[3] Lyndon R., Schupp P. Combinatorial group theory. Springer-Verlag, 1977. / Русский перевод: Линдон Р., Шупп П. Комбинаторная теория групп. М.: Мир, 1980.

[4] Ol'shanskii A.Yu. Hyperbolicity of groups with subquadratic isoperimetric inequality // Int. J. Alg. and Comp. 1993. V. 1. № 3. P. 281–289.

[5] Ольшанский А.Ю. Периодические фактор-группы гиперболических групп // Мат. сборник. 1991. Т. 182. № 4. С. 543–567.

Переходные системы с максимальной вариативностью относительно кодирований состояний

С.Б. Родин

Введение

В статье изучаются переходные системы, обладающие тем свойством, что все операторы, задаваемые всевозможными кодированиями данной переходной системы, различны. Данное свойство называется свойством максимальности.

Прежде всего для каждого натурального n приведен пример переходной системы с n состояниями, обладающей этим свойством.

Затем сформулирован критерий свойства максимальности в терминах порождающих полугруппы преобразований множества состояний Q, индуцированных входными последовательностями переходной системы. А именно, переходная система обладает свойством максимальности тогда и только тогда, когда для образующих переходной системы найдется только тривиальная перестановка, коммутирующая с ними.

В последней части статьи приведены две асимптотические оценки (верхняя и нижняя) количества переходных систем с n состояниями, не обладающих свойством максимальности (где n – произвольное натуральное число).

Основные понятия и определения

Определение 1. Под *переходной системой* V понимается тройка (A, Q, φ), где A, Q – конечные множества, φ – функция, определенная на множестве $Q \times A$ и принимающая значения из Q [1].

Множества A и Q называются соответственно *входным алфавитом* и *алфавитом состояний* переходной системы V. Функция φ называется *функцией переходов* переходной системы V [1].

Далее рассматриваем переходные системы с входным алфавитом $A = \{0, 1\}$.

Всякой переходной системе V можно сопоставить полугруппу V^S, а именно, совокупность преобразований множества состояний Q, индуцированных входными последовательностями переходной системы, другими словами, если
$X^S = \{s : Q \to Q | \exists a \in A$ такое, что $s(q) = \varphi(q, a)$ для всех $q \in Q\}$, то $V^S = \langle X^S \rangle$, то есть полугруппа V^S порождается множеством X^S [3].

Обозначим $s_0(q) = \varphi(q, 0)$, $s_1(q) = \varphi(q, 1), q \in Q$.

Определение 2. *Кодированием* переходной системы назовем взаимно однозначное отображение F множества Q в E_2^K, где число K определяется соотношением $K =]\log_2 n[, n = |Q|$. $F(q)$ назовем кодом состояния q.

Каждое кодирование F переходной системы задает булев оператор $\hat{\varphi} : E_2^{K+1} \to E_2^K$, который на элементах $x = (a, F(q))$, где $a \in E_2, F(q) \in E_2^K$ определяется соотношением $\hat{\varphi}(x) = F(\varphi(q, a))$, а на остальных наборах $\hat{\varphi}(x)$ определяется произвольно.

Определение 3. Будем говорить, что переходная система V с n состояниями обладает свойством максимальности, если все операторы, задаваемые всевозможными ее кодированиями, различны.

1. Существование переходных систем, обладающих свойством максимальности

Покажем, что для каждого фиксированного n существует переходная система с n состояниями, обладающая свойством максимальности. Причем число операторов, получаемых при ее всевозможных кодированиях, равно $C_{2^K}^n \cdot n!$.

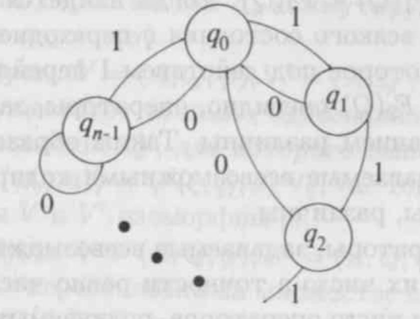
Заметим, что для любого n число всевозможных кодирований некоторой переходной системы V с n состояниями равно $C_{2^K}^n \cdot n!$, где $K =]\log_2 n[$.

В самом деле, число всевозможных кодирований некоторой переходной системы V с n состояниями равно числу взаимно однозначных отображений n-элементного множества в 2^K-элементное множество. Число подмножеств из n элементов множества из 2^K элементов равно $C_{2^K}^n$. Число взаимно однозначных отображений множества из n элементов в множество из n элементов равно $n!$. Отсюда число кодирований равно $C_{2^K}^n \cdot n!$.

Приведем теперь пример такой переходной системы с n состояниями, что любые два ее кодирования задают разные операторы.

Обозначим $Q = \{q_0, ..., q_{n-1}\}$. Рассмотрим переходную систему $V = (A, Q, \varphi)$, где $A = \{0, 1\}$, у которой функция φ определяется следующим образом:

1) $\varphi(q_0, 0) = q_{n-1}$;
2) $\varphi(q_i, 0) = q_0, i = 1, ..., n-2$;
3) $\varphi(q_{n-1}, 0) = q_{n-1}$;
4) $\varphi(q_i, 1) = q_i + 1, i = 0, ..., n-2$;
5) $\varphi(q_{n-1}, 1) = q_0$.



На рисунке приведена диаграмма переходной системы V.

Докажем, что все операторы, задаваемые всевозможными кодированиями данной переходной системы, различны, причем число всевозможных операторов равно $C_{2^K}^n \cdot n!$. Обозначим через F_1 и F_2 два произвольных разных кодирования. Сначала рассмотрим случай, когда образ Q при первом кодировании совпадает с образом Q при втором кодировании (то есть $F_1(Q) = F_2(Q)$).

Пусть состояния q_i и q_j таковы, что $F_1(q_i) = F_2(q_j)$. Тогда рассмотрим $\varphi(q_i, 1)$ и $\varphi(q_j, 1)$. Если их коды не совпадают (то есть $F_1(\varphi(q_i, 1)) \neq F_2(\varphi(q_j, 1))$), то теорема доказана, так как соответствующие два оператора различны. Пусть их коды совпадают. В этом случае опять подействуем 1 на получившиеся состояния $\varphi(q_i, 1)$ и $\varphi(q_j, 1)$ и применим предыдущее рассуждение и т.д., пока не дойдем до q_{n-1} (то есть $\varphi(q_i, 1...1) = q_{n-1}$ и $\varphi(q_j, 1...1) = q_s$). Считаем, что $F_1(q_{n-1}) = F_2(q_s)$. Рассмотрим действие 0 на эти состояния:

$$\varphi(q_{n-1}, 0) = q_{n-1};$$

$$\varphi(q_s, 0) = q_0.$$

Предположим, что $F_1(q_{n-1}) = F_2(q_0)$. Тогда имеем следующую цепочку равенств $F_2(q_0) = F_1(q_{n-1}), F_1(q_{n-1}) = F_2(q_s) \Rightarrow F_2(q_0) = F_2(q_s)$. Но это означает, что два разных состояния имеют один и тот же код. Получаемое противоречие доказывает, что все операторы, задаваемые всевозможными кодированиями данной переходной системы различны в случае $F_1(Q) = F_2(Q)$.

Пусть теперь $F_1(Q) \neq F_2(Q)$. Тогда найдется $q \in Q$ такое, что $F_1(q) \notin F_2(Q)$. Для всякого состояния q переходной системы можно найти состояние, которое под действием 1 перейдет в q. В силу соотношения $F_1(q) \notin F_2(Q)$ очевидно, операторы, задаваемые первым и вторым кодированием различны. Таким образом, доказано, что все операторы, задаваемые всевозможными кодированиями данной переходной системы, различны.

Так как все операторы, задаваемые всевозможными кодированиями, различны, то их число в точности равно числу всех кодирований, таким образом число операторов, получаемых при всех кодированиях данной переходной системы равно $C_{2^K}^n \cdot n!$.

Приведенный пример показывает, что для каждого фиксированного n множество переходных систем с n состояниями со свойством максимальности не пусто. Прежде чем перейти к вопросу о мощности этого множества, докажем критерий свойства максимальности.

2. Критерий свойства максимальности

В этом параграфе будет сформулирован и доказан критерий свойства максимальности в терминах порождающих полугруппы переходной системы, который будет впоследствии использован для доказательства асимптотических оценок мощности множества переходных систем со свойством максимальности.

Пусть задана переходная система $V = (E_2, Q, \varphi)$, где $|Q| = n$. Обозначим через s_0, s_1 образующие полугруппы V^S переходной системы V.

Теорема 1. *Для того, чтобы переходная система V обладала свойством максимальности, необходимо и достаточно, чтобы любая нетривиальная перестановка σ не коммутировала либо с s_0, либо с s_1 (то есть либо $\sigma s_0 \neq s_0\sigma$, либо $\sigma s_1 \neq s_1\sigma$).*

Следствие. Для того, чтобы переходная система V не обладала свойством максимальности, необходимо и достаточно, чтобы нашлась нетривиальная перестановка σ, коммутирующая с s_0 и с s_1 (то есть $\sigma s_0 = s_0\sigma$ и $\sigma s_1 = s_1\sigma$).

Определение 4. Пусть $V = (A, Q, \varphi), V' = (A, Q', \varphi')$ – переходные системы, причем существует взаимно однозначное отображение ξ множества Q на множество Q', для которого выполняется следующее соотношение: $\xi(\varphi(q, a)) = \varphi'(\xi(q), a)\ \forall q, \forall a$. Тогда говорим, что переходные системы V и V' изоморфны [1].

Определение 5. Пусть $V = (A, Q, \varphi), V' = (A, Q, \varphi')$ – переходные системы. И пусть σ – перестановка на множестве состояний. Тогда, если $\varphi'(q, a) = \sigma(\varphi(\sigma^{-1}(q), a))$, то говорим, что переходная система V' получается из V перестановкой σ на множестве состояний.

Лемма 1. *Пусть переходные системы* $V=(E_2,Q,\varphi)$, $V'=(E_2,Q,\varphi')$ *изоморфны. Тогда для всякого кодирования* F *переходной системы* V *существует кодирование* F' *переходной системы* V' *такое, что порождаемые ими булевы операторы* $\hat{\varphi}$ *и* $\hat{\varphi}'$ *совпадают.*

Доказательство. Пусть $|Q| = n$. Пусть задано некоторое кодирование F переходной системы V, которое порождает оператор $\hat{\varphi}$. По определению изоморфизма переходных систем существует взаимно однозначное отображение ξ множества Q на себя, для которого выполняется соотношение $\xi(\varphi(q,a)) = \varphi'(\xi(q),a)$. Тогда положим по определению $F'(q) = F(\xi^{-1}(q))$. Покажем, что при таком кодировании получим оператор $\hat{\varphi}'$, совпадающий с $\hat{\varphi}$. По определению оператора $\hat{\varphi}$: $\hat{\varphi}(aF(q)) = F(\varphi(q,a))$. В силу изоморфности переходных систем имеем: $F(\varphi(q,a)) = F(\xi^{-1}(\varphi'(\xi(q),a)))$, $F(\xi^{-1}(\varphi'(\xi(q),a))) = F'(\varphi'(\xi(q),a))$ и $F'(\varphi'(\xi(q),a)) = \hat{\varphi}'(aF'(\xi(q),a))$. Следовательно $\hat{\varphi}(aF(q)) = \hat{\varphi}'(aF'(\xi(q)))$, где $aF(q) = aF'(\xi(q))$. Таким образом лемма 1 доказана.

Лемма 2. *Пусть для некоторого кодирования* F *переходной системы* $V = (E_2,Q,\varphi)$ *существует кодирование* F' *переходной системы* $V' = (E_2,Q,\varphi')$ *такое, что порождаемые ими булевы операторы* $\hat{\varphi}$ *и* $\hat{\varphi}'$ *совпадают, тогда переходные системы* V *и* V' *изоморфны.*

Доказательство. Чтобы доказать изоморфность переходных систем нужно указать взаимно однозначное отображение ξ множества Q на себя, для которого выполняется соотношение $\xi(\varphi(q,a)) = \varphi'(\xi(q),a)$ Определим отображение ξ следующим образом: $q' = \xi(q) \Leftrightarrow F'(q') = F(q)$. Очевидно, это отображение определено корректно (в силу взаимной однозначности кодирования F'). Это отображение взаимно однозначно. Действительно, если $\xi(q_1) = \xi(q_2) = q'$, то $F(q_1) = F'(q') = F(q_2)$. И в силу взаимной однозначности кодирования F имеем $q_1 = q_2$, то есть отображение ξ инъективно. А так как отображение ξ – отображение n-элементного множества на n-элементное множество, то оно взаимно однозначно. В силу того, что операторы $\hat{\varphi}$ и $\hat{\varphi}'$ совпадают, справедливо равенство $\hat{\varphi}(aF(q)) = \hat{\varphi}'(aF'(\xi(q)))$. Тогда по определению операторов $\hat{\varphi}$ и $\hat{\varphi}'$, $F(\varphi(q,a)) = \varphi(aF(q))$ и $F'(\varphi'(\xi(q),a)) = \hat{\varphi}'(aF'(\xi(q)))$. И следовательно $F(\varphi(q,a)) = F'(\varphi'(\xi(q),a))$. Откуда получаем равенство $\xi(\varphi(q,a)) = \varphi'(\xi(q),a)$. Тем самым лемма 2 доказана.

Следствие. Для двух различных переходных систем найдутся два различных кодирования, такие что порождаемые ими операторы совпадают, тогда и только тогда, когда заданные переходные системы изоморфны.

Лемма 3. *Переходная система* $V = (E_2,Q,\varphi)$ *обладает свойством максимальности тогда и только тогда, когда для любой нетривиальной перестановки на множестве состояний получаемая переходная система* $V' = (E_2,Q,\varphi')$ ***не является*** *изоморфной данной.*

Доказательство. Пусть $|Q| = n$ и s_0, s_1 – образующие полугруппы V^S переходной системы $V = (E_2,Q,\varphi)$.

Пусть переходная система V обладает свойством максимальности. Предположим, что существует нетривиальная перестановка на множестве состояний, такая что получаемая переходная система $V' = (E_2,Q,\varphi')$ является изоморфной данной. Тогда по лемме 1 для всякого кодирования переходной системы V найдется кодирование переходной системы V' такое, что порождаемые кодированиями операторы совпадают. Это означает, что для переходной системы существуют по крайней мере два кодирования, такие что порождаемые ими операторы совпадают. И, следовательно, переходная система V не обладает свойством максимальности. Полученное противоречие доказывает лемму 3 в одну сторону.

Обратно. Пусть для любой нетривиальной перестановки на множестве состояний получаемая переходная система $V' = (E_2,Q,\varphi')$ не является изоморфной данной переходной системе V. Предположим, что переходная система V не обладает свойством максимальности. Тогда существуют по крайней мере два кодирования F и F' переходной системы V, такие что порождаемые ими операторы совпадают. Рассмотрим переходную систему V', получаемую из V перестановкой σ такую, что $F(q) = F'(\sigma(q))$. Но тогда выполнены условия леммы 2, и следовательно, V и V' изоморфны. Мы пришли к противоречию. Лемма 3 полностью доказана.

Доказательство критерия.

Необходимость.

Пусть переходная система V обладает свойством максимальности. Тогда в силу леммы 3 для любой нетривиальной перестановки σ получаемая переходная система $V' = (E_2, Q, \varphi')$ не изоморфна V, то есть для любого взаимно однозначного отображения ξ множества Q на себя (то есть для любой перестановки на n-элементном множестве) существует q и существует a такие, что выполняется следующее соотношение: $\xi(\varphi(q,a)) \neq \varphi'(\xi(q),a)$. Но тогда и для тождественной перестановки i найдется q и найдется a такие, что $\varphi(q,a) \neq \varphi'(q,a) = \sigma(\varphi(\sigma^{-1}(q),a))$. Но это и означает, что σ не коммутирует либо с s_0 (если $a=0$), либо с s_1 (если $a=1$). Тем самым доказана необходимость.

Достаточность.

Докажем, что для любой перестановки σ получаемая переходная система V' не изоморфна V. Предположим противное. Пусть V и V' изоморфны. Тогда существует взаимно однозначное отображение ξ множества Q на себя (то есть перестановка на множестве Q) такое, что выполняется следующее соотношение: $\xi(\varphi(q,a)) = \varphi'(\xi(q),a), \forall q, \forall a$. По определению V' имеем $\varphi'(\xi(q),a) = \sigma(\varphi(\sigma^{-1}(\xi(q)),a)),\ \forall q, \forall a$. Объединяя оба равенства, получаем соотношение: $\sigma^{-1}(\xi(\varphi(q,a))) = \varphi(\sigma^{-1}(\xi(q)),a),\ \forall q, \forall a$. Но это означает, что перестановка $\sigma^{-1}\xi$ коммутирует с s_0 и с s_1. Полученное противоречие доказывает достаточность. Таким образом критерий доказан полностью.

3. Оценка числа переходных систем, обладающих свойством максимальности

Перейдем теперь к вопросу о числе переходных систем со свойством максимальности. В этом параграфе будут сформулированы и доказаны верхняя асимптотическая и нижняя асимптотическая оценки числа переходных систем с n состояниями, не обладающих свойством максимальности.

Теорема 2. *Обозначим через $V_{NM}(n)$ множество переходных систем с n состояниями, не обладающих свойством максимальности. Тогда справедлива оценка*

$$\lim_{n\to\infty} \frac{|V_{NM}(n)|}{n^{2n}} \leqslant \frac{1}{e^4\left(1-\frac{1}{e^2}\right)} < 1.$$

Теорема 3. *Справедлива оценка*

$$\lim_{n\to\infty} \frac{|V_{NM}(n)|}{n^{2n}} \geqslant \frac{1}{2e^4}\left(1 - \frac{1}{e^4\left(1-\frac{1}{e^2}\right)}\right) > 0.$$

Следствие. Обозначим через $V_M(n)$ множество переходных систем с n состояниями, обладающих свойством максимальности. Тогда справедлива оценка

$$\lim_{n\to\infty} \frac{|V_M(n)|}{n^{2n}} \geqslant 1 - \frac{1}{e^4\left(1-\frac{1}{e^2}\right)} > 0.$$

Прежде чем доказать теорему 2, докажем несколько вспомогательных утверждений.

Чтобы переходная система не обладала свойством максимальности, необходимо и достаточно, чтобы порождающие полугруппы преобразований, индуцированных входными последовательностями, коммутировали с некоторой перестановкой (критерий свойства максимальности). Но тогда для каждой перестановки найдем все переходные системы, с ней коммутирующие. Суммируя по всем перестановкам, получим, очевидно, верхнюю оценку для числа переходных систем, не обладающих свойством максимальности.

Определение 6. Говорим, что перестановка σ сохраняет некоторое множество N, если $N = \sigma(N)$ (совпадают как множества).

Утверждение 1. *Пусть перестановка σ и подстановка s коммутируют. Если перестановка σ сохраняет множество N, то:*

i) перестановка σ сохраняет полный прообраз отображения s множества N;

ii) перестановка σ сохраняет образ отображения s множества N.

Доказательство. Обозначим через $N' = s^{-1}(N)$ полный прообраз отображения s множества N. Предположим, что перестановка σ не сохраняет N', то есть $\exists i \in N'$, такое что $\sigma(i) \notin N'$. Это означает, что $s(\sigma(i)) \notin N$. В силу коммутативности σ и s получаем $\sigma(s(i)) \notin N$, где $s(i) \in N$ (так как $i \in N'$). Полученное противоречие доказывает утверждение i).

Докажем утверждение ii). Пусть перестановка σ сохраняет множество N, то есть $N = \sigma(N)$. Так как перестановка σ и подстановка s коммутируют, справедливо $\sigma(s(N)) = s(\sigma(N))$. В силу того, что перестановка σ сохраняет множество N, можно написать $s(\sigma(N)) = s(N)$. Откуда имеем равенство $\sigma(s(N)) = s(N)$. Данное равенство доказывает утверждение ii).

Пусть задана перестановка σ на n-элементном множестве $M = \{1, ..., n\}$. Обозначим через $S_\sigma(n)$ все подстановки на множестве M, коммутирующие с перестановкой σ.

Обозначим через $C_\sigma(n)$ количество подстановок на множестве M, коммутирующих с перестановкой σ.

Обозначим через $V_\sigma(n)$ множество всех переходных систем с n состояниями, таких что для каждой переходной системы из этого множества порождающие ее подстановки s_0 и s_1 коммутируют с σ (то есть $s_0\sigma = \sigma s_0, s_1\sigma = \sigma s_1$).

Обозначим через $C_{V_\sigma(n)}$ мощность множества $V_\sigma(n)$.

Утверждение 2. *Введем следующие обозначения:* $M = \{1, ..., n\}$, $M_1 = \{i_1, ... i_l\}$, $M_2 = M \setminus M_1$. *Пусть задана перестановка* $\sigma = (i_1 ... i_l)$ *на множестве* $M = \{1, ... n\}$. *Тогда подстановка* s, *с ней коммутирующая, имеет один из следующих видов: либо*

$$s = \begin{pmatrix} ......i_1.........i_l...... \\ ..\sigma^m(i_1)...\sigma^m(i_l).. \end{pmatrix}, \tag{1}$$

где $0 \leqslant m \leqslant l-1$ *и* $\forall j \in M_2, s(j) \in M_2$; *либо*

$$s = \begin{pmatrix} ...i_1...i_l... \\ ...k...k... \end{pmatrix}, \tag{2}$$

где $k \in M_2, \forall j \in M_2, s(j) \in M_2$.

Доказательство. Заметим, что перестановка σ сохраняет любой элемент множества M_2, то есть $\forall j \in M_2, \sigma(j) = j$. Значит, в силу утверждения 1, перестановка σ сохраняет элемент $s(j)$, где подстановка s коммутирует с перестановкой σ. Но σ сохраняет только элементы множества M_2, следовательно $s(j) \in M_2$.

Помимо элементов множества M_2 перестановка σ сохраняет множество M_1. Значит, если подстановка s коммутирует с перестановкой σ, то σ должно сохранять множество $s(M_1)$ (в силу утверждения 1). Если множество $s(M_1)$ содержит некоторый элемент i_p множества M_1, то оно должно содержать и элемент $\sigma(i_p)$, а следовательно и $\sigma(\sigma(i_p)), \sigma^3(i_p), ..., \sigma^l(i_p)$. То есть если множество $s(M_1)$ содержит элемент множества M_1, то оно содержит и все множество M_1.

Отсюда следует, что либо $s(M_1) = M_1$, либо $s(M_1) \subseteq M_2$.

Пусть $s(M_1) \subseteq M_2$, то есть $s(i_1) = k_1$, ..., $s(i_l) = k_l$, где $k_1 \in M_2$, ..., $k_l \in M_2$. Заметим, что перестановка σ сохраняет элемент k_1. Значит, перестановка σ сохраняет и его полный прообраз при отображении s, где подстановка s коммутирует с перестановкой σ. Следовательно, элемент $\sigma(i_1)$ лежит в полном прообразе отображения s элемента k_1, то есть $k_1 = s(\sigma(i_1)) = s(i_2) = k_2$. Продолжая рассуждения, получим, что $k_1 = k_2 = ... = k_l$, то есть подстановка s имеет вид $s = \begin{pmatrix} ...i_1...i_l... \\ ...k...k... \end{pmatrix}$, где $k \in M_2$, $\forall j \in M_2\ s(j) \in M_2$.

Пусть $s(i_1) = i_p = \sigma^{p-1}(i_1)$. По условию подстановка s коммутирует с перестановкой σ. Но тогда справедливо $s(i_2) = s(\sigma(i_1)) = \sigma(s(i_1)) = \sigma(i_p) = \sigma(\sigma^{p-1}(i_1)) = \sigma^{p-1}(\sigma(i_1)) = \sigma^{p-1}(i_2)$. Продолжая рассуждения, получим, что $\forall i_m \in M_1\ s(i_m) = \sigma^{p-1}(i_m)$, то есть подстановка s имеет вид $s = \begin{pmatrix} ....i_1..........i_l......... \\ ..\sigma^{p-1}(i_1)...\sigma^{p-1}(i_l).. \end{pmatrix}$, где $\forall j \in M_2\ s(j) \in M_2$ и $0 \leqslant p-1 \leqslant l-1$. Таким образом доказано, что если подстановка s коммутирует с заданной перестановкой, то она имеет один из указанных видов. Утверждение доказано.

Следствие. Пусть задана перестановка $\sigma = \sigma_1 \cdot ... \cdot \sigma_k$, где $\sigma_j = (i_1^j ... i_{l_j}^j)$, $j = 1, ..., k$. Обозначим $M_j = (i_1^j, ..., i_{l_j}^j)$, $j = 1, ..., k$. Тогда подстановка s, коммутирующая с перестановкой σ имеет вид

$$s = \begin{pmatrix} \ldots i_1^1 \ldots i_{l_1}^1 \ldots i_1^2 \ldots i_{l_2}^2 \ldots i_1^k \ldots i_{l_k}^k \\ \ldots p_1^1 \ldots p_{l_1}^1 \ldots p_1^2 \ldots p_{l_2}^2 \ldots p_1^k \ldots p_{l_k}^k \end{pmatrix},$$

где для каждого j либо $\{p_1^j, \ldots, p_{l_j}^j\}$ совпадает с множеством M_t, для некоторого $t \in \{1, \ldots, k\}$, либо $p_1^j = p_2^j = \ldots = p_{l_j}^j$, и не существует $t \in \{1, \ldots, k\}$ такого, что M_t содержит $\{p_1^j, p_2^j, \ldots, p_{l_j}^j\}$.

Справедливо и обратное утверждение.

Утверждение 3. *Всякая подстановка s, имеющая один из указанных видов: либо (1), либо (2), коммутирует с заданной перестановкой $\sigma = (i_1 \ldots i_l)$.*

Доказательство. Пусть подстановка имеет вид $s = \begin{pmatrix} \ldots\ldots i_1 \ldots\ldots\ldots i_l \ldots\ldots \\ \ldots\sigma^m(i_1)\ldots\sigma^m(i_l)\ldots \end{pmatrix}$, где $\forall j \in M_2$ $s(j) \in M_2$ и $0 \leqslant m \leqslant l-1$. Так как $\forall j \in M_2$ $s(j) \in M_2$, то $\forall j \in M_2 s(\sigma(j)) = s(j) = \sigma(s(j))$. $\forall i_p \in M_1$ $s(\sigma(i_p)) = s(i_{p+1}) = \sigma^m(i_{p+1}) = \sigma^m(\sigma(i_p)) = \sigma(\sigma^m(i_p)) = \sigma(s(i_p))$. Пусть подстановка имеет вид $s = \begin{pmatrix} \ldots i_1 \ldots i_l \ldots \\ \ldots k \ldots k \ldots \end{pmatrix}$, где $k \in M_2 \forall j \in M_2, s(j) \in M_2$. Аналогично предыдущему случаю, имеем $\forall j \in M_2$ $s(\sigma(j)) = s(j) = \sigma(s(j))$, $\forall i_p \in M_1$ $s(\sigma(i_p)) = s(i_{p+1}) = k = \sigma(k) = \sigma(s(i_p))$.

Утверждение 4. *Пусть задана перестановка $\sigma = (i_1 \ldots i_l)$ на множестве $M = \{1, \ldots, n\}$. Тогда число подстановок, с ней коммутирующих, равно $C_\sigma = n(n-l)^{n-l}$.*

Доказательство. Посчитаем количество подстановок первого и второго вида, коммутирующих с заданной перестановкой $\sigma = (i_1 \ldots i_l)$. Заметим, что число отображений множества M_2 в себя равно $(n-l)^{n-l}$ (оно содержит $n-l$ элементов). А число отображений множества M_1 на себя указанным способом равно l. Таким образом получаем $l(n-l)^{n-l}$ подстановок первого вида, коммутирующих с σ. Заметим, что число отображений множества M_1 в M_2 указанным способом равно $n-l$ (число элементов множества M_2). Значит, подстановок второго вида, коммутирующих с σ, $(n-l)(n-l)^{n-l}$. Следовательно, число подстановок, коммутирующих с σ, равно $C_\sigma(n) = n(n-l)^{n-l}$ Утверждение доказано.

Утверждение 5. *Пусть задана перестановка $\sigma = (i_1 \ldots i_l)$ на множестве $M = \{1, \ldots, n\}$. Мощность множества $V_\sigma(n)$ равна $C_{V_\sigma(n)} = n^2(n-l)^{2(n-l)}$.*

Доказательство. В силу утверждения 4 с перестановкой σ коммутирует $C_\sigma(n) = n(n-l)^{n-l}$ подстановок. А это и означает, что мощность множества $V_\sigma(n)$ равна $C_{V_\sigma(n)} = n^2(n-l)^{2(n_l)}$. Утверждение доказано.

Утверждение 6. *Пусть задана перестановка σ. И множество $M = \{1, \ldots, n\}$ разбивается на множества M_1 и M_2 таким образом, что σ сохраняет каждый элемент множества M_2 (то есть $\forall j \in M_2$ $\sigma(j) = j$), и мощность множества M_1 равна l, тогда мощность множества V_σ не превосходит $n^l(n-l)^{2(n-l)}$.*

Доказательство. Аналогично доказательству предыдущего утверждения. Пользуемся следствием из утверждения 4. То есть посчитаем количество подстановок указанного в следствии вида и возведем в квадрат. Пусть перестановка σ представляется в виде произведения двух независимых циклов. Тогда подстановки, с ней коммутирующие, разбиваются на четыре вида в зависимости от образов элементов циклов (первый – образы элементов циклов являются элементами циклов, второй – образы элементов первого цикла – элементы циклов, а образы элементов второго цикла не являются элементами циклов, третий – наоборот, образы элементов первого цикла не являются элементами циклов, а образы элементов второго цикла являются элементами цикла, и, наконец, четвертый – ни образы элементов первого цикла, ни образы элементов второго цикла не являются элементами циклов). Оценим число подстановок, принадлежащих каждому классу. Очевидно, первому принадлежит не более $l^2(n-l)^{n-l}$, второму $l(n-l)(n-l)^{n-l}$, третьему $(n-l)l(n-l)^{n-l}$, четвертому

$(n-l)^2(n-l)^{n-l}$. Суммируя получаем, что перестановок заданного вида не более $n^2(n-l)^{n-l}$. Если перестановка σ представляется в виде произведения k циклов, аналогичными рассуждениями получаем, что число перестановок, с ней коммутирующих, не превосходит $n^k(n-l)^{n-l}$. И так как максимально возможное число циклов равно $l/2$, то число подстановок, коммутирующих с заданной перестановкой σ, не превосходит $n^{l/2}(n-l)^{n-l}$. И число переходных систем не превосходит $n^l(n-l)^{2(n-l)}$. Утверждение доказано.

Утверждение 7. *Для мощности множества $V_l(n) = \bigcup_\sigma V_\sigma(n)$, где объединение берется по всем перестановкам σ таким, что множество $M = \{1, ..., n\}$ разбивается на множества M_1 и M_2 таким образом, что $\forall j \in M_2\ \sigma(j) = j$, и мощность множества M_1 равна l, справедлива оценка*

$$|V_l(n)| \leqslant n^{2l}(n-l)^{2(n-l)}.$$

Доказательство. Заметим, что l элементов из n можно выбрать C_n^l способами. А количество перестановок таких, что множество $M = \{1, ..., n\}$ разбивается на множества M_1 и M_2 таким образом, что $\forall j \in M_2, \sigma(j) = j$, и мощность множества M_1 равна l, не превосходит $l!$. Значит

$$|V_l(n)| \leqslant C_n^l l! n^l (n-l)^{2(n-l)} = n(n-l)...(n-l+1)n^l(n-l)^{2(n-l)} \leqslant \leqslant n^{2l}(n-l)^{2(n-l)}.$$

И, следовательно, утверждение доказано.

Утверждение 8. *Справедливо*

$$\lim_{n\to\infty} \frac{|\bigcup_{l=2}^n V_l(n)|}{n^{2n}} \leqslant \frac{1}{e^4\left(1-\frac{1}{e^2}\right)}.$$

Доказательство. В силу утверждения 7

$$\frac{|V_l(n)|}{n^{2n}} \leqslant \frac{n^{2l}(n-l)^{2(n-l)}}{n^{2n}} = \frac{(n-l)^{2(n-l)}}{n^{2(n-l)}} = \frac{\left(1-\frac{l}{n}\right)^{2n}}{\left(1-\frac{l}{n}\right)^{2l}} \leqslant \frac{\left(1-\frac{l}{n}\right)^{2n}}{\left(1-\frac{2}{n}\right)^4}.$$

$$\frac{|\bigcup_{l=2}^n V_l(n)|}{n^{2n}} \leqslant \frac{\sum_{l=2}^n |V_l(n)|}{n^{2n}} \leqslant \frac{1}{\left(1-\frac{2}{n}\right)^4} \cdot \sum_{l=2}^n \left(1-\frac{l}{n}\right)^{2n} \leqslant$$

$$\leqslant \frac{1}{\left(1-\frac{2}{n}\right)^4} \cdot \sum_{l=2}^n \frac{1}{e^{2l}} \leqslant \frac{1}{\left(1-\frac{2}{n}\right)^4} \cdot \frac{1}{e^4\left(1-\frac{1}{e^2}\right)}.$$

И следовательно,

$$\lim_{n\to\infty} \frac{|\bigcup_{l=2}^n V_l(n)|}{n^{2n}} \leqslant \frac{1}{e^4\left(1-\frac{1}{e^2}\right)}.$$

Утверждение доказано.

Доказательство теоремы 2. Заметим, что

$$V_{NM}(n) = \bigcup_{2\leqslant l\leqslant n} V_l(n).$$

Следовательно $|V_{NM}(n)| \leqslant \sum_{2\leqslant l\leqslant n} |V_l(n)|$. Но тогда справедлива оценка

$$\lim_{n\to\infty} \frac{|V_{NM}(n)|}{n^{2n}} \leqslant \lim_{n\to\infty} \frac{\sum_{2\leqslant l\leqslant n} |V_l(n)|}{n^{2n}}.$$

В силу утверждения 8 этот предел не превосходит $\frac{1}{e^4\left(1-\frac{1}{e^2}\right)}$. Теорема доказана.

Перейдем теперь к доказательству Теоремы 3. Для доказательства этой теоремы построим достаточно широкий класс переходных систем, обладающих свойством максимальности, такой что отношение его мощности к числу всех переходных систем не менее

$$\frac{1}{2e^4}\left(1-\frac{1}{e^4\left(1-\frac{1}{e^2}\right)}\right).$$

Пусть задано множество $M = \{1, ..., n\}$. Рассмотрим следующие множества переходных систем. Для каждой пары $1 \leqslant i < j \leqslant n$ рассмотрим такие переходные системы, что они не обладают свойством максимальности на перестановке (ij), и для каждой переходной системы ее образующие не коммутируют одновременно с перестановкой σ, такой, что $\sigma(i) = i$, $\sigma(j) = j$ (то есть множество переходных систем, принадлежащих множеству $V_{(ij)}(n)$ и не принадлежащих множествам V_σ, для любой указанной перестановки σ). Обозначим это множество $V^{i,j}(n)$.

Утверждение 9. *Мощность множества* $|V^{i,j}(n)| = n^2|V_M(n-2)|$.

Доказательство. Заметим, из утверждения 5 следует, что число переходных систем с n состояниями, не обладающих свойством максимальности на перестановке (ij), равно $n^2(n-2)^{2(n-2)}$. Так как мы рассматриваем такие переходные системы, что они не обладают свойством максимальности на перестановке (ij), то порождающие каждой переходной системы, как видно из доказательства утверждения 2, сохраняют множество $M \setminus \{i, j\}$. А число переходных систем с $n-2$ состояниями, обладающих свойством максимальности равно $|V_M(n-2)|$. Отсюда сразу следует наше утверждение.

Утверждение 10. *Пусть* $\{i_1, i_2\} \cap \{j_1, j_2\} = \emptyset$. *Тогда*

$$V^{i_1,i_2}(n) \cap V^{j_1,j_2}(n) = \emptyset.$$

Доказательство. Утверждение сразу следует из определения множеств V^{i_1,i_2}, V^{j_1,j_2}.

Утверждение 11. $V^{i_1,i_2}(n) \cap V^{i_2,i_3}(n) \subset V_{(i_1 i_2 i_3)}(n)$.

Доказательство. Пусть переходная система принадлежит $V^{i_1,i_2}(n)$ $\cap V^{i_2,i_3}(n)$. Значит, ее порождающие коммутируют с перестановкой $(i_1 i_2)$ и перестановкой $(i_2 i_3)$, а следовательно и с их произведением.

Обозначим через $\hat{V}_l(n)$ множество переходных систем с n состояниями, не обладающих свойством максимальности только на некотором цикле $(i_1 \ldots i_l)$ (то есть переходные системы с n состояниями, принадлежащие только множеству $V_{(i_1 \ldots i_l)}(n)$, и не принадлежащие множествам $V_\sigma(n)$, для любой перестановки σ, отличной от цикла $(i_1 \ldots i_l)$).

Утверждение 12.

$$\hat{V}_2(n) = \bigcup_{1 \leqslant i < j \leqslant n} V^{i,j}(n) \setminus \bigcup_{1 \leqslant i < j < k \leqslant n} \Big(V^{i,j}(n) \cap V^{i,k}(n)\Big) \cup \Big(V^{i,j}(n) \cap V^{j,k}(n)\Big).$$

Доказательство. Действительно, пусть задана некоторая переходная система, которая не обладает свойством максимальности только на транспозиции (ij). Но это означает, что она принадлежит множеству $V^{i,j}(n)$ и не принадлежит ни одному пересечению вида $V^{i,j}(n) \cap V^{i,k}(n)$, либо $V^{i,j}(n) \cap V^{j,k}(n)$ $\forall k \neq i, j$ (в силу утверждения 11). Утверждение доказано.

Утверждение 13. *Для мощности множества* $\hat{V}_2(n)$ *справедлива оценка*

$$|\hat{V}_2(n)| \geqslant \frac{n(n-1)}{2} n^2 |V_M(n-2)| - 2n^{2n-1}.$$

Доказательство.

$$\Big| \bigcup_{1 \leqslant i < j \leqslant n} V^{i,j}(n) \Big| \geqslant$$

$$\geqslant \sum_{1 \leqslant i < j \leqslant n} |V^{i,j}(n)| - \sum_{1 \leqslant i < j < k \leqslant n} |V^{i,j}(n) \cap V^{j,k}(n)| - \sum_{1 \leqslant i < j < k \leqslant n} |V^{i,j}(n) \cap V^{i,k}(n)|.$$

Следовательно

$$|\hat{V}_2(n)| \geqslant \sum_{1 \leqslant i < j \leqslant n} |V^{i,j}(n)| - \sum_{1 \leqslant i < j < k \leqslant n} |V^{i,j}(n) \cap V^{j,k}(n)| - \sum_{1 \leqslant i < j < k \leqslant n} |V^{i,j}(n) \cap V^{i,k}(n)|.$$

Мощность каждого множества пересечений не превосходит мощности множества $V_3(n)$. Но как видно из утверждения 5 $|V_3(n)| \leqslant n^{2n-1}$. Используя утверждение 9, получаем доказываемую оценку.

Доказательство теоремы 3. Так как $|V_{NM}| \geqslant |\hat{V}_2(n)|$, то

$$\lim_{n\to\infty} \frac{|V_{NM}(n)|}{n^{2n}} \geqslant \lim_{n\to\infty} \frac{|\hat{V}_2(n)|}{n^{2n}} \geqslant \lim_{n\to\infty} \frac{\frac{n(n-1)}{2} n^2 |V_M(n-2)|}{n^{2n}} - \lim_{n\to\infty} \frac{2n^{2n-1}}{n^{2n}}.$$

Но $\frac{2n^{2n-1}}{n^{2n}} = \frac{2}{n}$, а эта последовательность стремится к 0 при $n \to \infty$.

$$\lim_{n\to\infty} \frac{\frac{n(n-1)}{2} n^2 |V_M(n-2)|}{n^{2n}} = \lim_{n\to\infty} \frac{1}{2} \frac{n^3(n-1)(n-2)^{2(n-2)}}{n^{2n}} \frac{|V_M(n-2)|}{(n-2)^{2(n-2)}} =$$

$$= \lim_{n\to\infty} \frac{1}{2}\left(1-\frac{1}{n}\right) \frac{\left(1-\frac{2}{n}\right)^{2n}}{\left(1-\frac{2}{n}\right)^4} \frac{|V_M(n-2)|}{(n-2)^{2(n-2)}} =$$

$$= \lim_{n\to\infty} \frac{1}{2}\left(1-\frac{1}{n}\right) \frac{\left(1-\frac{2}{n}\right)^{2n}}{\left(1-\frac{2}{n}\right)^4} \lim_{n\to\infty} \frac{|V_M(n-2)|}{(n-2)^{2(n-2)}} \geqslant$$

$$\geqslant \frac{1}{2e^4}\left(1 - \frac{1}{e^4\left(1-\frac{1}{e^2}\right)}\right).$$

Это означает, что

$$\lim_{n\to\infty} \frac{|V_{NM}(n)|}{n^{2n}} \geqslant \frac{1}{2e^4}\left(1 - \frac{1}{e^4\left(1-\frac{1}{e^2}\right)}\right).$$

Теорема доказана.

В заключение автор выражает благодарность профессору С.В. Алёшину, под руководством которого выполнена данная работа.

Список литературы

[1] Кудрявцев В.Б., Алёшин С.В., Подколзин А.С. Введение в теорию автоматов. М.: Наука, 1985.

[2] Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. М.: Наука, 1982.

[3] Арбиб М.А. Декомпозиция автоматов и расширение полугрупп // Арбиб М.А. Алгебраическая теория автоматов, языков и полугрупп. М.: Статистика, 1975. С. 46–63.

Об одной модели оптимального рыночного поведения фирмы

А.Н. Сафиуллин

Предлагается модель фирмы, функционирующей в условиях рынка, и изучается такое ее поведение, которое позволяет ей максимизировать прибыль на заданном временном интервале.

Введение

Одной из общих моделей кибернетики является рассмотрение объектов, находящихся в среде и способных реагировать на нее. Рассмотренное во времени такое реагирование под влиянием среды считают поведением объекта в среде; оно может быть оценено с помощью некоторых критериев. Тем самым возникает задача выявления такого поведения, которое является оптимальным по указанным критериям.

Эта общая ситуация имеет много интерпретаций. Например, можно рассматривать реальную фирму в рыночных условиях как объект в среде. Процесс взаимодействия фирмы со средой управляем как фирмой, так и средой. Критерий такого поведения – учет взаимных «интересов», и акцентируемый на интересах фирмы он может означать стремление ее к максимальной прибыли на данном временном интервале.

В работе формализуются понятия фирмы и среды, вводятся конкретные критерии целесообразного поведения фирмы в среде и явно указываются ее оптимальные стратегии с вычислением доходов.