Math-Net.Ru

Общероссийский математический портал

В. И. Арнольд, Перестановки, *УМН*, 2009, том 64, выпуск 4, 3–44

DOI: <https://doi.org/10.4213/rm9313>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 44.207.124.84

26 апреля 2023 г., 16:43:41

УДК 519.12+519.22+512.542.7+514.144

Перестановки

В. И. Арнольд

Разбиения на циклы для случайных перестановок большого числа элементов сильно отличаются (своей статистикой) от таких же разбиений для алгебраических перестановок (заданных линейными или проективными преобразованиями конечных множеств).

В статье приведены таблицы, доставляющие те и другие статистики, а также их сравнение со статистиками инволюций или перестановок, все циклы которых имеют четные длины. Принадлежности точки циклам разных длин оказываются равновероятными событиями для случайных перестановок. Числа всех перестановок N элементов, все циклы которых имеют четные длины, оказываются квадратами целых чисел (а именно, чисел $(2N - 1)!!$).

Числа циклов проективных перестановок (над полем из нечетного простого числа элементов) всегда четны — эти и другие эмпирически обнаруженные теоремы в статье доказаны.

Библиография: 6 названий.

Ключевые слова: диаграммы Юнга, циклы, симметрическая группа, модулярная группа, проективная геометрия, статистика, инволюции, случайность.

СОДЕРЖАНИЕ

§ 1. Диаграммы Юнга циклов.....	3
§ 2. Статистика циклов случайных перестановок N точек.....	12
§ 3. Перестановки с циклами четной длины.....	14
§ 4. Проективные перестановки.....	24
§ 5. Перестановки фиксированного порядка и статистика инволюций.....	38
§ 6. Степень хаотичности распределения длин циклов случайных перестановок.....	40
Список литературы.....	43

§ 1. Диаграммы Юнга циклов

Перестановкой (конечного множества M) называется взаимно однозначное отображение $A: M \rightarrow M$ множества на себя.

Перестановки множества из N точек образуют симметрическую группу $S(N)$, состоящую из $N!$ элементов.

Каждая перестановка однозначно разбивается на свои *циклы*. Цикл $C \subset M$ длины a перестановки A состоит из a циклически переставляемых перестановкой A точек.

ПРИМЕР. Для “конечной окружности”

$$C = \mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$$

можно задать циклическую перестановку, например, формулой

$$A(c) = c + 1 \quad \forall c \in C.$$

Но есть и другие циклические перестановки той же конечной окружности C : их число равно $(N - 1)!$.

Разные циклы перестановки $A: M \rightarrow M$ не пересекаются, так что все множество M однозначно разбивается на циклы. Если число циклов равно y , то

$$M = C_1 \amalg C_2 \amalg \cdots \amalg C_y.$$

Мы упорядочим циклы по убыванию длин,

$$a_1 \geq a_2 \geq \cdots \geq a_y.$$

Возникающее разбиение

$$N = a_1 + a_2 + \cdots + a_y$$

числа N на натуральные слагаемые описывается *диаграммой Юнга циклов перестановки*.

Эта диаграмма состоит из N единичных квадратов, примыкающих друг к другу на плоскости: a_1 квадратов составляют первую строку, a_2 – вторую, и так до самой короткой последней строки из a_y квадратов.

ПРИМЕР. Перестановка $N = 6$ цифр

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 5 & 4 & 3 \end{array}$$

имеет диаграмму Юнга из $y = 3$ строк:

$$\begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & \square & \\ \hline \square & & \\ \hline \end{array} \quad \begin{array}{ll} C_1 = \{1, 6, 3\}, & a_1 = 3, \\ C_2 = \{4, 5\}, & a_2 = 2, \\ C_3 = \{2\}, & a_3 = 1. \end{array}$$

Настоящая статья посвящена статистике диаграмм Юнга циклов перестановок различного происхождения. Например, много неожиданного содержит уже статистика диаграмм Юнга циклов совершенно случайных перестановок N точек (в которой все $N!$ перестановок этих точек считаются равновероятными).

В качестве другого примера рассмотрим действие на конечном торе $\mathbb{Z}_n^2$ модулярной группы матриц

$$\mathrm{SL}(2, \mathbb{Z}_n)$$

второго порядка с определителем 1, элементами которой являются остатки от деления на n .

Конечный тор $\mathbb{Z}_n^2$ состоит из $N = n^2$ точек, и матрицы указанной группы переставляют эти точки (пример действия матрицы Фибоначчи $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ рассмотрен в статье [1], а другие подобные примеры – в [2] и в [3], [4]).

Мы рассмотрим также действие этой группы на “проективизированном конечном торе”, который определяется следующей конструкцией.

Точками проективизированного тора

$$P_n = P(\mathbb{Z}_n^2)$$

являются прямые, проходящие через начало координат на торе $\mathbb{Z}_n^2$.

Мы исследуем этот проективизированный тор при любом n ниже (§ 4, с. 24–27), но если число $n = p$ простое, то он состоит из $p + 1$ точки: соответствующие прямые задаются уравнениями вида

$$y = kx \quad (k = 0, 1, \dots, p-1, \infty)$$

(где значению $k = \infty$ соответствует вертикальная прямая $x = 0$).

Модулярная группа переставляет указанные прямые, так что ее матрицы определяют перестановки конечного множества P_n из $N(n)$ элементов (где $N(p) = p + 1$).

Когда $n = p$ – простое число, модулярная группа $\text{SL}(2, \mathbb{Z}_n)$ состоит из $p(p^2 - 1)$ матриц. На множестве P_n лучше действовать проективизированной версией этой группы,

$$\text{PSL}(2, \mathbb{Z}_n) = \text{SL}(2, \mathbb{Z}_n) / E_n,$$

где E_n – подгруппа скалярных матриц. Во многих случаях E_n состоит из 2 элементов, $E_n = \{\pm 1\}$, и тогда число элементов проективизированной группы (скажем, для нечетных простых $n = p$) есть $|\text{PSL}(2, \mathbb{Z}_p)| = p(p^2 - 1)/2$.

Как мы увидим, статистики диаграмм Юнга циклов $N!$ случайных перестановок N точек и получающихся $p(p^2 - 1)/|E_p|$ “проективных перестановок” $N(p)$ точек проективизированного тора P_n совершенно различны. Например, циклы типичной проективной перестановки обычно в несколько раз короче циклов типичной случайной перестановки тех же точек.

В качестве других примеров перестановок поучительны действия симметрий различных (правильных!) многогранников на конечные множества их вершин, граней, ребер, диагоналей и т. п. Удивительным образом, некоторые из этих геометрических объектов (включая, например, кубы Кеплера, вписанные им в додекаэдр) доставляют не простые ответы на алгебраические вопросы о действиях модулярной группы проективными перестановками множества P_n .

Другие поучительные примеры различающихся статистик доставляют другие множества перестановок, уже не обязательно образующие группы. Например, замечательными оказываются статистические свойства диаграмм Юнга инволюций решений уравнения $A^2 = 1$ на перестановку A , а также статистические свойства таких перестановок, все циклы которых имеют четные длины:

$$a_1 = 2b_1, \quad \dots, \quad a_y = 2b_y.$$

Многочисленные экспериментальные исследования в этом направлении привели меня к целому ряду неожиданных наблюдений, из которых я опишу в этом введении лишь некоторые.

ТЕОРЕМА 1. Числа m_s циклов разных длин s у всех $N!$ перестановок N точек составляют гармоническую последовательность делителей числа $N!$:

s	1	2	3	...	N
m_s	$N!$	$N!/2$	$N!/3$	...	$(N-1)!$

Эта теорема означает, что произведение $sm_s = N!$ не зависит от длины s цикла, так что включения любой точки множества из N элементов в цикл любой длины от 1 до s равновероятны.

ТЕОРЕМА 2. Среднее арифметическое $\hat{y}$ чисел циклов, $y(A)$, всех $N!$ перестановок A N точек составляет сумму N членов гармонического ряда:

$$\hat{y} = 1 + \frac{1}{2} + \dots + \frac{1}{N}.$$

ПРИМЕР. При $N \leq 8$ эти средние примерно таковы:

N	3	4	5	6	7	8
$\hat{y}$	1.83	2.08	2.28	2.45	2.59	2.72
$\gamma + \ln N$	1.68	1.96	2.19	2.37	2.51	2.65

ЗАМЕЧАНИЕ. Из теоремы 2 легко вытекает приближенная формула (погрешность которой стремится к 0 при $N \rightarrow \infty$):

$$\hat{y} \approx \gamma + \ln N,$$

где γ – постоянная Эйлера,

$$\gamma \approx 0.5772156649 \dots$$

ТЕОРЕМА 3. Число $Q_2(n)$ тех перестановок множества из $N = 2n$ точек, у которых длины всех циклов четны, является квадратом целого числа:

N	2	4	6	8	10
Q_2	1	9	225	11025	893025

а именно

$$Q_2(n) = ((2n-1)!!)^2 \quad (\text{где } m!! = m(m-2)(m-4)\dots).$$

Обратимся теперь к проективным перестановкам множества $P(n)$ (точками которого являются $N(n)$ прямых, проходящих через точку O конечной плоскости $\mathbb{Z}_n^2$). Эти проективные перестановки осуществляются действием на этой плоскости конечной модулярной группы $SL(2, \mathbb{Z}_n)$ (или действием на $P(n)$ ее проективизированной версии $PSL(2, \mathbb{Z}_n)$).

ТЕОРЕМА 4. Если $n = p$ – нечетное простое число, то каждая проективная перестановка ($N(n) = p+1$ точки множества $P(n)$) состоит из четного числа циклов.

ПРИМЕР. Для $p = 5$ (когда $N = 6$) проективизированная группа $\text{PSL}(2, \mathbb{Z}_5)$ состоит из $p(p^2 - 1)/2 = 60$ элементов. Она изоморфна группе вращений додекаэдра (а также группе $S^+(5)$ четных перестановок пяти кубов Кеплера, вписанных в него).

Двенадцать граней додекаэдра составляют 6 пар противоположных граней, центры обеих граней пары соединяет ось симметрии додекаэдра (пятого порядка).

Действие модулярной группы на множестве $P(5)$, состоящем из $N(5) = 6$ прямых конечного тора $\mathbb{Z}_5^2$, изоморфно представлению группы вращений додекаэдра перестановками его 6 осей симметрии (пятого порядка).

Диаграммы Юнга циклов 60 проективных перестановок множества $P(5)$ поэтому таковы (их четыре):

$$(6) = 5 + 1 = 3 + 3 = 2 + 2 + 1 + 1 = 1 + 1 + 1 + 1 + 1 + 1.$$

Все они имеют четные высоты $(2, 2, 4, 6)$, как и утверждает теорема 4.

Для $p = 7$ (когда $N = 8$) таким же образом получаются следующие пять диаграмм Юнга циклов (проективных перестановок 8 прямых):

$$(8) = 7 + 1 = 4 + 4 = 3 + 3 + 1 + 1 = 2 + 2 + 2 + 2 = 1 + \dots + 1.$$

Для $p = 2$ (когда число прямых есть $N(2) = 3$) группа $\text{PSL}(2, \mathbb{Z}_2) \approx S(3)$ состоит из всех симметрий треугольника, с тремя диаграммами Юнга

$$(3) = 3 = 2 + 1 = 1 + 1 + 1,$$

так что встречаются и нечетные числа циклов.

Для $n = 9$ число прямых составляет $N(9) = 12$. Проективные перестановки этих двенадцати прямых состоят, каждая, из четного числа циклов (являясь, к тому же, четной перестановкой этих 12 прямых, как и для нечетных простых значений n).

К сожалению, я не нашел ни соответствующего группе $\text{PSL}(2, \mathbb{Z}_9)$ правильного многогранника, ни (напрашивающегося) описания проективных перестановок, возникающих при действии “модулярных групп” $\text{PSL}(2, \mathbb{Z}_{p^\alpha})$ на множествах прямых в $\mathbb{Z}_{p^\alpha}^2$ в терминах проективной геометрии полей Галуа из p^α элементов.

Для описания статистик диаграмм Юнга циклов перестановок N элементов введем следующие характеристики этих перестановок:

- x – “длина диаграммы”, т. е. длина a_1 наибольшего цикла перестановки;
- y – “высота диаграммы”, т. е. число циклов перестановки;
- $\lambda = N/(xy)$ – “полнота диаграммы”, т. е. доля площади описанного прямоугольника, занятой диаграммой;
- $\mu = y/x$ – “асимметрия диаграммы”, отличающая высокие диаграммы (у которых $\mu > 1$) от длинных (у которых $\mu < 1$);
- T – период перестановки A (это наименьшее общее кратное длин ее циклов, т. е. наименьший период, для которого $A^T = 1$).

Между прочим, статистика параметров диаграмм Юнга циклов тех перестановок, для которых данное число T является периодом (т. е. все длины циклов

которых являются делителями фиксированного числа T), – тоже интересная задача, так как, например, проективные перестановки всегда удовлетворяют соотношениям типа Ферма–Эйлера для геометрических прогрессий модулярных матриц, $A^T = 1$, где $A \in \text{SL}(k, \mathbb{Z}_r)$.

Рассматривая какую-либо совокупность S перестановок (например, группу $S(N)$ или ее подмножество всех перестановок, все длины циклов которых четны), мы обозначаем через $\hat{f}$ среднее арифметическое значение параметров f диаграммы Юнга циклов перестановок A по совокупности S :

$$\hat{f} = \frac{1}{|S|} \sum_{A \in S} f(A)$$

(где $|S|$ есть число элементов в S , например, $|S(N)| = N!$, $|\text{SL}(2, p)| = p(p^2 - 1)$).

ТЕОРЕМА 5. *Средние значения характеристик диаграмм Юнга циклов по всем $N!$ перестановкам $N \leq 8$ точек таковы:*

N	3	4	5	6	7	8
$\hat{x}$	1.67	2.79	3.42	4.00	6.68	5.30
$\hat{y}$	1.83	2.08	2.28	2.45	2.59	2.72
$\hat{\lambda}$	0.87	0.83	0.75	0.70	0.78	0.67
$\hat{\mu}$	1.11	0.95	0.80	0.68	0.69	0.66
$\hat{T}$	1.67	2.79	3.92	4.54	6.20	7.42
$\hat{a}$	1.64	1.92	2.19	2.45	2.69	2.94
c	11	50	274	1 764	13 068	109 584

Здесь $\hat{a}$ – средняя длина циклов,

$$\hat{a} = \frac{N! N}{N! \hat{y}}$$

(сумма длин всех циклов всех $N!$ перестановок из группы $S(N)$ составляет $N \cdot N!$, а суммарное число c циклов всех $N!$ перестановок связано со средним числом $\hat{y}$ циклов в каждой из $N!$ перестановок соотношением $c = N! \hat{y}$).

ЗАМЕЧАНИЕ. Приведенная таблица позволяет предсказать многие (гипотетические) асимптотики, например, линейный в среднем рост с числом представляемых точек N и длины наибольшего цикла $\hat{x}$, и средней длины цикла, $\hat{a}$, и средней продолжительности $\hat{T}$ периода:

$$\begin{aligned} \hat{x} &\sim \alpha_1 N, & \alpha_1 &\approx \frac{5.30}{8} = 0.66, \\ \hat{a} &\sim \alpha_2 N, & \alpha_2 &\approx \frac{2.94}{8} = 0.37, \\ \hat{T} &\sim \alpha_3 N, & \alpha_3 &\approx \frac{7.48}{8} = 0.93. \end{aligned}$$

Но эти гипотезы не входят в формулировку теоремы 5.

Указанную в теореме 2 асимптотику высоты диаграммы $\hat{y}$ было бы трудно угадать из таблицы теоремы 5, так же как и соответствующие этому поведению $\hat{y}$ гипотезы $\hat{\lambda} \sim \alpha_4 / \ln N$, $\hat{\mu} \sim \alpha_5 (\ln N) / N$.

Рассмотрим теперь “проективные перестановки” $N(n)$ прямых конечной плоскости $\mathbb{Z}_n^2$ (проходящих через 0) действием “модулярной” группы $\text{SL}(2, \mathbb{Z}_n)$ (или, лучше, ее проективной версии $\text{PSL}(2, \mathbb{Z}_n)$). Обозначим через $Q(n)$ число элементов этой группы.

ТЕОРЕМА 6. *Средние значения характеристик диаграмм Юнга этих “проективных перестановок” N элементов даются при $n \leq 8$ следующей таблицей:*

n	2	3	4	5	6	7	8
N	3	4	6	6	12	8	12
$\hat{x}$	1.67	2.58	2.79	3.51	4.01	4.25	4.32
$\hat{y}$	1.83	2.17	2.92	2.57	4.67	2.95	4.58
$\hat{\lambda}$	0.87	0.77	0.84	0.75	0.78	0.77	0.76
$\hat{\mu}$	1.11	1.08	1.28	1.00	1.64	0.91	1.47
$\hat{T}$	1.67	2.58	2.79	3.51	4.01	4.25	4.32
$\hat{a}$	1.64	1.85	2.06	2.34	2.57	2.71	2.62
c	11	26	70	154	336	496	440
Q	6	12	24	60	72	168	96

Как и в случае полностью случайных перестановок, для случайных матриц рассматриваемые средние значения параметров $\hat{x}$, $\hat{a}$, $\hat{T}$ диаграмм Юнга циклов тоже приблизительно линейно растут с числом N переставляемых объектов,

$$\begin{aligned}\hat{x} &\sim \alpha'_1 N, & \alpha'_1 &\approx 0.36, \\ \hat{a} &\sim \alpha'_2 N, & \alpha'_2 &\approx 0.22, \\ \hat{T} &\sim \alpha'_3 N, & \alpha'_3 &\approx 0.36.\end{aligned}$$

Как видно, и длины циклов этих проективных перестановок, и их периоды раза в 2–3 меньше, чем если бы перестановки были случайными.

Вероятно, этот эффект станет еще заметнее при больших значениях параметра n рассматриваемой теории действия групп $\text{SL}(2, \mathbb{Z}_n)$, когда число прямых $N(n)$ станет гораздо большим, чем n .

А именно, из рассуждений, которыми Эйлер вывел свою мультипликативную формулу для дзета-функции, видно, что

$$N(n) = n \prod_p \left(1 + \frac{1}{p}\right),$$

где произведение берется по простым делителям числа n :

n	6	210	2 310
N	12	576	6 912

Число $N(n)$ превосходит некоторые числа n во сколько угодно раз (это следует из рассуждения, которым Эйлер доказывал бесконечность числа простых чисел).

Распределения диаграмм Юнга циклов перестановок по параметрам длины x и высоты y тоже сильно различаются для статистик по всем $N!$ перестановкам N точек и для проективных перестановок (индуцированных действием модулярной группы $SL(2, \mathbb{Z}_n)$ на прямые конечной плоскости $\mathbb{Z}_n^2$, проходящие через точку O).

Вот как выглядят эти распределения для симметрической группы $S(N)$ (при $N \leq 8$).

ТЕОРЕМА 7. Числа $\mathcal{F}_{x,y}$ тех перестановок N точек, диаграммы Юнга циклов которых имеют длину x и высоту y , даются при $N \leq 8$ следующими таблицами:

$x \uparrow$				
3	2			
2		3		
1			1	
	1	2	3	$y \rightarrow$

$N = 3$

$x \uparrow$					
4	6				
3		8			
2		3	6		
1				1	
	1	2	3	4	$y \rightarrow$

$N = 4$

$x \uparrow$						
5	24					
4		30				
3		20	20			
2			15	10		
1					1	
	1	2	3	4	5	$y \rightarrow$

$N = 5$

$x \uparrow$							
6	120						
5		144					
4		90	90				
3		40	120	40			
2			15	45	15		
1						1	
	1	2	3	4	5	6	$y \rightarrow$

$N = 6$

$x \uparrow$								
7	720							
6		840						
5		504	504					
4		420	630	210				
3			490	420	70			
2				105	105	21		
1							1	
	1	2	3	4	5	6	7	$y \rightarrow$

$N = 7$

$x \uparrow$									
8	5040								
7		5760							
6		3360	3360						
5		2688	4032	1344					
4		1260	4620	2520	420				
3			1120	2800	1120	112			
2				105	420	210	28		
1								1	
	1	2	3	4	5	6	7	8	y

$N = 8$

Проекции этих двумерных распределений на оси x и y доставляют (вовсе не очевидные) распределения $N!$ случайных перестановок N элементов по числу циклов (y) и по длине наибольшего цикла (x). А именно, из теоремы 7 вытекает

СЛЕДСТВИЕ. Распределения $N!$ перестановок N элементов по числам y циклов в перестановках и по длинам x наибольших циклов доставляются (для $N \leq 8$) следующими таблицами (в которых $\#$ означает “число перестановок”).

§ 2. Статистика циклов случайных перестановок N точек

Зафиксируем какой-либо цикл длины s перестановки N точек (которые мы будем обозначать символами $1, 2, \dots, N$).

Сосчитаем, сколько таких циклов имеется у всех $N!$ перестановок наших N точек. Назовем цикл *отмеченным*, если в нем выбран “начальный элемент” (как угодно). Мы сосчитаем число разных отмеченных циклов – чтобы получить просто число разных циклов, надо разделить полученный ответ на изучаемую длину циклов, s (так как цикл длины s можно отметить s способами).

Чтобы выбрать отмеченный цикл, надо выбрать подряд s различных точек из N возможных. Начальную точку можно выбрать N способами, сле-

дующую $- N - 1$ способом, и так далее: способов выбрать отмеченный цикл имеется

$$A(N, s) = N(N - 1) \cdots (N - s + 1) = N! / (N - s)!.$$

Чтобы этот цикл вошел в какую-либо определенную из $N!$ перестановок N точек, надо указать еще перестановку остальных $N - s$ точек. Таких перестановок имеется ровно $(N - s)!$ штук.

Следовательно, среди всех $N!$ перестановок N точек указанный отмеченный цикл встретится

$$A(N, s) \cdot (N - s)! = N!$$

раз.

Итак, в набор всех циклов всех $N!$ перестановок N точек входит ровно $N!/s$ циклов длины s (поскольку разных отмеченных циклов длины s там ровно $N!$ штук, а каждый цикл длины s отмечен s способами).

Теорема 1 доказана.

ПРИМЕР. При $N = 4$ двадцать четыре элемента симметрической группы $S(4)$ распределены по диаграммам Юнга циклов так:

I: (6 циклических перестановок из одного цикла длины 4).

II: (8 перестановок с неподвижной точкой и циклом длины 3: их 8 потому, что неподвижная точка может быть любой из четырех, а оставшиеся 3 можно упорядочить циклически двумя разными способами).

III: (таких перестановок из двух циклов длины 2 имеется 3, так как перестановка задается выбором одного из циклов, $C_4^2 = 6$, но, поскольку оба цикла можно поменять местами, эти 6 выборов дают лишь три разных инволюции).

IV: (таких перестановок с двумя неподвижными точками имеется 6, так как $C_4^2 = 6$).

Добавляя еще тождественное преобразование V (с четырьмя циклами длины 1), мы получим все 24 перестановки четырех элементов:

$$6 + 8 + 3 + 6 + 1 = 24.$$

(Полезно также истолковывать группу $S(4)$ как группу всех 24 вращений куба в себя: они произвольно переставляют его 4 большие диагонали.)

Сосчитаем теперь, сколько циклов разных длин имеют все наши 24 перестановки. В следующей таблице для каждой диаграммы Юнга I–V указаны числа $\sharp$ перестановок с такой диаграммой циклов и числа $\sharp_s$ циклов длины s в каждой из этих перестановок:

	$\sharp$	$\sharp_1$ ($\sharp\sharp_1$)	$\sharp_2$ ($\sharp\sharp_2$)	$\sharp_3$ ($\sharp\sharp_3$)	$\sharp_4$ ($\sharp\sharp_4$)
I	6	0 0	0 0	0 0	1 6
II	8	1 8	0 0	1 8	0 0
III	3	0 0	2 6	0 0	0 0
IV	6	2 12	1 6	0 0	0 0
V	1	4 4	0 0	0 0	0 0
Σ_s	24	24	12	8	6

В графе $\sharp\sharp_s$ указано число циклов длины s во всех $\sharp$ перестановках с указанной диаграммой Юнга $\mathscr{D}$, а в строке Σ_s – общее число этих циклов длины s :

$$\Sigma_s = \sum_{\mathscr{D}} (\sharp\sharp_s).$$

Таблица подтверждает теорему 1:

$$12 = \frac{24}{2}, \quad 8 = \frac{24}{3}, \quad 6 = \frac{24}{4}, \quad \sum_{\mathscr{D}} (\sharp\sharp_s) = \frac{N!}{s}.$$

Из доказанной теоремы получается сразу же средняя длина $\hat{a}$ цикла случайной перестановки N точек: сумма длин всех циклов всех $N!$ перестановок составляет $N \cdot N!$, а число этих циклов составляет $c = N!(1 + 1/2 + \dots + 1/N)$. (В нашем примере это $c = 50$).

Поэтому средняя длина цикла есть

$$\hat{a} = \frac{NN!}{c} = \frac{N}{1 + 1/2 + \dots + 1/N} \approx \frac{N}{\gamma + \ln N}$$

(в нашем примере $\hat{a} = \frac{4 \cdot 24}{50} = 1.92$ – это часть теоремы 5).

С другой стороны, среднее число циклов перестановки N точек есть

$$\hat{y} = \frac{c}{N!} = 1 + \frac{1}{2} + \dots + \frac{1}{N} \approx \gamma + \ln N$$

(в нашем примере $\hat{y} = \frac{50}{24} \approx 2.08$).

ЗАМЕЧАНИЕ. Интересно, что для других статистик (например, для проективных перестановок или для перестановок с циклами четной длины) равновероятность циклов разной длины вовсе не наблюдается: эти перестановки далеко не случайны, например, у проективных перестановок более длинные циклы встречаются реже, а более короткие – чаще, чем указывает доказанная теорема.

§ 3. Перестановки с циклами четной длины

Здесь доказывается теорема 3 (которая открыта была не из тех общих соображений, на которых основано это доказательство, а при анализе эмпирических результатов в другой области).

ЛЕММА. Число $I(n)$ различных инволюций без неподвижных точек на множестве из $N = 2n$ точек составляет $(2n - 1)!!$.

ДОКАЗАТЕЛЬСТВО. Будем обозначать наши точки символами $(1, 2, \dots, 2n)$. Инволюция σ переводит точку 1 в одну из $2n - 1$ остальных точек, притом любую.

Выкинем из наших $2n$ точек пару точек $(1, \sigma(1))$. На оставшихся $2n - 2$ точках инволюция σ действует, причем по-прежнему – без неподвижных точек. Следовательно, $I(n) = (2n - 1)I(n - 1)$, что и дает требуемый результат:

$$I(n) = (2n - 1)I(n - 1) = (2n - 1)(2n - 3)I(n - 2) = \dots$$

ЗАМЕЧАНИЕ. Другой способ посчитать число инволюций без неподвижных точек таков. Все такие инволюции разбиваются на орбиты, состоящие каждая из 2 точек, а потому являются сопряженными друг другу элементами симметрической группы $S(2n)$.

Будем сопрягать какую-нибудь одну такую инволюцию σ при помощи всех перестановок $A \in S(2n)$, т. е. по-разному перенумеровывая $2n$ точек:

$$\sigma' = A\sigma A^{-1}.$$

При разных выборах перенумерации (сопрягающего элемента A) будут, вообще говоря, получаться разные инволюции σ' . Но иногда $\sigma' = \sigma$ (тогда перестановка A является *симметрией* инволюции σ). Все симметрии данной инволюции σ образуют *стационарную группу* $H_\sigma \subset S(2n)$ инволюции σ . Их легко описать: симметрия произвольно переставляет n двухточечных орбит (“диполей”) инволюции σ , а каждую из этих орбит отправляет на новое место одним из двух способов (отличающихся переворачиванием этой диагональной орбиты). Итого стационарная группа H_σ состоит из

$$|H_\sigma| = 2^n n!$$

очевидных симметрий инволюции σ .

Все разные инволюции без неподвижных точек на нашем $2n$ -точечном множестве – это разные классы смежности симметрической группы $S(2n)$ по подгруппе H_σ . Поэтому их число равно

$$\frac{|S(2n)|}{|H_\sigma|} = \frac{(2n)!}{2^n n!}.$$

Заметим теперь, что $(2n)! = (2n)!! (2n - 1)!!$ и что $(2n)!! = 2 \cdot n \cdot 2 \cdot (n - 1) \cdot 2 \cdot (n - 2) \cdot \dots = 2^n \cdot n!$. Поэтому $|H_\sigma| = (2n)!!$, а число разных инволюций $2n$ -точечного множества без неподвижных точек составляет

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

ЗАМЕЧАНИЕ. Нам будет в дальнейшем полезно следующее обобщение предыдущего рассуждения.

Рассмотрим вместо инволюции σ какую-либо произвольную перестановку $\sigma \in S(N)$ множества из N точек, с диаграммой Юнга циклов

$$a_1 \geq a_2 \geq \dots \geq a_y, \quad N = a_1 + a_2 + \dots + a_y.$$

Стационарная группа перестановки σ (при действии симметрической группы $S(N)$ сопряжениями) легко может быть описана следующим образом.

Каждая симметрия, сохраняющая перестановку σ , должна переводить любой из циклов (любой длины s) перестановки σ в другой ее цикл такой же длины s , причем эта перестановка всех ρ_s циклов длины s произвольна.

Если же место образа цикла фиксировано, то отображение симметрии должно сохранять циклический порядок внутри цикла, т. е. должно просто сдвигать этот цикл вдоль себя (на любое расстояние из s возможных).

Итого *стационарная группа перестановки σ имеет порядок*

$$|H_\sigma| = \left(\prod a_i \right) \left(\prod (\rho_j!) \right),$$

где a_i – длины строк диаграммы Юнга перестановки σ , а ρ_j – числа повторений одной и той же длины строки (индекс j нумерует разные длины).

ПРИМЕР. Для инволюции без неподвижных точек длины строк имеют вид $a_1 = a_2 = \dots = a_n = 2$, поэтому $a_i = 2$, $\prod a_i = 2^n$ и $\rho_1 = n$, поэтому $\prod (\rho_j!) = n!$.

СЛЕДСТВИЕ. Число $I(\sigma)$ перестановок N точек с такой же, как у данной перестановки σ , диаграммой Юнга (со строками длин a_i , повторяющимися ρ_j раз) составляет

$$I(\sigma) = \frac{N!}{\left(\prod a_i \right) \left(\prod (\rho_j!) \right)}.$$

Вернемся теперь к перестановке A , имеющей только циклы четной длины. Чтобы подсчитать число таких перестановок, я сопоставлю ей пару инволюций без неподвижных точек.

Вот как определяется эта пара. Рассмотрим какой-либо цикл $x_1 \rightarrow x_2 \rightarrow \dots \rightarrow x_{2a} \rightarrow x_1$ четной длины для нашей перестановки. Мы построим по нему следующую пару инволюций (на $2a$ точках этого цикла):

I: $x_1 \leftrightarrow x_2, x_3 \leftrightarrow x_4, \dots, x_{2a-1} \leftrightarrow x_{2a}$;

II: $x_2 \leftrightarrow x_3, x_4 \leftrightarrow x_5, \dots, x_{2a} \leftrightarrow x_1$.

Чтобы эта конструкция была точной, надо выбрать “первый элемент” цикла. С этой целью занумеруем (произвольным образом) все наши $N = 2n$ точек номерами от 1 до $2n$. Тогда в изучаемом цикле существует элемент с наименьшим номером (в этой нумерации). Его и назовем начальным элементом x_1 .

Теперь обе инволюции без неподвижных точек, I и II, определены на нашем цикле. А так как то же можно сделать и сразу на всех циклах, то эти инволюции I и II без неподвижных точек однозначно определены нашей перестановкой $N = 2n$ точек всюду.

Докажем теперь, что построенное отображение

$$(I, II): X \rightarrow (Y \times Y)$$

отображает множество $X \subset S(2n)$ перестановок, все циклы которых имеют четные длины, на декартов квадрат множества $Y \subset S(2n)$ всех инволюций без неподвижных точек взаимно однозначно.

Действительно, пусть σ и τ – две такие инволюции.

Рассмотрим перестановки $P = \tau\sigma$ и $Q = \sigma\tau$. Они имеют циклы. Рассмотрим цикл перестановки P , начинающийся в точке x :

$$x, P(x), P^2(x), \dots, P^t(x) = x.$$

Обозначим через y точку σx .

ЛЕММА. Эта точка не может принадлежать построенному циклу.

Действительно, если бы $\sigma(x) = P^\alpha(x)$, то мы имели бы

$$\sigma(x) = (\tau\sigma\tau\sigma \cdots \sigma\tau)\sigma(x),$$

где число $2k + 1$ инволюций σ и τ , заключенных в скобки в правой части, нечетно. Поэтому мы можем записать это равенство в виде

$$\sigma x = B\rho C\sigma(x),$$

где $B = \tau\sigma\tau\sigma \cdots$ – произведение первых k , а $C = \cdots \sigma\tau$ – последних k инволюций произведения, а ρ – средняя инволюция (либо σ , либо τ).

Из соотношений $\sigma^2 = \tau^2 = 1$ следует, что $B^{-1} = (\tau\sigma \cdots)^{-1} = (\cdots \sigma\tau) = C$. Поэтому из $\sigma(x) = B\rho C(\sigma(x))$ следует, что

$$C(\sigma(x)) = \rho C(\sigma(x)).$$

Значит, если бы точка y принадлежала циклу $\{P^\alpha(x)\}$, то инволюция ρ (т. е. σ или τ) имела бы неподвижную точку $C(\sigma(x))$. Лемма доказана.

Из соотношения

$$Q(y) = \sigma\tau(y) = \sigma\tau\sigma(x) = \sigma(P(x))$$

видно, что преобразование σ переводит движение P цикла $\{P^\alpha(x)\}$ в движение Q цикла $\{Q^\alpha(y)\}$.

Точно так же

$$\tau Q(y) = \tau\sigma\tau(y) = P\tau(y),$$

поэтому преобразование τ переводит движение Q цикла $\{Q^\alpha(y)\}$ обратно в движение P цикла $\{P^\alpha(x)\}$.

При этом оба цикла одинаковой длины t $\{P^\alpha(x)\}$ и $\{Q^\alpha(y)\}$ не пересекаются (это проверяется так же, как то, что они не пересекаются в точке y , как это доказано выше).

Получается такая картина:

Теперь мы построим из пары инволюций σ, τ без неподвижных точек перестановку A с циклами четной длины. Действие этой перестановки на точки первого цикла, $\{P^\alpha(x)\}$, длины t мы определим как σ , а на точки второго цикла, $\{Q^\alpha(y)\}$, – как τ .

В результате мы получим орбиту точки x , состоящую из всех $2t$ точек обоих построенных раньше (для P и для Q) циклов длины t :

$$x \xrightarrow{A} \sigma(x) \xrightarrow{A} \tau\sigma(x) \xrightarrow{A} \sigma\tau\sigma(x) \xrightarrow{A} \tau\sigma\tau\sigma(x) \xrightarrow{A} \dots$$

При этом $A^2(x) = \tau\sigma(x) = P(x)$, поэтому

$$A^{2t}(x) = P^t(x) = x.$$

Совершенно так же,

$$y \xrightarrow{A} \tau(y) \xrightarrow{A} \sigma\tau(y) \xrightarrow{A} \tau\sigma\tau(y) \xrightarrow{A} \dots,$$

так что $A^2(y) = \sigma\tau(y) = Q(y)$, так что $A^{2t}(y) = Q^t(y) = y$.

Чтобы закончить конструкцию, надо еще договориться о том, с какой именно точки x начинать.

Решается этот вопрос так. Не заботясь об этом выборе, мы можем построить оба цикла длины t , как это описано выше. Все $2t$ точек этих двух циклов уже имеют какие-то (произвольные) номера в избранной заранее нумерации всех наших $N = 2n$ точек.

За точку x в описанной конструкции возьмем ту из этих $2t$ точек обоих циклов, номер которой минимален.

После этого выбора перестановка A однозначно определена (упорядоченной) парой инволюций (σ, τ) без неподвижных точек.

Если бы мы сделали выбор иначе, это означало бы, что модифицированная этим выбором перестановка, $\tilde{A}$, действовала бы (в наших обозначениях) на точку x не как $\tau\sigma$, а как $\sigma\tau$:

$$A(x) = \tau\sigma(x), \quad \tilde{A}(x) = \sigma\tau(x).$$

Но тогда $\tilde{A}(Ax) = \sigma\tau\tau\sigma(x) = x$, т.е. модификация заключалась бы в замене перестановки A на нашем цикле длины $2t$ обратной ей перестановкой $\tilde{A}$. Разумеется, четность длин всех циклов при этом не меняется.

Но указанный выше выбор, опирающийся на произвольную нумерацию точек, позволяет избежать допускаемого в нашей конструкции перестановки A произвола, так что получается действительно взаимно однозначное отображение $Y \times Y \rightarrow X$.

Это отображение, по своему построению, обратно рассмотренному выше отображению $(I, II): X \rightarrow Y \times Y$, сопоставляющему перестановке A с циклами четной длины пару инволюций без неподвижных точек. Тем самым доказана теорема 3:

$$|X| = |Y|^2 = ((2n - 1)!!)^2.$$

ЗАМЕЧАНИЕ. Кроме этой антирелятивистской конструкции (использующей не имеющую никакого инвариантного смысла исходную нумерацию точек, являющуюся вариантом “системы отсчета” в релятивизме), есть еще более инвариантное отображение

$$III: X \rightarrow Y,$$

оказывающееся расслоением с аналогичным базе Y слоем.

А именно, в каждом цикле четной длины у каждого элемента есть противоположный. Отображение III сопоставляет перестановке $A \in X$ (с циклами четной длины) ту инволюцию, которая отправляет каждую точку в диаметрально противоположную ей точку цикла.

Эта инволюция без неподвижных точек на нашем наборе $N = 2n$ точек имеет (двухточечные) дипольные орбиты. Эти n орбит составляют n -точечное пространство орбит Z .

Перестановка A набора $2n$ точек переставляет эти n диполей, так что возникает модифицированная перестановка $\hat{A}: Z \rightarrow Z$ n -точечного пространства орбит Z .

Исходные перестановки (с четными длинами циклов, переставляющие исходные $2n$ точек) можно классифицировать, поднимая разными способами индуцированные перестановки $\hat{A}$ n -точечного пространства диполей до перестановок A исходных $2n$ точек.

Подсчет числа таких поднятий приводит к ответу, равному $(2n - 1)!!$ (при фиксированной инволюции без неподвижных точек, определяющей диполи): но доказать это трудно, так как нужно доказывать странные тождества, вроде следующей теоремы:

$$\sum_{|\mathcal{D}|=n} \frac{n!}{(\Pi r_i)(\Pi(\rho_j!))} 2^{n-y} = (2n - 1)!!, \quad (3.1)$$

где суммирование идет по всем диаграммам Юнга $\mathcal{D}$ площади n . В каждом слагаемом y означает число строк диаграммы, r_i ($i = 1, \dots, y$) – длины этих строк, а ρ_j – числа повторений длин.

Это тождество верно, но я не знаю другого его доказательства, кроме приведенного выше анализа пар инволюций (σ, τ) , доставляющего число перестановок $2n$ точек с четными длинами циклов.

ПРИМЕР. При $n = 3$ диаграмм $\mathcal{D}$ площади 3 всего три, и входящие в приведенную выше формулу (3.1) величины имеют следующие значения:

$\mathcal{D}$	$\{r_i\}$	$\{\rho_j\}$	y
$\{3\}$	$\{1\}$	1
$\{2, 1\}$	$\{1, 1\}$	2
$\{1, 1, 1\}$	$\{3\}$	3

Все наше тождество (3.1) имеет в этом случае вид равенства

$$\frac{3!}{3 \cdot 1!} 2^{3-1} + \frac{3!}{2 \cdot 1!} 2^{3-2} + \frac{3!}{3!} 2^{3-3} = 5!!,$$

т. е.

$$8 + 6 + 1 = 15,$$

что и справедливо.

К сожалению, никакого естественного соответствия между этими пятнадцатью способами поднятия перестановок $\hat{A}$ и пятнадцатью инволюциями без неподвижных точек (на множестве из $2n = 6$ точек), составляющими пространство инволюций Y , не видно. Хотя числа элементов в обоих этих множествах одинаковы и равны 15, для числа инволюций, составляющих Y , мы получаем его в виде

$$15 = 5!! = 5 \cdot 3 \cdot 1 = \frac{6!}{6!!} = \frac{720}{48},$$

а для числа поднятий в виде

$$15 = 8 + 6 + 1.$$

Единственное доказательство тождества (3.1) в общем случае, которое я придумал, – это подсчет числа $(2n - 1)!!$ перестановок A с циклами четной длины, проведенный выше не с помощью факторизации A до $\hat{A}$, а другим, менее релятивистски инвариантным методом (использующим инволюции τ и σ и специальную “систему отсчета”, т. е. нумерацию $2n$ точек).

Но это (неинвариантное) доказательство было получено только благодаря тому, что ответ $(2n - 1)!!$ был уже получен мною эмпирически, за счет длинных вычислений левой части тождества (3.1) для первой дюжины значений параметра n .

Главным при этих вычислениях было доказательство следующего вспомогательного утверждения:

ЛЕММА. Число перестановок A $2n$ точек с циклами только четных длин, факторизующихся в данную фиксированную перестановку $\hat{A}$ (n точек – диполей фиксированной инволюции) с диаграммой Юнга $\mathcal{D}$ из y строчек, составляет 2^{n-y} .

ПРИМЕР. Пусть $n = 3$; перестановка $\hat{A}$ трех точек (u, v, w) имеет диаграмму Юнга

$$\mathcal{D} : \begin{array}{|c|c|} \hline u & v \\ \hline w & \\ \hline \end{array} \quad \text{из } y = 2 \text{ строчек:}$$

$$\hat{A}(u) = v, \quad \hat{A}(v) = u, \quad \hat{A}(w) = w.$$

В этом случае $2^{n-y} = 2^{3-2} = 2$.

Два разных поднятия перестановки $\hat{A}$ трех диполей

$$u = (U \leftrightarrow U'), \quad v = (V \leftrightarrow V'), \quad w = (W \leftrightarrow W')$$

в виде перестановок шести точек этих трех диполей таковы:

$$A_1 : \begin{array}{|c|c|c|c|} \hline U & V & U' & V' \\ \hline W & W' & & \\ \hline \end{array}$$

$$A_2 : \begin{array}{|c|c|c|c|} \hline U & V' & U' & V \\ \hline W & W' & & \\ \hline \end{array}$$

Появляющееся в этой лемме число поднятий 2^{n-y} объясняет вид формулы (3.1) (в которой множитель $n!/((\text{Pr}_i)(\text{Pr}_j))$ пересчитывает перестановки n точек с диаграммой Юнга циклов $\mathcal{D}$).

Получающаяся в результате этих подсчетов статистика диаграмм Юнга циклов для $\sharp^2$ перестановок $N = 2n$ точек, у которых длины всех циклов четные, такова:

n	2	3	4	5	6	7	8
N	4	6	8	10	12	14	16
$\sharp$	3	15	105	945	10 395	135 135	2 027 025
c	4	23	176	1 689	19 524	264 207	4 098 238
$\hat{a}$	1.50	3.91	4.28	5.59	6.389	7.159	7.913
$\hat{T}$	3.33	4.93	6.41	8.98	10.01	14.07	15.002
$\hat{x}$	3.33	4.93	6.41	8.01	9.45	10.99	11.46
$\hat{y}$	1.33	1.53	1.67	1.79	1.88	1.96	2.02
$\hat{\lambda}$	1.00	0.80	0.86	0.82	0.80	0.86	0.76
$\hat{\mu}$	0.50	0.39	0.38	0.27	0.24	0.22	0.20

Сравнивая эту таблицу средних значений со средними значениями по всем $N!$ перестановкам такого же числа N элементов (с. 8), мы видим, что условие четности длин всех циклов уменьшает почти вдвое среднее число строк перестановок, а потому и сильно уменьшает значение параметра $\hat{\mu}$: диаграммы Юнга становятся значительно более вытянутыми в длину.

Еще сильнее этот эффект сказывается на распределении перестановок по значениям параметров длины и высоты. В следующих таблицах эти распределения для перестановок $2n$ точек с циклами четной длины показаны для фиксированного разбиения на диполи, т. е. сумма всех чисел перестановок таблицы составляет $(2n - 1)!!$. Истинные числа перестановок с данными значениями x

и y больше указанных в $(2n - 1)!!$ раз, но это не влияет на распределение вероятностей разных значений x и y .

При $n = 6$, т. е. для перестановок $N = 12$ точек с циклами четной длины, получается такое совместное распределение значений длины x и высоты y диаграммы Юнга циклов:

$x \uparrow$							
12	3 840						
10		2 304					
8		1 440	720				
6		640	960	160			
4			120	180	30		
2						1	
	1	2	3	4	5	6	y

При $n = 7$, $N = 14$ совместное распределение x и y такое:

$x \uparrow$							
14	46 080						
12		26 880					
10		16 128	8 064				
8		13 440	10 800	1 680			
6			7 840	3 360	280		
4				840	420	42	
2							1
	1	2	3	4	5	6	7 y

Для перестановок $2n = 16$ точек, все циклы которых имеют четные длины, распределение $((2n-1)!!$ таких перестановок с любой фиксированной дипольной структурой) по числам циклов y и длинам x наибольших циклов оказывается таково:

$x \uparrow$								
16	645 120							
14		368 640						
12		215 040	107 520					
10		172 032	129 024	21 504				
8		80 640	147 840	40 320	3 360			
6			35 840	44 800	8 960	448		
4				1 680	3 360	840	56	
2								1
	1	2	3	4	5	6	7	8 y

Чтобы объяснить удивительную информацию, содержащуюся в этом распределении, приведу еще картины проекции этого распределения на оси координат x и y (описывающие независимо распределения чисел циклов y и наибольших длин циклов x для случайных перестановок $2n = 16$ точек, у которых все циклы имеют четные длины):

Я надеюсь, что читатели подберут разумные асимптотики этих распределений вероятностей при $n \rightarrow \infty$ (хотя бы при помощи компьютерного подбора параметров естественно напрашивающихся формул, вроде $d_{\#}^{\#} = Ce^{ay-by^2} dy$ или $d_{\#}^{\#} = Cye^{-ky} dy$).

Еще более замечательным выводом из этих вычислений оказываются наблюдаемые распределения длин a всевозможных (а не только максимальных) циклов в перестановках с циклами четных длин: в отличие от распределения чисел циклов по их длинам для всех случайных перестановок N точек (где $\#(a) = N!/a$), для перестановок с циклами только четных длин число $\#(a)$ циклов данной (четной) длины a начинает с ростом a , начиная с некоторого места (похожего на среднюю длину $\hat{x}$ наибольшего цикла), возрастать. Вот распределение $\#(a)$ для перестановок $2n = 16$ точек:

При других значениях n получаются аналогичные распределения (формулы для которых я опять предоставляю отыскать читателям). Вот, например, ответ для $n = 7$:

Хотя нарисованные кривые и напоминают параболы, функция $\sharp(a)$ уж слишком близка к постоянной вблизи от точки минимума $a = 10$ (близкой к средней длине $\hat{x} \approx 10.99$ наибольшего цикла перестановок 14 точек с циклами четных длин). Приращение квадратичной функции на учетверенном расстоянии от минимума в 16 раз больше приращения на исходном расстоянии, а

$$\frac{73 - 24}{25 - 24} = 49$$

второе больше, чем нужно: для параболы $\sharp(8)$ должно было бы отклоняться от минимума $\sharp(10)$ второе больше, чем наблюдается (или же наблюдаемые значения 46 и 73 должны бы были быть 32 и 40).

§ 4. Проективные перестановки

Это – перестановки $N(n)$ точек следующего конечного аналога P_n проективной прямой. Начнем с конечной плоскости $\mathbb{Z}_n^2$, состоящей из n^2 точек (x, y) , где x и y – остатки от деления на n :

$$x \text{ и } y \text{ принадлежат } \mathbb{Z}_n = \mathbb{Z}/(n\mathbb{Z}).$$

Рассмотрим прямые, проходящие через начало координат. Если $n = p$ – простое число, то таких прямых имеется $p + 1$ штука: они задаются своим “наклоном” $k = y/x$, принадлежащим конечной проективной прямой

$$P(\mathbb{Z}_p) = \mathbb{Z}_p \amalg \infty$$

(точка $k = \infty$ соответствует “вертикальной прямой” $x = 0$).

ПРИМЕР. $P(\mathbb{Z}_3)$ состоит из четырех прямых A, B, C, D (где наклон k принимает значения $0, 1, 2, \infty$ соответственно).

Для любого целого числа n мы проведем аналогичную конструкцию, но трудность состоит в том, что деление на не равный 0 элемент кольца $\mathbb{Z}_n$ в этом случае не всегда возможно: если x – делитель числа n , то элемента $1/x$ в кольце $\mathbb{Z}_n$ нет, поскольку целое число xz , делясь на x , не будет давать при делении на n в остатке 1 ни при каком целом множителе z .

Чтобы справиться с этой трудностью, мы поступим следующим образом.

ОПРЕДЕЛЕНИЕ. Точка $(x, y) \in \mathbb{Z}_n^2$ называется *делимой*, если координаты x и y имеют общий множитель, на который делится число n :

$$(x, y) \in m\mathbb{Z}_n^2, \quad \text{где } m \text{ – делитель числа } n.$$

Это определение корректно потому, что при увеличении любой из координат на n свойство делимости вектора (x, y) на m сохраняется (поскольку m – делитель числа n).

Выкинем из конечного тора $\mathbb{Z}_n^2$ не только начало координат, но и все его делимые точки (если число $n = p$ простое, выкидывается только одно начало координат).

Пусть (x, y) – неделимая точка, а целое число u взаимно просто с n . Тогда точка с координатами (ux, uy) тоже неделимая.

Поэтому множество $M(n)$ всех неделимых точек тора $\mathbb{Z}_n^2$ инвариантно относительно умножения на элементы мультипликативной группы Эйлера

$$\Gamma(n) \subset \mathbb{Z}_n^*$$

состоящей из тех остатков от деления на n , которые взаимно просты с n .

Число элементов этой коммутативной группы Эйлера обозначается через $\varphi(n)$, функция φ называется *функцией Эйлера*.

ПРИМЕР. При малых n значения функции Эйлера таковы:

n	1	2	3	4	5	6	7	8	9	10	11	12
φ	1	1	2	2	4	2	6	4	6	4	10	4

Например, $\Gamma(4) = \{1, 3\}$, $\Gamma(9) = \{1, 2, 4, 5, 7, 8\}$. Для простого числа p имеем $\varphi(p) = p - 1$, $\varphi(p^2) = p^2 - p$; вообще, $\varphi(p^a) = p^{a-1}(p - 1)$.

Если натуральные числа u и v взаимно просты, то функция Эйлера мультипликативна:

$$\varphi(uv) = \varphi(u)\varphi(v).$$

ОПРЕДЕЛЕНИЕ. Проективной прямой P_n над $\mathbb{Z}_n$ называется факторпространство

$$P_n = \frac{M(n)}{\Gamma(n)}$$

множества

$$M(n) = \mathbb{Z}_n^2 \setminus \left(\bigcup_p p \mathbb{Z}_n^2 \right) \quad (4.1)$$

(где p пробегает простые делители числа n) неделимых точек тора по мультипликативному действию группы Эйлера на точки тора.

В формуле (4.1) суммирование множеств делимых точек можно проводить только по простым делителям p числа n (так как каждая делимая точка делится уже и на какой-либо простой делитель числа n).

ПРИМЕР. Пусть $n = 6$. Конечный тор $\mathbb{Z}_6^2$ состоит из 36 точек. Делимые среди них – это те точки, у которых обе координаты четны (их 9) или обе делятся на 3 (их 4), с пересечением только по одной точке 0, так что общее число делимых точек есть

$$9 + 4 - 1 = 12.$$

Следовательно, число неделимых точек есть

$$|M(6)| = 36 - 12 = 24.$$

Группа $\Gamma(6)$ состоит из $\varphi(6) = 2$ элементов, $\{1, 5\}$. Поэтому проективная прямая P_6 состоит из $|M(6)|/|\Gamma(6)| = 24/2 = 12$ точек $(A, B, C, D, E, F, G, H, J, K, L, M)$ следующей таблицы прямых тора $\mathbb{Z}_6^2$:

$$\begin{array}{llll} A : \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 5 \\ 0 \end{pmatrix}; & B : \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 5 \\ 5 \end{pmatrix}; & C : \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 5 \\ 4 \end{pmatrix}; & D : \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 5 \\ 3 \end{pmatrix}; \\ E : \begin{pmatrix} 1 \\ 4 \end{pmatrix}, \begin{pmatrix} 5 \\ 2 \end{pmatrix}; & F : \begin{pmatrix} 1 \\ 5 \end{pmatrix}, \begin{pmatrix} 5 \\ 1 \end{pmatrix}; & G : \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \end{pmatrix}; & H : \begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 3 \end{pmatrix}; \\ J : \begin{pmatrix} 2 \\ 5 \end{pmatrix}, \begin{pmatrix} 4 \\ 1 \end{pmatrix}; & K : \begin{pmatrix} 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \end{pmatrix}; & L : \begin{pmatrix} 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix}; & M : \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \end{pmatrix}. \end{array}$$

Группа $SL(2, \mathbb{Z}_n)$ (модулярных матриц из остатков на деления на n) действует на торе $\mathbb{Z}_n^2$, переводя в себя как множества делимых (и неделимых) точек, так и мультипликативное действие группы Эйлера.

Поэтому оно действует и на прямые тора, переводя их друг в друга: получается ее действие в виде перестановки всех точек проективной прямой $P(n)$. Эти перестановки $N(n)$ точек, составляющих множество $P(n)$, называются *проективными перестановками* $N(n)$ точек.

Эта подгруппа группы $S(N)$ всех перестановок этих точек оказывается очень интересной, и мы займемся ниже ее свойствами, в том числе статистикой диаграмм Юнга циклов проективных перестановок.

Вместо группы $SL(2, \mathbb{Z}_n)$ матриц с определителем 1 нам будет удобнее рассматривать ее факторгруппу

$$PSL(2, \mathbb{Z}_n) = SL(2, \mathbb{Z}_n)/E_n,$$

где E_n — подгруппа скалярных матриц $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$ в $SL(2, \mathbb{Z}_n)$. Элемент $\alpha \in \mathbb{Z}_n$ определяет такую скалярную матрицу с определителем 1, если $\alpha^2 = 1$ в $\mathbb{Z}_n$.

ПРИМЕР. Если $n = p$ – нечетное простое число, то скалярных матриц определителя 1 всего 2: единичная и минус единичная ($|E| = 2$, так как $\alpha^2 - 1 = (\alpha - 1)(\alpha + 1)$ и либо $\alpha = 1$, либо $\alpha = -1$). В этом случае, как нетрудно сосчитать,

$$|\mathrm{SL}(2, \mathbb{Z}_p)| = p(p^2 - 1),$$

поэтому

$$|\mathrm{PSL}(2, \mathbb{Z}_p)| = \frac{|\mathrm{SL}(2, \mathbb{Z}_p)|}{|E_p|} = \frac{p(p^2 - 1)}{2}.$$

На прямые проективная группа PSL действует так же, как исходная группа SL , так как E_n их не переставляет.

ПРИМЕР. Если $n = 8$, то скалярных матриц определителя 1 четыре ($1^2 = 1$, $3^2 = 1$, $5^2 = 1$, $7^2 = 1$ по модулю 8). В этом случае

$$|\mathrm{PSL}(2, \mathbb{Z}_8)| = |\mathrm{SL}(2, \mathbb{Z}_8)|/4 = 96.$$

Таким образом, среди $8! = 40\,320$ перестановок 8 точек проективных перестановок всего 96 штук. Числа $N(n)$ точек проективных прямых P_n и числа $Q(n)$ элементов групп $\mathrm{PSL}(2, \mathbb{Z}_n)$ при малых n таковы:

n	2	3	4	5	6	7	8	9	10	11	12
N	3	4	6	6	12	8	12	12	18	12	24
Q	6	12	24	60	72	168	96	324	360	660	288

Статистики параметров диаграмм Юнга циклов Q проективных перестановок N точек проективной прямой приведены ниже, но вначале несколько слов о числе $N(n)$ точек проективной прямой P_n в случае, когда число n не простое.

ТЕОРЕМА. Число точек проективной прямой P_n дается формулой

$$N(n) = n \prod_p \left(1 + \frac{1}{p}\right),$$

где p пробегает все простые делители числа n .

ПРИМЕР.

$$N(p) = p \left(1 + \frac{1}{p}\right) = p + 1.$$

$$N(p^a) = p^a \left(1 + \frac{1}{p}\right) = p^a + p^{a-1} = p^{a-1}(p + 1).$$

Доказательство теоремы следует методу Эйлера нахождения его выражения для дзета-функции (в виде произведения по простым числам).

Рассмотрим, например, случай $n = p^2$. Делимые точки делятся на p , поэтому каждая координата такой точки принимает одно из p возможных значений, так что число делимых точек тора $\mathbb{Z}_{p^2}^2$ составляет p^2 .

Значит,

$$|M(p^2)| = p^4 - p^2 = p^2(p^2 - 1).$$

В то же время значение функции Эйлера в точке p^2 есть

$$\varphi(p^2) = p(p - 1).$$

Поэтому

$$|P_{p^2}| = \frac{|M(p^2)|}{\varphi(p^2)} = \frac{p^2(p^2 - 1)}{p(p - 1)} = p(p + 1).$$

Точно так же

$$|P_{p^a}| = \frac{|M(p^a)|}{\varphi(p^a)} = \frac{(p^a)^2 - (p^{a-1})^2}{p^{a-1}(p - 1)} = \frac{p^{2(a-1)}(p^2 - 1)}{p^{a-1}(p - 1)} = p^{a-1}(p + 1).$$

Тем самым теорема доказана для всех примарных значений $n = p^a$.

С другой стороны, функция N мультипликативна в том смысле, что

$$N(uv) = N(u)N(v),$$

если натуральные числа u и v взаимно просты. Это видно из того, что остатки от деления на разные простые числа независимы: среди четных чисел делится на 3 такая же их доля, как и среди нечетных.

Вследствие этой мультипликативности справедливость теоремы для любого целого n вытекает из ее справедливости для примарных сомножителей. Например, для $n = p_1^{a_1} p_2^{a_2}$ с разными простыми p_1 и p_2 мы находим

$$N(p_1^{a_1} p_2^{a_2}) = \left(p_1^{a_1} \left(1 + \frac{1}{p_1} \right) \right) \left(p_2^{a_2} \left(1 + \frac{1}{p_2} \right) \right) = p_1^{a_1} p_2^{a_2} \left(1 + \frac{1}{p_1} \right) \left(1 + \frac{1}{p_2} \right),$$

что и требовалось доказать.

Вычисления диаграмм Юнга циклов проективных перестановок $N(n)$ -точечного множества P_n проводится следующим образом: составив список координат (x, y) точек $N(n)$ прямых и список $Q(n)$ матриц $g \in \text{SL}(2, \mathbb{Z}_n)$, порождающих группу $\text{PSL}(2, \mathbb{Z}_n)$ после факторизации по подгруппе скаляров E_n , мы явно вычисляем векторы (x, y) и находим, каким прямым они принадлежат – это и определяет проективную перестановку, заданную матрицей g .

ПРИМЕР. Пусть $n = 6$. Выше (на с. 26) указаны координаты точек $N(6) = 12$ прямых $(A, \dots, M)$, составляющих “проективную прямую” P_6 .

Для матрицы $g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ мы находим цикл

$$g \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad g \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad g \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \quad \dots, \quad g \begin{pmatrix} 1 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

из 6 прямых $A \rightarrow B \rightarrow C \rightarrow D \rightarrow E \rightarrow F(\rightarrow A)$. Точно так же, соотношения

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 5 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 5 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

доставляют цикл из 3 прямых, $Q \rightarrow H \rightarrow J(\rightarrow G)$. Наконец, соотношения

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

доставляют циклы длин 2 и 1, $K \rightarrow L(\rightarrow K)$, $M \rightarrow M$.

Итак, диаграмма Юнга проективной перестановки для матрицы g состоит из 4 строк длин 6, 3, 2 и 1 и имеет вид:

Сотни примеров подобного рода привели меня к статистикам, приведенным выше в теореме 6 на с. 9. Самым удивительным для меня выводом из этих вычислений оказалась теорема 4 (с. 6 выше): если число $n = p$ простое нечетное, то все диаграммы Юнга циклов проективных перестановок $N(p) = p + 1$ точки имеют обязательно четные числа строк y .

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 4. Эта теорема вытекает из следующего, тоже удивительного, факта:

ЛЕММА. *Всякая проективная перестановка $N = p + 1$ точки пространства P_p (где p – простое нечетное число) четна.*

Выведем теорему 4 из этой леммы. Изучаемая перестановка разбивается на циклы. Циклическая перестановка четной длины (например, транспозиция двух элементов) нечетна, а циклическая перестановка нечетной длины (например, вращение треугольника) четна.

Поэтому четность изучаемой перестановки множества P_p означает четность числа его циклов четных длин. Число же его циклов нечетных длин четно потому, что сумма длин всех циклов, $p + 1$, четна (ввиду нечетности числа p).

Значит, общее число y всех циклов есть сумма двух четных чисел – четного (ввиду четности перестановки) числа циклов четных длин и четного (ввиду четности общего числа переставляемых точек) числа циклов нечетных длин. Итак, y четно, что и выводит теорему из леммы.

ДОКАЗАТЕЛЬСТВО ЛЕММЫ. Хорошо известно и легко доказать, что модулярная группа $SL(2, \mathbb{Z})$ порождается двумя “элементарными операциями” – жордановыми клетками $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Поэтому достаточно проверить четность всего двух, соответствующих им, проективных перестановок.

В качестве задающих $p + 1$ прямую точек можно взять точки

$$z_k = (1, k), \quad k = 0, 1, \dots, p-1, \quad \text{и} \quad w = (0, 1).$$

Мы находим

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ k \end{pmatrix} = \begin{pmatrix} 1 \\ k+1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Поэтому проективная перестановка, соответствующая матрице $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, имеет два цикла, длин p и 1. Поскольку их длины нечетны, эта перестановка четна.

Для второй образующей, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, можно провести аналогичное вычисление, но можно и обойтись без него, просто переменяя номера координат x и y . Тогда матрица того же оператора примет вид матрицы уже рассмотренного примера. Поэтому эта вторая проективная перестановка имеет циклы таких же длин p и 1 и тоже четна. Лемма доказана.

Удивительно, однако, то, что обе эти проективные перестановки (а потому и числа строк y) оказываются четными не только при нечетных простых значениях n , но и во многих других случаях (например, для $n = 8$ или 9, но не для $n = 2$ и 4).

Но я не располагаю общим доказательством четности этих многочисленных проективных перестановок, а проверял их разными вычислениями для разных не простых значений n .

Четность перестановок очевидна для тех из них, которые являются коммутаторами (или входят в коммутант группы перестановок). Поэтому и для элементов коммутанта модулярной группы соответствующие им проективные перестановки четны.

Но некоторые элементы модулярной группы не входят в ее коммутант (например, образующие $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$). Это следует из наших вычислений потому, что вычисленное представление проективных перестановок 6 элементов множества P_4 имеют диаграммы Юнга с нечетным числом строк,

$$6 = 4 + 1 + 1 = 2 + 2 + 2$$

(а также из того, что проективные перестановки трехточечного множества P_2 содержат всю симметрическую группу $S(3)$).

Хотя эти вычисления коммутантов и коммутаторов не решают вопроса о четности проективных перестановок для не простого числа n , вопрос о явном описании коммутаторов групп $S(N(n))$ и $\text{PSL}(2, \mathbb{Z}_n)$ интересен и сам по себе, и для исследования коммутаторов возникающей последовательности расширений группы крашенных кос, дополняющих ее до группы всех кос (эти расшире-

ния – ядра естественных представлений группы $\text{kos } B(n)$ в соответствующие модулярные группы: $B(N) \rightarrow \text{SL}(2, \mathbb{Z}_n) \rightarrow S(N)$.

Кроме инвариантных подгрупп, доставляемых коммутантами и ядрами этих гомоморфизмов, следовало бы рассмотреть и естественные отображения на факторы по этим инвариантным подгруппам, определяющие интересные характеристические классы и характеристические числа (в виде функций на объемлющих группах). Примером является отображение модулярной группы $\text{SL}(2, \mathbb{Z})$ на ее фактор по коммутанту, сопоставляющее целочисленной матрице с определителем 1 остаток от деления на 24, равный нулю только для матриц из коммутанта.

Подобные функции на симметрических группах, на группах проективных перестановок и на группах kos также было бы интересно описать, имея в виду приложения не только к статистикам диаграмм Юнга циклов, но и ко многим другим вопросам (включая, например, теорию узлов, теорию алгебраических функций, теорию особенностей и симплектическую топологию, где эти характеристические числа появляются при тропическом перенесении теории многообразий Калаби–Яо на вполне интегрируемые гамильтоновы системы и монодромии их лагранжевых расслоений с особенностями над бифуркационными многообразиями каустического типа.

Наряду с рассматривавшимися выше группами случайных и проективных перестановок, есть еще один в некотором смысле промежуточный класс перестановок, происходящих из теории полей Галуа.

Рассмотрим поле Галуа (т. е. конечное поле) из p^2 элементов (где p – простое число). Элементы этого поля образуют “конечный тор” $\mathbb{Z}_p^2$ линейных комбинаций q с коэффициентами в $\mathbb{Z}_p$ двух образующих элементов 1 и f :

$$q = u \cdot 1 + v \cdot f.$$

Операция типа Фробениуса $q \mapsto q^k$ отображает этот конечный тор (из p^2 точек) на себя, переставляя между собой $p + 1$ прямую, выходящую на нем из начала координат.

Возникающие таким образом “перестановки типа Фробениуса” множества P_p из $N = p + 1$ точки частью являются проективными, а частью нет, но их число гораздо меньше, чем полное число $(p + 1)!$ всех случайных перестановок точек множества P_p .

Статистика диаграмм Юнга циклов этих “перестановок типа Фробениуса” – промежуточная между статистиками случайных и проективных перестановок точек множества P_p , но эти статистики предстоит еще изучить, хотя бы эмпирически.

Поля Галуа из p^a элементов приводят таким же образом к перестановкам прямых в a -мерном торе $\mathbb{Z}_p^a$, число которых составляет

$$N(p, a) = \frac{p^a - 1}{p - 1} = p^{a-1} + p^{a-2} + \cdots + p + 1.$$

Но статистику этих перестановок $N(p, a)$ точек никто еще не изучал (даже эмпирически, т. е. путем вычисления таблиц средних характеристик диаграмм Юнга циклов

$$\hat{x}(p, \alpha), \quad \hat{y}(p, \alpha), \quad \hat{\lambda}(p, \alpha), \quad \hat{\mu}(p, \alpha), \quad \hat{a}(p, \alpha), \quad \hat{T}(p, \alpha),$$

и распределений $c_s(p, a)$ всех $c(p, \alpha)$ циклов этих перестановок по их длинам s).

Приведу лишь несколько подобных таблиц для обычных проективных перестановок $N(n)$ точек пространств P_n (прямых на торах $\mathbb{Z}_n^2$).

ПРИМЕР 1. Пусть $n = 7$ (так что число прямых $N(n) = 8$).

Число проективных перестановок составляет 168. Эти 168 перестановок разделяются на 5 классов, соответствующих пяти диаграммам Юнга $\mathcal{D}$ циклов. В следующей таблице для каждого класса $\mathcal{D}$ выписаны число $\#(\mathcal{D})$ перестановок этого класса, числа $\#_s(\mathcal{D})$ циклов длины s в этих $\#(\mathcal{D})$ перестановках и значения параметров (x, y, λ, μ) диаграмм Юнга $\mathcal{D}$.

Затем указаны суммарные числа c_s циклов длины s (по всем $\Sigma = 168$ перестановкам), и средние значения параметров

$$\hat{x} = \frac{\sum_{\mathcal{D}} (\#(\mathcal{D})x(\mathcal{D}))}{(\Sigma = 168)} \quad \text{и т. д.}$$

$\mathcal{D}$	$\#$	$\#_1$	$\#_2$	$\#_3$	$\#_4$	$\#_8$	x	y	λ	μ
48	48	0	0	0	48	7	2	4/7	2/7
42	0	0	0	84	0	4	2	10	1/2
56	112	0	112	0	0	3	4	2/3	4/3
21	0	84	0	0	0	2	4	1	2
1	8	0	0	0	0	1	8	1	8
$\Sigma = 168$		168	84	112	84	48	4.25	2.95	0.77	0.91

Из этих данных получается полное число циклов

$$c = \sum (c_s) = 168 + 84 + 112 + 84 + 48 = 496$$

и средняя длина цикла

$$\hat{a} = \frac{8 \cdot 168}{c} \approx 2.71,$$

а также средний период проективной перестановки 8 элементов множества P_7 , равный

$$\hat{T} = \hat{x} = 4.25.$$

Распределение $\Sigma = 168$ перестановок по числу строк y получается из этой таблицы такое:

Распределение всех ($c = 496$) циклов наших 168 проективных перестановок по длинам a удивительно непохоже на распределения с. 6 для случайных перестановок и для перестановок с циклами четных длин на с. 23.

Вся приведенная статистика показывает существенные отличия статистики проективных перестановок от статистики всех $N!$ случайных перестановок N элементов (приведенной выше, на с. 8).

ПРИМЕР 2. Пусть $n = 8$ (так что число прямых $N(n) = 12$).

Проективных перестановок этих 12 прямых имеется 96. Они делятся на 7 классов по своим диаграммам Юнга циклов, $\mathcal{D}$. В тех же обозначениях, что в примере 1, таблица ответов получается такая:

$\mathcal{D}$	$\sharp$	$\sharp_1$	$\sharp_2$	$\sharp_3$	$\sharp_4$	$\sharp_8$	x	y	λ	μ
24	48	24	0	0	24	8	4	3/8	1/2
18	0	36	0	36	0	4	4	3/4	1
6	24	0	0	12	0	4	6	1/2	3/2
32	0	0	128	0	0	3	4	1	4/3
12	0	72	0	0	0	2	6	1	3
3	12	12	0	0	0	2	8	3/4	4
1	12	0	0	0	0	1	12	1	12
$\Sigma = 96$		96	144	128	48	24	4.32	4.58	0.76	1.47

Средняя длина наибольшего цикла $\hat{x} \approx 4.32$ похожа на $\hat{x} \approx 4.25$ примера 1, но среднее число циклов, $\hat{y} \approx 4.58$, почему-то раза в полтора выше, чем $\hat{y} \approx 2.95$ примера 1.

Общее число циклов c равно $96 + \dots + 24 = 440$, поэтому средняя длина $\hat{a}$ цикла равна

$$\frac{12 \cdot 96}{c} \approx 2.62.$$

Распределение всех $\Sigma = 96$ проективных перестановок 12 точек множества P_8 по числу циклов y такое:

Распределение всех $c = 440$ циклов по длинам a :

Это распределение кажется более понятным, чем странное превалирование циклов длины $a = 3$ при $n = 7$ (в примере 1 выше).

ЗАМЕЧАНИЕ. Наибольший возможный период $T(N)$ перестановок N точек растет с N гораздо быстрее, чем реализуемое проективными перестановками N точек пространства P_n значение.

Например, $T(20) \geq 420$ (поскольку $20 = 1 + 3 + 4 + 5 + 7$, а наименьшее общее кратное слагаемых равно 420), в то время как

$$N(19) = |P_{19}| = 20,$$

а наибольший период, реализуемый в $\text{PSL}(2, \mathbb{Z}_{19})$, составляет всего $19 \ll 420$. Ясно, что $T(N) = N!$, но можно построить примеры, где $T(N) > c\epsilon^{N^\alpha}$ с любым $\alpha < 1/2$. Например, $N(100) > 230\,000\,000$.

Для анализа асимптотики статистик проективных перестановок большого числа точек полезно, прежде всего, исследовать поведение при $n \rightarrow \infty$ числа $|P_n| = N(n)$ прямых тора $\mathbb{Z}_n^2$ (и числа $Q(n)$ элементов проективизированной модулярной группы $\text{PSL}(2, \mathbb{Z}_n)$).

Как видно из явной формулы

$$N(n) = n \prod_p \left(1 + \frac{1}{p}\right)$$

(где p пробегает все простые делители числа n), значение $N(n)$ может превосходить n во сколько угодно раз. Но числа n со столь большими значениями $N(n)/n$ встречаются настолько редко, что неясно даже то, не стремится ли к постоянной при $n \rightarrow \infty$ среднее значение коэффициента растяжения

$$K(n) = \frac{N(n)}{n} = \prod_p \left(1 + \frac{1}{p}\right).$$

Компьютерные вычисления Ф. Аикарди для $n \sim 10^7$ показывают, что чезаровские средние чисел $K(n)$ стремятся при $n \rightarrow \infty$ к константе $15/\pi^2 \approx 1.5198177 \dots$.

Точно так же неясен и вопрос о средней асимптотике числа

$$|E_n| = \frac{|\mathrm{SL}(2, \mathbb{Z}_n)|}{|\mathrm{PSL}(2, \mathbb{Z}_n)|},$$

без понимания которой трудно исследовать поведение величины

$$Q(n) = |\mathrm{PSL}(2, \mathbb{Z}_n)|.$$

Число $|E_n|$ есть число решений уравнения $z^2 = 1$ в $\mathbb{Z}_n$.

При простых нечетных значениях n вопрос не сложен, $|E_p| = 2$ и

$$Q(p) = \frac{p(p^2 - 1)}{2}.$$

Функция Q , видимо, мультипликативна:

$$Q(uv) = Q(u)Q(v), \quad \text{если } u \text{ и } v \text{ взаимно просты.}$$

Исследование среднего поведения функций Q , E и $1/E$ при стремлении аргумента n к бесконечности не просто.

ЗАМЕЧАНИЕ. Наивное рассуждение состоит в том, что квадраты m меньших вычетов по модулю $n = 2m$ независимо и равномерно распределены среди n остатков от деления на n .

В этом предположении можно сосчитать явно вероятность события $E_n = 2k$, состоящего в том, что единица встречается среди этих m квадратов k раз: она задается псевдопуассоновской формулой,

$$p_k = \frac{1}{2^k k!} \left(1 - \frac{1}{m}\right) \left(1 - \frac{2}{m}\right) \cdots \left(1 - \frac{k-1}{m}\right) \left(1 - \frac{1}{n}\right)^{m-k}.$$

Пуассоновость появляется асимптотически, когда k фиксировано, а m велико. Эти вычисления приводят к явным формулам для чезаровских средних последовательности значений E_n при $n \rightarrow \infty$.

Сравнение этого предсказания с эмпирическими значениями функции E позволили бы оценить степень правдоподобности естественной гипотезы о том, что наборы квадратичных вычетов по большим модулям n удовлетворяют (асимптотически, при $n \rightarrow \infty$) статистике Колмогорова наборов реализаций случайной величины (значения которой распределены равномерно среди остатков от деления на число n).

Ф. Аикарди вычислила числа $L(n)$ элементов конечных модулярных групп $SL(2, \mathbb{Z}_n)$ при $n = p^\alpha$, где p – простое число:

$$L(p^\alpha) = p(p^2 - 1)p^{3(\alpha-1)}. \quad (4.2)$$

Например, она нашла значения функции L в следующих точках:

n	4	9	10	12	14	16	20
L	48	648	720	1 152	2 016	3 072	5 760

Доказательство формулы (4.2) изложено ниже.

Я не умею выводить из нее асимптотику чезаровских средних

$$\hat{L}(n) = \frac{\sum_{m \leq n} L(m)}{n}$$

(или чезаровских средних для отношений $L(n)/n^3$).

Я предполагаю, что $Q(n)$ (или $L(n)$) есть число элементов группы симметрий некоторого $N(n)$ -вершинника, мультипликативного в том смысле, что если u и v взаимно просты, то соответствующий $n = uv$ $N(uv)$ -вершинник представляет собой прямое произведение умножаемых $N(u)$ -вершинника и $N(v)$ -вершинника, причем группа симметрий этого произведения представляет собой прямое произведение групп симметрий сомножителей.

Это объяснило бы, почему $Q(12) = Q(3)Q(4) = 12 \cdot 24 = 288$ и $L(12) = L(3)L(4) = 24 \cdot 48 = 1\,152$ (мультипликативности функций Q и $L \equiv Q/E$ совместны, так как функция E тоже мультипликативна).

ТЕОРЕМА. Число элементов группы $SL(2, \mathbb{Z}_n)$ составляет

$$L(n) = n\varphi(n)N(n),$$

(где φ – функция Эйлера, а N – число проходящих через точку $0 \in \mathbb{Z}_n^2$ прямых).

ПРИМЕР. Если $n = p$ простое, то $\varphi(n) = p - 1$, $N(n) = p + 1$, получается $L(n) = p(p^2 - 1)$.

Если $n = 20$, то $\varphi(n) = \varphi(4) \cdot \varphi(5) = 2 \cdot 4 = 8$, $N(n) = n(1 + 1/2)(1 + 1/5) = 36$, так что

$$L(20) = |\mathrm{SL}(2, \mathbb{Z}_{20})| = 20 \cdot 8 \cdot 36 = 5\,760.$$

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ. Мы должны сосчитать число реперов (e, f) определителя 1 в $\mathbb{Z}_n^2$. Вектор e должен быть неделимым. Поэтому он лежит на одной (определенной им) из проходящих через нуль прямых, имеется N возможностей выбора этой прямой.

На этой прямой имеется $\varphi(n)$ неделимых точек, выбор e опять произволен. Итак, вектор e может быть любым из $\varphi(n)N(n)$ векторов.

Когда вектор e выбран, линейное неоднородное уравнение равенства единице определителя пары e, f указывает, что конец вектора f лежит на параллельной e прямой. Целые точки на этой прямой есть. Например, точку f_0 доставляет (после выбора координат) цепная дробь для отношения координат точки e .

Число целых точек f на этой прямой в $\mathbb{Z}_n^2$ равно n (все они получаются из одной из них, f_0 , прибавлением вектора e с коэффициентами из $\mathbb{Z}_n$). Итого общее число базисов составляет $n\varphi(n)N(n)$.

§ 5. Перестановки фиксированного порядка и статистика инволюций

Сравнивая статистики перестановок n^2 точек конечного тора $\mathbb{Z}_n^2$, заданных преобразованием Фибоначчи с матрицей $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}: \mathbb{Z}_n^2 \rightarrow \mathbb{Z}_n^2$ со статистиками случайных перестановок n^2 элементов, я заметил большие различия.

Пытаясь объяснить эти различия, я обратил внимание на “матричное сравнение Ферма–Эйлера”

$$A^T \equiv 1 \pmod{n},$$

выполняющееся для некоторого периода $T(A)$ для автоморфизма $A \in \mathrm{SL}(2, \mathbb{Z}_n)$ тора $\mathbb{Z}_n^2$.

Из этого сравнения следует, что все циклы перестановки $A \in S(n^2)$ имеют своими длинами делители целого числа $T(A)$. Это ограничение на перестановки способно влиять на статистики их диаграмм Юнга циклов. Так возник естественный вопрос: *каковы средние асимптотики при $N \rightarrow \infty$ характеристик диаграмм Юнга циклов для перестановок $A \in S(N)$ N элементов, удовлетворяющих уравнению*

$$A^T = 1$$

(т. е. таких, у которых длины всех циклов являются делителями целого числа T)?

Этот вопрос применим и к перестановкам A $N = n^2$ точек конечного тора, и к проективным перестановкам его $N(n)$ прямых, составляющих его проективизацию P_n .

Хотя для практического использования ответа на этот вопрос нужно было бы еще знать асимптотическую статистику средних значений величин $T(A, n)$ (усредняя по выбору $A \in \text{SL}(2, \mathbb{Z}_n)$ и чезаровски усредняя по выбору параметра n), сам по себе этот вопрос тоже интересен и не тривиален (хотя ответ на него может оказаться странно зависящим от арифметической природы числа T).

Поэтому я решил начать исследование этих статистик с простейшего случая $T = 2$.

Ниже исследуются средние характеристики *инволюций* (перестановок $A \in S(N)$, для которых $A^2 = 1$).

Все такие инволюции классифицируются (с точностью до сопряженности, т. е. до перенумерации рассматриваемых N точек) числом своих неподвижных точек k (которое может принимать значения от 0 до N , четность которых совпадает с четностью числа N).

Предположим, для определенности, что число переставляемых точек N четно. Тогда число неподвижных точек k тоже четно, и статистика ответов задается следующим образом.

Обозначим число неподвижных точек через $k = 2a$ и число циклов длины 2 через l . Тогда $N = 2a + 2l$, $y = k + l = (k + N)/2$ – число инволюций с такой диаграммой Юнга циклов составляет, очевидно,

$$\sharp(k, N) = C_N^k (2l - 1)!! = C_N^k (N - k - 1)!! \quad (5.1)$$

(поскольку число инволюций $2l$ -точечного множества, не имеющих неподвижных точек, равно $(2l - 1)!!$, см. с. 14–16, § 3).

ПРИМЕР. При $N = 12$ общее число инволюций составляет $\sum = 140\,152$, а распределение их чисел циклов y таково:

Высоты y диаграмм Юнга циклов перестановок N точек периода $T = 2$ заключены между $N/2$ и N .

Максимальное значение $\sharp(k, N)$ достигается при таком значении k , что отношение

$$\frac{\sharp(k, N)}{\sharp(k + 2, N)} = \frac{(k + 1)(k + 2)}{N - k}$$

меньше 1 при меньших значениях k и больше 1 при больших значениях k . Мы получаем для критического значения $(k+2)^2 \approx N+2$, т. е.

$$y \approx \frac{N + \sqrt{N+2} - 2}{2};$$

средняя высота диаграммы, $\hat{y}$, также получает асимптотическое приближение $\hat{y} \approx N/2$ (с погрешностью порядка $\sqrt{N}$).

Как видим, свойство 2-периодичности ($T=2$) совершенно меняет всю статистику параметров диаграмм Юнга циклов перестановок, причем число неподвижных точек k для большинства перестановок N точек периода $T=2$ мало по сравнению с числом переставляемых точек (k порядка $\sqrt{N}$).

Формула (5.1) позволяет получить более точные асимптотики из центральной предельной теоремы Бернулли

$$C_N^k \sim \frac{2^{N+1}}{\sqrt{2\pi N}} e^{-t^2/2}, \quad k = \frac{N}{2} + \frac{\sqrt{N}}{2} t$$

и формулы Стирлинга

$$(2l-1)!! \sim 2^{l+\frac{1}{2}} \left(\frac{l}{e}\right)^l.$$

Подставляя эти асимптотики в формулу (5.1), мы находим распределение величины t вида

$$\rho(t) = C e^{-t^2/2 - pt}$$

(где не зависящие от k или t коэффициенты $C(N)$, $p(N)$ явно выписываются).

Из этой формулы следует, что среднее значение величины t есть p , причем оно достигается вблизи точки максимума функции плотности ρ . В терминах координаты k это соответствует полученному нами выше из соображений роста функции $\sharp(N, k)$ оптимальному значению k порядка $\sqrt{N}$, т. е. среднему числу циклов $\hat{y}$ близкому к $N/2$.

Для $N=12$ среднее значение $\hat{y}$, вычисленное по явно указанным выше частотам значений $y=6, \dots, y=12$, составляет

$$\hat{y} = \frac{1\,055\,088}{140\,152} \approx 7.528,$$

тогда как максимальное значение числа инволюций с y циклами достигается при $y=7$.

§ 6. Степень хаотичности распределения длин циклов случайных перестановок

Длины x_s строк диаграммы Юнга циклов случайной перестановки N точек кажутся на вид независимыми случайными величинами (равномерно распределенными на отрезке от 0 до N по теореме 1 (с. 6) о равновероятности попадания в цикл любой длины).

Эта (предположительная) независимость позволила бы применить к исследованию асимптотик при $N \rightarrow \infty$ статистик длин циклов соображения теории вероятностей.

Рассмотрим, например, распределение длины наибольшего цикла,

$$x = \max\{x_s\}.$$

Ограничимся сейчас случаем перестановок из y циклов, со строками суммарной длины N ,

$$x_1 + x_2 + \cdots + x_y = N, \quad (6.1)$$

упорядочивая их обычным для диаграмм Юнга способом,

$$x_1 \geq x_2 \geq \cdots \geq x_y. \quad (6.2)$$

Условие (6.1) определяет в y -мерном пространстве $\mathbb{R}^y$ симплекс размерности $y - 1$. Указанные выше предположения независимости влекут за собой равномерную распределенность случайной точки X с координатами x_s в симплексе (6.1). (Мы пренебрежем условием квантования, что значения координат целочисленны.) Мы вычислим сейчас среднее значение “длины наибольшего цикла” $x(X) = \max\{x_s\}$.

Неравенства (6.2) определяют в y -мерном евклидовом пространстве *камеру Вейля* симметрической группы $S(y)$. Симплекс (6.1) разбивается диагональными гиперплоскостями ($x_i = x_j$) на $y!$ камер Вейля, которые изометрически переводятся друг в друга симметрической группой $S(y)$.

Эта группа симметрий сохраняет и симплекс (6.1), и функцию x на нем. Поэтому среднее значение кусочно линейной функции x на симплексе (6.1) совпадает с ее средним значением на пересечении этого симплекса с камерой Вейля (6.2).

Это пересечение тоже является симплексом (размерности $y - 1$). Кусочно линейная функция x совпадает на нем с линейной функцией x_1 .

ЛЕММА. *Среднее значение линейной функции на симплексе равно среднему арифметическому ее значений в вершинах этого симплекса.*

Хотя это утверждение (о центре тяжести треугольника) хорошо известно, вот его формальное доказательство:

$$\begin{aligned} \int_0^1 u^\alpha (1-u) du \left(\int_0^1 u^\alpha du \right)^{-1} &= \frac{(\alpha+1)^{-1} - (\alpha+2)^{-1}}{(\alpha+1)^{-1}} \\ &= 1 - \frac{\alpha+1}{\alpha+2} = \frac{1}{\alpha+2}. \end{aligned}$$

В качестве линейной функции здесь рассматривается расстояние $z = 1 - u$ до плоскости грани $(\alpha+1)$ -мерного симплекса высоты 1 в евклидовом пространстве.

Объем α -мерного сечения $z = \text{const}$ пропорционален величине u^α (вследствие гомотетичности этих сечений).

Формула показывает, что центр масс $(\alpha + 1)$ -мерного симплекса удален от основания на $1/(\alpha + 2)$ часть длины высоты ($1/3$ для треугольника, $1/4$ для тетраэдра).

Тем самым лемма доказана для специальной линейной функции z . Но любая линейная функция представляет собой линейную комбинацию таких расстояний до гиперплоскостей граней симплекса. Поэтому справедливость леммы для любой линейной функции следует из ее справедливости в рассмотренном специальном случае.

Применим доказанную лемму к вычислению *среднего значения* $\hat{x}$ *изучаемой функции* $x(X) = \max\{x_s\}$ в симплексе (6.1). Оно совпадает со средним значением линейной функции x_1 по пересечению $(y - 1)$ -мерного симплекса (6.1) с камерой Вейля (6.2).

По лемме мы находим

$$\hat{x} = \frac{1}{y} \sum_{r=1}^y (x_1(p_r)),$$

где p_r пробегает все y вершин симплекса – пересечения с камерой Вейля.

Эти вершины являются нульмерными пересечениями диагоналей $x_i = x_j$ и граней симплекса (6.1). Поэтому в каждой такой вершине значения всех ненулевых координат равны между собой:

$$p_r = \left(\left(\frac{N}{r} \right) \geq \left(\frac{N}{r} \right) \geq \dots \geq \left(\frac{N}{r} \right) > 0 \geq 0 \geq \dots \right).$$

Все y вершин получаются при $r = 1, 2, \dots, y$.

Мы заключаем, что

$$x_1(p_r) = \frac{N}{r},$$

так что искомое среднее значение есть

$$\hat{x}(y) = \frac{N}{y} \left(1 + \frac{1}{2} + \dots + \frac{1}{y} \right) \approx \frac{N(\gamma + \ln y)}{y}.$$

Чтобы получить отсюда среднее значение $\hat{x}$ длины диаграммы Юнга циклов полностью случайной перестановки N точек, надо было бы сосчитать еще взвешенное среднее полученных чисел $\hat{x}(y)$ по всем значениям высоты y перестановки N точек.

Хотя мы выше и исследовали эти распределения (см. теорему 7 и с. 10–12), можно попытаться угадать ответ и просто подставив вместо переменной высоты диаграммы y уже исследованное среднее значение (теорема 2, с. 6)

$$\hat{y} = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{N} \sim \gamma + \ln N.$$

Эта подстановка дает значение

$$\hat{x}(\hat{y}) \sim \frac{N(\gamma + \ln(\gamma + \ln N))}{\gamma + \ln N} \sim \frac{N}{\ln N},$$

которое гораздо меньше и наблюдаемых эмпирически значений $\hat{x} \sim 0.6N$, и указанных В. Л. Гончаровым [5] (в 1942 г.) асимптотик.

Из этого различия можно сделать вывод, что предполагавшаяся выше независимость длин x_s разных строк диаграммы Юнга циклов случайной перестановки должна систематически нарушаться.

Например, можно предположить, что перестановки, один цикл которых сильно длиннее других, встречаются чаще, чем если бы длины всех циклов выбирались независимо.

Исследование имеющихся здесь корреляций между длинами разных циклов (хотя бы эмпирическое) было бы, я думаю, полезным вкладом в теорию случайных перестановок.

Его можно было бы даже сопроводить сравнением свойств наборов y длин строк $\{x_s\}$ с описанными в [2] свойствами распределений Колмогорова наборов y независимых значений случайной величины (принимающей, в данном случае, значения $1, 2, \dots, N$ с одинаковыми вероятностями $1/N$).

Колмогоров доказал [6], что распределение определенной им величины λ_n , измеряющей отклонение эмпирической функции распределения наблюдаемой выборки n значений от (непрерывной) теоретической функции распределения изучаемой случайной величины (это значение λ_n само является случайной величиной) стремится при $n \rightarrow \infty$ к универсальному распределению, заданному следующей функцией распределения Колмогорова:

$$\Phi(\lambda) = \sum_{k=-\infty}^{\infty} ((-1)^k e^{-2k^2 \lambda^2}).$$

Значение $\Phi(\lambda)$ – это вероятность того, что значение величины, распределенной по закону Колмогорова, не превосходит λ .

Вопрос о том, похоже ли распределение отклонений λ_y для длин циклов x_s типичных перестановок N элементов с y циклами на колмогоровскую асимптотику Φ , допускает эмпирическое компьютерное исследование, даже если математическое доказательство соответствующей предельной теоремы слишком трудно.

Вдобавок, даже эмпирическое наблюдение существенных отличий распределения значений λ_y для случайных перестановок N элементов с y циклами от колмогоровской асимптотики распределения Φ было бы указанием на новые, еще неизвестные, особенности распределения длин циклов случайных перестановок, которые могли бы найти статистические приложения и независимо от той проблемы установления “истинной асимптотической случайности” большинства перестановок N точек при стремлении N к бесконечности, которой посвящен этот раздел.

Список литературы

- [1] F. J. Dyson, H. Falk, “Period of a discrete cat mapping”, *Amer. Math. Monthly*, **99**:7 (1992), 603–614.
- [2] В. И. Арнольд, “Стохастические и детерминистские статистики орбит в хаотически выглядящих динамических системах”, *Тр. ММО*, **79** (2009).
- [3] V. I. Arnol'd, “Statistics of Young diagrams of cycles of dynamical systems for finite tori automorphisms”, *Mosc. Math. J.*, **6**:1 (2006), 43–56.

- [4] В. И. Арнольд, *Экспериментальное наблюдение математических фактов*, МЦНМО, М., 2006.
- [5] В. Л. Гончаров, “Из области комбинаторики”, *Изв. АН СССР. Сер. матем.*, **8**:1 (1944), 3–48; англ. пер.: V. L. Goncharov, “On the field of combinatory analysis”, *Amer. Math. Soc. Transl. Ser. 2*, **19** (1962), 1–46.
- [6] A. N. Kolmogoroff, “Sulla determinazione empirica di una legge di distribuzione”, *Giorn. Ist. Ital. Attuari*, **4**:1 (1933), 83–91; рус. пер.: А. Н. Колмогоров, “Об эмпирическом определении закона распределения”, *Теория вероятностей и математическая статистика*, Наука, М., 1986, 134–141.

В. И. Арнольд (V. I. Arnold)

Математический институт им. В. А. Стеклова РАН

Поступила в редакцию

04.08.2008