Структура графа на множестве перестановок S_n, задаваемая моделью ошибки в скрытом канале перестановки пакетов

Казаков И.Б.

Статья посвящена изучению структуры графа, порождаемой на множестве перестановок моделью ошибки канала перестановки пакетов, введенной в работе И.Б. Казакова "Кодирование в скрытом канале перестановки пакетов". Установлено, что граф можно разделить на слои, являющиеся независимыми множествами. Введено понятие характеристического графа перестановки и доказано, что номер слоя определятся числом его ребер. Получен результат о степенях вершин слоя в $(S_n)^2$, и на основании его дана оценка мощности конструируемого послойного кода. Разработан инстументарий для получения верхних оценок мощности кодов. Введены понятия симметрического слоя и разбиения графа. Приведены конкретные примеры разбиения S_n на призмы, а также на произведения графов — обобщение понятия призмы. Построено вложение в $E_{\frac{n(n-1)}{2}}$, S_n оказывается ограничением $E_{\frac{n(n-1)}{2}}$. Получен побочный результат алгебраического характера, связывающий размер подгруппы $H \subset S_n$ и содержание в ней n-шаговых перестановок.

Ключевые слова: перестановки, графовая структура, код, исправляющий ошибки

1. Введение

В работе изучается структура множества перестановок S_n, а также верхние и нижние эвристические оценки мощности кодов, исправляющих одну ошибку. Сама данная задача возникла из задачи передачи информации по скрытому каналу перестановки пакетов ([1]). Содержательно рассматривается следующая постановка: по некоему каналу связи передается группа из n пакетов, причем в порядке их передачи содержится

дополнительная информация; в процессе передачи этот порядок может меняться самопроизвольно, например могут самопроизвольно поменяться местами два соседних пакета. Это создает ошибки для кода, заданного перестановками.

Говоря более формально, рассматривается S_n — множество перестановок n элементов. Перестановка $\sigma \in S_n$ представляется как последовательность из n неповторяющихся чисел от 1 до n. На множестве S_n введена структура графа: две перестановки полагаются смежными, если они могут быть получены друг из друга применением транспозиции двух своих соседних элементов. Например, в S_4, перестановке 1234 смежны 2134, 1243, 1324. В терминах, введенных в [1], это соответствует первой модели ошибки. Далее этот граф будет обозначаться так же, как и множество перестановок: S_n, и мы будем отождествлять вершины графа с соответствующими перестановками.

Второй степенью графа, далее обозначаемой как $(S_n)^2$, называется граф над теми же перестановками как вершинами со следующим отношением смежности: две вершины в $(S_n)^2$ смежны тогда и только тогда, когда они или непосредственно смежны в S_n, или же в S_n есть ещё одна вершина, с которой эти две смежны. То есть, если в S_n между ними имеется путь длины 1 или 2. Кодом, исправляющим одну ошибку, (далее просто кодом), называется такое подмножество $K \subset S_n$, которое является независимым множеством относительно структуры графа $(S_n)^2$.

Главный результат работы — это обнаружение слоистой структуры S_n, позволяющей строить эвристический послойный код, и тем самым оценивать снизу мощность максимального кода. Во-вторых, на основе высокой степени симметрии S_n предложено понятие разбиений графа, которые дают метод получения верхних оценок. Получены также побочные результаты о вложении рассматриваемого графа в E_n (множества последовательностей из 0 и 1), а также лемма о подгруппах $H \subset S_n$.

2. Слоистая структура S_n

Выделим в S_n единичную перестановку $e = [1, 2, 3, \ldots, n]$, и скажем, что она лежит в нулевом слое.

Определение 2.1. *Пусть $\sigma \in S_n$. Если длина минимального пути между e и σ равна k, то скажем, что σ лежит в k-ом слое $S_{n,k}$.*

Таким образом, $S_n = S_{n,0} \sqcup S_{n,1} \sqcup \ldots$

Установим ряд простых свойств графа S_n:

Утверждение 2.1. *В S_n нет замкнутых путей нечётной длины.*

Доказательство. Очевидно, т.к. каждый шаг пути это умножение перестановки на транспозицию соседних позиций, то на каждом шаге перестановка меняет свою чётность и поэтому через нечётное число шагов вернуться на прежнее место нельзя. □

Утверждение 2.2. *Пусть $\sigma_1, \sigma_2 \in S_{n,k}$. Тогда они не могут быть смежны.*

Доказательство.
1. Предположим, что они смежны. Составим путь из 3-х частей: $e \to \sigma_1$(k шагов), $\sigma_1 \to \sigma_2$(1 шаг), $\sigma_2 \to e$(k шагов).
2. Всего получился замкнутый путь из 2k+1 шагов, что противоречит предыдущему утверждению.

□

Утверждение 2.3. *Пусть $\sigma_1 \in S_{n,k}$, σ_2 смежно с σ_1. Тогда или $\sigma_2 \in S_{n,k+1}$, или $\sigma_2 \in S_{n,k-1}$.*

Доказательство.
1. $e \to \sigma_1$(k шагов), $\sigma_1 \to \sigma_2$(1 шаг) $\Rightarrow e \to \sigma_2$(k+1 шаг) $\Rightarrow \sigma_2$ лежит в k+1-ом слое или выше(т.е. в слоях с меньшими номерами).
2. Предположим, что $\sigma_2 \notin S_{n,k-1} \sqcup S_{n,k+1}$.
3. Тогда, так как также и $\sigma_2 \notin S_{n,k}$, то σ_2 лежит выше слоя $k-1$. А это означает, что существует путь $l : e \to \sigma_2$, такой что $|l| < k-1$.
4. Построим путь $l' : e \to \sigma_2(|l|$ шагов), $\sigma_2 \to \sigma_1$(1 шаг). Итого $|l'| < k$.
5. А следовательно, σ_1 лежит выше k-ого слоя. Что противоречит условию.
6. Если σ_1 лежит в нулевом слое, то за один шаг можно попасть только в 1-ый слой, так как нет путей, короче, чем путь длины 1.
7. Если σ_1 лежит в 1-ом слое, то σ_2 может лежать лишь в 0-ом или 2-ом слоях, и из п.3 противоречие получается непосредственно.
8. Если σ_1 лежит в последнем слое, то просто можно считать, что $S_{n,k+1} = \emptyset$, и дальнейшие рассуждения аналогичны.

□

Таким образом, при любом проходе пути мы на каждом его шаге идём или на слой вниз, или на слой вверх. Общее же их количество в S_n установим далее.

3. Характеристические графы

Введенное разбиение графа на слои пока что весьма тривиально. Для получения содержательных результатов нужно ввести множество вспомогательных понятий и связать их с введенным разбиением. Первым таким вспомогательным понятием будет характеристический граф, соответствующий перестановке. Такое соответствие дает разбиение S_n на множества по числу ребер в характеристичеком графе. Как будет показано далее, это разбиение совпадает с введенным выше разбиением по слоям. Этот факт позволит перейти к глубокому анализу слоистой структуры S_n.

Для отношения смежности пары вершин $\sigma_1, \sigma_2 \in S_n$ мы будем использовать обозначение $\sigma_1 \sim \sigma_2$.

Перестановка $\sigma \in S_n$ представима как последовательность $[\sigma[1] \dots \sigma[n]]$, как было указанно в введении.

Определение 3.1. *Пусть $\sigma \in S_n$. Характеристическим графом назовём $G_\sigma = (V, E)$, где $V = \{1, 2, 3, \dots, n\}$, а $(i, j), (j, i) \in E$ (граф ненаправлен) $\Leftrightarrow$ или $i < j$, и $\sigma = [\dots, j, \dots, i, \dots]$(т.е. значение j идёт ранее значения i), или же $i > j$, и $\sigma = [\dots, i, \dots, j, \dots]$.*

То есть в G_σ между вершинами i и j есть ребро, тогда и только тогда, когда в σ они стоят в порядке убывания.

Количество ребёр в G_σ будем обозначать через $s(\sigma)$. Несложгно увидеть, что значение $s(\sigma)$ меняется в пределах от 0 до $\frac{n(n-1)}{2}$.

Лемма 3.1. *Пусть σ_2 получена из σ_1 перестановкой позиций k, $k+1$.*

Тогда G_{σ_2} содержит те же ребра, что и G_{σ_1}, также включая ребро $(\sigma_1[k], \sigma_1[k+1])$, если его там(в G_{σ_1}) не было, и исключая, если оно там было.

Доказательство.
1. Обращение порядка $\sigma_1[k]$, $\sigma_1[k+1]$ в последовательности σ есть по определению характеристического графа инверсия наличия заданного в условии ребра. Нужно лишь показать, что все остальные рёбра, как и их отсутствия остались на месте.
2. Значения всех позиций, кроме k, $k+1$, не изменились. Следовательно, рёбра(как и их отсутвие) вида $(\sigma[r_1], \sigma[r_2])$, где $r_1, r_2 \neq k, k+1$ остались на месте.
3. Пусть s — некая позиция, $s \neq k, k+1$. Тогда, или $s < k$, или $s > k+1$.

4. В случае $s < k$ $[\ldots, \sigma_1[s], \ldots, \sigma_1[k], \sigma_1[k+1], \ldots]$ перешло в $[\ldots, \sigma_1[s], \ldots, \sigma_1[k+1], \sigma_1[k], \ldots]$, т.е. как $\sigma_1[s]$ стояло перед обоими $\sigma_1[k]$ и $\sigma_1[k+1]$, так оно и осталось стоять.
5. В случае $s > k+1$ $[\ldots, \sigma_1[k], \sigma_1[k+1], \ldots, \sigma[s], \ldots]$ перешло в $[\ldots, \sigma_1[k+1], \sigma_1[k], \ldots, \sigma[s], \ldots]$, т.е. как $\sigma_1[s]$ стояло после обоих $\sigma_1[k]$ и $\sigma_1[k+1]$, так оно и осталось стоять.
6.Откуда следует, что и рёбра(и их отстутствие) вида $(\sigma[s], \sigma[k]), (\sigma[s], \sigma[k+1])$, где $s \neq k, k+1$ остались на месте.

□

Лемма 3.2.
Выполнены следующие импликации:

a) $\sigma_1 \sim \sigma_2 \Rightarrow |s(\sigma_1) - s(\sigma_2)| = 1$
b) $s(\sigma_1) \neq 0 \Rightarrow \exists \sigma_2 \ |\sigma_1 \sim \sigma_2| \ s(\sigma_2) = s(\sigma_1) - 1$
c) $s(\sigma_1) \neq \frac{n(n-1)}{2} \Rightarrow \exists \sigma_2 \ |\sigma_1 \sim \sigma_2| \ s(\sigma_2) = s(\sigma_1) + 1$

Доказательство.
1. Пункт а) непосредственно следует из леммы 1, по которой характеристические графы смежных вершин различаются ровно на одно ребро.
2. $s(\sigma_1) \neq 0 \Rightarrow \sigma_1$ не является монотонно возрастающей последовательностью. $\Rightarrow \exists k \ \sigma_1[k] > \sigma_1[k+1] \Rightarrow$ в G_{σ_1} есть ребро $(\sigma_1[k], \sigma_1[k+1])$.
3. Получим σ_2 перестановкой позиций $k, k+1, \sigma_2 \sim \sigma_1$. В G_{σ_2} ребро из предыдущего пункта исчезло, и $s(\sigma_2) = s(\sigma_1) - 1$.
4. $s(\sigma_1) \neq \frac{n(n-1)}{2} \Rightarrow \sigma_1$ не является монотонно убывающей последовательностью. $\Rightarrow \exists k \ \sigma_1[k] < \sigma_1[k+1] \Rightarrow$ в G_{σ_1} нет ребра $(\sigma_1[k], \sigma_1[k+1])$.
5. Получим σ_2 перестановкой позиций $k, k+1, \sigma_2 \sim \sigma_1$. В G_{σ_2} ребро из предыдущего пункта возникло, и $s(\sigma_2) = s(\sigma_1) + 1$.

□

Таким образом, на каждом шаге любого пути в S_n мы либо увеличиваем $s(\sigma)$ на 1, либо уменьшаем его же на 1.

Следствие 3.1. *От e до σ есть путь длины $s(\sigma)$.*

Доказательство. Действительно, возьмём σ и будем переходить к смежным вершинам с меньшим на 1 значением $s(\sigma)$, покуда мы не достигнем e, для которого единственного $s(e) = 0$.

□

Следствие 3.2. *Между e и σ нет никакого пути короче длины $s(\sigma)$.*

Доказательство.
1. В силу вышеизложенного, длина любого пути между e и σ равна s_1+s_2, где s_1 — количество шагов пути, на которых $s(\sigma)$ увеличивалось на 1, а s_2 — количество шагов, на которых оно уменьшалось на 1.
2. И тогда $s(\sigma) = s_1 - s_2$. Но $s_1 + s_2 \geq s_1 - s_2$, причём равенство достигается лишь при $s_2 = 0$.

□

Вывод. *$\sigma \in S_{n,s(\sigma)}$, то есть множества вида $\{\sigma | s(\sigma) = k\}$ в точности совпадают со слоями $S_{n,k}$. И всего в S_n имеется $1 + \frac{n(n-1)}{2}$ слоёв соответственно значениям $s(\sigma) = 0, \ldots, \frac{n(n-1)}{2}$.*

Докажем также однозначность восстановления перестановки по её характеристическому графу.

Лемма 3.3. *(о единственности)* $G_{\sigma_1} = G_{\sigma_2} \Rightarrow \sigma_1 = \sigma_2$

Доказательство.
I. Вспомогательные понятия.
1. $V = \{1, 2, \ldots, n\}$ — множество вершин G_σ.
2. Пусть $v \in V$. Тогда

$$L_v^\sigma = \{\sigma[k] | \sigma[k] \text{ стоит левее } v \text{ в последовательности } \sigma\}$$

3. Пусть $v \in V$. Тогда

$$R_v^\sigma = \{\sigma[k] | \sigma[k] \text{ стоит правее } v \text{ в последовательности } \sigma\}$$

4.Из этих определений очевидно следует $V = L_v^\sigma \sqcup \{v\} \sqcup R_v^\sigma$, так как любое $w \in V$ стоит или левее v, или правее, или есть само v, причём все три возможности взаимоисключающи.
II. Однозначное восстановление L_v, R_v по G_σ.
1. Пусть даны перестановки σ_1, σ_2, такие что $G_{\sigma_1} = G_{\sigma_2}$.
2. Зафиксируем $v \in V$. И выберем некое $w \in L_v^{\sigma_1}$.
3. Возможны два случая: $w > v$ или $v < w$.(вершины, взятые как их номера)
4. Рассмотрим случай $w > v$. Тогда по определению оказывается, что (v, w) — ребро G_{σ_1}, а значит, оно ребро и G_{σ_2}.
5. И также по определению оказывается, что и в σ_2 $w \in L_v^{\sigma_2}$(при $w > v$)
6. Рассмотрим случай $w < v$. Тогда по определению оказывается, что (v, w) — не ребро G_{σ_1}, а значит, оно не ребро и G_{σ_2}.

7. И также по определению оказывается, что и в σ_2 $w \in L_v^{\sigma_2}$(при $w < v$)
8. Таким образом $L_v^{\sigma_1} \subset L_v^{\sigma_2}$. Переставив σ_1, σ_2 местами, и докажем также и $L_v^{\sigma_2} \subset L_v^{\sigma_1}$. Таким образом $L_v^{\sigma_2} = L_v^{\sigma_1}$.
9. И, следовательно, также и $R_v^{\sigma_2} = R_v^{\sigma_1}$(см.I.4)
III. Доказательство $L_{v_1}^{\sigma} = L_{v_2}^{\sigma} \Rightarrow v_1 = v_2$.
1. Предположим $v_1 \neq v_2$, при истинной посылке.
2. По I.4 V $= L_{v_1}^{\sigma} \sqcup \{v_1\} \sqcup R_{v_1}^{\sigma} = L_{v_2}^{\sigma} \sqcup \{v_2\} \sqcup R_{v_2}^{\sigma} \Rightarrow \{v_1\} \sqcup R_{v_1}^{\sigma} = \{v_2\} \sqcup R_{v_2}^{\sigma}$
3. И так как $v_1 \neq v_2$, то $v_1 \in R_{v_2}^{\sigma}$, $v_2 \in R_{v_1}^{\sigma}$.
4. И это означает, что в последовательности σ v_1 правее v_2, и v_2 правее v_1. Противоречие.
IV. Тождество первых членов.(база индукции)
1. Пусть $v_1 = \sigma_1[1]$, $v_2 = \sigma_2[1]$.
2. Тогда $L_{v_1}^{\sigma_1} = L_{v_1}^{\sigma_2} = \emptyset$, $L_{v_2}^{\sigma_1} = L_{v_2}^{\sigma_2} = \emptyset$.(см. однозначность по II.)
3. По III получаем, что $v_1 = v_2$, т.е. $\sigma_1[1] = \sigma_2[1]$.
V. Шаг индукции.
1. Пусть при $\forall i < k$ $\sigma_1[i] = \sigma_2[i]$.
2. Положим $v_1 = \sigma_1[k]$, $v_2 = \sigma_2[k]$.
3. Тогда $L_{v_1}^{\sigma_1} = L_{v_2}^{\sigma_2} = \{\sigma_1[1], \ldots, \sigma_1[k-1]\} = \{\sigma_2[1], \ldots, \sigma_2[k-1]\}$.
4. По II.5 $L_{v_1}^{\sigma_2} = L_{v_1}^{\sigma_1} = L_{v_2}^{\sigma_2} = L_{v_2}^{\sigma_1}$.
5. По III отсюда следует $v_1 = v_2$, т.е. $\sigma_1[k] = \sigma_2[k]$.

□

4. Простые перестановки

Для изучения отношения смежности в $(S_n)^2$ следует рассмотреть пути длины 1 и 2 в S_n. Таким путям, независимо от начала пути в силу симметрии(конкретно: автоморфизмы нашего графа S_n, которые являются умножением на некую перестановку) соответствуют транспозиции двух соседних элементов или же произведение двух соседних. Стало быть, дальнейшим направлением исследования будет рассмотрение свойств перестановок такого вида. При этом будет использован вышевведённый инструмент характеристический граф.

Примечание. *Перестановка $\sigma \in S_n$ отождествляется с последовательностью $[\sigma(1), \ldots, \sigma(n)]$. Напомним это ещё раз. Применение другой перестановки к данной это действие на отождествленную с ней последовательность. Так как сама такая последовательность — это результат действия перестановки на последовательность $[1, \ldots, n]$, то*

действие на неё ещё одной перестановки равносильно умножению слева на эту вторую перестановку.

Определение 4.1. *Простыми перестановками будем называть перестановки следующих 2-х типов:*

Определение 4.2. *Одношаговая перестановка — транспозиция 2-х соседних позиций.*

Определение 4.3. *Двушаговая перестановка — произведение 2-х одношаговых. Множество двушаговых перестановок обозначим как O.*

Двушаговые перестановки также разделим на два вида: коммутативные и некоммутативные.

Определение 4.4. *Двушаговая коммутативная перестановка — это перестановка вида $(i, i+1)(j, j+1)$, где $i, i+1 \neq j, j+1$. Их множество обозначим как O_1*

Утверждение 4.1. *Характеристический граф двушаговой коммутативной перестановки содержит два ребра без общих вершин (и только эти рёбра) $(i, i+1)$ и $(j, j+1)$*

Доказательство. Действительно, такая перестановка взятая как последовательность выглядит как $[1, \ldots, i-1, i+1, i, i+2, \ldots, j-1, j+1, j, j+2, \ldots, n]$, в убывающем порядке стоят подпоследовательности из 2-х элементов $[i+1, i]$ и $[j+1, j]$, и причём только они. Что и соответствует этим рёбрам характеристического графа. □

Двушаговая перестановка — это произведение двух одношаговых. Можно ли по данной двушаговой восстановить однозначно одношаговые, как произведение которых она получена? Покажем далее, что ответ на этот вопрос положителен.

Определение 4.5. *Если по двушаговой перестановке однозначно восстанавливается пара одношаговых (вместе с порядком перемножения, если он значим), перемножением которых она получается, то такую двушаговую перестановку назовём однозначной.*

Следствие 4.1. *Всякая двушаговая коммутативная перестановка однозначна.*

Доказательство.
1. Пусть $\sigma = (i, i+1)(j, j+1) = (i', i'+1)(j', j'+1)$ — разложения на одношаговые перестановки, причём если коммутируют первые перестановки (это мы предполагаем), то коммунитируют и вторые. Это так, ибо если бы вторые перестановки бы не коммутировали, то множество подвижных точек σ было бы равно 4 (произведение 2-х независых транспозиций имеет 4 подвижных точки), а с другой 3 (получился бы цикл из трёх позиций, если у двух перемножаемых одношаговых имеется общая позиция), что противоречиво. Иначе говоря, множества коммутативных и некоммутативных двушаговых перестановок (как они будут определены далее) не пересекаются.
2. Рассмотрим характеристический граф $G_\sigma = (V, E)$. Тогда по утверждению $E = \{(i, i+1), (j, j+1)\} = \{(i', i'+1), (j', j'+1)\}$
3. Откуда либо $(i, i+1) = (i', i'+1)$ и $(j, j+1) = (j', j'+1)$, либо $(i, i+1) = (j', j'+1)$ и $(j, j+1) = (i', i'+1)$. В обоих случаях σ оказывается разложенной на одну и ту же неупорядоченную пару одношаговых перестановок.

□

Определение 4.6. *Двушаговые некоммутативные перестановки — это все остальные (кроме коммутативных), причём их имеется два подвида: вида* $(i, i+1)(i+1, i+2) = (i, i+1, i+2)$ *и вида* $(i+1, i+2)(i, i+1) = (i, i+2, i+1)$. *Их множество обозначим как* O_2.

Утверждение 4.2. $G_{(i,i+1,i+2)} = (V, E)$, *где* $E = \{(i, i+1), (i, i+2)\}$.

Доказательство. Запишем как последовательность $[1, \ldots, i-1, i+1, i+2, i, i+3, \ldots, n]$, в убывающем порядке стоят 2-х элементные подпоследовательности $[i+1, i]$, $[i+2, i]$, и притом только они. □

Утверждение 4.3. $G_{(i,i+2,i+1)} = (V, E)$, *где* $E = \{(i+2, i), (i+2, i+1)\}$

Доказательство. Запишем последовательность $[1, \ldots, i-1, i+1, i+2, i, i+3, \ldots, n]$, в убывающем порядке стоят 2-х элементные подпоследовательности $[i+2, i]$, $[i+2, i+1]$, и притом только они.

□

Непосредственно рассматривая два случая подвидов, и объединяя эти утверждения, получаем:

Следствие 4.2. *Характеристический граф двушаговой некоммутативной перестановки содержит всегда два ребра с одной общей вершиной и только их, причём выполнено следующее:*

a) Этим рёбрам инциденты три вершины с подряд идущими номерами i, $i+1$, $i+2$.

b) Общей вершиной является или i, *или* $i+2$. *При этом, если общая вершина* i *(как минимальная из этих трёх по номеру) — это эта перестановка имеет подвид* $(i, i+1, i+2)$, *а если* $i+2$ *(как максимальная из этих трёх по номеру) — то подвид* $(i, i+2, i+1)$. *Из единственности перестановки заданного характеристического графа следует, что эти подвиды не пересекаются.*

Следствие 4.3. *Двушаговые некоммутативные перестановки однозначны.*

Доказательство.
1. Известно, что она не может быть разложена в произведение коммутирующих одношаговых. По предыдущему следствию по двушаговой перестановке однозначно определяется её вид, судя по тому, какая вершина в её характеристическом графе инцидентна двум рёбрам.
I. Перестановка вида $\sigma = (i, i+1, i+2)$.
1. Предположим, что $\sigma = (i, i+1)(i+1, i+2) = (i, i+1, i+2) = (j, j+1, j+2) = (j, j+1)(j+1, j+2)$ — два различных разложения, $i \neq j$.
2. Тогда, с одной стороны $G_\sigma = G_{(i,i+1,i+2)} = (V, \{(i, i+1), (i, i+2)\})$, а с другой $G_\sigma = G_{(j,j+1,j+2)} = (V, \{(j, j+1), (j, j+2)\})$
3. Откуда следует, что либо $(i, i+1) = (j, j+1)$ и $(i, i+2) = (j, j+2)$(откуда $i = j$, противоречие), либо $(i, i+1) = (j, j+2)$ и $(j, j+1) = (i, i+2)$(что очевидный абсурд вида $1 = 2$, см. модуль разности между номерами вершин, инцидентных ребру).
II. Перестановка вида $\sigma = (i, i+2, i+1)$.
1. Предположим, что $\sigma = (i+1, i+2)(i, i+1) = (i, i+2, i+1) = (j, j+2, j+1) = (j+1, j+2)(j, j+1)$ — два различных разложения, $i \neq j$.
2. Тогда, с одной стороны $G_\sigma = G_{(i,i+2,i+1)} = (V, \{(i+2, i), (i+2, i+1)\})$, а с другой $G_\sigma = G_{(j,j+2,j+1)} = (V, \{(j+2, j), (j+2, j+1)\})$
3. Откуда следует, что либо $(i+2, i) = (j+2, j)$ и $(i+2, i+1) = (j+2, j+1)$(откуда $i = j$, противоречие), либо $(i+2, i) = (j+2, j+1)$ и $(j+2, j) = (i+2, i+1)$(что очевидный абсурд вида $2 = 1$, см. модуль разности между номерами вершин, инцидентных ребру).

□

Совокупно доказана:

Теорема 4.1. *Всякая двушаговая перестановка однозначна, или иначе выражаясь, если $\sigma_1, \sigma_2, \sigma_1', \sigma_2'$ — одношаговые и выполнено $\sigma_1\sigma_2 = \sigma_1'\sigma_2'$, то $\sigma_1 = \sigma_1'$ и $\sigma_2 = \sigma_2'$ или же может быть $\sigma_1 = \sigma_2'$, $\sigma_2 = \sigma_1'$, если σ_1, σ_2 коммутируют.*

Укажем теперь количество двушаговых перестановок обоих классов.

Лемма 4.1. $|O| = |O_1| + |O_2|$, *где* $|O_1| = \frac{(n-3)(n-2)}{2}$, $|O_2| = 2(n-2)$. *Откуда всего* $|O| = \frac{(n+1)(n-2)}{2}$.

Доказательство.
1. Одношаговую перестановку можно выбрать $n-1$ способами.
2. 3-цикл вида $(i, i+1, i+2)$ [а также равным образом и вида] $(i, i+2, i+1)$ можно выбрать $n-2$ способами(по $n-2$ возможным i).
3. Всего упорядоченных пар различных одношаговых перестановок ровно $(n-1)(n-2)$ штук.
4. Из п.2 прямо следует, что ($n-2$ на каждый вид) $|O_1| = 2(n-2) =$ количество упорядоченных пар перестановок с пересекающимися позициями.(теорема об однозначности)
5. Следовательно, упорядоченных пар с непересекающимися позициями всего $(n-1)(n-2) - 2(n-2) = (n-3)(n-2)$.
6. А каждая двушаговая коммутативная перестановка соответвует ровно двум таким из п.5.(теорема об однозначности). Следовательно, коммутативных перестановок $|O_2| = \frac{(n-3)(n-2)}{2}$.

□

5. Слои как подграфы в $(S_n)^2$

Из любой вершины S_n, как уже выяснено, ребра ведут или на слой ниже, или на слой выше. Никакие ребра не ведут на этот же слой. А следовательно, сам слой, рассматриваемый как подграф в S_n не имеет ни единого ребра, то есть слой являтся в S_n независимым множеством.

Теперь же исследуем слой как подграф в $(S_n)^2$.

Определение 5.1. *Граф слоя k: $G_k = (V_k, E_k)$, где $V_k = S_{n,k}$, а $(\sigma_1, \sigma_2) \in E_k \Leftrightarrow (\sigma_1, \sigma_2) \in (S^n)^2$, где S^n взято со структурой графа модели 1.*

Исследуем далее степени вершин G_k. Для этого надо подсчитать число путей из 2-х символов от заданного $\sigma \in S_{n,k}$, которые ведут в тот же слой.

Лемма 5.1. *Пусть $\sigma \in S_n$, α — одношаговая перестановка. Тогда $\sigma\alpha \sim \sigma$.*

И обратно, если $\sigma \sim \sigma_1$, то $\sigma_1 = \sigma\alpha$, где α — одношаговая перестановка.

Доказательство.
I.
1. Пусть $\alpha = (i, i+1)$.
2. Последовательность $\sigma = [\ldots, \sigma[i], \sigma[i+1], \ldots]$.
3. Последовательность $\sigma\alpha = [\ldots, \sigma[i+1], \sigma[i], \ldots]$ оказалась полученной из исходной σ перестановкой 2-х соседних позиций, а следовательно, смежна с ней в S_n.
II.
1. Пусть σ_1 получена из σ перестановкой i, $i+1$ позиций.
2. Т.е. $\sigma = [\ldots, \sigma[i], \sigma[i+1], \ldots]$, $\sigma_1 = [\ldots, \sigma[i+1], \sigma[i], \ldots]$.
3. Положим $\alpha = (i, i+1)$. Тогда $\sigma\alpha = [\ldots, \sigma[\alpha[i]]\ \sigma[\alpha[i+1]], \ldots] = [\ldots, \sigma[i+1]\ \sigma[i], \ldots] = \sigma_1$.

□

Необходимо различить пути длины 2, ведущие из данной вершины в вершину из того же слоя, от путей, которые ведут на два слоя вверх/вниз. Этим путям соответствуют двушаговые перестановки.

Определение 5.2. *Двушаговая перестановка n называется нормальной относительно $\sigma \in S_{n,k}$, если $\sigma n \in S_{n,k}$. Множество таких перестановок обозначим как N_σ.*

Из них множество коммутативных обозначим как N_σ^1.

Множество некоммутативных — как N_σ^2.

Определение 5.3. *$\sigma \in S_{n,k}$: $N(\sigma)$ — множество смежных с σ в графе G_k*

Лемма 5.2. *$deg_{G_k}(\sigma) = |N(\sigma)| = |N_\sigma|$.*

Доказательство.

I. Отображение $f_1 : N(\sigma) \to N_\sigma$.
1. Пусть $\sigma_1 \in N(\sigma)$. Тогда существует путь $\sigma \to \sigma_2 \to \sigma_1$ в S_n. И тогда по лемме 1 $\sigma_2 = \sigma\alpha_1$, $\sigma_1 = \sigma_2\alpha_2$, где α_1, α_2 одношаговы.
2. Отсюда $\sigma_1 = \sigma\alpha_1\alpha_2 = \sigma n$, где n двушагово.
3. Сопоставим этому $\sigma_1 \to n$, т.е. $f_1(\sigma_1) = \sigma^{-1}\sigma_1$.

II. Отображение $f_2 : N_\sigma \to N(\sigma)$.
1. Пусть $n \in N_\sigma$. Тогда $n = \alpha_1\alpha_2$, α_1, α_2 одношаговые.
2. Рассмотрим $\sigma' = \sigma n = \sigma\alpha_1\alpha_2$.
3. Так как $n \in N_\sigma$, то $s(\sigma') = s(\sigma n)$. Рассмотрим путь $\sigma \to \sigma\alpha_1 \to \sigma\alpha_1\alpha_2$. По этому пути длины 2 придём в тот же слой, в котором находится его начало σ.
4. Откуда σ смежно с $\sigma\alpha_1\alpha_2 = \sigma n = \sigma'$ в G_k, и, следовательно, $\sigma' \in N(\sigma)$.
5. Сопоставим этому $n \to \sigma'$, т.е. $f_2(n) = \sigma n$.
III. Взаимообратность.
1. $n \in N_\sigma : f_1 \circ f_2(n) = f_1(\sigma n) = \sigma^{-1}\sigma n = n$.
2. $\sigma_1 \in N(\sigma) : f_2 \circ f_1(\sigma_1) = f_2(\sigma^{-1}\sigma_1) = \sigma\sigma^{-1}\sigma_1 = \sigma_1$.
3. Так как $N_\sigma, N(\sigma)$ — конечные множества, то из взаимообратности f_1, f_2 следует $|N_\sigma| = |N(\sigma)|$.

□

6. Понятие сигнатуры перестановки

Для дальнейнего изучения путей длины 2 (или нормальных перестановок), ведущих в тот же слой, требуется ещё одно вспомогательное средство, которое так же, как и характеристический граф, является способом классификации перестановок.

Определение 6.1. *Пусть $\sigma \in S_n$. Сигнатурой $p(\sigma)$ назовём последовательность из $n-1$ нулей и единиц, такую, что $p(\sigma)[k] = 1 \Leftrightarrow (\sigma[k], \sigma[k+1]) \in G_\sigma$, т.е. k-ый элемент сигнатуры равен 1, тогда и только тогда, когда $\sigma[k] > \sigma[k+1]$.*

Лемма 6.1. *Пусть $\sigma_1 = \sigma\alpha$, где $\alpha = (k, k+1)$.*

Тогда $p(\sigma_1)$ отличается от $p(\sigma)$ в k-ой позиции, может отличаться лишь в соседних с k-ой позициях, а во всех остальных позициях они тождественны.

Доказательство.
1. $\sigma = [\ldots, \sigma[k]\ \sigma[k+1], \ldots]$. Тогда $\sigma_1 = [\ldots, \sigma[\alpha[k]]\ \sigma[\alpha[k+1]], \ldots] = [\ldots, \sigma[k+1]\ \sigma[k], \ldots]$.
2. Из этого сразу видно, что «возрастаемость-убываемость» может изменяться лишь у трёх пар(взятых как подпоследовательности из 2-х элементов) соседних элементов, а именно у стоящих в парах позиций: $[k-1, k]$, $[k, k+1]$, $[k+1, k]$, причём в паре $[k, k+1]$ это свойство точно изменяется.

3. Поэтому изменяется k-ая позиция сигнатуры, а также могут меняться только её соседние(если они есть.)

□

Примечание. *Словом «возрастаемость-убываемость» обозначена абстракция общего рода от двух видов «возрастаемость» и «убываемость», которые соответственно субстантивированные свойства последовательности возрастать или убывать. То что «возрастаемость-убываемость» последовательности изменилась означает, что эта последовательность из убывающей стала возрастающей или обратно.*

Далее мы установим некое соответствие между сигнатурой и нормальными перестановками (а значит и путями длины 2, ведущими в тот же слой).

Определение 6.2. *A_σ — это множество пар позиций элементов сигнатуры $p(\sigma)$, которые не стоят рядом и имеют нетождественные значения, то есть множество пар вида 10, 01. Порядок в паре не важен.*

Лемма 6.2. $|N_\sigma^1| = |A_\sigma|$.

Доказательство.

I. $f_1 : A_\sigma \to N_\sigma^1$
1. Пусть пара позиций $\{x, y\} \in A_\sigma$, т.е. $p(\sigma)[x] \neq p(\sigma)[y]$, $|x - y| > 1$.
2. Сопоставим ей двушаговую перестановку $n = (x, x + 1)(y, y + 1)$.
3. Так как $|x - y| > 1$, то n — коммутативная двушаговая перестановка.
4. Сначала рассмотрим например случай $p(\sigma)[x] = 0$, $p(\sigma)[y] = 1$.
5. По определениям: $p(\sigma)[x] = 0 \Leftrightarrow (\sigma[x], \sigma[x + 1]) \notin G_\sigma \Leftrightarrow \sigma[x] < \sigma[x + 1]$
6. $p(\sigma)[y] = 1 \Leftrightarrow (\sigma[y], \sigma[y + 1]) \in G_\sigma \Leftrightarrow \sigma[y] > \sigma[y + 1]$
7. Рассмотрим $\sigma_1 = \sigma n = [\ldots, \sigma[n[x]]\ \sigma[n[x + 1]], \ldots, \sigma[n[y]]\ \sigma[n[y + 1]], \ldots] = [\ldots, \sigma[n[x + 1]]\ \sigma[n[x]], \ldots, \sigma[n[y + 1]]\ \sigma[n[y]], \ldots]$.
То есть домножение на n справа — это перестановка местами x, $x + 1$ позиций и y, $y + 1$ позиций.
8. А это означает, что G_{σ_1} было получено из G_σ добавлением ребра $(\sigma[x], \sigma[x + 1])$ и удалением ребра $(\sigma[y], \sigma[y + 1])$. Общее число рёбер не изменилось, $s(\sigma n) = s(\sigma)$.
9. Откуда следует, что n — нормальная перестановка относительно σ.(в этом случае)
10. Случай с $p(\sigma)[x] = 1$, $p(\sigma)[y] = 0$ разбирается аналогично: ребро $(\sigma[x], \sigma[x + 1])$ удаляется, а ребро $(\sigma[y], \sigma[y + 1])$ добавляется.

11. Итак, $f_1(\{x,y\}) = (x,x+1)(y,y+1)$.
II. $f_2 : N_\sigma^1 \to A_\sigma$.
1. Пусть теперь $n = (x,x+1)(y,y+1)$, $n \in N_\sigma^1$.
2. Тогда сопоставим $n \to \{x,y\}$ (пара).
3. И так как n коммутативно, то $|x-y| > 1$.
4. Предположим, что $p(\sigma)[x] = p(\sigma)[y] = 0$. Тогда $(\sigma[x], \sigma[x+1]), (\sigma[y], \sigma[y+1]) \notin G_\sigma$.
5. Но тогда $G_{\sigma n}$ получено из G_σ добавлением двух этих рёбер.(см.I.7). Откуда $s(\sigma n) = s(\sigma) + 2$, $s(\sigma n) \neq s(\sigma)$, что противоречит нормальности n.
6. Аналогично, если $p(\sigma)[x] = p(\sigma)[y] = 1$, то эти же два ребра удаляются, откуда $s(\sigma n) = s(\sigma) - 2$, $s(\sigma n) \neq s(\sigma)$, что противоречит нормальности n.
7. По п.5,6 получаем $p(\sigma)[x] \neq p(\sigma)[y]$, т.е.(совокупно с п.3) $\{x,y\} \in A_\sigma$
8. Итак, $f_2((x,x+1)(y,y+1)) = \{x,y\}$.
III. Взаимообратность f_1, f_2 очевидна, откуда $|N_\sigma^1| = |A_\sigma|$.

□

7. Сигнатура и нормальные некоммутативные перестановки

Нормальность рассматривается относительно предзаданного σ.

Некоммутативные нормальные перестановки имеются, как известно по определению, двух типов:

Определение 7.1. *Первого типа* $\alpha_i^1 = (i,i+1)(i+1,i+2)$.

Определение 7.2. *Второго типа* $\alpha_i^2 = (i+1,i+2)(i,i+1)$ *,где i пробегает значения от 1 до* $n-2$.

Установим далее, при каких условиях на σ выполнено $\alpha_i^1, \alpha_i^2 \in N_\sigma^2$.

Домножение на α_i^1:

$\sigma\alpha_i^1 = [\ldots, \sigma[i]\ \sigma[i+1]\ \sigma[i+2], \ldots](i,i+1)(i+1,i+2) = [\ldots, \sigma[i+1]\ \sigma[i]\ \sigma[i+2], \ldots](i+1,i+2) = [\ldots, \sigma[i+1]\ \sigma[i+2]\ \sigma[i], \ldots]$

И следовательно $G_{\sigma\alpha_i^1}$ получено из G_σ инверсией наличия рёбер $(\sigma[i], \sigma[i+1])$, $(\sigma[i], \sigma[i+2])$. Поэтому для того, чтобы $s(\sigma\alpha_i^1) = s(\sigma)$ (т.е. $\alpha_i^1 \in N_\sigma^2$), нужно, чтобы одно и только одно из этих рёбер было в G_σ.

Домножение на α_i^2:

$\sigma\alpha_i^2 = [\ldots, \sigma[i]\ \sigma[i+1]\ \sigma[i+2], \ldots](i+1, i+2)(i, i+1) = [\ldots, \sigma[i]\ \sigma[i+2]\ \sigma[i+1], \ldots,](i, i+1) = [\ldots, \sigma[i+2]\ \sigma[i]\ \sigma[i+1], \ldots]$

И следовательно $G_{\sigma\alpha_i^2}$ получено из G_σ инверсией наличия рёбер $(\sigma[i+2], \sigma[i])$, $(\sigma[i+2], \sigma[i+1])$. Поэтому для того, чтобы $s(\sigma\alpha_i^2) = s(\sigma)$(т.е. $\alpha_i^2 \in N_\sigma^2$) нужно, чтобы одно и только одно из этих рёбер было в G_σ.

Далее будем использовать эти установленные критерии нормальности.

Лемма 7.1. *Пусть* $p(\sigma)[i] = p(\sigma)[i+1] = 0$. *Тогда* $\alpha_i^1, \alpha_i^2 \notin N_\sigma^2$.

Доказательство.
1. Из условий следует, что $\sigma[i] < \sigma[i+1] < \sigma[i+2]$.
2. Откуда $(\sigma[i], \sigma[i+1]) \notin G_\sigma$, $(\sigma[i], \sigma[i+2]) \notin G_\sigma$. И следовательно $\alpha_i^1 \notin N_\sigma^2$.
3. Также $(\sigma[i], \sigma[i+2]) \notin G_\sigma$, $(\sigma[i+1], \sigma[i+2]) \notin G_\sigma$. И следовательно $\alpha_i^2 \notin N_\sigma^2$.

□

Лемма 7.2. *Пусть* $p(\sigma)[i] = p(\sigma)[i+1] = 1$. *Тогда* $\alpha_i^1, \alpha_i^2 \notin N_\sigma^2$.

Доказательство.
1. Из условий следует, что $\sigma[i] > \sigma[i+1] > \sigma[i+2]$.
2. Откуда $(\sigma[i], \sigma[i+1]) \in G_\sigma$, $(\sigma[i], \sigma[i+2]) \in G_\sigma$. И, следовательно, $\alpha_i^1 \notin N_\sigma^2$.
3. Также $(\sigma[i], \sigma[i+2]) \in G_\sigma$, $(\sigma[i+1], \sigma[i+2]) \in G_\sigma$. И, следовательно, $\alpha_i^2 \notin N_\sigma^2$.
ч.т.д.

□

Лемма 7.3. *Пусть* $p(\sigma)[i] = 0$, $p(\sigma)[i+1] = 1$. *Тогда одна и только одна из перестановок* α_i^1, α_i^2 *нормальна.*

Доказательство.
1. По условию $\sigma[i] < \sigma[i+1] > \sigma[i+2]$.
2. Далее разберём два возможных случая: $\sigma[i] < \sigma[i+2]$ и $\sigma[i] > \sigma[i+2]$.
I. $\sigma[i] < \sigma[i+2]$
1. Тогда $(\sigma[i], \sigma[i+1]) \notin G_\sigma$, $(\sigma[i+1], \sigma[i+2]) \in G_\sigma$, $(\sigma[i], \sigma[i+2]) \notin G_\sigma$.
2. Откуда $\alpha_i^1 \notin N_\sigma^2$, $\alpha_i^2 \in N_\sigma^2$.
II. $\sigma[i] > \sigma[i+2]$
1. Тогда $(\sigma[i], \sigma[i+1]) \notin G_\sigma$, $(\sigma[i+1], \sigma[i+2]) \in G_\sigma$, $(\sigma[i], \sigma[i+2]) \in G_\sigma$.
2. Откуда $\alpha_i^1 \in N_\sigma^2$, $\alpha_i^2 \notin N_\sigma^2$.

□

Лемма 7.4. *Пусть* $p(\sigma)[i] = 1$, $p(\sigma)[i+1] = 0$. *Тогда одна и только одна из перестановок* α_i^1, α_i^2 *нормальна.*

Доказательство.
1. По условию $\sigma[i] > \sigma[i+1] < \sigma[i+2]$.
2. Далее разберём два возможных случая: $\sigma[i] < \sigma[i+2]$ и $\sigma[i] > \sigma[i+2]$.
I. $\sigma[i] < \sigma[i+2]$
1. Тогда $(\sigma[i], \sigma[i+1]) \in G_\sigma$, $(\sigma[i+1], \sigma[i+2]) \notin G_\sigma$, $(\sigma[i], \sigma[i+2]) \notin G_\sigma$.
2. Откуда $\alpha_i^1 \in N_\sigma^2$, $\alpha_i^2 \notin N_\sigma^2$.
II. $\sigma[i] > \sigma[i+2]$
1. Тогда $(\sigma[i], \sigma[i+1]) \in G_\sigma$, $(\sigma[i+1], \sigma[i+2]) \notin G_\sigma$, $(\sigma[i], \sigma[i+2]) \in G_\sigma$.
2. Откуда $\alpha_i^1 \notin N_\sigma^2$, $\alpha_i^2 \in N_\sigma^2$.

□

Таким образом, для любых двух соседних тождественных позиций транспозиций соответвующие некоммунативные перестановки не являются нормальными, а для соседних нетождественных нормальной является одна из двух некоммутативных (соответвующих).

Обозначим через B_σ множество пар (порядок в паре не важен) соседних позиций сигнатуры $p(\sigma)$ с нетождественными значениями в этих позициях.

Совокупно доказана:

Теорема 7.1. $|B_\sigma| = |N_\sigma^2|$

Пусть $ind(\sigma)$ количество единиц среди элементов сигнатуры $p(\sigma)$, а C_σ — количество пар (порядок не важен) позиций сигнатуры $p(\sigma)$ с нетождественными значениями.

Тогда, с одной стороны, $C_\sigma = A_\sigma \sqcup B_\sigma \Rightarrow |C_\sigma| = |A_\sigma| + |B_\sigma| = |N_\sigma^1| + |N_\sigma^2| = |N_\sigma|$

А с другой, выбирая из $p(\sigma)$ $ind(\sigma)$ единиц и $n - 1 - ind(\sigma)$ нулей, получаем $|C_\sigma| = ind(\sigma)(n - 1 - ind(\sigma))$.

Окончательный результат:

Теорема 7.2. *При* $\sigma \in G_k$, $deg_{G_k}(\sigma) = |N_\sigma| = |C_\sigma| = ind(\sigma)(n - 1 - ind(\sigma))$.

8. Послойный код

Применим вышеполученный теоретический результат.

Так как $\sigma \in S_{n,k}$ может быть смежна лишь с перестановками из соседних слоёв $k-1$, $k+1$, то в S_n можно построить следующий код, исправляющий одну ошибку (т.е. независимое множество в $(S_n)^2$):

Возьмём слои 0-ой, 3-ий, 6-ой и так далее. В каждом найдём независимое множество в графе G_{3k}, п потом получим код как объединение этих независимых множеств.

Аналогично такого же рода код получится с 1-ым, 4-ым, 7-ым $(3k+1)$ и т.д. слоями, а также 2-ым, 5-ым, 8-ым и т.д. $(3k+2)$

Построив эти три кода, можно выбрать из них больший код. Так как теперь нам известны степени вершин в G_k, то мы можем произвести оценку мощности этих кодов.

Из теории графов известно (см. например [2], теорема 25.1), что $\alpha_0(G) \geq \sum\limits_{\sigma \in V} \frac{1}{1+deg(\sigma)}$, где $\alpha_0(G)$ — число независимости графа G, $deg(\sigma)$ — степень вершины σ.

Следствие 8.1. $\alpha_0(G_k) \geq \sum\limits_{\sigma \in S_{n,k}} \frac{1}{1+ind(\sigma)(n-1-ind(\sigma))}$

Определение 8.1. *Вклад перестановки* σ*:* $R(\sigma) = \frac{1}{1+ind(\sigma)(n-1-ind(\sigma))}$

Определение 8.2. *Число k-ого слоя:* $h_k = \sum\limits_{\sigma \in S_{n,k}} R(\sigma)$.

Таким образом, $\alpha_0(G_k) \geq h_k$.

Как уже известно, всего слоев $\frac{n(n-1)}{2} + 1$.

Пусть

$$H_0 = \sum_{0 \leq 3k \leq \frac{n(n-1)}{2}} h_{3k},$$

$$H_1 = \sum_{0 \leq 3k+1 \leq \frac{n(n-1)}{2}} h_{3k+1},$$

$$H_2 = \sum_{0 \leq 3k+2 \leq \frac{n(n-1)}{2}} h_{3k+2}.$$

По построению, мощности первого, второго и третьего кодов соответственно не меньше $\lceil H_0 \rceil$, $\lceil H_1 \rceil$, $\lceil H_2 \rceil$.($\lceil x \rceil$ — операция округления вверх).

Алгоритм расчёта H_0, H_1, H_2:

1) Проходим по всем перестановкам $\sigma \in S_n$, с каждой из которых делаем следующее:

2) Вычисляем её слой $s(\sigma)$, и вклад в сумму $R(\sigma)$.

3) В зависимости от $s(\sigma)\ mod\ 3$, прибавляем этот вклад(соответственно остаткам 0, 1, 2) в накопители H_0, H_1, H_2 (начальное их значение, разумеется, 0).

И так как этот алгоритм проходит по всем $\sigma \in S_n$ по одному разу, а деление вкладов $R(\sigma)$ между суммами H_0, H_1, H_2 дизъюнктивно, то данный алгоритм, работающий линейное относительно $|S_n|$ время (пренебрегая сложностью вычисления $ind(\sigma)$, $s(\sigma)$), действительно их вычислит.

Алгоритмы вычисления $ind(\sigma)$, $s(\sigma)$ элементарны.

Были проведены испытания для пространств S_3 —S_9.

Получена следующая таблица результатов:

	S_3	S_4	S_5	S_6	S_7	S_8	S_9
$\lceil H_0 \rceil$	2	4	10	38	184	1086	7532
$\lceil H_1 \rceil$	1	3	10	37	183	1086	7531
$\lceil H_2 \rceil$	1	3	9	37	183	1085	7531

9. Симметрические слои

Строение S_n может быть рассматриваемо и ещё с одной точки зрения: с точки зрения разбиения его на такие слои-подграфы, каждый из которых является графом строения S_{n-1} (в модели ошибки 1).

Определение 9.1. *k-ый симметрический слой* $S_{n/k} = \{\sigma \in S_n \mid \sigma[1] = k\}$

Очевидно, что как подграф $S_{n/k} \cong S_{n-1}$, так как можно абстрагироваться от первой позиции, а перестановка соседних оставшихся (со 2-ой по n-ую) непосредственно является перестановкой соседних в исходном S_n.

Итак, $S_n = S_{n/1} \sqcup \ldots \sqcup S_{n/n}$.

Пусть $\sigma \in S_{n/k}$. Тогда оно смежно с $n-1$ другими перестановками: $n-2$ из того же симметрического слоя $S_{n/k}$, а с одной из другого $S_{n/k'}$, причём $k' = \sigma[2]$.

Но $S_{n/k}$ в силу изоморфности S_{n-1} само разбивается на симметрические слои второго порядка, каждый из которых изоморфен S_{n-2}, причём принадлежность к определённому слою определена значением $\sigma[2]$.

$S_{n/k} = S_{n/k/1} \sqcup \ldots \sqcup S_{n/k/k-1} \sqcup S_{n/k/k+1} \sqcup \ldots \sqcup S_{n/k/n}$

Каждая вершина $\sigma \in S_{n/k/k'}$ $n-3$ ребрами соединена с вершинами из этого же подслоя, одним ребром — с вершиной из $S_{n/k/k'_1}$ (т.е. этого

же слоя, но другого подслоя), а ещё одним — с вершиной из $S_{n/k'/k}$ (эта вершина получается из данной перестановкой $\sigma[1]$, $\sigma[2]$).

Теперь же рассмотрим пары (k, k'), $k, k' \in \{1, \ldots, n\}$, $k \neq k'$, а также подслои $S_{n/k/k'}$, $S_{n/k'/k}$, то есть разобьём S_n на пары таких вот подслоёв.

Переход между этими подслоями осуществляется перестановкой первой и второй позиций, движение в самих слоях — перестановками всех остальных. Ясно, что эти два движения независимы друг от друга.

[Коммутация: если $\alpha(1) = 1$, $\alpha(2) = 2$, то $\alpha(12) = (12)\alpha$].

Определение 9.2. *Пусть $G = (V, E)$ — некоторый граф. Призмой этого графа $G \times 2 = (V_1, E_1)$ назовём граф, у которого $V_1 = \{(g, i) \mid g \in V, i \in \{0, 1\}\}$, а $((g_1, i_1), (g_2, i_2)) \in E_1 \Leftrightarrow$ или $i_1 = i_2$, и $(g_1, g_2) \in E$; или $i_1 \neq i_2$, и $g_1 = g_2$.*

Чтобы получить призму, нужно взять два экземпляра G, и соединить рёбрами одни и те же вершины в этих экземплярах.

Таким образом, подграф $S_{n/k/k'} \sqcup S_{n/k'/k}$ образует призму вида $S_{n-1} \times 2$. Всего таких пар подслоёв $\frac{n(n-1)}{2}$ штук, то есть S_n разбивается на $\frac{n(n-1)}{2}$ призм вида $S_{n-2} \times 2$.

10. Разбиения

Дадим способ оценки сверху мощности кода. Для этого введем понятие разбиения и рассмотрим вышеопределенное разбиение S_n на призмы.

Определение 10.1. *$G = (V, E)$, $V = V_1 \sqcup \ldots \sqcup V_r$. Разбиением G называются подграфы $G_1, G_2, \ldots, G_r$, $G_i = (V_i, E_i)$, $(a, b) \in E_i \Leftrightarrow a, b \in V$ и $(a, b) \in E$.*

Определение 10.2. *Кодовое число $k(G) = \alpha_0(G^2)$ — это мощность максимального кода на G, исправляющего 1 ошибку.*

Лемма 10.1. *Пусть $G_1, G_2, \ldots, G_r$ — разбиение графа G. Тогда $k(G) \leq k(G_1) + k(G_2) + \ldots + k(G_r)$.*

Доказательство.
1. Дано $G = (V, E)$, $V = V_1 \sqcup V_2 \sqcup \ldots \sqcup V_r$, $G_i = (V_i, E_i)$. Пусть $K \subset V$ — максимальный код, исправляющий одну ошибку($|K| = k(G)$), то есть K — максимальное независимое множество в G^2.
2. Положим $K_i = K \cap V_i$. Также зададим произвольные $a, b \in K_i$.

3. Предположим, что между a, b в G_i существует путь длины не более 2. Тогда этот путь будет также и путём в G, так как G_i подграф G. Но так как $a, b \in K$, то такого пути быть не может. Из противоречия следует, что K_i код в G_i.
4. И так как по определению $|K_i| \leq k(G_i)$, то $k(G) = |K| = |K_1| + |K_2| + \ldots + |K_r| \leq k(G_1) + k(G_2) + \ldots + k(G_r)$.

□

Применительно к разбиению S_n на призмы $S_{n-1} \times 2$ получаем оценку:

Теорема 10.1. $k(S_n) \leq \frac{n(n-1)}{2}\ k(S_{n-2} \times 2)$.

Например $k(S_5) \leq 10k(S_3 \times 2) = 20$ (а оценка сверху совершенным кодом была бы ≤ 24), так как $S_3 \times 2$ — это шестиугольная призма, и нетрудно убедиться, что её кодовое число действительно равно 2.

Примечание. *Все эти рассуждения переносятся и на рассмотрение кода с большим числом ошибок.*

Примечание. *Однако, в применении к S_6 и далее эта оценка оказывается бесполезной, так как она слабее соответствующей оценки совершенного кода.*

11. Произведение графов. Разбиение S_n на произведения

Введенные выше понятия и полученные результаты поддаются обобщению.

Определение 11.1. *Пусть $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ — графы.*
Их произведением $G_1 \times G_2 = (V, E)$ назовём граф, где $V = V_1 \times V_2$, и при $g_1, g_1' \in V_1$; $g_2, g_2' \in V_2$ ребро $((g_1, g_2), (g_1', g_2')) \in E \Leftrightarrow$
или $g_1 = g_1'$, и $(g_2, g_2') \in E_2$;
или $g_2 = g_2'$, и $(g_1, g_2') \in E_1$

Понятие призмы графа $G \times 2$ оказывается частным случаем — это произведение графа на отрезок типа 0-1.

Теперь мы можем рассматривать последовательность $\sigma[1], \ldots, \sigma[n]$ следующим образом: разобьём её на последовательные отрезки длин n_1, $n_2, \ldots, n_p$; $n_1 + n_2 + \ldots + n_p = n$, то есть:
$\sigma_1 = \sigma[1], \ldots, \sigma[n_1]$

$\sigma_2 = \sigma[n_1 + 1], \ldots, \sigma[n + 1 + n_2]$
$\ldots$
$\sigma_p = \sigma[n_1 + \ldots + n_{p-1}], \ldots, \sigma[n_1 + \ldots + n_p]$

И далее, разобьём все перестановки, применённые к данной последовательности, на 2 класса: сохраняющие элементный состав всех отрезков $\sigma[1], \ldots, \sigma[p]$ и все остальные.

Перестановка первого класса может быть разложена на произведение коммутирующих множителей $\alpha_1, \ldots, \alpha_p$, где α_i переставляет элементы лишь внутри отрезка $\sigma[i]$ и нигде более.

И поэтому результаты применения перестановок первого класса на σ совокупно образуют подграф в S_n.

Определение 11.2. *Определим отношение $\sim$ в данном разделе следующим образом: $\sigma \sim \sigma'$ тогда и только тогда, когда $\sigma' = \sigma\alpha$, где α — перестановка первого класса (т.е. σ_1 и есть результат применения α к σ как последовательности).*

Лемма 11.1. *Заданное отношение является отношением эквивалентности.*

Доказательство.
1. $\sigma \sim \sigma$, т.к. $\sigma = \sigma e$, а e сохраняет элементный состав всех $\sigma_1, \ldots, \sigma_p$.
2. $\sigma \sim \sigma' \Leftrightarrow \sigma' = \sigma\alpha \Leftrightarrow \sigma = \sigma'\alpha^{-1}$. Перестановка α — первого класса, значит и α^{-1} тоже первого класса, так как если в одну сторону можно переставить позиции σ, сохраняя элементный состав $\sigma_1, \ldots, \sigma_p$, то с этим же свойством это же можно сделать и в обратную сторону.
3. $\sigma \sim \sigma', \sigma' \sim \sigma'' \Rightarrow \sigma'' = \sigma'\alpha_1 = \sigma\alpha_2\alpha_1$. После применения каждой из α_1, α_2 к σ элементный состав $\sigma_1, \ldots, \sigma_p$ не изменился, и, следовательно, это же верно и для $\alpha_1\alpha_2$.

□

Таким образом, существует разбиение S_n на подграфы, каждый из которых изоморфен $S_{n_1} \times S_{n_2} \times \ldots \times S_{n_p}$. Мощность множества $|S_{n_1} \times S_{n_2} \times \ldots \times S_{n_p}| = n_1! \ldots n_p!$

Следовательно, всего таких подграфов в разбиении $\frac{n!}{n_1! \ldots n_p!}$, и аналогично предыдущему пункту получаем:

Теорема 11.1. $k(S_n) \leq \frac{n!}{n_1! \ldots n_p!}\ k(S_{n_1} \times S_{n_2} \times \ldots \times S_{n_p})$

12. Вложение в $E_{\frac{n(n-1)}{2}}$

Приведем ещё один результат, имеющий отношение к задаче построения кода.

Каждый характеристический граф G_σ задаётся наличием/отсутствием каждого из рёбер между парами вершин из $\{1, 2, 3, \ldots, n\}$, а общее число этих рёбер равно $\frac{n(n-1)}{2}$.

Поэтому G_σ может быть рассматриваемо как последовательность из $\frac{n(n-1)}{2}$ нулей и единиц, где $G_\sigma[i] = 1 \Leftrightarrow$ i-ое ребро лежит в G_σ.

Каждой перестановке $\sigma \in S_n$ соответвует характеристический граф G_σ, причём, как это было доказано (см. лемму о единственности), разным σ_1, σ_2 соответствуют разные характеристические графы $G_{\sigma_1}, G_{\sigma_2}$, и, следовательно, и разные последовательности из $\frac{n(n-1)}{2}$ нулей и единиц.

$E_{\frac{n(n-1)}{2}}$ рассматривается как граф, a смежно с b в $E_{\frac{n(n-1)}{2}} \Leftrightarrow a$, b отличаются в одной позиции.

Таким образом, получается некое инъективное отображение $f : S_n \to E_{\frac{n(n-1)}{2}}$.

Лемма 12.1. *$\sigma_1 \sim \sigma_2$ (в смысле смежности в S_n) $\Rightarrow f(\sigma_1) \sim f(\sigma_2)$ (в смысле смежности в $E_{\frac{n(n-1)}{2}}$, т.е. отличия в одной позиции)*

Доказательство.
1. Пусть $\sigma_1 \sim \sigma_2$. Тогда их характеристические графы G_{σ_1}, G_{σ_2} отличаются на одно ребро.
2. И, следовательно, $f(\sigma_1)$ отличается от $f(\sigma_2)$ лишь в одной позиции.

□

Определение 12.1. *Порядковый граф перестановки $\hat{G}_\sigma$ — это полный ориентированний граф на вершинах $\{1, 2, 3, \ldots, n\}$, рёбра которого идут от вершины, номер которой стоит левее в последовательности $[\sigma[1], \ldots, \sigma[n]]$, к номеру вершины, стоящей в ней же правее.*

Характеристический и порядковый графы связаны по следующему правилу: если $(a, b) \notin G_\sigma$, то в $\hat{G}_\sigma(a, b)$ идёт от меньшего значения к большему, а иначе наоборот.

И, следовательно, инверсия направления одного ребра (a, b) в G_σ приводит к смене направления у (a, b) в $\hat{G}_\sigma$.

И при этом всегда получается направленный цикл, когда это происходит с ребром $(\sigma[i], \sigma[j])$ (для определённости считаем, что $i < j$; а иначе в рассмотрении переставим в этом ребре вершины местами), где $j - i > 1$,

потому что в порядковом графе задана как цепочка $\sigma[i] \to \sigma[k] \to \sigma[j]$ для некоторого k: $i < k < j$, так и ребро $\sigma[i] \to \sigma[j]$(и именно поэтому замена этого ребра на $\sigma[j] \to \sigma[i]$ создаёт 3-цикл). Что несовместимо с транзитивностью.

Следствие 12.1. *Инверсия наличия одного ребра, не являющегося ребром вида* $(\sigma[i], \sigma[i+1])$*, делает граф из характеристического* G_σ *таким, который вообще не есть характеристический граф какой-нибудь перестановки* $\sigma \in S_n$.

Лемма 12.2. *(обратное утверждение)* $f(\sigma_1) \sim f(\sigma_2) \Rightarrow \sigma_1 \sim \sigma_2$.

Доказательство.
1. $f(\sigma_1) \sim f(\sigma_2) \Rightarrow G_{\sigma_1}, G_{\sigma_2}$ отличаются на одно ребро (ребро $\sigma \equiv$ позиция G_σ).
2. По вышедоказанному, так как это характеристические графы, то G_{σ_2} может быть получено из G_{σ_1} лишь инверсией ребра вида $(\sigma[i], \sigma[i+1])$.
3. А это означает, что σ_2 получена из σ_1 перестановкой i и $i+1$-ых позиций. $\Rightarrow \sigma_1 \sim \sigma_2$.

□

Таким образом, в $E_{\frac{n(n-1)}{2}}$ есть подмножество T, такое что $\left(E_{\frac{n(n-1)}{2}}\right)_{|T} \cong S_n$.

Лемма 12.3. *Пусть* K *— независимое множество в* $\left(E_{\frac{n(n-1)}{2}}\right)^2$.

Тогда $K \cap T$ *независимо в* $\left(\left(E_{\frac{n(n-1)}{2}}\right)_{|T}\right)^2$.

Доказательство.
1. Пусть $a, b \in K \cap T$. Предположим, что между a и b есть путь, рёбра которого лежат в $\left(E_{\frac{n(n-1)}{2}}\right)_{|T}$.
2. Тогда эти рёбра лежат и в $E_{\frac{n(n-1)}{2}}$, так как это подграф.
3. Но наличие пути длины не более 2 в $E_{\frac{n(n-1)}{2}}$ между $a, b \in K$ противоречит независимости K в $\left(E_{\frac{n(n-1)}{2}}\right)^2$.

□

Аналогично и для кодов с большим числом ошибок.

Это даёт нам некий метод построения кодов в S_n: строим сначала код в $E_{\frac{n(n-1)}{2}}$ (а таких кодов известно много — ими занимается обычная теория кодирования), а потом ограничиваем построенный код на подмножество T.

Однако, $|S_n| = n!$, а $\left|E_{\frac{n(n-1)}{2}}\right| = 2^{\frac{n(n-1)}{2}}$. И поэтому $\frac{|S_n|}{\left|E_{\frac{n(n-1)}{2}}\right|} \to 0$, что при больших n создаёт затруднения того вида, что «элементы кода будут попадать в T с исчезающе малой вероятностью».

13. Алгебраические коды

При исследовании был непреднамеренно получен побочный результат алгебраического характера, имеющий отношение к строению подгрупп $H \subset S_n$.

Определение 13.1. *Код $K \subset S_n$ назовём алгебраическим, если он является подгруппой S_n относительно операции перемножения перестановок.*

Лемма 13.1. *Подгруппа $H \subset S_n$ является алгебраическим кодом, исправляющим одну ошибку, тогда и только тогда, когда она не содержит простых перестановок (см.4.1.3).*

Доказательство.
1. Пусть α — простая перестановка, такая что $\alpha \in H$.
2. Тогда $e, \alpha \in H$ (H — подгруппа), $\alpha = e\alpha$.
3. А значит, α как последовательность получена из $e = [1, \ldots, n]$ применением простой перестановки α.
4. То есть, между элементами e и α есть путь (в терминах модели ошибки 1) длины не более чем 2. Откуда немедленно следует, что H - не код.
5. Обратно, пусть H - не код. Тогда есть такие $g_1, g_2 \in H$, между которыми есть путь длины не более 2.
6. Что равносильно тому, что $g_2 = g_1\alpha$, где α - некая простая перестановка.
7. Но это означает, что $\alpha = g_1^{-1}g_2 \in H$ (в силу свойств подгруппы).

□

В оценках из [1] было установлено, что всякий код в S_n, исправляющий одну ошибку, содержит не более $(n-1)!$ элементов.

Следствие 13.1. *Пусть $H \subset S_n$ —- подгруппа, $|H| > (n-1)!$*

Тогда H содержит простую перестановку, т.е. или транспозицию двух соседних, или произведением двух таки одношаговых перестановок.

Данный результат может быть обобщён и на большее количество ошибок.

Теорема 13.1. *Если $H \subset S_n$ — подгруппа и $|H| > q_{err}$, где q_{err} — ограничение сверху на код, исправляющий err ошибок, то H среди своих элементов содержит произведение не более чем $2err$ одношаговых перестановок.*

Доказательство аналогично: достаточно заменить понятие «простая перестановка» на понятие «произведение не более 2err одношаговых».

Список литературы

[1] Казаков И. Б. Кодирование в скрытом канале перестановки пакетов// Программная инженерия. — 2018. — Т. 9, №4. — С. 163–173.

[2] Емеличев В.А., Мельников О.И., Сарванов В.И., Тышкевич Р.И. Лекции по теории графов. М.: Наука, 1990. 384 с.

The structure of a graph induced on the set of permutations S_n by an error model of a covert channel based on packet permutations

Kazakov I.B.

The paper I.B. Kazakov, "Encoding in a covert channel of packet permutations" introduced a number of error models for codes over sets of permutations. Such error models induce graph structure on sets of permutations. Our research is focused on properties of these graphs. We show that the graphs consist of layers of independent sets; the layer that contains the given permutation is determined by the number of edges in the characteristic graph of the permutation. We estimate vertex degrees in the layers of the graph $(S_n)^2$ and use this estimate to bound the cardinality of an error-correcting kayer-based code. After that we develop a number of aids that allow to obtain upper bounds of code cardinality. We introduce the notions of symmetric layers and graph partitions and decompose S_n for some values of n into prisms and into graph products, i.e. generalised prisms. We also embed the graph S_n into $E_{\frac{n(n-1)}{2}}$. Finally establish a connection between sizes

of subgroups $H \subset S_n$ and presence of n-step permutations in these subgroups.

Keywords: permutations, graph structure, error-correcting code