АМВ. ДЗ на неделю 5.

Прохоров Юрий, 771

Задача 1

Имеются окрашенные прямоугольные таблички трёх типов: черный квадрат размера 2×2, белый квадрат того же размера и серый прямоугольник 2×1 (последний можно поворачивать на $90°$). Нужно подсчитать число способов F_n замостить полосу размера $2\times n$. Найдите явную аналитическую формулу для F_n и вычислите F_{30000} по модулю 31.

Решение:

$$F_1 = 1, \qquad F_2 = 4 \text{ (см. ниже)}$$

Вычислим $F_n,\ n \geq 3$. Верхнюю правую клетку можно покрыть 4 способами. Они изображены на рисунке выше: белым квадратом, черным квадратом, вертикальным прямоугольником и горизонтальным прямоугольником.

1. Если покрыть белым или черным квадратом 2×2, то останется покрыть полосу $2\times(n-2)$. Для этого есть F_{n-2} способов.

2. Если покрыть вертикальным прямоугольником, то оставшуюся полосу размера $2\times(n-1)$ можно покрыть F_{n-1} способами.

3. Если покрыть горизонтальным прямоугольником, то под ним обязательно нужно будет поставить другой такой же прямоугольник. Поэтому останется покрыть полосу размера $2\times(n-2)$.

$$F_n = F_{n-1} + 3F_{n-2}$$

$$\lambda^2 - \lambda - 3 = 0, \qquad \lambda_{1,2} = \frac{1 \pm \sqrt{13}}{2}$$

$$F_n = C_1\lambda_1^n + C_2\lambda_2^n$$

После подстановки начальных условий находим:

$$F_n = \frac{1}{\sqrt{13}}\left(\left(\frac{1+\sqrt{13}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{13}}{2}\right)^{n+1}\right)$$

Нам нужно вычислить $F_n \bmod p,\ n = 30000,\ p = 31$. Рассмотрим F_n как элементы кольца $\mathbb{Z}_{31}[\sqrt{13}]$. Если 13 — квадратичный вычет по модулю 31, то

$$\mathbb{Z}_{31}[\sqrt{13}] \cong \mathbb{Z}_{31}$$

и все выражения $\sqrt{13}$ можно заменить на некоторое число. Кроме того, $p = 31$ — простое, поэтому это кольцо является полем, так как любой элемент обратим.

Проверим, является ли 13 квадратичным вычетом по модулю p. Проверяем критерий:

$$a - \text{ квадратичный вычет} \qquad \Longleftrightarrow \qquad \exists x \ : \ a \equiv x^2 \mod p \qquad \Longleftrightarrow \qquad a^{\frac{p-1}{2}} \equiv 1 \mod p$$

По простому модулю $p = 31$:

$$13^{15} = 169^7 \cdot 13 = 14^7 \cdot 13 = 196^3 \cdot 14 \cdot 13 = 10^3 \cdot 182 = 7 \cdot 10 \cdot (-4) = 10 \cdot 3 = -1$$

Значит, 13 — квадратичный невычет. Тем не менее,

$$\mathbb{Z}_{31}[\sqrt{13}] \cong \mathbb{Z}_{31}[x]/(x^2 - 13) = \mathbb{GF}[31^2],$$

поэтому будет вычислять F_n в этом поле.

$$F_n = \frac{1}{x}\left(\left(\frac{1+x}{2}\right)^{n+1} - \left(\frac{1-x}{2}\right)^{n+1}\right) = x \cdot 13^{-1}\left(\left((1+x)2^{-1}\right)^{n+1} - \left((1-x)2^{-1}\right)^{n+1}\right)$$

Найдем обратные элементы 13^{-1} и 2^{-1} с помощью алгоритма Евклида:

$$13x \equiv 1 \mod 31 \qquad \Longleftrightarrow \qquad 13x + 31y = 1$$

$$\begin{aligned} 31\begin{pmatrix} 0 \\ 1 \end{pmatrix}\ 13\begin{pmatrix} 1 \\ 0 \end{pmatrix} \longrightarrow\ & 13\begin{pmatrix} 1 \\ 0 \end{pmatrix}\ 5\begin{pmatrix} -2 \\ 1 \end{pmatrix} \longrightarrow\ 5\begin{pmatrix} -2 \\ 1 \end{pmatrix}\ 3\begin{pmatrix} 5 \\ -2 \end{pmatrix} \longrightarrow \\ & \longrightarrow\ 3\begin{pmatrix} 5 \\ -2 \end{pmatrix}\ 2\begin{pmatrix} -7 \\ 3 \end{pmatrix} \longrightarrow\ 2\begin{pmatrix} -7 \\ 3 \end{pmatrix}\ 1\begin{pmatrix} 12 \\ -5 \end{pmatrix} \end{aligned}$$

$$x = 12, \qquad y = -5$$

Итак, $13^{-1} = 12,\ 2^{-1} = 16$. Второе число найдено подбором.

$$F_n = 12x\Big(16^{n+1}(1+x)^{n+1} - 16^{n+1}(1-x)^{n+1}\Big) = 12 \cdot 16^{n+1}x\Big((1+x)^{n+1} - (1-x)^{n+1}\Big)$$

$\mathbb{Z}_{31}[x]/(x^2 - 13)$ является полем из $p^q = 31^2$ элементов, где q — степень неприводимого многочлена. Множество элементов поля без нуля образует мультипликативную группы из $(p^2 - 1)$ элементов. По теореме Лагранжа, порядок любого элемента делит порядок группы, то есть

$$\forall f \neq 0 \ : \ f^{p^2-1} = f^{960} = 1$$

В связи с этим,

$$16^{n+1} = 16^{30001} = 16^{30001 \bmod 31} = 16^{241} = 2^{964} = 2^4 = 16$$
$$(1+x)^{n+1} = (1+x)^{241}, \qquad (1-x)^{n+1} = (1-x)^{241}$$

Вычислим $(1+x)^{240}$:

- $(1+x)^2 = 1 + 2x + x^2 = 2x + 14$
- $(1+x)^4 = 4 \cdot 13 + 56x + 196 = 186 - 6x = -6x$
- $(1+x)^8 = 36 \cdot 13 = 5 \cdot 13 = 3$
- $(1+x)^{16} = 9$
- $(1+x)^{32} = 19$
- $(1+x)^{64} = 20$
- $(1+x)^{128} = -3$

$$(1+x)^{240} = (1+x)^{128}(1+x)^{64}(1+x)^{32}(1+x)^{16} = (-3) \cdot 20 \cdot 19 \cdot 9 = 4 \cdot 19 \cdot 20 = 1$$

Аналогично,

$$(1-x)^{240} = 1$$

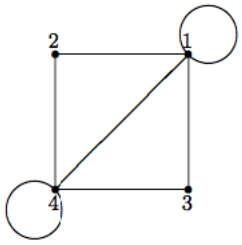
Тогда

$$F_n = 12 \cdot 16x(1 + x - 1 + x) = 12x^2 \cdot 32 = 12 \cdot 13 = 1$$

Задача 2

Выполните задачи 1, Д-1 из приложенного файла (все по 1 баллу).

Решение:
Для графа



составим матрицу инциденций:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

(i) Пусть $a_{ij}^{(k)}$ — элементы матрицы A^k.

Лемма. *a_{ij}^n — число путей длины n из вершины i в вершину j.*

Доказательство:
Докажем по индукции. База: $n = 1$. Утверждение верно по определению матрицы инцидентности.

Пусть верно при $n = k - 1$. Докажем, что верно при $n = k$. Путь длины n $i \to j$ можно разбить на два путя: $i \to t$ и $t \to j$ для некоторого t длин $n - 1$ и 1 соответственно. Тогда число путей $i \to j$ таких, что предпоследняя вершина есть t равно $a_{it}^{(n-1)} \cdot a_{tj}^{(1)}$. Суммируя по всем t, имеем:

$$a_{ij}^{(n)} = \sum_{t=1}^{n} a_{it}^{(n-1)} a_{tj}^{(1)}$$

Такие числа как раз получаются при перемножении матриц A^{k-1} и A. □

Из этой леммы следует, что если g_n — число всех путей длины n из вершины 1, то g_n есть сумма элементов первой строки матрицы A^n. Можно g_n представить в виде:

$$g_n = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix} A^n \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

В частности

$$g_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 4 + 2 + 2 + 4 = 12$$

(ii) Пусть h_n — число всех путей длины n из вершины 2. Из симметрии графа видно, что число всех путей длины n из вершин 3 и 4 равно h_n и g_n соответственно. Тогда можно составить систему при $n \geq 3$:

$$\begin{cases} g_n = 2g_{n-1} + 2h_{n-1} \\ h_n = 2g_{n-1} \end{cases}$$

Тогда получаем рекурренту

$$g_n = 2g_{n-1} + 4g_{n-2}$$
$$\lambda^2 - 2\lambda - 4 = 0, \qquad \lambda_{1,2} = 1 \pm \sqrt{5}$$
$$g_n = C_1\lambda_1^n + C_2\lambda_2^n$$

После подстановки начальных условий, имеем:

$$g_n = \frac{1}{4\sqrt{5}}\left((1+\sqrt{5})^{n+2} - (1-\sqrt{5})^{n+2}\right)$$

(*iii*) Оценим прямое вычисление g_n по рекуррентной формуле. Число рекуррентных вызовов оценивается формулой:

$$g_n = 2g_{n-1} + 4g_{n-2} + 1$$
$$g_n = C_1\lambda_1^n + C_2\lambda_2^n - \frac{1}{5}$$

При больших n:

$$g_n \approx 1.271 \cdot (1+\sqrt{5})^n - 0.071 \cdot (1-\sqrt{5})^n \approx 1.271 \cdot (1+\sqrt{5})^n$$

При $n = 20000$ число рекурсивных вызовов:

$$g_n \approx 2.86 \cdot 10^{10200}$$

(*iv*) Всего возможных остатков от деления на произвольное m ровно m. Всего различных пар остатков m^2. Из формулы

$$g_n = 2g_{n-1} + 4g_{n-2}$$

видно, что остаток от деления g_n на произвольное число m однозначно определяется парой предыдущих остатков. Число различных пар не превосходит m^2, поэтому среди первых $m^2 + 1$ пар, по принципу Дирихле, найдется одинаковая пара. Значит, после них все будет повторяться. то есть последовательность периодична.

Период, как ясно из рассуждений, не превосходит m^2.

Чтобы произвести таким образом вычисление, нужно в худшем случае вычислить все первые $m^2 + 1$ значений g_n и найти среди них повторение. Затем нужно найти остаток n от деления на получившийся период τ. Деление производится за $O(\log^2 n)$. Итоговая сложность:

$$O(m^2 + \log^2 n).$$

При $n = 20000,\ m = 29$ потребуется порядка m^2 операция для вычисления.

(*v*) Заметим, что число $a = 5$ является квадратичным вычетом по модулю $p = 29$. Для этого вычислим символ Лежандра:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv 5^{14} \equiv (-4)^7 \equiv (-4)\cdot 6^2 \equiv 1 \mod 29$$

Он равен 1, значит, 5 — действительно квадратичный вычет по модулю 29. Несложно подобрать

$$5^2 \equiv 11 \mod 29$$

В силу квадратичности вычета, кольцо

$$\mathbb{Z}_{29}[\sqrt{5}] \cong \mathbb{Z}_{29}$$

Поэтому корень можно заменять на элемент этого поля. Поле является мультипликативной группой по умножению, то есть каждый ненулевой элемент обратим, значит, деление можно заменять умножением на обратный. Кроме того, порядок любого элемента кратен порядку группы

$$\forall x \neq 0 \ : \ x^{p-1} = x^{28} = 1$$

Итак, имеем

$$g_n = \frac{1}{4\cdot 11}\Big(12^{n+2} - (-10)^{n+2}\Big) = \frac{1}{15}(12^{20002} - (-10)^{20002}) = 2(12^{10} - 10^{10}) = 2\cdot 22 = 15$$

Для оценки трудоемкости будем считать, что нам уже дан сам квадратный корень квадратичного вычета, поэтому остается только провести вычисления. Надо за $O(\log^2 n)$ поделить n на $p = 29$ отстатком. Затем возвести число в степень не больше p за $O(\log p)$. Поэтому итоговая трудоемкость

$$O(\log^2 n + \log p)$$

(*vi*) Пусть p — простое число, а $(P^2 + 4Q)$ не является квадратичным вычетом по модулю p. Тогда

$$\mathbb{Z}_p\big[\sqrt{P^2+4Q}\big] \cong \mathbb{Z}_p[x]/(x^2 - P^2 - 4Q) \cong \mathbb{GF}[p^2]$$

$$\mathbb{Z}_{23}[\sqrt{5}] \cong \mathbb{Z}_{23}[x]/(x^2 - 5)$$

Далее решаем аналогично задаче 1.

$$g_n = \frac{1}{4\sqrt{5}}\Big((1+\sqrt{5})^{n+2} - (1-\sqrt{5})^{n+2}\Big) = \frac{x}{20}\Big((1+x)^{n+2} - (1-x)^{n+2}\Big) = -8x\Big((1+x)^{n+2} - (1-x)^{n+2}\Big)$$

$$(1+x)^{p^2-1} = (1+x)^{528} = 1, \quad (1-x)^{528} = 1 \qquad \Longrightarrow$$

$$g_{10000} = -8x\Big((1+x)^{10002 \bmod 528} - (1-x)^{10002 \bmod 528}\Big) = -8x\Big((1+x)^{-30} - (1-x)^{-30}\Big)$$

Найдем обратные к $1+x$ и $1-x$ в поле. Заметим, что

$$(1+x)(1-x) = 1 - x^2 = -4 \qquad \Longrightarrow \qquad (-4)^{-1}(1+x)(1-x) = 1$$

Тогда видно, что

$$(1+x)^{-1} = -6(1-x) = 6(x-1), \qquad (1-x)^{-1} = -6(x+1)$$

$$g_{10000} = -8x\cdot 6^{30}\Big((x-1)^{30} - (x+1)^{30}\Big) = -8x\cdot 6^{30}\Big((1-x)^{30} - (1+x)^{30}\Big)$$

$$6^{30} = 36^{15} = 13^{15} = 169^7\cdot 13 = 8^7\cdot 13 = 64^3\cdot 104 = (-5)^3\cdot 12 = -60\cdot 2 = 18 = -5$$

- $(1+x)^2 = 1 + 2x + x^2 = 6 + 2x$
- $(1+x)^4 = 36 + 4x^2 + 24x = 13 - 3 + x = 10 + x$
- $(1+x)^8 = 100 + 5 + 20x = 13 - 3x$
- $(1+x)^{16} = 169 + 45 - 2\cdot 39x = 8 - 1 - 6x = 7 - 9x$
- $(1+x)^{32} = 49 + 81\cdot 5 - 2\cdot 63x = 3 - 55 + 12x = 12x - 6$

Аналогично,

$$(1-x)^{32} = -12x - 6$$

$$g_{10000} = 40x\Big((1-x)^{-2}(1-x)^{32} - (1+x)^{-2}(1+x)^{32}\Big) = 40x\Big(36(1+x)^2\cdot(-6)(1+2x) - 36(x-1)^2\cdot 6(2x-1)\Big) =$$
$$= -6x\cdot 36(-6)\Big((6+2x)(1+2x) + (6-2x)(2x-1)\Big) = 169x\big(6 + 4x^2 + 14x - 6 - 4x^2 + 14x\big) = 8x\cdot 5x = 16$$

Оценим трудоемкость, считая, что известна аналитическая формула для g_n. Поиск обратных элементов требует алгоритма Евклида и $O(\log p)$ операций. Деление с остатком требует $O(\log^2 n)$ времени. Вычисление степеней многочленов требует $O(\log p^2) = O(\log p)$ операций. Итого

$$O(\log p + \log^2 n).$$

(*vii*) Отметим справедливость следующей формулы

$$\begin{pmatrix} g_n \\ g_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix}^{n-1} \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}$$

Действительно, при $n = 1$ она верна, а при предположении, что формула верна при $n = k - 1$:

$$\begin{pmatrix} g_k \\ g_{k+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix}^{k-2} \begin{pmatrix} g_1 \\ g_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} g_{k-1} \\ g_k \end{pmatrix} = \begin{pmatrix} g_k \\ 2g_k + 4g_{k-1} \end{pmatrix}$$

формула также верна и для n. Тогда по индукции она верна $\forall n$. Обозначим $P = 2,\ Q = 4$:

$$g_n = Pg_{n-1} + Qg_{n-2}, \qquad P > 0,\ Q > 0$$

$$\begin{pmatrix} g_n \\ g_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ Q & P \end{pmatrix}^{n-1} \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}$$

Найдем собственные значения матрицы:

$$|A - \lambda E| = \begin{vmatrix} -\lambda & 1 \\ Q & P - \lambda \end{vmatrix} = \lambda^2 - P\lambda - Q = 0, \qquad D = P^2 + 4Q > 0$$

Заметим, что это как раз характеристическое уравнение рекуррентного соотношения. Пусть $\lambda_{1,2} \in \mathbb{R},\ (\lambda_1 \neq \lambda_2)$ — его корни. Пусть $\mathbf{u_1}, \mathbf{u_2}$ — собственные векторы, соответствующие этим собственным значениям. Корни различны и действительны, следовательно, по теореме Жордана, существует базис из собственных векторов. U — матрицы перехода — состоит из столбцов $\mathbf{u_1}, \mathbf{u_2}$.

$$A = U\Lambda U_{-1}, \qquad \Lambda = \mathrm{diag}(\lambda_1, \lambda_2)$$

$$A^{n-1} = U\Lambda^{n-1}U^{-1} = U\mathrm{diag}(\lambda_1^{n-1}, \lambda_2^{n-1})U^{-1}$$

$$\begin{pmatrix} g_n \\ g_{n+1} \end{pmatrix} = U\mathrm{diag}(\lambda_1^{n-1}, \lambda_2^{n-1})U^{-1} \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}$$

После всех перемножений как раз получается выражение вида

$$g_n = C_1\lambda_1^n + C_2\lambda_2^n$$

Так мы обосновали корректность метода решений рекуррентных соотношений через характеристическое уравнение.

Теперь продолжим эти рассуждения, чтобы получить «аналог» малой теоремы Ферма. Получим достаточное условие, что $A^k = E$ при вычислениях по простому модулю p в поле $\mathbb{Z}_p[x]/(x^2 - P^2 - 4Q)$. Элементам матриц U, U^{-1} соответствуют некоторые элементы этого поля.

Пусть в поле $\lambda_1^k = 1,\ \lambda_2^k = 1$. В качестве такого k можно взять $(p^2 - 1)$ — порядок мультипликативной группы поля. Тогда

$$A^k = U\mathrm{diag}(\lambda_1^k, \lambda_2^k)U^{-1} = UEU^{-1} = E$$

Итого имеем следующее соотношение:

$$\begin{pmatrix} 0 & 1 \\ Q & P \end{pmatrix}^{p^2-1} = 1 \qquad \text{в поле } \mathbb{Z}_p[x]/(x^2 - P^2 - 4Q)$$

Задача 3

Пусть язык $L \in \mathcal{NP}$. Покажите, что он полиномиально сводится (по Карпу) к языку $STOP$ описаний пар (M, ω) машин Тьюринга и входов таких, что M останавливается на входе ω.

Решение:
Известно, что $SAT \in \mathcal{NP}$-*complete*, поэтому $L \leq_p SAT$. Покажем, как полиномиально свести SAT к проблеме останова $STOP$.

Построим машину Тюринга M_0, которая будет принимать на вход некоторую КНФ ϕ и будет проверять ее выполнимость (за экспоненциальное время, очевидно). Если КНФ выполнима, то пусть M_0 останавливается с ответом «1», а если невыполнима — то пусть M_0 не дает никакого ответа и зацикливается.

$$M_0(\phi) = \begin{cases} 1, & \phi \in SAT \\ \perp, & \phi \notin SAT \end{cases}$$

Таким образом, сводимость f будет по формуле ϕ выдавать пару (M_0, ϕ). Ясно, что это делается за полиномиальное время, так как описание МТ конечно. Из определения МТ M_0 видно, что

$$\phi \in SAT \qquad \Longleftrightarrow \qquad f(\phi) = (M_0, \phi) \in STOP$$

Итак,

$$\left.\begin{array}{l} L \leq_p SAT \\ SAT \leq_p STOP \end{array}\right\} \qquad \Longrightarrow \qquad L \leq_p STOP$$

Задача 4

Пусть стало известно, что $\mathcal{NP}C \cap co\text{-}\mathcal{NP} \neq \varnothing$. Верно ли, что отсюда следует, что $\mathcal{NP} = co\text{-}\mathcal{NP}$.

Решение:
Да, верно. Обозначим за L такой язык, что

$$L \in \mathcal{NP}\text{-}complete \ \cap \ co\text{-}\mathcal{NP}$$

Также будем пользоваться следующим утверждением (которое я доказывал в прошлый раз):

$$L \in NP\text{-}complete \qquad \Longleftrightarrow \qquad \overline{L} \in co\text{-}\mathcal{NP}\text{-}complete$$

(a) Пусть $M \in \mathcal{NP}$. Покажем, что $M \in co\text{-}\mathcal{NP}$.

$$L \in \mathcal{NP}c \qquad \Longrightarrow \qquad M \leq_p L, \qquad \Big[x \in M \iff f(x) \in L\Big]$$

$$L \in co\text{-}\mathcal{NP} \qquad \Longrightarrow \qquad \Big[y \notin L \iff \exists s \ : \ R(y,s) = 1\Big]$$

Из этих двух утверждений следует, что

$$x \notin M \iff f(x) \notin L \iff \exists s : R(f(x), s) = 1$$

А это есть определение того, что $\overline{M} \in \mathcal{NP}$, то есть $M \in co\text{-}\mathcal{NP}$. В качестве сертификата непринадлежности $x \notin M$ берем сертификат непринадлежности $f(x) \notin L$ и проверяем его верификатором R языка L.

(b) Пусть $M \in co\text{-}\mathcal{NP}$. Покажем, что $M \in \mathcal{NP}$.

Обозначим язык $N = \overline{M} \in \mathcal{NP}$. Требуется показать, что $\overline{N} \in \mathcal{NP}$, то есть $N \in co\text{-}\mathcal{NP}$. А это как раз следует из пункта (a).

Задача 5

Рассматривается язык L выполнимых формул от n переменных вида $C_1 \wedge C_2 \wedge \ldots \wedge C_m$, где каждый C_k имеет один из трех видов: $(x_i \equiv x_j)$, $(\overline{x_i} \equiv x_j)$, $(x_i \equiv \overline{x_j})$, $(\overline{x_i} \equiv \overline{x_j})$.

(i) Верно ли, что этот язык $\mathcal{NP}$–полон?

(ii) Верно ли, что если каждый C_k будет иметь вид $(x_{i_1}^{\alpha_{i_1}} \equiv x_{i_2}^{\alpha_{i_2}} \equiv \ldots \equiv x_{i_l}^{\alpha_{i_l}})$, то язык будет $\mathcal{NP}$–полон? (Под $x_i^{\alpha_i}$ понимается либо x_i, либо $\overline{x_i}$)

Решение:

(i) Если $\mathcal{P} = \mathcal{NP}$, то верно. Если $\mathcal{P} \neq \mathcal{NP}$, то неверно.

Нам известно, что язык двудольных («двараскрашиваемых») графов 2-$COLOUR \in \mathcal{P}$. Построим полиномиальную сводимость $L \leq_p$ 2-$COLOUR$. Пусть $x_1, \ldots, x_n$ — все переменные формулы ϕ данного вида, а формула состоит из m эквиваленций.

Преобразование f формулы ϕ в граф G:

1. Проверим, выполнима ли каждая эквиваленция по отдельности. То есть если какое-то $C_k = (a_k \equiv \neg a_k)$, то выдаем какой-то граф, в котором заведомо нет 2-раскраски, например, K_5.
2. Создадим $2n$ вершин. Вершины пометим всеми возможными литералами.
3. Соединим ребром все вершины x_i и $\neg x_i$.
4. Для каждого $C_k = (a_k \equiv b_k)$:
добавим ребра $[a_k, \neg b_k]$ и $[\neg a_k, b_k]$.

Ясно, что все шаги занимают полиномиальное время. Покажем, что они корректны.

Пусть ϕ выполнима. Тогда в ней нет противоречивых эквиваленций и шаг 1 будет пройден. Пусть α — выполняющий набор, пусть $\mathbf{a}$ — соответствующий набор литералов, которые обращаются в 1 на наборе α. Покрасим в графе литералы из $\mathbf{a}$ в один цвет, а все остальные в другой. Покажем, что такая раскраска корректна.

Допустим, она некорректна. Тогда между какими-то литералами из набора $\mathbf{a}$ есть ребро либо между литералами из дополнения этого набора $\overline{\mathbf{a}}$ есть ребро. Для определенности, будем считать, что

$$\exists a_i, a_j \in \mathbf{a} \ : \ [a_i, a_j] \in G, \qquad a_i, a_j \text{ отвечают различным переменным}$$

Ребро между литералами для разных переменных могло появиться только на шаге 4, поэтому в формуле ϕ была одна из эквиваленций $(a_i \equiv \neg a_j)$ или $(\neg a_i \equiv a_j)$. То тогда набор литералов $\mathbf{a}$ не может быть выполняющим, так как такая эквиваленция обратится на нем в 0 — противоречие.

Пусть в G есть раскраска. Тогда $G \neq K_5$ и формула прошла шаг 1, значит, в ней нет противоречивых эквиваленций. Пусть $\mathbf{a}$ — литералы, окрашенные в один цвет, $\overline{\mathbf{a}}$ — в другой цвет. Так как в G есть ребра $[x_i, \neg x_i]$, то в $\mathbf{a}$ и $\overline{\mathbf{a}}$ все литералы отвечают различным переменным. Покажем, что набор литералов $\mathbf{a}$ является выполняющим.

Допустим, не является. Тогда существует $C_k = (a_k \equiv b_k)$ такое, что $a_k \in \mathbf{a}$, $b_k \notin \mathbf{a}$, то есть литералы $a_k = 1$, $b_k = 0$ на этом наборе. Тогда $\neg b_k \in \mathbf{a}$. Но шаге 4 в G появится ребро $[a_k, \neg b_k]$ между двумя литералами из $\mathbf{a}$, окрашенными в один цвет. Противоречие.

Таким образом, мы показали, что $L \in \mathcal{P}$.

(ii) Задача также лежит в $\mathcal{P}$.

Здесь под знаком + будем понимать операцию XOR или бинарного сложения. Используем тождества:

$$(a_1 \equiv a_2) = a_1 + a_2 + 1$$

$$(a_1 \equiv a_2 \equiv a_3) = ((a_1 \equiv a_2) \equiv a_3) = a_1 + a_2 + a_3$$

$$\ldots$$

$$(a_1 \equiv a_2 \equiv \ldots \equiv a_n) = a_1 + a_2 + \ldots + a_n + (n - 1 \bmod 2)$$

На основе этого можно сформулировать утверждение

$$(a_1 \equiv a_2 \equiv \ldots \equiv a_n) = 1 \qquad \Longleftrightarrow \qquad \text{четное число литералов принимает значение 0}$$

Алгоритм проверки выполнимости формулы ϕ:

1. Вычислим значения каждого блока формулы C_k при нулевом наборе. Пусть $\mathbf{b}$ — вектор этих значений (имеем размерность m).

2. Для каждой переменной x_j, $j = 1, \ldots, n$ вычислим m-мерный вектор $\mathbf{a_j}$. В k-ой позиции этого вектора:

$$\mathbf{a_j^k} = \begin{cases} 1, & \text{переменная } x_j \text{ входит в блок } C_k \\ 0, & \text{переменная } x_j \text{ не входит в блок } C_k \end{cases}$$

Этот вектор означает следующее: если мы положим все переменные нулями, а $x_j = 1$, то, вследствие утверждения выше, значения всех блоков формулы ϕ при таком наборе будут равны

$$\phi = \mathbf{b} + \mathbf{a_j}$$

Таким образом, наша задача сводится к тому, что надо среди векторов $\mathbf{a_1}, \ldots, \mathbf{a_n}$ найти такие, который можно прибавить к $\mathbf{b}$ и получить единичный вектор. Другими словами, надо решить систему

$$c_1\mathbf{a_1} + c_2\mathbf{a_2} + \ldots + c_n\mathbf{a_n} = \mathbf{b} + \mathbf{1} = \neg\mathbf{b}, \qquad c_j \in \{0, 1\}$$

3. Методом Гаусса проверяем разрешимость системы

$$A\mathbf{c} = \neg\mathbf{b}, \qquad A = \left(\mathbf{a_j}\right)_{j=1}^{n} \quad \text{(столбцы)}$$

над полем $\{0, 1\}$. Если система разрешима, то формула ϕ выполнима (причем выполняющий набор — решение системы). Иначе формула ϕ невыполнима.

Полиномиальность алгоритма следует из того, что метод Гаусса является полиномиальным при вычислениях по модулю 2. Корректность алгоритма была доказана по ходу его описания.

Задача 6

Подбрасываем «честную» монету 10 раз. Подсчитайте вероятности следующих событий:

(i) (1/6 балла) число выпавших «орлов» равно числу «решек»;

(ii) (1/6 балла) выпало больше «орлов» чем «решек»;

(iii) (1/6 балла) при $i = 1, \ldots, 5$ одинаковы результаты i-го и $11 - i$-го бросаний;

(iv) (1/2 балла) «орел» выпал не менее четырех раз подряд.

Решение:
(i) Будем рассматривать результат бросания монеток как случайную строку $x \in \{0, 1\}^{10}$. 0 — «орел», 1 — «решка». Всего таких строк 2^{10}. Строк, в которых ровно 5 единиц C_{10}^5.

$$P\{5 \text{ «орлов»}\} = p_1 = \frac{C_{10}^5}{2^{10}} \approx 0.246$$

(ii) В силу того, что монета честная:

$$P\{\text{«орлов» больше «решек»}\} = P\{\text{«решек» больше «орлов»}\}$$

Тогда из равенства

$$P\{\text{«орлов» больше «решек»}\} + P\{\text{«решек» больше «орлов»}\} + P\{5 \text{ «орлов»}\} = 1$$

следует

$$P\{\text{«орлов» больше «решек»}\} = p_2 = \frac{1 - p_1}{2} \approx 0.377$$

(iii) Требуется найти число палиндромов в языке $\{0, 1\}^{10}$. Между палиндромами в это языке и всеми словами в языке $\{0, 1\}^5$ есть взаимно однозначное соответствие, поэтому вероятность получить палиндром:

$$p_3 = \frac{|\{0, 1\}^5|}{|\{0, 1\}^{10}|} = \frac{2^5}{2^{10}} = \frac{1}{32} \approx 0.031$$

(iv) Пусть T_n — число слов длины n, в которых встречается «0» 4 раза подряд.

$$T_1 = T_2 = T_3 = 0, \qquad T_4 = 1$$

Пусть $n \geq 5$. Рассмотрим 5 исчерпывающих случаев:

1. На последней позиции стоит 1. Тогда число нужных слов есть T_{n-1}.
2. На последних двух позициях стоит 10. Тогда число нужных слов есть T_{n-2}.
3. На последних трех позициях стоит 100. Тогда число нужных слов есть T_{n-3}.
4. На последних четырех позициях стоит 1000. Тогда число нужных слов есть T_{n-4}.
5. На последних четырех позициях стоит 0000. Тогда число нужных слов есть 2^{n-4}.

$$T_n = T_{n-1} + T_{n-2} + T_{n-3} + T_{n-4} + 2^{n-4}$$

Вычисляем:

$$T_5 = 3,\ T_6 = 8,\ T_7 = 20,\ T_8 = 48,\ T_9 = 111,\ T_{10} = 251$$

Искомая вероятность:

$$p_4 = \frac{T_{10}}{2^{10}} = \frac{251}{1024} \approx 0.245$$

Задача 7

(*i*) Вычислите условную вероятность, что при бросаний двух игральных костей на первой выпало шесть, если сумма равна семи.

(*ii*) При двух бросках игральной кости выпало X_1 и X_2, соответственно. Вычислите $\mathbb{E}\{\max\{X_1, X_2\}\} + \mathbb{E}\{\min\{X_1, X_2\}\}$.

(*iii*) Независимы ли события: «при броске кубика выпало четное число» и «при броске кубика выпало число, кратное трём»?

(*iv*) Найти вероятность, что случайно выбранный граф на n вершинах является простым циклом; найти её предел при $n \to \infty$.

Решение:
Пусть x_1, x_2 — результаты двух бросков игральных костей.

(*i*) По определению условной вероятности:

$$P\{x_1 = 6 \mid x_1 + x_2 = 7\} = \frac{P\{(x_1 = 6) \wedge (x_1 + x_2 = 7)\}}{P\{x_1 + x_2 = 7\}} = \frac{P\{(x_1 = 6) \wedge (x_2 = 1)\}}{P\{x_1 + x_2 = 7\}} =$$
$$= \frac{P\{x_1 = 6\} \cdot P\{x_2 = 1\}}{P\{x_1 + x_2 = 7\}} = \frac{\frac{1}{6} \cdot \frac{1}{6}}{\frac{6}{36}} = \frac{1}{6}$$

(*ii*) По свойству линейности (применяем его два раза):

$$\mathbb{E}[\max(x_1, x_2)] + \mathbb{E}[\min(x_1, x_2)] = \mathbb{E}\big[\max(x_1, x_2) + \min(x_1, x_2)\big] = \mathbb{E}[x_1 + x_2] = \mathbb{E}[x_1] + \mathbb{E}[x_2] = 2\mathbb{E}[x_1] = 7$$

(*iii*) Проверим определение независимых событий:

$$P\big\{(3 \mid x) \wedge (2 \mid x)\big\} = P\{3 \mid x\} \cdot P\{2 \mid x\}$$

$$\frac{1}{6} = \frac{1}{2} \cdot \frac{1}{3} \quad - \quad \text{верно} \qquad \Longrightarrow \qquad \text{события независимы}$$

(*iv*) Будем считать, что граф является циклом тогда и только тогда, когда в нем есть цикл, в котором задействованы все ребра, то есть эйлеров цикл. Также заметим, что простой эйлеров цикл является гамильтоновым циклом. Итак, граф является простым циклом тогда и только тогда, когда в графе есть гамильтонов эйлеров цикл.

Посчитаем число таких графов на n вершинах. Гамильтонов цикл имеет ровно n ребер. Значит, любой такой граф содержит ровно n ребер. По критерию Эйлера, эйлеров цикл есть тогда и только тогда, когда степень каждой вершины четна и граф связен. Цикл не может проходить через одну вершину дважды, так как он гамильтонов, поэтому степень каждой вершины должна быть равна 2. Итак, если G — простой

цикл, то степень каждой вершины равна 2 и граф связен.

Покажем, что обратное тоже верно. Аналогично доказательству теоремы Эйлера, берем любую вершину и идем в любую сторону, пока куда-то не придем (это возможно, так как степень каждой вершины равна 2). Если вернулись обратно через $< n$ ребер, то, значит, граф несвязен — противоречие. Тогда в G есть цикл из n ребер, не имеющий самопересечений.

Посчитаем число таких графов. Возьмем вершину с номером 1. Ее можно соединить со следующей $n-1$ способами. Из следующей можно провести еще одно ребро $n-2$ способами, и так далее. В итоге из n-ой вершины можно замкнуть цикл одним способом. Всего способов так построить граф:

$$(n-1)(n-2)\dots 2\cdot 1 = (n-1)!$$

Но так мы посчитали ориентированные циклы. Число неориентированных циклов в 2 раза меньше:

$$A_n = \frac{(n-1)!}{2}$$

Всего графов на n вершинах $2^{C_n^2}$, так как каждое из C_n^2 может как быть, так и не быть. Тогда искомая вероятность:

$$p_n = \frac{(n-1)!}{2^{1+C_n^2}}$$

При $n \to \infty$:

$$\log p_n = \Theta(n\log n - n^2) \longrightarrow -\infty \qquad \Longrightarrow \qquad p_n \longrightarrow 0$$

Задача 8

Две урны содержат одинаковое количество шаров. Шары окрашены в белый и черный цвета. Из каждой урны вынимают по n шаров с возвращением, где $n \geq 3$. Найдите n и «состав» каждой урны, если вероятность того, что все шары, взятые из первой урны, белые, равна вероятности того, что все шары, взятые из второй урны, либо белые, либо черные.

Решение:
Пусть в урнах было по N шаров, в первой было k белых шаров, во второй было m белых шаров. Приравняем вероятности из условия задачи:

$$\left(\frac{k}{N}\right)^n = \left(\frac{m}{N}\right)^n + \left(\frac{N-m}{N}\right)^n$$

$$k^n = m^n + (N-m)^n, \qquad n > 2$$

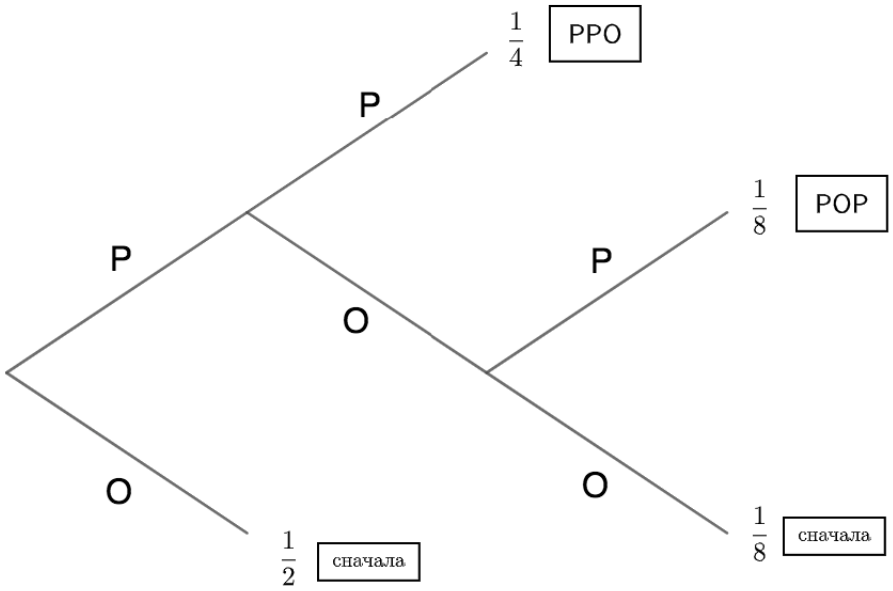
Во Великой теореме Ферма, такое уравнение не имеет решений в натуральных числах. Поэтому одно из слагаемых равно 0 ($k \neq 0$, т.к. правая часть положительна). Значит, либо $m = 0$, либо $m = N$. В любом случае $k = N$.

Итак, n — любое, в первой урне все шары белые, а во второй урне все шары одного цвета (любого).

Задача 9

Симметричную монетку бросают неограниченное число раз. Какая из последовательностей встретится раньше с большей вероятностью: РОР или РРО?

Решение:



Пусть x — вероятность того, что раньше будет PPO. Тогда $(1-x)$ — вероятность того, что раньше будет POP. Построим дерево бросков (см. выше). Если мы приходим в лист, где написано «сначала», то мы перемещаемся в корень дерева, и снова вероятности победы x и $(1-x)$ соответственно.

Найдем вероятность победы PPO:

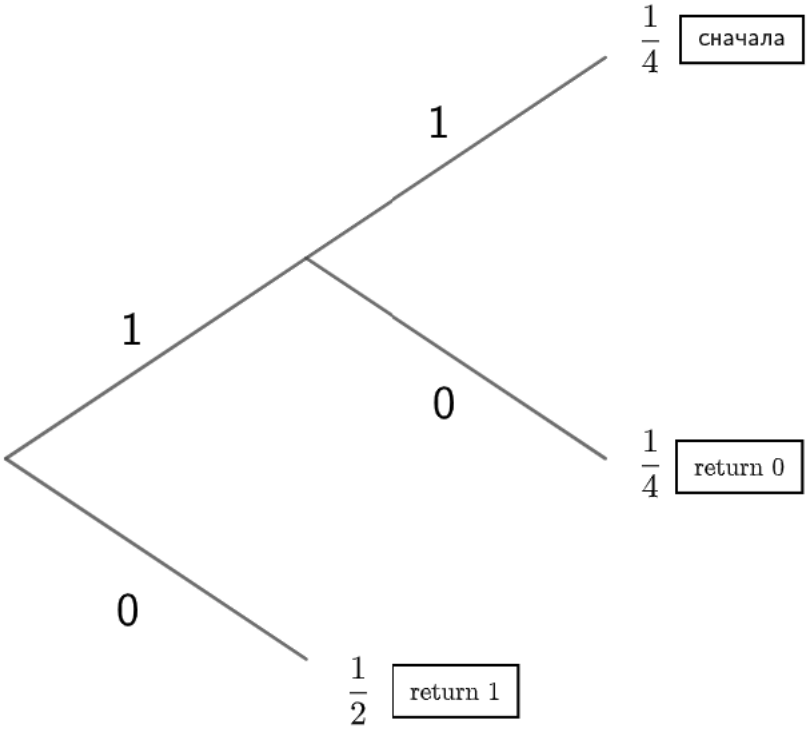
$$x = \frac{1}{4} + \frac{1}{8}x + \frac{1}{2}x \qquad \Longrightarrow \qquad x = \frac{2}{3}$$

Значит, вероятность того, что раньше встретится PPO, в два раза больше вероятности, что раньше встретится POP.

Задача 10

(i) Имеется генератор случайных битов, выдающий 0 и 1 с вероятностью 1/2. Предложите алгоритм, использующий этот генератор и выдающий 0 с вероятностью 1/3 и 1 с вероятностью 2/3. Оцените его время работы в лучшем и в худшем случае.
(ii) Обратно: из генератора $(1/3; 2/3)$ получите $(1/2)$.

Решение:
(i) Построим дерево работы алгоритма, которое можно воспринимать как что-то, подобное ДКА.



Найдем вероятность того, что вернется 0, аналогично предыдущей задаче:

$$x = \frac{1}{4} + \frac{1}{4}x \qquad \Longrightarrow \qquad x = \frac{1}{3}$$

В лучшем случае, он будет работать 1 такт, в худшем случае он будет работать бесконечно.

Покажем, что не существует конечного генератора. Допустим, существует конечный алгоритм, работающий $\leq N$ тактов. Дополним его бинарное дерево до полного дерева с N ярусами (возможно последние запросы случайных битов будут бесполезными). Тогда число k листьев, из которых алгоритм вернет 0 должно составлять треть всех исходов, так как попадание в каждый лист равновероятно:

$$\frac{k}{2^N} = \frac{1}{3} \qquad \Longleftrightarrow \qquad 2^N = 3k$$

Это противоречие.

Также для интереса посчитаем среднее время работы (мат. ожидание) A алгоритма. Пусть p_n — вероятность проработать n тактов.

$$p_0 = 0, \qquad p_1 = \frac{1}{2}, \qquad p_2 = \frac{1}{4}$$

При $n \geq 3$ нужно обязательно на после первых двух запросов вернуться в корень, поэтому

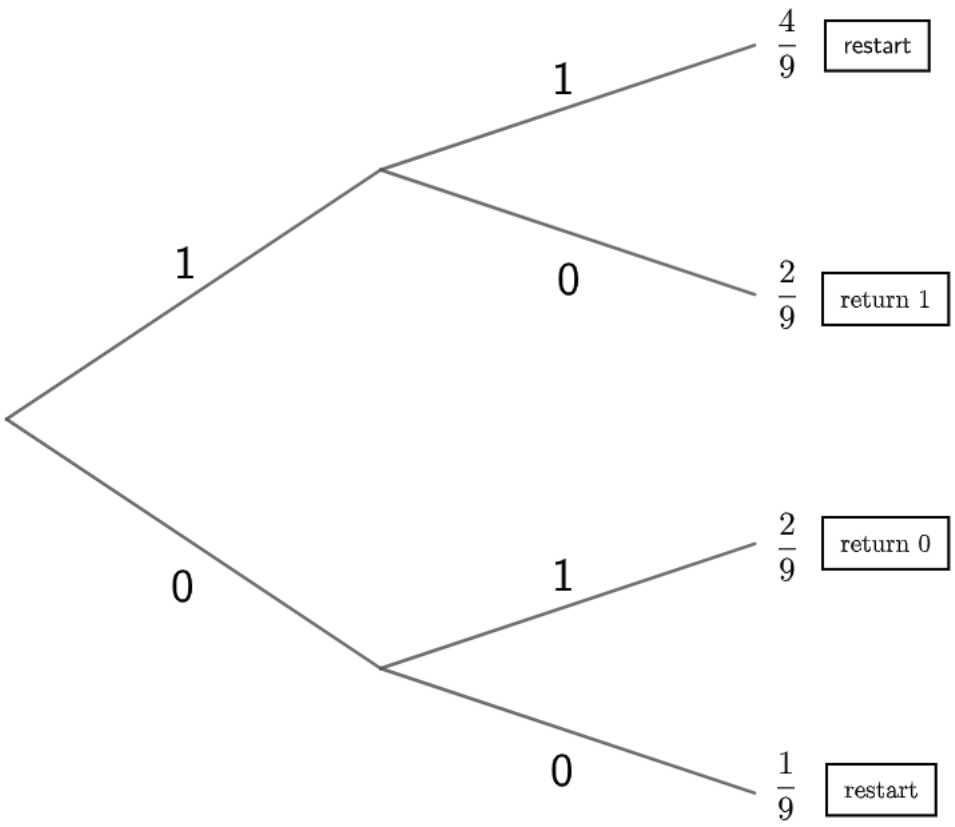
$$p_n = \frac{1}{4}p_{n-2}$$

$$A = \sum_{n=1}^{\infty} np_n = 1 + \sum_{n=3}^{\infty} \frac{n}{4}p_{n-2} = 1 + \sum_{n=1}^{\infty} \frac{(n+2)p_n}{4} = 1 + \frac{1}{4}A + \frac{1}{2}\sum_{n=1}^{\infty} p_n = 1 + \frac{A}{4} + \frac{1}{2} = \frac{6+A}{4}$$

$$A = 2$$

Для сравнения, алгоритм, предложенный в задаче 9 и решающей ту же самую задачу, работает в среднем $4\frac{2}{3}$ такта.

(*ii*) Дерево алгоритма:



Вероятность нуля:

$$x = \frac{2}{9} + \frac{5}{9}x \qquad \Longrightarrow \qquad x = \frac{1}{2}$$

В лучшем случае время работы — 2 такта, в худшем — бесконечно.