i}$.

Ясно, что если код префиксный, то никакие два отрезка не пересекаются, а сумма длин отрезков не превзойдет 1. □

Пример 1.6. В нашем примере



Код Шеннона–Фано. Рассмотрим задачу оптимального (с минимизацией длин кодовых слов) кодирования сообщений над q-буквенным алфавитом.

Пусть вероятности появления букв в словах известны и упорядочены по убыванию: $p_1 \geqslant \ldots \geqslant p_q$.

Уложим на прямой без пропусков неперекрывающиеся отрезки длин $p_1, \ldots, p_q$ и обозначим i-й из полученных отрезков через S_i, а их объединение — через S.

Коды тех букв a_i, для которых отрезок S_i попал на левую половину отрезка S, будут начинаться на 0, а коды тех букв, для отрезок S_i попал на правую половину отрезка S, будут начинаться на 1.

Один из отрезков (центральный) может не попасть целиком ни на левую, ни на правую половину. С ним поступим так. Если этот отрезок первый или последний, то начнём его код с, соответственно, 0 или 1. Иначе отнесём его куда угодно.

Далее применяем данное правило к незакодированным ещё буквам, код которых начинается на 0, и к буквам, код которых начинается на 1, приписывая к к строящимся кодам 0 либо 1, пока не будут закодированы все буквы.

Полученный код называют кодом Шеннона-Фано. Легко видеть, что он является префиксным.

Можно показать, что средняя длина кодового слова $\sum p_i l_i$ может превосходить *шенноновскую энтропию* $H = \sum p_i(-\log p_i)$ менее, чем на 1.

1.2 Действие группы на множестве

Действие группы на множестве: два определения. Все конечные группы — конечнопорождённые, то есть обладающие конечным числом *образующих*.

Обозначения для конечнопорождённых групп: $\langle S \mid R \rangle$, где S — множество образующих, R — совокупность соотношений для образующих. Пример: $\langle a \mid a^n \rangle$ — циклическая группа порядка n. $|S|$ — *ранг группы*.

Пусть заданы

- Конечная группа $\langle G, \circ, e \rangle$, $|G| = n$.
- Конечное множество Ω, $|\Omega| = N$.
- $Bij(\Omega)$ — множество всех биекций на Ω.
- $S(\Omega) \cong S_N$ — *симметрическая группа* множества Ω — множество всех подстановок элементов $\omega_1, \ldots, \omega_N$ группы:

$$S(\Omega) = \langle Bij(\Omega), *, 1_\Omega \rangle = \langle \sigma_1, \ldots, \sigma_{N-1} \mid \sigma_i^2, (\sigma_i\sigma_{i+1})^3, \sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } |i-j| > 1 \rangle,$$

где $*$ — символ суперпозиции подстановок,
1_Ω — единичная подстановка,
σ_i — транспозиция, меняющая местами i-й элемент множества Ω с $i+1$-м.

Будут даны два определения для действия группы G на множестве Ω. *Обозначение*: $G \underset{\alpha}{:} \Omega$ или, при фиксированных G и Ω — просто α.

Определение 1.7 (I). $\alpha \in \mathrm{Hom}\,(G, S(\Omega))$.

Например, всегда имеется *тривиальное действие* $\forall\, g \in G : \alpha(g) = 1_\Omega$, порождённое тривиальным гомоморфизмом $G \to 1_\Omega$.

Если $C(G) = 1$ (любой элемент Ω может быть переведён в любой), то действие $G \underset{\alpha}{:} \Omega$ называют *транзитивным*.

Действие α группы G на множестве Ω называют *эффективным*, если

$$\forall\, g, h \in G\ \exists\, \omega \in \Omega :\ g(\omega) \neq h(\omega).$$

Будем далее рассматривать лишь эффективные действия групп на множествах.

Определение 1.8 (II). $\alpha = \langle\, G,\, \Omega;\, \circ,\, \diamond,\, e\,\rangle$ — *двухосновная алгебра*, где *редукт* $\langle\, G,\, \circ,\, e\,\rangle$ есть группа, а $G \times \Omega \xrightarrow{\diamond} \Omega$ — бинарная операция, записываемая как $g(\omega)$, причём данные операции удовлетворяет аксиомам

$$1)\ \ e(\omega) = \omega; \qquad 2)\ \ (g \circ h)(\omega) = h(g(\omega)).$$

Элементы g группы G порождают перестановки на Ω. Часто вместо «*элемент g (группы G)*» будем говорить «*перестановка (элемента Ω)*».

При записи $g(\omega)$ естественно определяется операция $g^k(\omega)$ для $k \in \mathbb{Z}$:

$$g^0 = e \ \text{ и если } g(\omega') = \omega, \ \text{то } g^{-1}(\omega) = \omega'.$$

Зафиксируем перестановку $g \in G$ и введём отношение эквивалентности $\sim_g$ на Ω —

$$\omega \sim_g \omega' \ \triangleq\ \underset{\mathbb{Z}}{\exists}\, k\ :\, g^k(\omega) = \omega'.$$

Рефлексивность (R), симметричность (S) и транзитивность (T) отношения $\sim_g$ легко показываются.

Классы эквивалентности $\sim_g$ называются *g-циклами.*

Действительно, легко видеть, что элементы этих классов образуют циклы:

$\omega \xrightarrow{g} \omega' \xrightarrow{g} \ldots \xrightarrow{g} \omega$, *и у каждого элемента — по единственной входящей и исходящей стрелке.*

Обозначения:

- $C(g)$ — число g-циклов (смежных классов по эквивалентности $\sim_g$).
- $\nu_1, \nu_2, \ldots, \nu_N$ — количества циклов длины $1, 2, \ldots, N$.
  Понятно, что $\sum\limits_{k=1}^{N} \nu_k = C$ и $\sum\limits_{k=1}^{N} k \cdot \nu_k = N$.
- $\langle \nu_1, \nu_2, \ldots, \nu_N \rangle = Type(g)$ — *тип перестановки* g, упорядоченная совокупность количеств циклов.

Например, если

$$\Omega = \{1, \ldots, 10\} \text{ и } g = (1,9,3)(2,6)(4,8,10),$$
$$\text{то } Type(g) = \langle 2, 1, 2, 0, \ldots, 0 \rangle.$$

Введём отношение эквивалентности $\sim_G$ на Ω по всей группе G —

$$\omega \sim_G \omega' \triangleq \exists\limits_{G} g : g(\omega) = \omega'.$$

Свойства (R), (S) и (T) отношения $\sim_G$ очевидны.

Классы эквивалентности по $\sim_G$ называют *орбитами.*

Обозначения:

- Класс эквивалентности, в которую попадает элемент ω обозначаем $\mathrm{Orb}\,(\omega)$ $(= [\omega]_{\sim_G})$.
- Число получившихся орбит — $C(G)$.

Фиксатор перестановки и стабилизатор элемента множества. Рассмотрим равенство

$$g(\omega) \;=\; \omega.$$

При выяснении, когда оно выполняется, будем полагать неизменным либо g, либо ω.

1. g — const, то есть находим все элементы множества Ω, которые перестановка g оставляет на месте — это *фиксатор перестановки* $g \in G$:

$$\big\{\, \omega \in \Omega \mid g(\omega) \;=\; \omega \,\big\} \;=\; \mathrm{Fix}\,(g) \;\subseteq\; \Omega.$$

2. ω — const, то есть находим все перестановки g, которые оставляют данный элемент неподвижным — это *стабилизатор элемента* $\omega \in \Omega$:

$$\big\{\, g \in G \mid g(\omega) \;=\; \omega \,\big\} \;=\; \mathrm{Stab}\,(\omega) \;\subseteq\; G.$$

Легко показать, что *стабилизатор есть подгруппа группы* G, то есть справедливо

Утверждение 1.9. $\mathrm{Stab}\,(\omega) \;\leqslant\; G.$

Доказательство. Нужно удостоверится, что для любых элементов $g,\, h \in \mathrm{Stab}\,(\omega)$ их суперпозиция $g \circ h^{-1}$ также принадлежит $\mathrm{Stab}\,(\omega)$.

Но это действительно так, поскольку и g, и h, и h^{-1} не переводят ω в какой-либо другой элемент. Следовательно $(g \circ h^{-1})(\omega) = \omega$. □

Поэтому стабилизатор $\mathrm{Stab}\,(\omega)$ называют ещё *стационарной* (или *изотопической*) *подгруппой элемента* ω. $\mathrm{Stab}\,(\omega)$ будем также обозначать G_ω.

Утверждение 1.10. *Длина орбиты* $\mathrm{Orb}\,(\omega)$ *равна индексу стационарной подгруппы* G_ω *группы* G*:*

$$\big|\,\mathrm{Orb}\,(\omega)\big| \;=\; \big[G : G_\omega\big] \;=\; \frac{\big|G\big|}{\big|G_\omega\big|}.$$

Доказательство. Ясно, что

$$\begin{aligned}\mathrm{Orb}\,(\omega) \;&=\; \{\; g(\omega) \mid g \in G \;\} \;= \\ &= \{\; (h \circ g)(\omega) \mid g \in G,\, h \in G_\omega \;\}\,.\end{aligned}$$

Таким образом, между множеством $\{G_\omega g\}$, $g \in G$ правых смежных классов G по стационарной подгруппе G_ω элемента $\omega \in \Omega$ и его орбитой $\mathrm{Orb}\,(\omega)$ существует взаимно однозначное соответствие. Применяя далее теорему Лагранжа, получим

$$\big|\,\mathrm{Orb}\,(\omega)\big| \;=\; \big|\,\{G_\omega g\}\,\big| \;=\; \big[\,G : G_\omega,\big]. \qquad \square$$

1.3 Измерение информации слов

Орбита и композиция слова. Далее будем рассматривать множество $\Omega = X^n$ всех слов длины $n \geqslant 1$

в конечном алфавите X и действие на нём симметрической группы S_n, переставляющей всеми возможными способами буквы внутри слова.

Ясно, что если в слове $x \in X^n$ все буквы разные, то при действии $S_n \underset{\alpha}{:} X^n$ все перестановки породят разные слова и $\big|\operatorname{Orb}(x)\big| = n!$. Если же x содержит одинаковые буквы, то результаты действия на x разных перестановок из S_n могут совпадать.

Композицией слова $x \in X^n$, состоящего из q различных букв, назовём кортеж

$$(m_1, \ldots, m_q),$$

где m_i — число вхождений буквы a_i в слово x, $i = \overline{1,q}$.

Перестановка букв в слове не меняет количеств их вхождений, отсюда все слова одной орбиты имеют одну и ту же композицию.

Ясно также, что для слова $x \in X^n$ с композицией $(m_1, \ldots, m_q)$ стационарная подгруппа G_x изоморфна прямому произведению симметрических групп:

$$G_x \cong S_{m_1} \times \ldots \times S_{m_q}.$$

Пример 1.11. Пусть $X = \{a, b\}$, $n = 5$.

Рассмотрим действие $S_5 \underset{\alpha}{:} X^5$ симметрической группы S_5 всех $5! = 120$ перестановок букв на 5-буквенные слова над X. Пусть $x = ababb$. Определим величину и состав орбиты $\operatorname{Orb}(x)$.

$$\big|\operatorname{Orb}(x)\big| = \big[\, S_5 : \operatorname{Stab}(x) \,\big] = \frac{|S_5|}{\big|\operatorname{Stab}(x)\big|},$$

$$\operatorname{Stab}(x) \cong S_2 \times S_3 \;\Rightarrow\; \big|\operatorname{Stab}(x)\big| = 2 \cdot 6 = 12 \;\Rightarrow$$

$$\Rightarrow \ \big|\ \mathrm{Orb}\,(x)\ \big| \ = \ \frac{5!}{2!\cdot 3!} \ = \ \frac{120}{12} \ = \ 10.$$

Пусть $x = ababb$, его композиция — $(2,3)$. Выпишем все слова-элементы орбиты $\mathrm{Orb}\,(ababb)$:

$aabbb$	$ababb$	$abbab$	$abbba$	$baabb$
$babab$	$babba$	$bbaab$	$bbaba$	$bbbaa$

Безусловная и условная информация слов

Определение 1.12. *Безусловной 0-информацией* $I_0(x)$ слова $x \in X^n$, состоящего из q различных букв, называется величина

$$I_0(x) = \log \big|\ \mathrm{Orb}\,(x)\big| = \log \frac{n!}{m_1!\cdot \ldots \cdot m_q!},$$

где $\mathrm{Orb}\,(x)$ — орбита слова x при действии $S_n \underset{\alpha}{:} X^n$.

Пример 1.13. Пусть $X = \{\ a, b, c, d\ \}$, $n = 4$.

$I_0(aaaa) \ = \ \log \dfrac{4!}{4!} \ = \ 0$ — ясно, что минимально возможное значение 0-информации есть 0, оно достигается на словах, состоящих из одной повторяющейся буквы;

$I_0(abaa) \ = \ \log \dfrac{4!}{3!\cdot 1!} \ = \ 2;$

$I_0(abab) \ = \ \log \dfrac{4!}{2!\cdot 2!} \ = \ \log 6;$

$I_0(abcd) \ = \ \log \dfrac{4!}{1!\cdot \ldots \cdot 1!} \ = \ \log 24$ — ясно, что максимально возможное значение 0-информации

слова из X^n есть $\log n!$, оно достигается на словах, состоящих из всех различных букв.

Вместе со словами вида

$$x = x_1 \dots x_n \in X^n$$

будем рассматривать алфавит Y и слова

$$y = y_1 \dots y_n \in Y^n.$$

При этом не исключено $X = Y$.

Группа S_n, действуя на X^n (переставляя позиции букв), действует и на Y^n.

Рассмотрим стационарную подгруппу $G_y \leqslant S_n$ слова $y \in Y^n$ — все перестановки букв, сохраняющие слово y. Под её действием слова из X^n разбиваются на орбиты, которые называют *условными*.

Определение 1.14. *Условной информацией* слова $x \in X^n$ относительно слова $y \in Y^n$ назовём величину

$$I_0(x/y) = \log \big[\, G_y : G_x \cap G_y \,\big].$$

Пример 1.15. Пусть $X = \{\, a, b \,\}$, $Y = \{\, 0, 1 \,\}$.

1. $n = 3,\ x = aab,\ y = 111$:

$$I_0(x) = \log \frac{3!}{2! \cdot 1!} = \log 3, \quad I_0(y) = \log \frac{3!}{3!} = 0,$$
$$G_x = \{\, e, (12) \,\},\ G_y = S_3,\ |S_3| = 6,\ G_x \cap G_y = G_x,$$
$$I_0(x/y) = \log 6/2 = \log 3, \quad I_0(y/x) = \log 2/2 = 0.$$

2. $n = 5,\ x = aabab,\ y = 11000$:

$$I_0(x) = I_0(y) = \log \frac{5!}{2! \cdot 3!} = \log 10$$

(x и y — слова с одинаковой композицией),

$$G_x = \{\, e,\ (124),\ (142),\ (12),\ (24),\ (14),\ (35),\ \dots \,\} \cong$$

$$\cong S_2 \times S_3 \ \Rightarrow\ \big|G_x\big| = 2! \cdot 3! = 12,$$

$$G_y = \{\, e,\ (12),\ (345),\ (354),\ (34),\ (45),\ (35),\ \dots \,\} \cong$$

$$\cong S_2 \times S_3 \ \Rightarrow\ \big|G_y\big| = 12,$$

$$G_x \cap G_y = \{\, e,\ (12),\ (35),\ (12)(35) \,\},\ \big|G_x \cap G_y\big| = 4,$$

$$I_0(x/y) = I_0(y/x) = \log 12/4 = \log 3.$$

Очевидно, $I_0(x/x) = 0$ и более того: справедливо

Утверждение 1.16. $\qquad I_0(x/y) = 0 \ \Leftrightarrow\ G_y \subseteq G_x.$

Доказательство.

$$I_0(x/y) = \log \big[G_y : G_x \cap G_y\big] = \log \frac{\big|G_y\big|}{\big|G_x \cap G_y\big|} = 0 \ \Leftrightarrow$$

$$\Leftrightarrow\ \big|G_y\big| = \big|G_x \cap G_y\big| \ \Leftrightarrow\ G_y \subseteq G_x.$$

□

Определение 1.17. Слова $x \in X^n$ и $y \in Y^n$ такие, что $I_0(y/x) = I_0(x/y) = 0$ называют *эквивалентными*.

Ясно, что если слова x и y эквивалентны, то $G_x = G_y$, то есть x переходит в y при некоторой биекции между буквами алфавитов X и Y.

Произведение слов. Неравенства для количеств информации. Пусть

$$x = x_1 \dots x_n \in X^n \text{ и } y = y_1 \dots y_n \in Y^n,$$

тогда *произведение* (в данном порядке) *слов* x *и* y есть слово

$$z = x \times y = x_1 y_1 \dots x_n, y_n$$

в алфавите $Z = X \times Y$.

Утверждение 1.18.

$$I_0(x \times y) = I_0(x) + I_0(y/x) = \\ = I_0(y) + I_0(x/y) = I_0(y \times x).$$

Доказательство. Пусть F, H и G — такие конечные группы, что $F \leqslant H \leqslant G$. Ясно, что

$$\frac{|G|}{|F|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|F|}.$$

По теореме Лагранжа это равенство эквивалентно

$$[G : F] = [G : H] \cdot [H : F].$$

Поскольку

$$G_{x \times y} = G_x \cap G_y \text{ и } G_{x \times y} \leqslant G_x \leqslant G,\ G_{x \times y} \leqslant G_y \leqslant G,$$

подставляем в указанное равенство

$$F = G_x \cap G_y, \text{ последовательно } H = G_x \text{ и } H = G_y,$$

и переходя к логарифмам — получаем требуемое. □

Утверждение 1.19.

$$1)\ I_0(x/y) \leqslant I_0(x), \qquad 2)\ I_0(x \times y) \leqslant I_0(x) + I_0(y).$$

Доказательство. Переходя к орбитам замечаем, что орбита элемента x под действием стационарной подгруппы G_y есть его подорбита под действием всей группы G.

Второе неравенство следствие первого и равенства для $I_0(x \times y)$. □

Взаимная информация слов

Определение 1.20. *Взаимной информацией n-слов x и y* назовём величину

$$I_0(x : y) = I_0(x) + I_0(y) - I_0(x \times y) = \\ = I_0(x) - I_0(x/y) = I_0(y) - I_0(y/x) = I_0(y : x).$$

При $I_0(x : y) = 0$ слова x и y назовём *независимыми.*

Интуитивно $I_0(x : y)$ есть количество информации, содержащейся в векторе x относительно вектора y и наоборот.

Из *Утверждения* 1.19 следует, что $I_0(x : y) \geqslant 0$, а если слова независимы, то

$$I_0(x) = I_0(x/y) \text{ и } I_0(y) = I_0(y/x).$$

Пример 1.21. Рассмотрим слова из *Примера* 1.15.

1. $n = 3$, $x = aab$, $y = 111$

$I_0(x) = \log 3$, $I_0(y) = 0$, $I_0(x/y) = \log 3$, $I_0(y/x) = 0$,
$I_0(x : y) = I_0(x) - I_0(x/y) = \log 3 - \log 3 = 0$,
$I_0(y : x) = I_0(y) - I_0(y/x) = 0 - 0 = 0$,

то есть слова x и y независимы.

2. $\underline{n = 5,\ x = aabab,\ y = 11000}$

$$I_0(x) = I_0(y) = \log 10,\quad I_0(x/y) = I_0(y/x) = \log 3.$$
$$I_0(x : y) = I_0(y : x) = I_0(x) - I_0(x/y) =$$
$$= \log 10 - \log 3 = \log (10/3).$$

и слова x и y не являются независимыми.

Пример 1.22. Рассмотрим слова $x \in X^n$ и $y \in Y^n$, состоящие из q и k букв и с композициями $(m_1, \ldots, m_q)$ и $(n_1, \ldots, n_k)$ соответственно.

Составим $q \times k$ таблицу

$$M_{q\times k} = \| m_{ij} \|,$$

где m_{ij} — число замен i-го символа слова x на j-й символ слова y.

В таблице M суммы элементов строкам будут равняться $m_1, \ldots, m_q$, а по столбцам — $n_1, \ldots, n_k$.

Тогда, как можно показать:

$$I_0(y/x) = \log \frac{m_1!}{m_{11}! \ldots m_{1k}!} + \log \frac{m_2!}{m_{21}! \ldots m_{2k}!} + \ldots$$
$$\ldots + \log \frac{m_q!}{m_{q1}! \ldots m_{qk}!}.$$

Пусть для примера $X = \{a, b, c\}$, $Y = \{1, 2, 3\}$, $n = 9$ и

$x =$	a	b	a	a	c	b	c	a
$y =$	1	2	2	1	3	2	1	3

Композиции слов: $x - (4, 2, 2)$, $y - (3, 3, 2)$.

Таблица замен букв:

$$M = \begin{array}{|c|ccc|c|} \hline x \diagdown y & 1 & 2 & 3 & \# \\ \hline a & 2 & 1 & 1 & 4 \\ b & & 2 & & 2 \\ c & 1 & & 1 & 2 \\ \hline \# & 3 & 3 & 2 & 8 \\ \hline \end{array}$$

Тогда

$$I_0(y/x) = \log \frac{4!}{2!\,1!\,1!} + \log \frac{2!}{2!} + \log \frac{2!}{1!\,1!} = \\ = \log 12 + 0 + \log 2 = \log 24.$$

Производя аналогичные вычисления по столбцам, получим

$$I_0(x/y) = \log \frac{3!}{2!\,1!} + \log \frac{3!}{2!\,1!} + \log \frac{2!}{1!\,1!} = \\ = 2\log 3 + \log 2 = \log 18.$$

Для безусловной информации I_0 получим значения

$$I_0(x) = \log \frac{8!}{4!\,2!\,2!} = \log 420,$$
$$I_0(y) = \log \frac{8!}{3!\,3!\,2!} = \log 560.$$

Взаимная информация:

$$I_0(x:y) = I_0(x) - I_0(x/y) = \log \frac{420}{18} = \log \frac{70}{3}, \\ = I_0(y) - I_0(y/x) = \log \frac{560}{24} = \log \frac{70}{3}.$$

Группировка значений. Если на алфавите X задана эквивалентность $\sim$, то буквы из одного смежного класса отождествляются.

Утверждение 1.23. *В результате отождествления некоторых букв алфавита информация слова уменьшается: если x и x' — исходное и новое слова, то*

$$I_0(x') = I_0(x) - I_0(x/x').$$

Пример 1.24. Пусть в слове

$$x = a\ b\ a\ a\ c\ b\ c\ a$$

буквы b и c отождествляются. Тогда

$$x' = a\ b\ a\ a\ b\ b\ b\ a,$$

а при вычислении $I_0(x/x')$ можно ограничиться таблицей отождествляемых букв

$$M = \begin{array}{c|cc|c} & b & c & \\ \hline b & 2 & 2 & 4 \end{array}$$

Отсюда

$$I_0(x/x') = \log \frac{4!}{2! \cdot 2!} = \log 6, \quad I_0(x) = \log 420,$$

$$I_0(x') = I_0(x) - I_0(x/x') = \log \frac{420}{6} = \log 70.$$

Прямой подсчёт: $I_0(x') = \log \dfrac{8!}{4! \cdot 4!} = \log 70.$

Пусть в результате наблюдений получена последовательность данных — вектор x, который требуется закодировать *бинарным словом*. Потребуем, чтобы новое слово x' содержало как можно больше информации об исходном слове, то есть чтобы значение $I_0(x')$ было максимальным. Это достигается при равенстве, возможно приблизительном, количеств 0 и 1 в x'.

В результате приходим к *квантильному квантованию по вариационному ряду*: упорядочиваем значения x по возрастанию и кодируем значением 0 первую половину отсортированных данных, а значением 1 — вторую.

Пусть, например, в результате наблюдений получены данные

$$x = 0{,}16;\ 0{,}1;\ 0{,}7;\ 0{,}1;\ 0{,}18;\ 1{,}15,$$

которые требуется закодировать *бинарными* словами. Для этого составляем вариационный ряд и кодируем первые 3 по порядку значения (ниже порога 0,17) нулём, а последние 3 — единицей.

При кодировании *двухбитными* словами 00, 01, 10 и 11 — разбиваем вариационный ряд на 4 приблизительно равных интервала и т. д.

1.4 Методы теории информации в задачах распознавания

Вычисление информативности признака. Прецедентная информация задач распознавания образов может быть описана *матрицей информаций*, строки которой соответствуют объектам, столбцы — признакам, а дополнительный столбец содержит символы классов, которым принадлежат объекты.

Будем рассматривать задачу распознавания с *качественными признаками*, когда

- каждый признак принимает значения из множества $X = \{1, 2, \ldots, m\}$,

- имеется k непересекающихся классов, закодированных символами $Y = \{1, 2, \ldots, k\}$,
- имеется n прецедентов.

Информативность признака $x \in X^n$ по отношению к информационному вектору символов классов $y \in Y^n$ объектов будем измерять величиной $I_0(x : y)$.

Пример 1.25. Пусть имеется $n = 9$ прецедентов и

$$\begin{array}{rccccccccc} x = & 2 & 2 & 2 & 2 & 2 & 1 & 2 & 2 & 2 \\ y = & 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 3 \end{array}$$

Тогда

$$I_0(x) = \log \frac{9!}{8! \cdot 1!} = \log 9,$$
$$I_0(y) = \log \frac{9!}{3! \cdot 3! \cdot 3!} = \log 1680$$

и таблица замен символов при переходе $x \to y$:

$$M = \begin{array}{c|ccc|c} & 1 & 2 & 3 & \\ \hline 1 & & 1 & & 1 \\ 2 & 3 & 2 & 3 & 8 \\ \hline & 3 & 3 & 3 & 9 \end{array}$$

$$I_0(y/x) = \log \frac{1!}{1!} + \log \frac{8!}{3! \cdot 2! \cdot 3!} = \log 560,$$
$$I_0(x/y) = 2 \log \frac{3!}{3!} + \log \frac{3!}{1! \cdot 2!} = \log 3,$$
$$I_0(x : y) = I_0(x) - I_0(x/y) = \log 9 - \log 3 = \log 3,$$
$$I_0(y : x) = I_0(y) - I_0(y/x) = \log 1680 - \log 560 =$$
$$= \log 1680/560 = \log 3.$$

Чистые классификаторы и чистые шумы

Определение 1.26. Признак x относительно информационного вектора символов классов y назовём

- *чистым классификатором*, если x и y эквивалентны $(I_0(y/x) = I_0(x/y) = 0 \Leftrightarrow G_x = G_y)$;
- *чистым шумом*, если x и y независимы $(I_0(x : y) = I_0(y : x) = 0)$.

Ясно, что если признак x —

— чистый классификатор, то информационный вектор y безошибочно восстанавливается, так как в этом случае существует биекция $x \leftrightarrow y$;

— чистый шум, то он не даёт никакой информации об информационном векторе y.

Нижний порог информативности признака. Для того, чтобы исключить «шумящие» признаки из дальнейшего рассмотрения, введём *нижний порог* h_1 *информативности признака* и отбросим все признаки объектов с информативностью, меньшей h_1.

Нижний порог h_1 естественно выбирать в процентах от максимально возможной информативности $I(y)$ по Хартли.

Пример 1.27. 1. Для информационного вектора $y = (\,1\ 1\ 1\ 2\ 2\ 2\ 3\ 3\ 3\,)$ символов классов $Y = \{\,1, 2, 3\,\}$ имеем:

$$I(y) = \log|Y^n| = \log 3^9 = \log 19683 \approx 14{,}26.$$

Если выбрать $h_1 = 24\%$, то все признаки x с информативностями $I_0(x : y) < 3{,}42 = 14{,}26 \cdot 0{,}24$ исключаются из дальнейшего рассмотрения.

Кластеры признаков

Утверждение 1.28. *Функция*

$$\rho(x^i, x^j) = \frac{1}{2}\left(I_0(x^i/x^j) + I_0(x^j/x^i)\right)$$

является метрикой на множестве признаков — слов из X^n.

Назовём

- ρ — *информационной метрикой*;
- *кластером признаков* — подмножество близких друг к другу признаков относительно ρ.
  Ясно, что значение ρ между такими признаками близко к 0.

Пример 1.29 (*Кластеры признаков – продолжение Примеров* 1.25, 1.27). Пусть информация о прецедентах в задаче распознавания задана матрицей с качественными признаками

	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	y
1	2	2	2	1	2	2	1	1	1
2	2	2	2	2	2	2	1	1	1
3	2	2	2	1	1	2	1	1	1
4	2	1	1	2	1	1	1	2	2
5	2	1	1	2	1	1	2	1	2
6	1	1	1	2	1	1	1	2	2
7	2	1	1	1	2	2	1	2	3
8	2	1	1	1	2	2	2	2	3
9	2	2	1	1	2	2	1	2	3

Значение $I(y) \approx 14{,}26$ вычислено в Примере 1.27.

1. Подсчитаем информативность $I_0(x^i : y)$, $i = \overline{1,8}$ признаков по отношению к информационному вектору y:

	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8
$I_0(x^i : y)$	1,8	6,2	8,3	6,2	6,2	8,3	1,4	6,3

Приняв порог $h_1 = 24\%$, отбрасываем признаки x^1 и x^7 как малоинформативные — с $I_0(x : y) < 3{,}42$.

2. Составим таблицу расстояний оставшихся признаков:

ρ	x^2	x^3	x^4	x^5	x^6	x^8
x^2	0	3,5	8,4	8,4	5,2	6,8
x^3		0	8,4	8,4	6,0	3,5
x^4			0	6,8	3,5	8,8
x^5				0	3,5	8,8
x^6					0	8,4
x^8						0

Анализ таблицы расстояний позволяет разбить исследуемые признаки на два кластера: $\{ x^2, x^3, x^8 \}$ и $\{ x^4, x^5, x^6 \}$.

Пример 1.30 (*Прогнозирование запаса руды для месторождения*). Значения бинарных признаков:

y — запас руды (1/0 — больше/меньше 1 млн тонн),
x^1 — приуроченность к горизонтам слюдистых сланцев,
x^2 — приуроченность к горизонтам амфиболитов,
x^3 — близость к контакту со слюдистыми сланцами,
x^4 — близость к контакту с амфиболитами,
x^5 — присутствие тел амфиболитов,
x^6 — обилие даек,

x^7 — пиритизация,
x^8 — пропилитизация,
x^9 — ожелезнение,
x^{10} — аргиллитизация,
x^{11} — наличие вторичных ореолов свинца и цинка,
x^{12} — развитие складок.

	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}	y
1	0	1	0	0	0	1	1	1	0	0	1	1	1
2	0	1	1	1	0	0	1	0	1	0	1	1	1
3	0	1	0	1	1	1	0	1	0	0	0	0	1
4	0	0	1	0	1	0	1	0	1	1	1	1	1
5	1	1	0	1	0	1	1	0	1	0	1	0	1
6	1	0	1	0	1	1	0	1	0	1	0	1	0
7	1	0	1	0	1	1	1	0	0	1	0	0	0
8	1	0	0	1	1	1	0	1	0	0	0	0	0
9	1	0	1	1	0	0	0	0	1	0	0	1	0
10	0	1	1	0	1	1	0	1	0	1	0	1	0
11	0	0	1	1	1	1	0	0	0	0	0	1	?
12	0	0	0	1	0	1	0	0	1	0	1	1	?

1. Вычислим информативность признаков $I_0(x^i : y)$, $i = \overline{1, 12}$:

x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}
2,8	2,8	1,24	0,3	1,24	0,3	2,8	0,3	1,24	1,24	6,1	0

Поскольку $I(y) = \log 2^{10} = 10$, то при выборе $h_1 = 25\%$ останутся признаки

$$x^1,\ x^2,\ x^7 \ \text{ и } \ x^{11}$$

с информативностями $\geqslant h_1 \cdot 10 = 2{,}5$ относительно y.

2. Составим таблицу расстояний этих признаков:

ρ	x^1	x^2	x^7	x^{11}
x^1	0	7,2	9,7	8,6
x^2		0	9,7	8,6
x^7			0	3,75
x^{11}				0

Анализ таблицы позволяет провести следующую кластеризацию признаков:

$$\{x^7, x^{11}\}, \quad \{x^1\}, \quad \{x^2\},$$

что приводит к снижению размерности признакового пространства.

Сложные признаки. Если x^i и x^j — признаки, то признак $x^{i,j} = x^i \times x^j$ назовём *сложным*.

Утверждение 1.31. *Информативность $I_0(y : (x^i \times x^j))$ сложного признака $x^i \times x^j$ по отношению к информационному вектору символов классов y удовлетворяет неравенству*

$$I_0(y : (x^i \times x^j)) \geqslant I_0(y : x^i) + I_0(y : x^j) - I_0(x^i : x^j).$$

Поскольку значение $I_0(x^i : x^j)$ монотонно возрастает от 0 при увеличении зависимости признаков x^i и x^j (суммарной длины фрагментов, получающихся перекодировкой), справедливо следующее правило:

При образовании сложного признака следует объединять признаки, лежащие в разных кластерах, то есть для которых $I_0(x^i : x^j) = \min$.

Введём второй параметр настройки h_2, равный минимально допустимой информативности сложного признака. На практике h_2 выбирают $\geqslant 60\%$ от $I(y)$.

В *Примерах* 1.25, 1.29 было выделено два кластера признаков:

$$\left\{x^2, x^3, x^8\right\} \quad \text{и} \quad \left\{x^4, x^5, x^6\right\}.$$

Выберем $h_2 = 80\%$ и получим порог $0{,}8 \cdot 14{,}26 = 11{,}4$ для формирования сложных признаков.

Вычислив значение $I_0(y : (x^i \times x^j))$ для признаков из разных классов, найдём, что информативность сложных признаков

$x^{3,6}$ — достаточна,

$x^{2,4}$ — недостаточна,

$x^{2,4,8}$ — уже достаточна.

Пример 1.32 (*Формирование сложных признаков — продолжение Примера* 1.30). Положим $h_2 = 60\%$, что установит порог информативности $0{,}6 \cdot 10 = 6$ для формируемых сложных признаков.

Образуем сложный признак $x^{1,11} = x^1 \times x^{11} = x$. Его взаимную относительно информационного вектора y информативность $I_0(x : y)$ определим по таблице переходов значений x в значения y, которая, в свою очередь, строится по соответствующим столбцам матрицы информаций. Для компактности будем записывать столбцы матрицы информаций в виде строк.

x^1	0	0	0	0	1	1	1	1	1	0
x^{11}	1	1	0	1	1	0	0	0	0	0
y	1	1	1	1	1	0	0	0	0	0

	0	1	
01		3	3
00	1	1	2
11		1	1
10	4		4
	5	5	10

$$
\begin{aligned}
I_0(x) &= \log \frac{10!}{3!\,2!1!\,4!} = \log 12600, \\
I_0(x/y) &= \log \frac{5!}{1!\,4!} + \log \frac{5!}{3!\,1!\,1!} = \log 100, \\
I_0(x:y) &= I_0(x:y) = I_0(x) - I_0(x/y) = \\
&= \log \frac{12600}{100} = \log 126 \approx 6{,}98 > 6,
\end{aligned}
$$

то есть сложный признак $x = x^1 \times x^{11}$ удовлетворяет условию информативности.

Аналогично находим, что информативность > 6 имеют сложные признаки $x^{2,11}$, $x^{1,2,7}$ и $x^{7,11}$ и осуществляем переход в новое признаковое пространство полученных сложных признаков.

Как вычислить значение сложного признака? Значения $y(x)$ сложного признака x данного объекта определяют в зависимости от третьего параметра настройки h_3, принимающего целочисленные значения и выражающего «*степень значимости*» признака.

Обозначим через n_1 и n_0 число единичных и, соответственно, нулевых значений информационного вектора, соответствующих данному значению полученного сложного признака x.

Полагаем

$$
y(x) = \begin{cases} 1, & \text{если } n_1 - n_0 \geqslant h_3, \\ 0, & \text{если } n_0 - n_1 \geqslant h_3, \\ -, & \text{иначе (отказ от распознавания).} \end{cases}
$$

В рассматриваемом примере примем $h_3 = 2$.

Для признака $x = x^{1,11}$ имеем (дублируем таблицу):

x	0	1		$y(x)$
01		3	3	1
00	1	1	2	–
11		1	1	–
10	4		4	0

$I_0(y : (x^{11} \times x^2)) = 8$ — это относительная информативность, «вес» признака

Тогда, например, для 1, 11 и 12-го объектов получим $f_1(x) = 1$ (справочно), $f_{11}(x) = -$, $f_{12}(x) = 1$.

Для признака $x = x^{11,2}$:

x	0	1		$y(x)$
11		3	3	1
01	1	1	2	–
10		1	1	–
00	4		4	0
	5	5	10	

$I_0(y : (x^{11} \times x^2)) = 8$

Для признака $x = x^{1,2,7}$:

x	0	1		$y(x)$
011		2	2	1
010	1	1	2	–
001		1	1	–
111		1	1	–
100	3		3	0
101	1		1	–
	5	5	10	

$I_0(y : (x^1 \times x^2 \times x^7)) = 8$

Для признака $x = x^{11,7}$:

x	0	1		$y(x)$
11		4	4	1
00	4	1	5	0
01	1		1	–
	5	5	10	

$I_0(y : (x^{11} \times x^7)) = 6{,}4$

Сложные признаки выступают в качестве *элементарных классификаторов*. Далее производится голосование по элементарным классификаторам и вычисляется классификация $\widehat{y}$:

Номер объекта	$x^{1,11}$	$x^{2,11}$	$x^{1,2,7}$	$x^{7,11}$	$\widehat{y}$
11	00 –	00 0	000 –	00 0	0
12	01 1	01 –	000 –	01 –	1

Глава 2

Теория перечисления Пойа

2.1 Лемма Бёрнсайда

Рассматриваем действие $G \underset{\alpha}{:} T$ группы G на множестве T. Напомним, что число орбит (классов эквивалентности) при действии G на T обозначаем $C(G)$.

Лемма 2.1 (Бёрнсайда). *Если группа конечная G действует на конечном множестве T, то*

$$C(G) = \frac{1}{|G|}\sum_{g\in G}\Big|\operatorname{Fix}(g)\Big| = \frac{1}{|G|}\sum_{t\in T}\Big|\operatorname{Stab}(t)\Big|;$$

при этом первое равенство составляет леммой Бёрнсайда[1)].

Доказательство. Пусть $|G| = n$, $|T| = N$ и действие $G \underset{\alpha}{:} T$ задаётся $n \times N$ матрицей $A = \|g_i(t_j)\|$, $i = \overline{1,n}$, $j = \overline{1,N}$.

Подсчитаем двумя различными способами — по столбцам и по строкам матрицы A — мощность множества

[1)] Уильям Бёрнсайд сформулировал и доказал эту лемму в 1897 г., однако О. Коши в 1845 г. и Ф. Фробениусу в 1887 г. уже была известна соответствующая формула. Поэтому эта лемма иногда называют *леммой не-Бёрнсайда*.

$$M \;=\; \big\{\, (g,t) \in G \times T \mid g(t) = t \,\big\}.$$

В результате получим

$$\sum_{g\in G} \Big|\operatorname{Fix}(g)\Big| \;=\; \big|M\big| \;=\; \sum_{t\in T} \Big|\operatorname{Stab}(t)\Big|.$$

Если $x \sim_G y$, то это элементы одной орбиты и $\operatorname{Orb}(x) = \operatorname{Orb}(y)$. Тогда по теореме Лагранжа —

$$\big|\operatorname{Stab}(x)\big| \;=\; \frac{|G|}{|\operatorname{Orb}(x)|} \;=\; \frac{|G|}{|\operatorname{Orb}(y)|} \;=\; \big|\operatorname{Stab}(y)\big|.$$

Выберем по представителю $t_1, \ldots, t_{C(G)}$ из всех $C(G)$ орбит. Тогда

$$\big|M\big| \;=\; \sum_{t\in T} \Big|\operatorname{Stab}(t)\Big| \;=\; \sum_{i=1}^{C(G)} \big|\operatorname{Stab}(t_i)\big|\cdot\big|\operatorname{Orb}(t_i)\big| \;=$$

$$=\; \sum_{i=1}^{C(G)} \frac{|G|}{\big|\operatorname{Orb}(t_i)\big|}\cdot\big|\operatorname{Orb}(t_i)\big| \;=\; |G| \sum_{i=1}^{C(G)} 1 \;=\; |G|\cdot C(G).$$

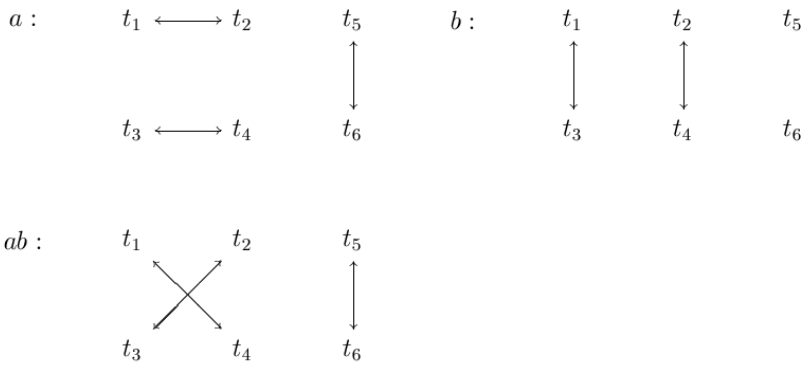
□

Пример 2.2. Действие четверной группы Клейна $V_4 = \{\, e,\, a,\, b,\, ab \,\}$ на множестве $T = \{\, t_1, \ldots, t_6 \,\}$, $n = 4$, $N = 6$.

$\circ$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

$g * t$	t_1	t_2	t_3	t_4	t_5	t_6
e	t_1	t_2	t_3	t_4	t_5	t_6
a	t_2	t_1	t_4	t_3	t_6	t_5
b	t_3	t_4	t_1	t_2	t_5	t_6
ab	t_4	t_3	t_2	t_1	t_6	t_5

Удобнее отобразить перестановки графически.



$$Type(e) = \langle 6,0,0,0,0,0\rangle, \quad Type(a) = \langle 0,3,0,0,0,0\rangle,$$
$$Type(b) = \langle 2,2,0,0,0,0\rangle, \quad Type(ab) = \langle 0,3,0,0,0,0\rangle.$$
$$C(e) = 6,\ C(a) = C(ab) = 3,\ C(b) = 4.$$
$$\mathrm{Stab}\,(t_1) = \mathrm{Stab}\,(t_2) = \mathrm{Stab}\,(t_3) = \mathrm{Stab}\,(t_4) = e \leqslant V_4,$$
$$\mathrm{Stab}\,(t_5) = \mathrm{Stab}\,(t_6) = \langle e, b\rangle \leqslant V_4.$$
$$\mathrm{Fix}\,(a) = \mathrm{Fix}\,(ab) = \varnothing,\ \mathrm{Fix}\,(b) = \{t_5, t_6\},\ \mathrm{Fix}\,(e) = T.$$
$$\big|\,\mathrm{Orb}\,(t_1)\big| = \frac{4}{1} = 4, \quad \big|\,\mathrm{Orb}\,(t_5)\big| = \frac{4}{2} = 2.$$

$$C(V_4) \;=\; \frac{1}{4}\sum_{g\in G}\big|\,\mathrm{Fix}\,(g)\big| = \frac{6+2}{4} \;=\; 2 \;=$$
$$= \;\frac{1}{4}\sum_{t\in\Omega}\big|\,\mathrm{Stab}\,(t)\big| = \frac{4\cdot 1 + 2\cdot 2}{4} \;=\; 2.$$

Как применять лемму «не-Бёрнсайда?»

Для определения числа классов эквивалентности надо представить *эквивалентные элементы множества* T *как классы эквивалентности* действия $G \underset{\alpha}{:} T$ некоторой группы G на T и по лемме определить $C(G)$.

Задача 2.1 (про слова; решение прямым использованием леммы Бёрнсайда). Составляются слова длины $l \geqslant 2$ из алфавита $A = \{ a_1, \ldots, a_q \}$. Слова считаются эквивалентными, если они получаются одно из другого перестановкой крайних букв.

Определить число S неэквивалентных слов.

Решение. $T = A^l$ — множество слов длины l в алфавите A, $|T| = N = q^{\,l}$.

Надо представить эквивалентности как орбиты некоторого действия подходящей группы G на T.

Очевидно, двукратная крайних букв перестановка не меняет ничего, и поэтому подходит $G \cong \mathbb{Z}_2 = \{ e, f \}$. Действие f: переставляет в слове крайние буквы.

Число S неэквивалентных слов = число классов эквивалентности действия $\mathbb{Z}_2 \underset{\alpha}{:} T$ —

$$\big|\operatorname{Fix}(e)\big| = \big|T\big| = q^{\,l}, \qquad \big|\operatorname{Fix}(f)\big| = q^{l-2} \cdot q = q^{l-1}.$$

$$S = C(\mathbb{Z}_2) = \frac{1}{2} \sum_{g \in G} \big|\operatorname{Fix}(g)\big| = \frac{q^{l-1}(q+1)}{2}\,.$$

Теория Пойа эффективна для применения в отношении объектов, имеющих большую внутреннюю симметрию.

Классическими примерами являются здесь платоновы тела и «ожерелья».

Платоновы тела — правильные 3-мерные многогранники. Рассматриваем их группы вращений (самосовмещений) в 3-мерном пространстве.

Платоновы тела	Группа вращения	Порядок группы
тетраэдр	T (тетраэдра)	12
куб и октаэдр	O (октаэдра)	24
икосаэдр и додекаэдр	Y (икосаэдра)	60

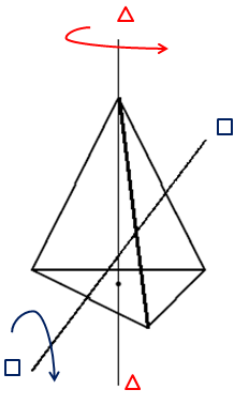
Икосаэдр имеет 20 граней, 30 рёбер и 12 вершин.

Октаэдр

Икосаэдр

Додекаэдр

T — группа вращения тетраэдра



$T = \langle t, f \mid t^3, f^2, (ft)^3 \rangle$, где:

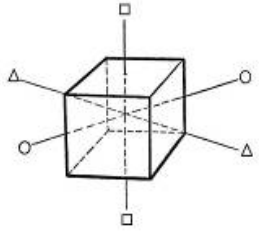
t — вращение на 120° вокруг оси, проходящей через вершину и центр тетраэдра (△—△); таких осей 4.

f — вращение на 180° вокруг оси, проходящей через центры двух противоположных рёбер (□—□); таких осей 3.

$$|T| = (3-1)\cdot 4 + (2-1)\cdot 3 + 1 = 12.$$

Тетраэдр двойственен самому себе, поэтому действие на грани совпадает с действием на вершины.

O — группа вращения октаэдра (= куба)



$O = \langle t, f, r \mid t^4,\ f^2,\ r^3,\ (fr)^4 \rangle$, где:
t — вращение на $90°$ вокруг оси, проходящей через середины двух противоположных граней (□—□), таких осей 3;
f — вращение на $180°$ вокруг оси, проходящей через середины двух противоположных рёбер (○—○), таких осей 6;
r — вращение на $120°$ вокруг оси, проходящей через две противоположные вершины (△—△) таких осей 4.

$$|O| \ = \ 3 \cdot 3 + 1 \cdot 6 + 2 \cdot 4 + 1 \ = \ 24.$$

Поскольку $|G| = |G_x| \cdot [G : G_x]$, то число элементов в группе вращения правильного многогранника есть $\left|E_0\right| \cdot \left|V\right|$, где $\left|E_0\right|$ — число рёбер, выходящих из одной вершины (= порядок стационарной подгруппы вершины, то есть все вращения, оставляющие её на месте), а $\left|V\right|$ — число вершин многогранника (= индекс группы по стационарной подгруппе).

Цикловой индекс. Существует универсальный способ вычисления $C(G)$ — количества классов эквивалентности (= орбит).

Сопоставим каждой перестановке $g \in G$ вес $w(g)$ по правилу:

$$Type(g) = \langle \nu_1, \ldots, \nu_N \rangle \ \Rightarrow \ w(g) = \underbrace{x_1^{\nu_1} \cdot \ldots \cdot x_N^{\nu_N}}_{\text{моном}}.$$

Определение 2.3. Средний вес подстановок в группе называется *цикловым индексом* действия $G \underset{\alpha}{:} T$:

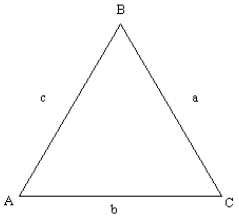
$$P(G \underset{\alpha}{:} T, x_1, \ldots, x_N) = \frac{1}{|G|} \sum_{g \in G} w(g) = \\ = \frac{1}{|G|} \sum_{g \in G} x_1^{\nu_1} \cdot \ldots \cdot x_N^{\nu_N}.$$

(Это производящий полином многих переменных)

Будем также использовать обозначения $P_G(x_1, \ldots, x_N)$ и P_G, $P(G)$.

Пример 2.4. Вычислим цикловой индекс действия группы всех преобразований правильного треугольника в себя (то есть оставляющих его неподвижным), на его стороны.

Решение. T — вершины треугольника, $N = 3$.
$G \cong S_3$ — все перестановки сторон, $|G| = n = 3! = 6$.



$G \underset{\alpha}{:} T$ — самодействие группы S_3
Треугольник — самодвойственная фигура $\Rightarrow$
$\Rightarrow$ действие на стороны $=$
$=$ действие на вершины

$G = T = \langle t, f \mid t^3, f^2, t^2 f = tf \rangle$,

t — вращение вокруг центра на 120° в данном направлении;

f — отражение относительно выбранной оси, проходящей через вершину и центр треугольника.

$$Im(G \underset{\alpha}{:} T) \cong \\ \cong \{ e, \underbrace{(ABC)}_{t}, \underbrace{(ACB)}_{t^2}, \underbrace{(BC)}_{f}, \underbrace{(AC)}_{tf}, \underbrace{(AB)}_{t^2 f} \}.$$

$g \in S_3$	$Type(g)$	$w(g)$	# мономов
e	$\langle\, 3,\, 0,\, 0 \,\rangle$	x_1^3	1
$t,\, t^2$	$\langle\, 0,\, 0,\, 1 \,\rangle$	x_3^1	2
$f,\, tf,\, t^2 f$	$\langle\, 1,\, 1,\, 0 \,\rangle$	$x_1^1 x_2^1$	3
Всего			6

$$P(S_3) \;=\; \frac{1}{6}\left[\, x_1^3 + 2x_3^1 + 3x_1^1 x_2^1 \,\right],$$

— цикловой индекс *самодействия группы* S_3, или, что то же, *группы симметрии треугольника*.

Применение циклового индекса. Пусть заданы множество T, группа G и действие $G \underset{\alpha}{:} T$.

1. Припишем каждому элементу T одно из r значений (неформально: покрасим в один из r цветов). Всего, очевидно, имеется r^N раскрасок.

2. Не будем различать раскраски, если при преобразовании $g : t \to t'$ элемент t' раскрашен также как и t. Например, поворот на 90° — не даёт нового раскрашивания вершин квадрата:

Вопрос: Сколько существует неэквивалентных раскрасок = классов эквивалентности?
Ответ: Это значение вычисляется через цикловой индекс. Имеем —

1. Каждый класс эквивалентности это g-цикл; их $C(g) = \nu_1 + \ldots + \nu_N$ штук.

2. Каждая перестановка $g \in G$ с типом $\langle\, \nu_1,\, \ldots,\, \nu_N \,\rangle$ будет иметь $|\operatorname{Fix}(g)| = r^{C(g)}$ неподвижных точек: каждый класс эквивалентности это g-цикл, их $C(g)$.

Отсюда, по лемме Бёрнсайда, число полученных классов эквивалентности = неэквивалентных раскрасок:

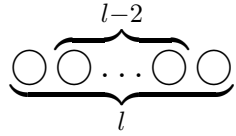
Утверждение 2.5.

$$C(G \underset{\alpha}{:} T) \;=\; P(G \underset{\alpha}{:} T,\, r,\, \ldots,\, r).$$

Задачи на применение циклового индекса

Задача 2.2 (про слова; решение, использующее цикловой индекс). Определить число S неэквивалентных слов длины $l \geqslant 2$ в q-буквенном алфавите, если эквивалентными считаются слова, получающиеся друг из друга перестановкой крайних букв.

Было решение: $S = \frac{q^{\,l}+q^{\,l-1}}{2}$.
Новое решение: $G = \{\, e,\, g \,\} \cong \mathbb{Z}_2$;

T: 

$g \in G$	$Type(g)$	$w(g)$	# мономов
e	$\langle\, l,\, 0,\, \ldots,\, 0 \,\rangle$	x_1^l	1
g	$\langle\, l-2,\, 1,\, 0, \ldots,\, 0 \,\rangle$	$x_1^{l-2}x_2^1$	1

Цикловой индекс: $P(x_1,\, \ldots,\, x_l) \;=\; \dfrac{1}{2}\bigl[x_1^l + x_1^{l-2}x_2^1\bigr]$.

$$S \;=\; P(q,\, \ldots,\, q) \;=\; \frac{q^{\,l}+q^{\,l-1}}{2}.$$

Классическая комбинаторная задача об ожерельях

- *Ожерелье* — окружность, на которой на равных расстояниях по дуге располагаются «бусины».

- *Задача об ожерельях*: сколько различных ожерелий можно составить из N бусин r цветов?
- Какие ожерелья считать неразличимыми? *Варианты*: если одно получается из другого *самосовмещением* —
  1) только *поворотом* в плоскости (*каруселъ*, самодействие циклической группы $\mathbb{Z}_N$;
  2) *поворотом* и *переворотом в пространстве* — самодействие *группы диэдра (двойной пирамиды)* D_N.

Задача 2.3 (об ожерельях $N = 5$, $r = 3$; 1-й вариант). Сколько разных ожерелий можно составить из 5 бусин 3 цветов?

1. Ожерелья одинаковы, если одно получается из другого *поворотом*.

Решение. $G \cong \mathbb{Z}_5 = \langle t \rangle$, $t^5 = e$, $n = 5$.

Элемент $\mathbb{Z}_5$	$Type(g)$	$w(g)$	# мономов
e	$\langle\, 5,\, 0,\, 0,\, 0,\, 0 \,\rangle$	x_1^5	1
$t,\, t^2,\, t^3,\, t^4$	$\langle\, 0,\, 0,\, 0,\, 0,\, 1 \,\rangle$	x_5	4

Цикловой индекс: $P(x_1, \ldots, x_5) = \dfrac{1}{5}\left[\, x_1^5 + 4x_5 \,\right]$.

$$\#Col(3) = P(3, \ldots, 3) = \frac{3^5 + 4 \cdot 3}{5} = 51.$$

Задача 2.4 (Олимпиады «*Покори Воробьёвы горы – 2009*»). Для 50 детей детского сада закуплены 50 одинаковых тарелок. По краю каждой тарелки равномерно расположено 5 белых кружочков.

Воспитатели хотят перекрасить какие-либо из этих кружочков в другой цвет так, чтобы все тарелки стали различными.

Какое наименьшее число дополнительных цветов потребуется им для этого?

Как должны были решать школьники.

Пусть требуется r цветов. Отбросим r вариантов раскраски в один цвет. Число остальных вариантов —

без учёта возможности поворота тарелки: $r^5 - r$;

с учётом поворота: $\dfrac{r^5 - r}{5}$ (каждый вариант повторяется 5 раз).

Итого: $\#Col(r) = \dfrac{r^5 - r}{5} + r = \dfrac{r^5 + 4r}{5}$ и при 2-х дополнительных цветах — $\#Col(3) = 51$.

Решая эту задачу мы доказали *малую теорему Ферма*:

Теорема 2.6 (Ферма). *Если целое a не делится на простое число p, то $a^{p-1} \equiv_p 1$.*

Доказательство. Число раскрасок более, чем в один из a цветов с учётом поворота — $\frac{a\left(a^{p-1}-1\right)}{p}$ — целое число. Отсюда, если $a \not\vdots p$, то $(a^{p-1} - 1) \vdots p$, то есть $a^{p-1} \equiv_p 1$. □

Задача 2.5 (об ожерельях $N = 5$, $r = 3$; 2-й вариант).

2. Ожерелья одинаковы, если одно получается из другого *поворотом и/или переворотом*.

Решение. D_n — *группа диэдра* порядка $2n$: $D_n = \langle\, t, f \mid t^n,\ f^2,\ tft = f \,\rangle;\ G = D_5$.

Элемент D_5	$Type(g)$	$w(g)$	# мономов
e	$\langle\, 5,\ 0,\ 0,\ 0,\ 0 \,\rangle$	x_1^5	1
$t,\ t^2,\ t^3,\ t^4$	$\langle\, 0,\ 0,\ 0,\ 0,\ 1 \,\rangle$	x_5	4
$f,\ tf,\ \ldots,\ t^4f$	$\langle\, 1,\ 2,\ 0,\ 0,\ 0 \,\rangle$	$x_1x_2^2$	5
Всего			10

Цикловой индекс: $P = \dfrac{1}{10}\left[\, x_1^5 + 4x_5 + 5x_1x_2^2 \,\right]$.

$$\#Col(3) = P(x_1, \ldots, x_5)\Big|_{x_1 = \ldots = x_5 = 3} = \\ = \frac{3^5 + 4 \cdot 3 + 5 \cdot 3^3}{10} = 39.$$

Задача 2.6 (о раскраске сторон квадрата). Сколько существует различно окрашенных квадратов, если их стороны раскрашивают в r цветов?

Решение. Группа самосовмещения квадрата в пространстве — группа диэдра $D_4 = \langle\, t,\ f,\ s \,\rangle$, $|D_4| = 8$, которая порождается тремя образующими:

t : вращение на 90° вокруг центра в выбранном направлении;

f : симметрия относительно оси, проходящей через середины противоположных *сторон* — 2 оси;

s : симметрия относительно оси, проходящей через противоположные вершины *вершин* — 2 оси.

При самодействии группы D_4 $(N = 4)$ её элементы будут иметь следующие веса:

e : единичная перестановка оставит все стороны на месте, то есть имеются 4 цикла длины 1, вес x_1^4 (1 перестановка);

t, t^3 : стороны циклически переходят друг в друга по и против часовой стрелки, длина цикла 4, вес x_4^1 (2 перестановки);

t^2 : стороны переходят в противоположные, что даёт два цикла длины 2, вес — x_2^2 (1 перестановка);

f : две противоположные стороны на месте, остальные две меняются местами, то есть имеются два единичных цикла и один длины 2, вес — $x_1^2 x_2^1$ (1 перестановка, 2 оси);

s : в двух парах смежных сторон элементы меняются местами, что даёт два цикла длины 2, вес — x_2^2 (1 перестановка, 2 оси).

$g \in D_4$	$Type(g)$	$w(g)$	#
e	$\langle 4,0,0,0\rangle$	x_1^4	1
t, t^3	$\langle 0,0,0,1\rangle$	x_4^1	2
t^2	$\langle 0,2,0,0\rangle$	x_2^2	1
f	$\langle 2,1,0,0\rangle$	$x_1^2 x_2$	2
s	$\langle 0,2,0,0\rangle$	x_2^2	2

$$P_{D_4}(x_1, \ldots, x_4) = \frac{1}{8}\left[\, x_1^4 + 2x_4 + 3x_2^2 + 2x_1^2 x_2 \,\right].$$

Число раскрасок квадрата в r цветов:

$$P_{D_4}(r, \ldots, r) = \frac{1}{8}\left[\, r^4 + 2r + 3r^2 + 2r^3 \,\right].$$

В частности, в два и три цвета:

$$\#Col(2) = \frac{2^4 + 4 \cdot 2^2 + 2^4}{2^3} = 2 + 2 + 2 = 6,$$
$$\#Col(3) = \frac{3^4 + 2 \cdot 3 + 3^4}{8} = 21.$$

Задача 2.7 (раскраска граней куба в два цвета). Грани куба раскрашивают в 2 и 3 цвета.
Сколько существует различно окрашенных кубов?

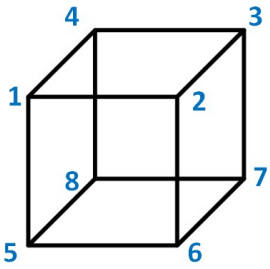
Решение. Обозначение: F множество граней куба; $|F| = N = 6$. Выберем некоторую грань куба (квадрат) и обозначим её ①, а параллельную ей — ②.
Перенумеруем последовательно вершины грани ① числами $1, \ldots, 4$, а вершины грани ② — числами $5, \ldots, 8$ так, что вершина с номером i смежна с вершиной с номером $i + 4$, $i = 1, 2, 3, 4$.

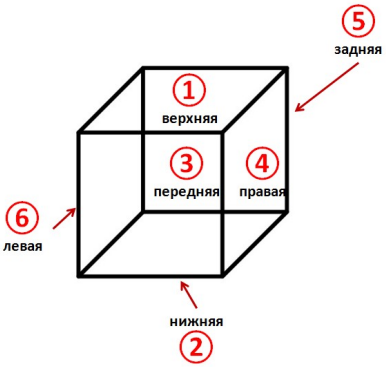
Перестановки далее указаны для случая, когда ось вращения

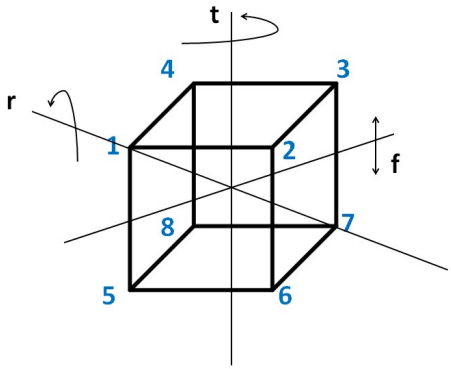
$\langle t \rangle$ проходит через середины граней ① и ②,
$\langle f \rangle$ проходит через середины рёбер (3-7) и (1-5),
$\langle s \rangle$ проходит через вершины (1) и (7),

а грани обозначены: (1-2-6-5) через ③, параллельная ей грань — ⑤, грань (2-3-7-6) — через ④, параллельная ей грань — ⑥.

$g \in O$	перестановка	$Type(g)$	$w(g)$	#
e	(①)…(⑥)	$\langle 6, 0, \ldots \rangle$	x_1^6	1
t, t^3	(①)(②)(③④⑤⑥)	$\langle 2, 0, 0, 1, 0, \rangle$	$x_1^2 x_4$	6
t^2	(①)(②)(③⑤)(④⑥)	$\langle 2, 2, 0, \ldots \rangle$	$x_1^2 x_2^2$	3
f	(①②)(③⑥)(④⑤)	$\langle 0, 3, 0, \ldots \rangle$	x_2^3	6
r, r^2	(①③⑥)(②④⑤)	$\langle 0, 0, 2, 0, \ldots \rangle$	x_3^2	8
Всего				24







$$P(x_1, \ldots, x_6) = \frac{1}{24}\left[\, x_1^6 + 6x_1^2x_4 + 3x_1^2x_2^2 + 6x_2^3 + 8x_3^2 \,\right].$$

$$\#Col(2) = \frac{1}{24}\left[2^6 + 12 \cdot 2^3 + 3 \cdot 2^4 + 8 \cdot 2^2\right] = 10,$$
$$\#Col(3) = \frac{1}{24}\left[3^6 + 12 \cdot 3^3 + 3 \cdot 3^4 + 8 \cdot 3^2\right] = 48.$$

Цикловой индекс действия группы октаэдра на множестве R рёбер куба ($|R| = N = 12$):

$g \in O$	$Type(g)$	$w(g)$	#
e	$\langle\, 12,\, 0,\, \ldots \,\rangle$	x_1^{12}	1
t, t^3	$\langle\, 0,\, 0,\, 0,\, 3,\, 0,\, 0 \,\rangle$	x_4^3	$3 \cdot 2 = 6$
t^2	$\langle\, 0,\, 6,\, 0,\, \ldots \,\rangle$	x_2^6	3
f	$\langle\, 2,\, 5,\, 0,\, \ldots \,\rangle$	$x_1^2 x_2^5$	6
r, r^2	$\langle\, 0,\, 0,\, 4,\, 0,\, \ldots \,\rangle$	x_3^4	$4 \cdot 2 = 8$
Всего			24

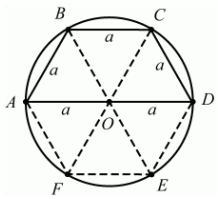
$$P(O \underset{\alpha}{:} R) \;=\; \frac{1}{24}\big[\, x_1^{12} + 6x_4^3 + 3x_2^6 + 6x_1^2 x_2^5 + 8x_3^4 \,\big].$$

Цикловой индекс действия группы октаэдра на множестве V вершин куба ($|V| = N = 8$):

$g \in O$	$Type(g)$	$w(g)$	#
e	$\langle\, 8,\, 0,\, \ldots \,\rangle$	x_1^8	1
t, t^3	$\langle\, 0,\, 0,\, 0,\, 2,\, 0,\, 0 \,\rangle$	x_4^2	$3 \cdot 2 = 6$
t^2	$\langle\, 0,\, 4,\, 0,\, \ldots \,\rangle$	x_2^4	3
f	$\langle\, 0,\, 4,\, 0,\, \ldots \,\rangle$	x_2^4	6
r, r^2	$\langle\, 2,\, 0,\, 2,\, 0,\, \ldots \,\rangle$	$x_1^2 x_3^2$	$4 \cdot 2 = 8$
Всего			24

$$P(O \underset{\alpha}{:} V) \;=\; \frac{1}{24}\big[\, x_1^8 + 6x_4^2 + 9x_2^4 + 8x_1^2 x_3^2 \,\big].$$

Задача 2.8. Найти цикловой индекс транзитивного самодействия группы $\mathbb{Z}_6$.



Решение. Обозначим последовательно вершины правильного шестиугольника буквами $A, \dots, F$, $\mathbb{Z}_6 = \langle t \rangle$, t — поворот на $60°$.

$g \in \mathbb{Z}_6$	$Type(g)$	$w(g)$
$e = (A)\dots(F)$	$\langle\, 6,\, 0,\, 0,\, 0,\, 0,\, 0 \,\rangle$	x_1^6
$g = (ABCDEF)$	$\langle\, 0,\, 0,\, 0,\, 0,\, 0,\, 1 \,\rangle$	x_6
$g^2 = (ACE)(BDF)$	$\langle\, 0,\, 0,\, 2,\, 0,\, 0,\, 0 \,\rangle$	x_3^2
$g^3 = (AD)(BE)(CF)$	$\langle\, 0,\, 3,\, 0,\, 0,\, 0,\, 0 \,\rangle$	x_2^3
$g^4 = (AEC)(BFD)$	$\langle\, 0,\, 0,\, 2,\, 0,\, 0,\, 0 \,\rangle$	x_3^2
$g^5 = (AFEDCB)$	$\langle\, 0,\, 0,\, 0,\, 0,\, 0,\, 1 \,\rangle$	x_6

$$P_{\mathbb{Z}_6} = \frac{1}{6}\big[\, x_1^6 + x_2^3 + 2x_3^2 + 2x_6 \,\big] = \frac{1}{6}\sum_{d|6} \varphi(d) x_d^{6/d};$$

$$D(6) = \{\, 1, 2, 3, 6 \,\},\ \varphi(1) = \varphi(2) = 1,\ \varphi(3) = \varphi(6) = 2$$

Приведём без вывода цикловой индекс самодействия $\mathbb{Z}_n$:

$$P(\mathbb{Z}_n) = \frac{1}{n}\sum_{d|n} \varphi(d) x_d^{n/d}, \quad \varphi - \text{функция Эйлера.}$$

Задача 2.9. Найти цикловой индекс действия группы симметрии правильного n-угольника (группы диэдра) D_n на его вершины (стороны).

Решение. $|D_n| = 2n$, $n > 2$.
1. При *нечётных* n: $D_n = \langle\, t,\, f \,\rangle$, где

t — вращение на $360^\circ/n$ вокруг центра квадрата, $\langle t \rangle \cong \mathbb{Z}_n$;

r — симметрия относительно прямой, проходящей через вершину и центр многоугольника, $\langle r \rangle \cong \mathbb{Z}_2$, n осей.

$$P(D_n) = \frac{1}{2n}\left[\sum_{d|n} \varphi(d) x_d^{n/d} + n x_1 x_2^{(n-1)/2}\right] = \\ = \frac{1}{2} P(\mathbb{Z}_n) + \frac{1}{2} x_1 x_2^{(n-1)/2}.$$

2. При *чётных* n: $D_n = \langle\, t,\, f,\, s \,\rangle$, где

t — то же;

f — симметрия относительное прямой, проходящей через середины противоположных сторон, $\langle f \rangle \cong \mathbb{Z}_2$, $n/2$ осей;

s — симметрия относительное прямой, проходящей через противоположные вершин, $\langle s \rangle \cong \mathbb{Z}_2$, $n/2$ осей.

$$P(D_n) = \frac{1}{2n}\left[\sum_{d|n} \varphi(d) x_d^{n/d} + \frac{n}{2} x_2^{n/2} + \frac{n}{2} x_1^2 x_2^{n/2-1}\right] = \\ = \frac{1}{2} P(\mathbb{Z}_n) + \frac{1}{4}\left[x_2^{n/2} + x_1^2 x_2^{n/2-1}\right].$$

Приведём без вывода цикловой индекс самодействия S_n:

$$P(S_n) = \sum_{\substack{(j_1,\ldots,j_n)\in\mathbb{N}_0^n \\ 1j_1+2j_2+\ldots+nj_n=n}} \frac{x_1^{j_1}x_2^{j_2}\ldots x_n^{j_n}}{(1^{j_1}j_1!)(2^{j_2}j_2!)\ldots(n^{j_n}j_n!)},$$

2.2 Теорема Пойа

К множеству T, $|T| = N$, группе G, $|G| = n$ и действию $G \underset{\alpha}{:} T$ добавим множество $R = \{c_1, \ldots, c_r\}$, меток («красок»), и совокупность функций

R^T — приписывания меток элементам T

(*раскрашиваний*).

Группа G, действуя на T, действует и на R^T — операция $\circ : R^T \times G \overset{\circ}{=} R^T$.

Придадим вес элементам R: $w(c_i) = y_i$, $i = \overline{1,r}$.

Теорема 2.7 (Редфилда-Пойа; 1927, 1937[2)]). *Цикловой индекс действия группы G на R^T есть*

$$W(R^T) = (G \underset{\alpha}{:} R^T, y_1, \ldots, y_r) = \\ = P(G \underset{\alpha}{:} T, x_1, \ldots, x_N)\Big|_{x_k = y_1^k+\ldots+y_r^k,\ k=\overline{1,N}}.$$

[2)] Впервые опубликована Д. Г. Редфилдом в 1927 г., но его работа осталась незамеченной. Независимо доказана Д. Пойа в 1937 г. с демонстрацией применимости результата к перечислению химических соединений.

Следствие (лемма Бёрнсайда). *Если все веса выбраны одинаковыми (то есть* $y_1 = \ldots = y_r = 1$*), то* $x_1 = \ldots = x_N = r$ *и* $W(R^T)$ *— число классов эквивалентности*

$$W(R^T) = P(G \underset{\alpha}{:} T, r, \ldots, r).$$

Что можно определить (подсчитать) с помощью:

леммы Бёрнсайда — общее число неэквивалентных разметок (раскрасок);

теоремы Редфилда-Пойа — число разметок, содержащих данное количество элементов конкретного цвета.

Усложним задачу об ожерельях:

Задача 2.10 (об ожерельях $N = 5$, $r = 3$, продолжение, более сложный вариант). Цвета — *красный*, синий, зелёный. Ожерелья одинаковы, если одно получается из другого поворотом и переворотом. Сколько имеется ожерелий, имеющих ровно 2 *красные* бусины?

Решение. Было: $G = D_5$, цикловой индекс

$$P(x_1, \ldots, x_5) = \frac{1}{10}\left[x_1^5 + 4x_5 + 5x_1x_2^2\right],$$

всего ожерелий $P(3, \ldots, 3) = 39$ (только поворот — их 51).

$x_1 = y_1 + y_2 + y_3$, $x_2 = y_1^2 + y_2^2 + y_3^2$, $x_5 = y_1^5 + y_2^5 + y_3^5$.

$$\left\{\begin{array}{ll} w(\text{красный}) & = y_1, \\ w(\text{синий}) & = y_2, \\ w(\text{зелёный}) & = y_3, \end{array}\right. \Rightarrow \left\{\begin{array}{l} y_1 = y, \\ y_2 = y_3 = 1, \end{array}\right. \Rightarrow$$

$$\Rightarrow \left\{\begin{array}{ll} x_1 & = y + 2, \\ x_2 & = y^2 + 2, \\ x_5 & = y^5 + 2. \end{array}\right. \qquad P(y) = \sum_{i=1}^{5} u_i y^i;$$

$$u_2 = ?$$

$$P(y) = \frac{1}{10}\Big[\,(y+2)^5 + 4(y^5+2) + 5(y+2)(y^2+2)^2\,\Big] =$$

$$= \frac{1}{10}\Big[\,\ldots + C_5^2 2^3 y^2 + \ldots + 5(y+2)(y^4+4y^2+4)\,\Big] =$$

$$= \frac{1}{10}\Big[\,\ldots + (10\cdot 8 + 5\cdot 2\cdot 4)y^2 + \ldots\,\Big].$$

$$u_2 = 8 + 4 = 12.$$

Задача 2.11. Вершины куба помечают красными и синим цветами. Сколько существует

1) разнопомеченных кубов;
2) кубов, у которых половина вершины красные;
3) кубов, у которых не более 2 красных вершин?

Решение. Цикловой индекс действия группы O на вершины куба —

$$P(O \underset{\alpha}{:} V;\, x_1, \ldots x_8) = \frac{1}{24}\big[\,x_1^8 + 6x_4^2 + 9x_2^4 + 8x_1^2x_3^2\,\big].$$

1) $\#Col(2) = P(2, \ldots, 2) =$

$$= \frac{2^8 + 6\cdot 2^2 + 9\cdot 2^4 + 8\cdot 4\cdot 4}{3\cdot 2^3} = 23.$$

2) $w(\text{красный}) = y$, $w(\text{синий}) = 1$,
$x_k = y^k + 1$, $k = \overline{1,8}$:

$$\#Col(4,4) = \frac{1}{24}\Big[(y+1)^8 + 6\cdot(y^4+1)^2 + 9\cdot(y^2+1)^4 + \\ + 8\cdot(y+1)^2(y^3+1)^2 \Big] = \\ = \frac{1}{24}\big[\ldots + C_8^2 y^2 + C_8^4 y^4 + 6\cdot 2y^4 \ldots + \\ \ldots + 9(\ldots + 4y^2 + 6y^4 + \ldots) + 8(y^2+2y+1)(y^6+2y^3+1) \big].$$

$$u_4 = \frac{1}{24}\big[70 + 9\cdot 6 + 6\cdot 2 + 8\cdot 2\cdot 2 \big] = \frac{168}{24} = 7.$$

3) $\#Col(\leqslant 2, *) = u_0 + u_1 + u_2$, очевидно $u_0 = u_1 = 1$.

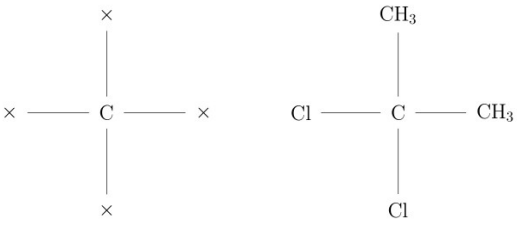
$$u_2 = \frac{28 + 36 + 8}{24} = 3.$$

$\#Col(\leqslant 2, *) = 1 + 1 + 3 = 5$.

Задача 2.12. Рассмотрим молекулы 4-валентного углерода C, где на месте $\times$ могут находится

CH_3 — метил,	C_2H_5 — этил,
H — водород,	Cl — хлор.

Например — дихлорбутан (на рисунке).



Найти

1) общее число M всех молекул;

2) число молекул с $H = 0, 1, 2, 3, 4$ присоединёнными атомами водорода.

Решение. Какая группа действует и на каком множестве? Группа T на множестве вершин тетраэдра.

$g \in T$	$Type(g)$	$w(g)$	#
e	$\langle\, 4, 0, 0, 0 \,\rangle$	x_1^4	1
$t,\ t^2$	$\langle\, 1, 0, 1, 0 \,\rangle$	$x_1 x_3$	$4 \cdot 2 = 8$
f	$\langle\, 0, 2, 0, 0 \,\rangle$	x_2^2	3

$$P(T \underset{\alpha}{:} V) \;=\; \frac{1}{12}\big[\, x_1^4 + 8x_1x_3 + 3x_2^2 \,\big]$$

1. Имеем 4 радикала, поэтому $x_1 = \ldots = x_4 = 4$ и

$$M \;=\; P(x_1,\, \ldots,\, x_4) \;=\; \frac{4^4 + 8 \cdot 4 \cdot 4 + 3 \cdot 4^2}{3 \cdot 4} \;=\; 36.$$

2. Веса: $y_1 = \mathrm{H}$, $y_2 = y_3 = y_4 = 1$.
Подстановка в P: $x_k \;=\; \mathrm{H}^k + 3,\ k = \overline{1,4}$.

$$P(H) \;=$$

$$= \frac{1}{12}\big[\ (\mathrm{H}+3)^4 + 8\,(\mathrm{H}+3)\left(\mathrm{H}^3+3\right) + 3\left(\mathrm{H}^2+3\right)^2\ \big] \;=$$

$$= \frac{1}{12}\big[\ \left(\mathrm{H}^4 + 4\cdot\mathrm{H}^3\cdot 3 + 6\cdot\mathrm{H}^2\cdot 9 + 4\cdot\mathrm{H}\cdot 27 + 81\right) +$$

$$+ 8\left(\mathrm{H}^4 + 3\mathrm{H}^3 + 3\mathrm{H} + 9\right) + 3\left(\mathrm{H}^4 + 6\mathrm{H}^2 + 9\right)\big] \;=$$

$$= 1\cdot\mathrm{H}^4 + 3\cdot\mathrm{H}^3 + 6\cdot\mathrm{H}^2 + 11\cdot\mathrm{H} + 15.$$

Итого имеется молекул с числом атома водорода: с 4-мя — 1 шт., с 3-мя — 3 шт., с 2-мя — 6 шт., с 1-м — 11 шт., без атомов водорода — 15 шт., всего — $1 + 3 + 6 + 11 + 15 \;=\; 36$.

Задача 2.13 (об ожерельях со стоимостью). Стоимости каменей для ожерелий равны: красного — 1 ед., синего — 2 ед., зелёного — 3 ед. Сколько существует ожерелий из 15 таких камней, стоимость которых равна 30 ед.?

Решение. Цикловой индекс самодействия группы диэдра (было ранее):

$$P(D_n) = \frac{1}{2n}\sum_{d|n}\varphi(d)x_d^{n/d} + \begin{cases} \frac{1}{2}x_1 x_2^{(n-1)/2}, & n \text{ нечётно}, \\ \frac{1}{4}\left[x_2^{n/2} + x_1^2 x_2^{n/2-1}\right], & n \text{ чётно}, \end{cases}$$

Для $n = 15$: $D(15) = \{\,1,\,3,\,5,\,15\,\}$

$$\varphi(1) = 1, \quad \varphi(3) = 2, \quad \varphi(5) = 4, \quad \varphi(15) = 8.$$

$$P_{D_{15}} = \frac{1}{30}\left[\,x_1^{15} + 2x_3^5 + 4x_5^3 + 8x_{15}^1 + 15x_1x_2^7\,\right].$$

С учётом стоимости камней необходимая подстановка в цикловой индекс:

красный — $y_1 = y$, синий — $y_2 = y^2$, зелёный — $y_3 = y^3$,

откуда $x_k = y^k + y^{2k} + y^{3k}$.

$$W = \frac{1}{30}\Big[\,\left(y + y^2 + y^3\right)^{15} + 2\left(y^3 + y^6 + y^9\right)^5 + \\ + 4\left(y^5 + y^{10} + y^{15}\right)^3 + 8\left(y^{10} + y^{30} + y^{45}\right)^1 + \\ +15\left(y + y^2 + y^3\right)\left(y^2 + y^4 + y^6\right)^7\,\Big] = \ldots + u_{30}y^{30} + \ldots.$$

$$u_{30} = 59\,788.$$

2.3 Задачи с решениями

Задача 2.14. Найти цикловой индекс для следующим образом определённого самодействия четверной группы Клейна
$V_4 = \{ e, a, b, ab \mid a^2 = b^2 = (ab)^2 = e^2 = e,\ ab = ba \}$:

1. $e : \begin{pmatrix} e & a & b & ab \\ e & a & b & ab \end{pmatrix}$, $a : \begin{pmatrix} e & a & b & ab \\ a & e & ab & b \end{pmatrix}$,
$b : \begin{pmatrix} e & a & b & ab \\ b & ab & e & a \end{pmatrix}$, $ab : \begin{pmatrix} e & a & b & ab \\ ab & b & a & e \end{pmatrix}$;
2. $e : \begin{pmatrix} e & a & b & ab \\ e & a & b & ab \end{pmatrix}$, $a : \begin{pmatrix} e & a & b & ab \\ a & e & b & ab \end{pmatrix}$,
$b : \begin{pmatrix} e & a & b & ab \\ e & a & ab & b \end{pmatrix}$, $ab : \begin{pmatrix} e & a & b & ab \\ a & e & ab & b \end{pmatrix}$.

Решение. Везде группа Клейна V_4 действует на свои же элементы.

1)

g	$Type(g)$	$w(g)$	#
e	$\langle \underline{4}, 0, 0, 0 \rangle$	x_1^4	1
a, b, ab	$\langle 0, 2, 0, 0 \rangle$	x_2^2	3

$$P_{V_4} = \frac{1}{4}\left[x_1^4 + 3x_2^2 \right].$$

2)

g	$Type(g)$	$w(g)$	#
e	$\langle \underline{4}, 0, 0, 0 \rangle$	x_1^4	1
a, b	$\langle \underline{2}, 1, 0, 0 \rangle$	$x_1^2 x_2$	2
ab	$\langle 0, 1, 0, 0 \rangle$	x_2	1

$$P'_{V_4} = \frac{1}{4}\left[x_1^4 + 2x_1^2 x_2 + x_2 \right].$$

Первая группа перестановок есть нормальная подгруппа S_4, а вторая — нет.

Задача 2.15. На стеклянных пластинах рисуют одинаковые прямоугольники (не квадраты) и раскрашивают их *вершины* в 3 цвета. Сколько можно нарисовать таких различных прямоугольников?

Решение. Найдём цикловой индекс $P(R \underset{\alpha}{:} V)$ действия группы R самосовмещений прямоугольника в пространстве на его вершины.

$g \in R$	$Type(g)$	$w(g)$	#
e	$\langle\, 4,\, 0,\, 0,\, 0 \,\rangle$	x_1^4	1
t	$\langle\, 0,\, 2,\, 0,\, 0 \,\rangle$	x_2^2	1
f	$\langle\, 0,\, 2,\, 0,\, 0 \,\rangle$	x_2^2	2

$$P(\mathbb{R} \underset{\alpha}{:} V;\, x_1,\, x_2,\, x_3,\, x_4) \;=\; \frac{1}{4}\big[\, x_1^4 + 3x_2^2 \,\big]$$

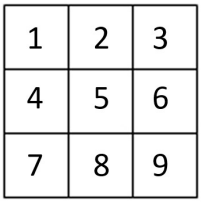
Число прямоугольников:

$$\#Col(3) \;=\; P(\mathbb{R} \underset{\alpha}{:} V; 3, \ldots, 3) \;=\; \frac{81+27}{4} \;=\; 27$$

Задача 2.16. Квадратная стеклянная пластина разделена на 9 равных квадратов, которые раскрашиваются в один из 2 цветов.
Сколько существует разноокрашенных пластин?

Решение. На множество T из $N = 9$ квадратов стеклянной пластики действует группа $D_4 = \langle\, t,\, f,\, s \,\rangle$, $t^4 = f^2 = s^2 = e$, где

t — вращение на 90° вокруг центра квадрата;



f — отражение относительно прямой, проходящей через середины противоположных сторон;

s — отражение относительно прямой, проходящей противоположные вершины.

Определяем цикловой индекс действия D_4 на T.

$g \in D_4$	перестановка	$Type(g)$	$w(g)$	#
e	$(1)\dots(9)$	$\langle 9,0,\dots\rangle$	x_1^9	1
t, t^3	$(5)(1397)(2684)$	$\langle 1,0,0,2,\dots\rangle$	$x_1x_4^2$	2
t^2	$(5)(19)(37)(28)(79)$	$\langle 1,4,0,\dots\rangle$	$x_1x_2^4$	1
$s, f, \dots$	$(2)(5)(8)(13)(48)(79)$	$\langle 3,3,0,\dots\rangle$	$x_1^3x_2^3$	4
				8

Цикловой индекс:

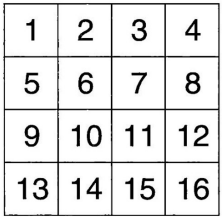
$$P = \frac{1}{8}\left[\, x_1^9 + 2x_1x_4^2 + x_1x_2^4 + 4x_1^3x_2^3 \,\right],$$

поэтому

$$\#Col(2) = \frac{2^9 + 2\cdot 2^3 + 2^5 + 4\cdot 2^3\cdot 2^3}{2^3} = 102.$$

Задача 2.17. *Компостером* назовём квадратную таблицу 4×4, в которой каждая клетка может быть либо пустой, либо содержать в центре символ $\bullet$.

Сколько существует различных компостеров, если не различать те, которые могут быть получены



один из другого самосовмещениями в пространстве? К аналогичной задаче сводится задача о числе фотошаблонов рисунков соединений для интегральных схем.

Решение. Найдём цикловой индекс действия группы диэдра D_4 на 16 клеток компостера.
$D_4 = \langle t, f, s \rangle$, $t^4 = f^2 = s^2 = e$, $|D_4| = 8$.

g	перестановка	$Type(g)$	$w(g)$	#
e	$(1)\dots(16)$	$\langle 16, 0, \dots \rangle$	x_1^{16}	1
t, t^3	$(1,4,16,13)\dots(6,7,11,10)$	$\langle 0, 0, 0, 4, \dots \rangle$	x_4^4	2
t^2	$(1,16)\dots(6,11)$	$\langle 0, 8, 0 \dots \rangle$	x_2^8	1
f	$(1,4)\dots(10,11)$	$\langle 0, 8, 0, \dots \rangle$	x_2^8	2
s	$(1)\dots(16)(2,5)\dots(12,15)$	$\langle 4, 6, 0, \dots \rangle$	$x_1^4 x_2^6$	2

Цикловой индекс действия группы D_4 на элементы компостера:

$$P(x_1, \dots, x_4) = \frac{1}{8}\left[x_1^{16} + 2x_4^4 + 3x_2^8 + 2x_1^4 x_2^6 \right].$$

Наличие/отсутствие в клетке символа $\bullet$ описывается их отображением в двухэлементное множество (раскраске в два цвета), поэтому число C различных компостеров есть

$$C = P(2, 2, \dots) = \frac{2^{16} + 2^5 + 3 \cdot 2^8 + 2^{11}}{2^3} = 8548.$$

Задача 2.18. Найти число различных вариантов раскраски *граней* куба в 2 и 3 цвета.

Решение. Цикловой индекс:

$$P(O \underset{\alpha}{:} F) = \frac{1}{24}\big[\, x_1^6 + \underline{6x_1^2x_4} + 3x_1^2x_2^2 + \underline{6x_2^3} + 8x_3^2 \,\big].$$

$$\#Col(2) = (1/(3\cdot 2^3))(2^6 + 12\cdot 2^3 + 3\cdot 2^4 + 2^5) = 10.$$
$$\#Col(3) = (3\cdot 8)(3^6 + 12\cdot 3^3 + \cdot 3^5 + 8\cdot 3^2) = 57.$$

Задача 2.19. Определить число различных раскрасок всех граней правильной 4-угольной пирамиды Π в 3 цвета.

Решение. Занумеруем последовательно боковые грани Π числами $1, \ldots 4$, а основание — 5.
$G \cong \mathbb{Z}_4 = \langle\, t \,\rangle$, t — вращение на 90°.

$g \in \mathbb{Z}_4$	$Type(g)$	$w(g)$	#
$e = (1)(2)(3)(4)(5)$	$\langle\, 5,\, 0,\, 0,\, 0,\, 0 \,\rangle$	x_1^5	1
$t, t^3 = (1234)(5)$	$\langle\, 1,\, 0,\, 0,\, 1,\, 0 \,\rangle$	x_1x_4	2
$t^2 = (12)(34)(5)$	$\langle\, 1,\, 2,\, 0,\, 0,\, 0 \,\rangle$	$x_1x_2^2$	1

$$P(x_1, \ldots, x_5) = \frac{1}{4}\big[\, x_1^5 + 2x_1x_4 + x_1x_2^2 \,\big],$$
$$P(3, \ldots, 3) = \frac{3^5 + 2\cdot 3^2 + 3^3}{4} = \frac{9\cdot 32}{4} = 72.$$

Задача 2.20. Найти число раскрасок всех граней усечённой правильной четырёхугольной пирамиды в 3 цвета.

Решение. Пронумеруем грани П: боковые — с 1 по 4 по часовой стрелке, основания — 5 и 6. Группа, действующая на П — $\mathbb{Z}_4 = \langle t \rangle$, t — поворот на 90° по часовой стрелке.

$g \in \mathbb{Z}_4$	перестановка	$Type(g)$	$w(g)$	#
e	$(1)\dots(6)$	$\langle 6, 0, \dots \rangle$	x_1^6	1
t, t^3	$(1234)(5)(6)$	$\langle 2, 0, 0, 1, 0, 0 \rangle$	$x_1^2 x_4$	2
t^2	$(12)(34)(5)(6)$	$\langle 2, 2, 0, \dots \rangle$	$x_1^2 x_2^2$	1

Цикловой индекс $P = \frac{1}{4}\left[x_1^6 + 2x_1^2 x_4 + x_1^2 x_2^2 \right]$.

$$\#Col(3) = \frac{3^6 + 2 \cdot 3^2 + 3^4}{4} = \frac{3^3(27 + 2 + 3)}{4} = 216.$$

Задача 2.21. Найти число различных вариантов раскраски *граней* тетраэдра в 2 и 3 цвета.

Решение. $P(T \underset{\alpha}{:} F, x_1, \dots, x_4) =$

$$= \frac{1}{12}\left[x_1^4 + 8x_1 x_3 + 3x_2^2 \right].$$

$$\#Col(2) = \frac{2^4 + 11 \cdot 2^2}{3 \cdot 2^2} = \frac{4 + 11}{3} = 5\,.$$

$$\#Col(3) = \frac{3^4 + 11 \cdot 3^2}{3 \cdot 4} = \frac{27 + 33}{4} = \frac{60}{4} = 15.$$

Задача 2.22. Найти число различных вариантов раскраски *рёбер* тетраэдра в 2 и 3 цвета.

Решение. Группа $T = \langle t, f \rangle$, $t^3 = f^2 = e$, $|T| = 12$, где

t — вращение на 120° вокруг оси, проходящей через вершину и центр симметрии, 4 оси;

f — вращение на 180° вокруг оси, проходящей через середины противоположных рёбер, 3 оси.

Обозначим через E множество рёбер тетраэдра — $|E| = 6$ — и обозначим их цифрами от 1 до 6, считая, что рёбра 1, 2 и 3 инцидентны одной вершине, а ось вращения, задаваемого элементом f, проходит через середины рёбер 1 и 6.

Найдём цикловой индекс.

$g \in T$	$Type(g)$	$w(g)$	#
$e = (1)\dots(6)$	$\langle 6, 0, \dots \rangle$	x_1^6	1
$t, t^2 = (123)(456)$	$\langle 0, 0, 2, 0, \dots \rangle$	x_3^2	8
$f = (1)(23)(45)(6)$	$\langle 2, 2, 0, \dots \rangle$	$x_1^2 x_2^2$	3
			12

$$P(T \underset{\alpha}{:} E, x_1, \dots, x_6) = \frac{1}{12}\left[x_1^6 + 8x_3^2 + 3x_1^2 x_2^2 \right].$$

$$\#Col(2) = \frac{2^6 + 8 \cdot 2^2 + 3 \cdot 2^4}{3 \cdot 2^2} = \frac{15 + 9 + 12}{3} = 12,$$

$$\#Col(3) = \frac{3^6 + 8 \cdot 3^2 + 3 \cdot 3^4}{3 \cdot 4} = 87.$$

Задача 2.23. Найти число различных вариантов раскраски *рёбер* куба в 2 цвета.

Решение. Цикловой индекс:

$$P(O \underset{\alpha}{:} R) = \frac{1}{24}\big[\, x_1^{12} + 6x_4^3 + 3x_2^6 + 6x_1^2x_2^5 + 8x_3^4 \,\big].$$

$$\#Col(2) = \frac{2^{12} + 6 \cdot 2^3 + 3 \cdot 2^6 + 7 \cdot 2^7}{3 \cdot 2^3} = 218.$$

Задача 2.24. Найти число различных вариантов раскраски *вершин* куба в 2 и 3 цвета.

Решение. Цикловой индекс:

$$P(O \underset{\alpha}{:} V) = \frac{1}{24}\big[\, x_1^8 + 6x_4^2 + 9x_2^4 + 8x_1^2x_3^2 \,\big].$$

$$\#Col(2) = \frac{2^8 + 6 \cdot 2^2 + 9 \cdot 2^4 + 2^7}{3 \cdot 2^3} = 23,$$

$$\#Col(3) = \frac{3^8 + 6 \cdot 3^2 + 9 \cdot 3^4 + 8 \cdot 3^4}{3 \cdot 8} = 333.$$

Задача 2.25. Сколькими геометрически различными способами три абсолютно одинаковые мухи могут усесться в вершинах правильного семиугольника, нарисованного на листе бумаги?

Решение. Множество T — вершины семиугольника, на которые действует группа $\mathbb{Z}_7 = \langle\, t \,\rangle$, $t^7 = e$.

$g \in \mathbb{Z}_7$	$Type(g)$	$w(g)$	#
e	$\langle\, 7,\, 0,\, \ldots \,\rangle$	x_1^7	1
$t,\, t^2,\, \ldots,\, t^6$	$\langle\, 0,\, \ldots,\, 0,\, 1 \,\rangle$	x_7	6

Цикловой индекс самодействия $\mathbb{Z}_7$:

$$P_{\mathbb{Z}_7}(x_1,\, \ldots,\, x_7) = \frac{1}{7}\big[\, x_1^7 + 6x_7 \,\big] = \frac{1}{7}\sum_{d|7} \varphi(d) x_d^{7/d}.$$

Число различных раскрасок в 2 цвета (муха есть/нет), при условии окраски ровно 3 вершин из 7 есть коэффициент u_3 при y^3 после подстановки $x_1 \mapsto y+1,\ x_7 \mapsto y^7+1$ в $P_{\mathbb{Z}_7}$:

$$P(y) = \frac{1}{7}\left[\,(y+1)^7 + 6(y+1)\,\right] = \frac{1}{7}\left[\,\ldots + C_7^3 y^3 + \ldots\,\right].$$

$$u_3 = \frac{7!}{7\cdot 3!\cdot 4!} = \frac{5\cdot 6}{2\cdot 3} = 5.$$

Задача 2.26. Боковые грани правильной 6-угольной пирамиды окрашиваются в красный, синий и зелёный цвета. Определить

(а) число различных 2- и 3-цветных пирамид;
(б) число пирамид с одной красной гранью;
(в) число пирамид, у которых не менее трёх красных граней.

Решение. Имеем транзитивное самодействие $\mathbb{Z}_6$.

(а) *Общее число пирамид.*

$$P(\mathbb{Z}_6) \;=\; \frac{1}{6}\sum_{d|6}\varphi(d)\,x_d^{6/d} \;=\; \frac{1}{6}\left[\,x_1^6 + x_2^3 + 2x_3^2 + 2x_6\,\right].$$

$$\#Col(2) \;= \frac{1}{2\cdot 3}\left[2^6 + 2^3 + 2\cdot 2^2 + 2\cdot 2\right] \;=\; \frac{4\cdot 21}{3} \;=\; 14.$$

$$\#Col(3) \;= \frac{1}{6}\left[3^6 + 3^3 + 2\cdot 3^2 + 2\cdot 3\right] \;=\; \frac{780}{6} \;=\; 130.$$

(б, в) *Число пирамид с* 1 *и* $3 \leqslant$ *красными гранями.* Полагаем $y_1 = y,\ y_2 = y_3 = 1$ (следим за красными гранями), $x_1 = y+2,\ x_2 = y^2+2,\ x_3 = y^3+2.$

$$P(y) = \frac{1}{6}\big[\,(y+2)^6+(y^2+2)^3+2(y^3+2)^2+2(y^6+2)\,\big] =$$
$$= \frac{1}{6}\big[u_0 + u_1 y + u_2 y^2 + \ldots + u_6 y^6\big] =$$
$$= \frac{1}{6}\big[\,\big(2^6 + 2^3 + 2^3 + 4\big) + 6\cdot 2^5 y +$$
$$+ \big(16\cdot 15 + 2\cdot 3\cdot 2^2\big)\, y^2 + \ldots\,\big].$$

$u_0 = 84/6 = 14,\ u_1 = 2^5 = 32,\ u_2 = (240{+}24)/6 = 44.$

Число пирамид с:
(б) одной красной гранью — $u_1 = 32$,
(в) не менее, чем 3 красными гранями — $\#Col(3) - (u_0 + u_1 + u_2) = 130 - (14 + 32 + 44) = 130 - 90 = 40.$

Задача 2.27. Имеются плоские бусины, окрашенные с одной стороны в красный, синий и зелёный цвета. Составляют ожерелья, содержащие по 8 шт. таких бусин в равноотстоящих точках окружности. Определить

а) число различных 3-цветных ожерелий;

б) число ожерелий, у которых не менее трёх красных бусин?

Решение. Здесь везде — транзитивное самодействие циклической группы $\mathbb{Z}_8$.

$D(8) = \{1, 2, 4, 8\},\ \varphi(1) = \varphi(2) = 1,\ \varphi(4) = 2,\ \varphi(8) = 4,$

$$P(\mathbb{Z}_8) = \frac{1}{8}\sum_{d|8} \varphi(d)\, x_d^{8/d} = \frac{1}{8}\big[\,x_1^8 + x_2^4 + 2x_4^2 + 4x_8\,\big].$$

а) *Общее число ожерелий*:

$$\#Col(3) = \frac{3^8 + 3^4 + 2 \cdot 9 + 4 \cdot 3}{8} = 834.$$

б) Подсчитаем *число X ожерелий, в которых число красных бусин не более* 3 (то есть 0, 1 и 2) и вычтем полученное количество из 834.
Полагаем $y_1 = y,\ y_2 = y_3 = 1$ (следим только за бусинами красного цвета).

Найдём коэффициенты u_0, u_1, u_2 при y_0, y_1, y_2 в производящем многочлене W при подстановке $x_k = y^k + 2,\ k = 1, \ldots, 8$.

$$P(\mathbb{Z}_8) = \frac{1}{8}\left[\, x_1^8 + x_2^4 + 2x_4^2 + 4x_8 \,\right]$$

$$W = \frac{1}{8}\left[\, (y+2)^8 + (y^2+2)^4 + 2(y^4+2)^2 + 4(y^8+2) \,\right] =$$
$$= u_0 + u_1 y + u_2 y^2 + \ldots + u_8 y^8 =$$
$$= \frac{1}{2^3}\left[\, (2^8 + 2^4 + 2\cdot 2^2 + 8) + 8\cdot 2^7 y + (C_8^2 \cdot 2^6 + 4 \cdot 2^3) y^2 + \ldots \,\right].$$
$$u_0 = 2^5 + 2 + 1 + 1 = 36, \qquad u_1 = 128,$$
$$u_2 = 28 \cdot 8 + 4 = 224 + 4 = 228.$$

Отсюда $\#Col(3\ \leqslant) = 834 - (36 + 128 + 228) = 834 - 392 = 442$.

Задача 2.28. Грани куба раскрашивают в два цвета — красный и синий. Сколько существует кубов

1) различно окрашенных?
2) у которых не менее 4 граней красные ($\#Col(\geqslant 4)$)?

Решение. Цикловой индекс:

$$P(O \underset{\alpha}{:} F) = \frac{1}{3 \cdot 2^3}\big[\, x_1^6 + \underline{6x_1^2x_4} + 3x_1^2x_2^2 + \underline{6x_2^3} + 8x_3^2 \,\big].$$

1) $\#Col(2) = \dfrac{2^6 + 12 \cdot 2^3 + 3 \cdot 2^4 + 2^5}{3 \cdot 2^3} = \dfrac{30}{3} = 10.$

2) Полагаем $w(1) = y$, $w(2) = 1$,
$x_k = y^k + 1$, $k = \overline{1,6}$.

$$W = \frac{1}{24}\big[\, (y+1)^6 + 6(y+1)^2(y^4+1) + 3(y+1)^2(y^2+1)^2 + \\ + 6(y^2+1)^3 + 8(y^3+1)^2 \,\big].$$

$\#Col(\geqslant 4) = u_4 + u_5 + u_6$ — число кубов с 4, 5 и 6 красными гранями соответственно. Очевидно $u_5 = u_6 = 1$.

Раскрывая W, находим:

$$W = \frac{1}{24}\big[\, \ldots + C_6^4 y^4 + \ldots + 6(y^2+2y+1)(\underline{y^4}+1) + \\ + 3(\underline{y^2}+2y+1)(\underline{y^4}+2\underline{y^2}+1) + \\ + 6(y^6 + 3\underline{y^4} + 3y^2 + 1) + 8(y^6 + 2y^3 + 1) \,\big].$$

$$u_4 = \frac{15+6+9+18}{3 \cdot 8} = \frac{5+2+3+6}{8} = \frac{16}{8} = 2.$$

Итого $\#Col(\geqslant 4) = 1 + 1 + 2 = 4$.

Задача 2.29. Для раскраски сторон квадрата на стеклянной пластинке используют 3 цвета — красный, синий и зелёный. Сколько можно получить

1) разнораскрашенных квадратов?
2) квадратов с 1 красным ребром и не более 2 синих?

Решение. Цикловой индекс:

$$P(D_4) = \frac{1}{8}\left[x_1^4 + 2x_4 + 3x_2^2 + 2x_1^2x_2 \right]$$

$$1)\ \#Col(3) = \frac{1}{8}[3^4 + 2\cdot 3 + 3\cdot 3^2 + 2\cdot 3^2\cdot 3] = \frac{81+6+27+54}{8} = \frac{168}{8} = \frac{87+81}{8} = 21.$$

2) При раскраске в 3 цвета: $x_k = y_1^k + y_2^k + y_3^k,\ k = \overline{1,4}$. Следим только за красным (y_1) и синим (y_2) цветами: $x_k = y_1^k + y_2^k + 1\,,\ k = \overline{1,4}$. Находим $u_{10} + u_{11} + u_{12}$.

$$W = \frac{1}{8}\left[(y_1 + (y_2+1))^4 + 2(y_1^4 + y_2^4 + 1) + \right.$$
$$\left. + 3(y_1^2 + (y_2^2+1))^2 + 2(y_1 + (y_2+1))^2(y_1^2 + y_2^2 + 1) \right] =$$

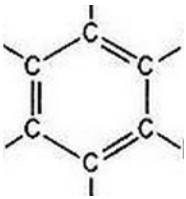
нас интересуют только члены с y_1^1

$$\frac{1}{8}\left[y_1^4 + 4y_1^3(y_2+1) + 6y_1^2(y_2+1)^2 + \underline{4y_1(y_2+1)^3} + (y_2+1) + \dots \right.$$
$$\left. \dots + 2(y_1^2 + \underline{2y_1(y_2+1)} + (y_2+1)^2)(y_1^2 + y_2^2 + 1) \right] =$$
$$= \frac{1}{8}[\dots + 4y_1(y_2+1)^3 + 4y_1(y_2+1)(y_2^2+1))] =$$
$$= \frac{1}{8}\left[\dots + 4y_1(y_2^3 + \underline{3y_2^2 + 3y_2^1 + 1}) + \right.$$
$$\left. + 4y_1(y_2^3 + \underline{y_2 + y_2^2 + 1}) \right] =$$

нас интересуют только члены с y_2^0, y_2^1 и y_2^2 при y_1 (синих рёбер — 0, 1, 2)

$$= \frac{1}{8}\left[4\cdot 7 + 4\cdot 3 \right] = \frac{4\cdot 10}{8} = 5.$$

Задача 2.30. Присоединяя к свободным связям углерода бензольного кольца атомы водорода H или метил CH_3, можно получить молекулы разных веществ (ксилол, бензол и др.).



1) Сколько химически разных молекул можно получить таким путём?

2) Сколько из них молекул с присоединёнными $0, \ldots, 6$ атомами водорода?

Решение. Самодействие группы диэдра D_6.
1) Имеем $D_6 = \langle\, t,\, f,\, s \,\rangle$, $t^6 = f^2 = s^2 = e$, $|D_6| = 12$ — группа диэдра порядка 6, где

t — вращение на 60° вокруг центра квадрата;

f — симметрия относительно прямой, проходящей через середины противоположных сторон (3 оси);

s — симметрия относительно прямой, проходящей через противоположные вершины (3 оси).

Пронумеруем последовательно вершины правильного 6-угольника $1, \ldots, 6$.

Перестановки ниже указаны для случая, когда ось f проходит через середины сторон (2-3) и (5-6), а ось s — через вершины 1 и 4.

$g \in D_6$	перестановка	$Type(g)$	$w(g)$	#
e	$(1)\dots(6)$	$\langle\, 6,\, 0,\, \dots\, 0 \,\rangle$	x_1^6	1
t, t^5	(123456)	$\langle\, 0,\, \dots,\, 0,\, 1 \,\rangle$	x_6^1	2
t^2, t^4	$(135)(246)$	$\langle\, 0,\, 0,\, 2, \dots\, 0 \,\rangle$	x_3^2	2
t^3	$(14)(25)(36)$	$\langle\, 0,\, 3,\, 0, \dots\, 0 \,\rangle$	x_2^3	1
f	$(14)(23)(56)$	$\langle\, 0,\, 3,\, 0,\, \dots\, 0 \,\rangle$	x_3^2	3
s	$(1)(4)(26)(35)$	$\langle\, 2,\, 2,\, 0,\, \dots \,\rangle$	$x_1^2x_2^2$	3
				12

$$P(D_6) = \frac{1}{12}\big[x_1^6 + 2x_6 + 2x_3^2 + 4x_2^3 + 3x_1^2x_2^2\big].$$

Всего молекул — подстановка $x_1 = \dots = x_6 = 2$ (H и метил CH_3):

$$M \;=\; \frac{64+4+8+32+3\cdot 16}{3\cdot 4} \;=\; \frac{39}{3} \;=\; 13.$$

2) *Число молекул с* $0, \dots, 6$ *атомами водорода* — обозначение $y_1 = \mathrm{H}$, $y_2 = 1$
и подстановка $x_k = \mathrm{H}^k + 1$, $k = \overline{1,6}$ в P.

$$\begin{aligned} W \;=\; \frac{1}{12}\big[\,&(\mathrm{H}+1)^6 + 3(\mathrm{H}+1)^2(\mathrm{H}^2+1)^2 + 4(\mathrm{H}^2+1)^3 + \\ &+ 2(\mathrm{H}^3+1)^2 + 2(\mathrm{H}^6+1)\,\big] \;= \\ &= \mathrm{H}^6 + \mathrm{H}^5 + 3\cdot\mathrm{H}^4 + 3\cdot\mathrm{H}^3 + 3\cdot\mathrm{H}^2 + \mathrm{H} + 1\,. \end{aligned}$$

Итого: молекул с числом атомов водорода (как радикала) — $\mathrm{H} = 0$, 1, 5 и 6 — по 1 шт., $\mathrm{H} = 2$, 3 и 4 — по 3 шт., всего — 13.

Задача 2.31. Сколько существует ожерелий из 6 красных и 12 синих бусин?

Решение. Цикловой индекс самодействия группы диэдра (было ранее)

$$P(D_n) = \frac{1}{2n}\sum_{d|n}\varphi(d)x_d^{n/d} + \begin{cases} \frac{1}{2}x_1 x_2^{(n-1)/2}, & n \text{ нечётно}, \\ \frac{1}{4}\left[x_2^{n/2} + x_1^2 x_2^{n/2-1}\right], & n \text{ чётно}, \end{cases}$$

$n = 6 + 12 = 18,\ D(18) = \{1,\ 2,\ 3,\ 6,\ 9,\ 18\},$

$$\begin{array}{lll} \varphi(1) = 1, & \varphi(3) = 2, & \varphi(9) = 6, \\ \varphi(2) = 1, & \varphi(6) = 2, & \varphi(18) = 6. \end{array}$$

По формуле: $P(D_{18}) =$

$$= \frac{1}{36}\left[x_1^{18} + x_2^9 + 2x_3^6 + 2x_6^3 + 6x_9^2 + 6x_{18}^1\right] + \frac{1}{4}\left[x_2^9 + x_1^2 x_2^8\right] =$$

$$= \frac{1}{36}\left[x_1^{18} + 10x_2^9 + 2x_3^6 + 2x_6^3 + 6x_9^2 + 6x_{18}^1 + 9x_1^2 x_2^8\right].$$

$x_k = y^k + 1, \quad W =$

$$= \frac{1}{36}\left[(y+1)^{18} + 10(y^2+1)^9 + 2(y^3+1)^6 + 2(y^6+1)^3 + \right.$$
$$\left. + 6(y^9+1)^2 + 6(y^{18}+1) + 9(y+1)^2(y^8+1)^8\right] =$$
$$= \frac{1}{36}\Big[\ \ldots + \big(C_{18}^6 + 10C_9^3 + 2C_3^1 + 2C_6^2 + 0 + 0 +$$
$$+\ 9(C_8^2 + C_8^3)\big)\, y^6\Big] =$$
$$= \frac{1}{36}\left[\ \ldots + (18654 + 840 + 6 + 30 + 756)y^6\right] =$$
$$= 561y^6. \qquad \textit{Ответ.}\ 561.$$

Задача 2.32. Найти число различных раскрасок рёбер куба в красный и синий цвета с 5 красными рёбрами.

Решение. Ранее был найден цикловой индекс действия группы O на рёбра куба:

$$P(O \underset{\alpha}{:} R) = \frac{1}{24}\left[x_1^{12} + 6x_4^3 + 3x_2^6 + 6x_1^2x_2^5 + 8x_3^4 \right].$$

Проведём подстановку $x_k = y^k + 1$:

$$\begin{aligned} W &= \frac{1}{24}\left[(y+1)^{12} + 6(y^4+1)^3 + 3(y^2+1)^6 + \right. \\ &\quad \left. + 6(y+1)^2(y^2+1)^5 + 8(y^3+1)^4 \right] = \\ &= \frac{1}{24}\left[\ldots + \left(C_{12}^5 + 6C_2^1C_5^2\right) y^5 \right] = \\ &= \frac{1}{24}\left[\ldots + (792 + 6 \cdot 2 \cdot 10)\, y^5 \right] = \ldots + \frac{792+120}{24} = \\ &= \ldots + (33+5)y^5 = \ldots + 38y^5. \end{aligned}$$

Ответ: 38.

Глава 3

Структурный (синтаксический) подход в распознавании образов

3.1 Введение в синтаксический подход к распознаванию образов

Подходы к решению задачи распознавания образов. Объекты характеризуются набором признаков.

1. *Дискриминантный (признаковый) подход.* Признаки образуют метрическое пространство, точки которого соответствуют объектам. Классификация происходит сравнением точки нового объекта с точками прецедентов (объект к объектам).

Методы:

- метрические (kNN, ...);
- разделяющие поверхности (SVM, ...);
- потенциальные функции;
- логические;
- статистические;
- ...

Математический аппарат — метрические теории, логические функции, математическая статистика, дискретная математика ...

При *дискриминантном подходе* необходимо

1) сформировать признаковое пространство;
2) для каждого класса иметь достаточное число прецедентов.

Для распознавания используется информация о взаимном расположении объектов в некотором пространстве признаков (возможно, не совпадающим с исходным). При этом, как правило, игнорируется информация: (1) объект-признак; (2) структурная.

2. *Реляционный подход*. Объекты (и группы объектов) описываются наборами признаков. Классификация происходит сравнением признаков нового объекта с признаками прецедентов.

Классификация происходит сравнением множества признаков нового объекта с признаками прецедентов (признаки к признакам).

Подходы:

1) анализ формальных понятий (АФП, FCA) — формализация понятия в виде пары объём-содержание.
2) статистические методы распознавания;
3) алгебро-информационный подход (см. главу 1);
4) ...

Математический аппарат — теория алгебраических решёток, алгебра логики, теория информации.

3. *Синтаксический (структурный, лингвистический) подход.* Объект описывается набором своих элементарных частей (подобразов), связанных между в соответствии с некоторыми правилами. Признаки объекта — его подобразы и структура их связей. Классификация объекта происходит определением структуры связей его подобъектов.

Разные правила связи подобразов порождают разные классы объектов. Аналогия между структурой объекта и синтаксисом языка даёт возможность использовать аппарат *математической лингвистики.*

При *синтаксическом подходе* необходимо задать правило построения классов из примитивных элементов.

4. *Коллективные решающие правила.* Классификация осуществляется по решающему правилу, учитывающему информацию от элементарных классификаторов (ЭК).

1) голосование по результатам классификации ЭК;
2) разделение признакового пространства на области компетенции классификаторов;
3) алгебра над оценками за класс, выработанных ЭК (алгебраический подход).

5. *Искуственные нейронные сети* — многие из вышеперечисленных задач решаются автоматически, подбором параметров сети.

Синтаксическое распознавание. *Примеры* — распознавание

- *изображений и анализ сцен*: объекты обычно сложны, число требуемых признаков часто велико ⇒ удобство описания их через подобразы;
- *сигналов*: акустических (речь), электрических (ЭКГ, ЭЭГ, ...), электромагнитных (отражённые радиолокационные), оптических (изображения).

Составляющие подхода на примере распознавания/обработки изображений.

1. *Предобработка*:

1.1 Кодирование и аппроксимация — представление в виде, удобном для дальнейшей обработки:

- бинаризация черно-белых изображений,
- дискретизация непрерывного сигнала,
- представление функции конечным набором коэффициентов разложения по некоторой системе функций (Фурье, Уолша, Хаара, Радемахера, ...).

1.2 Фильтрация, восстановление и улучшения объекта — понижение уровня шума, восстановления искажений, улучшения качества.

2. *Построение описания объекта* на основе заранее заданных синтаксических операций:

1) выделение примитивов — элементарных частей объектов;

2) представление объекта в виде композиции примитивов в соответствии с данной структурой.

3. *Синтаксический анализ (грамматический разбор)* — получение синтаксического описания объекта через примитивы — построение дерева грамматического разбора.

Структурный подход обеспечивает высокое быстродействие: распознавание сводится к сравнению символьных описаний структур, а не исходных изображений $\Rightarrow$ преимущество при поиске в больших коллекциях графических документов.

Фильтрация, восстановление и улучшение сигнала — изменение его частотного состава (спектра).

Результат — повышение качества данных $\Rightarrow$ облегчение обнаружения заданных элементов сигнала, изображения.

1. Для обработки дискретных *линейных* сигналов применяют *линейную цифровую фильтрацию*, задаваемую *обобщенным разностным уравнением цифрового фильтра*:

$$y(n) = \sum_{i \in I} b_i x(n-i) + \sum_{j \in J} a_j y(n-j),$$

где $x(n)$ и $y(n)$ — соответственно входной и выходной сигналы,

b_i, a_j — *коэффициенты фильтра*,

I, J — *параметры фильтра*: интервалы $\mathbb{Z}$,

содержащие 0.

Частные случаи:

- $a_j = 0$ для всех $j \in J$ — *нерекурсивный* фильтр, иначе — *рекурсивный*;
- все коэффициенты фильтра суть константы — *фильтр с постоянными коэффициентами*, иначе — *адаптивный*.

Примеры 3.1 (цифровых фильтров).

1. *Сглаживание пятёрками* —

$$y(n) = \frac{1}{5}\big[\,x(n-2)+x(n-1)+x(n)+x(n+1)+x(n+2)\,\big].$$

2. *Фильтр нижних частот* (*фильтр Хемминга*) —

$$y(n) = \frac{1}{8}x(n) + \frac{1}{4}x(n-1) + \frac{1}{4}x(n-2) + \\ + \frac{1}{4}x(n-3) + \frac{1}{8}x(n-4).$$

3. *Сглаживающий дифференциатор* —

$$y(n) = \frac{1}{8}\big[\,x(n-8)+x(n-7)+x(n-6)+x(n-5) - \\ - x(n-3) - x(n-2) - x(n-1) - x(n)\,\big].$$

4. *Численное интегрирование по методу трапеций* —

$$y(n) = y(n-1) + \frac{1}{2}x(n) + \frac{1}{2}x(n-1).$$

2. *Для фильтрации изображений* используют операции, инвариантные ко времени и к изменению положения: *сглаживание*, *повышение контраста*, ...

Основной приём — свёртка с окном $g(x, y)$, определённом на прямоугольнике (u, v) и равном 0 вне его:

$$f(x,y) \mapsto f_g(x,y) = (f * g)(x,y) = \\ = \int\limits_{(u,v)\in D} g(x-u,\, y-v) f(u,v)\, du\, dv \approx \\ \approx \sum_{(u,v)\in D} g(x-u,\, y-v) f(u,v).$$

1) *Сглаживание* — подавление шума, усреднение значений по некоторой окрестности — интегрирование с весом.

Пример:

$$g(x,y) = \frac{1}{|D|}, \quad g(x,y) = \frac{1}{6} \cdot \begin{array}{|c|c|c|}\hline 1/2 & 3/4 & 1/2 \\ \hline 3/4 & 1 & 3/4 \\ \hline 1/2 & 3/4 & 1/2 \\ \hline \end{array}$$

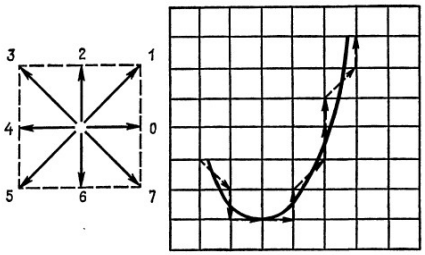
div — коэффициент нормирования, для того чтобы средняя интенсивность оставалась не изменой.

2) *Повышение контраста* — дифференцирование: $\triangle f = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2}$.

$$g_1(x,y) = \begin{array}{|c|c|c|}\hline -1 & -2 & -1 \\ \hline -2 & +12 & -2 \\ \hline -1 & -2 & -1 \\ \hline \end{array}, \quad g_2(x,y) = \begin{array}{|c|c|c|}\hline 0 & -1 & 0 \\ \hline -1 & +5 & -1 \\ \hline 0 & -1 & 0 \\ \hline \end{array}$$

Выделение терминальных элементов: пример
Пример: схема *цепного кодирования*:

- на изображение накладывают сетку и узлы сетки, наиболее близкие к точкам изображения соединяют отрезками прямых;
- каждому полученному отрезку присваивают восьмеричное число.



В результате изображение представляется последовательностью/ями восьмеричных чисел (7600212212).

Свойства цепного кодирования:

- легко выполнимы операция растяжения, определение длины кривой, поиск самопересечений и др.
- применимо для границ произвольной связности.

Метод применялся для распознавания рукопечатного текста, классификации фотографий треков частиц в пузырьковой и искровой камерах, ...

3.2 Языки описания образов

Выбор терминальных элементов — первый этап построения синтаксической модели образов.

Требования к терминальным элементам (примитивам):

- они должны служить основными элементами образов и обеспечивать адекватное описание объекта в терминах заданных структурных отношений;
- их выделение и распознавание должны легко осуществляться.

Эти требования часто противоречат друг другу.
Примеры терминальных элементов:

- для речевых образов — совокупность фонем (звуков, минимальных различимых единиц языка).
- для рукописного текста — штрихи.

Языки и порождающие грамматики

Определение 3.2. *Порождающая грамматика* G есть четверка конечных множеств

$$G = \langle T, N, S, R \rangle,$$

где

T — алфавит *терминальных* символов;
N — алфавит *нетерминальных (вспомогательных)* символов, $T \cap N = \varnothing$;
$S \in N$ — *начальный* (стартовый) символ;

R — совокупность *правил вывода* (подстановок последовательностей символов).

$V = T \cup N$.

A^+ — *транзитивное замыкание алфавита* A, все слова конечной длины без пустого λ, $|\lambda| = 0$,
$A^* = A^+ \cup \lambda$.

Язык $L(G)$, *порождаемый грамматикой* G —

$$L(G) = \{ x \in T^* \mid \exists \text{ вывод } S \Rightarrow x \} \subset T^*.$$

Порождающие грамматики по форме правил подстановки разделены на 4 типа (Н. Хомский, 1957).

Грамматики типа 0 — *неограниченные*
Самый широкий класс: не имеет каких-либо ограничений на правила подстановки.

Пример 3.3. $T = \{ a, b, c \}$, $N = \{ S, A, B \}$

$$R: \quad \begin{array}{ll} S \to aAbc & Ab \to bA \\ Ac \to Bbcc & bB \to Bb \\ aB \to aaA & aB \to \lambda \end{array}$$

Грамматика порождает слова вида

$$x = a^n b^{n+2} c^{n+2},\ n \geqslant 0.$$

$\overline{x} = a^n b^{n+2} c^{n+2},\ n \geqslant 0.$

Вывод слова bbcc:

$$S \Rightarrow aAbc \Rightarrow abAc \Rightarrow abBbcc \Rightarrow aBbbcc \Rightarrow bbcc.$$

Для использования этот класс *слишком широк*.

Грамматики типа 1 — контекстно-зависимые, КЗ.
Правила подстановки — вида $\alpha_1 A \alpha_2 \to \alpha_1 \beta \alpha_2$,
где $A \in N$, $\beta \in V^+$, $\alpha_1, \alpha_2 \in V^*$.

Пример 3.4. $T = \{ a, b, c \}$, $N = \{ S, A, B \}$

$$R: \quad \begin{array}{ll} S \to abc & S \to aAbc \\ Ab \to bA & Ac \to Bbcc \\ bB \to Bb & aB \to aaA \\ aB \to aa & \end{array}$$

Грамматика порождает слова вида $\overline{x} = a^n b^n c^n$, $n \geqslant 1$.

Грамматики типа 2 — контекстно-свободные, КС *(бесконтекстные)*.

Правила подстановки — вида

$$A \to \beta,$$

где $A \in N$, $\beta \in V^+$, т. е. заменяют вспомогательный символ A на непустую цепочку произвольных символов вне зависимости от контекста (окружения) A.

Пример 3.5. $T = \{ a, b \}$, $N = \{ S \}$

$$R: \quad \begin{array}{ll} S \to ab & S \to aSb \end{array}$$

Грамматика порождает слова вида $\overline{x} = a^n b^n$, $n \geqslant 1$.

Грамматики типа 3 — *автоматные (регулярные)*. Имеют правила подстановок вида

$$A \to aB \text{ (или, альтернативно, } A \to Ba) \text{ и } A \to a,$$

где $A \in N$, $B \in N^*$, $a \in T$.

Это самые простые из формальных грамматик: они контекстно-свободны, но с с ограниченным видом правил.

Грамматики типа 3 задают регулярные языки.

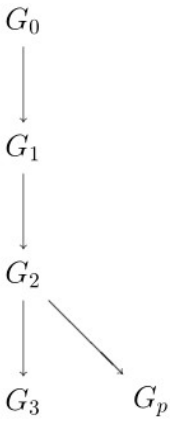


Рис. 3.1. Вложенность возможностей формальных грамматик

Пример 3.6. $T = \{ a, b \}$, $N = \{ S, A \}$

$$R: \quad S \to aA \qquad A \to aA \qquad A \to b$$

Эта грамматика порождает слова вида язык L_0, состоящий из слов вида $\overline{x} = a^n b$, $n \geqslant 1$.

Программные грамматики не входят в иерархию Хомского. В них устаналивается частичный порядок применения правил подстановок символов.

Определение 3.7. *Программная грамматика* G_p есть пятёрка конечных множеств

$$G_p = \langle T, N, S, P, J \rangle,$$

где T, N, S — как в грамматиках Хомского;

P — множество правил вывода;

J — множество *меток* правил: $J = \{ 1, \ldots, m \}$.

Правила вывода из P имеют вид

$$j \quad \alpha \to \beta \quad H \quad F,$$

где $j \in J$ — метка,

$H, F \subseteq J$ — два списка меток переходов при успехе и неудаче соответственно,

$\alpha \to \beta$ — правило подстановки (*ядро*), $\alpha \in T^*NT^*$, $\beta \in T^*$.

Программная грамматика действует следующим образом:

1. Сначала применяется правило с меткой 1.
2. При попытке применить правило j, то если это

   - возможно, оно применяется и выполняется переход к какому-то правилу из списка H;
   - невозможно, выполняется переход к какому-то правилу из списка F.

   Если список меток, к которому происходит обращение, пуст, то ОСТАНОВ.

Программные грамматики ограничивают выбор следующего правила подстановки.

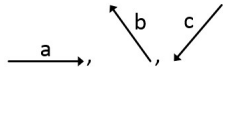
Пример 3.8. Построим автоматную (G_3), бесконтекстную (G_2) и программную (G_p) грамматики, порождающие язык

$$L = \{\, a^n b^n c^n \mid 1 \leqslant n \leqslant 3 \,\}.$$

Все грамматики будут иметь единый алфавит терминальных символов

$$T = \{\ a,\ b,\ c\ \}.$$

Грамматики Хомского, имеющие вид $G = \langle T, N, S, R \rangle$, будут отличаться алфавитами нетерминальных символов N и правилами R. Если считать, что

$T =$ 

и при присоединении элементов T к концу предшествующей стрелки присоединяется начало следующей, то L описывает равносторонние треугольники с длинами сторон 1, 2, 3.

1. *Автоматная грамматика*

$$N = \{\ S,\ A_1,\ A_2,\ B_{10},\ B_{20},\ B_{30},\ B_{21},\ B_{31},\ B_{32},\ C_1,\ C_2,\ C_3\ \}$$

и R:

$$\begin{array}{lll} S \to aA_1 & B_{10} \to bC_1 & B_{32} \to bC_3 \\ S \to aB_{10} & B_{20} \to bB_{21} & C_1 \to c \\ A_1 \to aA_2 & B_{21} \to bC_2 & C_2 \to cC_1 \\ A_1 \to aB_{20} & B_{30} \to bB_{31} & C_3 \to cC_2 \\ A_2 \to aB_{30} & B_{31} \to bB_{32} & \end{array}$$

2. *Бесконтекстная грамматика*

$N = \{\ S,\ A_1,\ A_2,\ B_1,\ B_2,\ B_3,\ C\ \}$ и R:

$$
\begin{array}{lll}
S \to aA_1C & A_1 \to aA_2C & B_2 \to bB_1 \\
A_1 \to b & A_2 \to aB_3C & B_1 \to b \\
A_1 \to aB_2C & B_3 \to bB_2 & C \to c
\end{array}
$$

Бесконтекстная грамматика (G_2) гораздо компактнее автоматной (G_3). Контекстно-зависимая грамматика (G_1) для данного языка не приведена, так как мало отличается от G_2.

3. *Программная грамматика* $G_p = \langle T,\ N,\ S,\ P,\ J \rangle$ $N = \{ S, B, C \}$, $J = \{ 1, \ldots, 5 \}$ и P:

Метка	Ядро	H	F
1	$S \to aB$	$2, 3$	$\varnothing$
2	$B \to aBB$	$2, 3$	$\varnothing$
3	$B \to C$	4	5
4	$C \to bC$	3	$\varnothing$
5	$C \to c$	5	$\varnothing$

Все правила данной грамматики имеют вид $A \to \beta$, $A \in N$, $\beta \in T^*$, такая программная грамматика называется *бесконтекстной*.

Бесконтекстная программная грамматика G_p, описывающая рассматриваемый язык оказалась ещё более компактной, чем бесконтекстная.

3.3 Конечные автоматы и регулярные выражения

Альтернативный к автоматной грамматике способ задания регулярного языка — использование конеч-

ного недетерминированного автомата, *генерирующего* данный язык.

Определение 3.9. *Конечный недетерминированный автомат* есть пятёрка $\widetilde{\mathcal{A}} = \langle X, K, \varphi, P, \psi \rangle$, где:

- X — конечный *выходной* алфавит (символы X *генерируются* автоматом $\widetilde{\mathcal{A}}$),
- K — конечное множество *состояний автомата*,
- φ — предикат на K, определяющий *начальные состояния*,
- ψ — предикат на K, определяющий *финальные состояния*,
- P — предикат на $K \times X \times K$, определяющий многозначную *функцию переходов*:
  если в $(i-1)$-й момент времени автомат находился в состоянии k' и $P(k', x, k) = 1$, то в i-й момент автомат может выдать символ x и перейти в состояние k.

Заметим, что конечные автоматы неполны по Тьюрингу.

Язык $L(\widetilde{\mathcal{A}}) \subset X^*$ *автомата* $\widetilde{\mathcal{A}}$ есть множество слов, которые могут появиться на его выходе. Слово $\overline{x} = x_1 \dots x_n$ принадлежит языку $L(\widetilde{\mathcal{A}})$, если существует такая конечная последовательность $k_0, k_1, \dots, k_n$ состояний $\widetilde{\mathcal{A}}$, что

1) $\varphi(k_0) = 1$ (k_0 — начальное состояние);
2) $P(k_{i-1}, x_i, k_i) = 1$, $i = \overline{1,n}$ (переход $k_{i-1} \to k_i$);

3) $\psi(k_n) = 1$ (k_n — финальное состояние).

Это эквивалентно истинности предиката

$$F(\overline{x}) = \bigvee_{k_0 \in K} \dots \bigvee_{k_n \in K} \varphi(k_0) \,\&\, \overset{n}{\underset{i=1}{\&}} P(k_{i-1},\, x_i,\, k_i) \,\&\, \psi(k_n),$$

где $F(\overline{x})$ — утверждение «*слово* $\overline{x} = x_1 \dots x_n$ *принадлежит языку* $L(\widetilde{\mathcal{A}})$».

Компактная запись предиката $F(\overline{x})$ — в виде матричного произведения. Обозначим:

$\varphi = [\ \varphi_1\ \dots\ \varphi_{|K|}\ ]$ — вектор-строка, $\varphi_k = \varphi(k)$;

$\psi = [\ \psi_1\ \dots\ \psi_{|K|}\ ]^T$ — вектор-столбец, $\psi_k = \psi(k)$;

$P_i = \left\| P(k', x_i, k) \right\|$ — квадратная порядка $|K|$ $(0,1)$-матрица переходов, отвечающая выходному символу x_i, $i = \overline{1,n}$ всего существует $|X|$ таких матриц);

$\otimes$ — матричное произведение с операциями сложения $\vee$ и умножения $\&$.

Тогда

$$F(\overline{x}) = \varphi \otimes \bigotimes_{i=1}^{n} P_i \otimes \psi. \tag{3.1}$$

Сложность вычисления этого предиката — $O(|K|^2 n)$.

Цель распознавания — определить

$$\overline{x} = x_1 \dots x_n \overset{?}{\in} L(\widetilde{\mathcal{A}}).$$

Эту задачу решает *распознающий детерминированный автомат.*

Определение 3.10. *Конечный детерминированный автомат* есть пятёрка $\mathcal{A} = \langle X, K, k_0, q, K' \rangle$, где

X — конечный *входной* алфавит (символы X *подаются на вход* автомата $\mathcal{A}$),

K — конечное множество состояний автомата,

$k_0 \in K$ — начальное состояние,

$q : K \times X \to K$ — *функция переходов*,

$K' \subset K$ — множество финальных состояний.

Если в $(i-1)$-й момент времени автомат $\mathcal{A}$ находился в состоянии k, а в i-й момент на его вход подан символ x, то $\mathcal{A}$ окажется в состоянии $q(k, x)$. Поэтому слово $\overline{x} = x_1 \dots x_n$, поданное на вход $\mathcal{A}$ однозначно определит последовательность его состояний

$$k_0,\ k_1 = q(k_0, x_1),\ \dots,\ k_n = q(k_{i-1}, x_n).$$

Автомат $\mathcal{A}$ распознаёт принадлежность слова $\overline{x}$ языку $L(\mathcal{A})$, если $k_n \in K'$.

Генерирующий автомат как грамматика. Пусть

$$\widetilde{\mathcal{A}} = \langle X, K, \varphi, P, \psi \rangle$$

— генерирующий автомат.

1. Назовём X и K — *терминальным и нетерминальным алфавитами* соответственно.

2. Функцию φ представим в виде подмножества $K^0 = \{ k \in K \mid \varphi(k) = 1 \}$ начальных состояний (*аксиом*).

3. Функции P и ψ выразим в виде подмножеств троек (k', x, k'') и пар (k, x), $k, k', k'' \in K$, $x \in X$ соответственно и будем называть их *правилами вывода*, совокупность которых обозначим R.

   При этом если справедливо $P(k', x, k'') = 1$, то тройку (k', x, k'')

   (a) запишем в виде правила $k' \to xk''$,

   (b) а если при этом справедливо ещё и $\psi(k'') = 1$, то вводим ещё и правило $k' \to x$.

В результате автомат $\widetilde{\mathcal{A}}$ представляется в виде регулярной грамматики как четвёрка

$$G(\widetilde{\mathcal{A}}) = \langle X, K, K^0, R \rangle,$$

которая определяет тот же язык $L \subset X^*$, что и исходный автомат следующим образом:

1) слово, состоящее из *единственного символа*, которое является одной из аксиом и считается выведенным в данной грамматике;

2) если слово $\overline{x}k'$, $\overline{x} \in X^*$, $k' \in K$ выведено и R содержит правило $k' \to x'k''$, то слово $\overline{x}x'k''$ тоже считается выведенным;

3) если слово $\overline{x}k'$, $\overline{x} \in X^*$, $k' \in K$ выведено и R содержит правило $k' \to x'$, то слово $\overline{x}x'$ тоже считается выведенным.

Ясно, что возможен и обратный переход — от регулярной грамматики к автомату.

Недетерминированный конечный автомат и регулярная грамматика — два эквивалентных способа задания регулярных языков.

Регулярные выражения. Введем следующие три операции на множестве языков.

1. *Итерация языка* L есть язык, обозначаемый L^* и определяемый следующим образом:

$$1)\ \lambda \in L^*; \qquad 2)\ \left\{ \begin{array}{l} \overline{x} \in L^*, \\ \overline{y} \in L, \end{array} \right. \Rightarrow\ \overline{x}\,\overline{y} \in L^*.$$

2. *Конкатенация* L_1L_2 *языков* L_1 *и* L_2 есть язык

$$L_1L_2 = \{\ \overline{x}\,\overline{y} \mid \overline{x} \in L_1,\ \overline{y} \in L_2\ \}$$

3. *Объединение* $L_1 \cup L_2$ *языков* L_1 *и* L_2.

Регулярные языки можно также задать с помощью *регулярных выражений* по следующим правилам.

1. $\varnothing$ — регулярное выражение, обозначающее пустое множество слов.
2. $\#$ — регулярное выражение, обозначающее язык, состоящий из единственного пустого слова (нулевой длины).
3. Для каждого символа $x \in X$ запись x — регулярное выражение, обозначающее язык, состоящий из единственного однобуквенного слова x.

4. Если α — регулярное выражение языка L, то $(\alpha)^*$ — регулярное выражение для итерации языка L^*.

5. Если α_1 и α_2 — регулярные выражения языков L_1 и L_2 соответственно, то

   $\alpha_1\alpha_2$ — регулярное выражение для конкатенации L_1L_2,

   α_1, α_2 — регулярное выражение для объединения $L_1 \cup L_2$.

Например, $a(b, c)^*$ — регулярное выражение, задающее множество слов, начинающихся символом a, вслед за которым идёт любая (возможно пустая) последовательность, составленная из символов b и c.

Пример 3.11 (*записи регулярного языка*). Зададим различными эквивалентными способами язык L, состоящий из простейших операторов присваивания. Это множества слов вида

$$\langle \textit{идентификатор} \rangle = \\ = \langle \text{«}\textit{сумма произведений идентификаторов}\text{»} \rangle,$$

в алфавите $X = \{\, a,\ b,\ c,\ +,\ \times,\ = \,\}$.

Здесь *идентификатор* — слово длины $\geqslant 1$, состоящее букв a, b, c:

$$(a, b, c)(a, b, c)^*.$$

1. *Регулярное выражение*:

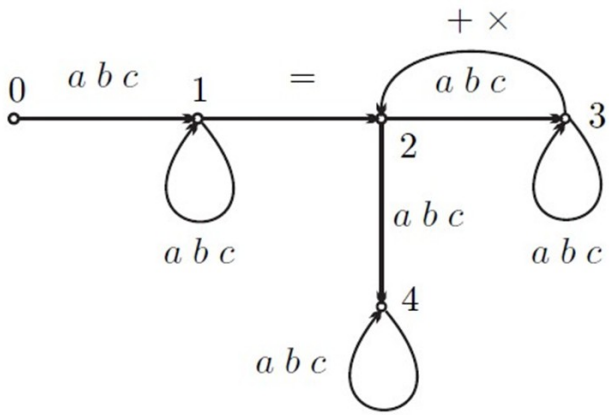
$$(a, b, c)(a, b, c)^* = ((a, b, c)(a, b, c)^*(+, \times))^* (a, b, c)(a, b, c)^*.$$

У всех рассматриваемых ниже автоматов будет единый алфавит

$$T = \{\, a,\ b,\ c,\ =,\ +,\ \times \,\}$$

терминальных символов

2. *Недетерминированный автомат.*
Выходной алфавит — $X = T$, множество состояний $K = \{0, 1, 2, 3, 4\}$ есть множество вершин графа. Начальное состояние — 0, конечное — 4.



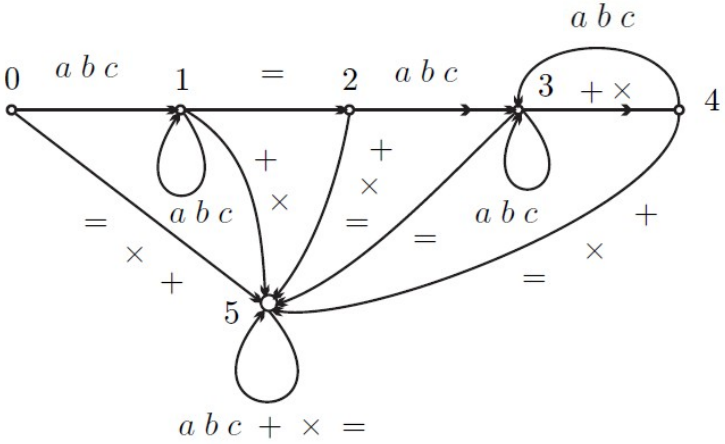
Если стрелке $k' \to k''$ приписан символ x, то $P(k', x, k'') = 1$ (для всех других троек функция $P = 0$), т. е. P принимает значение 1 на следующих тройках:

$(0, a, 1)$, $(0, b, 1)$, $(0, c, 1)$, $(3, a, 3)$, $(3, b, 3)$, $(3, c, 3)$,
$(1, a, 1)$, $(1, b, 1)$, $(1, c, 1)$, $(3, +, 2)$, $(3, \times, 2)$,
$(1, =, 2)$, $(2, a, 4)$, $(2, b, 4)$, $(2, c, 4)$,
$(2, a, 3)$, $(2, b, 3)$, $(2, c, 3)$, $(4, a, 4)$, $(4, b, 4)$, $(4, c, 4)$.

3. *Регулярная грамматика.*
$N = \{\, 0,\ 1,\ 2,\ 3,\ 4 \,\}$, начальный символ $S = 0$, правила R:

$0 \to a1,\ 0 \to b1,\ 0 \to c1,\ \ 3 \to +2,\ 3 \to \times 2,$
$1 \to a1,\ 1 \to b1,\ 1 \to c1,\ \ 2 \to a4,\ 2 \to b4,\ 2 \to c4,$
$1 \to = 2,\qquad\qquad\qquad\ \ 4 \to a4,\ 4 \to b4,\ 4 \to c4,$
$2 \to a3,\ 2 \to b3,\ 2 \to c3,\ \ 4 \to a,\ 4 \to b,\ 4 \to c,$
$3 \to a3,\ 3 \to b3,\ 3 \to c3.$

4. *Детерминированный автомат, распознающий язык* L: Входной алфавит $X = T$, множество состояний $K = \{0, \ldots, 5\}$, начальное состояние — 0, конечное — 3.



Стрелки задают функцию переходов: если стрелка начинается в вершине k', заканчивается в вершине k'' и на ней записан символ x, это обозначает, что $q(k', x) = k''$.

Любое правильное слово автомат переводит в состояние 3, а любое неправильное — в какое-то другое.

При структурном подходе задача распознавания состоит в построении алгоритма, который для любого слова $\overline{x}$ определяет, принадлежит ли оно языку L.

Эта задача не трудна, если регулярный язык выражен с помощью генерирующего автомата: распознающий автомат определяется через множество последовательностей, для которых матричное произведение (3.1) равно 1.

Штрафные автоматы и языки. Для формализации сложных, нечётко определённых понятий (классов), а также вычисления оценок за класс, необходимо задание функции, выражающей степень уверенности принадлежности объекта классу. С этой целью введём понятие *штрафных автоматов и языков*.

Пусть X и K — два конечных множества, а три функции

$$\varphi : K \to \mathbb{R}_{\geqslant 0},$$
$$P : K \times X \times K \to \mathbb{R}_{\geqslant 0},$$
$$\psi : K \to \mathbb{R}_{\geqslant 0}.$$

определяют поведение генерирующего *штрафного автомата* $\mathcal{F}$:

- автомат может начать свою работу в любом состоянии $k \in K$, заплатив при этом штраф $\varphi(k)$;
- если автомат в $(i-1)$-й момент находился в состоянии k', то в i-й момент он может сгенерировать символ $x \in X$ и перейти в состояние k, заплатив штраф $P(k', x, k)$;
- находясь в любом состоянии k, автомат может завершить работу, заплатив штраф $\psi(k)$.

Штрафной язык L_f определяется

1) недетерминированным автоматом

$$\widetilde{\mathcal{F}} = \langle\, X,\, K,\, \varphi,\, P,\, \psi \,\rangle \text{ и}$$

2) числом $\varepsilon \geqslant 0$.

Его составляют те и только слова, штраф за генерирование которых не превосходит ε.

Регулярные языки — собственное подмножество штрафных.

Распознавание принадлежности последовательности $\overline{x} = x_1, x_2, \ldots, x_n$ заданному штрафному языку сводится к вычислению предиката

$$\widetilde{F}(\overline{x}, \varepsilon) \triangleq \min_{k_0} \min_{k_1} \ldots \min_{k_n} \Big\{ \varphi(k_0) + \\ + \sum_{i=1}^{n} P(k_{i-1},\, x_i,\, k_i) + \psi(k_n) \Big\} \leqslant \varepsilon$$

Полукольцо — алгебраическая структура, отличающаяся от кольца отсутствием требования существования *противоположного по сложению* элемента.

Рассмотрим ассоциативно-коммутативное полукольцо $\mathbb{R}_{\min,+}$ над $\mathbb{R}_{>0}$ с операциями сложения $\min$ и умножения $+$.

Обозначим в нем операцию матричного произведения $\odot$. Тогда та же формула запишется как

$$\widetilde{F}(\overline{x}, \varepsilon) \triangleq \varphi \odot \bigodot_{i=1}^{n} P_i \odot \psi \leqslant \varepsilon.$$

Задача остается простой: её формулировка указывает алгоритм решения с вычислительной сложностью $O(|K|^2 n)$.

3.4 Левенштейновская аппроксимация произвольного слова словом из регулярного языка

Введение в проблему. Пусть заданы

- L — регулярный язык, задаваемый генерирующим автоматом $\widetilde{\mathcal{A}} = \langle\, X,\, K,\, \varphi,\, P,\, \psi \,\rangle$;

- $d : X^* \times X^* \to \mathbb{R}_{\geqslant 0}$ — функция *отличия слова* $\overline{x}_2 \in X^*$ *от слова* $\overline{x}_1 \in X^*$.

  Отличие *не обязательно образует метрику* на множестве последовательностей: например, может быть даже несимметричной функцией.

Задача: построить алгоритм, который для каждого слова $\overline{x} \in X^*$ и каждого регулярного языка $L \subset X^*$ вычисляет *отличие слова* $\overline{x}$ *от языка* L — число

$$D(\overline{x}) \;=\; \min_{\overline{y}\,\in\, L} \{\, d(\overline{y},\, \overline{x}) \,\}.$$

Далее рассматривается случай, когда функция d принадлежит классу т. н. *левенштейновских функций*.

Операции редактирования слов. Определим три операции посимвольного редактирования слов и действительные неотрицательные функции их стоимости (все символы $x, x' \in X$, все слова $\overline{x} \in X^*$):

INsert (*вставка*) стоимостью $in(x)$

преобразовывает слово $\overline{x}_1\overline{x}_2$ в слово $\overline{x}_1 x \overline{x}_2$;

CHange (*замена*) стоимостью $ch(x, x')$

преобразовывает слово $\overline{x}_1 x \overline{x}_2$ в слово $\overline{x}_1 x' \overline{x}_2$;

DElete (*исключение*) стоимостью $de(x)$

преобразовывает слово $\overline{x}_1 x \overline{x}_2$ в слово $\overline{x}_1 \overline{x}_2$.

Стоимость последовательности операций есть сумма стоимостей операций, входящих в эту последовательность; стоимость пустой последовательности операций равна 0.

Определение 3.12. Стоимость $d(\overline{x}_1, \overline{x}_2)$ самой дешёвой последовательности редакторских операций, преобразующей $\overline{x}_1 \to \overline{x}_2$ называют *левенштейновым отличием слова* $\overline{x}_2$ *от слова* $\overline{x}_1$.

Пример: чтобы перевести слово КОНЬ в слово КОТ нужно совершить одно удаление и одну замену, поэтому расстояние Левенштейна при составляет при $de(x) = const$ и $ch(x, x') = const$

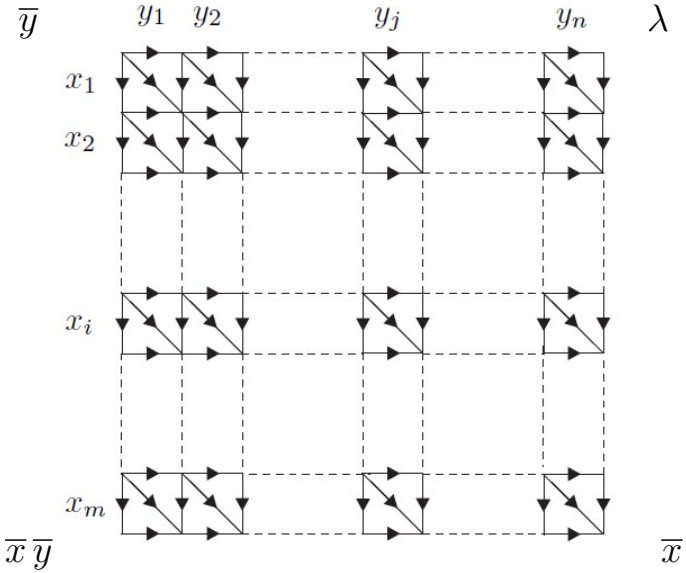
$$de(x) + ch(x, x').$$

Нахождение стоимости $d(\overline{x}_1, \overline{x}_2)$ в общем случае — непростая задача: *существует бесконечное количество последовательностей редакторских операций* преобразования $\overline{x}_1 \to \overline{x}_2$.

Наивный алгоритм вычисления $d(\overline{y}, \overline{x})$**.** Приведём известный и часто применяемый алгоритм вычисления функций Левенштейна, являющийся примером *псевдорешения*.

Пусть $\overline{x} = x_1, \ldots, x_m,\ \overline{y} = y_1, \ldots, y_n \in X^*$.

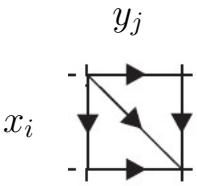
Алгоритм вычисления стоимости $d(\overline{y}, \overline{x})$ преобразования $\overline{y} \to \overline{x}$ зададим на графе $\Gamma_0(\overline{y}, \overline{x})$, в котором рёбра (стрелки) задают множество допустимых путей из левого верхнего угла графа в правый нижний.



Каждому пути соответствует последовательность *редакторских операций* преобразования $\overline{y} \to \overline{x}$ слов: прохождению пути по

- *вертикальной* стрелке в i-й строке соответствует *вставка* символа x_i;
- *горизонтальной* стрелке j-м столбце соответствует *исключение* символа y_j;

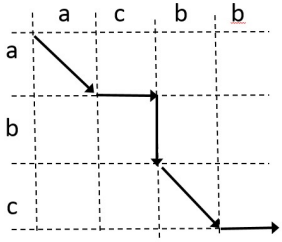
- *диагональной* стрелке в i-й и j-м столбце соответствует *замена* символов $y_j \mapsto x_i$.



i-ой строке приписан i-й символ слова $\overline{x}$.

j-му столбцу приписан j-й символ слова $\overline{y}$.

Пример 3.13. Пусть $X = \{a, b, c\}$.
Преобразуем по данному алгоритму слово $\overline{y} = acbb$ в слово $\overline{x} = abc$ по указанному пути:



Присвоим стрелкам неотрицательные длины, равные стоимости редакторских операций.

Длина каждой стрелки равна

вертикальной в i-й строке — стоимости $in(x_i)$;

горизонтальной в j-м столбце — стоимости $de(y_j)$;

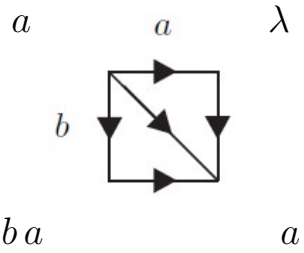
наклонной в i-ой строке и j-ом столбце — стоимости $ch(y_j, x_i)$.

Длина каждого пути есть стоимость последовательности операций, которые этот путь представляет.

Вроде бы: поиск самой дешевой последовательности редакторских операций преобразования $\overline{y} \to \overline{x}$ сводится к поиску кратчайшего пути на графе от верхнего левого угла к правому нижнему.

Покажем *ошибочность* данного предположения.

Пусть в алфавите $X = \{a, b, c, d\}$ даны слова $\overline{x} = b$, $\overline{y} = a$; необходимо вычислить $d(\overline{y}, \overline{x})$.



Решение. По данному графу $\Gamma_0(\overline{y}, \overline{x})$:

$$d(\overline{y}, \overline{x}) = \min\{ ch(a,b),\ de(a)+in(b),\ in(b)+de(a) \}.$$

Но имеется и много других вариантов, например:

$$a \xrightarrow{ch(a,c)} c \xrightarrow{de(c)} \lambda \xrightarrow{in(d)} d \xrightarrow{ch(d,b)} b$$

Граф Γ_0 представляет лишь очень малую часть всех возможных редакторских операций преобразования $a \to b$, и наивный алгоритм решает задачу правильно только в случае, когда Γ_0 содержит самую дешевую последовательность.

Вывод: задача определения левенштейнового отличия слова от заданного языка должна быть строго формализована.

Граф преобразований слов. Левенштейново отличие. Определим бесконечный направленный мультиграф Γ:

- $V(\Gamma) = X^*$;
- $E(\Gamma)$ составляют дуги 3 типов: in, ch и de; при этом две вершины, соответствующие словам вида
  1) $\overline{x}_1\overline{x}_2$ и $\overline{x}_1 x \overline{x}_2$ соединяют дуги типа
     — in длины $in(x)$ от *первой вершины ко второй* и типа
     — de длины $de(x)$ от *второй вершины к первой*;
  2) $\overline{x}_1 y \overline{x}_2$ и $\overline{x}_1 x \overline{x}_2$ соединяют дуги типа
     — ch длины $ch(y, x)$ от *первой вершины ко второй* и длины $ch(x, y)$ от *второй вершины к первой*.

Левенштейново отличие — функция

$$d : X^* \times X^* \to \mathbb{R}_{\geqslant 0},$$

значение которой $d(\overline{y}, \overline{x})$ для пары $\overline{y}, \overline{x}$ есть *длина кратчайшего пути* в Γ от вершины $\overline{y}$ до вершины $\overline{x}$.

Лемма 3.14 (о порядке редакторских операций). *Для любых двух слов $\overline{y}$ и $\overline{x}$ из X^* существует кратчайший путь*

1) *начинающийся последовательностью стрелок типа in,*
2) *за которой следует последовательность стрелок типа ch,*

3) и завершающийся последовательностью стрелок типа de,

причём любая из этих последовательностей может быть пустой.

Доказательство. Пусть

$$\overline{y},\ \overline{x}_1,\ \overline{x}_2,\ \ldots,\ \overline{x}_n,\ \overline{x}$$

— кратчайший путь от вершины $\overline{y}$ к вершине $\overline{x}$, который не обладает указанным свойством, что обнаруживается при последовательных переходах от $\overline{x}_{i-1}$ к $\overline{x}_i$ и от $\overline{x}_i$ к $\overline{x}_{i+1}$:

$$\overline{x}_{i-1} \xrightarrow{1} \overline{x}_i \xrightarrow{2} \overline{x}_{i+1}.$$

Это может произойти только в 3-х следующих ситуациях.

1. Дуга 1 имеет тип ch, а дуга 2 — тип in.

Пусть операция CHange заменяет в $\overline{x}_{i-1}$ символ x на x', а операция INsert вставляет в $\overline{x}_i$ символ x''.

Ясно, что можно поменять последовательность операций: сначала вставить в символ x'', а затем заменить символ x на x'; при этом результат $\overline{x}_{i+1}$ не изменится.

2. Дуга 1 имеет тип de, а дуга 2 — тип in.

Пусть операция DElete исключает из $\overline{x}_{i-1}$ символ x, а операция INsert вставляет в $\overline{x}_i$ символ x'.

Ясно, что можно поменять последовательность операций: сначала вставить в символ x', а затем исключить символ x; при этом результат $\overline{x}_{i+1}$ не изменится.

3. Дуга 1 имеет тип de, а дуга 2 — тип ch.

Это возможно в двух случаях:

$$\begin{cases} \overline{x}_{i-1} &= \overline{x}'x\overline{x}''y\overline{x}''', \\ \overline{x}_i &= \overline{x}'\overline{x}''y\overline{x}''', \\ \overline{x}_{i+1} &= \overline{x}'\overline{x}''z\overline{x}''', \end{cases} \quad \text{или} \quad \begin{cases} \overline{x}_{i-1} &= \overline{x}'y\overline{x}''x\overline{x}''', \\ \overline{x}_i &= \overline{x}'y\overline{x}''\overline{x}''', \\ \overline{x}_{i+1} &= \overline{x}'z\overline{x}''\overline{x}'''. \end{cases}$$

Заменяем в первом случае вершину $\overline{x}_i$ на $\overline{x}'x\overline{x}''z\overline{x}'''$, а во втором — на $\overline{x}'z\overline{x}''x\overline{x}'''$.

В обоих случаях получим новый путь с той же длиной, но в этом пути первая рассматриваемая стрелка будет иметь тип ch, а вторая — тип de.

Рассмотренные изменения последовательности операций возможны, поскольку буквы, над которыми проводятся преобразования — разные.

Поступаем аналогично, меняя последовательность операций: сначала заменяем данный символ в $\overline{x}_{i-1}$ на требуемый, а потом исключаем символ из полученного слова.

Последовательно изменяя путь от $\overline{y}$ до $\overline{x}$ по указанным правилам, найдем путь, в котором ни одна из указанных трех ситуаций не встретится. □

Эквивалентное определение левенштейнова отличия — на основе доказанной леммы.

1. Определим три частных отличия d_{in}, d_{ch} и d_{de} *по построенному кратчайшему пути*: они равны длинам пути по стрелкам соответствующего типа; при $\overline{y} = \overline{x}$ полагаем все отличия равными 0; а если пути по стрелкам данного типа нет, то полагаем соответствующее отличие равным ∞.

2. Введём новые «длинные» стрелки в графе Γ (ранее введённые — «короткие»):

- если слово $\overline{x}$ получено из $\overline{y}$ *вставкой* некоторых символов, то введём в граф Γ две длинные стрелки: типа in от $\overline{y}$ до $\overline{x}$ длины $d_{in}(\overline{y}, \overline{x})$ и типа de от $\overline{x}$ до $\overline{y}$ длины $d_{de}(\overline{x}, \overline{y})$;
- если слово $\overline{x}$ и $\overline{y}$ имеют *одинаковую длину*, введём в граф Γ длинную стрелку типа ch от $\overline{y}$ до $\overline{x}$ длины $d_{ch}(\overline{y}, \overline{x})$.

Ясно, что

- длина кратчайшего пути от $\overline{y}$ до $\overline{x}$ по коротким стрелкам равна длине кратчайшего пути по длинным стрелкам,
- и один из этих кратчайших путей содержит не более, чем *три* длинные стрелки типа in, ch и de, идущие друг за другом в указанном порядке.

Математическое представление этого высказывания —

$$d(\overline{y}, \overline{x}) = \min_{\overline{z}_1 \in X^*} \min_{\overline{z}_2 \in X^*} \Big\{ d_{in}(\overline{y}, \overline{z}_1) + \\ + d_{ch}(\overline{z}_1, \overline{z}_2) + d_{de}(\overline{z}_2, \overline{x}) \Big\}$$

ничего не даёт для конструктивного вычисления $d(\overline{y}, \overline{x})$ (двойной перебор по бесконечному множеству), но полезно, так как указывает, что вычисление левенштейнова отличия сводится к отысканию двух вспомогательных слов $\overline{z}_1$ и $\overline{z}_2$, причём $|\overline{y}| \leqslant |\overline{z}_1| = |\overline{z}_2| \geqslant |\overline{x}|$.

Основной результат. Пусть для конечного алфавита X заданы:

1) регулярный язык L как подмножество слов $\overline{x} = x_1, \ldots, x_n$ из X^*, генерируемых автоматом

$$\widetilde{\mathcal{A}} = \langle\, X, K, \varphi, P, \psi \,\rangle;$$

2) три функции in, ch и de на X^*, $(X^*)^2$ и X^* соответственно, определяющие левенштейново отличие слов $d : (X^*)^2 \to \mathbb{R}_{\geqslant 0}$.

Задача нахождения РЛ: создать алгоритм, который для каждого слова $\overline{x} \in X^*$ и каждой шестёрки функций $(\varphi, P, \psi, in, ch, de)$ вычисляет левенштейновское отличие

$$D(\overline{x}) \;=\; \min_{\overline{y} \in L} d(\overline{y}, \overline{x}).$$

Особенности задачи РЛ

Обычно рассматривают многомерные задачи нахождения $\sup_x f(x)$, $x \in G \subseteq X^n$ — оптимизации потерь, задаваемых целевой функцией $f(x)$, в которых

- количество переменных n (может быть и большое) заранее задано, в то время, как в задаче РЛ требуется найти слово $\overline{y}$ с *неизвестной заранее длиной из бесконечного множества*;
- оптимизируемая в задаче РЛ функция $d(\overline{y}, \overline{x})$, представлена не явной формулой, как обычно, а в виде *вспомогательной задачи* её поиска.

Основная задача — оптимизация найденной в результате решения вспомогательной задачи функции $d(\overline{y}, \overline{x})$. Вспомогательная задача сама по себе далеко не тривиальна.

Теорема 3.15 (основной результат по задаче РЛ). *Пусть X и K — два конечных множества, φ и ψ — предикаты на K, P — предикат на $K \times X \times K$, определяющие регулярный язык $L \subset X^*$ как множество слов $x_1, x_2, \ldots, x_n$, для которых истинен предикат*

$$\bigvee_{k_0 \in K} \ldots \bigvee_{k_n \in K} \varphi(k_0) \,\&\, \mathop{\&}_{i=1}^{n} P(k_{i-1}, x_i, k_i) \,\&\, \psi(k_n).$$

Пусть также

$$in : X \to \mathbb{R}, \quad ch : X \times X \to \mathbb{R}, \quad de : X \to \mathbb{R}$$

— три неотрицательные функции, определяющие левенштейновы отличия $d : X^* \times X^* \to \mathbb{R}$ и

$$D(\overline{x}) \;=\; \min_{\overline{y} \in L} d(\overline{y}, \overline{x}). \tag{3.1}$$

Тогда для каждой шестерки функций $(\varphi, P, \psi, in, ch, de)$ существует такая пара предикатов P' и ψ' на $K \times X \times K$ и K соответственно, что равенство

$$D(\overline{x}) \;=\; \min_{k_0 \in K} \ldots \min_{k_n \in K} \Big\{ \varphi(k_0) + \\ + \sum_{i}^{n} P'(k_{i-1}, x_i, k_i) + \psi'(k_n) \Big\}.$$

выполняется для любого слова $x_1 x_2 \ldots x_n \in X^*$.

Следствия и выводы

- Вычисление числа $D(\overline{x})$ по (3.1), вопреки всей сложности его определения, имеет сложность $O(|K|^2 n)$ что и при распознавании принадлежности слова $\overline{x}$ обыкновенному, не штрафному, регулярному языку.

- Суммарная сложность определения $\overline{y} \stackrel{?}{\in} L$ и вычисления $d(\overline{y}, \overline{x})$ имеет порядок

$$O\left(|K|^2|\overline{y}| + |\overline{y}||\overline{x}|\right).$$

Т.е. вычисление $D(\overline{x})$ имеет сложность $O\left(|K|^2|\overline{x}|\right)$, которая не зависит от $|\overline{y}|$, на которой достигается минимум, и более того, меньше, чем сложность вычисления числа $d(\overline{y}, \overline{x})$ для некоторых слов $\overline{y} \in L$.

Эти вытекающие из теоремы замечательные свойства априори неправдоподобны.

- *Редакционным предписанием* называется последовательность действий, необходимых для получения из первой строки второй кратчайшим образом. К рассмотренным действиям (вставить, заменить, удалить) добавляют MATch — совпадение.

  Найти только расстояние Левенштейна — более простая задача, чем найти ещё и редакционное предписание.

- Если к списку разрешённых операций добавить транспозицию (два соседних символа меняются

местами), приходим к понятию *расстояния Дамерау—Левенштейна.*

Оно используется

- при анализе текстов: Дамерау показал, что 80% ошибок при наборе текста человеком являются транспозициями;
- в биоинформатике.

Алгоритм конструктивного построения предикатов P' и ψ' может быть найден в книге *М. И. Шлезенгер, В. Главач. Десять лекций по статистическому и структурному распознаванию образов.* Известны издания — К.: Наукова думка и Kluwer Academic Publishers; книга доступна в интернете.

Замечания

1. Алгоритм реализует метод ближайшего соседа в случае, когда L есть регулярный язык, а d — есть функция Левенштейна.

2. Алгоритм требует большого перебора (возможно совместного) по множествам $|K|^3$, $|X|^2$.

3. Известны результаты по левенштейновой аппроксимации не только в рамках регулярных языков, но и в более общем случае контекстно-свободных языков.

Глава 4

Комбинаторные методы в анализе структур

4.1 Комбинаторика в кластеризации

Задача кластерного анализа. Пусть даны l-множество объектов, n-множество их признаков, *матрица информаций* $X_{l\times n}$ и число $k < l$.

Задача кластерного анализа состоит в том, чтобы на основании данных из X разбить множество объектов на k *кластеров* (подмножеств) так, чтобы объекты одного кластера были сходными, а объекты, принадлежащие разным кластерам — не-сходными. При этом разбиение должно удовлетворять некоторому критерию оптимальности — *целевой функции* (функционалу), выражающему уровень желательности данного разбиения.

Прямой метод кластеризации — перебором всевозможных разбиений на кластеры находят доставляющее оптимальное значение целевой функции.

Такая процедура практически выполнима лишь при малых l и k: например, если $l = 9$, $k = 4$ число возможных разбиений равно 7770.

Определение 4.1. Число $S(n, k)$ разбиений n-элементного множества на k *непустых* частей называется *числом Стирлинга II рода*.

Задача: определить значение $S(n, k)$.

Переформулировка задачи в терминах урновой схемы: найти число распределения n *различимых* шаров по k *неразличимым* урнам (ящикам), ни одна из которых *не должна остаться пустой.*

Замечание. Задача «почти наоборот» — найти число w распределений n *неразличимых шаров* по k *различимым урнам*, когда некоторые урны *могут остаться пустыми*, решается легко:

- пронумеруем урны $1, \ldots, k$ (урны различимы) и нарисуем подряд n одинаковых никак не помеченных кружков, обозначающих шары (они неразличимы);
- распределение шаров по урнам будем отмечать вставкой $k-1$ вертикальных штрихов между шарами;
- всего имеется $n+k-1$ мест, из которых $k-1$ занимают отрезки (или n мест — кружки), поэтому
$$w = C_{n+k-1}^{k-1} = C_{n+k-1}^{n}.$$

Энумераторы. Напоминание основных перечислительных правил для двух *независимых друг от друга* событий. Пусть первое событие может реализоваться m способами, а второе — n способами.

Правило суммы: *ровно одно из этих событий* может произойти $m+n$ способами.

Правило произведения: *оба события* могут произойти $m \cdot n$ способами.

Пример 4.2. В группе из 15 студентов и 10 студенток, возможен выбор

старосты — $15 + 10 = 25$ способами;

пары «студент-студентка» — $15 \cdot 10 = 150$ способами.

Определение 4.3. *Энумератором* события называется выражение в котором символы *независимых* исходов соединены

- *взаимоисключающие* — операцией *суммирования*;
- *происходящие совместно* — операцией *произведения*.

Такой выбор удобен тем, что *выполнение комбинаторных правил суммы и произведения обеспечивается свойством дистрибутивности* указанных арифметических операций.

Метод производящих функций — эффективный способ решения комбинаторных задач.

Пусть имеется множество $[n] = \{1, \ldots, n\}$ различимых элементов, из которого берётся m-элементная выборка, порядок элементов в которой не существенен. Нас будет интересовать число таких выборок.

Сопоставим элементам этого множества символы x_1, …, x_n. Каждый элемент может попасть или не попасть в выборку, и эти исходы несовместны. Факт попадания 1-го элемента в выборку обозначим x_1, не попадания — 1. Тогда событие, связанное с 1-м элементом описывается энумератором $1 + x_1$.

Аналогично записываем энумераторы событий включения/не включения в выборку для всех элементов $[n]$. Поскольку получение выборки — совместная реализация указанных событий, получаем, что энумератором события, состоящего в выборке m-подмножества из n-множества будет

$$F(x_1, \ldots, x_n) = (1 + x_1) \cdot (1 + x_2) \cdot \ldots \cdot (1 + x_n).$$

Раскрыв скобки в данной формуле, получим

$$F(x_1, \ldots, x_n) = \sum_{m=0}^{n} \sum_{\substack{n_m \subseteq [n] \\ |n_m| = m}} \prod_{i \in n_m} x_i.$$

Например

$$F(x_1, \ldots, x_4) = (1 + x_1) \cdot \ldots \cdot (1 + x_4) =$$

$$= (x_1x_2x_3x_4) + \overbrace{(x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4)}^{\text{4 произведения по 3 элемента}} +$$

$$+ \underbrace{(x_1x_2 + \ldots + x_3x_4)}_{\text{6 попарных произведений}} + \underbrace{(x_1 + x_2 + x_3 + x_4)}_{\text{4 слагаемых}} + 1.$$

Число мономов вида $\prod_{i \in n_m} x_i$, где n_m — некоторое m-элементное подмножество $[n]$ и будет равно искомому количеству m-выборок. Это число легко определить.

Представив, что элементы множества неразличимы, можем положить $x_1 = \ldots = x_n = x$, и тогда получим, что число указанных мономов есть коэффициент $C_n^m = \frac{n!}{m! \cdot (n-m)!}$ при x^m в разложении

$$(1 + x)^n = \sum_{m=0}^{n} C_n^m \, x^m.$$

Получен известный результат: C_n^m есть число выборок (*без повторений и учёта порядка в них*, или *сочетаний*) m объектов из n-элементного множества.

При этом $(1+x)^n$ есть *производящая функция* (ПФ) для конечной последовательности $C_n^0, \ldots, C_n^n$. Поскольку последовательность конечная, эта ПФ есть полином.

Если порядок элементов в выборке существенен, то число A_n^m таких m-выборок будет, очевидно, в $m!$ раз больше, т. е. $A_n^m = C_n^m \cdot m! = \frac{n!}{(n-m)!}$, и производящей функцией для них будет

$$(1+x)^n = \sum_{m=0}^{n} A_n^m \frac{x^m}{m!}.$$

Это пример *экспоненциальной производящей функции* (ЭПФ), точнее — полинома.

Выборки и размещения: различные случаи

1. *Выборки из n-множества объёма m с повторениями и с учётом порядка*

1) Пусть $n = 1$. Тогда имеется одна такая выборка и ЭПФ последовательности $(1, 1, \ldots)$ данных выборок будет

$$1 + x + 1 \cdot \frac{x^2}{2!} + \ldots + 1 \cdot \frac{x^m}{m!} + \ldots = e^x.$$

2) При $n > 1$ таких выборок будет n^m, а ЭПФ последовательности $(1, n, n^2, \ldots)$ —

$$\left(1 + x + \frac{x^2}{2!} + \ldots + \frac{x^m}{m!} + \ldots\right)^n = e^{xn} = \sum_{m \geqslant 0} n^m \frac{x^m}{m!}.$$

3) Пусть теперь *каждый элемент должен быть выбран не менее одного раза*: ЭПФ чисел таких выборок —

$$\left(x+\frac{x^2}{2!}+\ldots\right)^n=(e^x-1)^n \overset{\text{бином Ньютона}}{=} \sum_{j=0}^{n} C_n^j(-1)^j e^{(n-j)x} =$$

$$=\sum_{j=0}^{n} C_n^j(-1)^j \sum_{m\geqslant 0}\frac{(n-j)^m x^m}{m!} =$$

$$=\sum_{m\geqslant 0}\frac{x^m}{m!}\underbrace{\left(\sum_{j=0}^{n} C_n^j(-1)^j(n-j)^m\right)}_{\text{число таких выборок}}.$$

Это не то, что нам нужно (разбиение множества из n *различимых* элементов на $k=m$ *непустых* частей *без учёта порядка* в этих частях и самих частей = размещение *различимых* шаров по *неразличимым* урнам, пустых урн нет), но пригодится...

2. *Размещения n различимых шаров по k различимым урнам.*

В задаче *размещения* шаров рассуждаем аналогично (здесь урна выбирается неоднократно).

1) ЭПФ для случая, когда *урна i должна содержать n_i шаров*:

$$(x_1+\ldots+x_k)^n =$$

$$=\sum_{n_1+\ldots+n_k=n}\underbrace{\frac{n!}{n_1!\ldots n_k!}}_{\substack{\text{число таких размещений}=\\ \text{полиномиальный коэффициент}}} x_1^{n_1}\ldots x_k^{n_k}.$$

Например, распределение 21 голосующих в группы по 8, 7 и 6 человек возможно $\frac{21!}{8!\,7!\,6!} = 349\,188\,840$ способами.

2) ЭПФ числа размещений *n различимых шаров в одной урне*, т. е. последовательности $(1, 1, \dots)$ —

$$1 + x + \frac{x^2}{2!} + \dots + \frac{x^n}{n!} + \dots = \sum_{n\geqslant 0} = e^x.$$

3) ЭПФ числа k^n *размещений n различимых шаров в k различимых* урнах (1-й шар – в любой из k урн, 2-й также и т.д., порядок шаров в урне *несущественен*) — для последовательности $(1, k, k^2, \dots)$:

$$\left(1 + x + \frac{x^2}{2!} + \dots\right)^k = e^{kx} =$$

$$= 1 + kx + k^2\frac{x^2}{2!} + \dots + k^n\frac{x^n}{n!} + \dots$$

= числу выборок объёма n с повторениями из k элементов *с учётом порядка в выборке.*

Числа Стирлинга II рода. *Возвращаемся к нашей задаче.*

Утверждение 4.4. *Число $S(n,k)$ способов так распределить $n \geqslant 1$ различимых шаров по k неразличимым урнам (порядок шаров в урнах несущественен), что ни одна урна не оказывается пустой, равно*

$$S(n,k) = \frac{1}{k!}\sum_{j=0}^{k} C_k^j(-1)^j(k-j)^n, \qquad 1 \leqslant k \leqslant n.$$

Доказательство. Если урна одна ($k = 1$), то ЭПФ для последовательности $(0, 1, 1, \ldots)$ при $n = 0, 1, \ldots$ есть

$$x + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!} + \ldots = e^x - 1.$$

Если имеется урн k, то

$$\left(x + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!} + \ldots\right)^k = (e^x - 1)^k \overset{\text{уже вычисляли}}{=}$$

$$= \sum_{n \geqslant 0} \frac{x^n}{n!} \left(\sum_{j=0}^{k} C_k^j (-1)^j (k-j)^n\right).$$

Поскольку урны неразличимы, то

$$S(n, k) = \frac{1}{k!} \sum_{j=0}^{k} C_k^j (-1)^j (k-j)^n$$

— числа Стирлинга II рода. □

Утверждение 4.5 (Числа Стирлинга II рода: рекуррентная формула).

$$S(n, k) = S(n-1, k-1) + k \cdot S(n-1, k), \quad n > 0,\ k > 1.$$

Доказательство. Рассматриваем распределения n шаров по k урнам.

Выделим некоторый шар x. Тогда

1) если x — единственный шар в урне, то число таких распределений столько же, сколько существует распределений оставшихся $n - 1$ шаров по оставшимся $k - 1$ урнам, т. е. $S(n - 1, k - 1)$;

2) если вместе с x в урне имеются и другие шары, то такие распределения могут быть получены добавлением x к любой из k непустых урн, содержащих в сумме $n-1$ шаров, т. е. их всего $k \cdot S(n-1,k)$. □

По определению полагают $S(0,0)=1$.
Ясно, что $S(n,0)=S(n,k)=0$, $k>n>1$.

Числа $S(n,k)$ Стирлинга II рода могут задаваться таблицей:

$n \diagdown k$	1	2	3	4	5	6	7	8
1	1							
2	1	1						
3	1	3	1					
4	1	7	6	1				
5	1	15	25	10	1			
6	1	31	90	65	15	1		
7	1	63	301	350	140	21	1	

Пример. Все $S(4,2)=7$ разбиений 4-элементного множества $\{1,2,3,4\}$ на 2 блока:

$$1 \mid 234,\quad 2 \mid 134,\quad 3 \mid 124,\quad 4 \mid 123,$$
$$12 \mid 34,\quad 13 \mid 24,\quad 14 \mid 23.$$

Утверждение 4.6 (формула суммирования).

$$S(n,k) = \sum_{i=k-1}^{n-1} C_{n-1}^{i} S(i,k-1), \quad k \geqslant 2.$$

Доказательство. Выделим элемент x рассматриваемого n-элементного множества X.

Затем для каждого $j = 0, \ldots, n-k$ выделим из элементов $X \setminus x$ блок размера j — это можно сделать C_{n-1}^{j} способами — и присоединим x к этому блоку.

После этого для каждого j рассмотрим все $S(n-j-1, k-1)$ разбиения оставшегося $(n-j-1)$-элементного множества.

Все вышеописанные ситуации несовместны, т. е. перебирают разные разбиения. Таким образом,

$$S(n,k) = \sum_{j=0}^{n-k} C_{n-1}^{j} S(n-j-1, k-1)\,.$$

Выполняя замену переменной $i = n-j-1$, получаем

$$S(n,k) = \sum_{i=k-1}^{n-1} C_{n-1}^{n-i-1} S(i, k-1) = \sum_{i=k-1}^{n-1} C_{n-1}^{i} S(i, k-1)\,.$$

□

4.2 Числа Белла

Совокупность всех разбиений множества называют его *беллианом*. Количество таких разбиений n-элементного множества (мощность беллиана) —

$$B(n) = \sum_{k=1}^{n} S(n,k), \quad B(0) \stackrel{\text{def}}{=} 1.$$

Величины $B(n)$ называют *числами Белла*. Например, $B(3) = 5$, $B(8) = 4140$.

Эрик Темпл Белл (Eric Temple Bell, 1883–1960) — шотландский математик, работавший в США. Основные труды в области теории чисел. Разрабатывал т.н. «теневое исчисление»

(umbral calculus). Вице-президент Американского математического общества и член Национальной Академии Наук. Писал популярные книги по математике и истории математики, многие из которых стали классическими, а также стихи и под псевдонимом Джон Тэн — научную фантастику.

Беллиан можно рассматривать как ч.у. множество, упорядоченное по включению. Ясно, что это — ранжированное множество, и число элементов ранга k (число Уитни 2-го рода $W(k)$) в беллиане n-множества есть $S(n,k)$.

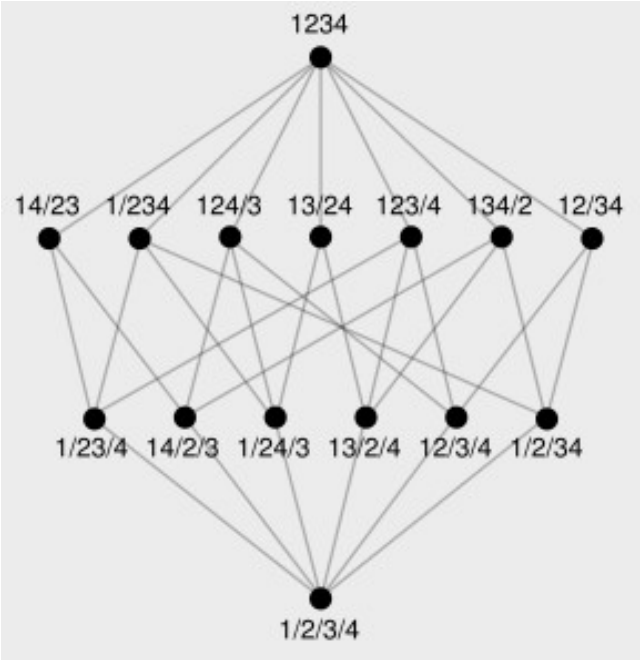


Рис. 4.1. Диаграмма Хассе беллиана множества [4]

.

Утверждение 4.7 (рекуррентная формула).

$$B(n+1) = \sum_{i=0}^{n} C_n^i B(i) = \sum_{i=0}^{n} C_n^i B(n-i).$$

Доказательство. Покажем второе равенство, т.к. первое следует из него в силу симметричности биномиальных коэффициентов.

Выбираем выделенный элемент исходного множества и для $i = 0, \ldots, n$, рассматривая поочерёдно все C_n^i блоков размера i оставшегося n-элементного множества, присоединяя к каждому из них по очереди выделенный элемент.

Для оставшихся $n-i$ элементов рассматриваем их всевозможные разбиения. □

n	0	1	2	3	4	5	6	7	8	9
$B(n)$	1	1	2	5	15	52	203	877	4 140	21 147

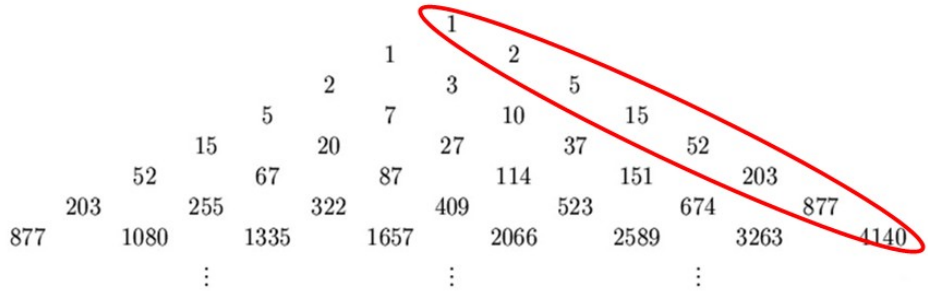
Числа Белла быстро растут.

Числа $B(n)$ могут быть построены при помощи *треугольника Белла*. Первая строка содержит 1, каждая следующая начинается числом, стоящим в конце предыдущей строки, каждое следующее число в строке равно сумме чисел, стоящих *слева* и *слева-сверху* от него. Числа Белла образуют последние числа в строках.

Убывающие факториальные степени:

$$x^{\underline{n}} = \underbrace{x(x-1)(x-2)\ldots(x-n+1)}_{n \text{ сомножителей}}, \quad n \geqslant 0.$$

Рассмотрим два базиса полиномов:



1) стандартный — $1,\ x,\ x^2,\ \ldots,\ x^n,\ \ldots$;
2) из убывающих факториальных степеней —
$$1,\ x^{\underline{1}},\ x^{\underline{2}},\ \ldots,\ x^{\underline{n}},\ \ldots.$$

Выразим обычные степени x^n через убывающие $x^{\underline{n}}$. Несколько первых случаев дают

$$x^0 = x^{\underline{0}}, \qquad x^2 = x^{\underline{2}} + x^{\underline{1}},$$
$$x^1 = x^{\underline{1}}, \qquad x^4 = x^{\underline{4}} + 6x^{\underline{3}} + 7x^{\underline{2}} + x^{\underline{1}}.$$
$$x^3 = x^{\underline{3}} + 3x^{\underline{2}} + x^{\underline{1}}, \quad x^5 = x^{\underline{5}} + 10x^{\underline{4}} + 25x^{\underline{3}} + 15x^{\underline{2}} + x^{\underline{1}}.$$

Замечаем, что коэффициенты в полиномах — числа Стирлинга II рода из приведённой ранее таблицы, прочитанные не слева направо, а справа налево.

Определение 4.8 (чисел Стирлинга II рода, формальное). *Числами Стирлинга II рода* называются числа $S(n,k)$, удовлетворяющие уравнениям

$$x^n = \sum_{k=0}^{n} S(n,k) \cdot x^{\underline{k}},\ n \geqslant 0,$$
$$S(n,0) = 0,\ S(n,n+k) = 0 \ \text{ для } k > 0.$$

Утверждение 4.9.

$$x^n = \sum_{k=0}^{n} S(n,k) \cdot x^{\underline{k}}, \quad n \geqslant 0.$$

Доказательство. Докажем формулу по индукции:

$x \cdot x^{\underline{k}} = x^{\underline{k+1}} + k \cdot x^{\underline{k}}$, так как $x^{\underline{k+1}} = x^{\underline{k}}(x-k)$, следовательно $x^n = x \cdot x^{n-1} = x \sum_k S(n-1,k) \cdot x^{\underline{k}} =$

$$= \sum_k S(n-1,k) \cdot x^{\underline{k+1}} + \sum_k S(n-1,k) k \cdot x^{\underline{k}} =$$
$$= \sum_k S(n-1,k-1) \cdot x^{\underline{k}} + \sum_k S(n-1,k) k \cdot x^{\underline{k}} =$$
$$= \sum_k \big(kS(n-1,k) + S(n-1,k-1)\big) \cdot x^{\underline{k}} = \sum_k S(n,k) \cdot x^{\underline{k}}.$$

Таким образом, числа Стирлинга II рода суть коэффициенты перехода от 2-го базиса к 1-му. □

4.3 Ещё комбинаторные числа

Числа Фибоначчи — элементы последовательности $u = u_0, u_1, \ldots$, определяемые рекуррентным соотношением

$$u_0 = u_1 = 1, \quad u_k = u_{k-1} + u_{k-2}, \ k \geqslant 2.$$

k	0	1	2	3	4	5	6	7	8	9	10	11	12
u_k	1	1	2	3	5	8	13	21	34	55	89	144	233

Справедливо соотношение

$$u_{k+1} u_{k-1} - u_k^2 = (-1)^{k+1}, \ k \geqslant 1. \qquad (4.1)$$

Заметим, что если бы в этом равенстве справа был 0, то оно бы описывало геометрическую прогрессию.

Это означает, что, поскольку последовательность u возрастающая, она асимптотически стремится к некоторой геометрической прогрессии.

Построим ПФ

$$F(x) = \sum_{k\geqslant 0} u_k x^k$$

для последовательности чисел Фибоначчи

$$u_0 = u_1 = 1,\ u_k = u_{k-1} + u_{k-2},\ k \geqslant 2.$$

$$F(x) = 1+x+\sum_{k\geqslant 2} u_k x^k = 1+x+\sum_{k\geqslant 2}(u_{k-1}+u_{k-2})x^k =$$
$$= 1 + x + x\sum_{k\geqslant 2} u_{k-1}x^{k-1} + x^2\sum_{k\geqslant 2} u_{k-2}x^{k-2} =$$
$$= 1 + x + x(F(x) - 1) + x^2F(x)\,.$$

Таким образом

$$F(x) = 1+ \not{x} + xF(x) - \not{x} + x^2F(x)\,,$$
$$F(x)(1 - x - x^2) = 1\,,$$
$$F(x) = \frac{1}{1 - x - x^2}\,.$$

Разлагаем полученную ПФ в ряд по x.

Находим разложение $F(x)$ на простые дроби:

$$1 - x - x^2 = (1 - ax)(1 - bx) = 1 - (a + b)x + abx^2$$
$$\begin{cases} ab = -1, \\ a + b = 1, \end{cases} \quad \Rightarrow$$

a и b — корни $z^2 - z - 1 = 0$, т. е. $a, b = \dfrac{1 \pm \sqrt{5}}{2}$.

Пусть $a \geqslant b$. Тогда

$$a = \frac{1+\sqrt{5}}{2} = \frac{1}{\varphi} = \varphi + 1,\ b = \frac{1-\sqrt{5}}{2} = -\varphi$$

$\varphi \approx 0,61803\ldots$ — золотое сечение. Теперь

$$F(x) = \frac{1}{(1-ax)\cdot(1-bx)} = \frac{A}{1-ax} + \frac{B}{1-bx}.$$

$$A - Abx + B - Bax = 1 \quad \Rightarrow \quad \left\{ \begin{array}{ll} A+B & = 1 \\ Ab+Ba & = 0 \end{array} \right. \quad \Rightarrow$$

$$\Rightarrow \quad A = \frac{a}{a-b}; \qquad B = -\frac{b}{a-b}.$$

Поскольку $\dfrac{1}{1-\alpha x} = \sum\limits_{k\geqslant 0} (\alpha x)^k$, то

$$F(x) = A\sum_{k\geqslant 0} a^k x^k + B\sum_{k\geqslant 0} b^k x^k = \sum_{k\geqslant 0} \frac{a^{k+1}-b^{k+1}}{a-b} x^k\,.$$

Учитывая, что $a - b = \sqrt{5}$, окончательно

$$u_k = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\right].$$

Задание: определите знаменатель геометрической прогрессии, к которой асимптотически стремится последовательность чисел Фибоначчи.

Методом линейных рекуррентных последовательностей было найдено характеристическое уравнение для чисел Фибоначчи:

$$P(x) = x^2 - x - 1 = 0,$$

оно имеет корни $a, b = \frac{1\pm\sqrt{5}}{2}$, и следовательно,

$$u_k = \beta_1 a^k + \beta_2 b^k.$$

Из начальных условий:

$$\begin{cases} \beta_1 + \beta_2 = 1 \\ \beta_1 a + \beta_2 b = 1 \end{cases} \Rightarrow \begin{cases} \beta_1 = \dfrac{1-b}{a-b} = \dfrac{a}{a-b} = A \\ \beta_2 = \dfrac{a-1}{a-b} = \dfrac{-b}{a-b} = B \end{cases}$$

и получаем уже найденную формулу.

Числа Каталана

Задача К-1. *В кассу за билетами стоит очередь из $2n$ человек, у каждого по купюре в 100 или 50 руб., причем этих купюр в очереди поровну — по n 50- и 100-рублевок. Билет стоит 50 руб., в начале продажи касса пуста. Найти число способов расположить очередь так, чтобы кассир всегда мог выдать сдачу.*

Ответ: n-е число Каталана.

Формализуем задачу: закодируем очередь с купюрами двоичным набором, заменяя 50-рублевки единицами, а 100-рублевки — нулями.

Задача К-2. *Найти число различимых двоичных наборов длины $2n$, в которых поровну нулей и единиц, и на любом начальном отрезке каждого такого набора число единиц не менее числа нулей.*

Если бы ограничения не было, то ответом было бы число $C_{2n}^n = \frac{(2n)!}{n!\,n!}$.

Решим задачу перебором для $n = 3$:

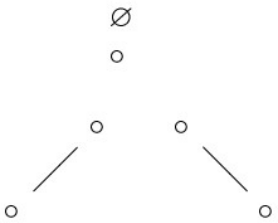
	1	2	3	4	5	6
1)	1	1	1	0	0	0
2)	1	1	0	1	0	0
3)	1	1	0	0	1	0
4)	1	0	1	1	0	0
5)	1	0	1	0	1	0

Задача К-3. *Найти число t_k неизоморфных двоичных деревьев с k вершинами.*

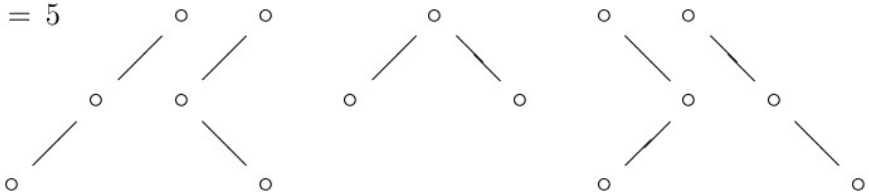
Ответ: это числа Каталана.

t_k =?

$t_0 = 1$
$t_1 = 1$
$t_2 = 2$



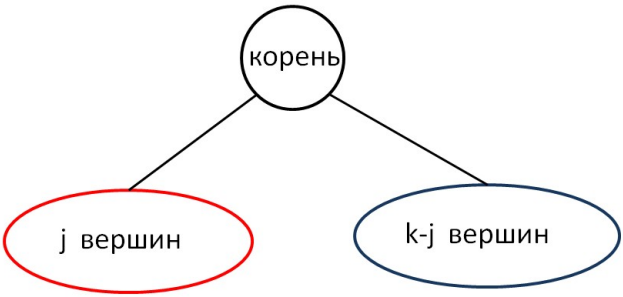
$t_3 = 5$



ПФ для последовательности чисел t_k:

$$C(x) = t_0 + t_1 x + t_2 x^2 + \ldots = \sum_{k \geqslant 0} t_k x^k.$$

Идея: представим ВТ с $k+1$-й вершиной как
корень + левое поддерево + правое поддерево



Отсюда $t_0 = 1,\ t_{k+1} = \sum\limits_{j=0}^{k} t_j t_{k-j},\ k > 0$ и

$$C(x) = 1 + \sum_{k\geqslant 1} t_k x^k = 1 + \sum_{k\geqslant 0} t_{k+1} x^{k+1} =$$

$$= 1 + x \sum_{k\geqslant 0} \Big(\sum_{j=0}^{k} t_j t_{k-j} \Big) x^k = 1 + xC^2(x)$$

— по правилу перемножения рядов:

$$A = \sum_{i\geqslant 0} a_i, \quad B = \sum_{i\geqslant 0} b_i, \qquad A \cdot B = \sum_{i\geqslant 0} \sum_{j=0}^{i} a_j a_{i-j}.$$

Решая квадратное уравнение

$$xC^2(x) - C(x) + 1 = 0,$$

получим

$$C(x) = \frac{1 \pm \sqrt{1-4x}}{2x}. \qquad (*)$$

Разложим $\sqrt{1-4x}$ в ряд:

$$(1-4x)^{1/2} = \sum_{k\geqslant 0} a_k\, x^k.$$

Имеем по биному Ньютона

$$a_0 = 1 \quad \text{и для } k>0: \quad a_k = (-1)^k \binom{1/2}{k} 4^k =$$

$$= \frac{1}{k!}\left(\frac{1}{2}\right)\left(\frac{1}{2}-1\right)\left(\frac{1}{2}-2\right)\ldots\left(\frac{1}{2}-k+1\right)\cdot(-2)^k\cdot 2^k =$$

умножаем на -2 каждую из k скобок

$$= \frac{1}{k!}(-1)(-1+2)(-1+4)\ldots(-1+2k-2)\cdot 2^k =$$

$$= -\frac{1}{k!}\,1\cdot 3\cdot\ldots\cdot(2k-3)\cdot 2^k\,.$$

Таким образом

$$(1-4x)^{1/2} = 1 - \sum_{k\geqslant 1}\frac{1\cdot 3\cdot\ldots\cdot(2k-3)\cdot 2^k}{k!}\cdot x^k =$$

(домножаем числитель и знаменатель на $2\cdot 4\cdot\ldots\cdot(2k-2)$)

$$= 1 - \sum_{k\geqslant 1}\frac{(2k-2)!\cdot 2\cdot 2^{k-1}}{k!\cdot 2\cdot 4\cdot\ldots\cdot(2k-2)}\cdot x^k =$$

(делим числитель и знаменатель на 2^{k-1} и заменим $k! = k\cdot(k-1)!$)

$$= 1 - \sum_{k\geqslant 1}\frac{(2k-2)!\cdot 2}{k\cdot(k-1)!\cdot(k-1)!}\,x^k =$$

$$= 1 - \sum_{k\geqslant 1}\frac{2}{k}\binom{2k-2}{k-1}\,x^k =$$

$$= \left(\text{замена } k\mapsto k+1\right) = 1 - \sum_{k\geqslant 0}\frac{2}{k+1}\binom{2k}{k}\,x^{k+1}\,.$$

Этот ряд надо подставить в $(*)$.

Понятно, что из условия $t_k \geqslant 0$ перед радикалом надо брать знак $(-)$:

$$C(x) = \sum_{k\geqslant 0} \frac{1}{k+1}\binom{2k}{k}x^k \qquad \text{и, таким образом}$$

$$t_k = \frac{1}{k+1}\binom{2k}{k} = \frac{1}{k+1}C_{2k}^k \qquad \textit{— числа Каталана.}$$

Убеждаемся, что $t_3 = \frac{1}{4}\binom{6}{3} = \frac{4\cdot5\cdot6}{1\cdot2\cdot3\cdot4} = 5.$

Замечание. В задаче об очереди в кассу вероятность того, что очередь в кассу *задержится*, равна $\frac{n}{n+1}$ и стремится к единице с ростом её длины.

Эжен-Шарль Каталан (Eugene-Charles Catalan, 1814–1894) — бельгийский математик. Написал более 200 мемуаров. Последовательность чисел Каталана была известна ещё Л. Эйлеру.

n-е число Каталана можно определить как количество —

- правильных скобочных структур длины $2n$;
- неизоморфных упорядоченных бинарных деревьев с корнем и $n+1$ листьями;
- $e(\mathbf{2}\times\mathbf{n})$;
- ...

Во II томе монографии *Р. Стенли* «Перечислительная комбинаторика» приведено 66 различных математических задач, в которых появляются числа Каталана.

4.4 Общая комбинаторная схема

Производящая функция выбора

Мультимножество — обобщение понятия множества, допускающее наличие нескольких экземпляров одного и того же элемента.

Если имеется бесконечное число экземпляров: $\{ *a, *b, 5 * c \}$ — n-элементное мультимножество.

Примеры: у целого числа имеется мультимножество простых множителей, у алгебраического уравнения — мультимножество корней. Пусть имеется n-элементное мультимножество $\{ *a_1, \ldots, *a_n \}$, из которого берётся выборка объёма m. Тогда ПФ такого выбора:

$$F(x_1, \ldots, x_n) = \prod_{i=1}^{n} \sum_{j} \alpha_{ij} x_i^j = \\ = \sum_{m_1+\ldots+m_n=m} u_{m_1,\ldots,m_n} x_1^{m_1} \ldots x_n^{m_n},$$

где

$$\alpha_{ij} = \begin{cases} 1, & \text{если может быть выбрано} \\ & j \text{ экземпляров } i\text{-го объекта} \\ 0, & \text{иначе,} \end{cases}$$

m_i — число выбранных i-х элементов,

$u_{m_1,\ldots,m_n}$ — число соответствующих выборок.

Если выбор элемента i_1 эквивалентен r выборам элемента i_2, то число переменных сокращают, полагая $x_{i_1} = x_{i_2}^r$. Когда все переменные могут быть выражены через одну из них, будем иметь

$$F(x) = \sum_{m \geqslant 0} u_m x^m.$$

Числа Белла, Стирлинга, Каталана и др. могут быть получены как частные случаи данной производящей функции.

Примеры 4.10. 1. Пусть X — обычное n-множество. Тогда каждый элемент может быть либо выбран, либо не выбран, т. е. $\alpha_{i0} = \alpha_{i1} = 1$, $\alpha_{i2} = \alpha_{i3} = \ldots = 0$. Следовательно

$$F(x) = (1 + x_1)(1 + x_2) \ldots (1 + x_n).$$

Если нас интересует только объём выборки m, то полагаем $x_1 = \ldots = x_n = x$ и

$$F(x) = (1 + x)^n = \sum_{m=0}^{n} C_n^m x^m,$$

т. е. таких выборок C_n^m (это мы и так знали).

2. Пусть $X = \{\, 2 * a_1,\ 3 * a_2,\ a_3,\ 4 * a_4 \,\}$.
Найдём число 5-элементных выборок из X.

Пусть u_m — число m-элементных выборок из X, возможны выборки объёма $m = 0, 1, \ldots, 10$.
По общей комбинаторной схеме ПФ таких выборок —

$$\sum_{m=0}^{10} u_m x^m =$$
$$= (1+x+x^2)(1+x+x^2+x^3)(1+x)(1+x+x^2+x^3+x^4) =$$
$$= 1+4x+9x^2+15x^3+20x^4+\underline{22}x^5+20x^6+15x^7+9x^8+$$
$$4x^9 + x^{10}, \qquad \text{и } u_5 = 22.$$

3. Дано мультимножество из n элементов, из которого берётся выборка объёма m, причём каждый элемент м/б выбран *не более* r *раз*, тогда

$$F(x) = (1 + x + \ldots + x^r)^n = \sum_{m=0}^{nr} u_m x^m.$$

4. Если число выбираемых элементов неограничено, то

$$F(x) = \big(1 + x + x^2 + \ldots\big)^n = \frac{1}{(1-x)^n}.$$

Разлагаем данную функцию в ряд, формально рассматривая биномиальные коэффициенты при отрицательных параметрах:

$$\frac{1}{(1-x)^n} = (1-x)^{-n} = \sum_{m\geqslant 0}(-1)^m \binom{-n}{m} x^m = \sum_{m\geqslant 0} u_m x^m.$$

Итого имеем

$$u_m = (-1)^m \binom{-n}{m} \triangleq \left(\!\binom{n}{m}\!\right) =$$
$$= (-1)^m \frac{(-n)(-n-1)\ldots(-n-m+1)}{m!} =$$
$$= \frac{(n+m-1)(n+m-2)\ldots n}{m!} = \binom{n+m-1}{m} =$$
$$= \binom{n+m-1}{n-1} = C^m_{n+m-1} = \overline{C}^m_n.$$

Пусть, например, $n = 3$; $A = \{*a, *b, *c\}$ и $m = 2$. Если бы это было обычное множество, то число выборок —

$$\binom{n}{m} = \binom{3}{2} = 3: \ (a,b),\ (a,c),\ (b,c).$$

Если рассматривается мультмножество, то добавляются (a,a), (b,b), (c,c):

$$\left(\!\binom{n}{m}\!\right) = \left(\!\binom{3}{2}\!\right) = \binom{4}{2} = 6.$$

$\overline{C}_n^m$ есть также и число решений уравнения

$$x_1 + x_2 + \ldots + x_n = m, \quad x_i \in \mathbb{N}_0,\ i = \overline{1,m},$$

порядок слагаемых *существенен*.

Представляем m одинаковых шариков лежащих на прямой в виде n групп, отделяемых друг от друга $n-1$ палочками, и пусть x_i есть число шариков в i-й группе. Вместе палочки и шарики составляют $n+m-1$ предмет, а назначить $n-1$ палочек можно

$$C_{n+m-1}^{n-1} = C_{n+m-1}^{m}, \qquad n \leqslant m$$

способами.

Было: число распределений n неразличимых шаров по $m = k$ различимым урнам, когда некоторые урны могут остаться пустыми —

$$w = C_{n+m-1}^{m-1} = C_{n+m-1}^{n}, \qquad m \leqslant n$$

(почувствуйте разницу ;))

5. В том же мультимножестве из n элементов берётся выборка объёма m, причём каждый элемент д/б выбран хотя бы 1 раз (т. е. $m \geqslant n \geqslant 1$).

ПФ искомых выборок есть

$$F(x) = \sum_{m\geqslant 0} u_m x^m = (x + x^2 + \dots)^n =$$
$$= \big(x(1 + x + x^2 + \dots)\big)^n = x^n(1 + x + x^2 + \dots)^n =$$
$$= x^n \sum_{m\geqslant 0} \left(\!\binom{n}{m}\!\right) x^m = \sum_{m\geqslant 0} \left(\!\binom{n}{m}\!\right) x^{m+n}.$$

Заменяя $m \mapsto m - n$, получаем

$$F(x) = \sum_{m\geqslant n} \left(\!\binom{n}{m-n}\!\right) x^m = \sum_{m\geqslant n} \binom{m-1}{m-n} x^m.$$

Задача о размене монет: сколькими способами можно разменять 1 руб. монетами достоинствами 1, 5, 10 и 50 коп.?

Решение. Строим ПФ представлений суммы в k копеек:

$$F(x) = \sum_{k\geqslant 0} u_k x^k = (1+x_1+x_1^2+\dots)\cdot\dots\cdot(1+x_4+x_4^2+\dots).$$

Учитываем достоинства монет: $x_1 = x$, $x_2 = x^5$, $x_3 = x^{10}$, $x_4 = x^{50}$. Поэтому

$$F(x) = \frac{1}{1-x} \cdot \frac{1}{1-x^5} \cdot \frac{1}{1-x^{10}} \cdot \frac{1}{1-x^{50}}.$$

Нам же нужно лишь значение u_{100}. Поэтому можно действовать следующим образом. Имеем

$$u_0 = u_1 = u_2 = u_3 = u_4 = 1,$$
$$u_5 = u_6 = u_7 = u_8 = u_9 = 2,\ u_{10} = 4.$$

10 коп. $= 10 \cdot 1$ коп. $= 5$ коп.$+5 \cdot 1$ коп. $= 2 \cdot 5$ коп. — итого 4 способа.

Положим

$$A(x) = \frac{1}{1-x} \cdot \frac{1}{1-x^5} \cdot \frac{1}{1-x^{10}} = a_0 + a_1 x + a_2 x^2 + \dots,$$
$$B(x) = \frac{1}{1-x} \cdot \frac{1}{1-x^5} = b_0 + b_1 x + b_2 x^2 + \dots,$$

причём $b_0 = b_1 = \dots = b_4 = 1$ (представление 0, 1, 2, 3 и 4 копеек) и, кроме того,

$$\frac{1}{1-x} = 1 + x + x^2 \dots .$$

Имеем

$$\begin{aligned} A(x) &= (1 - x^{50}) \cdot F(x)\,; \\ B(x) &= (1 - x^{10}) \cdot A(x)\,; \\ \frac{1}{1-x} &= (1 - x^5) \cdot B(x). \end{aligned}$$

Отсюда

$$\begin{cases} a_k = u_k - u_{k-50}\,, & \text{при } k \geqslant 50\,, \\ b_k = a_k - a_{k-10}\,, & \text{при } k \geqslant 10\,, \\ 1 = b_k - b_{k-5}\,, & \text{при } k \geqslant 5\,. \end{cases}$$

Из последнего соотношения: $b_5 = b_{k-5} + 1$, $k \geqslant 5$ и $b_k = \left\lfloor \frac{k}{5} \right\rfloor + 1$, $k \geqslant 0$, т. е.

$$B(x) \doteq (\underbrace{1, 1, 1, 1, 1}_{5 \text{ шт.}}, \underbrace{2, 2, 2, 2, 2}_{5 \text{ шт.}}, \underbrace{3, 3, 3, 3, 3}_{5 \text{ шт.}}, \dots).$$

Аналогично,

$$\begin{cases} u_k = a_k + u_{k-50}\,, & k \geqslant 50\,, \\ a_k = b_k + a_{k-10}\,, & k \geqslant 10\,. \end{cases}$$

Из первого равенства — $u_{100} = a_{100} + a_{50} + u_0$ и далее:

$$\begin{aligned} a_{100} &= b_{100} + b_{90} + \ldots + b_{60} + b_{50} + \ldots + b_{10} + a_0 \\ a_{50} &= b_{50} + b_{40} + \ldots + b_{10} + a_0 \,. \end{aligned}$$

Поскольку $u_0 = a_0 = 1$, имеем

$$\begin{aligned} u_{100} &= b_{100} + b_{90} + b_{80} + b_{70} + b_{60} + \\ &\quad + 2 \cdot (b_{50} + b_{40} + b_{30} + b_{20} + b_{10} + 1) + 1 = \\ &= 21+19+17+15+13+2\cdot(11+9+7+5+3+1)+1 = \\ &= 85 + 2 \cdot 36 + 1 = 86 + 72 = 158. \end{aligned}$$

Замечание. В общем случае, число представлений суммы в k единиц монетами по $r_1, \ldots, r_m$ единиц равно коэффициенту u_k в разложении по x ПФ

$$F(x) = \frac{1}{1 - x^{r_1}} \cdot \ldots \cdot \frac{1}{1 - x^{r_m}} \,.$$

Интерес представляет ПФ

$$F(x) = \frac{1}{1 - x} \cdot \frac{1}{1 - x^2} \cdot \frac{1}{1 - x^3} \cdot \ldots \,.$$

Коэффициент $u_n = p(n)$ разложения этой ПФ в ряд по x называется *числом разбиений* n — это число представлений n в виде суммы положительных целых слагаемых без учёта порядка. Для $p(n)$ *неизвестно выражение в замкнутом виде.*

Для первых значений n имеем

$$p(1) = 1,\ p(2) = 2,\ p(3) = 3,\ p(4) = 5,$$
$$p(6) = 11,\ p(7) = 15 \,.$$

Рамануджан показал, что

$$p(5n+4) \equiv_5 0\,, \quad p(7n+5) \equiv_7 0\,, \quad p(11n+6) \equiv_{11} 0\,.$$

$$p(n) \sim A_n e^{\pi\left(\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right)}$$

$$\text{где } A_n = \frac{1}{2\pi\sqrt{2}}\left(\frac{\pi}{\sqrt{6}\left(n-\frac{1}{24}\right)} - \frac{1}{2\left(n-\frac{1}{24}\right)^{3/2}}\right)$$

$$p(200) = 3\,972\,999\,029\,388 \text{— точное значение}$$

Сринива́са Рамануджа́н Айенго́р (англ. Srinivasa Ramanujan Iyengar, 1887–1920) — математический гений Индии. У него тамильское имя без фамилии: Рамануджан — имя, Сринивaса — отчество, Айенгор — каста. Не имея специального математического образования, доказал справедливость около 120 ранее неизвестных теоретико-числовых формул.

Доказано Рамануджаном:

$$\pi = \frac{9801}{2\sqrt{2}\sum\limits_{k=0}^{\infty}\left(\frac{(4k)!}{(k!)^4}\cdot\frac{1103+26390k}{(4\cdot 99)^{4k}}\right)}\,.$$

Уже при $k=100$ достигается огромная точность — 600 верных значащих цифр!

$$\sqrt{1+2\sqrt{1+3\sqrt{1+4\sqrt{1+\ldots}}}} = 3.$$

$$x^3+y^3+z^3 = w^3, \quad \text{где}$$
$$x = 3a^2+5ab-5b^2, \quad z = 4a^2-4ab+6b^2,$$
$$y = 5a^2-5ab-3b^2, \quad w = 6a^2-4ab+4b^2.$$

Г. Харди прокомментировал результаты Рамануджана: «Они должны быть истинными, поскольку если бы они не были истинными, то ни у кого не хватило бы воображения, чтобы изобрести их». Сам Рамануджан говорил, что формулы ему во сне внушает богиня Намагири Тхайяр.

4.5 Задачи с решениями

Задача 4.1. Показать, что $S(n, n-1) = C_n^2$.

Решение. 1. Из рекуррентного соотношения для чисел Стирлинга II рода

$$S(n,k) = kS(n-1,k) + S(n-1,n-1)$$

следует (подчёркнут итеративный член):

$$S(n,n-1) = \\ = (n-1)\underbrace{S(n-1,n-1)}_{=1} + \underline{S(n-1,n-2)} = \ldots$$

$$\ldots = (n-1) + (n-2) + \ldots + 1 = \frac{n(n-1)}{2} = C_n^2.$$

2. $S(n, n-1)$ есть число способов разместить n помеченных шаров по $n-1$ непомеченным урнам так, чтобы ни одна из урн не оказалось пустой. Ясно, что все урны, кроме одной будут содержать по 1 шару, и единственная урна будет содержать 2 шара. Число способов выбрать 2 шара для помещения в эту урну равно C_n^2.

Задача 4.2. Показать, что $S(n, n-2) = 3C_n^4 + C_n^3$, $n \geqslant 2$.

Решение. Полезная формула суммирования биномиальных коэффициентов *по нижнему индексу*:

$$\sum_{k=0}^{n} C_k^m = C_{n+1}^{m+1}, \qquad C_k^m = 0 \text{ при } m > k.$$

Из рекуррентного соотношения для чисел Стирлинга II рода последовательно получаем (подчёркнут итеративный член):

$$\begin{aligned} S(n,n{-}2) &= (n{-}2)S(n{-}1,n{-}2){+}\underline{S(n-1,n-3)} = \\ &= (n{-}2)C_{n-1}^2{+}(n{-}3)S(n{-}2,n{-}3){+}S(n{-}2,n{-}4) = \\ &= (n-2)C_{n-1}^2 + (n-3)C_{n-2}^2 + \underline{S(n-2,n-4)} = \dots \\ &= \sum_{i=1}^{n-2} C_{n-i}^2(n{-}i{-}\underline{1}) = \sum_{i=1}^{n-2} C_{n-i}^2(n{-}i{-}\underline{2}){+}\sum_{i=1}^{n-2} C_{n-i}^2 . \end{aligned}$$

Имеем далее

$$\begin{aligned} C_{n-i}^2(n-i-2) &= \frac{(n-i)!\,(n-i-2)}{2!(n-i-2)!} = \\ &= \frac{3!}{2!}\cdot\frac{(n-i)!}{3!(n-i-3)!} = 3\cdot C_{n-i}^3. \end{aligned}$$

Затем

$$\sum_{i=1}^{n-2} C_{n-i}^3 = \sum_{i=2}^{n-1} C_i^3 = \sum_{i=0}^{n-1} C_i^3 = C_n^4$$

— второе равенство получено по $C_n^k = 0$ при $n < k$, последнее — по формуле суммирования по нижнему индексу.

Аналогично $\sum_{i=1}^{n-2} C_{n-i}^2 = \sum_{i=2}^{n-1} C_i^2 = C_n^3$ и получаем требуемое.

Задача 4.3. Найти явный вид общего члена последовательности $u_0 = 1$, u_1, u_2, …, удовлетворяющую условиям

$$\sum_{j=0}^{k} u_j u_{k-j} \;=\; 1,\; k \in \mathbb{N}. \qquad (*)$$

Решение. Напоминание:

$$A \;=\; \sum_{i\geqslant 0} a_i\,, \quad B \;=\; \sum_{i\geqslant 0} b_i\,, \quad A\cdot B \;=\; C \;=\; \sum_{k\geqslant 0} c_k,$$

$$c_k \;=\; \sum_{j=0}^{k} a_j b_{k-j} \;-\; \textit{свёртка коэффициентов } a_i \text{ и } b_i\,.$$

Положим $F(x) \;=\; \sum_{k\geqslant 0} u_k\, x^k$. Ясно, что левая часть $(*)$ есть коэффициент при x в $\left(\sum_{k\geqslant 0} u_k\, x^k\right)^2$.

Положим $F(x) \;=\; \sum\limits_{k\geqslant 0} u_k\, x^k$. Тогда по $(*)$

$$F^{\,2}(x) \;=\; 1 + x + x^{\,2} + \ldots \;=\; \frac{1}{1-x}\,.$$

Следовательно,

$$F(x) \;=\; (1-x)^{-1/2} \;=\; \sum_{k\geqslant 0} \binom{-1/2}{k} (-1)^k x^k\,.$$

Находим u_k:

$$\begin{aligned} u_k \;&=\; (-1)^k \binom{-1/2}{k} \;= \\ &=\; (-1)^k \frac{\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)\left(-\frac{5}{2}\right)\ldots\left(-\frac{2k-1}{2}\right)}{k!} \;= \\ &=\; \frac{1\cdot 3\cdot 5\cdot \ldots \cdot (2k-1)}{2^k\, k!} \;=\; \frac{(2k-1)!!}{2^k\, k!}\,. \end{aligned}$$

Задача 4.4. Для последовательности $\left\{\, 2^k + 3^k \,\right\}_{k\geqslant 0}$ найти обычную и экспоненциальную ПФ.

Решение.

- Обычная ПФ:

$$F(x) = \sum_{k\geqslant 0} u_k x^k = \sum_{k\geqslant 0} 2^k x^k + \sum_{k\geqslant 0} 3^k x^k = \\ = \frac{1}{1-2x} + \frac{1}{1-3x} = \frac{2-5x}{1-5x+6x^2}.$$

- Экспоненциальная ПФ:

$$F(x) = \sum_{k\geqslant 0} u_k \frac{x^k}{k!} = \sum_{k\geqslant 0} \frac{2^k x^k}{k!} + \sum_{k\geqslant 0} \frac{3^k x^k}{k!} = e^{2x} + e^{3x}.$$

Задача 4.5. С помощью ПФ доказать тождество

$$C_{2n}^n = \sum_{k=0}^{n} \left(C_n^k\right)^2.$$

Решение.

$$(1+x)^{2n} = (1+x)^n (1+x)^n \Leftrightarrow \\ \Leftrightarrow \sum_{i=0}^{2n} C_{2n}^i x^i = \left(\sum_{k=0}^{n} C_n^k x^k\right)\left(\sum_{m=0}^{n} C_n^m x^m\right).$$

Сравнивая коэффициенты при x^n, получим

$$C_{2n}^n = \sum_{k=0}^{n} C_n^k C_n^{n-k} = \sum_{k=0}^{n} \left(C_n^k\right)^2.$$

Задача 4.6. Найти ПФ для последовательности чётных и нечётных номеров чисел Фиббоначи.

Решение. Пусть $F(x)$ — ПФ для $(u_0, u_1, u_2, u_3 \ldots)$. Тогда $F(-x)$ — ПФ для $(u_0, -u_1, u_2, -u_3 \ldots)$.

Имеем $\dfrac{F(x)+F(-x)}{2}$ — ПФ для $(u_0, 0, u_2, 0 \ldots)$.

Отсюда $\left.\dfrac{F(y)+F(-y)}{2}\right|_{y^2=x}$ — ПФ для $(u_0, u_2, u_4, \ldots)$

и

$\left.\dfrac{F(y)-F(-y)}{2y}\right|_{y^2=x}$ — ПФ для $(u_1, u_3, u_5, \ldots)$.

ПФ для чисел Фиббоначи: $F(x) = \dfrac{1}{1-x-x^2}$.

Имеем

$$\frac{1}{2}\left(\frac{1}{1-y-y^2} + \frac{1}{1+y-y^2}\right) = \frac{1-y^2}{1-3y^2+y^4}\,.$$

$$F(x)_{\text{чётн}} = \frac{1-x}{1-3x+x^2}\,.$$

$$\frac{1}{2y}\left(\frac{1}{1-y-y^2} - \frac{1}{1+y-y^2}\right) = \frac{y}{y\cdot(1-3y^2+y^4)}\,.$$

$$F(x)_{\text{нечётн}} = \frac{1}{1-3x+x^2}\,.$$

Задача 4.7. Вывести формулу для определителя $\triangle_n$ трёхдиагональной матрицы n-го порядка

$$\begin{pmatrix} 3 & 2 & 0 & 0 & \ldots & 0 \\ 1 & 3 & 2 & 0 & \ldots & 0 \\ 0 & 1 & 3 & 2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & 1 & 3 \end{pmatrix}$$

методами производящих функций и линейных рекуррентных последовательностей; считаем, что $\triangle_0 = 1$.

Решение. *1 — методом производящих функций*
Имеем $\triangle_1 = 3$ и $\triangle_{n+1} = 3\triangle_n - 2\triangle_{n-1}$ для $n \geqslant 1$.

Найдём производящую функцию

$$F(x) = \sum_{n\geqslant 0} u_n x^n = 1 + 3x + \sum_{n\geqslant 2} u_n x^n =$$
$$= 1 + 3x + \sum_{n\geqslant 2}(3u_{n-1} - 2u_{n-2})x^n =$$
$$= 1 + 3x + 3x\sum_{n\geqslant 2} u_{n-1}x^{n-1} - 2x^2\sum_{n\geqslant 2} u_{n-2}x^{n-2} =$$
$$= 1 + 3x + 3x(F(x) - 1) - 2x^2F(x) =$$
$$= 1 + 3xF(x) - 2x^2F(x) \Rightarrow$$
$$\Rightarrow F(x)(1-3x+2x^2) = 1 \Rightarrow F(x) = \frac{1}{1 - 3x + 2x^2}\,.$$

$$1 - 3x + 2x^2 = (1 - ax)(1 - bx) = 1 - (a + b)x + abx^2\,.$$
$$\begin{cases} a + b = 3\,, \\ ab = 2\,, \end{cases} \quad \Rightarrow a = 1\,,\ b = 2\,.$$
$$\frac{1}{(1-x)(1-2x)} = \frac{A}{1-x} + \frac{B}{1-2x} \Rightarrow$$
$$\Rightarrow A - 2Ax + B - Bx = 1 \Rightarrow$$
$$\Rightarrow \begin{cases} A + B = 1\,, \\ 2A + B = 0\,, \end{cases} \quad \Rightarrow A = -1\,,\ B = 2\,.$$
$$F(x) = \sum_{n\geqslant 0} u_n\, x^n = \frac{-1}{1-x} + \frac{2}{1-2x} =$$

$$= \sum_{n\geqslant 0}(-1)\,x^n + \sum_{n\geqslant 0} 2(2^n)\,x^n \;=$$

$$= \sum_{n\geqslant 0}(2^{n+1}-1)\,x^n \quad \Rightarrow \quad \triangle_n \;=\; 2^{n+1}-1.$$

2 — *методом л.р.с.*

Соотношение: $\triangle_{n+2} - 3\triangle_{n+1} + 2\triangle_n \;=\; 0.$

Характеристическое уравнение:

$$P(x) = x^2 - 3x + 2 = 0 \;\Rightarrow\; x_1 = 1,\; x_2 = 2.$$

Общее решение: $u_n = \beta_1 + \beta_2 \cdot 2^n.$

Используя начальные условия —

$$\begin{cases} \beta_1 + \beta_2 = 1 \\ \beta_1 + 2\beta_2 = 3 \end{cases} \Rightarrow \begin{cases} \beta_2 = 2 \\ \beta_1 = -1 \end{cases}.$$

Решение: $u_n = 2^{n+1} - 1.$

Задача 4.8. Сколькими способами можно разменять монету 20 коп. монетами по 1, 2, 3 и 5 коп.?

Решение. Строим ПФ по общей комбинаторной схеме.

$$F(\,x_1,\,\ldots x_5) \;=\; (\,1+x_1+x_1^2+\ldots)\cdot(\,1+x_2+x_2^2+\ldots)\cdot$$
$$(\,1+x_3+x_3^2+\ldots)\cdot(\,1+x_4+x_4^2+\ldots) \;=$$

(замена: $x_1 \mapsto x\,, \quad x_2 \mapsto x^2\,, \quad x_3 \mapsto x^3\,, \quad x_4 \mapsto x^5$)

$$= (\,1+x+x^2+\ldots)\cdot(\,1+x^2+x^4+\ldots)\cdot$$
$$(\,1+x^3+x^6+\ldots)\cdot(\,1+x^5+x^{10}+\ldots) \;=$$
$$= \frac{1}{1-x}\cdot\frac{1}{1-x^2}\cdot\frac{1}{1-x^3}\cdot\frac{1}{1-x^5} = \sum_{k\geqslant 0} u_k x^k\,;$$

u_k — число разменов k копеек.

Обозначим

$$A(x) = \frac{1}{1-x}\cdot\frac{1}{1-x^2}\cdot\frac{1}{1-x^3} = \sum_{k\geqslant 0} a_k x^k\,,$$

$$a_0 = a_1 = 1;\ a_2 = 2\,;$$

$$B(x) = \frac{1}{1-x}\cdot\frac{1}{1-x^2} = \sum_{k\geqslant 0} b_k x^k\,,\quad b_0 = b_1 = 1\,;$$

$$C(x) = \frac{1}{1-x} = 1 + x + x^2 + \ldots\,.$$

Непосредственно вычисляется

$$u_0 = u_1 = 1;\ u_2 = 2,\ u_3 = 3;\ u_4 = 4,\ u_5 = 6.$$

Имеем

$$A(x) = \sum_{k\geqslant 0} a_k x^k = (1-x^5)\cdot\sum_{k\geqslant 0} u_k x^k \ \Rightarrow$$

$$\Rightarrow\ u_k - u_{k-5} = a_k\,,\quad k\geqslant 5.$$

Аналогично

$$\begin{cases} a_k - a_{k-3} = b_k\,, & k\geqslant 3\,,\\ b_k - b_{k-2} = 1\,, & k\geqslant 2\,. \end{cases}$$

Или

$$\begin{cases} u_k = a_k + u_{k-5}\,, & k\geqslant 5\,,\\ a_k = b_k + a_{k-3}\,, & k\geqslant 3\,,\\ b_k = 1 + b_{k-2}\,, & k\geqslant 2\,. \end{cases}$$

Из последнего соотношения

$$B(x) \doteq (1,\,1,\,2,\,2,\,3,\,3,\,\ldots)\,,\quad \text{или}\quad b_k = \left\lfloor\frac{k}{2}\right\rfloor + 1.$$

Раскрываем

$$u_{20} = u_{15}+a_{20} = a_{20}+a_{15}+u_{10} = a_{20}+a_{15}+a_{10}+u_5.$$

$$\begin{aligned} a_{20} &= b_{20}+b_{17}+b_{14}+b_{11}+b_8+b_5+a_2 = 44,\\ a_{15} &= b_{15}+b_{12}+b_9+b_6+b_3+a_0 = 27,\\ a_{10} &= b_{10}+b_7+b_4+a_1 = 14. \end{aligned}$$

Окончательно, $u_{20} = 44+27+14+6 = 91.$

Задача 4.9. Найти асимптотику (скорость роста) чисел Каталана t_k при $k \to \infty$.

Решение. Имеем

$$t_k = \frac{1}{k+1}\binom{2k}{k} = \frac{1}{k+1}\cdot\frac{(2k)!}{k!\,k!},$$

и используя формулу Стирлинга $n! \sim \sqrt{2\pi n}\,(n/e)^n$ —

$$t_k \approx \frac{4^k}{k\sqrt{\pi k}}.$$

Глава 5

Случайные графы

5.1 Дискретная вероятность

Обозначения и напоминания

$\lfloor x \rfloor$ — *пол*: $\arg\max\limits_{n \in \mathbb{N}_0} \{\, n \leqslant x \,\}, \qquad 0 \leqslant x;$

$\lceil x \rceil$ — *потолок*: $\arg\min\limits_{n \in \mathbb{N}_0} \{\, x \leqslant n \,\}, \qquad 0 \leqslant x;$

K_n — полный граф на n вершинах;

2^M — булеан (множество всех подмножеств) множества M.

$\mathbf{2}^n$ — конечная булева алгебра с n атомами.

Случайное событие — может произойти или не произойти в результате некоторого испытания (опыта).

$\mathsf{P}[A]$ — вероятность *события* $A \in \{0, 1\}$, $0 \leqslant \mathsf{P}[A] \leqslant 1$.

$$\mathsf{P}[\overline{A}] = 1 - \mathsf{P}[A],$$

$$\mathsf{P}[A + B] = \mathsf{P}[A] + \mathsf{P}[B] - \mathsf{P}[A \cdot B],$$

$$\mathsf{P}\left[\sum_i A_i\right] \leqslant \sum_i \mathsf{P}[A],$$

$$\mathsf{P}[A \cdot B] = \mathsf{P}[A] \cdot \mathsf{P}[B], \text{ если события независимы,}$$
$$= \mathsf{P}[A] \cdot \mathsf{P}[B \mid A] = \mathsf{P}[B] \cdot \mathsf{P}[A \mid B], \text{ иначе.}$$

Если проводится n испытаний по схеме Бернулли с вероятностью единичного успеха p, то вероятность

$P_{\geqslant 1}$ наблюдать хотя бы один успех —

$$P_{\geqslant 1} = 1 - \underbrace{(1-p)^n}_{\substack{\text{вероятность наблюдать} \\ \text{ни одного успеха}}} = np - \frac{n(n-1)}{2}p^2 + \ldots \leqslant np$$

Случайной называется *величина*, которая в результате испытания может принять некоторое возможное значение, *неизвестное заранее*.

Или: случайная величина (с.в.) — функция, заданная на множестве элементарных исходов случайного эксперимента и переводящая их в некоторое множество чисел.

$\mathrm{E}[X]$ — математическое ожидание с.в. X;

$\mathrm{D}[X] = \mathrm{E}[X^2] - (\mathrm{E}[X])^2$ — дисперсия с.в. X.

Неравенство Чебышёва для *неотрицательной* случайной величины X с *конечным* математическим ожиданием $\mathrm{E}[X]$:

$$\mathsf{P}[X \geqslant \varepsilon] \leqslant \frac{\mathrm{E}[X]}{\varepsilon}.$$

Асимптотика при $n \to \infty$.

O: $f(n) = O(g(n)) \Leftrightarrow \left|\frac{f(n)}{g(n)}\right| \leqslant const$
— ограниченность сверху;

Ω: $f(n) = \Omega(g(n)) \Leftrightarrow \left|\frac{f(n)}{g(n)}\right| \geqslant const$
— ограниченность снизу;

Θ: $f(n) = \Theta(g(n)) \Leftrightarrow$ — ограниченность и сверху, и снизу;

o: $f(n) = o(g(n)) \Leftrightarrow \frac{f(n)}{g(n)} \to 0$.

Дискретная случайная величина: определение и примеры

Определение 5.1. Случайная величина называется *дискретной*, если пространство её элементарных исходов (носитель) $\Omega = \{\omega_0, \omega_1, \ldots\}$ не более, чем счётно.

Последовательность $p_0, p_1, \ldots$, где $p_k = \mathsf{P}[\omega_k]$, $k = 0, 1, \ldots$, $\sum_k p_k = 1$, называется *дискретным распределением* или *функцией вероятности*.

Примеры 5.2.

- *Распределение Бернулли* $B(p, q)$: $\Omega = \{0, 1\}$, $p_0 = p$, $p_1 = 1 - p = q$.

- *Биномиальное распределение* $Bi(n, k)$: результат n испытаний по схеме Бернулли с вероятностью $0 < p < 1$ каждое, $q = 1 - p$, $\Omega = \{0, 1, \ldots, n\}$:

$$1 = (p+q)^n = \sum_{k=0}^{n} \underbrace{\binom{n}{k} p^k q^{n-k}}_{p_k}$$

  — вероятность наблюдения k успехов, $0 \leqslant k \leqslant n$.

- *Отрицательное биномиальное распределение* (распределение Паскаля) $NBi(k, p)$: $\Omega = \{0, 1, \ldots\}$, $0 < q < 1$, $p = 1 - q$:

$$1 = \left(\frac{1-q}{1-q}\right)^n = (1-q)^n \cdot \frac{1}{(1-q)^n} =$$

$$= (1-q)^n \cdot \sum_{k\geqslant 0} \overline{C}_n^k q^k = \sum_{k\geqslant 0} \underbrace{\binom{n+k-1}{n-1} p^n (1-p)^k}_{p_k}$$

— распределение дискретной случайной величины равной количеству произошедших неудач в последовательности испытаний Бернулли с вероятностью успеха p, проводимой до n-го успеха; $\overline{C}_n^k$ — см. с. 136.

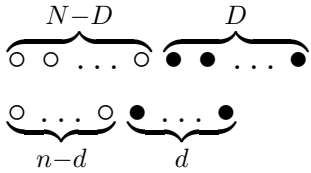
- *Распределение Пуассона* $Po(\lambda)$:
  $\Omega = \{0, 1, \ldots\}$, $\lambda > 0$.

$$1 = e^{-\lambda} e^{\lambda} = e^{-\lambda} \left(1 + \lambda + \frac{\lambda^2}{2!} + \ldots\right) = \sum_{k\geqslant 0} \underbrace{\frac{\lambda^k e^{-\lambda}}{k!}}_{p_k}$$

Вероятность $\mathsf{P}[A]$ случайного события $A \subseteq \Omega$ есть $\sum\limits_{\omega\in A} p(\omega)$.

Классический способ задания вероятностей: количество элементарных исходов конечно и все они имеют одинаковую вероятность. Тогда вероятность любого события при конечном $|\Omega|$ определяется как отношение его мощности к общему числу элементарных исходов.

Пример 5.3. *Гипергеометрическое распределение* $HGe(k; N, D, n)$: имеется множество из N объектов, из которых D дефектных; если из данного множества делается случайная n-выборка, то какова вероятность, что в ней окажется ровно d дефектных объектов?



$N \qquad 0 \leqslant D \leqslant N$

$n \qquad 0 \leqslant d \leqslant n \leqslant N$

$$p_d = \frac{C_{N-D}^{n-d} \cdot C_D^d}{C_N^n}.$$

5.2 Понятие о вероятностном методе

Доказательства в математике:

- *в конструктивных* доказательствах проводится предъявление требуемого объекта или алгоритм его построения;
- *в экзистенциальных* доказательствах доказывается, лишь что объект существует, поскольку является элементом некоторого непустого множества; к ним относятся доказательства с применением вероятностного метода.

Вероятностный метод, предложенный П. Эрдёшем в середине XX в., стал мощным инструментом для решения многих задач дискретной математики. *Идея метода очень проста:*

для доказательства существования объекта с данными свойствами определяют подходящее вероятностное пространство объектов, а затем показывают, что при случайном выборе объекта вероятность наличия у него интересующих свойств строго положительна.

Ясно, что данное вероятностное пространство должно обеспечивать ненулевую вероятность выбора любого своего объекта.

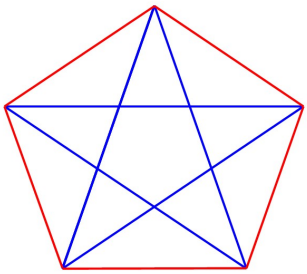
Пал Эрдёш (венг. Erdős Pál, 1913–1996) — венгерский «странствующий математик». Работал в самых разных областях современной математики: комбинаторика, теория графов, теория чисел, математический анализ, теория множеств, теория вероятностей... Количество написанных им научных статей, так же как и число его соавторов не имеет аналогов среди современных математиков.

Его имя носит несколько десятков теорем, гипотез (некоторые из которых были впоследствии доказаны), констант, неравенств, графов, пространств, моделей... Лауреат множества математических наград и основатель *премии Эрдёша*.

Числа Рамсея

Определение 5.4. *Число Рамсея* $R(k,l)$ есть такое наименьшее целое n, что *при любой раскраске ребёр* полного n-вершинного графа в синий и красный цвета существует либо красная клика k-клика, либо синяя клика l-клика.

Гипотеза: $R(3,3) \stackrel{?}{=} 5$.
Т.е. можно ли рёбра полного 5-вершинного графа раскрасить в синий и красный цвета так, чтобы не оказалось ни синего, ни красного треугольника?
Можно: ——⟶, т. е. $R(3,3) \geqslant 6$



Покажем, что $R(3,3) \leqslant 6$, откуда будет следовать, что $R(3,3) = 6$.

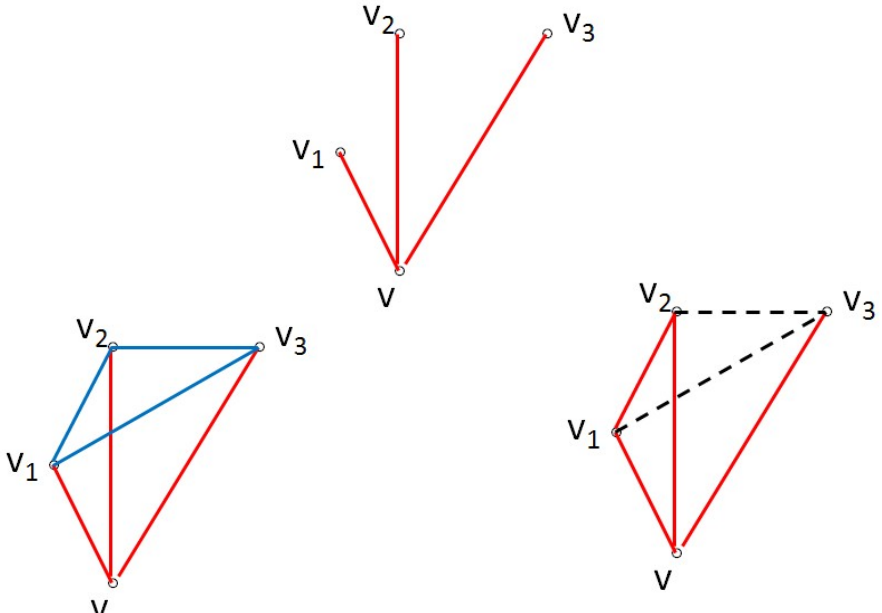
1. Ясно, что любой раскраске рёбер графа K_6 в синий и красный цвета каждой его вершине инцидентна либо не менее 3 синих рёбер, либо не менее 3 красных.

2. Рассмотрим произвольную вершину $v \in V(K_6)$ и пусть ей инцидентно 3 красных ребра (v, v_1), (v, v_2), (v, v_3). Тогда для рёбер (v_1, v_2), (v_2, v_3) и (v_3, v_1) возможны 2 случая:

1) все они синие, и тогда они образуют синий треугольник;

2) хотя бы одно из этих рёбер красное, например, (v_1, v_2), и тогда рёбра (v, v_1), (v_1, v_2), (v_2, v) образуют красный треугольник.

3. Если вершине $v \in V(K_6)$ ей инцидентно 3 синих ребра, рассуждения аналогичны.



Бытовой вариант значения $R(3,3)=6$: в группе из 6 человек любые трое либо знакомы друг с другом, либо друг друга не знают.

Ф. П. Рамсей[1)] показал, что число $R(k,l)$ конечно для любых k и l.

Числа Рамсея трудновычислимы: количество C_n всевозможных 2-раскрасок рёбер полного n-вершинного графа равно $2^{\binom{n}{2}}$, и, например

$$|V(K_{40})| = 40{\cdot}39/2 = 780, \quad C_{40} = 2^{780} \approx 6{,}36{\cdot}10^{234}.$$

Ясно, что $R(1,l)=1$ и $R(2,l)=l$.
Некоторые известные значения $R(k,l)$ и их оценки:

$R(k,l)$	3	4	5	6	7
3	6	9	14	18	23
4	9	18	25	36...41	49...61
5	14	25	**43**...**49**	58...87	80...143
6	18	36...41	58...87	**102**...**165**	113...298

П. Эрдёш и Д. Секереш установили рекуррентное неравенство

$$R(k,l) \leqslant R(k-1,l) + R(k,l-1), \quad k>2,\ l>2,$$

откуда следуют оценки $R(k,l) \leqslant C_{k+l-2}^{k-1}$ и $R(k,k) \leqslant (4-\delta(k))^k$, $\delta(k) \to 0$.

[1)] Фрэнк Пламптон Рамсей (Frank Plumpton Ramsey, 1903–1930) — английский математик, успевший внести также значительный вклад в философию и экономическую науку. Он доказал (1930), что упорядоченные конфигурации неизбежно присутствуют в любой большой структуре.

В статье 1935 г. П. Эрдёш и Д. Секереш переоткрыли числа Рамсея и доказали про них существенно более точные утверждения, чем установленные Ф. П. Рамсеем.

Эрдёш полагал, что в случае крайней необходимости человечество ещё способно найти $R(5,5)$, но не $R(6,6)$. Он нашёл способ получить нижнюю оценку диагональных чисел Рамсея, используя вероятностный метод.

Применение вероятностного метода: нижняя оценка диагонального числа Рамсея

Утверждение 5.5. *Если* $C_n^k \cdot 2^{1-C_k^2} < 1$, *то* $R(k,k) > n$. *Таким образом,* $R(k,k) > \lfloor 2^{k/2} \rfloor$ *для всех* $k \geqslant 3$.

Доказательство. Рассмотрим случайную раскраску ребер графа K_n в красный и синий цвета равновероятно и независимо друг от друга.

Определим для каждой k-клики K_k графа K_n, $k \leqslant n$ событие

$$M(K_k) = 1 \Leftrightarrow \textit{подграф } K_k \textit{ — монохроматический}$$

(или *одноцветный*, все его ребра являются либо являются красными, либо синими).

Ясно, что

$$\mathsf{P}[M(K_k)] = \frac{2}{2^{C_k^2}} = 2^{1-C_k^2} = p_k$$

(два варианта из $2^{C_k^2}$ возможных 2-цветных раскрасок всех C_k^2 рёбер подграфа).

Т. к. существует C_n^k вариантов выбора подграфа K_k, то вероятность $P_{\geqslant 1}$ того, что по крайней мере одно из событий $M(K_k)$ *произойдет* —

$$0 \leqslant \mathsf{P}_{\geqslant 1} = 1 - (1-p_k)^{C_n^k} \leqslant C_n^k \cdot 2^{1-C_k^2} < 1.$$

Тогда вероятность $1-\mathsf{P}_{\geqslant 1}$, что *ни одного такого события не произойдёт* строго положительна, т. е. существует 2-раскраска графа K_n без одноцветных (красных или синих) k-клик и $R(k,k) > n$.

Если $k \geqslant 3$ и $n = \lfloor 2^{k/2} \rfloor$, то

$$C_n^k 2^{1-C_k^2} = \frac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{k!}\cdot 2^{1-k^2/2+k/2} < \\ < \frac{n^k}{k!}\cdot\frac{2^{1+k/2}}{2^{k^2/2}} \leqslant \frac{\not{2}^{k^2/2}}{k!}\cdot\frac{2^{1+k/2}}{\not{2}^{k^2/2}} < 1,$$

следовательно, $R(k,k) > n = \lfloor 2^{k/2} \rfloor$ для всех $k \geqslant 3$. □

Принцип Дирихле: если n кроликов рассажены в k клеток, то гарантировать, что в одной из клеток находится более одного кролика, можно если $n > k$, а если $k > n$, то как минимум одна клетка пуста. Вариант — «принцип голубей и ящиков» (Pigeonhole principle). Теория Рамсея обобщает этот принцип.

Числа Рамсея в общем случае: $R(k_1, k_2; r)$, $2 \leqslant r$ — мощность подмножеств вершин графа, т. е. рассматриваются гиперграфы; у нас $r = 2$.

Фактически теория Рамсея утверждает, что любая большая структура обязательно содержит упорядоченную подструктуру = *полная неупорядоченность невозможна.* Это относится, например, к бесчисленным группам звёзд Вселенной, большой совокупности случайно разбросанных камешков или последовательности чисел, полученных бросанием игральной кости.

Из доказательства $R(k,k) > \lfloor 2^{k/2} \rfloor$, $k \geqslant 3$ следует, что существует реберная 2-раскраска графа K_n *без одноцветных клик* $K_{2\log_2 n}$.

Как найти такую раскраску явно?

Полная проверка *одного* подграфа K_k — $2^{C_k^2} = 2^{k^2/2-k/2}$ вариантов.

Для больших k при $n = \lfloor 2^{k/2} \rfloor$ выполнено

$$C_n^k \cdot 2^{1-C_k^2} < \frac{2^{1+k/2}}{k!} \left(\frac{n}{2^{k^2/2}}\right)^k \leqslant \frac{2^{1+k/2}}{k!} \ll 1,$$

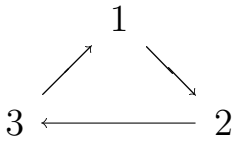
поэтому случайная раскраска графа K_n с большой вероятностью не содержит одноцветных подграфов $K_{2\log_2 n}$.

Применение вероятностного метода: турниры

Определение 5.6. *Турнир* T на множестве из n игроков есть результат ориентации ребер K_n.

Турнир T обладает свойством S_k, *если для каждого* k*-элементного подмножества* игроков найдется хотя бы один игрок, который побеждает их всех — *победитель*.

Например, циклически ориентированный треугольник с $V = \{1, 2, 3\}$ и $E = \{(1, 2), (2, 3), (3, 1)\}$ обладает свойством S_1 (но не S_3!).



Проблема Шютте — верно ли, что для любого конечного k *существует турнир* T *(с более чем* k *вершинами), обладающий свойством* S_k*?*

Случайный турнир — турнир, получаемый из полного графа выбором для каждой пары его вершин u и v независимо и равновероятно либо дуги (u, v), либо дуги (v, u).

При этом все $2^{C_n^2}$ возможных турниров на множестве V равновероятны.

Идея: если n достаточно велико по сравнению с k, то случайный турнир на множестве $V = \{1, \ldots, n\}$ с большой вероятностью обладает свойством S_k.

Теорема 5.7 (Эрдёш, 1963). *Если* $C_n^k \left(1 - 2^{-k}\right)^{n-k} < 1$, *то существует турнир на* n *вершинах, обладающий свойством* S_k.

Доказательство. Рассмотрим случайный турнир на множестве $V = \{1, \ldots, n\}$.

Для каждого k-элементного подмножества вершин $K \subseteq V$ определим событие N_k, состоящее в том, что *не существует* победителя K.

Поскольку для каждой вершины $v \in V \setminus K$ вероятность того, что v *не есть* победитель K равна $1 - 2^{-k}$, и все $n - k$ событий, соответствующих различным выборам вершин v, независимы, то

$$\mathsf{P}[N_k] \;=\; \left(1 - 2^{-k}\right)^{n-k}.$$

Оценим вероятность $P_{\geqslant 1}$ того, что *хотя бы одно* событие N_k произошло:

$$P_{\geqslant 1} = \mathsf{P}\left[\sum_{\substack{K \subseteq V \\ |K|=k}} N_k\right] \;\leqslant\; \sum_{\substack{K \subseteq V \\ |K|=k}} \mathsf{P}[N_k] = C_n^k \left(1 - 2^{-k}\right)^{n-k} < 1.$$

Следовательно, с положительной вероятностью ни одно из событий N_k *не происходит*, откуда следует существование турнира на n вершинах, обладающий свойством S_k. □

5.3 Модели случайных графов

Модель $G(n,p)$ Эрдёша–Реньи — исторически первая модель случайного графа.

На множестве $V_n = \{1, \ldots, n\}$ вершин вводим множество рёбер E, соединяя пару вершин ребром с заданной вероятностью $p \in (0,1)$ независимо от всех остальных пар вершин. Таким образом, ребра появляются в соответствии со схемой Бернулли, из C_n^2 испытаний с вероятностью единичного успеха p.

Ясно, что E — случайное множество. Случайный граф в модели Эрдёша–Реньи: $(V_n, E) \in G(n,p)$.

В аксиоматике Колмогорова получим дискретное вероятностное пространство

$$\Omega_n = \{G = (V_n, E)\}, \quad \mathcal{F}_n = \mathbf{2}^{\Omega_n},$$
$$\mathsf{P}_{n,p}[G] = p^{|E|}(1-p)^{C_n^2 - |E|}.$$

Элементы сигма-алгебры $\mathcal{F}_n$ — наборы графов. Вероятность, с которой граф на n вершинах обладает данным свойством A:

$$\mathsf{P}_{n,p}[\mathcal{A}] = \sum_{G \in \mathcal{A}} \mathsf{P}_{n,p}[G],$$

где множество $\mathcal{A} \in \mathcal{F}_n$ состоит из всех графов, для которых выполнено свойство A.

Теорема 5.8. *Пусть c — const и $p = p(n) \sim \frac{c}{n}$ в модели $G(n,p)$. Тогда количество треугольников в случайном графе имеет асимптотически пуассоновское распределение с параметром $\lambda = \frac{c^3}{6}$.*

Свойство A *выполнено почти всегда* или *с большой вероятностью*[2)], если

$$\mathsf{P}_{n,p}[\mathcal{A}] \to 1 \quad \text{при } n \to \infty.$$

Теорема 5.9. *Пусть $G \in G(n,p)$ и $p = p(n) = c\,\dfrac{\ln n}{n}$, c — const. Тогда почти всегда если*

- *$c > 1$, то граф G связен,*
- *$c < 1$, то граф G не является связным.*

Доказательство. 1. Случай $c > 1$.
Введем случайную величину на пространстве $G(n,p)$:

$$X_n = X_n(G) = \begin{cases} 0, & \text{если } G \text{ связен,} \\ k, & \text{если у } G \text{ ровно } k \text{ компонент.} \end{cases}$$

Т. о. X_n принимает значения 0, 1, 2, ...

Покажем, что при $n \to \infty$

$$\mathsf{P}_{n,p}[X_n = 0] \to 1, \text{ что равносильно } \mathsf{P}_{n,p}[X_n > 1] \to 0.$$

По неравенству Чебышёва: $\mathsf{P}_{n,p}[X_n \geqslant 1] \leqslant \mathrm{E}[X_n]$, и нам остается обосновать стремление к нулю $\mathrm{E}[X_n]$.

Представим X_n в виде суммы

$$X_n = X_{n,1} + \ldots + X_{n,n-1},$$

где $X_{n,k} = X_{n,k}(G)$ — число k-вершинных компонент графа G.

Занумеруем все k-элементные подмножества множества вершин V_n случайного графа в некотором (произвольном) порядке: $K_1, \ldots, K_{C_n^k}$. Тогда, в свою очередь —

[2)] *whp* — with high probability)

$$X_{n,k} \;=\; X_{n,k,1} + \ldots + X_{n,k,C_n^k},$$

поскольку

$$X_{n,k,i} \;=\; X_{n,k,i}(G) \;= \\ = \begin{cases} 1, & \text{если } K_i \text{ образует компоненту } G, \\ 0, & \text{иначе.} \end{cases}$$

В итоге $$\mathrm{E}[X_n] \;=\; \sum_{k=1}^{n-1} \sum_{i=1}^{C_n^k} \mathrm{E}[X_{n,k,i}].$$

Очевидно,

$$\mathrm{E}[X_{n,k,i}] = \mathsf{P}_{n,p}[K_i \text{ образует компоненту в } G] \leqslant \\ \leqslant \mathsf{P}_{n,p}[\text{ из } K_i \text{ в } V_n \setminus K_i \text{ нет рёбер в } G].$$

Получая последнее неравенство, мы пренебрегли условием связности той части графа G, которая «сидит» на множестве вершин K_i (такую часть принято называть *индуцированным подграфом*, символически $G|_{K_i}$).

Далее,

$$\mathsf{P}_{n,p}\,[\text{из } K_i \text{ в } V \setminus K_i \text{ нет ребер в } G] \;=\; (1-p)^{k(n-k)},$$

и, значит,

$$\mathrm{E}[X_n] \;\leqslant\; \sum_{k=1}^{n-1} \sum_{i=1}^{C_n^k} (1-p)^{k(n-k)} \;=\; \sum_{k=1}^{n-1} C_n^k (1-p)^{k(n-k)}.$$

Последняя сумма симметрична в том смысле, что её слагаемые при k и $n-k$ равны. Рассмотрим $k = 1$:

$$n(1-p)^{n-1} \;\leqslant\; ne^{-p(n-1)} \;=\; ne^{-\frac{c(\ln n)(n-1)}{n}} \;= \\ = \; n\left(\frac{1}{n}\right)^{c(1+o(1))} \;= \; o(1), \quad \text{поскольку } \; c > 1.$$

Оставшаяся часть рассуждения состоит в доказательстве того, что слагаемые с $k > 1$ и $k < n-1$ пренебрежимо малы по сравнению с первым слагаемым.

Соответствующую выкладку мы пропустим. Если же поверить в её справедливость, то получится, что вся сумма доминируется первым и последним слагаемыми, а стало быть, и она стремится к нулю.

Теорема для случая $c > 1$ доказана.

2. Случай $c < 1$.

Обозначим через X_n количество изолированных вершин в случайном графе. Запишем

$$X_n = X_{n,1} + \ldots + X_{n,n},$$

где

$$X_{n,k} = X_{n,k}(G) = \begin{cases} 1, & \text{если вершина } k \in V_n \\ & \quad \text{— изолированная в } G; \\ 0, & \text{иначе.} \end{cases}$$

Тогда $\mathrm{E}[X_n] = \mathrm{E}[X_{n,1}] + \ldots + \mathrm{E}[X_{n,n}]$.

В свою очередь

$$\mathrm{E}[X+n,k] = \mathsf{P}_{n,p}[k \text{ — изолированная в } G] = (1-p)^{n-1}.$$

Таким образом,

$$\mathrm{E}[X_n] = n(1-p)^{n-1} = n\,(1-p)^n(1+o(1)) = \\ = (1+o(1))\,ne^{-c\ln n} = (1+o(1))\,n^{1-c}.$$

Заметим, что ввиду неравенства $c < 1$ выполнено $\mathrm{E}[X_n] \to \infty$.

Посчитаем дисперсию случайной величины X_n:

$$D[X_n] = \mathrm{E}[X_n^2] - (\mathrm{E}[X_n])^2 = \\ = \mathrm{E}[X_{n,1} + \ldots + X_{n,n}]^2 - (\mathrm{E}[X_n])^2 = \\ = \mathrm{E}[X_{n,1}^2 + \ldots + \mathrm{E}[X_{n,n}^2] + \sum_{i \neq j} \mathrm{E}[X_{n,i}X_{n,j}] - (\mathrm{E}[X_n])^2 = \\ = \mathrm{E}[X_{n,1}] + \ldots + \mathrm{E}[X_{n,n}] + \sum_{i \neq j} \mathrm{E}[X_{n,i}X_{n,j}] - (\mathrm{E}[X_n])^2 = \\ = \mathrm{E}[X_n] + \sum_{i \neq j} \mathrm{E}[X_{n,i}X_{n,j}] - (\mathrm{E}[X_n])^2.$$

Далее,

$$\mathrm{E}[X_{n,i}X_{n,j}] = \mathsf{P}[i \text{ и } j \text{ изолированы в } G] =$$

$$= (1-p)^{2n-1} = (1+o(1))(1-p)^{2n},$$

$$\sum_{i\neq j} \mathrm{E}[X_{n,i}X_{n,j}] = n(n-1)(1+o(1))(1-p)^{2n} =$$
$$= (1+o(1))\, n^{2-2c} = (1+o(1))(\mathrm{E}[X_n])^2.$$

В итоге

$$\mathrm{D}[X_n] = \mathrm{E}[X_n] + (1+o(1))(\mathrm{E}[X_n])^2 - (\mathrm{E}[X_n])^2 =$$
$$= o\left((\mathrm{E}[X_n])^2\right).$$

По неравенству Чебышёва

$$\mathsf{P}_{n,p}[G \text{ связен}] \leqslant \mathsf{P}_{n,p}[X_n = 0] = \mathsf{P}_{n,p}[X_{\leqslant}0] =$$
$$= \mathsf{P}_{n,p}[-X_n \geqslant 0] =$$
$$= \mathsf{P}_{n,p}\Big[\mathrm{E}[X_n] - X_n \geqslant \mathrm{E}[X_n]\Big] \leqslant \tfrac{\mathrm{D}[X_n]}{(\mathrm{E}[X_n])^2} = o(1).$$

и вторая часть теоремы доказана. □

Надежность сети: обсуждение результатов

1. *Сохранение связанности графа при* $p \to 0$.

При $n \to \infty$, $p = c\frac{\ln n}{n} \to 0$ (довольно быстро), но при $c > 1$ *граф остаётся связным.*

2. *Резкий скачок связности.*

Функция $p(n) = \frac{\ln n}{n}$ служит границей перехода от «почти всегда связности» к «почти всегда несвязности».

Такой переход принято называть *фазовым*, а соответствующую функцию $p(n)$ — *пороговой.*

Теорема 5.10. *Пусть* $p = c\dfrac{\ln n}{n}$ *в модели* $G(n,p)$. *Тогда если* $c > 3$, *то при* $n > 100$

$$\mathsf{P}_{n,p}[\, G \text{ связен},] \geqslant 1 - \frac{1}{n}.$$

Следующая теорема содержит в себе еще более глубокую информацию о природе связности-надежности. Она была доказана самими Эрдёшем и Реньи (см. [1–3]).

Теорема 5.11 (Эрдёш и Реньи). *Пусть* $p = p(n) = \dfrac{c}{n}$ *в модели* $G(n,p)$. *Тогда если*

- $c < 1$, *то найдется такая константа* $\beta = \beta(c)$, *что почти всегда размер каждой связной компоненты случайного графа не превосходит* $\beta \ln n$;
- $c > 1$, *то найдется такая константа* $\gamma = \gamma(c)$, *что почти всегда в случайном графе есть ровно одна компонента размера* $\geqslant \gamma n$.

Снова фазовый переход — с пороговой функцией $p = \frac{1}{n}$: если вероятность ребра в $c > 1$ раз

- *ниже порога*, то все связные компоненты графа, скорее всего, крошечные (имеющие логарифмический размер от общего числа вершин n);
- *выше порога*, то, скорее всего, найдется компонента с числом вершин порядка n. Такая компонента называется *гигантской*.

Эволюция графа. Уточнения теоремы Эрдёша–Реньи:

- при $c > 1$, помимо единственной гигантской компоненты, все остальные компоненты снова логарифмические;

- верны не только неравенство
  Hug = «размер гиганской компоненты» $\geqslant \gamma n$,
  но и асимптотика $Hug \sim \gamma n$.

Изменение свойств случайного графа при изменении вероятности ребра p — *эволюция графа*.

Терминология А. М. Райгородского: *история мира* в модели $G(n,p)$.

$p \ll \frac{1}{n}$ — весь граф поделен на несвязанные между собой логарифмические кусочки («*феодализм*»);

$p \gg \frac{1}{n}$ — гигантская компонента («*империя*»);

$p \gg \frac{\ln n}{n}$ — «империя» уничтожает «окраины» и добивается всеобщей связности («*мировое господство*»).

Устройство «мира» «внутри фазовых переходов» т. е. при: $p \sim \dfrac{1}{n}$ — всё сложно; для $p \sim \dfrac{\ln n}{n}$.

Теорема 5.12. *Пусть* $p = \dfrac{\ln n + c + o(1)}{n}$ *и* $G \in G(n,p)$. *Тогда*

$$\mathsf{P}_{n,p}\left[G \text{ связен}\right] \to e^{-e^{-c}}.$$

В частности, при $p = \frac{\ln n}{n}$ *вероятность стремится к* e^{-1}.

Здесь уже речь не идёт о «почти всегда связности» или «почти всегда несвязности»: асимптотическая вероятность связности есть, но она лежит в строгих пределах от 0 до 1.

Закон нуля и единицы. Язык логики первого порядка

Говорят, что свойство случайного графа *подчиняется закону 0 и 1*, если оно *почти наверное* либо выполняется, либо нет.

Язык логики первого порядка LG-I для описания свойств графов — содержит символы:

- *предметных переменных* — x, y, ..., обозначают вершины графа;
- *отношения* $\sim$ смежности вершин и $=$ — их равенства;
- *логических связок* — $\neg$, $\vee$, $\&$, $\supset$, $\equiv$;
- *кванторов* — $\forall$, $\exists$ по предметным переменным;
- скобок (,) — *вспомогательные символы*, обеспечивающие правильное чтение выражений.

Правила образования конечных выражений (*формул языка*) — обычные известны читателю.

Примеры 5.13 (формул *LG-I*). 1. *Граф содержит треугольник*:

$$\exists x \exists y \exists z : (x \sim y) \,\&\, (y \sim z) \,\&\, (z \sim x).$$

2. *Отсутствие изолированной вершины*:

$$\forall x \exists y : x \sim y.$$

3. *Радиус графа не больше 2*:

$$\exists x \forall y : \neg(x = y) \,\&\, \neg(x \sim y) \supset \exists z : (x \sim z) \,\&(z \sim y).$$

Не все свойства графа выразимы на языке *LG-I*, например «*граф связен*»:

$$\forall x\, \forall y\, \exists n \in \mathbb{N}_0\, \exists x_1, \ldots, x_n : \\ (x \sim x_1)\,\&\,(x_1 \sim x_2)\,\&\,\ldots\,\&\,(x_n \sim y),$$

поскольку утверждение $\exists n \in \mathbb{N}_0$ невыразимо на языке I-го порядка[3]. Совокупность свойств, описываемых языком логики первого порядка весьма богата, интересна и подчиняется исключительно красивым законам.

Теорема 5.14. *При $p = const$ свойство графа $G \in G(n,p)$, которое возможно записать на языке первого порядка, подчиняется закону 0 и 1.*

Теорема доказывается с помощью игры Эренфойхта. Рассмотрим её вариант на графах.

Игра Эренфойхта $EHR[G,H,t]$**.** Пусть G и H — два графа с непересекающимися множествами вершин. Игру ведут два игрока — *Новатор* (H) и *Консерватор* (K)[4]. Игроки ходят по очереди, отмечая вершины в графах.

Сначала *Новатор* объявляет t — количество ходов, которое сделает каждый игрок. Затем

1-й полуход H: *Новатор* выбирает *один из графов и отмечает некоторую вершину в нём.*

[3] это выражение в *слабой логике II-го порядка*, использующей нелогическое понятие натурального числа

[4] В оригинале — *Spoiler* (разрушитель) и *Duplicator* (повторитель); используя те же инициалы, их иногда называют *Самсон* и *Далила*.

1-й полуход K: *Консерватор* отмечает какую-либо вершину *в другом графе*.

Далее опять H выбирает граф и отмечает некоторую вершину в нём, K отмечает какую-либо вершину в другом графе и т. д.

К концу игры выбрано, не важно кем, по t вершин из каждого графа.

Пусть $x_1, \ldots, x_t$ — вершины, выбранные из $V(G)$, а $y_1, \ldots, y_t$ — вершины, выбранные из $V(H)$ на ходе $i = \overline{1,t}$. Эти упорядоченные наборы определяют отображение φ подграфа G' на подграф H' на выбранных вершинах. *Консерватор* выигрывает, если φ — изоморфизм, т. е. $G' \cong H'$, иначе выигрывает H.

Поскольку $EHR[G,H,t]$ — детерминированная игра с полной информацией без ничьих, то *один из игроков должен иметь выигрышную стратегию*.

Утверждение 5.15. *Пусть G и H — графы.*

1. *$G \cong H$ если и только если в игре Эренфойхта Консерватор имеет выигрышную стратегию.*
2. *Если $G \ncong H$ и один из этих графов обладает, а другой — не обладает некоторым свойством S, выразимым на языке I-го порядка, то существует такое $t = t(S)$, что Новатор имеет выигрышную стратегию в игре $EHR[G,H,t]$.*

Игра Эренфойхта $EHR[G,H,t]$: поиграем

1. Если графы *изоморфны*, то выигрышная стратегия *Консерватор* — помечать вершину, изоморфную выбранной H.

2. Для сигнатуры $\sigma = \{=, <\}$ покажем, что две однотипные алгебраические системы (АС) этой сигнатуры с носителями $\mathbb{N}$ и $\mathbb{Z}$ не являются изоморфными (среди натуральных чисел есть наименьшее, а среди целых — нет).

Покажем, что в игре Эренфойхта для этих АС новатор *Новатор* имеет выигрышную стратегию.

- *Новатор* объявляет, что игра будет проведена в $t = 2$ хода и помечает число 1.
- В ответ *Консерватор* обязан пометить некоторое число $m \in \mathbb{Z}$.
- На 2-м ходу *Новатор* помечает в $\mathbb{Z}$ любое число, строго меньшее m.

Теперь *Консерватор* проигрывает при любом ответном ходе: пометить на $\mathbb{N}$ число, меньшее 1, он не может.

3. Покажем в той же сигнатуре, что АС $\mathbb{Z}$ и $\mathbb{Q}$ не изоморфны (порядок на рациональных числах плотен, а на целых — нет), т. е. что в игре Эренфойхта новатор *Новатор* всегда может выиграть.

- *Новатор* объявляет, что игра будет проведена в $t = 3$ хода и на первых двух ходах помечает числа 0 и 1 из $\mathbb{Z}$.
- В ответ *Консерватор* помечает некоторые числа $q_1, q_2 \in \mathbb{Q}$ ($q_1 < q_2$, иначе *Новатор* заведомо выиграет).
- На 3-м ходу *Новатор* помечает помечает в $\mathbb{Q}$ любое число, лежащее строго между q_1 и q_2.

Т. к. в $\mathbb{Z}$ между 0 или 1 нет целых чисел, *Консерватор* проигрывает при любом своём ходе.

4. Пусть S обозначает свойство $\forall\, x\ \exists\, y : x \sim y$ отсутствия изолированной вершины, граф G имеет изолированную вершину (обладает свойством S), а H — не имеет.

Покажем, что тогда *Консерватор* не имеет выигрышной стратегии в игре Эренфойхта.

- *Новатор* объявляет, что игра будет проведена в $t = 2$ хода и отмечает изолированную вершину x в G.
- В ответ *Консерватор* помечает произвольную вершину в $y_1 \in H$.
- На 2-м ходу *Новатор* помечает вершину в $y_2 \in H$, смежную с y_1.

Теперь *Консерватор* гарантировано проигрывает, т. к. не может выбрать в G вершину, смежную с x.

Стратегии: *Новатор* выбирает некоторые «специфические элементы», а *Консерватор* на другой структуре старается выбрать элементы «максимально похожие» на них.

Французско-алжирский математик *Р. Фраиссе* в своей докторской диссертации (1953) предложил метод «вперёд-назад» для определения, являются ли две алгебраические структуры АС *элементарно эквивалентными* (в них одновременно истины или ложны одни и те же формулы данной сигнатуры АС). Чуть позже метод переоткрыл *Асан Дабсович Тайманов* (1917–1990). В терминах игры метод переформулирован А. Эренфойхтом[5)].

[5)] Анже́й Эренфо́йхт (Andrzej Ehrenfeucht, 1932) — польско-американский математик.

Идея метода Фраисе-Эренфойхта — одна из самых универсальных в логике XX в.: она оказалась плодотворно применимой к широкому спектру логик и АС.

Будем говорить, что функция $p = p(n)$ удовлетворяет закону 0 или 1, если при $n \to \infty$ для графа $G(n, p(n))$ ему подчиняется любое его свойство, выразимое на языке I-го порядка.

Теорема 5.16. *Функция $p = p(n)$ удовлетворяет закону 0 или 1 если и только если для любого t*

$$\lim_{m,n\to\infty} \mathsf{P}\left[\, \textit{Консерватор выигрывает игру } EHR[\,G(n,p(n)),\, H(m,p(m)),\, t\,]\,\right] = 1,$$

где $G(n, p(n))$, $H(m, p(m))$ — независимые случайные графы в модели Эрдёша–Реньи с непересекающимися множествами вершин.

Замечание. Когда задано вероятностное распределение по (G, H), существует вероятность P того, что игра $EHR[\,G, H, t\,]$ будет выиграна *Консерватором*, и эта вероятность P должна стремиться к единице.

Доказательство. Докажем только необходимость.

Предположим, что значение $p = p(n)$ не удовлетворяет закону 0 или 1. Пусть свойство S такое, что для $0 < c < 1$ справедливо

$$\lim_{n\to\infty} \mathsf{P}\left[\,\text{граф } G(n,p(n)) \text{обладает свойством } S\,\right] = c.$$

Пусть $t = t(A)$ удовлетворяет условию теоремы.
С предельной вероятностью $2c(1-c) > 0$ ровно

один из графов $G(n, p(n))$ и $H(n, p(n))$ будет обладать свойством S, поэтому победит H, что противоречит предположению. □

Эта теорема — своеобразный мост между математической логикой и случайными графами.

Теорема 5.17. *При $p = n^{-\alpha}$, где $\alpha > 0$ — рациональное число, свойство графа $G \in G(n, p)$, которое возможно записать на языке первого порядка, подчиняется закону 0 и 1.*

Покажем существенность рациональности α. Рассмотрим свойство S = граф содержит треугольник. По теореме 5.8 с $c = 1$ имеем

$$\mathsf{P}[S] \sim 1 - e^{-1/6},$$

т. е. эта вероятность не равна ни 0, ни 1.

5.4 Модели Интернета

Каким законам подчиняется рост Интернета? — вопрос естественно возник в 1990-е, когда Интернет только зарождался и возникла необходимость построить адекватную модель его развития.

А.-Л. Барабаши и Р. Альбе́рт[6)] нашли ряд важных эмпирических закономерностей в поведении Ин-

[6)] А́льберт-Ла́сло Бараба́ши (Albert-L'aszl'o Barabási, 1967) — физик, работает в Университетах США. Член Американского физического общества, иностранный член венгерской Академии наук.

Рика́ Альбе́рт (Réka Albert, 1972) — профессор физики и биологии в Пенсильванском университете (США).

На момент публикации совместной работы Р. Альберт — аспирантка А.-Л. Барабаши.

тернета. Эти закономерности впоследствии формализовывали многие авторы. Модели Барабаши–Альберт применяют для описания также социальных, биологических, транспортных и т.д. сетей.

Терминология

Вершины — структурные единицы в Интернете: сайты (Интернет-граф), хосты (хост-графы), статические-html страницы (HyperText Markup Language, веб-графы), владельцы и пр.

Рёбра (*дуги*) — соединяют вершины, между которыми имеются ссылки, т. е. имеются *кратные* — и ребра, и петли.

Плотный граф — граф, в котором число рёбер близко к максимальному.

Разреженный граф (противоположное свойство) — граф, имеющий малое число рёбер.

Расстояние в графе — число рёбер в кратчайшем рёберном пути.

Диаметр связанного графа — максимальное расстояние между вершинами, символически $\operatorname{diam} G$.

Если диаметр мал, то граф *тесный*.

Независимое множество — совокупность вершин графа никакие две из которых не соединены ребром (индуцированный этим множеством подграф состоит из изолированных вершин). Максимальный размер независимого множества графа G обозначают $\alpha(G)$.

Хроматическое число $\chi(G)$ — минимальное число цветов, в которые можно раскрасить вершины графа так, чтобы концы любого ребра имели разные цвета.

Обхват $girth(G)$ — длина кратчайшего цикла в G.

Гигантская компонента. Пусть дана последовательность графов $\{ G_n = (V_n\, E_n) \}$ такая, что $\lim\limits_{n\to\infty} |V_n| = +\infty$.

Говорят, что графы G_n содержат *гигантскую компоненту связности*, если $\exists\, \gamma > 0\ \forall\, n$:

$\big|$ *наибольшая компонента связности* $G_n \big| \geqslant \gamma \big|V_n\big|$.

Степени вершин — $\text{indeg}\ \ v, \text{outdeg}\ \ v, \deg v$ — входящая, исходящая и полная степень вершины v.

Вторые степени вершин — можно определить по-разному: число вершин на расстоянии 2 от v, число вершин на расстоянии $\leqslant 2$ от v, сумма степеней вершин на расстоянии 1 от v и др.

Пейджранк — ... (*рассмотрим далее*).

Web-граф — орграф, вершинами которого являются документы (в основном статические html-страницы) сети Интернет, а дугами — гипертекстовые ссылки между ними. Имеет сотни миллионов вершин.

В структуре web-графа также было выделено удивительно большое число специфических топологических структур, таких как двудольные клики небольшого размера (до 10 html-страниц). Это связывают с наличием неявных кибер-сообществ: групп ресурсов сходной тематики, имеющих общие «авторитетные»

страницы. Двудольные клики интерпретируются как ядро подобных сообществ — они состоят из множества «фанатских» и «авторитетных» страниц, причем все страницы из первого множества ссылаются на страницы второго.

На практике используют «мини» web-графы, сгенерированные на основе некоторой модели. Основная задача моделирования — охватить все его особенности, и создание новой модели обычно являлось ответом на обнаружение неизвестных свойств web-графа.

Построение хорошей математической модели интернета сразу же даёт качественно новые инструменты для улучшения информационного поиска, выявления спама, прогнозирования распространения информации в социальных сетях и в интернете в целом. С другой стороны, математические модели интернета оказываются весьма похожими на модели биологических сообществ, модели межбанковского взаимодействия и др.

Наблюдения Барабáши–Альбéрт.

1. Веб-граф весьма *разрежен*: у него в k-вершином подграфе примерно kt ребер, где $k \geqslant 1$ — константа, что отличается по порядку от числа C_k^2 рёбер у полного k-вершинного графа.

2. *Диаметр* веб-графа *невелик*: в 1999 г. он имел величину 5...7 — граф *тесен* (при условии неориентированности дуг).

Это — известное свойство социальных сетей — «мир тесен» (small-word phenomenon, свойство «ма-

лого мира»):

- любые два человека в мире знакомы через 5...6 рукопожатий;
- с любого сайта можно перейти на любой другой за 5...7 переходов (если находимся в гигантской компоненте).

Если учитывать ориентацию рёбер, то диаметр $\approx 10...20$. Эти параметры не меняются долгие годы.

3. Веб-граф характеризуется *степенным законом распределения степеней вершин*: вероятность того, что некоторая вершина v веб-графа имеет степень d, оценивается как

$$\mathsf{P}\,[\deg\ v = d\,] \approx \frac{c}{d^{\lambda}},$$

где $\lambda = const$, а c — нормирующий множитель, вычисляемый из условия $\sum \mathsf{P} = 1$.

Реальные биологические, социальные, транспортные и т.д. сети подчиняются такому же степенному закону с разными $\lambda \in (2,3)$:

веб-графы $\lambda \approx 2{,}1$; хост-графы $\lambda \approx 2{,}3$.

Попытаемся применить модель Эрдёша–Реньи для описания роста Интернета и подобных сетей.

1. Подбором вероятности p *можно добиться разреженности и тесноты* (при $p = \Theta(1/n)$, хотя и не с наблюдаемыми параметрами).

2. Степенной закон распределения степеней вершин *не может быть получен* в схеме Бернулли. Действительно, в модели $G(n,p)$ степень

каждой вершины случайного графа биномиальна с параметрами $n-1$ и p, и при $p=\Theta(1/n)$ данное биномиальное распределение аппроксимируется *пуассоновским*, а не степенным.

Вывод: *модель Эрдёша–Реньи не применима* для описания роста Интернета.

Модели предпочтительного присоединения. Модель Боллобаша-Риордана

Предложения Л.-А. Барабаши и Р. Альберт по моделированию процесса формирования Интернета:

- считаем, что в каждый момент времени появляется новый сайт, который ставит фиксированное количество ссылок на своих предшественников;
- вероятность, с которой новый сайт поставит ссылку на один из прежних сайтов, пропорциональна числу уже имевшихся на тот сайт ссылок.

Это модель *предпочтительного присоединения* (preferential attachment) — «имущему дастся, а у неимущего отнимется».

Барабаши и Альберт никак не конкретизировали, какую именно из таких моделей они предлагают рассматривать. Показано, что эти модели могут быть исключительно разнородными по своим свойствам.

Одну из наиболее адекватных формализаций модели Барабаши–Альберт предложили в начале 2000-х годов Б. Боллобаш и О. Риордан.

Модель Боллобаша-Риордана (динамическая модификация)

Сначала строится последовательность случайных графов G_1^1, G_1^2, ..., в которой у графа с номером n число вершин и ребер равно n;

Затем из неё формируется последовательность G_k^1, G_k^2, ..., в которой у графа с номером n число вершин равно n, а число ребер — kn, $k \in \mathbb{N}$.

Конкретно:

1. Начинаем с графа G_1^1 с одной вершиной и одной петлёй.

2. Когда граф G_1^{n-1} с $n-1$ вершиной $n-1$ рёбрами построен, добавим к нему вершину n и ребро (n, i), $i \in \{1, \ldots, n\}$, при этом

   - петля (n, n) возникнет с вероятностью $1/(2n-1)$;
   - ребро (n, i) возникнет с вероятностью $\deg\, i/(2n-1)$, где $\deg\, i$ — степень вершины i в графе G_1^{n-1}.

   Распределение вероятностей задано корректно:

$$\sum_{i=1}^{n-1} \frac{\deg i}{2n-1} + \frac{1}{2n-1} = \frac{2(n-1)}{2n-1} + \frac{1}{2n-1} = 1,$$

   Случайный граф G_1^n, удовлетворяющий принципу предпочтительного присоединения, построен.

3. Строим граф G_k^n. Для этого берем граф G_1^{kn} и
   1) делим множество его вершин на последовательные части размера k;

   2) объявляем каждую часть вершиной, а ребра сохраняем: рёбра внутри части образуют кратные петли, а между двумя различными частями — кратные ребра.

   В результате вершин стало n, а ребер — осталось по-прежнему kn.

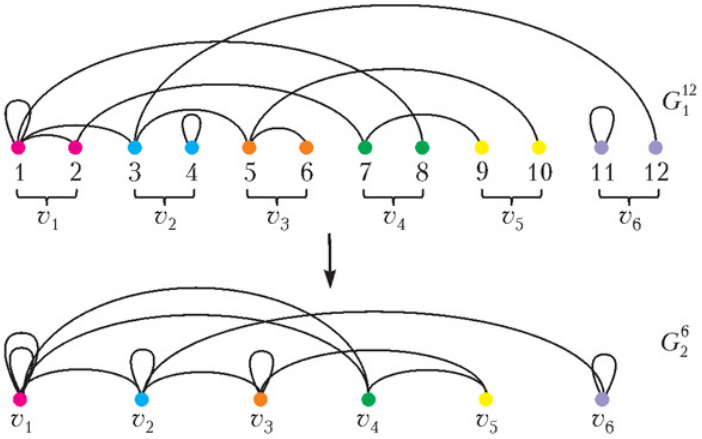


Рис. 5.1. Модель Боллобаша–Риордана: иллюстрация к последнему шагу

Модель Боллобаша-Риордана (статическая модификация) — по своим характеристикам практически неотличима от динамической.

Построим *линейную хордовую диаграмму* (linearized chord diagram, LCD):

1) зафиксируем на оси абсцисс на плоскости $2n$ точек $1, 2, \ldots, 2n$;

2) разобьем эти точки на пары, а элементы каждой пары соединим дугой, лежащей в верхней полуплоскости.

Дуги в LCD могут пересекаться, лежать друг под дружкой, но не могут иметь общих вершин.

Количество различных LCD:

$$l_n = (2n-1)(2n-3)\dots 1 = \\ = \frac{(2n)!}{2n(2n-2)(2n-4)\dots 2} = \\ = \frac{(2n)!}{2^n n(n-1)(n-2)\dots 1} = \frac{(2n)!}{2^n n!}.$$

Если LCD случайная, то вероятность появления каждой — $1/l_n$.

По каждой LCD построим граф:

1) идём слева направо по оси абсцисс, пока не встретим впервые *правый* конец какой-либо дуги; пусть его номер i_1;
2) объявляем набор $\{1, \dots, i_1\}$ первой вершиной будущего графа (склеиваем их);
3) снова идем от $i_1 + 1$ направо до первого правого конца i_2 какой-либо дуги и объявляем второй вершиной графа набор $i_1 + 1, \dots, i_2$; и т. д.

Получаем n вершин, а ребра порождаем дугами: вершины соединяем ребром, если между соответствующими наборами есть дуга; ребра ориентируем *справа налево*, петли возникают аналогично: граф с n вершинами и n ребрами построен.

Граф с n вершинами и kn ребрами получаем как в динамической модели.

Теорема 5.18 (Боллобаш и Риордан). *Обозначим* $D_n = \frac{\ln n}{\ln \ln n}$*; тогда для любого* $k \geqslant 2$ *и любого* $\varepsilon > 0$

$$\mathsf{P}\left[\,\left|\operatorname{diam} G_k^n - D_n\right| \leqslant \varepsilon\,\right] \to 1, \quad n \to \infty.$$

Вывод: диаметр графа G_k^n *плотно сконцентрирован* около D_n.

У веб-графа порядка 10^7–10^8 вершин; подставляя эти значения, получим

$$5{,}8 \leqslant D_n \leqslant 6{,}2$$

— *фантастическое попадание!* $D_n < 7$ даже при $n = 10^9$.

В рамках модели Боллобаша–Риордана получены оценки распределений (при разных её модификациях/упрощениях и ограничениях на параметры)

- вторых степеней вершин;
- количества рёбер между вершинами заданных степеней;
- *кластерных коэффициентов* (один из их видов: вероятность того, что соседи вершины соединены ребром);
- числа копий фиксированного графа: треугольников, тетраэдров и т.д.; наличие клик объясняется действиями спамеров, которые искусственно расставляют ссылки, желая повысить рейтинги сайтов, заплативших за раскрутку;
- пейджранка.

Теоретические распределения в разной степени совпадают с эмпирически наблюдаемыми. Например,

- степенной закон распределения степеней вершин получен с $\lambda = 3$;
- число треугольников в модели оценивается как $\Theta(\ln^3 n)$, а реально — n^α;
- в модели практически отсутствуют плотные двудольные подграфы и т. д.

Предложены и другие модели Интернета: модель копирования, Холма–Кима, Купера–Фриза, Бакли–Остгауза и др. Они показывают разную точность описания различных параметров графов.

5.5 Пейджранк

Пейджранк $PR(i)$ — характеристика вершины i веб-графа (V, E), уточняющая понятие 1-й степени, 2-й степени и т.д.

$$PR(i) = d \sum_{j \to i} \frac{PR(j)}{\text{outdeg } j} + \frac{d}{|V|} \sum_{j \in \mathcal{D}} PR(j) + \\ + \frac{1-d}{|V|}, \quad i = 1, 2, \ldots, |V|,$$

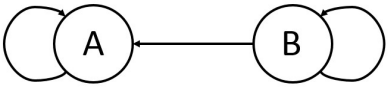
где $\mathcal{D}$ — множество вершин, исходящие степени которых равны 0, $d \in (0, 1)$ — *демпфирующий фактор* (константа).

$(1 - d)$ — *вероятность телепортации*: считаем, что пользователь при блуждании по сети с вероятностью d переходит по ссылке, а с вероятностью $1 - d$

— на случайную страницу т. е. *возможен переход на любую страницу.*

Пейджранк (PageRank) — метод вычисления веса страницы путём подсчёта важности ссылок на неё.

Пример 5.19. 1.

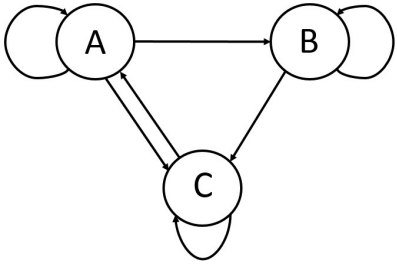


$$\begin{cases} PR(A) = d \cdot PR(A) + \dfrac{d}{2} \cdot PR(B) + \dfrac{1-d}{2}, \\ PR(B) = \dfrac{d}{2} \cdot PR(B) + \dfrac{1-d}{2}. \end{cases}$$

$$\begin{cases} PR(A) = \dfrac{1}{2-d}, \\ PR(B) = \dfrac{1-d}{2-d}. \end{cases} \qquad d \in (0,1) \Rightarrow PR(A) > PR(B).$$

Например, при $d = 0{,}85$: $PR(A) = 0{,}87$, $PR(B) = 0{,}13$.

2.



$$\begin{aligned} \text{outdeg } A &= 3 \\ \text{outdeg } B &= 2 \\ \text{outdeg } C &= 2 \end{aligned}$$

$$\begin{cases} PR(A) = d\left(\dfrac{PR(A)}{3} + \dfrac{PR(C)}{2}\right) + \dfrac{1-d}{3}, \\ PR(B) = d\left(\dfrac{PR(A)}{3} + \dfrac{PR(B)}{2}\right) + \dfrac{1-d}{3}, \\ PR(C) = d\left(\dfrac{PR(A)}{3} + \dfrac{PR(B)}{2} + \dfrac{PR(C)}{2}\right) + \dfrac{1-d}{3}. \end{cases}$$

При $d \in (0,1)$: $PR(C) > PR(A) > PR(B)$, $d = 0{,}85 \Rightarrow PR(C) \approx 0{,}45$, $PR(A) \approx 0{,}29$, $PR(B) \approx 0{,}26$.

Пейджранк придумали Л. Пейдж и С. Брин[7)].

Пейджранк: вычисление.
В исходной модели Боллобаша–Риордана G_m^n пейджранк не считали (там трудно работать с петлями).

Позже был предложен алгоритм вычисления пейджранка в ещё одной конкретизации модели Барабаши–Альберт:

- начинаем с вершины 0 без петель, но полагаем её вес m;
- добавляем вершину 1 и из неё ставим m ссылок на 0, полагаем вес вершины 0 равным $2m$, а вес вершины 1 равным m;
- дальнейшие вершины, появляясь на свет, выставляют свои m ссылок независимо, каждую с вероятностью, пропорциональной весам существующих вершин, которые равны сумме их входящих степеней и m:

$$\mathsf{P}[n{+}1 \to i] = \frac{\text{indeg}\quad i+m}{\sum\limits_{k=0}^{n}(\text{indeg}\quad k+m)} = \frac{\text{indeg}\quad i+m}{2mn+m}.$$

[7)] Лоуренс «Ларри» Пейдж (Lawrence «Larry» Page, 1973) — разработчик и сооснователь (совместно с Сергеем Брином) поисковой системы Google.

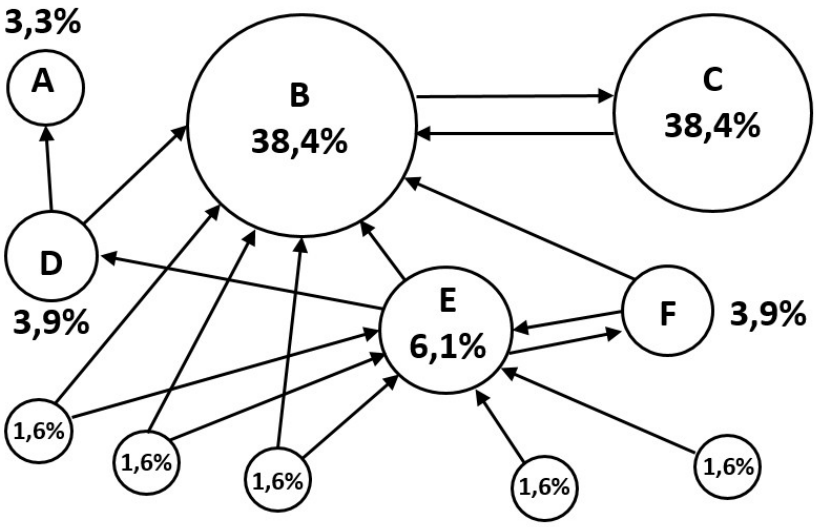
Сергей Михайлович Брин (англ. Sergey Brin, 1973) — американский предприниматель и учёный в области BT, IN и экономики. Родители Сергея Брина — выпускники Мехмата МГУ (1970 и 1971 годов).

Л. Пейдж и С. Брин входят в число самых богатых людей планеты (17-е и 20-е места в Forbes-2014).

Показано, что в данной модели плотность пейджранка $p_n(x) \approx \Theta\left(x^{-\frac{3+d}{1+d}}\right)$ — *степенной закон.*

При $d = 0,85$ получим $\lambda \approx 2,1$, что близко к эмпирическим данным.

Пример 5.20 (*вычисления PageRank*).



$PR(C) > PR(E)$, хотя indeg $C <$ indeg E, но ссылка на C исходит из очень важной страницы B $\Rightarrow$ она имеет большой вес.

Без телепортации все пользователи в конечном итоге попадают на страницы A, B или C. При наличии телепортации из A можно попасть на любую страницу в этой Сети, даже при indeg $A = 0$.

Модель поиска в интернет

- Страницы Интернета неэквивалентны и эта неэквивалентность описывается величиной $PR(v)$, $v \in V_n$.

- Вероятности перехода между страницами содержат две компоненты: обусловленную реальными связями между ними и возможностью попадания на любую страницу (телепортация).
- Если по запросу пользователя найдено множество страниц $W \subset V_n$, то релевантную информацию нужно искать на страницах, имеющих наибольшее значение $PR(v)$, $v \in W$.
- В настоящее время классические пейджранки уже не употребляются.
- Изучалось распределение рейтинга PageRank (PR) в web-графе. Исследование показало, что это распределение, также как и число ссылающихся страниц, подчиняется экспоненциальному закону с коэффициентом 2,1, но корреляция между этими параметрами очень невелика, а значит, страница с большим количеством входящих ссылок может получить очень низкий PR[8)].

Надстройка для браузера Google Toolbar

- PageRank каждой веб-страницы — целое число от 0 до 10 (важность этой страницы с точки зрения Google).
- Механизм расчёта PageRank и что в точности обозначает это значение, не раскрывается.
- По некоторым данным, эти значения обновляются лишь несколько раз в год и показывают

[8)] Подобный результат очень обрадовал ИПС, в частности Google, ведущую постоянную борьбу с компаниями-оптимизаторами сайтов (SEO).

значения PageRank страниц на логарифмической шкале.

Замечена особенность: Page Rank выше 5 могут получить сайты только довольно старые или очень большие проекты (сайты) с большим количеством посещений.

- Поисковая система Google использует более 200 ранжирующих сигналов, лишь одним из которых является PageRank, но он до сих пор играет существенную роль.

Борьба со спамом

Линковые кольца: ссылки по кругу. Как «раскрутить» сайт S — он должен поместиться в ТОП выдачи поиска?

Жульнический метод: договориться с сайтами S1, ..., Sn, которые обладают высоким индексом цитирования (заплатить им), чтобы они ссылались на S.

С точки зрения поисковой системы, сайт, процитированный респектабельным сайтом, резко повышает свой «вес» при ранжировании в ходе составления списка выдачи по запросу.

1. Самое простое — ссылки по кругу: S1 ставил ссылку на S2, S2 — на S3, ..., Sn — на S1.

Это «линковое кольцо». Такую схему быстро научились отлавливать, но название осталось.

2. Сейчас типичная конструкция — двудольный граф.

Таких линковых колец в интернете — сотни тысяч.

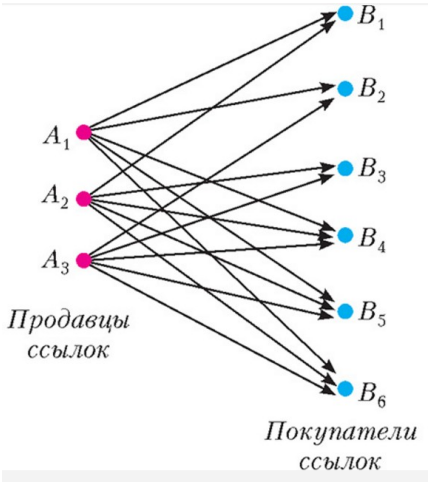


Рис. 5.2. Линковое кольцо в виде двудольного графа

Задача поисковой системы — автоматическое выявить такие искусственно завышенные «индексы цитирования».

Как можно обнаружить мошейничество

1) разрабатывают адекватную модель интернета без спама;
2) подсчитывают вероятностные характеристики тех или иных графовых структур в построенной модели и в «подозрительном» фрагменте интернета;
3) если данные характеристики существенно отличаются, то, скорее всего, обнаружено кольцо.

Например, для данного двудольного фрагмента находят реальное количество μ рёбер между долями и математическое ожидание M таких рёбер в модели. Если M значительно меньше μ $M \ll \mu$, то, скорее всего, данная структура аномальная.

5.6 Задачи с решениями

Задача 5.1. Доказать неравенство

$$R(k,l) \leqslant R(k-1,l) + R(k,l-1), \quad k > 2,\ l > 2.$$

Решение. Очевидно $R(2,l) = 2$ и $R(k,2) = k$.
Применим математическую индукцию по числу $s = k + l$.
По доказанному ранее

$$6 = R(3,3) \leqslant R(3,2) + R(2,3) = 3 + 3.$$

Пусть существование чисел $R(k-1,l)$ и $R(k,l-1)$ установлено.

Рассмотрим полный n-граф, где $n = R(k-1,l) + R(k,l-1)$, рёбра которого окрашены в красный и синий цвета.

Обозначим

v — произвольно выбранную вершину графа;

V_r — множество вершин, соединённых с v *красным* ребром, $|V_r| = n_1$;

V_b — множество вершин, соединённых с v *синим* ребром, $|V_b| = n_2$.

Справедливо равенство

$$n = n_1 + n_2 = R(k-1,l) + R(k,l-1).$$

Рассмотрим два случая

1) $n_1 \geqslant R(k-1,l),\ n_2 < R(k,l-1)$;
2) $n_2 \geqslant R(k-1,l),\ n_1 < R(k-1,l)$.

В случае 1) по определению числа $R(k-1,l)$ в подграфе V_r найдутся одноцветные либо синий l-подграф, либо красный $k-1$-подграф, и тогда добавляя к красному $k-1$-подграфу вершину v получим одноцветный красный k-подграф.

Случай 2) рассматривается аналогично.

Задача 5.2. Показать, что $R(3,4) > 8$.

Решение. В правильном 8-угольнике раскрасим

- стороны и соединяющие противоположные вершины диагонали — в красный цвет,
- остальные диагонали — в синий.

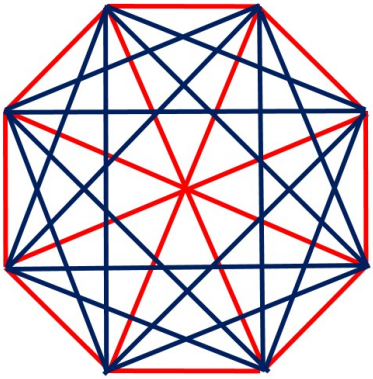


Рис. 5.3. к задаче 5.2

Нетрудно убедиться (см. рис. 5.3), что при такой раскраске нет ни красного 3-угольника, ни синего 4-угольника.

Задача 5.3. Доказать неравенство

$$R(k,l) \leqslant C_{m+k-2}^{k-1},\ k \geqslant 2,\ l \geqslant 2.$$

Решение. Применяем математическую индукцию по числу $s = k + l$.

Если $s = 6$, т. е. $k = l = 3$, то неравенство

$$6 = R(3,3) \leqslant C_{3+3-2}^{3-1} = C_4^2 = 6$$

выполняется.

Пусть $R(k-1,l) \leqslant C_{k+l-3}^{k-2}$, $R(k,l-1) \leqslant C_{k+l-3}^{k-1}$.

Тогда, используя доказанное в задаче 5.1 неравенство

$$R(k,l) \leqslant R(k-1,l) + R(k,l-1), \quad k > 2,\ l > 2$$

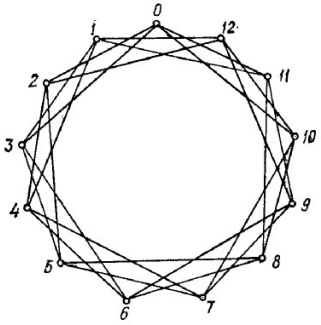
и свойство биномиальных коэффициентов, получим оценку

$$R(k,l) \leqslant R(k-1,l) + R(k,l-1) \leqslant \\ \leqslant C_{k+l-3}^{k-2} + C_{k+l-2}^{k-1} = C_{k+l-2}^{k-1}.$$

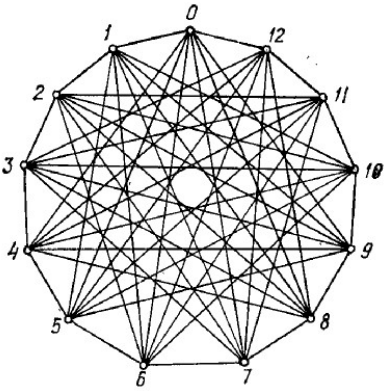
Задача 5.4. Найти раскраску в два цвета полного 13-графа такую, что ни один 3-подграф не является красным и ни один 5-подграф не является синим.

Решение. Занумеруем вершины 13-графа числами от 0 до 12.

Ребро, соединяющее вершины i и j будем раскрашивать в красный цвет, если $i-j \equiv_{13} 2$ или $i-j \equiv_{13} 3$, а остальные — в синий.



Красный подграф



Синий подграф

Глава 6

Решение булевых уравнений

6.1 Основные понятия булевой алгебры (напоминание)

Зачем нужно уметь решать булевы уравнения?

- Функциональная диагностика логических устройств.
- Логически синтез дискретных устройств.
- Логические модели объекта в распознавании и классификации (связь объект-признак-класс).

Определение 6.1. Булевой алгеброй $\mathcal{B}$ называется множество B, содержащее по крайней мере два элемента — o (нуль) и ι (единица), с заданными на нём бинарными операциями $\sqcup$ (объединения), $\sqcap$ (пересечения) и унарной операцией $'$ (дополнения). При этом для любых $x, y, z \in B$ выполняются следующие законы (аксиомы) булевой алгебры:

$$
\begin{aligned}
Com\sqcup:&\ \ x \sqcup y = y \sqcup x,\\
Com\sqcap:&\ \ x \sqcap y = y \sqcap x,\\
Dtr1:&\ \ (x \sqcup y) \sqcap z = (x \sqcap z) \sqcup (y \sqcap z),\\
Dtr2:&\ \ (x \sqcap y) \sqcup z = (x \sqcup z) \sqcap (y \sqcup z),\\
\sqcup o:&\ \ x \sqcup o = x, \qquad\qquad \sqcap \iota:\ \ x \sqcap \iota = x,
\end{aligned}
$$

$$Cmp': \ x \sqcup x' = \iota, \qquad Isl': \ x \sqcap x' = o,$$
$$Inv': (x')' = x,$$
$$\iota': \ \iota' = o, \qquad o': \ o' = \iota,$$
$$DeM1: \ (x \sqcup y)' = x' \sqcap y',$$
$$DeM2: \ (x \sqcap y)' = x' \sqcup y',$$
$$\sqcup\iota: \ x \sqcup \iota = \iota, \qquad \sqcap o: \ x \sqcap o = o,$$
$$Ass\sqcup: \ x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z,$$
$$Ass\sqcap: \ x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z,$$
$$Id\sqcup: \ x \sqcup x = x, \qquad Id\sqcap: \ x \sqcap x = x,$$
$$Abs1: \ x \sqcap (x \sqcup y) = x,$$
$$Abs2: \ x \sqcup (x \sqcap y) = x.$$

Множество B называется *носителем* булевой алгебры $\mathcal{B}$, а o и ι — *выделенными элементами* или *универсальными гранями*.

Введённые операции называют *абстрактными*, поскольку ни они сами, ни носитель, на котором они определены, никак не конкретизируются.
В приложениях элементы булевой алгебры интерпретируются как подмножества некоторых множеств, события, высказывания, сигналы и др.

Лемма 6.2 (основные свойства элементов булевой алгебры). *Для любых элементов x и y булевой алгебры справедливы следующие утверждения:*

1) $x \sqcup y = o \Leftrightarrow x = y = o$ *и*
   $x \sqcap y = \iota \Leftrightarrow x = y = \iota$;

2) *следующие четыре соотношения эквивалентны —*
   $x \sqcap y = x, \quad x \sqcup y = y, \quad x' \sqcup y = \iota, \quad x \sqcap y' = o$;

3) *лемма о единственности дополнения —*

$$\begin{cases} x \sqcap y = o \\ x \sqcup y = \iota \end{cases} \Leftrightarrow \quad y = x'.$$

Принцип двойственности для булевой алгебры Пусть V — выражение или равенство булевой алгебры.

Обозначения для результата одновременной замены всех символов в V:

$V^\sharp$ — $\sqcap \leftrightarrow \sqcup$ и $\iota \leftrightarrow o$;

$V^\flat$ — $x \leftrightarrow x'$, где x — элемент носителя, не являющийся универсальной гранью;

V^* — когда производятся обе указанные замены.

Принцип двойственности Если V —

— булево равенство, истинное для любых входящих в него элементов, то равенства $V^\sharp$, $V^\flat$ и V^* также истинны.

— выражение булевой алгебры, то $V^* = V'$.

Системы аксиом для булевой алгебры Приведённая системы из 21-ой аксиомы избыточна.

1. Пары аксиом Com, Dtr, вместе с $\sqcup o$, $\sqcap \iota$, Cmp' и Isl'

   (первые 8 из приведенных выше законов).

   Данная система не является независимой: например, каждый из законов $\sqcup o$ и $\sqcap \iota$ выводим из остальных семи.

2. Пары законов законов Dtr, Abs вместе с Cmp' и Isl'.

   Это единственная кратчайшая (6 аксиом) известная на сегодняшний день безызбыточная самодвойственная система аксиом булевой алгебры.

3. $Com\sqcup$, $Ass\sqcup$ и уравнение Роббинса:

$$((x \sqcup y)' \sqcup (x \sqcup y')')' = x.$$

Алгебры множеств: определение

- $A \neq \varnothing$ — множество, $\mathcal{P}(A)$ — множество всех подмножеств (булеан) A;
- $\mathcal{S}(A)$ — некоторая совокупность подмножеств A, устойчивая относительно объединения $\cup$, пересечения $\cap$ и дополнения до A ($^-$), а также содержащая $\varnothing$ и A.
- Понятно, что $\{\varnothing, A\} \subseteq \mathcal{S}(A) \subseteq \mathcal{P}(A)$.

АС $\langle \mathcal{S}(A), \underbrace{\cup, \cap, {}^-, \varnothing, A}_{\text{сигнатура}} \rangle$ — алгебра множеств.

Алгебра множеств с носителем $\mathcal{P}(A)$ — тотальная (над A),
а с двухэлементным носителем $\{\varnothing, A\}$ — тривиальная.

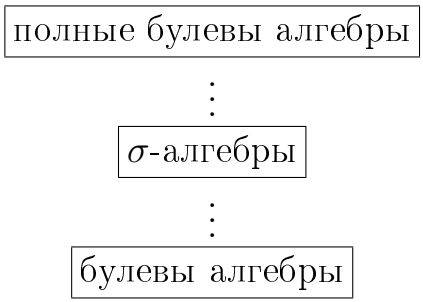
Утверждение 6.3. *Всякая алгебра множеств $\mathcal{S}(A)$ есть булева алгебра с нулём $\varnothing$ и единицей A.*

σ- и полные булевы алгебры

Пример 6.4 (*из аксиоматики теории вероятностей*). σ-алгебра подмножеств пространства элементарных событий есть алгебра множеств и, следовательно, булева алгебра.

Булева алгебра, в которой операции $\sqcup$ и $\sqcap$ определены для произвольной совокупности её элементов называется полной.

Любая алгебра множеств — полная



Булева алгебра отображений

Теорема 6.5. *Пусть* $\mathcal{B} = \langle B, \sqcup, \sqcap, ', o, \iota \rangle$ *— булева алгебра и* A *— непустое множество. Тогда множество* B^A *всех отображений из* A *в* B *также будет булевой алгеброй относительно «поточечных» операций* $\dot\sqcup$, $\dot\sqcap$ *и* $'$*:*

$$(f')(x) = (f(x))'$$

$$(f \dot\sqcup g)(x) = f(x) \sqcup g(x), \quad (f \dot\sqcap g)(x) = f(x) \sqcap g(x),$$

для любых $f, g \in B^A$*. Нулём и единицей* B^A *будут постоянные отображения* $f_0(x) \equiv o$ *и* $f_1(x) \equiv \iota$ *соответственно;* $x \in A$.

Доказательство. Проверка аксиом булевой алгебры. □

При $A = B^n$ получим булеву алгебру B^{B^n} всех функций из B^n в B, и если $B = \mathbf{2}$ — булеву алгебру $\mathbf{2}^{\mathbf{2}^n}$ всех булевых функций от n переменных. Изоморфизм булевых алгебр: определение

Определение 6.6. Пусть даны две булевы алгебры B_1 и B_2 и биекция $\varphi\colon B_1 \to B_2$ такая, что равенства

$$\varphi(x \sqcup y) = \varphi(x) \sqcup \varphi(y)\,, \quad \varphi(x \sqcap y) = \varphi(x) \sqcap \varphi(y)\,, \quad \varphi(x') = \varphi(x)$$

справедливы для всех $x, y \in B_1$.
Тогда говорят, что φ — булев изоморфизм между B_1 и B_2, а данные алгебры булево изоморфны (символически $B_1 \cong_b B_2$).

Замечание. Из указанных равенств следует

$$\varphi(o) = o \text{ и } \varphi(\iota) = \iota :$$

Действительно: $\varphi(o) = \varphi(x \sqcap x') = \varphi(x) \sqcap \varphi(x') = \varphi(x) \sqcap \varphi(x)' = o$ и аналогично для $\varphi(\iota)$.

Изоморфизм булевых алгебр: примеры

Пример 6.7. 1. Тривиальная алгебра множеств, очевидно, изоморфна алгебре $\mathbf{2} = \langle \{0, 1\}, \vee, \cdot, {}^-, 0, 1 \rangle$, которую будем называть алгеброй высказываний или алгеброй Буля (символ $\cdot$ в формулах будем, как правило, опускать, но иногда использовать вместо него символ $\&$).

2. Определим для булевой алгебры $\mathcal{B} = \langle B, \sqcup, \sqcap, ', o, \iota \rangle$ двойственную к ней

$\mathcal{B}^* = \langle B^*, \sqcup^*, \sqcap^*, '^*, o^*, \iota^* \rangle$, положив $B^* = B$, $\sqcup^* = \sqcap$, $\sqcap^* = \sqcup$, $'^* = '$, $o^* = \iota$, $\iota^* = o$. В силу принципа двойственности будем иметь $B^* \cong_b B$.

3. Тотальная алгебра над n-элементным множеством $A = \{a_1, \ldots, a_n\}$ изоморфна булевой алгебре n-мерных двоичных векторов $\mathbf{2}^n$.

Булевы подагебры. Теорема Стоуна о представлении Если $\mathcal{B}$ — булева алгебра и B_1 такое подмножество её носителя, что все операции на B_1 являются сужениями операций на B, то B_1 — подалгебра B (символически $\mathcal{B}_1 \leqslant \mathcal{B}$).

Теорема 6.8 (Стоун). *Всякая булева алгебра изоморфна подходящей алгебре множеств: для любой булевой алгебры $\mathcal{B}$ существует такое множество M, что $\mathcal{B} \hookrightarrow \mathcal{P}(M)$.*

Теорема Стоуна утверждает, что $\mathcal{B} \cong_b \mathcal{B}_1 \leqslant \mathcal{P}(M)$.

Алгебраические кольца Кольцом называется АС $\langle R, +, \cdot, 0 \rangle$, где R — множество, содержащее элемент нуль (0), на котором определены две бинарные операции сложение $(+)$ и умножение $(\cdot)$ такие, что для любых $x, y, z \in R$ справедливы соотношения

$$(x + y) + z = x + (y + z), \quad x + y = y + x,$$
$$x + 0 = x, \quad \forall x \, \exists y \colon (x + y = 0)$$

(указанное означает, что редукт $\langle R, +, 0 \rangle$ кольца есть абелева группа по сложению, или модуль) и

$$(x+y)\cdot z \;=\; x\cdot z + y\cdot z\,, \qquad x\cdot(y+z) \;=\; x\cdot y + x\cdot z,$$

(дистрибутивность умножения по отношению к сложению). Алгебраические кольца: напоминание Нуль кольца единственен.
Элемент y такой, что $x+y \;=\; 0$ называют обратным к x, его обозначение $(-x)$ в силу единственности.

Если умножение обладает свойством ассоциативности

$$(x\cdot y)\cdot z \;=\; x\cdot(y\cdot z)$$

и/или коммутативности

$$x\cdot y \;=\; x\cdot y,$$

то и кольцо называют соответствующе.

Если кольцо содержит единицу 1 — уникальный элемент, для которого

$$x\cdot 1 \;=\; 1\cdot x \;=\; x,$$

то говорят о кольце с единицей (унитальном): $\langle\, R,\, +,\, \cdot,\, 0,\, 1\,\rangle$. Булевы кольца

Определение 6.9. Ассоциативное кольцо, обладающие свойством $x^2 = x$ для любого своего элемента называется булевым кольцом.

Теорема 6.10. *Булево кольцо* $\langle\, R,\, +,\, \cdot,\, 0\,\rangle$ *коммутативно и* $-x \;=\; x$.

Теорема 6.11. *Пусть* $\mathcal{B} \;=\; \langle\, B,\, \sqcup,\, \sqcap,'\,,\, o,\, \iota\,\rangle$ — *булева алгебра.*
Для любых $x,\, y \in B$ *положим*

$$x+y \;=\; (x\sqcap y')\sqcup(x'\sqcap y)\,, \quad x\cdot y \;=\; x\sqcap y.$$

Тогда $AC\,\mathcal{B}^* = \langle\, B,\, +,\, \cdot,\, o,\, \iota \,\rangle$ *— булево кольцо с единицей* ι.

Основным примером булева кольца и является как раз кольцо $\langle\, \mathcal{P}(A),\, \oplus,\, \cap,\, \varnothing,\, A \,\rangle$.

Теорема 6.12. *Пусть* $\mathcal{R} = \langle\, R,\, +,\, \cdot,\, 0,\, 1 \,\rangle$ *— булево кольцо с единицей.*
Для любых $x,\, y \in R$ *положим*

$$x \sqcup y = x + y + x \cdot y, \quad x \sqcap y = x \cdot y\,, \quad x' = x + 1.$$

Тогда $AC\,\mathcal{R}^* = \langle\, R,\, \sqcup,\, \sqcap,'\,,\, 0,\, 1 \,\rangle$ *— булева алгебра.*

Определение 6.13. АС $\langle\, B,\, \sqcup,\, \sqcap,'\,,\, \sqsubseteq,\, o,\, \iota \,\rangle$ такая, что $\langle\, B,\, \sqcup,\, \sqcap,'\,,\, o,\, \iota \,\rangle$ — булева алгебра, а отношение $\sqsubseteq$ задаются по правилу

$$x \sqsubseteq y \;\triangleq\; x \sqcap y = x \;\; (\text{или} \;\; x \sqsubseteq y \;\triangleq\; x \sqcup y = y)$$

называется булевой структурой.

Булева алгебра = дистрибутивная решётка с дополнениями и в ней справедлив модулярный закон

$$Mod:\; x \sqsubseteq y \;\Rightarrow\; x \sqcup (y \sqcap z) = y \sqcap (x \sqcup z)$$

Конусы и грани ч.у. множества

Определение 6.14. Пусть $\langle\, P,\, \sqsubseteq \,\rangle$ — ч.у. множество и $A \subseteq P$.
Множества $A^{\triangle}$ и $A^{\triangledown}$ определяемые условиями

$$A^{\triangle} = \left\{ x \in P \mid \underset{A}{\forall} a \;(\, a \sqsubseteq x) \right\} \quad \text{и}$$

$$A^{\triangledown} = \left\{ x \in P \mid \underset{A}{\forall} a \;(\, x \sqsubseteq a) \right\}$$

называются *верхним* и *нижним конусами множества* A,
а их элементы — *верхними* и *нижними гранями множества* A соответственно.

Для одноэлементного множества $A = \{a\}$ используются обозначения $a^{\triangle}$ и $a^{\triangledown}$.

Понятно, например, что если $a \sqsubseteq b$, то $a^{\triangle} \cap b^{\triangledown} = [a, b]$.

Определение 6.15. Пусть $\langle P, \sqsubseteq \rangle$ — ч.у. множество и $A \subseteq P$.
Если в $A^{\triangle}$ существует наименьший элемент, то он называется *точной верхней гранью множества* A и обозначается $\sup A$.
Если в $A^{\triangledown}$ существует наибольший элемент, то он называется *точной нижней гранью множества* A и обозначается $\inf A$.

Если $\sup A$ или $\inf A^{\triangle}$ существует, то $\sup A = \inf A^{\triangle}$ и двойственно,
если $\inf A$ или $\sup A^{\triangledown}$ существует, то $\inf A = \sup A^{\triangledown}$.

6.2 Булевы многочлены

Определение 6.16. Пусть $X_n = \{x_1, \ldots, x_n\}$ — n-элементное множество *неизвестных* или *переменных*.

Булевыми многочленами над X_n называют строки символов, удовлетворяющие следующим условиям:

1) $x_1, \ldots, x_n, 0, 1$ — булевы многочлены;

2) если p и q — булевы многочлены, то таковыми являются и $(p \sqcup q)$, $(p \sqcap q)$, (p').

Таким образом, булевы многочлены — формулы из переменных и констант 0 и 1 над множеством символов $\{ \sqcup, \sqcap, ' \}$.

Множество всех булевых многочленов над X_n обозначаем M_n.

Запись $p = q$ (читается: данные многочлены равны) означает *синтаксическое тождество* многочленов p и q, т. е. они *совпадают как строки символов.*

Далее пользуемся известными правилами экономии скобок (опускаем внешние скобки, учитываем приоритет операций) и считаем, что многочлены равны, если они совпадают при восстановлении всех скобок.

Булев многочлен над n (далее $n \geqslant 1$) переменными можно рассматривать как многочлен над $n+1$ переменной, поэтому

$$M_1 \subset M_2 \subset \ldots \subset M_n \subset M_{n+1} \subset \ldots .$$

M_n не есть булева алгебра, т.к., например, $x_1 \sqcup x_2 \neq x_2 \sqcup x_1$.

Для отождествления подобных выражений введём понятие полиномиальной функции.

Определение 6.17. Пусть $\mathcal{B} = \langle B, \sqcup, \sqcap, ', o, \iota \rangle$ — булева алгебра и p — булев многочлен из M_n.
Обозначим через $p_{\mathcal{B}}(b_1, \ldots, b_n)$ элемент из B, который получается из p заменами $x_i \mapsto b_i \in B$, $i = 1, \ldots, n$, $0 \mapsto o$, $1 \mapsto \iota$. Тогда отображение

$$p_{\mathcal{B}} : B^n \to B$$

называется *полиномиальной функцией* (п.ф.), *индуцированной булевым многочленом* p *на* $\mathcal{B}$.

Пример. Пусть $p = x_1 \sqcup x_2$ и $\mathcal{B} = \mathbf{2}^3$ с носителем $\{0, \overline{a}, b, c, \overline{ab}, ac, bc, 1\}$.

Тогда

$$p_{\mathcal{B}}(a, b) = a \vee b = ab;\ p_{\mathcal{B}}(a, 1) = a \vee 1 = 1;\ p_{\mathcal{B}}(a, ab) = a \vee ab = ab.$$

Пример, как разные булевы многочлены могут индуцировать одну и ту же полиномиальную функцию.

Пример 6.18 (*везде* $n = 2$). 1. Пусть $p = x_1 \sqcup x_2$, $q = x_2 \sqcup x_1$ и $\mathcal{B} = \mathbf{2}$. Тогда

$$p \neq q,\ p_{\mathcal{B}} = a \vee b,\ \ q_{\mathcal{B}} = b \vee a,\ a, b \in \{0, 1\},\ \text{т. е. } p_{\mathcal{B}} = q_{\mathcal{B}},$$

поскольку при любой замене в этих выражениях букв a и b элементами $\{0, 1\} = \mathbf{2}$ получим один и тот же элемент.

2. Пусть $p = (x_1 \sqcup x_2)'$, $q = x_1' \sqcap x_2'$ и $\mathcal{B} = \mathcal{P}(A)$, $A \neq \varnothing$.

Тогда опять

$$p \neq q, \text{ и } \ p_{\mathcal{B}} = \overline{X \cup Y},\ \ q_{\mathcal{B}} = \overline{X} \cap \overline{Y},$$

где $X, Y \subseteq A$, и снова $p_{\mathcal{B}} = q_{\mathcal{B}}$.

Определение 6.19. Два булевых многочлена $p, q \in M_n$ называются *эквивалентными*, символически $p \sim q$, если равны их полиномиальные функции на $\mathbf{2}$: $p \sim q \;\Leftrightarrow\; p_{\mathbf{2}} = q_{\mathbf{2}}$.

$\sim$ — отношение эквивалентности на M_n (легко проверяется).

Пример 6.20 (*предыдущий*, $n = 2$; $a, b \in \{0,1\} = \mathbf{2}$). 1. Если $p = x_1 \sqcup x_2$, $q = x_2 \sqcup x_1$, то

$$p_{\mathbf{2}} = a \vee b = b \vee a = q_{\mathbf{2}} \text{ и } p \sim q.$$

2. Если $p = (x_1 \sqcup x_2)'$, $q = x_1' \sqcap x_2'$, то

$$p_{\mathbf{2}} = \overline{a \vee b} = \overline{a} \cdot \overline{b} = q_{\mathbf{2}} \text{ и снова } p \sim q.$$

Обозначим через $P_n(\mathcal{B}) = \{\, p_{\mathcal{B}} \mid p \in M_n \,\}$ множество полиномиальных функций, индуцированных всеми многочленами из M_n на $\mathcal{B}$.

Например, пусть $\mathcal{B} = \mathbf{2}^3 = \langle\, \{0,1\}^3, \vee, \cdot, {}^-, 0, 1 \,\rangle$. Тогда $P_n(\mathbf{2}^3)$ — все функции, выражающиеся формулами от аргументов $x_1, \ldots, x_n$ над множеством связок $\{\, \vee, \cdot, {}^- \,\}$, причём каждый аргумент может принимать любое из 8 значений $\{0,1\}^3$.

Обозначим для булевой алгебры $\mathcal{B}$ с носителем B через $F_n(\mathcal{B})$ множество всех функций из B^n в B : $F_n(\mathcal{B}) \triangleq B^{B^n}$.
Ясно, что это есть булева алгебра и $|P_n(\mathcal{B})| \subset F_n(\mathcal{B})$.

Тогда, например, $\left|F_1(\mathbf{2}^3)\right| = 8^8 = 16\,777\,216$, а $P_1(\mathbf{2}^3) = \{\, [0]_\sim, [1]_\sim, [x]_\sim, [\bar{x}]_\sim \,\}$, т. е. $\left|P_1(\mathbf{2}^3)\right| = 4$.

Теорема 6.21. *Если* $\mathcal{B} = \langle B, \sqcup, \sqcap, ', o, \iota \rangle$ *— булева алгебра, то*

$$1.\ P_n(\mathcal{B}) \leqslant F_n(\mathcal{B}); \qquad 2.\ P_n(\mathcal{B})/\!\sim\ \cong_b P_n(\mathbf{2}).$$

Доказательство. 1. Убедимся в устойчивости множества функций $P_n(\mathcal{B})$ относительно операций $\sqcup$, $\sqcap$, $'$, а также в принадлежности ему постоянных функций $f_0 \equiv o$ и $f_1 \equiv \iota$.

Для $\sqcup$ и $b = (b_1, \ldots, b_n) \in B^n$ имеем

$$(p_{\mathcal{B}} \sqcup q_{\mathcal{B}})(b) \ = \ p_{\mathcal{B}}(b) \sqcup q_{\mathcal{B}}(b) \ = \ (p \sqcup q)_{\mathcal{B}}(b) \in P_n(\mathcal{B})$$

для произвольного $b \in B^n$ и аналогично для $\sqcap$ и $'$. Кроме того, $p_{\mathcal{B}}(0) = o$, $p_{\mathcal{B}}(1) = \iota$.

2. Определим отображение $\varphi\colon P_n(\mathbf{2}) \to P_n(\mathbf{2})/\!\sim$, переводящее п.ф. $p_{\mathbf{2}}$ в класс эквивалентности $[p]_\sim \in P_n(\mathbf{2})/\!\sim$.

Данное определение корректно, т.к.

$$p_{\mathbf{2}} \ = \ q_{\mathbf{2}} \ \Rightarrow \ p \sim q \ \Rightarrow \ [p]_\sim = [q]_\sim.$$

Легко проверить, что φ и есть искомый булев изоморфизм. □

С помощью теоремы Стоуна показывается, что полиномиальные функции, соответствующие эквивалентным многочленам, совпадают на любой булевой алгебре, а не только на $\mathbf{2}$, то есть справедлива

Теорема 6.22. *Пусть* $p, q \in M_n$ *и* $p \sim q$. *Тогда для произвольной булевой алгебры* $\mathcal{B}$ *справедливо* $p_{\mathcal{B}} = q_{\mathcal{B}}$.

Следствия (полиномиальная полнота алгебры Буля $\mathbf{2}$). 1. $F_n(\mathbf{2}) \ = \ P_2$ *и* $|P_n(\mathbf{2})/\!\sim| \ = \ 2^{2^n}$.

Это означает, что любая булева функция (из $\mathbf{2}^n$ в $\mathbf{2}$) является полиномальной функцией. Поэтому говорят, что алгебра $\mathbf{2}$ полиномиально полна.

2. *Если $\mathcal{B} \not\cong_b \mathbf{2}$ и мощность носителя $\mathcal{B}$ есть m (в конченом случае $m = 2^k$), то*

$$\left|P_n(\mathcal{B})\right| = \left|P_n(\mathcal{B})/\sim\right| = 2^{2^n} < m^{m^n} = |F_n(\mathcal{B})|,$$

т. е. $P_n(\mathcal{B}) \subset F_n(\mathcal{B})$.

Это означает, что $\mathbf{2}$ — единственная полиномиально полная алгебра.

Традиционное для дискретной математики обозначение $F_n(\mathbf{2}) = P_2$ или P_2^n.

Часто возникает потребность заменить данный многочлен эквивалентным ему более простым многочленом.

Для этого вводят т.н. нормальные формы многочленов: ДНФ, КНФ и, аналогично, АНФ (полиномы Жегалкина) для булева кольца соответствующей булевой алгебры.

Совокупность нормальных форм обеспечивает наличие системы представителей для каждого класса эквивалентности множества M_n.

ЊРазложение Шеннона булевой функции $f(x) \in P_2$

$$f(x) = ax \vee b\overline{x} = f(1)x \vee f(0)x$$

6.3 Преобразования булевых уравнений. Простейшие уравнения в 2

Будем решать «*булевы уравнения*» задаваемые полиномами.
Равенство $p = q$ говорит, что многочлены p и q идентичны.

Определение 6.23. Пару $(p,\, q)$, где $p, q \in M_n$, назовём (булевым) уравнением.

Пусть $\mathcal{B}$ — булева алгебра с носителем B.
Элемент $(b_1,\, \ldots,\, b_n) \in B^n$ называется решением уравнения $(p,\, q)$ в булевой алгебре $\mathcal{B}$, если

$$p_{\mathcal{B}}(b_1,\, \ldots,\, b_n) \,=\, q_{\mathcal{B}}(b_1,\, \ldots,\, b_n).$$

Множество $\left\{\, (p_i,\, q_i) \mid i = \overline{1,m} \,\right\}$ образует систему уравнений.
Решением системы называют общее решение всех её уравнений.

Уравнение $(p,\, q)$ допустимо записывать в виде $p = q$.

Например, $\overline{x}_1 x_2 \vee x_3 \,=\, x_1(x_2 \vee x_3)$ — уравнение в $\mathbf{2}$, а (101) — его решение, поскольку в $(\overline{1}\cdot 0)\vee 1 = 1\cdot(0\vee 1)$.

Теорема 6.24 (о преобразовании булевых уравнений). *Уравнения $p \,=\, q$ и $(p \sqcap q') \sqcup (p' \sqcap q) \,=\, 0$, где p и q — булевы многочлены, имеют одни и те же решения.*

Доказательство. Пусть

$$p, q \in M_n, \quad \mathcal{B} \,=\, \langle\, B,\, \sqcup,\, \sqcap,'\,,\, o,\, \iota \,\rangle$$

— булева алгебра и $(b_1, \ldots, b_n) \in B^n$.
Положим $a = p_{\mathcal{B}}(b_1, \ldots, b_n)$ и $b = q_{\mathcal{B}}(b_1, \ldots, b_n)$. Тогда

$$a = b \Rightarrow (a \sqcap b') \sqcup (a' \sqcap b) = (a \sqcap a') \sqcup (a' \sqcap a) = o \sqcup o = o,$$

и

$$(a \sqcap b') \sqcup (a' \sqcap b) = o \;\Leftrightarrow\; \left\{ \begin{array}{l} a \sqcap b' = o \\ a' \sqcap b = o \end{array} \right. \overset{DeM1}{\Longleftrightarrow}$$

$$\Leftrightarrow \left\{ \begin{array}{l} a \sqcap b' = o \\ a \sqcup b' = \iota \end{array} \right. \;\Leftrightarrow\; a = b'' \;\Leftrightarrow\; a = b\,.$$

□

Следствия (преобразование уравнения $p = q$ к виду $r = 0$).

Уравнения

$$p = q \quad и \quad (p \sqcap q) \sqcup (p' \sqcap q') \;=\; 0,$$

где p и q — булевы многочлены, имеют одни и те же решения в любой булевой алгебре.

Уравнение будем, как правило, сразу записывать в сигнатуре указанной булевой алгебры и считать переменные $x_1, \ldots$ её элементами.

2. *Любое булево уравнение (или систему), заданную в алгебре логики* **2** *можно привести к эквивалентным видам $p = 0$ и $q = 1$, где p, q — ДНФ и/или КНФ.*

   Справедливость утверждения следует из полиномиальной полноты алгебры **2**.

3. *Система* $\{ (p_i, q_i) \mid i = \overline{1, m} \}$ *эквивалентна одному уравнению*

$$p_1q_1' \vee p_1'q_1 \vee p_2q_2' \vee p_2'q_2 \vee \ldots \vee p_mq_m' \vee p_m'q_m \;=\; 0.$$

Решение булевых уравнений: примеры

① Решим булево уравнение $x_1 = x_2$ в $\mathbf{2}$.

Преобразуем уравнение

$$x_1 = x_2 \;\Leftrightarrow\; (x_1\overline{x}_2) \vee (\overline{x}_1x_2) = 0 \;\Leftrightarrow$$
$$\Leftrightarrow\; (x_1 \vee \overline{x}_1) \cdot (x_1 \vee x_2) \cdot (\overline{x}_1 \vee \overline{x}_2) \cdot (x_2 \vee \overline{x}_2) \;\Leftrightarrow$$
$$\Leftrightarrow\; (x_1 \vee x_2) \cdot (\overline{x}_1 \vee \overline{x}_2) = 0.$$

В $\mathbf{2}$ это эквивалентно условиям

$$\left[\begin{array}{l} x_1 \vee x_2 \;=\; 0, \\ x_1' \vee x_2' \;=\; 0, \end{array}\right. \quad \text{откуда} \quad \left[\begin{array}{l} x_1 = x_2 = 0, \\ x_1 = x_2 = 1. \end{array}\right.$$

Т.о. решениями исходного уравнения будут наборы (00) и (11) из $\mathbf{2}^2$.

② Решим булево уравнение $x_1 \cdot x_2 = x_3$ в $\mathbf{2}$.

Преобразуем уравнение

$$x_1{\cdot}x_2 \;=\; x_3 \;\Rightarrow\; (\overline{x}_1{\vee}x_2{\vee}x_3)(x_1{\vee}\overline{x}_2{\vee}x_3)(\overline{x}_1{\vee}\overline{x}_2{\vee}\overline{x}_3) \;=\; 0$$

Отсюда получаем искомые решения: (000), (010), (100), (111).

Замечание: получение для данной формулы эквивалентной КНФ, вообще говоря, сопряжено со столь значительными вычислительными трудностями, что может оказаться практически невозможным.

③ Решить заданную в $\mathbf{2}$ систему БУ

$$\{\, (x_1x_2,\; x_1x_3 \vee x_2),\; (x_1 \vee \overline{x}_2,\; x_3) \,\}.$$

Перепишем систему в привычном виде

$$\begin{cases} x_1x_2 & = x_1x_3 \vee x_2, \\ x_1 \vee \overline{x}_2 & = x_3. \end{cases}$$

По теореме о преобразовании булевых уравнений эта система эквивалентна единственному уравнению

$$x_1x_2\overline{(x_1x_3 \vee x_2)} \vee \overline{(x_1x_2)}(x_1x_3 \vee x_2) \vee (x_1 \vee \overline{x}_2)\overline{x}_3 \vee \\ \vee \overline{(x_1 \vee \overline{x}_2)}x_3 = 0.$$

Преобразуя левую часть в СКНФ, получим эквивалентное заданной системе уравнение

$$(x_1 \vee x_2 \vee \overline{x}_3)(\overline{x}_1 \vee \overline{x}_2 \vee \overline{x}_3) = 0,$$

т. е. решениями системы будут наборы (001) и (111) из $\mathbf{2}^3$.

Важное замечание Когда решение ищется не в простейшей алгебре $\mathbf{2}$, а в произвольной булевой алгебре, следование

$$D_1 \sqcap \ldots \sqcap D_l = o \Rightarrow \left[\begin{array}{l} D_1 = o, \\ \ldots \\ D_l = o \end{array} \right.$$

не имеет места.

Поэтому, например, в произвольной булевой алгебре $\mathcal{B} = \langle B, \sqcup, \sqcap, ', o, \iota \rangle$ решением уравнения

$$x_1 \sqcap x_2 = o$$

будет $(b, (b')^{\triangledown}) \in B^2$ и для $\mathcal{B} = \mathbf{2}^3$ подходит пара ненулевых элементов

$$((100), (010)) \in (\mathbf{2}^3)^2.$$

6.4 Уравнения с одним неизвестным

Далее нас будет интересовать зависимость значений одних неизвестных решения БУ от других.

- Пусть (p, q) — уравнение в булевой алгебре $\mathcal{B}$ и $p, q \in M_{n+m},\ n, m \geqslant 0,\ n + m \geqslant 1$.
- Множество неизвестных с индексами m, $m + 1$, $\ldots, n + m$ назовём параметрами.
- Элементы носителя $\mathcal{B}$, соответствующие аргументам-параметрам полиномиальных функций $p_{\mathcal{B}}$ и $q_{\mathcal{B}}$ будем обозначать символами a, b, ...
- Формулу вида

  $$p_{\mathcal{B}}(x_1, \ldots, x_n, a, \ldots) = q_{\mathcal{B}}(x_1, \ldots, x_n, a, \ldots)$$

  будем называть *булевым уравнением с параметрами и n неизвестными (в алгебре $\mathcal{B}$)*.

Алгоритм 1

Пусть дано БУ $p = q$ с одним неизвестным x в булевой структуре $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \sqsubseteq, o, \iota \rangle$. Шаг ① Приводим уравнение $p = q$ к равносильному с o в правой части: $r = 0$.

Шаг ② Приводим уравнение $r = 0$ к равносильному уравнению вида

$$(a \sqcap x) \sqcup (b \sqcap x') = o,$$

где элементы B a и b — параметры.

Шаг ③ Заменяем полученное уравнение на эквивалентную систему

$$\begin{cases} a \sqcap x = o, \\ b \sqcap x' = o. \end{cases}$$

Шаг ④ Если $b \not\sqsubseteq a'$, то исходное уравнение решений не имеет.

Иначе $\boxed{b \sqsubseteq a' \Leftrightarrow a \sqcap b = o}$ — *условие разрешимости уравнения* и его решение — любой элемент x из B такой, что

$$b \sqsubseteq x \sqsubseteq a' \text{ — решение в } \textit{интервальной форме}$$
$$\Leftrightarrow x \in b^{\triangle} \cap (a')^{\triangledown}$$

или

$$x = (b \sqcup u) \sqcap a' = (a' \sqcap u) \sqcup b,$$
$$u \text{ — произвольный элемент } B$$
$$\text{— решение в } \textit{функциональной форме}$$
$$x = (a' \sqcap u) \sqcup (b \sqcap u')$$
$$\text{— } \textit{симметричная функциональной форма.}$$

Теорема 6.25 (основная о решении булевых уравнений). *Результатом выполнения Алгоритма 1 является решение булева уравнения относительно единственного неизвестного.*

Доказательство. Проведём обоснование шагов алгоритма.

Шаг ① Основанием для равносильной замены $p = q \Rightarrow r = 0$ служит теорема о преобразовании булевых уравнений.

Шаг ② Приведение уравнения вида $r = 0$ к равносильному $(a \sqcap x) \sqcup (b \sqcap x') = o$ основано на разложении Шеннона по переменной x.

Выражение последнего вида назовём канонической формой булева уравнения.

Шаг ③ Замена уравнение в канонической форме на эквивалентную систему

$$a \sqcap x = o,\ b \sqcap x' = o$$

основывается на лемме об основных свойствах элементов булевой алгебры.

Шаг ④ Обоснование:
1. Имеем $b \sqsubseteq x \sqsubseteq a'$,

$$a \sqcap x = o \Leftrightarrow (a \sqcap x) \sqcup a' = a' \Leftrightarrow$$
$$\Leftrightarrow (a \sqcup a') \sqcap (x \sqcup a') = a' \Leftrightarrow$$
$$\Leftrightarrow x \sqcup a' = a' \Leftrightarrow x \sqsubseteq a'$$
$$\text{и аналогично } b \sqcap x' = 0 \Leftrightarrow b \sqsubseteq x.$$

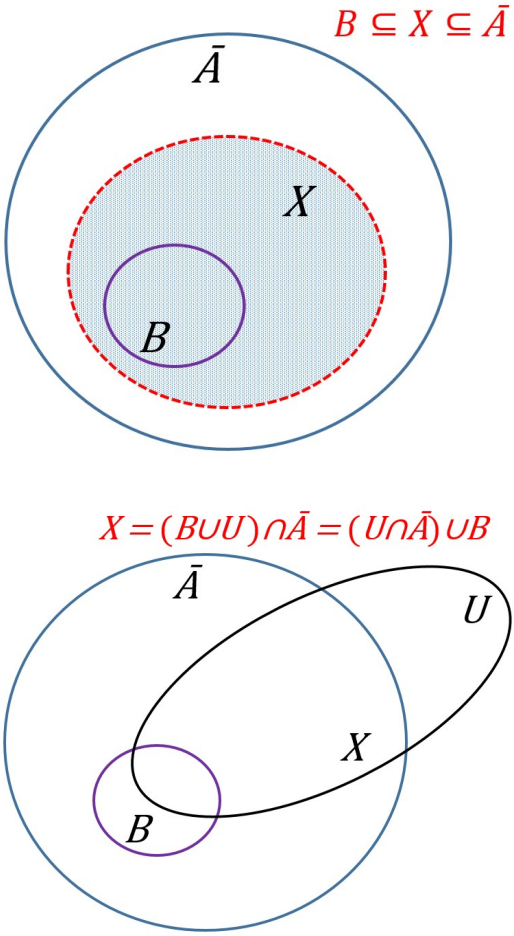
2. $b \sqsubseteq a' \Leftrightarrow b \sqcap a' = b \Leftrightarrow a \sqcap b = o$ — условие существования решения.

3. Справедливость формулы решения в функциональной форме следует из

$$\begin{cases} b \sqsubseteq x \\ x \sqsubseteq a' \end{cases} \Leftrightarrow \begin{cases} x = b \sqcup u \quad \text{для некоторого } u \in B \\ x \sqcap a' = x \end{cases} \Leftrightarrow$$
$$\Leftrightarrow x = (b \sqcup u) \sqcap a'.$$

Равенство $x = (b \sqcup u) \sqcap a' = (a' \sqcap u) \sqcup b$ при $b \sqsubseteq a'$ выражает модулярный закон.

Симметричная функциональной форма:



$$x = (a' \sqcap u) \sqcup b = (a' \sqcap u) \sqcup (b \sqcap (u \sqcup u') = (a' \sqcap u) \sqcup (b \sqcap u'),$$

поскольку $b \sqcap u' \sqsubseteq b \sqsubseteq a' \sqsubseteq x$. □

Решение БУ $(A \cap X) \cup (B \cap \overline{X})$: диаграмма Венна

В частном случае $\mathcal{B} = \mathbf{2}$ по интервальной формуле получим решения:

a	b	x
0	0	$\{0,1\}$
0	1	1
1	0	0
1	1	$\varnothing$

Эти решения, естественно, совпадают с решениями по функциональной формуле, если положить $u = 0$ и $u = 1$:

$$b \leqslant \overline{a} \;\Rightarrow\; b \leqslant x \leqslant \overline{a} \;\Leftrightarrow\; \left[\begin{array}{l} x = \overline{a}, \\ x = b. \end{array}\right.$$

Решение БУ $\widetilde{\alpha} \cdot \widetilde{x} \vee \widetilde{\beta} \cdot \overline{\widetilde{x}}$ в $\mathbf{2}^n$.
Если $B = \mathbf{2}^n$, то имеем многомерный вариант предыдущего случая:

- интервальная форма при $\widetilde{\beta} \preccurlyeq \overline{\widetilde{\alpha}}$ задаёт булев подкуб $\mathbf{2}^n$, натянутый на вершины $\widetilde{\beta}$ и $\overline{\widetilde{\alpha}}$ (при $\widetilde{\beta} \succcurlyeq \overline{\widetilde{\alpha}}$ решений нет);

- в функциональной форме $\widetilde{x} = (\widetilde{\beta} \vee \widetilde{\upsilon}) \cdot \overline{\widetilde{\alpha}}$ полагаем $\upsilon = (- \ldots -)$, операции $\vee$ и $\cdot$ применяем к векторам из $\mathbf{2}^n$ покомпонентно по правилам

$$\widetilde{\alpha} \vee \widetilde{\beta} = \max\left\{\widetilde{\alpha}, \widetilde{\beta}\right\}, \; \widetilde{\alpha} \cdot \widetilde{\beta} = \min\left\{\widetilde{\alpha}, \widetilde{\beta}\right\}, \; 0 \leqslant - \leqslant 1,$$

и в полученном векторе $\widetilde{x}$ символы $(-)$ заменяем на 0 и 1 всевозможными способами.

Например, если в $\mathbf{2}^4$ имеем

$$\widetilde{\alpha} = (0001) \;\text{ и }\; \widetilde{\beta} = (1000), \text{ то } \widetilde{x} = (1 - -0),$$

и решениями исходного уравнения будет любой из векторов (1000), (1010), (1100), (1110).

Решение БУ с одним неизвестным: пример Решим булево уравнение $x \sqcup c = d$ в произвольной булевой структуре $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \sqsubseteq, o, \iota \rangle$.

Шаг ① $x \sqcup c = d \Leftrightarrow ((x \sqcup c)' \sqcap d) \sqcup ((x \sqcup c) \sqcap d') = o$.

Шаг ② $((x \sqcup c)' \sqcap d) \sqcup ((x \sqcup c) \sqcap d') =$

$$= (x' \sqcap c' \sqcap d) \sqcup (x \sqcap d') \sqcup (c \sqcap d') =$$
$$= (x' \sqcap c' \sqcap d') \sqcup (x \sqcap d') \sqcup (x \sqcap c \sqcap d') \sqcup (x' \sqcap c \sqcap d') =$$
$$= (x \sqcap \underbrace{(d' \sqcup (c \sqcap d'))}_{d'}) \sqcup (x' \sqcap ((c' \sqcap d) \sqcup (c \sqcap d'))) = o.$$

Шаг ③ Имеем

$$\begin{cases} d' \sqcap x = o, \\ ((c' \sqcap d) \sqcup (c \sqcap d')) \sqcap x' = o \end{cases}.$$

Шаг ④ Исходное уравнение имеет решение, если и только если

$$(c' \sqcap d) \sqcup (c \sqcap d') \sqsubseteq d.$$

Покажем, что данное условие эквивалентно $c \sqsubseteq d$:

$$((c' \sqcap d) \sqcup (c \sqcap d')) \sqsubseteq d \Leftrightarrow (c' \sqcap d) \sqcup (c \sqcap d') \sqcup d = d \Leftrightarrow$$
$$\Leftrightarrow d \sqcup (c \sqcap d') = d \Leftrightarrow (d \sqcup (c \sqcap d')) \sqcap c = d \sqcap c \Leftrightarrow$$
$$\Leftrightarrow (c \sqcap d) \sqcup (c \sqcap d') = d \sqcap c \Leftrightarrow c = c \sqcap d \Leftrightarrow c \sqsubseteq d.$$

Общее решение исходного уравнения —

$$x = ((c' \sqcap d) \sqcup (c \sqcap d') \sqcup u) \sqcap d = (c' \sqcap d) \sqcup (u \sqcap d) = d \sqcap (c' \sqcup u),$$

где u — произвольный элемент B.

Булевы «неравенства» Методы решения уравнений в булевой алгебре позволяют решать и «неравенства»

Теорема 6.26. *Следование* $p \sqsubseteq q$ *и уравнение* $p \sqcap q' = o$ *имеют одни и те же решения.*

Доказательство.

$$p \sqsubseteq q \;\Leftrightarrow\; p \sqcap q = p \;\Leftrightarrow\; \overbrace{((p \sqcap q) \sqcap p')}^{=o} \sqcup ((p \sqcap q)' \sqcap p) = o \;\Leftrightarrow$$
$$\Leftrightarrow\; (p' \sqcup q') \sqcap p = o \;\Leftrightarrow\; p \sqcap q' = o.$$

□

6.5 Беспараметрические уравнения со многими неизвестным в алгебре логики

Идея метода — многократное применение Алгоритма 1 при последовательном исключении булевых неизвестных.

Опишем метод для уравнений в булевой структуре

$$\mathbf{2} = \langle \{0,1\}, \vee, \cdot, {}^{-}, \leqslant, 0, 1 \rangle.$$

Пусть БУ задано в виде $f(x_1, \ldots, x_n) = 0$ $(*)$, где f — полином.

Определим формулы

$$f_p(x_1, \ldots, x_p) = \mathop{\&}_{(\alpha_{p+1}, \ldots, \alpha_n)} f(x_1, \ldots, x_p, \alpha_{p+1}, \ldots, \alpha_n),$$
$$\alpha_i \in \{0, 1\},\ i = \overline{p+1, n},\ p = \overline{1, n},$$

где конъюнкция берётся по всем двоичным наборам $(\alpha_{p+1}, \ldots, \alpha_n)$.

Итерционный алгоритм исключения переменных
Алгоритм 2

Шаг 1. Записываем исходное уравнение в форме $f_n = 0$, к которой применяем разложение Шеннона по переменной x_n:

$$f_n(x_1, \ldots, x_{n-1}, 1) \cdot x_n \vee f_n(x_1, \ldots, x_{n-1}, 0) \cdot \overline{x}_n = 0.$$

Из обоснования Алгоритма 1 следует, что это равенство эквивалентно

$$f_n(x_1, \ldots, x_{n-1}, 0) \leqslant x_n \leqslant \overline{f_n(x_1, \ldots, x_{n-1}, 1)}$$

при условии выполнения соотношения

$$\underbrace{f_n(x_1, \ldots, x_{n-1}, 1) \cdot f_n(x_1, \ldots, x_{n-1}, 0)}_{f_{n-1}(x_1, \ldots, x_{n-1})} = 0.$$

На следующем шаге решаем уравнение $f_{n-1}(x_1, \ldots, x_{n-1}) = 0$.

Шаг $n - p + 1$. Рассматривается уравнение

$$f_p(x_1, \ldots, x_p) = 0, \quad p \in \{n, n-1, \ldots, 1\},$$

которое можно записать в форме (разложение по x_p)

$$f_p(x_1, \ldots, x_{p-1}, 1) \cdot x_p \vee f_p(x_1, \ldots, x_{p-1}, 0) \cdot \overline{x}_p = 0.$$

В свою очередь, данное уравнение эквивалентно соотношению

$$f_p(x_1, \ldots, x_{p-1}, 0) \leqslant x_p \leqslant \overline{f_p(x_1, \ldots, x_{p-1}, 1)},$$

при условии справедливости

$$\underbrace{f_p(x_1, \ldots, x_{p-1}, 1) \cdot f_p(x_1, \ldots, x_{p-1}, 0)}_{f_{p-1}(x_1, \ldots, x_{p-1})} = 0\,.$$

На следующем шаге решаем уравнение $f_{p-1}(x_1, \ldots, x_{p-1}) = 0$.

Шаг n. Решается уравнение

$$f_1(x_1) = 0,$$

откуда получаем

$$f_1(0) \leqslant x_1 \leqslant \overline{f_1(1)}$$

и условие его разрешимости

$$f_0 = f_1(0) \cdot f_1(1) = 0.$$

Из обоснования описанного алгоритма вытекает

Теорема 6.27. *Если $f_0 \neq 0$, то уравнение $(*)$ не имеет решений.*
Иначе, его решение описывается рекуррентным соотношением ($p = n, n-1, \ldots, 1$)

$$f_p(x_1, \ldots, x_{p-1}, 0) \leqslant x_p \leqslant \overline{f_p(x_1, \ldots, x_{p-1}, 1)}.$$

Применяя Алгоритм 2 к уравнению $(*)$: для

определения разрешимости — необходимо вычислить f_0;

нахождения хотя бы одного решения — из последнего неравенства $f_1(0) \leqslant x_1 \leqslant \overline{f_1(1)}$ необходимо найти одно значение $b_1 = x_1$, по которому из предпоследнего неравенства найти одно значение b_2 и т.д.

В результате будет получен набор $(b_1, \ldots, b_n)$ — решение исходного уравнения.

нахождения всех решений — из последнего неравенства находят все допустимые значения $b_1 = x_1$, затем для каждого из найденных b_1 из предпоследнего неравенства находят все допустимые значения b_2 и т.д.

Алгоритм 2: обсуждение. Разделение задач нахождения хотя бы одного решения БУ и всех его связано с тем, что БУ может иметь очень большое число корней. Например, для систем БУ вида

$$\text{ДНФ}_i = 1, \quad i = \overline{1, m},$$

у которых число переменных равно n, число элементарных конъюнкций во всех ДНФ одинаково и равно t, число букв во всех элементарных конъюнкциях одинаково и равно r среднее число решений равно $2^n(1-(1-2^{-r})^t)^m$.

Эти задачи в конечных булевых алгебрах могут быть решены тривиальной проверкой всех комбинаций значений переменных, однако это требует чрезвычайно большого перебора.

Все существующие универсальные методы решения систем БУ не позволяют элиминировать этот пе-

ребор. Причём остаётся открытым вопрос о принципиальной возможности такой элиминации.

Алгоритм 2: пример 1. Найти все решения уравнения $x_1 \supset x_2 = 1$ в структуре **2**.

Шаг ① Записываем исходное уравнение в форме

$$f_2(x_1, x_2) = x_1 \cdot \overline{x}_2 = 0.$$

Применяем разложение Шеннона по переменной x_2 имеем

$$x_1 \cdot \overline{x_2} = f_2(x_1, 1) \cdot x_2 \vee f_2(x_1, 0) \cdot \overline{x}_2 = 0,$$

откуда $f_2(x_1, 1) = 0$ и $f_2(x_1, 0) = x_1$.

Полученное уравнение эквивалентно «двойному неравенству»

$$f_2(x_1, 0) \leqslant x_2 \leqslant \overline{f_2(x_1, 1)}$$

или

$$x_1 \leqslant x_2 \leqslant 1. \qquad (1)$$

при условии $f_1(x_1) = \underbrace{f_2(x_1, 0) \cdot f_2(x_1, 1)}_{\equiv 0} = 0$, которое тривиально выполняется.

Шаг ② Уравнение

$$f_1(x_1) = f_2(x_1, 0) \cdot f_2(x_1, 1) = 0,$$

записывается в форме

$$f_1(1) \cdot x_1 \vee f_1(0) \cdot \overline{x}_1 = 0,$$

где $f_1(1) = f_1(0) = 0$, а его решение в интервальной форме записывается как

$$f_1(0) \leqslant x_1 \leqslant \overline{f_1(1)}$$

или

$$0 \leqslant x_1 \leqslant 1 \qquad (2)$$

при тривиальной выполнимости условия

$$f_0 = \underbrace{f_1(1) \cdot f_1(0)}_{\equiv 0} = 0.$$

Найдём решения исходного уравнения.

Из соотношения (2) получаем значения для x_1:

$$x_1^{(0)} = 0, \quad \text{и} \quad x_1^{(1)} = 1.$$

Их необходимо подставить в (1) для определения x_2.

Подставляя $x_1^{(0)}$, получаем соотношение

$$0 \leqslant x_2 \leqslant 1,$$

откуда $x_2^{(00)} = 0$ и $x_2^{(01)} = 1$, а подставляя $x_1^{(1)}$ —

$$1 \leqslant x_2 \leqslant 1,$$

откуда $x_2^{(1)} = 1$.

Т.о. решениями исходного уравнения будут векторы (00), (01), (11) из $\mathbf{2}^2$, что соответствует строкам с единичным значением функции в таблице операции импликации.

Алгоритм 2: пример 2. Найти все решения уравнения $x_1 \cdot x_2 = x_3$ в алгебре логики.

Шаг ① Преобразовываем исходное уравнение:

$$f_3(x_1, x_2, x_3) = x_1x_2\overline{x}_3 \vee \overline{(x_1x_2)}x_3 =$$
$$= x_1x_2\overline{x}_3 \vee (\overline{x}_1 \vee \overline{x}_2)x_3 = x_1x_2\overline{x}_3 \vee \overline{x}_1x_3 \vee \overline{x}_2x_3 = 0$$

и применяем разложение Шеннона по переменной x_3:

$$f_3(x_1, x_2, x_3) = \underbrace{(\overline{x}_1 \vee \overline{x}_2)}_{f_3(x_1,x_2,1)} \cdot x_3 \vee \underbrace{x_1 x_2}_{f_3(x_1,x_2,0)} \cdot \overline{x}_3 = 0.$$

Решение полученного уравнения в интервальном виде:

$$x_1 x_2 \leqslant x_3 \leqslant \overline{\overline{x}_1 \vee \overline{x}_2} = x_1 x_2. \qquad (1)$$

Условие такого представления —

$$f_2(x_1, x_2) = f_3(x_1, x_2, 1) \cdot f_3(x_1, x_2, 0) = (\overline{x}_1 \vee \overline{x}_2) x_1 x_2 = 0$$

выполняется.

Шаг ② Подставляя в $f_2(x_1, x_2)$ вместо x_2 значения 0 и 1, получаем

$$f_2(x_1, 1) = f_2(x_1, 0) = 0\,.$$

Это влечёт

$$0 \leqslant x_2 \leqslant 1 \qquad (2)$$

при тривиально выполняемом условии

$$f_1(x_1) = f_2(x_1, 1) \cdot f_2(x_1, 0) = 0$$

такого представления.

Шаг ③ Для x_1 получаем интервальное решение

$$0 \leqslant x_1 \leqslant 1 \qquad (3)$$

при $f_0 = f_1(1) \cdot f_1(0) = 0$.

Т.о. исходное уравнение имеет решение и из (3) и (2) получаем $x_1, x_2 \in \{0, 1\}$, а из (2.1) — $x_1 \cdot x_2 \leqslant x_3 \leqslant x_1 \cdot x_2$.

Отсюда решения: (000), (010), (100), (111), совпадающие с ранее найденными.

Алгоритм 2' Алгоритм 2 может быть модифицирован: на $(n - p + 1)$-м шаге проводить разложение

Шеннона возможно по любой переменной с индексом $1, 2, \ldots, p$ и не обязательно по x_p.

Для этого определим функции

$$f_p(\widetilde{x}) = \underset{\widetilde{\alpha}}{\&} f(\widetilde{x}, \widetilde{\alpha}), \quad p = \overline{1,n}, \qquad (**')$$

где $\widetilde{x} = (x_{j_1}, \ldots, x_{j_p})$, $\widetilde{\alpha} = (\alpha_{i_{p+1}}, \ldots, \alpha_{i_n}) \in \mathbf{2}^{n-p}$ и

$$f_{p,k}(\widetilde{x}', 1) = f_p(\widetilde{x})\big|_{x_k=1}, \quad f_{p,k}(\widetilde{x}', 0) = f_p(\widetilde{x})\big|_{x_k=0}.$$

Алгоритм, получающийся из алгоритма Алгоритм 2 заменой определения функций f_p с $(**)$ на $(**')$, выбором тем или иным способом на каждом, кроме последнего, шаге индекса $k \in \{j_1, \ldots, j_p\}$ и заменами $f_p(x_1, \ldots, x_{p-1}, 1) \mapsto f_{p,k}(\widetilde{x}', 1)$ $f_p(x_1, \ldots, x_{p-1}, 0) \mapsto f_{p,k}(\widetilde{x}', 0)$, назовём Алгоритмом 2'.

Алгоритм 2': пример. Найти по Алгоритму 3' все решения (уже решённого) уравнения $x_1 \cdot x_2 = x_3$ в $\mathbf{2}$.

Шаг ① Для уравнения $x_1x_2\overline{x}_3 \vee \overline{x}_1x_3 \vee \overline{x}_2x_3 = 0$ применим разложение Шеннона по переменной x_1 $(k = 1)$:

$$f_3(x_1, x_2, x_3) = (x_2 \vee x_3)(\overline{x}_2 \vee \overline{x}_3) \cdot x_1 \vee \\ \vee (x_2 \vee x_3)(\overline{x}_2 \vee x_3) \cdot \overline{x}_1 = 0,$$

откуда

$$f_{3,1}(x_2, x_3, 1) = x_2\overline{x}_3 \vee \overline{x}_2x_3, \quad f_{3,1}(x_2, x_3, 0) = x_3.$$

Записываем решение данного уравнения в интервальном виде:

$$x_3 \leqslant x_1 \leqslant \overline{x_2\overline{x}_3 \vee \overline{x}_2 x_3} = x_2x_3 \vee \overline{x}_2\overline{x}_3.$$

Условие такого представления —

$$f_2(x_1, x_2) = f_3(x_1, x_2, 1) \cdot f_3(x_1, x_2, 0) = \overline{x}_2 x_3 = 0.$$

Шаг ② Подставляя в $f_2(x_2, x_3)$ вместо x_2 $(k = 2)$ значения 0 и 1, получаем

$$f_{2,2}(x_3, 1) = 0\,, \quad f_{2,2}(x_3, 0) = x_3\,.$$

Это влечёт

$$x_3 \leqslant x_2 \leqslant 1$$

при тривиально выполняемом условии

$$f_1(x_3) = f_{2,2}(x_3, 1) \cdot f_{2,2}(x_3, 0) = 0.$$

такого представления.

Шаг ③ Для x_3 получаем интервальное решение

$$0 \leqslant x_3 \leqslant 1$$

при $f_0 = 0$.

Рассматривая значения x_3, x_2 и x_1 (в данном порядке) с учётом условия $(*)$, получаем их возможные значения

$$\begin{aligned} x_3 &= 1 \;\Rightarrow\; x_2 = 1 \;\Rightarrow\; x_1 = 1, \\ x_3 &= 0 \;\Rightarrow\; x_2 = 0 \;\Rightarrow\; x_1 \in \{0, 1\}, \\ x_3 &= 0 \;\Rightarrow\; x_2 = 1 \;\Rightarrow\; x_1 = 0. \end{aligned}$$

т. е. решения исходного уравнения суть те же векторы (000), (010), (100) и (111).

Наиболее трудоёмкой процедурой данного метода является построение формул f_p. В процессе их построения необходимо производить подстановки наборов значений переменных в f_p. В частности при построении f_0 надо подставить 2^n наборов и общее число

операций будет порядка $\omega \cdot 2^n$,
где ω — сложность подстановки одного набора.

6.6 Решение уравнений в АНФ

Определение 6.28. Константу 1 и выражения вида $x_{i_1} \cdot \ldots \cdot x_{i_r}$, где $\varnothing \neq \{i_1, \ldots, i_r\} \subseteq \{1, \ldots n\}$ называют *элементарными монотонными конъюнкциями* над $X_n = \{0, 1, x_1, \ldots, x_n\}$.

Алгебраический полином над X_n есть либо 1 (полином длины 0), либо выражение вида

$$K_1 + \ldots + K_s,$$

где K_i — попарно различные элементарные монотонные конъюнкции над X_n; $i = 1, \ldots, s$, s — *длина полинома.*

Под записью $p = q$ понимают *синтаксическое тождество* полиномов p и q.

Pl_n — множество всех алгебраических полиномов над X_n.

Ясно, что $Pl_1 \subset Pl_2 \subset \ldots \subset Pl_n \subset Pl_{n+1} \subset \ldots$.

Заметим, что Pl_n не является кольцом, поскольку, например, $x_1 \cdot x_1 \neq x_1$, $x_1 \cdot x_2 \neq x_2 \cdot x_1$ и $K_1 + K_2 \neq K_2 + K_1$.

Для отождествления подобных выражений воспользуемся понятием полиномиальной функции.

Определение 6.29. Пусть $\mathcal{R} = \langle R, +, \cdot, 0, 1 \rangle$ — булево кольцо и p — полином из Pl_n.

Обозначим через $p_{\mathcal{R}}(r_1, \ldots, r_n)$ элемент из R, который получается из p заменами $x_i \mapsto r_i \in R$, $i = 1, \ldots, n$, $0 \mapsto o$, $1 \mapsto \iota$. Тогда отображение

$$p_{\mathcal{R}} : R^n \to R$$

назовём *полиномиальной функцией, индуцированной алгебраическим полином p на $\mathcal{R}$.*

Определение 6.30. Два многочлена $p, q \in Pl_n$ называются эквивалентными (символически $p \sim q$), если равны их полиномиальные функции на $\{0,1\} = \mathbf{2}$, т. е. $p \sim q \Leftrightarrow p_{\mathbf{2}} = q_{\mathbf{2}}$.

Обозначим $P_n(\mathcal{R}) = \{p_{\mathcal{R}} \mid p \in Pl_n\}$ — множество всех полиномиальных функций, индуцированных полиномами из Pl_n на R.

Теорема 6.31. *$Pl_n/\sim$ есть булево кольцо, и $Pl_n/\sim \cong P_n(\mathbf{2})$.*

Элементы $Pl_n/\sim$ называют полиномами Жегалкина (ПЖ).

Теорема Жегалкина и разложение Рида

Теорема 6.32 (И.И.Жегалкин). *Всякая булева функция единственным образом представима в виде полинома Жегалкина.*

Разложение Рида булевой функции $f \in P_2$

$$f(x) = a \cdot x + b = (f(0) + f(1)) \cdot x + f(0)$$

Рассмотрим в булевом кольце уравнение вида

$$a_1 Q_1(x_1, \ldots, x_n) + \ldots + a_r Q_r(x_1, \ldots, x_n) = b, \qquad (*)$$

где $a_1, \ldots, a_r, b \in \{0, 1\}$ — известные коэффициенты, $Q_1(x_1, \ldots, x_n), \ldots, Q_r(x_1, \ldots, x_n)$ — попарно различные монотонные конъюнкции над

Для упрощения записи будем пользоваться сокращением

$$\overline{a} = a + 1.$$

Теорема 6.33 (о существовании решения уравнения в булевом кольце). *Уравнение* $(*)$ *имеет хотя бы одно решение, если*

$$b \cdot \overline{a}_1 \cdot \ldots \cdot \overline{a}_r = 0. \qquad (**)$$

Доказательство. Необходимость. Пусть уравнение $(*)$ имеет корни, а условие $(**)$ не выполняется.
Подставив корни в $(*)$, получим тождество

$$a_1 Q_1 \cdot \ldots \cdot a_r Q_r = b,$$

умножив которое на $\overline{a}_1 \cdot \ldots \cdot \overline{a}_r$, получим $(**)$, что противоречит допущению.

Достаточность. Рассмотрим уравнение с одним неизвестным

$$a \cdot x + b = 0. \qquad (1)$$

Пусть условие $a \cdot b \equiv 0$ выполняется.
Тогда $x = b$ есть корень уравнения (1): действительно, имеем $a \cdot b + b = \overline{a} b$.

Пусть условие $a \cdot b = 0$ выполняется.
Тогда $x = b$ есть корень уравнения (1): действительно, имеем

$$a \cdot b + b \;=\; \overline{a}b.$$

Пусть условие теоремы справедливо для уравнения вида $(*)$ с n неизвестными. Покажем, что в этом случае оно справедливо и для уравнения вида $(*)$ с $n+1$ неизвестными.

Представим уравнение с $n+1$ неизвестными в виде:

$$(a_0 + a_1 Q_1(x_1, \ldots, x_n) + \ldots + a_r Q_r(x_1, \ldots, x_n))x_{n+1} + \\ + b_0 + b_1 P_1(x_1, \ldots, x_n) + \ldots + b_k Q_k(x_1, \ldots, x_n) \;=\; 0.$$

Запишем условие $(**)$ относительно неизвестных $x_1, \ldots, x_n$:

$$\overline{a_0 x_{n+1}} \cdot \ldots \cdot \overline{a_r x_{n+1}} \cdot b_0 \overline{b}_1 \ldots \overline{b}_k \;=\; 0. \qquad (2)$$

Ясно, что булеву функцию $f(x)$ от переменной x можно представить в виде

$$f(x) \;=\; x(f(0) + f(1)) + f(0)\,. \qquad (3)$$

Из (2) и (3) получим

$$x_{n+1}(b_0 \overline{b}_1 \ldots \overline{b}_k + a_0 \overline{a}_1 \ldots \overline{a}_r \cdot b_0 \overline{b}_1 \ldots \overline{b}_k) + b_0 \overline{b}_1 \ldots \overline{b}_k \;=\; 0\,.$$

Используя условие, полученное для (1), получаем

$$\overline{a}_0 \overline{a}_1 \ldots \overline{a}_r \cdot b_0 \overline{b}_1 \ldots \overline{b}_k \;=\; 0\,.$$

□

Решение уравнения $ax+b=0$ в булевом кольце

Теорема 6.34 (о решении уравнения в булевом кольце). *Если уравнение* (1) *имеет решение, то все они описываются соотношением*

$$x = b + \overline{a} \cdot \lambda(x), \tag{4}$$

где $\lambda(x)$ *— произвольная функция от переменной* x.

Доказательство. Покажем сначала, что (4) является корнем (1).

Перепишем (1) в виде $ax = b$.
По $(**)$ это уравнение имеет решение, если $b\overline{a} \equiv 0$. Подставив (4) в (1), получим $ab + b = 0$ или $ab = b$, что, по лемме об основных свойствах элементов булевой алгебры эквивалентно $0 = b\overline{a}$.
Т.о. выполнение необходимого условие существования решений влечёт справедливость того, что (4) есть корень (1).

Докажем теперь, что (4) описывает все корни (1). Пусть существует такой корень β, что

$$\beta \neq b + \overline{a} \cdot \lambda(x) \tag{5}$$

ни при каких значениях функции $\lambda(x)$.
Это означает, что выполняется условие $(\beta + b)a \neq 0$.

В этом случае можно найти такое $\epsilon \not\equiv 0$, что $(\beta + b) \cdot a = \epsilon$, откуда

$$\beta \cdot \overline{a} = b \cdot a + \epsilon\,. \tag{6}$$

Подставляя β в (1) мы должны получить тождество

$$(\beta + b) \cdot a \;=\; \epsilon\,,$$

или, используя (6) — $b{\cdot}a{+}\epsilon{+}b \;\equiv\; 0\,, \qquad b{\cdot}\overline{a}{+}\epsilon \;\equiv\; 0.$

Но, согласно теореме о существовании решения уравнения в булевом кольце, $b\overline{a} \;\equiv\; 0$ и тогда $\epsilon \;\equiv\; 0$, что противоречит (5). Значит, β не является корнем уравнения (1). □

Итерационно применяя формулу для решения уравнения с одним неизвестным, можно получить алгоритм решения уравнений вида $(*)$ со многими неизвестными.

Решение уравнения в булевом кольце: пример. Решим уравнение с тремя неизвестными

$$a_0 + a_1x_1x_2x_3 + a_2x_3 \;=\; 0. \tag{7}$$

Пусть условие $(**)$ выполняется, т. е. $a_0\overline{a}_1\overline{a}_2 \;=\; 0$. Запишем условие разрешимости относительно x_3 —

$$a_0(a_1x_1x_2 + \overline{a}_2) \;=\; 0 \tag{8}$$

и разрешимости полученного условия относительно x_2 —

$$a_0\overline{a}_2(a_0a_1x_1 + 1) \;=\; 0\,.$$

Отсюда находим x_1:

$$x_1 \;=\; a_0\overline{a}_2 + \overline{a_0a_1\overline{a}_2}\cdot\lambda_1, \tag{9}$$

где $\lambda \in \{0, 1\}$.

Из (8) и (9) получаем x_2:

$$x_2 \;=\; a_0\overline{a}_2 + \overline{a_0a_1\overline{a}_2 + a_0a_1a_2\lambda_1}\cdot\lambda_2, \tag{10}$$

а из (9), (10) и (7) — x_3:

$$x_3 \;=\; a_0 + \overline{a_0a_1\overline{a}_2 + \overline{a}_0\lambda_1\lambda_2}\cdot\lambda_3.$$