О порядке элемента в группе автоматных подстановок

Н. Г. Бокк

Построена серия групповых автоматов конечных порядков вида 2^n. Для автоматов с абелевой внутренней группой приведен критерий определения порядка по строению группы. Показана невозможность такого критерия для произвольной внутренней группы.

Ключевые слова: автоматные подстановки, групповые автоматы, внутренняя полугруппа, порядок автомата.

1. Введение

Одной из центральных проблем теории автоматов является задача определения порядка автомата как элемента группы AS_2 автоматных подстановок [1, 3]. На сегодняшний день не известно общего алгоритма нахождения порядка, более того, даже для фиксированных автоматов с небольшим числом состояний определение порядка оказывается очень сложной вычислительной задачей. В данной работе мы будем рассматривать важный подкласс групповых автоматов в AS_2. Мы покажем, что в этом классе конечность порядка накладывает дополнительные ограничения на строение автоматов, что позволяет в отдельных случаях определить порядок по порождающим внутренней группы. Также мы построим для каждого порядка, допустимого для автомата из AS_2, групповой автомат такого порядка. Тем самым, мы продемонстрируем, что выбранный подкласс так же богат элементами различных порядков, как и вся группа AS_2.

2. Основные определения и результаты

Под термином автомат мы будем подразумевать инициальный связный приведенный автомат $\mathfrak{a} = (\{0,1\}, Q, \{0,1\}, \hat{\phi}, \hat{\psi}, q_0)$ с входным и выходным алфавитами $\{0,1\}$, реализующий в каждом состоянии функцию не выпускающую значений. Условимся обозначать множество состояний автомата $\mathfrak{a}$ за Q, функцию перехода по 0 за $\tau_0 = \hat{\phi}(q,0)$, по 1 за $\tau_1 = \hat{\phi}(q,1)$ и функцию выхода состояния q за $\psi(q) = \hat{\psi}(q,x)$, $\psi(q) \in \{x, \overline{x}\}$. В качестве внутренней полугруппы автомата будем рассматривать полугруппу подстановок на множестве Q, порождённую τ_0, τ_1. Обозначим класс групповых автоматов в AS_2, то есть таких, для которых внутренняя полугруппа является группой, за A. Будем говорить, что автомат $\mathfrak{a}$ реализует группу G, если $G(\mathfrak{a}) \cong G$, где под $G(\mathfrak{a})$ понимается внутренняя полугруппа $\mathfrak{a}$.

В группе AS_2 для каждого автомата $\mathfrak{a}$ существует обратный, который обозначим через $\mathfrak{a}^{-1}$. В множестве групповых автоматов A рассмотрим подмножество H тех автоматов, для которых обратный также групповой. Множество H является подгруппой в AS_2, доказательство этого утверждения сводится к проверке, что произведение двух групповых автоматов дает групповой автомат, см. [1].

Для нашего исследования важно, что все групповые автоматы конечного порядка необходимо лежат в H, а для автоматов этой подгруппы выполнено следующее ограничение на функции выхода.

Утверждение 1. *Если $\mathfrak{a} \in A$, то $\mathfrak{a} \in H$ равносильно тому, что для любого состояния q автомата $\mathfrak{a}$ выполнено $\psi(\tau_0^{-1}(q)) = \psi(\tau_1^{-1}(q))$.*

Ключевым моментом является рассмотрение действия циклической группы $<\tau_0^{-1}\tau_1>$ на множестве состояний автомата. Из утв. 1 следует, что для каждого автомата из H все состояния произвольной орбиты указанного действия реализуют одну и ту же функцию выхода.

Определение. Орбитой $\mathcal{O}$ состояния $q \in Q$ автомата $\mathfrak{a}$ назовем множество $\{(\tau_0^{-1}\tau_1)^k(q), k \in \mathbb{N}\}$, то есть орбиту действия $<\tau_0^{-1}\tau_1> \,: Q$.

Утверждение 2. *Если $\mathfrak{a} \in A$, то $\mathfrak{a} \in H$ равносильно тому, что для каждой орбиты $\mathcal{O}$ автомата $\mathfrak{a}$: $q_1, q_2 \in \mathcal{O} \Rightarrow \psi(q_1) = \psi(q_2)$.*

При доказательстве основных результатов мы будем активно использовать строение орбит, а так же их взаимное «расположение», для наглядности пояснений условимся называть множество состояний, достижимых из орбиты за один такт времени, *слоем* над орбитой. Или более формально, с учетом того, что $\tau_1(\mathcal{O}) = \tau_0(\mathcal{O})$:

Определение. Слоем над орбитой $\mathcal{O}$ назовём множество состояний $\tau_1(\mathcal{O}) = \{q \in Q | \ \tau_1^{-1}(q) \in \mathcal{O}\}$.

Для автоматов с абелевой внутренней группой слой над орбитой всегда сам является орбитой, отсюда можно извлечь простой критерий определения порядка по группе.

Теорема 1. *Автомат $\mathfrak{a}$, реализующий абелеву группу в качестве внутренней, имеет бесконечный порядок для произвольной не циклической группы. Для циклической группы, при условии, что $G(\mathfrak{a}^{-1})$ является группой, — порядок 2, иначе — бесконечность.*

В некотором смысле завершает исследование автоматов с абелевой внутренней группой следующее утверждение.

Теорема 2. *Любая нетривиальная абелева группа с не более чем двумя порождающими может быть реализована как внутренняя группа автомата из $A \backslash H$.*

Необходимость рассмотрения $G(\mathfrak{a}^{-1})$, возникшая в случае с циклической группой, характерна для любой группы, которая реализуется автоматом конечного порядка.

Теорема 3. *Любая нетривиальная группа, имеющая реализацию в H, имеет реализацию в $A \backslash H$.*

Как следствие теоремы 3 мы получаем, что любая нетривиальная группа, имеющая реализацию автоматом конечного порядка (который неизбежно попадет в H), имеет так же реализацию автоматом из $A \backslash H$, то есть заведомо бесконечного порядка.

Этот факт не позволяет нам только по внутренней группе $G(\mathfrak{a})$ определить порядок автомата. С другой стороны, проверка условия принадлежности автомата к H не требует вычислительных затрат, так как процедура обращения автомата в AS_2 очень проста. Основная

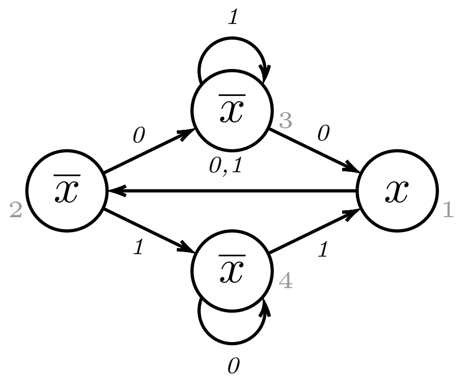

Рис. 1.

сложность заключается в том, что элементы бесконечного порядка содержатся также и в H.

То есть для конечности порядка $\mathfrak{a}$ не достаточно того, чтобы $G(\mathfrak{a})$ и $G(\mathfrak{a}^{-1})$ были группами. Более того, даже если мы фиксируем конкретные представления этих групп в S_n и конкретные пары их порождающих, всё равно это не позволит однозначно определить порядок $\mathfrak{a}$. Пример такого автомата представлен на рис. 1.

Для изображенного автомата $\mathfrak{a}$ порядок зависит от начального состояния:

$$\mathrm{ord}(\mathfrak{a}_1) = \mathrm{ord}(\mathfrak{a}_2) = 2, \quad \mathrm{ord}(\mathfrak{a}_3) = \mathrm{ord}(\mathfrak{a}_4) = \infty,$$

хотя совершенно ясно, что никакие внутренние групповые структуры не изменяются при смене начального состояния.

В целом группа H, а с ней и групповые автоматы, не уступает объемлющей AS_2 по разнообразию возможных порядков элементов. Известным результатом для AS_2 является тот факт, что в этой группе есть автомат порядка 2^n для произвольного целого неотрицательного n, и другие конечные порядки недопустимы, см. [1]. Для H выполнено аналогичное утверждение.

Теорема 4. *Для произвольного натурального n существует групповой автомат $\mathfrak{a}_n$ порядка 2^n с $n \cdot 2^{n-1}$ состояниями.*

3. Строение автоматов из H

В первую очередь нас интересует строение автоматов конечного порядка. Все они лежат в H (и наследуют особенности структуры), так как автомат $\mathfrak{a}^{\operatorname{ord}\mathfrak{a}-1}$ как композиция групповых сам групповой и $\mathfrak{a}^{\operatorname{ord}\mathfrak{a}-1} \cong \mathfrak{a}^{-1}$.

Строение автоматов из H описано в утв. 1 и 2. Напомним процедуру обращения автомата в AS_2, которую мы будем использовать в доказательствах: изменяются только переходы из состояний, реализующих на выходе отрицания, переход по 0 становится переходом по 1 и наоборот. Функции переходов и выхода, а так же состояния полученного автомата $\mathfrak{a}^{-1}$, будем обозначать штрихами.

Доказательство утверждения 1. Необходимость докажем от противного. Предположим, что найдутся состояния q_0, q_1 автомата $\mathfrak{a}$ такие, что $\tau_0(q_0) = \tau_1(q_1)$, но $\psi(q_0) \neq \psi(q_1)$. Пусть $\psi(q_0) = \bar{x}$, а $\psi(q_1) = x$. При обращении изменятся функции переходов из q_0, но переходы из q_1 останутся прежними. Значит, для состояний q_0', q_1' автомата $\mathfrak{a}^{-1}$ будет выполнено $\tau_1'(q_0') = \tau_1'(q_1')$, то есть в $\mathfrak{a}^{-1}$ происходит склейка по 1. Заметим, что если $\mathfrak{a} \in H$, то по определению $\mathfrak{a}^{-1} \in A$, где склейки недопустимы. Таким образом, мы получили противоречие с тем, что $\mathfrak{a}^{-1}$ групповой.

В обратную сторону, при выполнении указанного условия легко видеть, что при обращении не возникает склеек — это и означает, что полученный автомат групповой.

Доказательство утверждения 2. Покажем, что утв. 2 эквивалентно утв. 1. Состояния q_0, q_1, для которых $\tau_0(q_0) = \tau_1(q_1)$, лежат в одной орбите, поэтому выполнение условия утв. 2 влечет выполнение условия утв. 1. Обратно, рассмотрим произвольное q из некоторой орбиты $\mathcal{O}$. Тогда выполнение условия утв. 1 дает равенство $\psi(q) = \psi(\tau_0^{-1}\tau_1(q))$, применяя его k раз, получим $\psi(q) = \psi((\tau_0^{-1}\tau_1)^k(q))$, где k — порядок циклической группы $<\tau_0^{-1}\tau_1>$. Таким образом мы обойдем всю орбиту $\mathcal{O}$ и получим, что во всех её состояниях реализуется функция $\psi(q)$.

4. Строение автомата с абелевой внутренней группой

В этом разделе мы покажем специфику строения автомата, реализующего абелеву группу G, и докажем теоремы 1 и 2. Везде под абелевой группой будем понимать абелеву группу с не более чем двумя порождающими.

4.1. Порядок автомата с абелевой внутренней группой

Покажем, что из абелевых групп только циклические имеют реализацию автоматами конечного порядка.

Лемма 1. *Для любой орбиты $\mathcal{O}$ автомата, реализующего абелеву G, выполнено, что слой над $\mathcal{O}$ сам является орбитой.*

Доказательство. Рассмотрим произвольное $q \in \mathcal{O}$. Из условия коммутативности операции в G следует, что $(\tau_0^{-1}\tau_1)\tau_0(q) = \tau_1(q)$, значит, $\tau_0(q)$ и $\tau_1(q)$ — «соседние» элементы слоя над орбитой $\mathcal{O}$ — лежат в одной орбите. Двигаясь по орбите $\mathcal{O}$, мы обойдем и весь слой над ней и получим, что все его состояния составляют орбиту (не обязательно отличную от $\mathcal{O}$).

Лемма 2. *Для любой реализации $\mathfrak{a} \in H$ циклической группы G выполнено* $\mathrm{ord}(\mathfrak{a}) = 2$*, для остальных абелевых групп нет реализации в группе H.*

Доказательство. Пусть автомат $\mathfrak{a} \in H$ реализует абелеву группу G. Рассмотрим произвольную орбиту $\mathcal{O}(\mathfrak{a})$. Покажем, что все состояния $\mathcal{O}$ неотличимы. Пусть $q_1, q_2 \in \mathcal{O}$. Заметим, что для любой входной последовательности α выполнено, что $\alpha(q_1), \alpha(q_2)$ попадут в одну орбиту (применим k раз лемму 1, где k — длина α). Так как $\mathfrak{a} \in H$, по утв. 2 $\psi(\alpha(q_1)) = \psi(\alpha(q_2))$ для произвольной конечной α, что и означает неотличимость q_1 и q_2. Таким образом, каждая орбита $\mathfrak{a}$ состоит ровно из одного состояния, так как мы рассматриваем только приведенные автоматы. Равенство $q = \mathcal{O}_q$ означает, что из q осуществляется безусловный переход. Приведенный автомат из A с более чем одним состоянием, со всеми безусловными переходами имеет порядок 2. Заметим, что для такого автомата $\tau_0 = \tau_1$, то есть внутренняя группа $G(\mathfrak{a}) =< \tau_0, \tau_1 >\cong< \tau_0 >$ циклическая. Итак, если предположить, что для не циклической абелевой G есть реализация в H, мы придем к противоречию, так как в не циклической группе заведомо выполнено $\tau_0 \neq \tau_1$, это завершает доказательство леммы.

Доказательство теоремы 1. По лемме 2 не циклические группы не имеют реализации в H, что означает, что любая реализация такой группы окажется в $A\backslash H$ и будет иметь бесконечный порядок. Для реализации циклической группы, лежащей в H, по той же лемме порядок равен двум. Осталось заметить, что в формулировке теоремы в явном виде указано условие принадлежности к H, то есть $G(\mathfrak{a}^{-1})$ является группой.

4.2. Реализация абелевой группы автоматом бесконечного порядка

Доказательство теоремы 2. Для циклической группы $\mathbb{Z}_n$ построим автомат с n состояниями: достаточно взять цикл длины n за τ_0, положить $\tau_1 = e$ и приписать отрицание ровно одному состоянию. Для абелевой группы G с двумя порождающими τ, σ выполнено $G \cong< \tau >_k \oplus < \sigma >_m$, где за k, m обозначены порядки τ, σ в G соответственно. Доказательство этого факта можно найти в [2]. Дальше мы рассмотрим множества Q_i, $i = \overline{1, k}$ по m состояний в каждом и соединим их так, чтобы они стали орбитами и чтобы слой над орбитой $\mathcal{O}_i$ совпадал с $\mathcal{O}_{i+1}$ при $i < k$ и слой над $\mathcal{O}_k$ совпадал с $\mathcal{O}_1$. Так же припишем одному произвольному состоянию отрицание. Заметим, что полученный автомат $\mathfrak{a}$ неприводим, так как для групповых автоматов приводимость означает, что у каждого состояния есть хотя бы одно неотличимое от него. Поскольку у нас только одно состояние, которому приписано отрицание, неотличимых от него в $\mathfrak{a}$ нет.

5. Связь реализаций группы автоматами из H и $A\backslash H$

На примере абелевых не циклических групп мы увидели, что группа может иметь реализацию в $A\backslash H$, но не иметь реализации в H. Покажем, что обратная ситуация невозможна. Как уже отмечалось, это означает, что внутренняя группа произвольного автомата конечного порядка, если она нетривиальна, имеет реализацию автоматом бесконечного порядка.

Доказательство теоремы 3. Рассмотрим автомат $\mathfrak{a} \in H$, реализующий некоторую группу G с порождающими τ_0, τ_1. Пронумеруем состояния и зафиксируем функции выхода, дальше будем менять только функции перехода между состояниями. Пусть $\mathfrak{a}_0$ — автомат с функциями перехода $\sigma_0 = \tau_1^{-1}\tau_0^{-1}$, $\sigma_1 = \tau_1^{-1}$. Заметим, что $\mathfrak{a}_0$ неприводим. Действительно, пусть q_1^0, q_2^0 — произвольные два состояния $\mathfrak{a}_0$. Предъявим различающую последовательность. Рассмотрим соответствующие состояния q_1, q_2 в исходном автомате $\mathfrak{a}$. Он неприводим, поэтому для q_1, q_2 существует различающая последовательность

$$\alpha = \tau_0^{k_1}\tau_1^{l_1}\dots\tau_0^{k_m}\tau_1^{l_m},\ k_i, l_i \in \mathbb{N}\cup\{0\},\ m \in \mathbb{N},\ i = \overline{1,m}.$$

Исходя из того, что $\sigma_0^{-1}\sigma_1 = (\tau_0^{-1})^{-1}(\tau_1^{-1})^{-1}\tau_1^{-1} = \tau_0$ и $\sigma_1^{-1} = \tau_1$, получим различающую последовательность α_1 для q_1^1, q_2^1

$$\alpha_1 = (\sigma_0^{-1}\sigma_1)^{k_1}(\sigma_1^{-1})^{l_1}\dots(\sigma_0^{-1}\sigma_1)^{k_m}(\sigma_1^{-1})^{l_m}.$$

Полученный автомат $\mathfrak{a}_0$ реализует ту же группу G, что и $\mathfrak{a}$, так как мы выразили порождающие групп $G(\mathfrak{a})$ и $G(\mathfrak{a}_0)$ друг через друга. Если $\mathfrak{a}_0 \in A\backslash H$, то наше утверждение доказано. Иначе $\mathfrak{a}_0 \in H$ и по утв. 2 все состояния каждой из орбит $\mathfrak{a}_0$ реализуют одинаковые функции. Покажем, что орбита $\mathcal{O}_{q^0}$ состояния q^0 в $\mathfrak{a}_0$ совпадает с циклом в $\mathfrak{a}$ по 0, содержащим q. Действительно, $<\sigma_0^{-1}\sigma_1>=<\tau_0>$, значит, и действия этих групп на Q совпадают. Тогда получим, что в исходном автомате $\mathfrak{a}$ все циклы по 0 состоят из состояний с одинаковым выходом. Аналогично можно построить автомат $\mathfrak{a}_1$ с функциями перехода $\kappa_0 = \tau_0^{-1}\tau_1^{-1}$, $\kappa_1 = \tau_0^{-1}$. Если $\mathfrak{a}_1 \in H$, то в исходном автомате $\mathfrak{a}$ все циклы по 1 состоят из состояний с одинаковым выходом.

Исходный автомат $\mathfrak{a}$ связный и групповой, значит, любое его состояние достижимо из начального по некоторой последовательности символов. Если оба автомата $\mathfrak{a}_0, \mathfrak{a}_1$ лежат в H, переход по любому символу в $\mathfrak{a}$ не изменяет функции выхода. Получим, что в $\mathfrak{a}$ все состояния реализуют одну и ту же выходную функцию и неотличимы, значит, состояние ровно одно и $G(\mathfrak{a}) = e$. По условию $G \neq e$ и мы получили противоречие с тем, что $\mathfrak{a}_0, \mathfrak{a}_1 \in H$. Значит, один из построенных автоматов $\mathfrak{a}_0, \mathfrak{a}_1$ даст реализацию G автоматом из $A \backslash H$.

6. Построение группового автомата конечного порядка

В данном разделе мы дадим конструктивное доказательство теоремы 4 и построим групповой автомат порядка 2^n для произвольного натурального n.

6.1. Процедура построения

Автоматы $\mathfrak{a}_n$ будут обладать следующими свойствами:

1) множество состояний Q автомата $\mathfrak{a}_n$ разбивается на n подмножеств — уровней — таких, что в момент времени t автомат обязательно находится в состоянии уровня $t(\operatorname{mod} n)$ (для удобства будем считать, что указанная функция принимает значения от 1 до n).
2) В каждом уровне по 2^{n-1} состояний.
3) Уровень, соответствующий моменту времени m, где $1 \leqslant m \leqslant n$, состоит из 2^{m-1} орбит по 2^{n-m} состояний в каждой.

Все перечисленные свойства относятся к структуре переходов автомата. Поясним сначала индуктивную процедуру построения такой структуры безотносительно функций выхода.

В качестве $\mathfrak{a}_1$ возьмем автомат с одним состоянием, с безусловным переходом из него в себя. Все три условия для него выполнены.

Зададим на базе $\mathfrak{a}_n$ переходы для $\mathfrak{a}_{n+1}$. Возьмем два экземпляра структуры автомата $\mathfrak{a}_n$, обладающего указанными свойствами, второй экземпляр обозначим $\mathfrak{a}'_n$. Также возьмем 2^n состояний, из которых сформируем «нулевой» уровень автомата $\mathfrak{a}_{n+1}$.

Первый уровень каждого из автоматов $\mathfrak{a}_n$ и $\mathfrak{a}'_n$ состоит из одной орбиты с 2^{n-1} состояниями. Так как мы рассматриваем орбиты действия циклической группы $<\tau_0^{-1}\tau_1>$ то все состояния одной орбиты могут быть естественным образом «упорядочены» в порядке обхода, то есть можно считать следующим по орбите за q элемент $(\tau_0^{-1}\tau_1)(q)$. Занумеруем числами от 1 до 2^{n-1} состояния орбит первых уровней автоматов $\mathfrak{a}_n, \mathfrak{a}'_n$ в соответствии с этим «порядком», начиная с произвольного состояния в каждой орбите.

Мы хотим подключить между уровнями 1 и n автоматов $\mathfrak{a}_n, \mathfrak{a}'_n$ новые состояния, поэтому разорвем переходы, ведущие с последнего уровня на первый. Новые переходы на первый уровень из добавленных состояний установим, как изображено на рис. 2.

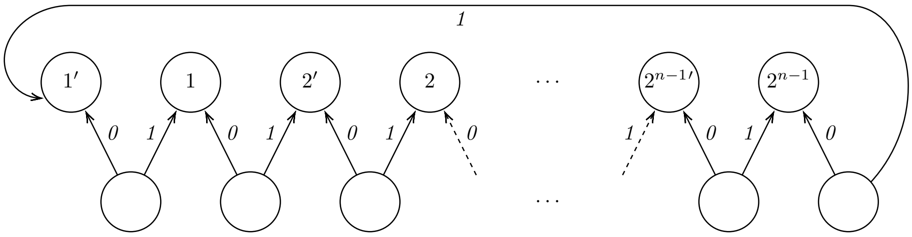

Рис. 2.

Теперь все добавленные состояния образуют одну орбиту длины 2^n, а в слое над ней лежат две орбиты первых уровней автоматов $\mathfrak{a}_n$ и $\mathfrak{a}'_n$, причём их состояния в слое чередуются. Будем изображать такое соединение, как показано на рис. 3, указывая количество состояний в орбитах.

Определим переходы из последнего уровня автоматов $\mathfrak{a}_n, \mathfrak{a}'_n$ в новую орбиту. Положим безусловный переход из каждого состояния q уровня n в состояние $\tau_1^{-n}(q)$. Это действительно состояние нового, «нулевого», уровня, так как каждый шаг против направления перехода переводит нас на уровень ниже. В качестве начального выберем произвольное состояние «нулевого» уровня. Мы завершили построение автомата $\mathfrak{a}_{n+1}$ и легко видеть, что для него все указанные усло-

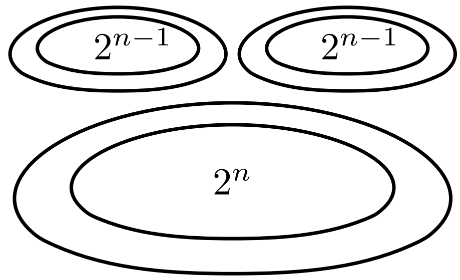

Рис. 3.

вия выполнены. Начав с $\mathfrak{a}_1$ с одним состоянием, для $\mathfrak{a}_n$ мы получим структуру, изображенную на рис. 4 справа.

Для автомата $\mathfrak{a}_n$ осталось определить функции выхода для каждой орбиты и зафиксировать в качестве начального одно из состояний первого уровня. Сделаем это следующим образом: рассмотрим путь по тождественной единице длины n из начального состояния и припишем отрицания только тем орбитам, через которые пройдет этот путь. На каждом уровне тогда будет ровно одна орбита, реализующая отрицание. Полученный автомат изображен на рис. 4 слева (закрашены орбиты, реализующие отрицание). Ниже мы покажем, что его порядок равен 2^n.

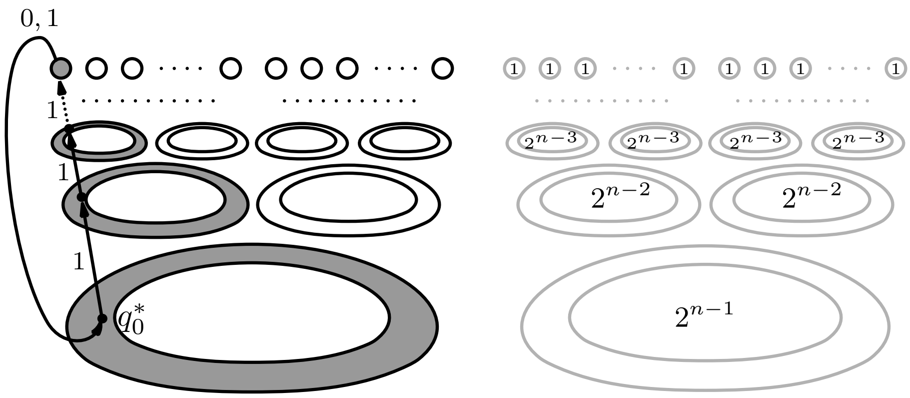

Рис. 4.

6.2. Доказательство корректности построенного примера

Докажем, что степень автомата $\mathfrak{a}_n$ действительно 2^n. Покажем сначала, что выполнено неравенство $\mathrm{ord}(\mathfrak{a}_n) \leqslant 2^n$, а затем, что степени $\mathfrak{a}_n$ меньшие 2^n не дадут тождественную функцию выхода.

Лемма 3. *Для любой орбиты $\mathcal{O}$ уровня m автомата $\mathfrak{a}_n$, где $1 < m \leqslant n$, на каждом более низком уровне есть ровно одна орбита, из которой можно подняться в $\mathcal{O}$, не осуществляя переходов с уровня n на уровень 1.*

Доказательство. Утверждение совершенно ясно из способа построения: все переходы, которые ведут в произвольную орбиту, исходят только из одной орбиты предыдущего уровня. Это правило нарушается только для орбиты первого уровня, но мы запретили переходы последнего уровня на первый.

Лемма 4. *Если для некоторой последовательности входных символов α длины m и двух состояний q_1, q_2 выполнено, что $\alpha(q_1), \alpha(q_2)$ попадают в одну орбиту $\mathcal{O}$ (при том, что мы не совершаем перехода с последнего уровня $\mathfrak{a}_n$ на первый), тогда для произвольной последовательности β длины не превышающей m образы состояний $\beta(q_1), \beta(q_2)$ попадут в одну орбиту.*

Доказательство. Состояния q_1, q_2 находятся на одном уровне k, иначе по последовательности α они бы попадали на разные уровни, а значит, и в разные орбиты. По лемме 3 мы можем заключить, что q_1, q_2 лежат в одной орбите, а также, что по начальному участку α длины $l \leqslant m$ будет осуществлен переход в некоторую орбиту, общую для q_1, q_2, ведь на уровне $k + l$ тоже только одна орбита, из которой можно попасть в $\mathcal{O}$, либо же это и есть $\mathcal{O}$.

Расстояние по орбите между состояниями q_1, q_2 на каждом шаге (пока их образы продолжают попадать в одну орбиту) уменьшается вдвое. Достаточно вернуться к рис. 2, где показан способ соединения орбит в $\mathfrak{a}_n$. Мы можем совершить m переходов вверх, без расхождения в разные орбиты, значит, расстояние между q_1, q_2 кратно 2^m. Осталось заметить, что верно и обратное: если расстояние по орбите между состояниями четно, то при переходе по любому символу (но общему для двух состояний) они остаются в одной орбите.

Таким образом, нам безразлично, какую последовательность β мы будем синхронно подавать на наши состояния: пока её длина не превышает m, расстояние между образами исходных состояний остается четным и нет расхождения в две орбиты, лемма доказана.

Лемма 5. *Для каждого состояния q автомата $\mathfrak{a}_n$, следуя по произвольному пути из q по направлению переходов, проходя в первый раз через первый уровень, мы окажемся в состоянии q_1, из которого по тождественной единице можно подняться в орбиту $\mathcal{O}$, содержащую q.*

Доказательство. Отступим на шаг назад из состояния первого уровня q_1, на уровень n, обозначим состояние, в которое мы попали за q_n. Раз мы попали в q_n из q, значит, в q_n можно подняться из орбиты $\mathcal{O}$. По лемме 3 любой путь с первого уровня в q_n пройдет через эту орбиту. С другой стороны, из q_n мы по определению $\mathfrak{a}_n$ переходим в такое состояние первого уровня, из которого по тождественной единице можем подняться в q_n, то есть из q_1 ведет путь по тождественной единице в q_n и он неизбежно проходит через орбиту $\mathcal{O}$, это и утверждает лемма.

Перейдем теперь к рассмотрению степеней автомата $\mathfrak{a}_n$. Заметим, что произвольная степень $\mathfrak{a}_n$ сохраняет уровневую структуру. Действительно, каждое состояние автомата $\mathfrak{a}_n^m$ может быть представлено как последовательность из m состояний $\mathfrak{a}_n$, при этом в момент времени t все эти m состояний будут из уровня $t (\operatorname{mod} n)$.

Лемма 6 (основная). *У автомата $\mathfrak{a}_n^{2^k}$, $k \leqslant n$, нет отрицаний на уровнях $1, \ldots, k$.*

Доказательство. Проведем доказательство индукцией по параметру k. Будем задавать состояние q автомата $\mathfrak{a}_n^{2^k}$ последовательностью состояний $q_1, \ldots, q_{2^k}$ автомата $\mathfrak{a}$, причем $\psi'(q) = \psi(q_1) \cdot \dots \cdot \psi(q_{2^k})$, где ψ' — функция выхода $\mathfrak{a}_n^{2^k}$.

База индукции: $k = 2$. Любое состояние $\mathfrak{a}_n^2$ первого уровня реализует композицию двух отрицаний, то есть тождественную функцию, так как на первом уровне $\mathfrak{a}_n$ по построению все состояния реализуют отрицание.

Пусть наше утверждение доказано для $k = m$, покажем, что у $\mathfrak{a}_n^{m+1}$ нет отрицаний на первых $m+1$ уровнях. Заметим, что $\mathfrak{a}_n^{2^{m+1}} = (\mathfrak{a}_n^{2^m})^2$, значит, на первых m уровнях автомата $\mathfrak{a}_n^{2^{m+1}}$ реализуются композиции двух тождественных функций. Осталось показать, что нет отрицаний на уровне $m+1$.

Начальное состояние автомата $\mathfrak{a}_n^{2^{m+1}}$ задается следующим образом:

$$\underbrace{q_0 \cdots q_0}_{2^m} \underbrace{q_0 \cdots q_0}_{2^m}.$$

При прохождении первых m уровней на вход второго множества из 2^m состояний будет подаваться тот же символ, что и на вход первого, опять же по той причине, что у $\mathfrak{a}^{2^m}$ нет отрицаний на первых m уровнях. Две половины набора состояний в начальный момент времени идентичны. По указанному свойству они останутся идентичны и до момента времени $m+1$ включительно. Значит, при первом попадании на уровень $m+1$ реализуется тождественная функция выхода:

$$\psi(q_{2^m}) \cdot \cdots \cdot \psi(q_1) \cdot \psi(q_{2^m}) \cdot \cdots \cdot \psi(q_1) = (\psi(q_{2^m}))^2 \cdot \cdots \cdot (\psi(q_1))^2 = x.$$

Однако дальше возможно расхождение и при следующем прохождении через уровень $m+1$ половины состояний не будут совпадать. Для нас существенно, чтобы каждая функция выхода, входящая в композицию, встречалась в ней дважды. Покажем, что на уровне $m+1$ для двух половин состояний:

$$\underbrace{q_1 \ldots q_{2^m}}_{2^m} \underbrace{q'_1 \ldots q'_{2^m}}_{2^m}$$

всегда выполнено, что q_i и q'_i, где $1 \leqslant i \leqslant 2^m$, лежат в одной орбите. Это обеспечит равенство $\psi(q_i) = \psi(q'_i)$, а вместе с тем и тождественный общий выход автомата $\mathfrak{a}_n^{2^{m+1}}$ на уровне $m+1$.

Проследим за парой состояний, расположенных на позиции i в обеих половинах. В момент первого попадания на уровень $m+1$ эти состояния идентичны, значит, лежат в одной орбите, обозначим её $\mathcal{O}$. При прохождении на первый уровень по лемме 5 мы попадем в q_j, q_s

такие, что из каждого можно подняться по тождественной единице в $\mathcal{O}$. К полученной паре состояний можно применить лемму 4, взяв в качестве α последовательность 1^m. Это означает, что для любой последовательности β длины не превышающей m из q_j, q_s мы поднимемся в одну орбиту.

Покажем, что на уровне не выше m на вход i-го состояния обеих половин попадает один и тот же символ. Представим $\mathfrak{a}_n^{2^{m+1}}$ в виде $\mathfrak{a}_n^{i-1} \cdot \mathfrak{a}_n^{2^m} \cdot \mathfrak{a}_n^{2^m-i+1}$. Отсюда видно, что символ, поступающий на вход i-го состояния первой половины проходит перед попаданием на вход i-го состояния другой половины через автомат $\mathfrak{a}_n^{2^m}$, у которого нет отрицаний на нижних m уровнях. Значит, при любой входной последовательности γ на вход i-х состояний обеих половин будет подаваться $\mathfrak{a}_n^{i-1}(\gamma)$, и q_i, q_i', в которые мы поднимемся из q_j, q_s, будут лежать в одной орбите уровня $m+1$. Таким образом,

$$\psi(q'_{2^m}) \cdot \dots \cdot \psi(q'_1) \cdot \psi(q_{2^m}) \cdot \dots \cdot \psi(q_1) = (\psi(q_{2^m}))^2 \cdot \dots \cdot (\psi(q_1))^2 = x.$$

Заметим, что наши рассуждения можно повторить для новых состояний q_i, q_i' и получить, что из них мы через n шагов перейдём в два состояния, снова попадающие в одну орбиту. Значит, при каждом прохождении через уровень $m+1$ будет реализовываться тождественная функция выхода. Шаг индукции, а вместе с ним лемма, доказаны.

Следствие 1. $\mathfrak{a}_n^{2^n} = \mathrm{id}$.

Следствие означает, что порядок $\mathfrak{a}_n$ делит 2^n. Покажем теперь, что для любого порядка вида 2^k, где $k < n$, автомат $\mathfrak{a}_n^{2^k}$ не эквивалентен тождественному.

Лемма 7. *Пусть* $\alpha = \overline{\alpha_n \dots \alpha_1} = \underbrace{0\dots0}_{n}$, *тогда* $\mathfrak{a}_n^{2^k}(\alpha) = \underbrace{0\dots0}_{n-k-1} 1 \underbrace{0\dots0}_{k}$.

Доказательство. Покажем, что для любой двоичной последовательности входа $\alpha_1, \dots, \alpha_n$, не равной тождественной единице, и соответствующей ей последовательности выхода $\beta_1, \dots, \beta_n$ автомата $\mathfrak{a}_n$ выполнено соотношение:

$$\overline{\beta_n \dots \beta_1} = \overline{\alpha_n \dots \alpha_1} + 1,$$

где под сложением мы подразумеваем сложение двоичных чисел.

Действительно, пока $\alpha_i = 1$, в качестве функции выхода реализуется отрицание и на выходе $\beta_i = 0$. Пусть α_j — первый 0, поступивший на вход, соответственно $\beta_j = 1$, и по τ_0 мы переходим в орбиту, реализующую тождественную функцию. Дальше, по построению $\mathfrak{a}_n$, мы перемещаемся уже только по таким орбитам до момента времени $t = n + 1$. Значит, при $i \geqslant j$ выполняется $\alpha_i = \beta_i$. Фактически нами описан алгоритм прибавления единицы к двоичному числу.

Подав на вход первого из 2^k автоматов $\mathfrak{a}_n$ тождественный ноль, мы при прохождении через каждый автомат будем прибавлять единицу к нашему числу и получим на выходе 2^k в двоичной записи, что и утверждает лемма.

Таким образом, мы показали, что степень автомата $\mathfrak{a}_n$ в точности равна 2^n. Для завершения доказательства теоремы 4 надо убедиться, что количество состояний полученного автомата $n \cdot 2^{n-1}$. Это действительно так по построению: состояния $\mathfrak{a}_n$ разбиваются на n уровней по 2^{n-1} состояний в каждом.

В заключение автор выражает искреннюю благодарность своему научному руководителю С. В. Алёшину за помощь и поддержку на всех этапах выполнения работы.

Список литературы

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

[2] Винберг Э. Б. Курс алгебры // М.: Факториал пресс, 2002.

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