Последовательности де Брёйна и Универсальные Циклы
РЕШЕНИЯ

A Для начала

A.1 **Ответ.** Нет.

Предположим, что такая расстановка существует. Рассмотрим какое-нибудь число, например, 1. Пусть оно написано k раз, тогда оно встречается в $5k$ различных пятёрках. С другой стороны, количество пятёрок, в которых оно должно встречаться — это количество способов выбрать 4 числа из оставшихся. Но C_{99}^4 не делится на 5, поэтому получаем противоречие.

A.2 **Ответ.** Такая последовательность существует.

Сначала пронумеруем как-нибудь все возможные пятёрки натуральных чисел: например, пятёрку из чисел $(1, 2, 3, 4, 5)$ занумеруем единицей, потом занумеруем все пятёрки с суммой 16, потом с суммой 17 и так далее.

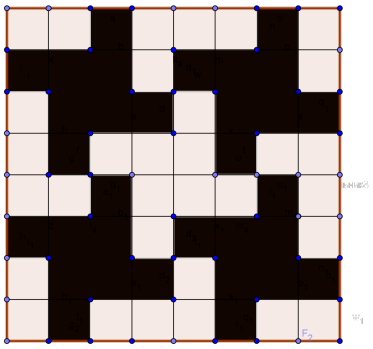
Пусть есть какая-то конечная последовательность натуральных чисел такая, что в ней встречаются все пятёрки с 1-й по k-ю и никакая пятёрка не повторяется дважды (при этом могут встречаться пятёрки с номерами, большими k). Покажем, что эту последовательность можно продолжить на конечное число членов вправо так, чтобы встретилась пятёрка с номером $k + 1$ и не возникло повторений.

В самом деле, если $(k + 1)$-я пятёрка уже встречается, то ничего делать не требуется. Иначе допишем справа 10 чисел $b_1, b_2, b_3, b_4, b_5, a_1, a_2, a_3, a_4, a_5$, где $a_1, \ldots, a_5$ — числа $(k+1)$-й пятёрки, а b_i — произвольные различные числа, большие всех остальных записанных (включая $a_1, \ldots, a_5$).

Бесконечное количество раз продолжая так последовательность, получим бесконечную последовательность натуральных чисел. То, что в ней встретятся все пятёрки, очевидно. Покажем, что никакая пятёрка не встретится дважды. В самом деле, пусть какая-то пятёрка записана дважды, тогда она оказалась записана дважды после какого-то шага, чего быть не может.

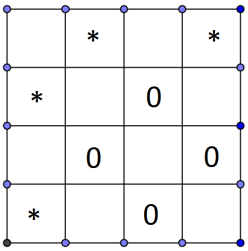
A.3 а) **Ответ.** Можно.

На рисунке приведён кусок плоскости 8×8. Попробуйте отыскать подобный узор, выглянув из окна.



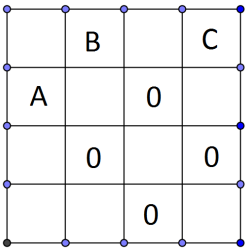
б) **Ответ.** Нельзя.

Показывается это несложным перебором. Предположим, что такая расстановка нулей и единиц существует, тогда все различные диагональные квадратики раскрашены по-разному (различными называются диагональные квадратики, не переводящиеся друг в друга параллельным переносом на вектор вида $(4a, 4b)$.) Всё дальнейшее будем рисовать на развёртке *тора* 4×4, белый и чёрный цвета заменим единичками и нулями.



Сначала найдём диагональный квадратик, в котором стоят четыре нуля.

Покажем, что во всех клетках, отмеченных звёздочками, должны стоять единицы. Эти четыре клетки по отношению к четырём найденным нулям расположены *одинаково*, поэтому достаточно показать для одной из них.

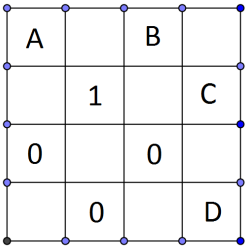


Пусть в A стоит 0, тогда в B и C стоит 1 (иначе ещё раз встретятся четыре нуля.) Но тогда два раза встретится расстановка «1 сверху, три нуля снизу».

Если на месте звёздочек стоят единицы, то уже есть все восемь расстановок единиц и нулей, в которых единиц чётное число. Заметим, что любой диагональный квадратик состоит либо из четырёх неотмеченных клеток, либо из четырёх отмеченных.

В восьми неотмеченных клетках должны встречаться всевозможные расстановки типа «три нуля и единица» и «три единицы и нуль».

Не умаляя общности, в четырёх клетках цифры стоят так же, как на рисунке.



Предположим, что на месте A стоит 0. Тогда из соображений чётности на месте B и C стоят нули, а на месте D — единица, легко видеть, что такая расстановка не подходит.

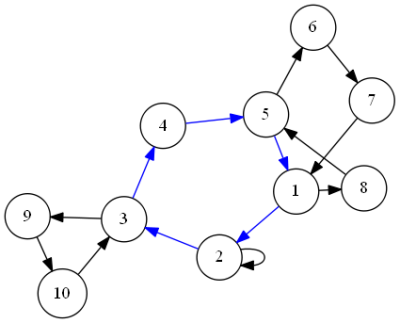
Если же на месте A стоит 1, то на месте B и C также должны стоять единицы, а на месте D – ноль. Тоже не подходит.

B Последовательности де Брёйна и ориентированные графы

B.4 Если есть эйлеров цикл, то, двигаясь по нему, в каждую вершину заходим столько же раз, сколько и выходим (сбалансированность); между любыми двумя рёбрами есть путь по циклу, а так как нет изолированных вершин, к каждой вершине примыкает по ребру и между любыми двумя вершинами есть путь по циклу циклу (сильная связность).

Пусть орграф сильносвязен и сбалансирован. Существование эйлерова цикла будем доказывать по индукции по количеству рёбер, база (0 рёбер) очевидна.

Выйдем из какой-нибудь вершины и будем идти по стрелкам, пока не придём в вершину, в которой уже были. Таким образом, в графе есть цикл C.



Удалим из орграфа рёбра этого цикла. Полученный орграф будет сбалансированным, но не обязательно связным.

Лемма. *Если сбалансированный орграф связен (то есть связен как граф, если забыть про ориентацию рёбер), то он сильно связен.*

Доказательство. Рассмотрим произвольную вершину v. Пусть A – множество вершин, в которые можно добраться из v, а B – все остальные вершины. Пусть B непусто. Тогда есть рёбра из B в A, но нет рёбер из A в B, значит, сумма по всем вершинам множества A количества входящих рёбер будет больше, чем количества исходящих. Но она – ноль из-за сбалансированности графа, противоречие. □

Итак, при удалении C граф распадается на сбалансированные сильносвязные компоненты, в каждой из которых по предположению индукции есть эйлеров цикл. Для каждой из этих компонент отметимна цикле C по одной вершине. Тогда искомый эйлеров цикл во всём графе строится так: идём по отрезку цикла C до очередной отмеченной точки, проходим по эйлерову циклу компоненты, возвращаясь в ту же точку, снова идём по C до следующей отмеченной точки и так далее.

B.5 Построим ориентированный граф, который в дальнейшем будем называть *графом де Брёйна* $G(n, k)$.

Вершинами его будут k^{n-1} последовательностей длины $n-1$ над k-буквенным алфавитом, а из вершины $a_1a_2\dots a_{n-1}$ ведёт ребро в $b_1b_2\dots b_{n-1}$, если $a_2 = b_1$, $a_3 = b_2$, $\dots$, $a_{n-1} = b_{n-2}$. Таким образом, рёбра $G(n, k)$ соответствуют последовательностям длины n и их всего k^n.

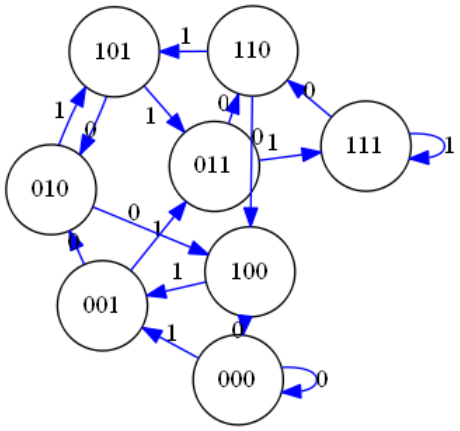


Рис. 1: $G(4, 2)$.

Вообще, каждому слову длины $n + a$ соответствует ориентированый путь длины $a + 1$. Вершины этого пути — это $(n-1)$-буквенные подслова нашего слова в порядке их появления.

На каждом ребре напишем последнюю букву соответствующего слова. Тогда, если последнее ребро пути соответствует слову $a_1a_2\dots a_k$, то буквы, написанные на предыдущих $k-1$ рёбрах этого пути, образуют слово $a_1a_2\dots a_{k-1}$.

Исходящая и входящая степень любой вершины равны k. Граф сильно связен, так как слово $a_1a_2\dots a_{k-1}$ соединено с $b_1b_2\dots b_{k-1}$ путём, соответствующим слову $a_1a_2\dots a_{k-1}b_1b_2\dots b_{k-1}$.

Значит, в $G(n,k)$ есть эйлеров цикл. Циклическая последовательность, образованная буквами, записанными на его последовательных рёбрах, будет последовательностью де Брёйна, так как подслова длины n соответствуют различным рёбрам графа.

B.6 База индукции: $k=0$.

Если мы сможем выбрать несколько рёбер так, чтобы из каждой вершины выходило ровно одно выбранное и в каждую вершину входило рово одно выбранное, то мы покрасим эти рёбра в первый цвет, удалим их и воспользуемся индукционным предположением для $k-1$.

Воспользуемся *леммой Холла*: если есть несколько девушек и юношей и для любого m любые m юношей знают в совокупности хотя бы m девушек, то можно для каждого юноши выбрать знакомую девушку так, чтобы для разных юношей были бы выбраны разные девушки.

Поместим в каждую вершину графа по юноше и по девушке и познакомим каждого юношу с теми девушками, к которым от него ведёт ориентированное ребро.

Предположим, что условия леммы Холла не выполняются: есть группа из m_1 юношей, и они знают в совокупности $m_2 < m_1$ девушек. Из вершин, в которых сидят эти юноши, выходит в совокупности km_1 рёбер, при этом все рёбра идут в множество из m_2 вершин. Значит, в какую-то из вершин ведёт хотя бы $\frac{km_1}{m_2} > k$ рёбер, противоречие.

Итак, выберем при помощи леммы Холла пары «юноша-девушка» и выберем в графе соответствующие рёбра. Из каждой вершины будет выходить ровно одно выбранное, в каждую вершину будет входить ровно одно выбранное, получили то, что хотели.

B.7 b) Упорядочим все буквы. Алгоритм будет выглядеть так: начинаем с $k-1$ нуля, на каждом шаге пишем максимальную возможную букву с тем условием, чтобы никакое слово длины k не повторилось дважды. Если получится сделать так $k^n - n + 1$ операцию, то если зациклить полученный результат, получится последовательность де Брёйна.

Интерпретация: дан граф де Брёйна $G(n,k)$, начинаем с вершины $000\dots0$. Движемся по рёбрам, каждый раз выбирая непроведённое ребро с наибольшей написанной буквой.

Предположим, что пришли в вершину, все рёбра из которой уже проведены. Это может быть только первая вершина пути, то есть $00\dots0$, так как во все остальные входили столько же раз, сколько из них выходили.

В этом пути должно встречается ребро $00\dots0$, иначе можно было бы двигаться дальше, добавив его к концу пути.

Рассмотрим все рёбра, по которым построенный путь не проходит, и покрасим их в серый цвет, серые рёбра, на которых написан 0, покрасим в чёрный цвет.

Лемма: ориентированного цикла, состоящего из чёрных рёбер, нет. Предположим противное. Найдётся путь длины k из чёрных рёбер, тогда последнее ребро этого пути соответствует слову $0\dots00$, но по этому ребру мы проходили. Противоречие.

Пусть есть хотя бы одно чёрное или серое ребро v_1v_2. В вершину v_2 входили меньше k раз, значит, из неё выходили меньше k раз и не выходили по ребру с написанным нулём. Значит, из v_2 выходит некоторое чёрное ребро v_2v_3. Аналогично, есть чёрное ребро v_3v_4 и так далее, в конечном итоге получим цикл из чёрных рёбер, а этого не может быть по лемме.

Пункт а) – частный случай при $k=2$.

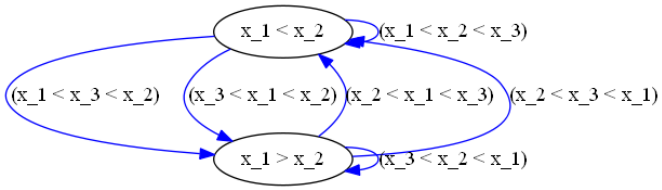
C Фокусы и универсальные циклы.

C.1 Пусть есть две последовательности чисел $a_1, a_2, \dots, a_n$ и $b_1, b_2, \dots, b_n$ такие, что в каждой из последовательностей все числа различны. Будем говорить, что они *упорядочены одинаковым образом*, если для любой пары индексов $i \neq j$ либо $a_i < a_j$ и $b_i < b_j$, либо, наоборот, $a_j > a_i$ и $b_j > b_i$.

Рассмотрим множество S_n способов упорядочить множество $\{1, 2, \ldots, n\}$. В S_n ровно $n!$ элементов, каждый из них называется *перестановкой длины* n. Фокуснику удастся фокус, если он придумает циклическую последовательность из $n!$ различных чисел такую, что все $n!$ различных кусков последовательности длины n упорядочены по-разному.

Для этого построим ориентированный граф $\mathbb{S}_n$, вершинами которого являются всевозможные перестановки длины $n-1$, а рёбра проводятся согласно следующему правилу. Для каждой перестановки $s \in S_n$ определим её *начало* как перестановку длины $n-1$, упорядоченную так же, как элементы s без последнего. Аналогично определим *конец* перестановки s (например, у перестановки 31542 началом является 2143, а концом — 1432). Наконец, для каждой $s \in S_n$ проведём ребро из её начала в конец.

Элементы S_n удобно записывать в виде системы неравенств на переменных $x_1, \ldots, x_n$, как показано на рисунке.



Граф $\mathbb{S}_3$

Покажем, что в $\mathbb{S}_n$ есть эйлеров цикл. В самом деле, из каждой вершины выходит n рёбер и в каждую вершину входит n рёбер, это — количество способов расположить новое число на числовой прямой относительно $n-1$ различных чисел. Проверим сильную связность: пусть s_1 и s_2 — две перестановки длины $n-1$. Рассмотрим какую-нибудь последовательность длины $2n-2$, состоящую из различных чисел и такую, что первые $n-1$ членов упорядочены способом s_1, а последние $n-1$ членов — способом s_2. Тогда рёбра пути, соединяющего s_1 с s_2 в графе $\mathbb{S}_n$ — это перестановки, соответствующие всем кускам последовательности длины n.

Выберем какой-нибудь эйлеров цикл в $\mathbb{S}_n$, пусть его рёбра в порядке следования соответствуют перестановкам s_1, s_2, …, $s_{n!}$. Возьмём $n!$ переменных $y_1, \ldots y_{n!}$ и будем считать, что $y_{n!+k} = y_k$. Каждая перестановка s_i задаёт систему неравенств на переменных $x_1, \ldots, x_n$. Запишем такую же систему неравенств, заменив каждую переменную x_k на y_{i+k-1}. Например, если s_3 задавала систему $x_2 > x_1 > x_3$, то мы запишем $y_4 > y_3 > y_5$. Наша цель — заменить переменные y_i числами так, чтобы выполнялось каждое из записанных неравенств.

Для каждой s_i проведём $\frac{n(n-1)}{2}$ ориентированных рёбер между $y_i, \ldots, y_{i+n-1}$, стрелка $y_{i_1} \to y_{i_2}$ соответствует неравенству $y_{i_1} > y_{i_2}$. Мы получили новый ориентированный граф H на вершинах $y_1, \ldots, y_{n!}$.

Лемма. *В графе H нет ориентированных циклов.*

Доказательство. Ребро $y_i \to y_j$ графа H назовём *идущим вправо*, если $j - i \in \{1, 2, \ldots, n-1\}$, и *идущим влево*, если тому же множеству принадлежит $i - j$. При $n > 2$ каждое ребро H принадлежит ровно одному из этих множеств, и если в H есть ребро $y_i \to y_j$, то ребра $y_j \to y_i$ в H нет.

Предположим противное. Рассмотрим в H ориентированный цикл с наименьшим количеством рёбер. Пусть у него есть два последовательных ребра, идущих в разные стороны — скажем, $y_i \to y_j$, идущее влево, и $y_j \to y_k$, идущее вправо. Все эти рёбра проведены для перестановки s_j; по той же причине ребро $y_i \to y_k$ также существует, и наш цикл можно сократить. Это противоречит выбору цикла.

Итак, если в H есть ориентированный цикл, то есть и ориентированный цикл C, все рёбра которого ведут в одном направлении — скажем, влево. С другой стороны, для некоторого индекса t перестановка s_t задаёт неравенства $x_1 < x_2 < \cdots < x_n$; тогда в H есть рёбра $y_{t+n-1} \to y_{t+n-2} \to \cdots \to y_t$. Но в цикле C должны встретиться две вершины из $y_t, \ldots, y_{t+n-1}$; ребро между ними будет идти вправо. Это противоречие завершает доказательство леммы. □

Поскольку циклы в H отсутствуют, мы можем ввести на переменных y_i частичный порядок: $y_{i_1} \succ y_{i_2}$, если из y_{i_1} в y_{i_2} ведёт путь в H.

Возьмём один из минимальных элементов, присвоим ему значение 1. Возьмём какой-нибудь минимальный из оставшихся, присвоим значение 2, и так далее для всех переменных y_i. Все нужные неравенства будут автоматически выполнены.

C.2 Решение можно найти в статье J. R. Johnson, Universal cycles for permutations, Discrete Math., 309(2009), pp. 5264–5270.

C.3 Решение во многом аналогично решению **C.1**.

Будем говорить, что две последовательности $(a_1, a_2, \ldots, a_n)$ и $(b_1, b_2, \ldots, b_n)$ *разбиты одинаково*, если для любых $i \neq j$ либо $a_i = a_j$ и $b_i = b_j$, либо $a_i \neq a_j$ и $b_i \neq b_j$. Обозначим через P_n множество разных разбиений последовательностей длины n.

Можно проверить, что в P_5 ровно 52 элемента, поэтому фокус удастся, если фокусник сумеет расположить по окружности 52 числа так, что все 52 последовательных пятёрок чисел будут разбиты по-разному.

Вот пример такой последовательности:

ББББКЧЧЧКККББКККЧКЧКПЧЧПБППБППЧПБББКЧППКЧПЧБЧПКЧПДКБК

Здесь вместо чисел стоят буквы П, К, Б, Ч, обозначающие карточные масти, и одна буква Д, обозначающая джокера. Можно взять обычную карточную колоду, заменить пиковую даму на джокера и продемонстрировать этот фокус.

Сейчас мы покажем, как получить такую последовательность с минимумом перебора (правда, у нас может получиться больше пяти различных чисел); мы работаем с P_5, но подобный метод позволяет находить универсальные циклы для P_n при всех $n > 4$.

Рассмотрим ориентированный граф $\mathbb{P}_5$, вершинами которого являются элементы P_4, а рёбра соответствуют элементам P_5 следующим образом. Для разбиения p из P_5 определим его *начало* и *конец* как разбиения из P_4, разбитые так же, как первые и последние $n-1$ элемент в p, соответственно. В графе $\mathbb{P}_5$ для каждого $p \in P_5$ проведём ребро от начала π к его концу. Скажем, разбиение 12324 задаст ребро $1232 \to 1213$.

Покажем, что $\mathbb{P}_n$ сильно связен. Пусть нужно найти путь между разбиениями p_1 и p_2. Рассмотрим последовательность длины $2n-2$, первая половина которой разбита так же, как p_1, а вторая — так же, как p_2. Тогда подпоследовательности длины n образуют рёбра нужного пути.

Сбалансированность также легко проверяется: если элемент P_4 содержит k различных элементов, то каждое исходящее и входящее ребро соответствует добавлению нового элемента, который либо равен одному из имеющихся, либо отличен от всех; таким образом, исходящая и входящая степени нашего элемента равны $k+1$.

Значит, в графе $\mathbb{P}_5$ можно найти эйлеров цикл. Каждый эйлеров цикл в $\mathbb{P}_5$ задаёт систему равенств и неравенств на множестве переменных $y_1, \ldots, y_{52}$, расставленных по циклу (способом, аналогичным введённому в **C.1**.

Если в системе есть равенство $y_i = y_j$, соединим эти переменные белым ребром, если же есть неравенство $y_i \neq y_j$, то соединим их чёрным ребром. Будем говорить, что полученная система противоречива, если есть две переменные, между которыми есть чёрное ребро и цепочка белых рёбер (это соответствует тому, что можно вывести соотношение $y_i \neq y_i$). Если система непротиворечива, то нужную расстановку чисел по кругу можно получить, заменив на одно и то же число те переменные, между которыми есть путь из белых рёбер.

Итак, осталось показать, что эйлеров цикл можно выбрать так, чтобы полученная система была непротиворечивой.

Прежде всего, заметим по аналогии с **C.1**, что если система противоречива, то существует противоречие вида

$$y_{i_1} = y_{i_2} = \cdots = y_{i_k} \neq y_{i_1},$$

где все стрелки $y_{i_j} \to y_{j+1}$ ведут вправо.

Рассмотрим последовательность $W = 113112222213311$. Она соответствует пути длины 11 в графе $\mathbb{P}_5$.

Лемма 1. *Если эйлеров цикл содержит сей путь, то получается непротиворечивая система.*

Доказательство. Рассмотрим 15 переменных (не умаляя общности, $y_1, \ldots, y_{15}$), участвующих в системах рёбер этого пути. Легко видеть, что любой путь, ведущий вправо и соединяющий какую-либо переменную

среди $y_1, \ldots, y_5$ с какой-либо из переменных $y_{11}, \ldots, y_{15}$, содержит хотя бы два чёрных ребра. Значит, противоречивого пути указанного вида нет. □

Лемма 2. *Путь, определённый последовательностью W, продолжается до эйлерова цикла.*

Доказательство. Удалим из $\mathbb{P}_5$ рёбра этого пути, заменив их на одно ребро из начала пути в его конец. Нам надо показать, что полученный граф сбалансирован и сильно связен. Первое очевидно; для второго (из-за сбалансированности) достаточно показать слабую связность.

Покажем, что любую последовательность из 4 символов можно продолжить вправо так, что полученная последовательность будет кончаться на 5 различных цифр, и при этом в ней не встретится подслова длины 5, разбитого так же, как какое-либо из подслов слова W.

Рассмотрим последовательность (a, b, c, d), где некоторые символы одинаковые. Попробуем приписать справа абсолютно новый символ e, это получится, если никакое подслово W не разбито так же, как (a, b, c, d, e). Попробуем к полученной последовательности приписать ещё один абсолютно новый символ, и так далее. Если удастся сделать так 4 раза, то мы получили что хотели. Иначе в некий момент добавление нового символа привело к появлению разбиения, соответствующего пятибуквенному подслову из W.

Что это может быть за подслово? Его последняя буква должна отличаться от остальных, значит, есть три варианта.

(a) Появилось 12113. Тогда вместо приписывания 3 припишем 2345.

(b) Появилось 33331. Но все рёбра, идущие из вершины, соответствующей разбиению 0000, уже входят в путь, соответствующий W, так что эту вершину следует просто удалить из нового графа.

(c) Появилось 33312. Тогда вместо 2 припишем 3245.

Лемма доказана. □

Эти две леммы дадут в совокупности всё, что нужно.

C.4 Рассмотрим полный граф на n вершинах, занумерованных числами $1, 2, \ldots, n$. Тогда то, что требуется сделать — этой найти в этом (неориентированном) графе эйлеров цикл. Он, очевидно, существует при нечётных n и не существует при чётных n.

C.5 Рассмотрим окружность, разбитую на n равных частей, и пронумеруем точки разбиения последовательно числами от 1 до n. Тогда тройка чисел задаёт разбиение окружности на три дуги. Будем говорить, что два трёхэлементных подмножества *имеют один разностный тип*, если упорядоченные с точностью до циклического сдвига тройки длин этих дуг равны. (Чтобы определить длины дуг, можно упорядочить числа и найти три циклические разности.)

Пример: при $n = 8$ множества $\{1, 3, 7\}$ и $\{1, 5, 3\}$ имеют один разностный тип $(2, 2, 4)$. Множества $\{1, 2, 5\}$ и $\{1, 4, 5\}$ имеют разные типы $(1, 3, 4)$ и $(3, 1, 4)$ соответственно.

Если n не делится на 3, то количество разностных типов есть $\frac{C_n^3}{n} = \frac{(n-1)(n-2)}{6}$.

Для начала покажем, как построить требуемую в условии конструкцию при $n = 8$. Всего есть 7 разностных типов:

$$(1, 1, 6), \quad (2, 2, 4), \quad (2, 3, 3), \quad (1, 2, 5), \quad (5, 2, 1), \quad (1, 3, 4), \quad (4, 3, 1).$$

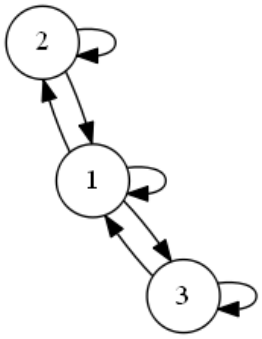
Далее мы хотим выбрать в каждом типе (x, y, z) одну из упорядоченных пар $x \to y$, $y \to z$ или $z \to x$. Сделаем в этих семи типах соответственно такой выбор:

$$1 \to 1, \qquad 2 \to 2, \qquad 3 \to 3, \qquad 1 \to 2, \qquad 2 \to 1, \qquad 1 \to 3, \qquad 3 \to 1.$$

Получился связный и сбалансированный ориентированный граф. В нём есть эйлеров цикл, при этом сумма чисел в цикле сравнима с 5 по модулю 8:

$$(1 \to 1 \to 2 \to 2 \to 1 \to 3 \to 3 \to) 1 \to \ldots$$

Запишем этот цикл в виде бесконечной периодической последовательности (a_k). Тогда последовательность $b_k = a_1 + \cdots + a_k$, взятая по модулю 8, будет периодична с периодом $7 \cdot 8 = 56$.



Покажем, что в этой последовательности любая тройка остатков по модулю 8 встречается. В самом деле, любую тройку остатков можно представить в виде $(x, x+k_1, x+k_1+k_2) \mod 8$ так, что в последовательности a_i встречается подряд пара k_1, k_2. Пусть $a_i = k_1, a_{i+1} = k_2$. Тогда $a_{i+8n} = k_1, a_{i+1+8n} = k_2$ для любого n. Так как $a_1 + \cdots + a_8 \equiv 5 \mod 8$, то найдётся такое n, что число $b_{8n+i-1} \equiv a_1 + \cdots + a_{i-1} + n(a_1 + \cdots + a_8)$ сравнимо с x по модулю 8.

Тогда тройка $b_{8n+i-1}, b_{8n+i}, b_{8n+i+1}$ — это именно то, что нам надо.

Перейдём к общей конструкции.

Лемма. *Для любого $n \geq 8$, не дедящегося на 3, в каждом из разностных типов можно выбрать упорядоченную пару так, чтобы $\frac{(n-1)(n-2)}{6}$ полученных рёбер образовывали сбалансированный сильносвязный орграф. (Естественно, вершинами графа будут ровно те числа, из которых выходит хотя бы одно ребро.)*

Доказательство. Рассмотрим два случая.

Случай 1: n чётно. Если в разностном типе есть два одинаковых числа, мы возьмём эти два числа; получим петли $i \to i$ для всех i от 1 до $n/2-1$. Если же все три числа различные, выбросим наибольшее. Полученный граф на вершинах $1, \ldots, n/2-1$ будет сбалансированным, так как вместе с каждым ребром $i \to j$ есть ребро $j \to i$, и сильно связным, так как каждое из чисел $2, \ldots, n/2-1$ соединено рёбрами обоих направлений с 1.

Случай 2: n нечётно. Множеством вершин будут числа от 1 до $(n-1)/2$. Если в типе есть пара равных чисел, выбираем её; получается по петле на каждой из вершин. Если все три числа разные, то выбрасываем наибольшее число, кроме двух случаев. Эти случаи — две тройки $(2, (n-1)/2-1, (n-1)/2)$ и $(2, (n-1)/2, (n-1)/2-1)$. Для них мы выбираем соответственно $(n-1)/2 \to 2$ и $2 \to (n-1)/2$.

Полученный граф снова сбалансирован, а сильно связен он потому, что каждое число, кроме $(n-1)/2$, соединено с 1 напрямую, а $(n-1)/2$ соединено с двойкой. □

Обозначим построенный граф через L_n; в нём $[\frac{n-1}{2}]$ вершин и есть петля $1 \to 1$. Нам потребуется ещё один граф, который обозначим $\mathbb{L}_n$. В $\mathbb{L}_n$ будет $n[\frac{n-1}{2}]$ вершин, каждая вершина кодируется парой (k, i), где k — остаток по модулю n, i — вершина в L_n. Для каждого ребра $i \to j$ графа L_n в графе $\mathbb{L}_n$ проводится n рёбер (по одному для каждого k) вида $(k, i) \to (k+i, j)$.

Из сбалансированности L_n следует сбалансированность $\mathbb{L}_n$. Покажем, что он сильно связен. Для сбалансированного графа сильная связность эквивалентна связности, поэтому достаточно показать, что из любой вершины можно добраться до $(0, 1)$. В самом деле, так как в L_n из любой вершины можно добраться до 1, то в $\mathbb{L}_n$ из любой вершины можно попасть в вершину вида $(k, 1)$. При этом для всех k в $\mathbb{L}_n$ есть ребро $(k, 1) \to (k+1, 1)$. Двигаясь по таким рёбрам, можно дойти до $(0, 1)$.

Итак, в $\mathbb{L}_n$ есть эйлеров цикл. Его длина равна C_n^3, и для любого k и любого ребра $i \to j$ графа L_n в этом цикле встретится последовательная тройка вершин $(k, i), (k+i, j), (k+i+j, *)$ (нас не интересует, что стоит на месте звёздочки). Значит, если записать последовательность первых координат вершин цикла, в этой последовательности встретится любая тройка остатков по модулю n.

D Начало перечисления

D.1 Граф $\mathcal{L}G$ связен тогда и только тогда, когда для любых двух рёбер e_1, e_2 графа G есть ориентированный путь, первым ребром которого является e_1, а последним — e_2.

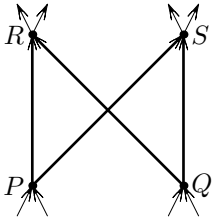
Пусть G связен и e_1, e_2 — два его ребра. Из конца e_1 можно прийти в начало e_2 по некоторой последовательности рёбер T, тогда G есть путь e_1Te_2.

Пусть $\mathcal{L}G$ связен. Граф G будет связен, если любая вершина является началом некоторого ребра и концом некоторого ребра. Действительно, тогда для нахождения пути из v_1 в v_2 достаточно найти путь от ребра с началом в v_1 до ребра с концом в v_2.

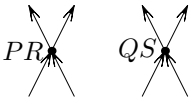
Предположим, что это не выполняется; не умаляя общности, из вершины v не выходит ни одного ребра. Так как v не изолирована, в неё входит какое-то ребро e. Кроме этого ребра, в G есть другое ребро e'. Но тогда не существует пути, первым ребром которого является e, а последним — e'. Противоречие.

D.2 В графе $\mathcal{L}G$ исходящие и входящие степени каждой вершины также равны двум. В $\mathcal{L}G$ есть вершины P, Q, R, S, из вершин P и Q идёт по ребру в R и S.

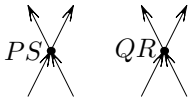
Граф $\mathcal{L}G_1$ получается из $\mathcal{L}G$ так: рёбра PS, PR, QS и QR удаляются, вершины P и R склеиваются в вершину (PR), а вершины Q и S склеиваются в (QS). Аналогично можно описать $\mathcal{L}G_2$: удаляются те же четыре ребра, вершины P и S склеиваются в (PS), вершины Q и R склеиваются в (QR).



Graph $\mathcal{L}G$



Graph $\mathcal{L}G_1$



Graph $\mathcal{L}G_2$

Рёбра PR, QS, PS и QP графа $\mathcal{L}G$ будем называть *особыми*, вершины (PR), (QS), (PS) и (QP) в графах $\mathcal{L}G_1$ и $\mathcal{L}G_2$ также будем называть особыми.

Назовём *великой четвёркой* неупорядоченное множество из четырёх путей в графе $\mathcal{L}G$ таких, что их множества рёбер не пересекаются и в объединении дают все рёбра графа $\mathcal{L}G$, кроме четырёх особых. Таким образов, в каждой великой четвёрке есть по два пути, начинающиеся в R, два пути, начинающиеся в S, два пути, заканчивающиеся в Q, и два пути, заканчивающиеся в P.

В графе $\mathcal{L}G_1$ (аналогично в $\mathcal{L}G_2$) великая четвёрка соответствует четвёрке путей, содержащих все рёбра графа, начинающихся и кончающихся в особых вершинах и не содержащих особых вершин кроме начальных и конечных. Будем считать, что в графах $\mathcal{L}G$, $\mathcal{L}G_1$ и $\mathcal{L}G_2$ великая четвёрка одна и та же.

Каждый эйлеров цикл в $\mathcal{L}G$ особыми рёбрами разбивается на четыре куска, образующие великую четвёрку. Аналогично, эйлерова цикл в $\mathcal{L}G_1$ или $\mathcal{L}G_2$ через каждую из особых вершин проходят по два раза и разбиваются на великую четвёрку.

Задача будет решена, если мы докажем, что каждой великой четвёрке в $\mathcal{L}G$ соответствует 4 эйлерова цикла, а в $\mathcal{L}G_1$ и $\mathcal{L}G_2$ суммарно 2 эйлеровых цикла.

Великая четвёрка путей в $\mathcal{L}G$ может быть трёх типов.

(a) По одному пути, ведущему из R в P, из R в Q, из S в P и из S в Q.

(b) По два пути, ведущих из R в P и из S в Q.

(c) По два пути, ведущих из R в Q и из S в P.

Разберём все случаи.

(a) Будем обозначать пути великой четвёрки $R \dots P$, $R \dots Q$, $S \dots P$ и $S \dots Q$. Есть 6 способов циклически их упорядочить. Каждый способ можно записать в виде

$$X_1 \dots Y_1 X_2 \dots Y_2 X_3 \dots Y_3 X_4 \dots Y_4,$$

где X_i — это начала путей, а Y_i — их концы. При каждом способе возникают четыре пары вершин Y_iX_{i+1}. Если множества этих пар совпадают с $\{PS, PR, QS, QR\}$, то этому способу соответствует эйлеров цикл в $\mathcal{L}G$. Если получается $\{PR, PR, QS, QS\}$, то это эйлеров цикл в $\mathcal{L}G_1$, если $\{PS, PS, QR, QR\}$ — то эйлеров цикл в $\mathcal{L}G_2$. Выпишем эти способы.

(i) $R \dots PR \dots QS \dots PS \dots Q$ — множество $\{PR, QS, QR, PS\}$, цикл в $\mathcal{L}G$;
(ii) $R \dots PR \dots QS \dots QS \dots P$ — множество $\{PR, QS, QS, PR\}$, цикл в $\mathcal{L}G_1$;
(iii) $R \dots PS \dots PR \dots QS \dots Q$ — цикл в $\mathcal{L}G$;
(iv) $R \dots PS \dots PS \dots QR \dots Q$ — цикл в $\mathcal{L}G_2$;
(v) $R \dots PS \dots QR \dots QS \dots P$ — цикл в $\mathcal{L}G$;
(vi) $R \dots PS \dots QS \dots PR \dots Q$ — цикл в $\mathcal{L}G$.

Итак, имеем 4 цикла в $\mathcal{L}G$ и по циклу в $\mathcal{L}G_1$ и $\mathcal{L}G_2$.

(b) Всё происходит так же, как в предыдущем пункте, но у двух пар путей будет одинаковое обозначение: два (разных) пути $R \dots P$ и два разных пути $S \dots Q$.

(i) $R \dots PR \dots PS \dots QS \dots Q$ — цикл в $\mathcal{L}G$;
(ii) $R \dots PR \dots PS \dots QS \dots Q$ — снова цикл в $\mathcal{L}G$. Хотя написано то же самое, следует иметь в виду, что это другой порядок, так как два из путей великой четвёрки переставлены.
(iii) $R \dots PS \dots QR \dots PS \dots Q$ — цикл в $\mathcal{L}G_2$;
(iv) $R \dots PS \dots QS \dots QR \dots P$ — цикл в $\mathcal{L}G$;
(v) $R \dots PS \dots QR \dots PS \dots Q$ — цикл в $\mathcal{L}G_2$;
(vi) $R \dots PS \dots QS \dots QR \dots P$ — цикл в $\mathcal{L}G$.

4 цикла в $\mathcal{L}G$ и два цикла в $\mathcal{L}G_2$.

(c) Полностью аналогично предыдущему пункту.

D.3 Ответ: $2^{2^{n-1}-n}$**,**

Мы приводим решение, предложенное А. Зиминым.

Понятно, что $B(2, n) = \epsilon(G(2, n))$. Будем доказывать по индукции, что $\epsilon(G(2, n)) = \frac{2^{2^{n-1}}}{2^n}$.

Несложно понять, что $\mathcal{L}G(2, n) = G(2, n + 1)$. В самом деле, вершины $G(2, n + 1)$ соответствуют рёбрам $G(2, n)$, а рёбра $G(2, n + 1)$ соответствуют бинарным словам длины $n + 1$, то есть путям в $G(2, n)$ длины 2.

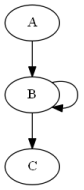
Лемма. *Пусть орграф G содержит n вершин, исходящие и входящие степени всех вершин равны 2. Тогда $\epsilon(\mathcal{L}G) = 2^{n-1}\epsilon(G)$.*

Заметим, что индукционный переход мгновенно следует из леммы: в $G(2, n)$ число вершин равно 2^{n-1}, поэтому

$$\epsilon(\mathcal{L}G(2, n)) = 2^{2^{n-1}-1}2^{2^{n-1}-n} = \frac{2^{2^n}}{2^{n+1}}.$$

Доказательство леммы. Будем доказывать лемму индукцией по количеству вершин. База: $n = 1$. Такой граф является вершиной с двумя петлями, в нём один эйлеров обход, в его рёберном графе, как несложно убедиться, тоже.

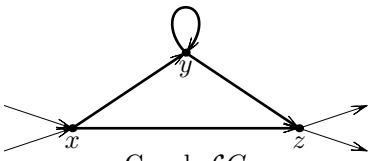
Переход $n \to n + 1$. Пусть в G есть вершина с двумя петлями, тогда она даёт отдельную компоненту связности и у обоих графов нет эйлеровых циклов.



Пусть в G есть вершина B с петлёй. Тогда в эйлеровом цикле после прохода по ребру AB нужно идти по петле $B \to B$, а после по ребру $B \to C$. Заменой вершины B на ребро AC получим граф G_1.

При этом $\epsilon G = \epsilon G_1$. Графы $\mathcal{L}G$ и $\mathcal{L}G_1$ отличаются в одном фрагменте, как показано на рисунке ниже ($x = A \to B, y = B \to B, z = B \to C$).

Каждому эйлерову циклу в $\mathcal{L}G_1$ соответствуют два цикла в $\mathcal{L}G$: дважды входим и выходим в вершину xyz и в $\mathcal{L}G$ есть два способа её обойти: $x \to y \circlearrowleft y \to z$ и $x \to z$. Два цикла получатся в зависимости от того, в каком порядке мы их применяем.



Graph $\mathcal{L}G$

Graph $\mathcal{L}G_1$

Тогда

$$\epsilon(G) = \epsilon(G_1) = \frac{1}{2^{n-1}}\epsilon(\mathcal{L}G_1) = \frac{1}{2^n}\epsilon(\mathcal{L}G).$$

Посмотрим теперь на вершину, в которой нет петель. Построим графы G_1 и G_2, как в задаче **D2**. В каждом из них по $n-1$ вершине и они удовлетворяют условию леммы. Каждый эйлеров цикл в G соответствует одному циклу в G_1 или в G_2. Итак, $\epsilon(G) = \epsilon(G_1) + \epsilon(G_2)$,

$$\epsilon(\mathcal{L}G) = 2(\epsilon(\mathcal{L}G_1) + \epsilon(\mathcal{L}G_2)) = 2 \cdot 2^{n-1}(\epsilon((G_1) + \epsilon(G_2))) = 2^n\epsilon(G).$$

Лемма доказана.

E Торы де Брейна

Общее замечание. В этой секции мы будем рассматривать буквы алфавита $X_k = \{1, 2, \ldots, k\}$ как остатки по модулю k, чтобы с ними можно было производить арифметические операции. Имея дело с клетчатой решеткой, мы обычно будем обозначать j-ю клетку в i-й строке через (i, j).

E.1 Для удобства построим тор типа $(k, k^{u-1}, 1, u)_k$ и отразим его относительно главной диагонали.

Для начала предположим, что $u \geq 3$. Пусть $c_1, c_2, c_3, \ldots, c_{k^{u-1}}$ - последовательность де Брейна ранга $u-1$ над алфавитом $X_k = \{1, 2, \ldots, k\}$; продолжим ее, чтобы получить бесконечную k^{u-1}−периодическую последовательность. Поставим в клетку (i, ℓ), $\ell > 0$, решетки число

$$a_{i,\ell} = i + \sum_{s=1}^{\ell} c_s$$

(сложение происходит по модулю k). Аналогично продолжим расстановку и для $\ell \leq 0$.

Каждое число встречается в периоде $c_1, c_2, \ldots, c_{k^{u-1}}$ ровно k^{u-2} раз; так как $u \geq 3$, сумма $\sum_{s=1}^{k^{u-1}} c_s$ делится на k. Тогда расстановка действительно является k^{u-1}-периодической по горизонтали и k-периодической по вертикали, то есть дает тор искомого размера. (Обратите внимание, что периодичность также выполняется для $u = 2$ и нечетного k.)

Остается показать, что каждые u чисел $x_0, \ldots, x_{u-1}$ встречаются подряд в некоторой строке. Поскольку (c_i) - последовательность де Брейна, найдется ℓ, для которого $c_{\ell+i} = x_i - x_{i-1}$ при $i = 1, \ldots, u-1$. Поскольку числа $a_{1,\ell}, \ldots, a_{k,\ell}$ попарно различны, найдется r такой что $a_{r,\ell} = x_0$. По нашей конструкции

$$a_{r,\ell+i} = a_{r,\ell} + \sum_{s=1}^{i} c_{\ell+s} = x_0 + \sum_{s=1}^{i}(x_s - x_{s-1}) = x_i,$$

то есть мы нашли необходимый прямоугольничек $1 \times u$.

Теперь рассмотрим случай $u = 2$ и $k \geq 3$. Нам нужно заполнить строки тора $k \times k$ числами $1, 2, \ldots, k$, так что каждая паря чисел встречается подряд в некоторой строке. В терминах графа де Брейна $G(2, k)$, определенного в решении задачи **B.5**, нам нужно разбить ребра этого графа на k циклов длины k.

Если k нечетно, $k = 2t + 1$, можно использовать циклы

$$\big(a \to (a+1) \to a \to (a+2) \to a \to \cdots \to a \to (a+t) \to a \to a\big)$$

при $a = 1, 2, \ldots, k$. (В этом случае также проходит и предыдущий метод.)

Если k четно, $k = 2t$, мы можем начать с циклов

$$C_a = \big(a \to (a+1) \to a \to (a+2) \to a \to \cdots \to a \to (a+t-1) \to a\big)$$

при $a = 1, 2, \ldots, 2t$. Длина каждого из этих циклов равна $2t - 2$, и они покрывают все ребра кроме ребер вида $x \to x$ и $x \to x + t$. Несложно проверить, что можно добавить к циклу C_{2i-1} ребра $(t + i - 1) \to (i - 1) \to (t + i - 1)$, а к циклу C_{2i} две петли $2i \to 2i$ и $(2i + 1) \to (2i + 1)$. Получим искомое разбиение.

E.2 Пусть $\ldots, c_1, c_2, \ldots, c_{k^2}, \ldots$ - перидически продолженная в обе стороны последовательность де Брейна ранга 2 над алфавитом X_k. Мы поместим в строки решетки сдвиги этой последовательности. В $i-$й строке запишем последовательность, сдвинутую вправо на $0 + 1 + \cdots + (i - 1)$ клеток. То есть i-я строка будет представлять собой $i - 1$-ю, сдвинутую на $i - 1$. По сравнению с первой строкой $(k^2 + 1)$-я сдвинута на $1 + 2 + \cdots + k^2$; что делится на k^2, то есть расстановка действительно задает тор $k^2 \times k^2$.

Для любого квадратика 2×2, его нижний и верхний ряды встречаются в последовательности де Брейна. Если верхний ряд встречается на расстоянии s влево от нижнего, то искомый квадратик встретится в объединении s-й и $s + 1$-й строк.

E.3 Для решения этой задачи можно модифицировать метод из предыдущей. Опять же, будем строить тор $(k^{u(v-1)}, k^u, v, u)_k$. Пусть $R = k^{u(v-1)}$ и $S = k^u$.

Возьмем последовательность де Брейна ранга u (с периодом длины S). Мы будем записывать ее сдвиги в строки, причем сдвинем $i-$ю строку относительно $i-1$-й на d_i вправо (то есть $i-$я строка будет сдвинута относительно нулевой на $d_1 + \cdots + d_i$. Для того, чтобы расстановка была R-периодичной по вертикали, нам нужно условие $d_{i+R} = d_i$ и чтобы сумма $d_1 + \cdots + d_R$ делилась на S. Чтобы получить все возможные прямоугольники $v \times u$, просто нужно, чтобы все последовательности из $v - 1$ сдвигов встречались в последовательности (d_i). Тогда в качестве (d_i) можно взять последовательность де Брейна ранга $v - 1$ над алфавитом X_S.

Но сумма чисел в периоде (d_i) равна

$$k^{u(v-2)} \cdot (1 + 2 + \cdots + k^u),$$

и это число делится на k^u для $k, u, v \geq 2$, за исключением случая, когда $v = 2$ и k четно.

E.4 Решение для случая $k = 2$ уже было приведено для задачи **A.3a)**; поэтому будем предполагать, что $k \geq 4$.

Шаг 1. Построим последовательность де Брейна $C = (c_1, \ldots, c_{k^2})$ ранга 2 с дополнительным учловием $c_{k^2/2} = c_{k^2}$. Рассмотрим граф де Брейна $G(2, k)$ и разобьем его ребра на группы $M_i = \{(\ell, \ell + i) : \ell = 1, 2, \ldots, k\}$. Распределим эти группы на два равных семейства, так чтобы M_1 и M_{k-1} были в разных семействах. То есть мы разделили все ребра между двумя подграфами, каждый из которых сильно связный и сбалансированный.

Возьмем эйлеровы циклы в этих подграфах и склеим их в общей вершине v. Мы получим эйлеров цикл во всем графе, который дает нужную последовательность.

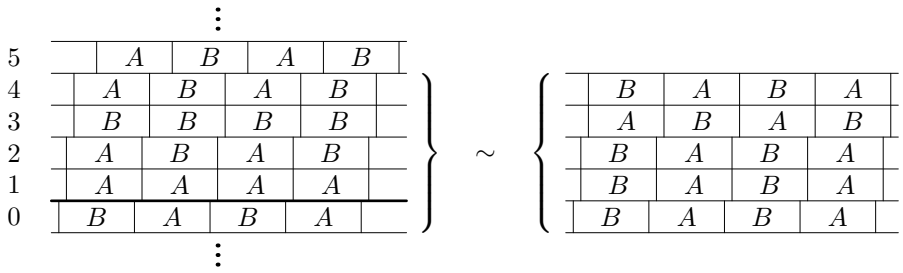
Шаг 2. Теперь проделаем почти такую же процедуру как в **E.2**. Рассмотрим построенную последовательность C и обозначим через A и B ее первую и вторую половины. Заметим, что каждая последовательность из двух букв встречается либо в последовательности с периодом A, либо в последовательности с периодом B. (Здесь как раз пригождается дополнительное свойство последовательности)

Поставим последовательность с периодом C в строки с номерами с 4 по k^2, так что относительные сдвиги двух соседних строк принимают значения от 0 до $k^2 - 1$, кроме 0, 1, $k^2/2$, и $k^2/2 + 1$. Сумма всех чисел от 0 до $k^2 - 1$ сравнима с $k^2/2$ по модулю k^2, так что k^2-я (как и нулевая) строка будет сдвинута относительно четвертой на $k^2/2 - 2$.

Поместим во вторую строку ту же самую последовательность, сдвинув ее на одну клетку влево относительно четвертой строки. Наконец, поместим последовательность с периодом A в первую строку и

последовательность с периодом B в третью строку. Сдвинем их так, чтобы части A в первой и второй строке были строго одна над другой и то же самое для частей B в третьей и четвертой строках (см. рисунок).

Поскольку мы несколько изменили расстановку по сравнению с **E.2**, необходимо проверить, что квадратики 2×2 в строках с нулевой по четвертую такие же, как они были бы при использовании обычных последовательностей де Брейна с относительными сдвигами 0, 1, $k^2/2$, и $k^2/2+1$. Легко видеть, что квадратики в строках 1–2 и 3–4 такие же, как они были бы для обычных строк де Брейна с относительными сдвигами на 0 и $k^2/2$, тогда как квадратики в строках 0–1 и 2–3 такие же, как они были бы в парах строк со сдвигами на 1 и $k^2/2+1$.



E.5 Есть несколько подобных конструкций. Мы изложим ту, которая использует задачу **E.6**

Предположим, что $k > 2$. Возьмем тор де Брейна типа $(k^2, k^2, 2, 2)_k$, построенный в **E.2** (для нечетных k) или в **E.4** (для четных k). Можно проверить, что в обеих конструкциях сумма буква в каждой строке 0 (это почти тривиально для обычной последовательности де Брейна, для половинок из задачи **E.4** нужно вспомнить явную конструкцию). Тогда можно применить **E.6** к этому тору и отразить относительно диагонали, чтобы получить нужный тор типа $(k^4, k^2, 2, 3)_k$.

К сожалению, этот метод не работает для $k = 2$, поскольку в (в сущности единственной) конструкции тора де Брейна типа $(4, 4, 2, 2)_2$ суммы по строкам нечетны. Но можно применить следующий подход. Два столбца тора $(4, 4, 2, 2)_2$ содержат все восемь различных прямоугольников 3×1, то есть нужно скомпоновать их так, чтобы получить все возможные сочетания. Одна из таких расстановок приведена на картинке снизу.

1	1	0	0	1	0	1	1	1	0	0	1	1	0	1	1
0	0	1	1	0	1	1	1	0	0	1	1	0	0	1	0
0	0	1	1	0	0	0	1	0	1	1	0	0	0	0	1
0	0	1	1	0	0	1	0	0	0	1	1	0	1	1	1

E.6 Для последующего применения мы докажем более общее утверждениет, в котором R и S не обязательно степени k, но просто натуральные числа, для которых $RS = k^{uv}$. Рассуждение будет похоже на то, которое применялось для **E.1**.

Шаг 1. Теперь нам нужно построить последовательность длиннее, чем обычная последовательность де Брейна. А именно, нам понадобится циклическая последовательность букв алфавита X_k с периодом $p_1, p_2, \ldots, p_{Sk^v}$, такая что для любого слова $x_1 \ldots x_v$ и числа $\ell = 1, 2, \ldots, S$ найдется такое $i \equiv \ell \pmod S$, такое что $p_{i+1} = x_1$, $p_{i+2} = x_{i+2}$, $\ldots$, $p_{i+v} = x_v$. То есть любое слово длины v в алфавите X_k встретится ровно S раз в периоде.

Чтобы доказать это, рассмотрим другой граф G'. Его вершины будут иметь вид $(w; i)$, где w - слово длины $v-1$ в алфавите X_k, а $i \in \{1, 2, \ldots, S\}$ (мы будем рассматривать индексы i как остатки по модулю S). Если обычный граф де Брейна $G(v, k)$ содержит ребро из w_1 в w_2, проведем ребро из $(w_1; i)$ в $(w_2; i+1)$ для любого $1, 2, \ldots, S$. Очевидно, что G' сбалансирован и сильно связен, то есть в нем найдется эйлеров цикл. Посмотрев на этот цикл как на слово, мы получим нашу последовательность. Нужное слово $x_1 \ldots x_v$ в позиции, сравнимой с i по модулю S, в точности соответствует ребру $(x_1 \ldots x_{v-1}; i) \to (x_2 \ldots x_v; i+1)$.

Шаг 2. Теперь построим нужный тор типа $(R, Sk^v, u, v)_k$. Обозначим через $a_{i,j}$ букву в позиции (i, j) в данном торе. Рассмотрим клетку (I, J) ів новом торе и пусть $j = J \mod S$. Тогда мы поставим в эту

клетку число

$$A_{I,J} = p_J + \sum_{m=1}^{I} a_{m,j}.$$

Из-за условий, наложенных на первоначальный тор, новая расстановка R-периодична по вертикали. Очевидно, что она также Sk^v-периодично по горизонтали.

Каждая строка нового тора удовлетворяет тем же условиям, что и последовательность, построенная в Шаге 1. Действительно, подслова из of (p_j) в позициях, сравнимых с i по модулю S - это просто всевозможные слова, и при переходе к другой строке в тех же местах будут встречаться эти слова, к которым покомпонентно прибавлено фиксированное слово.

Легко видеть, что построенный тор содержит любой прямоугольник $(u+1)\times v$. Пусть $(x_{i,j})$ - расположение чисел в таком прямоугольнике. Пусть $y_{i,j} = x_{i+1,j} - x_{i,j}$. Расстановка $(y_{i,j})$ встречается где-то в старом торе, скажем, в позиции с $(\alpha+1, \beta+1)$ по $(\alpha+u, \beta+v)$. Тогда новый тор содержит необходимую расстановку в одной из k^v позиций $(\alpha+1, \beta+1+\mu S)$–$(\alpha+u+1, \beta+v+\mu S)$ при $\mu = 0, 1, \ldots, k^v-1$, аналогично **E.1**.

Замечание. Исходя из свойств строк несложно заметить, что суммы в строках полученного тора делятся на k. Поэтому можно применить это действие несколько раз, каждый раз отражая получившийся тор относительно главной диагонали.

Более того, можно показать, что достаточно отражать через раз, если Sk^{v-2} делится на k. Действительно, пусть $p_1, \ldots, p_{Sk^v}$ — период в некоторой строке в торе, получившемся после первой итерации. Столбец после второй итерации будет иметь вид

$$\alpha, \quad \alpha+p_1, \quad \alpha+(p_1+p_2), \quad \ldots, \quad \alpha+(p_1+\cdots+p_{Sk^v-1}).$$

Сумма этих чисел сравнима по модулю k с

$$-p_1 - 2p_2 - \cdots - (Sk^v-1)p_{Sk^v-1} \equiv -\big(p_1+p_{k+1}+\cdots+p_{Sk^v-k+1}\big) - 2\big(p_2+p_{k+2}+\cdots+p_{Sk^v-k+2}\big) - \cdots.$$

В каждой скобке любая буква встречается Sk^{v-2} раз; это число делится на k, то есть общая сумма также делится на k.

E.7 Начав с конструкции из **E.5**, применим **E.6** трижды, чтобы получить

$$(k^4, k^2, 2, 3)_k \xrightarrow{(1)} (k^4, k^5, 3, 3)_k \xrightarrow{(2)} (k^4, k^8, 4, 3)_k \xrightarrow{(3)} (k^8, k^8, 4, 4)_k;$$

иногда отражая. Чтобы доказать, что **E.6** применимо в данном случае, нам нужно показать, что соответствующие суммы в строке/столбце делятся на k на каждом из трех шагов. Для шага (3) это следует из замечания после **E.6**. Если $k > 2$, то то же выполнено для шагов (1) и (2), мы получали тор $(k^4, k^2, 2, 3)_k$ по тому же алгоритму. В исключительном случае $k = 2$, можно проверить необходимое условие вручную (картинка в конце **E.5**).

В этом месте стоит сказать, что не все торы типа $(k^4, k^2, 2, 3)_k$ удовлетворяют необходимому условию.

E.8 Для начала докажем утверждение для четных $n = 2t$ индукцией по t. Случаи $t = 1, 2$ уже разбирались выше.

Предположим, что тор типа $(k^{2t^2}, k^{2t^2}, 2t, 2t)$ уже был построен, и **E.6** было применено несколько раз, чтобы увеличить вертикальную сторону тора. Тогда достаточно применить **E.6** еще несколько раз

$$\begin{aligned}
\big(k^{2t^2}, k^{2t^2}, 2t, 2t\big)_k &\longrightarrow \big(k^{2t^2}, k^{2t(t+1)}, 2t+1, 2t\big)_k \\
&\longrightarrow \big(k^{2t^2+2t+1}, k^{2t(t+1)}, 2t+1, 2t+1\big)_k \\
&\longrightarrow \big(k^{2(t+1)^2}, k^{2t(t+1)}, 2t+1, 2t+2\big)_k \\
&\longrightarrow \big(k^{2(t+1)^2}, k^{2(t+1)^2}, 2t+2, 2t+2\big)_k.
\end{aligned}$$

Каждый раз утверждение **E.6** применимо благодаря замечанию после доказательства.

Предположим, что n нечетно, но k - точный квадрат, то есть $n = 2t+1$ и $k = a^2$, a нечетно. Тогда можем провести похожую индукцию. Для базового случая $t = 0$, достаточно расположить $1, 2, \ldots, a^2$ в клетках

квадрата $a \times a$, так чтобы сумма в каждом столбце делилась бы на на a^2 (нам нужно это условие, чтобы применить **E.6**). Для этого нужно разбить эти числа на a групп с равными суммам, что как известно возможно.

Для шага индукции предположим, что тор типа $(a^{(2t+1)^2}, a^{(2t+1)^2}, 2t+1, 2t+1)_k$ уже построен, и **E.6** было применено в прошлый раз, чтобы увеличить вертикальную сторону тора (если вообще было применено). Тогда достаточно применить **E.6** следующим образом

$$\begin{aligned}
\left(a^{(2t+1)^2}, a^{(2t+1)^2}, 2t+1, 2t+1\right)_k &\longrightarrow \left(a^{(2t+1)^2}, a^{(2t+1)(2t+3)}, 2t+2, 2t+1\right)_k \\
&\longrightarrow \left(a^{2t^2+8t+5}, a^{(2t+1)(2t+3)}, 2t+2, 2t+2\right)_k \\
&\longrightarrow \left(a^{(2t+3)^2}, a^{(2t+1)(2t+3)}, 2t+2, 2t+3\right)_k \\
&\longrightarrow \left(a^{(2t+3)^2}, a^{(2t+3)^2}, 2t+3, 2t+3\right)_k.
\end{aligned}$$

Опять-таки, применимость следует из замечания.

E.9 Случай четного n полностью аналогичен этому случаю в предыдущей задаче.

Предположим, что $n = 2t+1$ и $k = a^2$, a четно. Если $n = 1$, то утверждение очевидно. Для $n \geq 3$, мы также используем индукцию по t, но нам надо сперва проверить случай $t = 1$. Мы проверим его при помощи **E.10**. По этой задаче найдется тор де Брейна типа $(a^5, a^3, 2, 2)$. Кроме того, анализ конструкции в **E.10** показывает, что сумма чисел в каждой строке делится на k. То есть мы можем применить **E.6** дважды, чтобы получить

$$(a^5, a^3, 2, 2)_k \quad \longrightarrow \quad (a^9, a^3, 2, 3)_k \quad \longrightarrow \quad (a^9, a^9, 3, 3)_k,$$

как и требовалось.

Шаг индукции доказывается в точности как в предыдущей задаче.

E.10 Как обычно, введем обозначения $k = 2st$, $R = 4st^2$, $S = 4s^3t^2$.

Шаг 1. Найдем s циклических последовательностей $L_1, L_2, \ldots, L_s$, каждая длины $R = k^2/s$, таких что любое двухбуквенное слово в алфавите X_k встречается как подслово ровно в одной из этих последовательностей. Это может быть сделано в точности как в шаге 1 из **E.4**, только тепрь нужно разбить все ребра на s групп $G_1, \ldots, G_s$, каждая из R ребер, так что эти группы дают сбалансированные сильно связные подграфы. Эйлеровы циклы в этих подграфах тогда дают искомые последовательности.

Мы снова разбиваем ребра $G(2, k)$ на k групп $M_i = \{(\ell, \ell + i) : \ell = 1, 2, \ldots, k\}$. В начале мы распределяем в G_i ребра групп M_{i-1} и M_{k-i}; из этого уже следует, что все подграфы будут сильно связны. Затем мы распределяем остальные группы поровну между G_i -ми. Это завершает построение.

Шаг 2. Теперь мы построим нужный тор. Каждый столбец будет содержать лишь одну из последовательностей $L_1, \ldots, L_s$, сдвинутую некоторым образом. Мы фиксируем начальный элемент каждой из последовательностей L_i; после чего можно говорить о сдвигах любых из них друг относительно друга.

Пусть $C = (c_1, \ldots, c_{s^2})$ - последовательность де Брейна ранга 2 над алфавитом X_s. Теперь заполним столбцы следующим образом. Пусть I - номер столбца, и i - его остаток по модулю s^2, так что $I = i + s^2 \cdot j$. Тогда этот столбец будет содержать L_{c_i}, и будет сдвинут на j относительно предыдущего столбца.

Рассмотрим столбцы с нулевого по S-й. Мы утверждаем, что любой квадратик 2×2 встречается в этих столбцах. Действительно, для любых двух индексов i, i' последовательность L_i будет следовать за $L_{i'}$ ровно R раз, и все эти относительные сдвиги будут различны; это доказывает наше утверждение.

Остается найти период нашей расстановки. Поскольку $S = Rs^2$, $S-$й столбец будет сдвинут относительно нулевого на $(0 + 1 + \cdots + (R-1)) \cdot s^2$. Если s четно, то это число делится на R, то есть мы получили тор с периодами R и S.

Предположим ,что s нечетно . Тогда, к сожалению, общий сдвиг делится только на $R/2$. Но в этом случае мы можем применить ту же модификацию, что и в **E.4**. А именно, в шаге 1 мы можем разбить одну из групп G_i (скажем, G_2) на две сбалансированные сильно связные половинки. Тогда соответствующая последовательность L_2 также может быть построена так, чтобы состоять из двух половинок, заканчивающихся на одну и ту же букву. Тогда можно применить тот же трюк, что и в **E.4**. Детали остаются читателю для проверки.

Примечание: Для решения этой задачи можно применить и другую конструкцию.

F Продолжение перечисления

F.1 Зафиксируем некоторое ребро, выходящее из v, и будем считать, что оно является первым в любом эйлеровом цикле. Рассмотрим произвольный эйлеров цикл C. Для каждой вершины $u \neq v$, отметим последнее ребро этого цикла, выходящее из u. Обозначим подграф из отмеченных рёбер через T.

Предположим, что в T нашелся неориентированный цикл ω; так как исходящая степень каждой вершины в T равна единице, ω также является ориентированным циклом. Возьмем в ω ребро e, которое встречается в C последним. Пусть $u = t(e)$; заметим, что $u \neq v$, ибо в графе T из v не выходит рёбер. Но тогда ребро f цикла ω, выходящее из u, должно встречаться в C позже; в противном случае при построении C после ребра e уже не получится выйти из u, а закончиться цикл должен в v. Это противоречие показывает, что T ацикличен. Значит, если пойти из любой вершины графа G по отмеченным ребрам, рано или поздно мы придём в вершину, из которой рёбер не идёт, а это может быть только v. Таким образом, T является ориентированным остовным деревом с корнем в v.

Итак, каждому эйлерову циклу C мы сопоставили ориентированное остовное дерево T; посчитаем, скольким циклам соответствует T. Оно соответствует тем эйлеровым циклам, которые, выйдя из v по фиксированному ребру, проходили по какому-то ребру дерева T только тогда, когда это ребро оставалось единственной возможностью продолжить обход; сейчас мы научимся восстанавливать все эти циклы.

В каждой вершине $u \neq v$ есть ровно $(outdeg(u)-1)!$ способов установить порядок, в котором цикл должен проходить по исходящие из u ребрам не из T (оставшееся ребро обязано быть последним). В вершине v есть ровно $(outdeg(v)-1)!$ способов установить порядок, в которым цикл должен проходить исходящие ребра после фиксированного. Покажем, что любому выбору этих порядков действительно соответствует эйлеров цикл.

Выйдем из v по фиксированному ребру и пойдем по ребрам, придерживаясь порядков во всех вершинах, пока не остановимся. Произойти это может только в вершине v; обозначим полученный цикл через C.. Предположим, что C не прошел по какому-то ребру из вершины u; тогда он не прошёл и по ребру e графа T, выходящему из u. Рассмотрев в T путь из u в v, мы найдём в T такие ребра e_1 и e_2, что $t(e_1) = s(e_2)$, а C прошел по e_2, но не по e_1. Но тогда все рёбра из $s(e_2)$ должны принадлежать C, однако ребро e_1, входящее в неё, не принадлежит C. Это противоречит сбалансированности G.

Таким образом, данному дереву соответствует ровно $\prod_{u \in V(G)} (outdeg(u)-1)!$ разных циклов, откуда и следует утверждение задачи.

Замечание. В качестве следствия мы немедленно получаем, что в сильно связном сбалансированном ориентированном графе число ориентированных остовных деревьев с данным корнем не зависит от выбора корня.

F.2 **Ответ.** $B(k,n) = k!^{k^{n-1}}/k^n$.

Из предыдущей задачи следует, что число $B(k,n)$ ровно в $(k-1)!^{k^{n-1}}$ раз больше числа ориентированных остовных деревьев с фиксированным корнем в графе де Брейна $G(k,n)$, то есть $B(k,n)$ в $\frac{(k-1)!^{k^{n-1}}}{k^{n-1}}$ раз больше общего числа $\tau(G(k,n))$ ориентированных остовных деревьев. Докажем индукцией по n, что $\tau(G(k,n)) = k^{k^{n-1}-1}$; отсюда немедленно воспоследует ответ.

База для $n = 1$ очевидна. Заметим, что $G(k,n+1) = \mathcal{L}G(k,n)$. Тогда, подставив в тождество Левина единицы вместо всех переменных, получим

$$\tau(G(k,n+1)) = \tau(G(k,n)) \cdot k^{(k-1)k^{n-1}},$$

откуда и следует переход индукции.

F.3 Доказательство приводится по статье H. Bidkhori, S. Kishore. A bijective proof of a theorem of Knuth. Combinatorics, Probability and Computing, vol. 20, is. 01, 2011, и картинки позаимствованы оттуда же.

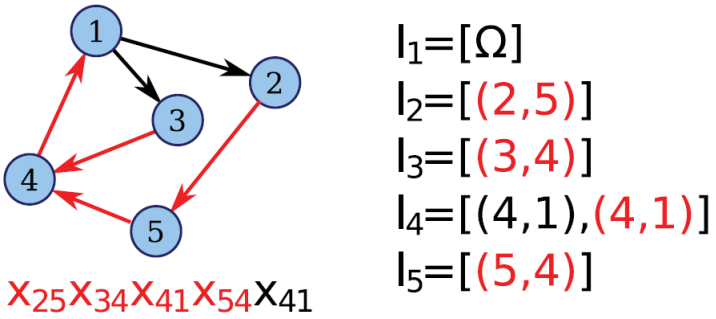
Раскроем все скобки в обеих частях предполагаемого равенства и докажем, что получаются одинаковые наборы мономов. Для этого нам потребуется следующее понятие.

Определение F.3 *Древесным массивом в графе G будем называть набор из упорядоченных списков ℓ_v для каждой вершины v, удовлетворяющий следующим условиям:*

а) Каждый список ℓ_v имеет длину $indeg(v)$. Все элементы этого списка — ребра, исходящие из v (возможно, с повторами), за исключением последнего элемента ровно одного из списков, соответствующего некоторой вершине v_0; этот элемент является символом Ω.

б) Последние элементы всех остальных списков образуют ориентированное остовное дерево с корнем в вершине v_0.

На рисунке ниже показан пример древесного массива.



Сопоставим каждому древесному массиву моном, в который каждая переменная x_e входит в такой степени, сколько раз ребро e содержится в массиве. Нетрудно видеть тогда, что древесные массивы в точности соответствуют мономам из правой части требуемого равенства (при этом массивы, в которых последние ребра списков образуют фиксированное дерево, соответствуют мономам, полученным из монома этого дерева из $\kappa^{edge}(G)$).

Таким образом, для доказательства нашего равенства достаточно построить биекцию между древесными массивами в G и остовными деревьми в $\mathcal{L}G$, при которой каждому дереву в $\kappa^{vertex}(\mathcal{L}G)$ соответствует тот же моном, который сопоставлен соответствующему ему древесному массиву. Пусть $\mathcal{A}$ — множество всех древесных массивов в G, а $\mathcal{T}$ — множество всех остовных ориентированных деревьев в $\mathcal{L}G$. Тогда мы собираемся построить алгоритмически взаимно-обратные отображения

$$\mathbf{\Sigma} : \mathcal{A} \to \mathcal{T} \qquad \text{и} \qquad \mathbf{\Pi} : \mathcal{T} \to \mathcal{A},$$

обладающие вышеуказанным свойством.

Пронумеруем все ребра G произвольным образом.

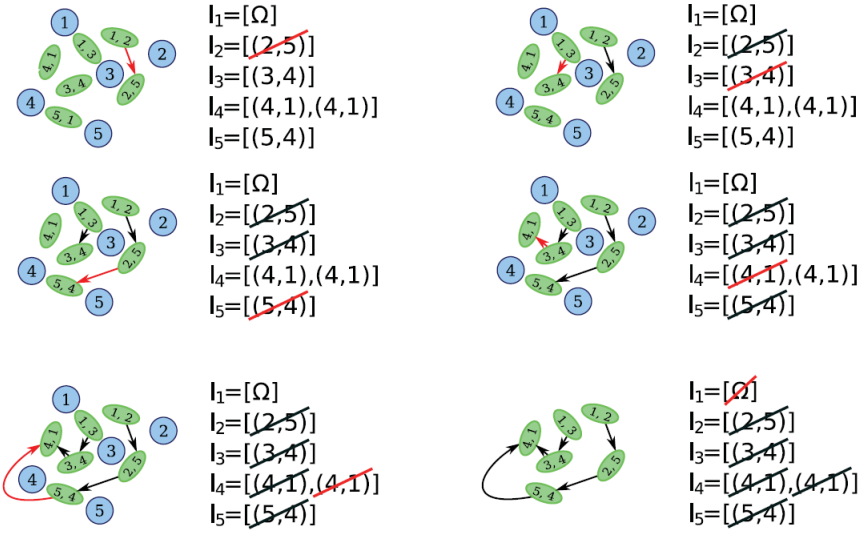
Построение $\mathbf{\Sigma}$. Рассмотрим массив $A \in \mathcal{A}$. Будем наращивать подграф T графа $\mathcal{L}G$ шаг за шагом, соответственно уменьшая A. Мы начнём с пустого T; когда A опустеет, определим $\mathbf{\Sigma}(A)$ как получившийся подграф T. Обозначим текущее состояние массива A и подграфа T после k-го шага через $A(k)$ и $T(k)$ соответственно.

На $(k+1)$-м шаге выберем ребро e с наименьшим номером, не входящее в $A(k)$ и имеющее нулевую исходящую степень в $T(k)$. Пусть g — первый элемент из списка $\ell_{t(e)}$ (в массиве $A(k)$). Определим $A(k+1)$, выкинув g из начала этого списка. Если $g = \Omega$, то закончим алгоритм, в противном случае добавим ребро $e \to g$ к графу $T(k)$, получая $T(k+1)$. На рисунке ниже показана работа этого процесса для того же древесного массива.

Пусть в G имеется d ребер. После k шагов найдутся k ребер, имеющих ненулевую исходящую степень в $T(k)$, а массив $A(k)$ будет содержать не более $d-1-k$ различных ребер. Значит, на $(k+1)$-м шаге можно будет выбрать искомое ребро e. При этом список $\ell_{t(e)}$ окажется не пустым, поскольку длина этого списка уменьшалась ровно тогда, когда использовалось входящее в $\ell_{t(e)}$ ребро, то есть не более, чем $indeg(t(e)) - 1$ раз.

Покажем, что в T нет ориентированных циклов. Действительно, если мы уже добавили к подграфу T рёбра $e_1 \to e_2, \ldots, e_{n-1} \to e_n$), то после этого добавить ребро $e_n \to e_1$) и замкнуть цикл нельзя, ибо уже в момент добавления ребра $e_1 \to e_2$ ребро e_1 отсутствовало в массиве.

Пусть теперь M — дерево в G, состоящее из последних ребер массива A, а r — его корень. Пусть $e = (u, w)$ — произвольное ребро в M (это ребро лежит в ℓ_u). Предположим, что в некоторый момент процесса



список ℓ_v опустел. Тогда в T уже есть рёбра, выходящие из всех рёбер графа G с концом в v; в частности, исходящая степень ребра e в графе T не равна нулю. Это значит, что оно было выбрано раньше, и в момент его выбора оно уже отсутствовало в A. Тогда в этот момент список ℓ_u был уже пуст. Итак, если список ℓ_v в какой-то момент опустел, то список ℓ_u опустел до этого.

Из этого следует, что в момент, когда опустеет список ℓ_r, все остальные списки должны быть уже пустыми. Значит, алгоритм закончится ровно через d шагов, и $T = \mathbf{\Sigma}(A)$ будет ориентированным остовным деревом. Несложно заметить, что получившееся дерево будет соответствовать тому же моному.

Построение $\mathbf{\Pi}$. Рассмотрим теперь ориентированное остовное дерево $S \in \mathcal{T}$ с корнем r. Начнем с пустого массива B и будем шаг за шагом увеличивать его, убирая ребра из S. Обозначим текущее состояние массива B и подграфа S через k шагов через $B(k)$ и $S(k)$ соответственно.

На k-м шаге рассмотрим все вершины в $S(k)$, исходящие степени которых равны 1, а входящие равны 0, и выберем среди них вершину e с наименьшим номером (напомним, что вершины $S(k)$ являются рёбрами в G). Пусть $e \to f$ — ребро графа $S(k)$, выходящее из e. Удалим это ребро из S и добавим f в конец списка $\ell_{t(e)}$. Когда в S не останется рёбер (что произойдёт через $d-1$ шагов), добавим Ω в конец списка $\ell_{t(r)}$.

Когда алгоритм прервется, длина каждого списка ℓ_v в B будет равна $indeg(v)$. Рассмотрим подграф M графа G, образованный последними ребрами всех списков. Пусть в нем есть ребро $f = (u, w)$, лежащее в ℓ_u. Покажем, что тогда список ℓ_v заполнился позже, чем список ℓ_u. Действительно, после заполнения списка ℓ_w вершина f графа S должна быть изолированной; значит, все рёбра, входящие в неё в исходном графе S, были уже обработаны раньше, а тогда и в списке ℓ_u вершина f появилась в последний раз раньше.

Отсюда следует, что в подграфе M не будет ориентированных циклов. Так как в нем из каждой вершины, кроме $t(r)$, исходит ровно одно ребро, M является ориентированным остовным деревом. Таким образом, B является древесным массивом, и мы полагаем $B = \mathbf{\Pi}(S)$.

Осталось показать, что алгоритмы, строящие $\mathbf{\Sigma}$ и $\mathbf{\Pi}$, дают взаимно обратные отображения. Пусть, например, $T = \mathbf{\Sigma}(A)$, и первые k шагов алгоритма, строящего $\mathbf{\Sigma}(\mathbf{A})$, удаляют из A ребра $f_1, \ldots, f_k$ и вставляют в T ребра $e_1 \to f_1)$, $\ldots$, $e_k \to f_k$ в таком порядке. Покажем индукцией по k, что первые k шагов алгоритма, строящего $B = \mathbf{\Pi}(\mathbf{T})$, вставляют в массив B ребра $f_1, \ldots, f_k$ и выкидывают из T ребра $e_1 \to f_1)$, $\ldots$, $e_k \to f_k)$ в таком же порядке.

База при $k = 0$ очевидна. Для перехода рассмотрим $(k+1)$-й шаг работы $\mathbf{\Pi}$. По предположению индукции, ребро $e_{k+1} \to f_{k+1}$ есть в подграфе $T(k)$. Далее, в $T(k)$ не может быть ребра вида $e \to e_{k+1}$, поскольку в противном случае оно было бы добавлено в T в процессе работы алгоритма $\mathbf{\Sigma}$ на шаге с номером $\ell > k+1$; но перед этим шагом в массиве $A(\ell - 1)$ уже не было ребра e_{k+1} — противоречие. Итак, e_{k+1} имеет в $T(k)$ нужные степени.

С другой стороны, если в $T(k)$ есть ребро $e \to e'$, и входящая степень e равна нулю, то номер e больше номера e_{k+1}; в противном случае мы должны были бы добавить в T ребро $e \to e'$ вместо $e_{k+1} \to f_{k+1}$ на $(k+1)$-м шаге работы $\mathbf{\Sigma}$. Таким образом, на $(k+1)$-м шаге работы $\mathbf{\Pi}$ мы действительно должны выкинуть из T ребро $e_{k+1} \to f_{k+1}$ и добавить в массив B ребро f_{k+1}.

Из доказанного утверждения следует, что $\mathbf{\Pi}(\mathbf{\Sigma}(A)) = A$ для всех $A \in \mathcal{A}$. Аналогично показывается, что $\mathbf{\Sigma}(\mathbf{\Pi}(T)) = T$ для любого $T \in \mathcal{T}$.

Примечание. Первоначальное доказательство Левина носило алгебраический характер и использовало технику работы с определителями.

G Последовательности де Брёйна через рекурренты

G.1 Доказательство утверждения этой задачи будет использовать алгебраическую технику, которая, возможно, неизвестна читателю. Если это так, то вы сможете впоследствии вернуться к нему, изучив соответствующие главы алгебры. Мы будем использовать некоторые классические алгебраические факты без доказательства.

Известно, что для любого n можно найти многочлен f степени n, неприводимый над полем F_2 из двух элементов; при этом остатки по модулю многочлена f образуют поле K из 2^n элементов. Для любого ненулевого элемента $u \in K$ выполнено равенство $u^{2^n-1} = 1$; более того, известно, что найдется такой ненулевой $\xi \in K$, что $\xi^t \neq 1$ для любого $0 < t < 2^n - 1$; тогда все ненулевые элементы поля K являются степенями элемента ξ.

Рассмотрим такой неприводимый многочлен g над F_2, что $g(\xi) = 0$. Тогда g делит многочлен $x^{2^n} - x$, все корни которого различны (это просто все элементы поля K). Значит, все корни g также различны и лежат в K. Его степень равна n, поскольку в $F_2(u)$ ровно 2^n элементов. Пусть $g = x^{k_1-1} + \cdots + x^{k_s-1} + x^n$, где $k_1 < k_2 < \cdots < k_s$. Определим шаблон, поставив символ X ровно в места с номерами $k_1, k_2, \ldots, k_s$.

Пусть $\xi = \xi_1, \xi_2, \ldots \xi_n$ — корни g. Система линейных уравнений

$$\begin{cases} x_1 + x_2 + \quad \cdots \quad + x_n &= 0 \\ \xi_1 x_1 + \xi_2 x_2 + \quad \cdots \quad + \xi_n x_n &= 0 \\ \qquad\qquad \vdots \qquad\qquad\qquad \vdots & \vdots \\ \xi_1^{n-2} x_1 + \xi_2^{n-2} x_2 + \cdots + \xi_n^{n-2} x_n &= 0 \\ \xi_1^{n-1} x_1 + \xi_2^{n-1} x_2 + \cdots + \xi_n^{n-1} x_n &= 1 \end{cases}$$

имеет единственное решение, поскольку определитель соответствующей матрицы не равен нулю как определитель Вандермонда. Нетрудно понять, что последовательность, заданная при помощи нашего шаблона, может быть определена про помощи формулы

$$a_k = x_1 \xi_1^k + \cdots + x_n \xi_n^k.$$

При $n > 1$ мы имеем $k_1 = 1$, поскольку g неприводим. Несложно видеть, что последовательность (a_k) будет периодична без предпериода, поскольку по любому ее куску длины n можно однозначно определить и следующий, и предыдущий куски. Если длина периода равна t, то из равенств $a_t = a_0$, $a_{t+1} = a_1, \ldots, a_{t+n-1} = a_{n-1}$ и единственности решения линейной системы получаем, что $x_1 \xi_1^t = x_1, \ldots, x_n \xi_n^t = x_n$. Поскольку хотя бы одно из x_i отлично от нуля, то $\xi_i^t = 1$. Значит, $t \geq 2^n - 1$, так как $F_2(\xi_i)$ изоморфно $F_2(u)$. С другой стороны, $t \leq 2^n - 1$, так как подпоследовательность из n нулей в нашей последовательности не встретится, а первое же повторение куска длины n приведет к периодичности.