8-я лекция курса "Теория дискретных функций"

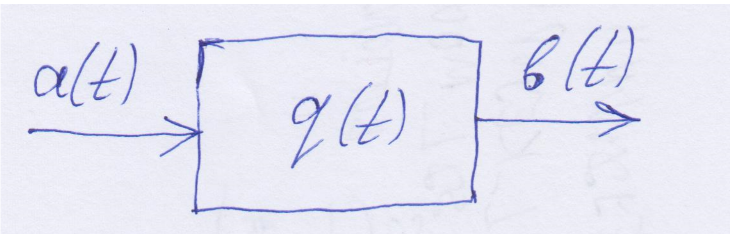
(1-й курс; лектор - проф. А.С.Подколзин)

Предыдущая лекция завершала раздел, посвященный k - значным логикам. Дальнейшее изложение отходит от учебника С.В.Яблонского "Введение в дискретную математику" и продолжается в русле монографии "Элементы теории автоматов" (В.Б.Кудрявцев, С.В.Алешин, А.С.Подколзин; М., "Наука", 1985). Впрочем, монография содержит существенно больше информации, чем будет затрагиваться данным курсом, и лучше пользоваться конспектами лекций.

Элементы теории автоматов

Аналогично тому, как непрерывные функции используются для описания непрерывных процессов, дискретные функции могут определять дискретные процессы. Изучением математических моделей дискретных процессов занимается теория автоматов. Существует множество таких моделей. Мы рассмотрим здесь всего три, и начнем с простейшей - абстрактных детерминированных конечных автоматов.

Начнем с неформальных рассмотрений. Дискретный процесс обычно предполагается происходящим в дискретном времени $t = 1, 2, 3, \ldots$. Представим себе техническое устройство, которое в каждый момент t дискретного времени находится в состоянии $q(t)$, принадлежащем конечному множеству Q возможных состояний. Из внешего мира на это устройство в момент t поступает некое воздействие $a(t)$, которое тоже будем считать принадлежащим конечному множеству A возможных воздействий. Наконец, само устройство отправляет во внешний мир некоторое ответное воздействие $b(t)$, принадлежащее конечному множеству B.



Детерминированность устройства означает, что его состояние в момент времени $t+1$ однозначно определяется состоянием $q(t)$ в момент t и входным сигналом $a(t)$. Естественно также предположить, что выходной сигнал $b(t)$ однозначно определяется по состоянию $q(t)$ и входному сигналу $a(t)$. Таким образом, для подходящих дискретных функций φ, ψ будем иметь:

$q(t+1) = \varphi(q(t), a(t))$

$b(t) = \psi(q(t), a(t))$

Если известны состояние $q(1)$ и входные сигналы $a(1), a(2), \ldots$, то эти соотношения позволяют однозначно определить $q(2), q(3), \ldots$ и $b(1), b(2), \ldots$, т.е. определить всю историю изменений, происходящих в устройстве. Фактически, мы получили математическую модель дискретного процесса. В случае модели непрерывного процесса использовались бы дифференциальные уравнения, что-нибудь типа:

$dq(t)/dt = \varphi(q(t), a(t))$

Эти модели достаточно похожи. Отличие лишь в том, что вместо производной для дискретного процесса берется переход от момента t к моменту $t+1$.

Приведенная выше модель была предложена Э.Ф.Муром, хотя и несколько в другом виде. В модели Мура выходной сигнал однозначно определялся состоянием автомата и выдавался еще до получения входного сигнала. Современная версия модели была предложена Мили.

Перейдем к точным определениям.

Конечным абстрактным детерминированным автоматом называется объект $V = (A, Q, B, \varphi, \psi)$, где A, Q, B - конечные множества; φ - функция, отображающая $Q \times A$ в Q; ψ - функция, отображающая $Q \times A$ в B. Множества A, Q, B называются, соответственно, входным алфавитом автомата V, алфавитом его состояний и выходным алфавитом. Функция φ называется функцией переходов, функция ψ - функцией выходов.

Если функция $\varphi(q, a)$ зависит от второго аргумента a фиктивно, то автомат называется автоматом Мура.

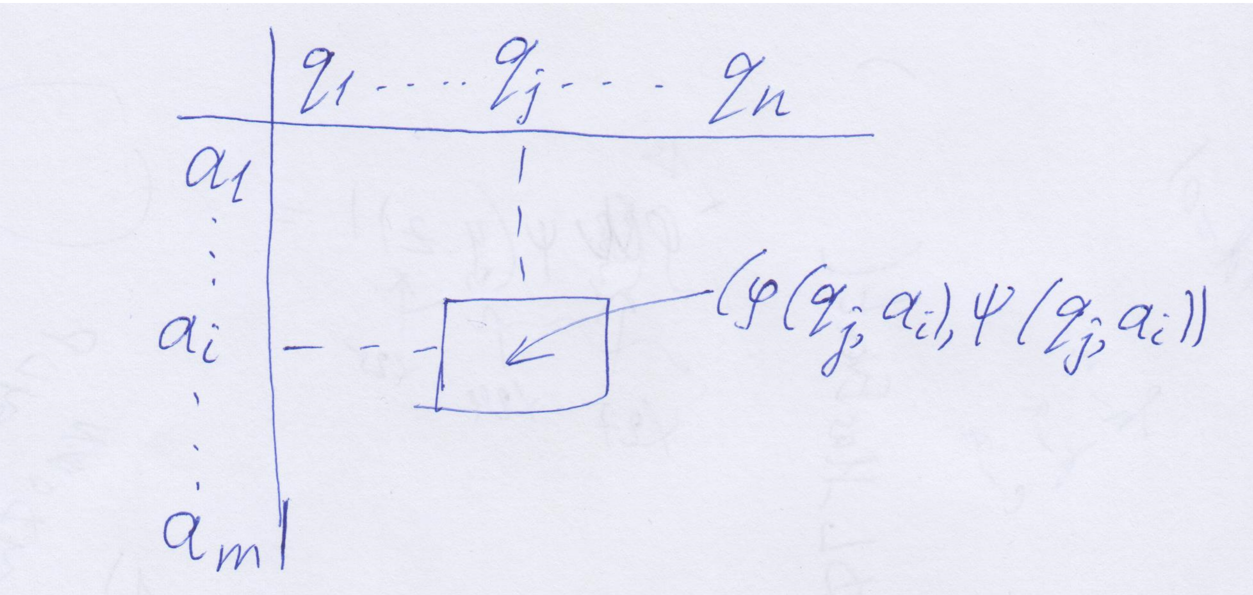
Если $A = A_1 \times \ldots A_m$, то говорим, что автомат имеет m входов. Если $B = B_1 \times \ldots B_p$, то говорим, что автомат имеет p выходов.

Далее, говоря об автоматах, для краткости, будем опускать слова "абстрактный детерминированный", называя их просто "конечный автомат" или "автомат".

Рассмотрим простейшие способы задания автоматов.

Задание автомата таблицей

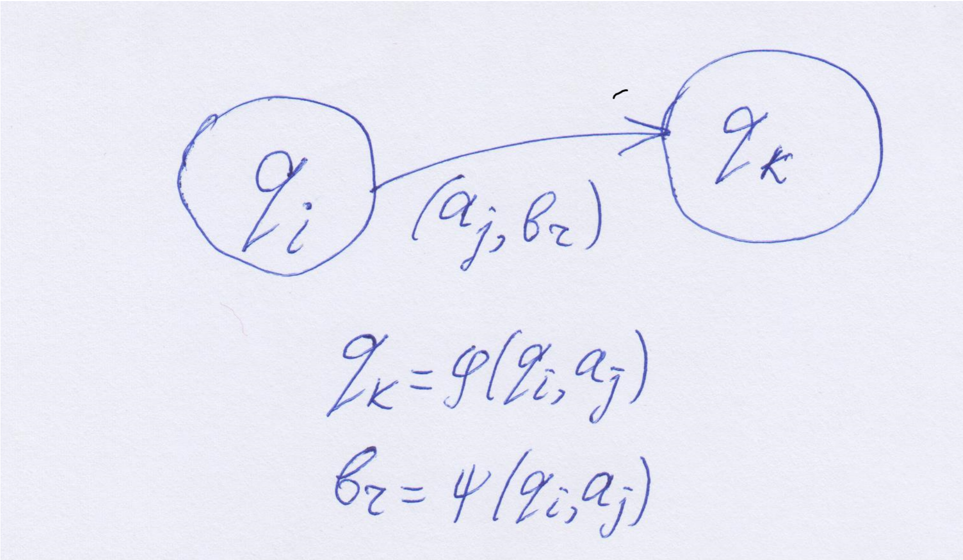
Конечные множества $A = \{a_1, \ldots, a_m\}$, $Q = \{q_1, \ldots, q_n\}$, $B = \{b_1, \ldots, b_p\}$ можно задавать непосредственным перечислением. Так как функции φ, ψ определены на конечных множествах, их можно задавать таблицами. Например, использовать совмещенную таблицу, в клетках которой указаны пары значений φ и ψ:



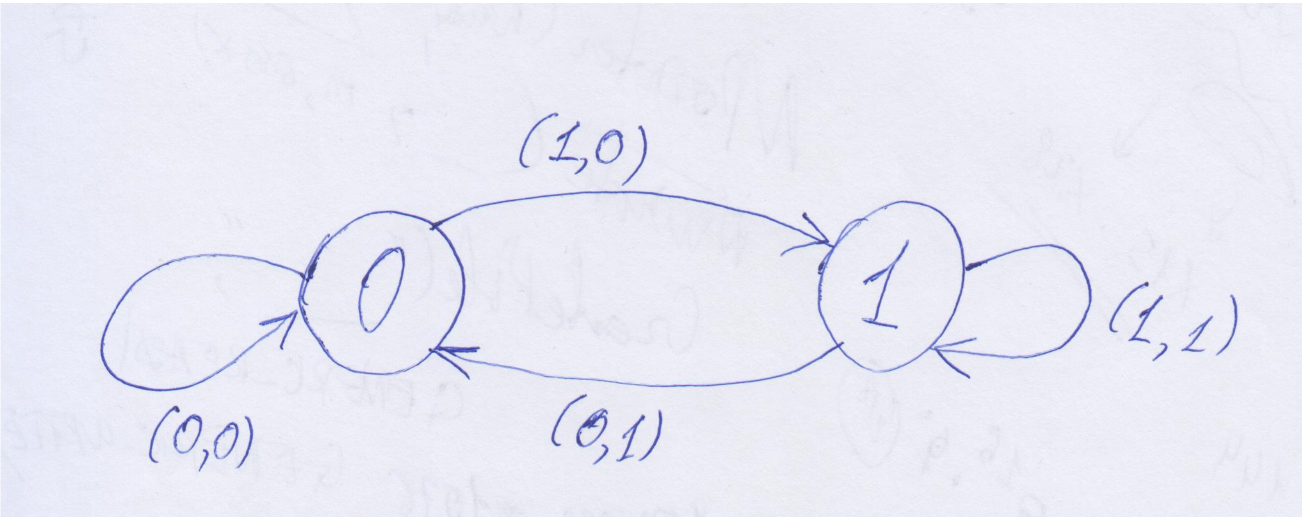
Данный способ задания автоматов используется крайне редко. Он громоздкий и не очень наглядный.

Задание автомата диаграммой Мура

Пусть алфавиты $A = \{a_1, \ldots, a_m\}$, $Q = \{q_1, \ldots, q_n\}$, $B = \{b_1, \ldots, b_p\}$ заданы перечислением. Для задания функций переходов и выходов можно ввести специальную диаграмму, называемую диаграммой Мура. На плоскости рисуются n кругов, в каждом из которых помещается символ соответствующего состояния $q_i; i = 1, \ldots, n$. Если $\varphi(q_i, a_j) = q_k; \psi(q_i, a_j) = b_r$, то от круга q_i к кругу q_k проводится стрелка, которой приписывается пара (a_j, b_r). Первый элемент пары обозначает входной символ, под действием которого автомат переходит из состояния q_i в состояние q_k, второй элемент - тот выходной символ, который при этом возникает.



Рассмотрим простой пример диаграммы Мура. Пусть $A = \{0, 1\}$, $Q = \{0, 1\}$, $B = \{0, 1\}$. Диаграмма имеет следующий вид:



Из диаграммы легко усматриваются соотношения:

$q(t + 1) = a(t)$

$b(t) = q(t)$

Таким образом, автомат "запоминает" в своем состоянии текущий входной сигнал и передает его на выход в следующий момент времени. Этот автомат называется автоматом единичной задержки.

Для автоматов Мура вид диаграммы можно упростить. Так как у этих атоматов выходной символ однозначно определяется состоянием, можно помещать его непосредственно в круге состояния, отделяя от символа состояния косой чертой. При этом отметками стрелок будут служить не пары, а только входные символы.

Вспомогательные функции, связанные с конечными автоматами

Введем ряд понятий и обозначений. Пусть $V = (A, Q, B, \varphi, \psi)$ - конечный автомат. Слова в алфавите A будем называть входными словами, слова в алфавите B - выходными словами, слова в алфавите Q - словами состояний. Как и ранее, пустое слово обозначаем Λ. Длину слова α обозначаем $|\alpha|$. Посредством $\alpha]_l$ обозначаем начало слова α, имеющее длину l. Множество всех слов в алфавите X обозначаем X^*. Слово α, повторенное k раз, обозначаем α^k.

Значение $\varphi(q, a)$ представляет собой то состояние, в которое автомат перейдет под действием единственной входной буквы a, значение $\psi(q, a)$ - тот выходной символ, который при этом появится. Иногда бывает необходимо рассматривать состояние и выходной символ, появляющиеся после подачи на вход автомата не единственной буквы, а целого слова, буква за буквой. Чтобы обозначать такие состояние и выходной символ, доопределим функции φ, ψ так, чтобы вторым аргументом была не буква алфавита A, а слово в этом алфавите. Функция φ доопределяется по индукции:

$\varphi(q, \Lambda) = q;$

$\varphi(q, \alpha a) = \varphi(\varphi(q, \alpha), a)$

Здесь α - слово в алфаавите A, a - буква этого алфавита.

Функция ψ доопределяется только на случай непустых входных слов, так как для получения символа на выходе необходимо наличие какого-то символа на входе:

$\psi(q, \alpha a) = \psi(\varphi(q, \alpha), a)$

Как и выше, α - слово в алфаавите A, a - буква этого алфавита.

Индукцией по длине слова без труда проверяются следующие соотношения:

$\varphi(q, \alpha_1\alpha_2) = \varphi(\varphi(q, \alpha_1), \alpha_2)$

$\psi(q, \alpha_1\alpha_2) = \psi(\varphi(q, \alpha_1), \alpha_2)$

Заметим, что однобуквенное слово не равно составляющей его букве. Поэтому, доопределяя φ и ψ на однобуквенные слова, мы вышли за рамки исходной области их определения.

Часто представляет интерес не только последнее состояние или последняя выходная буква, а все слово состояний, в которых автомат оказывался в последовательные моменты, и все выходное слово. Чтобы обозначить такие слова, вводятся функции $\overline{\varphi}$ и $\overline{\psi}$:

$\overline{\varphi}(q, \alpha) = \varphi(q, \alpha]_0)\varphi(q, \alpha]_1)\dots\varphi(q, \alpha)$

$\overline{\psi}(q, \alpha) = \psi(q, \alpha]_1)\psi(q, \alpha]_2)\dots\ \psi(q, \alpha)$

Здесь $\overline{\varphi}(q, \alpha)$ - слово состояний автомата, $\overline{\psi}(q, \alpha)$ - выходное слово.

Индукцией по длине слова легко проверить, что $\overline{\psi}(q, \alpha_1\alpha_2) = \overline{\psi}(q, \alpha_1)\overline{\psi}(\varphi(q, \alpha_1), \alpha_2)$

Функция $\overline{\psi}(q, \alpha)$ определяет выходное слово, выдаваемое автоматом в ответ на входное слово α, если вначале он находился в состоянии q. При фиксации q эта функция определяет отображение множества A^* входных слов в множество B^* выходных слов. Однако, при различном выборе начального состояния q будут получаться, вообще говоря, различные такие отображения. Чтобы фиксировать единственное отображение, вводится понятие инициального автомата.

Инициальным конечным автоматом называется объект $V_{q_1} = (A, Q, B, \varphi, \psi, q_1)$, где A, Q, B - конечные множества; $\varphi : Q \times A \to Q$; $\psi : Q \times A \to B$; $q_1 \in Q$. Фактически, это просто автомат с зафиксированным начальным состоянием q_1. Он реализует функцию $f(\alpha)$, заданную на множестве A^* и определенную равенством $f(\alpha) = \overline{\psi}(q_1, \alpha)$. Такие функции называются конечно-автоматными функциями. Другое их название - ограниченно-детерминированные функции, или, сокращенно, о.-д. функции. Мы им пользоваться не будем.

Конечно-атоматная функция осуществляет отображение множества A^* в множество B^*. Однако, не любое отображение такого типа является конечно-автоматной функцией. Во-первых, конечно-автоматная функция не изменяет длины слова. Во-вторых, автомат не умеет "заглядывать в будущее", т.е. каждая буква выходного слова должна однозначно определяться предшествующей частью входного слова. Например, автомат не может "переворачивать" слова, изменяя порядок их букв на противоположный. Конечность числа состояний автомата накладывает и другие ограничения.

Рассмотрим инициальный автомат $V_{q_1} = (A, Q, B, \varphi, \psi, q_1)$. Пусть $\alpha \in A^*$. Так как слово - функция, определенная на начальном отрезке натурального ряда, то i-я буква слова α равна $\alpha(i)$. Это дает основание записать слово α как $\alpha(1) \dots \alpha(s)$ для подходящего s. Рассмотрим слово $\kappa = \overline{\varphi}(q_1, \alpha)$ и слово $\beta = \overline{\psi}(q_1, \alpha)$. Длина слова κ на единицу больше длины слова α, а длина слова β равна длине слова α: $\kappa = \kappa(1)\kappa(2) \dots \kappa(s+1)$; $\beta = \beta(1) \dots \beta(s)$. Согласно определениям, выполняются следующие соотношения:

$\kappa(1) = q_1;$

$\kappa(t+1) = \varphi(\kappa(t), \alpha(t)); \quad t = 1, \dots, s$

$\beta(t) = \psi(\kappa(t), \alpha(t))$

Эти соотношения называются каноническими уравнениями конечного инициального автомата V_{q_1}.

Особый интерес предсталяет случай, когда $A = E_k \times \dots \times E_k$, $B = E_k \times \dots \times E_k$, $Q = E_k \times \dots \times E_k$, где $k \geq 2$ - натуральное. Пусть в первом равенстве имеется m сомножителей, во втором - p и в третьем - n. Тогда φ, ψ становятся вектор - функциями, и их можно задвать формулами в P_k. Чтобы переписать указанные выше канонические уравнения в векторной форме, обозначим $\alpha(t) = (a_1(t), \dots, a_m(t))$, $\beta(t) = (b_1(t), \dots, b_p(t))$, $\kappa(t) = (q_1(t), \dots, q_n(t))$, $q_1 = (q11, \dots, q_{1n})$. Канонические уравнения приобретают следующий вид:

$q_i(1) = q_{1i}; \quad (i = 1, \dots, n)$

$q_i(t+1) = \varphi_i(q_1(t), \dots, q_n(t), a_1(t), \dots, a_m(t)); \quad (i = 1, \dots, n)$

$b_j(t) = \psi_j(q_1(t), \dots, q_n(t), a_1(t), \dots, a_m(t)); \quad (j = 1, \dots, p)$

Правые части этих уравнений можно задавать с помощью формул k-значной логики, так что получаем еще один способ задания конечных автоматов. Практическую ценность имеет случай $k = 2$. При проектировании чипов вначале выписываются канонические уравнения, в правых частях которых расположены формулы алгебры логики. Обычно используются операции дизъюнкция, конъюнкция, отрицание, сумма по модулю 2. Созданы компьютерные программы, выполняющие дальнейшую обработку уравнений: формулы приводятся к виду дизъюнктивной нормальной формы, упрощаются как д.н.ф., снова сворачиваются, преобразуются в так называемый технологический базис, оптимизируются по площади и времени вычислений, и т.д.

Преобразование конечными автоматами периодических последовательностей

Изучение конечных автоматов начнем с простейшего их свойства, связанного с преобразованием периодических входных последовательностей. Кажется правдоподобным, что ввиду конечности множества состояний атомат должен будет дважды оказаться в одном и том же состоянии, при одинаковых фазах входной последовательности в эти два момента. Тогда далее на его выходе будет периодически повторяться фрагмент, имевший место между указанными моментами, и выходная последовательность тоже окажется периодической. Мы докажем этот факт и выясним, как связаны периоды входной и выходной последовательностей. Предварительно дадим ряд определений.

Пусть $V_q = (A, Q, B, \varphi, \psi, q)$ - инициальный конечный автомат, $\alpha = \alpha(1)\alpha(2)\ldots$ - бесконечная последовательность символов алфавита A. Иными словами, α - функция натурального аргумента, принимающая значения в A. Множество таких последовательностей будем обозначать A^∞. Определим последовательность $\beta = \overline{\psi}(q, \alpha)$ соотношением $\beta(i) = \psi(q, \alpha(1)\ldots\alpha(i)); \quad i = 1, 2, 3, \ldots$. Будем говорить , что инициальный автомат V_q преобразует входную последовательность α в выходную последовательность β.

Нетрудно проверить, что если $\alpha = \alpha'\alpha''$, где $\alpha' \in A^*$; $\alpha'' \in A^\infty$, то

$\overline{\psi}(q, \alpha) = \overline{\psi}(q, \alpha')\overline{\psi}(\varphi(q, \alpha'), \alpha'')$.

Последовательность $\alpha = \alpha(1)\alpha(2)\ldots$ из A^∞ назовем периодической, если существуют натуральные τ, τ', такие, что для любого $i \geq \tau' + 1$ выполняется $\alpha(i) = \alpha(i + \tau)$. Величину τ' называем длиной предпериода, величину τ - длиной периода.

Теорема. Конечный инициальный автомат $V_{q_1} = (A, Q, B, \varphi, \psi, q_1)$, имеющий n состояний, преобразует любую периодическую последовательность $\alpha, \alpha \in A^\infty$, имеющую наименьшую длину периода τ, в периодическую последовательность с наименьшей длиной периода вида $\theta \cdot m$, где $\theta | \tau$, $m \in \{1, \ldots, n\}$. Если $|A| \geq 3, |B| \geq 2$, то каждое такое значение вида $\theta \cdot m$ достигается при некоторых автомате V_q и последовательности α.

Пусть $V_{q_1} = (A, Q, B, \varphi, \psi, q_1)$; $|Q| = n$; последовательность $\alpha = \alpha(1)\alpha(2)\ldots$ - периодическая с длиной периода τ и предпериодом τ'. Тогда для любого $i \geq \tau' + 1$ выполнено $\alpha(i) = \alpha(i + \tau)$. Обозначим $\alpha_1 = \alpha(1)\ldots\alpha(\tau')$, $\alpha_2 = \alpha(\tau' + 1)\ldots\alpha(\tau' + \tau)$. Очевидно, α имеет вид $\alpha_1\alpha_2\alpha_2\ldots$.

Так как число стояний автомата равно n, то в последовательности $\varphi(q_1, \alpha_1\alpha_2)$, $\varphi(q_1, \alpha_1\alpha_2\alpha_2), \ldots, \varphi(q_1, \alpha_1\alpha_2^{n+1})$, имеющей $n + 1$ член, встречается не более n различных элементов. Следовательно, существуют такие $i_1, i_2; 1 \leq i_1 < i_2 \leq n + 1$, что:

$\varphi(q_1, \alpha_1\alpha_2^{i_1}) = \varphi(q_1, \alpha_1\alpha_2^{i_2})$.

Обозначим $q = \varphi(q_1, \alpha_1\alpha_2^{i_1})$, $\alpha_3 = \alpha_2^{i_2 - i_1}$. Тогда приведенное выше равенство приобретает следующий вид:

$q = \varphi(q, \alpha_3)$.

Из этого равенства ясно, что автомат будет периодически возвращаться в состояние q, а выходная последовательность, начиная с некоторого момента, будет образована повторяющимися словами $\overline{\psi}(q, \alpha_3)$. Этот же факт можно получить чуть более формальным путем:

Обозначим $\alpha' = \alpha_1 \alpha_2^{i_1}$; тогда последовательность α, путем группировки ее членов, можно представить в виде $\alpha' \alpha_3 \alpha_3 \alpha_3 \ldots$.

Поэтому $\overline{\psi}(q_1, \alpha) = \overline{\psi}(q_1, \alpha')\overline{\psi}(q, \alpha_3\alpha_3\alpha_3 \ldots)$.

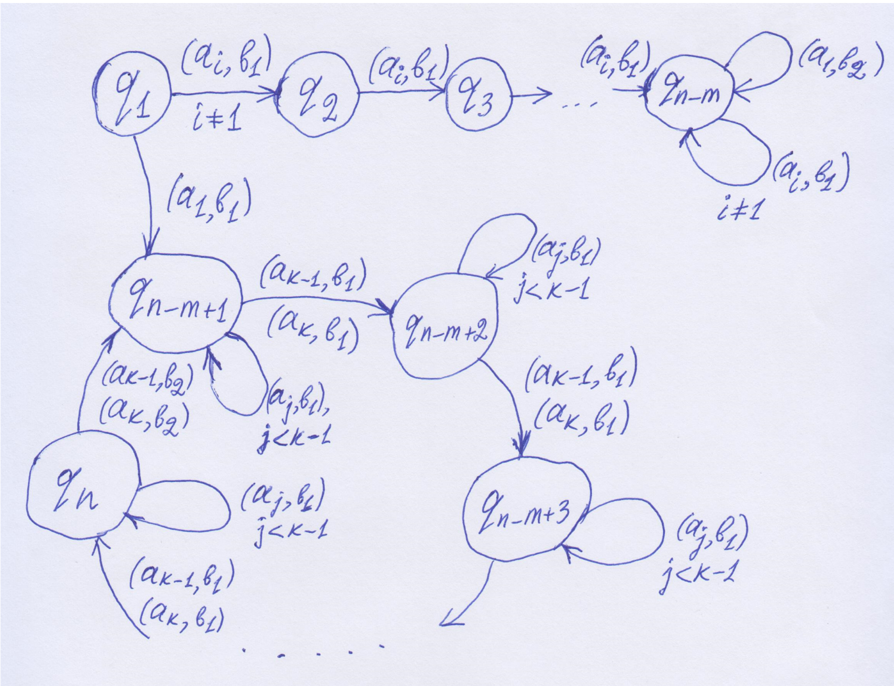
Однако, $\overline{\psi}(q, \alpha_3\alpha_3\alpha_3 \ldots) = \overline{\psi}(q, \alpha_3)\overline{\psi}(q, \alpha_3\alpha_3\alpha_3 \ldots)$.

Применяя это равенство повторно, получим:

$\overline{\psi}(q_1, \alpha) = \overline{\psi}(q_1, \alpha')\overline{\psi}(q, \alpha_3)\overline{\psi}(q, \alpha_3) \ldots$.

Таким образом, $\overline{\psi}(q_1, \alpha)$ - периодическая последовательность с длиной периода, равной длине слова α_3, т.е равной $(i_2 - i_1)\tau$. Следовательно, наименьшая длина периода последовательности является делителем этого числа и представима в виде $\theta \cdot m$, где θ делит τ, а m делит $i_2 - i_1$. Так как $i_2 - i_1 \in \{1, \ldots, n\}$, то $m \in \{1, \ldots, n\}$, и первая половина теоремы доказана.

Обратно, пусть $A = \{a_1, \ldots, a_k\}, k \geq 3, B = \{b_1, \ldots, b_p\}, p \geq 2$. Рассмотрим произвольное натуральное τ и произвольный натуральный делитель θ числа τ. Пусть $m \in \{1, \ldots, n\}$. Определим инициальный атомат V_{q_1} следующей диаграммой Мура:



На этой диаграмме изображен случай $m < n$. Если $m = n$, то верхняя часть отсутствует, а начальное состояние q_1 есть состояние q_{n-m+1}, расположенное на нижнем цикле. Хотя диаграмма и выглядит несколько громоздко, принцип ее устройства достаточно простой.

Если первая входная буква отлична от a_1, то из состояния q_1 автомат будет под действием каждой новой входной буквы перемещаться вправо по верхней цепочке состояний. В конце концов он дойдет до состояния q_{n-m}, в котором и останется навсегда. Варьируя входную букву, при этом можно будет добиться появления на его выходе любой из букв b_1, b_2.

Если первая входная буква - a_1, то автомат переходит к состоянию q_{n-m+1} нижнего цикла. При появлении на входе любой из букв a_{k-1}, a_k автомат сдвигается вдоль цикла по часовой стрелке на одно состояние. Если на вход поступает какая-либо другая буква, автомат не изменяет своего состояния. Все время при движении вдоль цикла на выходе автомата будет появляться символ b_1. Единственное исключение - переход от состояния q_n к состоянию q_{n-m+1}, где появляется символ b_2.

Рассмотрим слова $\alpha_1 = a_1^{\theta-1}a_{k-1}, \alpha_2 = a_1^{\theta-1}a_k, \alpha_3 = \alpha_1^{\tau/\theta-1}\alpha_2$.

Пусть сначала $\theta > 1$. Возьмем периодическую последовательность $\alpha = \alpha_3\alpha_3\alpha_3\ldots$. Так как в слове α_3 буква a_k появляется лишь один раз (в конце этого слова), то наименьший период последовательности α равен длине слова α_3, т.е. равен $\theta \cdot (\tau/\theta - 1 + 1) = \tau$. Так как $\theta > 1$, то слово α_3 начинается с буквы a_1. Следовательно, автомат сразу перейдет в нижний цикл и начнет перемещаться по нему. Пока на вход поступает буква a_1, автомат будет сохранять свое состояние. Это продолжается $\theta - 1$ момент, а затем на вход поступает последняя буква слова α_1 либо α_2, т.е. одна из букв a_{k-1}, a_k. Она вызывает переход автомата в следующее состояние цикла. Таким образом, в каждом состоянии цикла автомат будет находиться ровно θ моментов. Пока он не дойдет до перехода из состояния q_n в состояние q_{n-m+1}, на выходе будет возникать символ b_1, и лишь при указанном переходе появится символ b_2. Время, затраченное на однократное прохождение цикла, равно произведению θ на число m состояний цикла. Таким образом, выходная последовательность, начиная с некоторого момента, будет образована периодически повторяющимися фрагментами $b_1^{\theta \cdot m-1}b_2$, т.е. имеет наименьший период $\theta \cdot m$.

Случай $\theta = 1$ совсем простой, так как здесь число состояний автомата не меньше требуемой длины периода выходной последовательности. Для него немного скорректируем приведенную выше диаграмму Мура: стрелку от q_1 к q_{n-m+1} проведем для входных символов a_{k-1}, a_k, а стрелку от q_1 к q_2 - для всех остальных входных символов. Прочие рассуждения при этом сохраняются.

Теорема доказана.

Заметим, что приведенный пример обладает еще одним важным свойством. Автомат не просто имеет n состояний, но любые два из них можно "отличить" друг от друга, подобрав подходящее входное слово таким образом, чтобы выходные слова для этих состояний отличались. Ради этого свойства и была введена верхняя часть диаграммы. Его проверка рекомендуется в качестве самостоятельного упражнения.