Секция 6

# ПРИКЛАДНАЯ ТЕОРИЯ АВТОМАТОВ

УДК 681.3; 519.711

## К-МОДЕЛЬ ХИЩНИК — ЖЕРТВА В ЭКОЛОГИЧЕСКОЙ НИШЕ

Ю. В. Березовская, В. А. Воробьев

*Каузальная сеть* (К-сеть) — это маркированная сеть Петри, в которой для каждого перехода задана интенсивность события перехода как функция от маркировки входных позиций перехода. Вид этих функций зависит от предметной области и задаётся отдельно в каждом конкретном случае. Потоки событий переходов простейшие, т. е. стационарные (интенсивности меняются медленно), ординарные и без последействия.

Как и сеть Петри, К-сеть может использоваться для моделирования сложных систем, состоящих из множества взаимодействующих элементов, такие системы будем называть популяциями. Абстрагируясь от природы популяции, будем называть её элементы автоматами. Автомат может, как обычно, менять состояние сам, а может зависеть от любого числа автоматов, находящихся в подходящих состояниях. Популяции автоматов пригодны для исследования разнообразных массовых объектов: биологических, экономических и технических систем, параллельных программ [1]. С этой целью автоматы должны иметь стохастические характеристики — вероятности переходов в каждом такте. Поскольку число состояний популяции чрезвычайно велико, вычисления проводятся не для всех состояний популяции, а для среднего числа автоматов в различных состояниях. Таким образом, полученный случайный процесс представляет динамику популяции «в среднем». Трудность состоит в том, что в известном методе динамики средних все компоненты независимы друг от друга. Между тем основное свойство, которое влияет на поведение популяции, — взаимодействия между автоматами. Следует как-то учесть эти взаимодействия в методе динамики средних. Отсутствие метрики в популяции позволяет исследовать такие случайные системы, используя достижения теории параллельных процессов [2].

**Определение 1.** *Каузальная сеть* — это двудольный граф $G = \langle Q, D, \mathrm{In}, \mathrm{Out}, M, R\rangle$, где

- $Q = \{q_i : i = 0, 1, \ldots, n\}$ — множество позиций, соответствующее множеству состояний, на которых определены все автоматы;
- $D = \{d_j : j = 1, 2, \ldots, m\}$ — множество переходов автоматов из состояния в состояние;
- $\mathrm{In}$ — функция предшествования, которая ставит в соответствие каждой паре $(q_i, d_j)$ неотрицательное число $k_{ij} \geqslant 0$, где $k_{ij}$ — вес дуги из позиции $q_i$ в переход $d_j$; если соответствующей дуги нет, $k_{ij} = 0$;
- $\mathrm{Out}$ — функция следования, которая ставит в соответствие каждой паре $(d_j, q_i)$ неотрицательное число $k_{ij} \geqslant 0$, где $k_{ji}$ — вес дуги из перехода $d_j$ в позицию $q_i$; если соответствующей дуги нет, $k_{ji} = 0$;

— $M_t = \{N_{it} : i = 1, 2, \ldots, n\}$ — вектор маркировки, своими компонентами задающий число автоматов, находящихся в момент времени $t$ в каждом из состояний множества $Q$;
— $R = \{p_j(M_t(^*d_j)) : j = 1, \ldots, m\}$ — вектор-функция интенсивностей переходов, определяющая среднее число срабатываний перехода $d_j$ в течение одного такта, или число таких срабатываний в единицу времени, зависящее от маркировки множества $^*d_j$ — входных позиций перехода.

Позиция $q_0 \in Q$ называется внешней, имеет сколь угодно большое или единичное (если надо) значение маркера $N_0$, не меняет его при переходах и не изображается на рисунке графа. Состояния автоматов и позиции множества $\{q_i : i = 1, \ldots, n\}$ назовём собственными. Граф $G$ изображает причинно-следственные связи между состояниями автоматов и интенсивности этих связей.

В отличие от канонической сети Петри множество весовых коэффициентов дуг каузальной сети — это положительные действительные числа, приписанные входным и выходным дугам $j$-го перехода: $k_{ij}$ или $k_{ji}$ соответственно. Точно так же мы будем допускать действительные числа в качестве маркеров $N_i$ для позиций. Это позволит маркировать сеть вероятностями состояний автоматов и вообще избавиться от целых чисел. В таких случаях будем считать популяцию счётным множеством.

Компьютерное описание графа каузальной сети (K-модель) — это статическая часть — маркировка $M_0$ в начальный момент времени $t = 0$ и динамическая часть — описание переходов. Каждый переход $d_j$ описывается тремя выражениями: 1) перечисление множества $^*d_j$ с коэффициентами $k_{ij}$; 2) перечисление множества $d_j^*$ с коэффициентами $k_{ji}$ и 3) интенсивность $p_j(M_t(^*d_j))$ перехода. В общем случае описание перехода — это выражение вида $^*d_j > d_j^* : p_j(M_t(^*d_j)) :$ тип перехода. Тип перехода зависит от зоны действия и расположения автоматов в системе. *Линейный* переход соответствует дальнодействию в системе, нелинейные переходы: *раствор* — равномерному распределению автоматов во всей системе (как медведи в тайге) и *смесь* — собранию взаимодействующих автоматов в одном месте (как птичий базар). Внешнее состояние в K-модели изображается звёздочкой *.

Интерпретация предложенного описания популяции зависит от единицы времени равной длительности такта. Если единица времени достаточно мала, то $p_j \ll 1$ — вероятности переходов в течение такта, а $p_j(M_t(^*d_j))$ — среднее число автоматов, изменяющих состояние за такт. Если единица времени велика, то $p_j$ — интенсивности переходов одного автомата, а величины $p_j(M_t(^*d_j))$ — это интенсивности потоков допустимых переходов на всём множестве автоматов, готовых к переходу. В первом случае мы имеем синхронную модель популяции и можем потактно вычислять вектор $M_t$, во втором — асинхронную модель, которая порождает систему уравнений [1], подобных уравнениям Колмогорова — Чепмена.

Для иллюстрации простой популяции рассмотрим известную модель «хищник — жертва» в ограниченной экологической нише. Пусть $H$ — число хищников, $ZH$ — число живых жертв, $M$ — число экологических мест, $P$ — количество убитых жертв, т. е. пищи для воспроизводства хищников. Описание K-сети настолько простое, что не нуждается в длинных комментариях:
$H(0) = 50$, $ZH(0) = 50$, $M(0) = 100$, $P(0) = 0$ (полная ёмкость ниши $N = 200$ особей);
$ZH,\ M > 2ZH : 0{,}01 \cdot \min\{ZH, M\}$ : линейно (если место есть, то жертва его найдёт и родит новую);
$H, H > M : 0{,}01H$ : линейно (хищник обязательно умирает от голода и старости);

$H, ZH > H, M, P : 0{,}05\dfrac{H \cdot ZH}{N}$ : раствор (хищник должен найти и убить жертву, и будет пища);

$H, P > 2H : 0{,}05\dfrac{H \cdot P}{N}$ : смесь (хищники находят принесённую пищу и размножаются).

На рис. 1 показаны результаты реализации этой модели программой «Популяция». Моделирование обходится без получения системы нелинейных дифференциальных уравнений динамики средних.

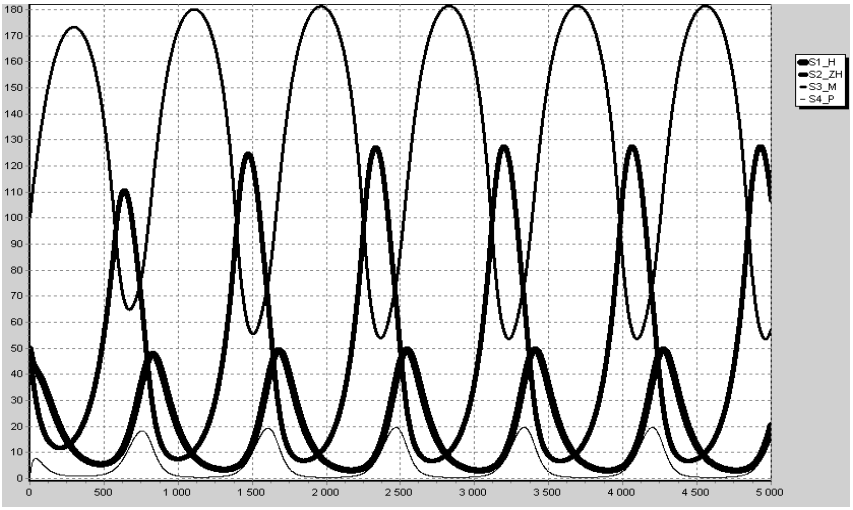


Рис. 1. Хищники и жертвы в ограниченной экологической нише. $H$ — количество хищников; $ZH$ — количество жертв; $M$ — количество экологических мест; $P$ — количество добытой пищи

Следует заметить, что в предлагаемой программе моделирования вовсе не обязательно подробно описывать вероятности переходов, заданные здесь формулами. Достаточно задать только численные характеристики — коэффициенты модели (здесь 0,01 и 0,05) и типы нелинейных переходов. Остальные части вероятностей переходов ($\min\{ZH, M\}$ и $H \cdot ZH/N$) стандартны и вычисляются программой согласно типу перехода.

## ЛИТЕРАТУРА

1. *Воробьев В. А., Кочнев А. И.* Популяционное моделирование коллективного поведения автоматов // Вестник Томского госуниверситета. Приложение. 2007. № 23. С. 270–275.
2. *Ачасова С. М., Бандман О. Л.* Корректность параллельных вычислительных процессов. Новосибирск: Наука, 1990. 314 с.

УДК 512.5

# О СКЕЛЕТНЫХ АВТОМАТАХ

В. Н. Салий

Под автоматом понимается тройка $A = (S, X, \delta)$, где $S$ и $X$ — конечные непустые множества (состояний и входных сигналов соответственно); $\delta : S \times X \to S$ — отображение, называемое функцией переходов. Функция переходов продолжается на множество $S \times X^*$, где $X^*$ — совокупность всех конечных слов над алфавитом $X$: по опре-

делению, $\delta(s,e)=s$ для любого $s\in S$ и пустого слова $e$ и $\delta(s,px)=\delta(\delta(s,p),x)$ для любых $s\in S$, $x\in X$, $p\in X^*$.

Автомату $A$ сопоставляется диаграмма переходов — мультиграф $G(A)$, вершинами которого являются элементы множества $S$ и дуги помечены элементами из $X$: из вершины $s$ в вершину $s'$ ведет дуга с меткой $x$, если $\delta(s,x)=s'$.

Говорят, что состояние $s'$ достижимо в автомате $A$ из состояния $s$, если существует входное слово $p\in X^*$, такое, что $\delta(s,p)=s'$. В этом случае пишут $(s,s')\in\tau$, и так определенное отношение $\tau\subseteq S\times S$ называют отношением достижимости в автомате $A$. Его симметричная часть $\sigma=\tau\cap\tau^{-1}$ называется отношением взаимной достижимости в автомате $A$. Классы эквивалентности $\sigma$ называют слоями автомата $A$. В [1] введено понятие каркаса автомата. Каркас автомата $A$ — это упорядоченное множество $(F(A),\leqslant)$, элементами которого являются слои автомата $A$, а порядком на множестве слоев $F(A)=A/\sigma$ — отношение, обратное отношению достижимости $\tau$. Очевидно, что для любого автомата $A$ выполняются неравенства $1\leqslant|F(A)|\leqslant|S|$. Если $|F(A)|=1$, т. е. отношение $\sigma$ универсально, автомат $A$ называется сильносвязным. Если же $|F(A)|=|S|$, т. е. отношение $\sigma$ тождественно, $\sigma=\Delta$, автомат $A$ назовем скелетным. В скелетном автомате отношение достижимости $\tau$ является порядком на множестве состояний $S$.

Поскольку в скелетном автомате $A$ все слои одноэлементны, можно считать, что в этом случае каркасом является множество $S$, упорядоченное обратной достижимостью $\tau^{-1}$, так что $s\geqslant s'$ означает, что состояние $s'$ достижимо из состояния $s$.

Нумерацией состояний автомата называется биективное отображение множества его состояний $S$ на начальный отрезок $[1,m]$ натурального ряда. Нумерация, по определению, является правильной, если состояния, достижимые из данного состояния, имеют меньшие, чем у него, номера.

**Теорема 1.** В автомате $A$ существует правильная нумерация состояний тогда и только тогда, когда $A$ — скелетный автомат.

Подмножество $S'\subseteq S$ называется устойчивым в автомате $A$, если $\delta(s,x)\in S'$ для любых $s\in S'$ и $x\in X$. Если $S'$ устойчиво в $A$, то, ограничивая функцию переходов $\delta$ на $S'\times X$, получают подавтомат $A'=(S',X,\delta)$. Совокупность $\mathrm{Sub}A$ всех подавтоматов автомата $A$, упорядоченная отношением $A_1\leqslant A_2\iff S_1\subseteq S_2$, где $A_i=(S_i,X,\delta)$, $i=1,2$, является дистрибутивной решеткой. Это решетка подавтоматов автомата $A$.

Известно [2], что для каждого автомата $A$ существует автомат $B$ с двумя входными сигналами, такой, что $\mathrm{Sub}A\cong\mathrm{Sub}B$, и что не всегда найдется автономный (т. е. с $|X|=1$) автомат $B$ с такой же, как у $A$, решеткой подавтоматов. Минимизацию по числу состояний дает следующее предложение.

**Теорема 2.** Пусть $A=(S,X,\delta)$ и $B=(T,Y,\gamma)$ — автоматы, такие, что $\mathrm{Sub}A\cong\mathrm{Sub}B$. Тогда $|T|\geqslant|F(A)|$. При этом существует скелетный автомат $B$, такой, что $\mathrm{Sub}A\cong\mathrm{Sub}B$ и $|T|=|F(A)|$.

Пусть $K$ — некоторый класс автоматов и $A\notin K$. Как можно путем в том или ином смысле минимальных изменений в структуре автомата $A$ получить из него автомат $A'$ из класса $K$? В числе допустимых приемов реконструкции автомата можно рассматривать, например, отождествление некоторых вершин (факторизация), введение дополнительных состояний и/или входных сигналов (расширения), перенаправление дуг диаграммы переходов, удаление дуг (замена их петлями) и т. п.

Показано, как путем удаления минимального числа дуг в диаграмме переходов $G(A)$ можно получить из данного автомата $A$ скелетный автомат.

Подробное изложение представленных результатов можно найти в [3].

ЛИТЕРАТУРА

1. *Салий В. Н.* Каркас автомата // Прикладная дискретная математика. 2010. №1(7). С. 63–67.
2. *Богомолов А. М., Салий В. Н.* Алгебраические основы теории дискретных систем. М.: Наука, 1997. 368 с.
3. *Салий В. Н.* Скелетные автоматы // Прикладная дискретная математика. 2011. №2(12). С. 73–76.

УДК 004.056.55

## АТАКА АППАРАТНОГО СБОЯ НА РЕАЛИЗАЦИЮ ШИФРА ЗАКРЕВСКОГО НА ОСНОВЕ ПЕРЕСТРАИВАЕМОГО АВТОМАТА[1]

В. Н. Тренькаев

В последние годы растет количество криптографических атак, использующих особенности реализации, так называемые атаки по побочным каналам (side channel attacks) [1], которые часто дают более мощный результат, чем классический криптоанализ. Рассматривается вариант такой атаки — атака на основе сбоев (fault attack), когда криптоаналитик имеет возможность оказать на шифратор внешнее физическое воздействие и вызвать ошибки (сбои) в процессе его работы. Предложена атака аппаратного сбоя на реализацию шифра Закревского на базе перестраиваемого автомата [2]. Предполагается, что нештатные условия получаются созданием кратковременной ошибки в процессе работы шифратора в виде фиксирования требуемого значения одного бита. Криптоанализ шифра Закревского как автоматного шифра сводится к построению простого условного эксперимента по восстановлению (идентификации) автомата из заданного класса.

Конечный автомат задаётся пятеркой $(X, S, Y, \psi, \varphi)$, где $S$ — конечное непустое множество состояний; $X$ и $Y$ — конечные входной и выходной алфавиты соответственно, причем $|X| = |Y|$; $\psi : X \times S \to S$ и $\varphi : X \times S \to Y$ — функции переходов и выходов соответственно.

Под перестраиваемым понимается автомат с возможностью выбора функции переходов из заданного множества. Структура перестраиваемого автомата, на базе которого реализуется шифр Закревского, представлена на рис. 1, где компоненты $\psi_0$ и $\psi_1$ реализуют функции $\psi_0 : X \times S \to S$ и $\psi_1 : X \times S \to S$ соответственно. Компонента Key реализует функцию $C : X \times S \times K \to \{0, 1\}$, где $K$ — конечное множество настроек. На схеме представлен также мультиплексор Mux, который в зависимости от значения функции $C_k(x, s) = C(x, s, k)$ осуществляет выбор одного из двух возможных состояний $\psi_0(x, s)$ и $\psi_1(x, s)$, «пропуская» его далее в регистр памяти Reg, где в каждый момент автоматного времени хранится текущее состояние. Компонента Out реализует функцию выходов $\varphi(x, s)$, такую, что при любом $s \in S$ функция $\varphi_s(x) = \varphi(x, s)$ является биекцией из $X$ в $Y$ и все биекции $\varphi_s(x), s \in S$, различные. Каждой настройке $k \in K$ перестраиваемого автомата соответствует автомат Закревского $Z^{(k)} = (X, S, Y, \psi^{(k)}, \varphi)$, у которого $\psi^{(k)}(x, s) = \psi_c(x, s)$ для всех $(x, s) \in X \times S$ и $c = C_k(x, s)$. Функции $\psi_0$ и $\psi_1$ устроены так [2], что автомат $Z^{(k)}$ сильносвязный. Автомат $Z^{(k)^{-1}} = (Y, S, X, \psi^{(k)}, \varphi')$,

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт №П1010).

где $\varphi'(y, s) = x$, если $\varphi(x, s) = y$, обратен автомату $Z^{(k)}$. В одном и том же начальном состоянии $s_0$ автоматы $Z^{(k)}$ и $Z^{(k)^{-1}}$ представляют собой алгоритмы соответственно шифрования и расшифрования на ключе $(k, s_0) \in K \times S$ и в совокупности образуют то, что называется шифром Закревского.

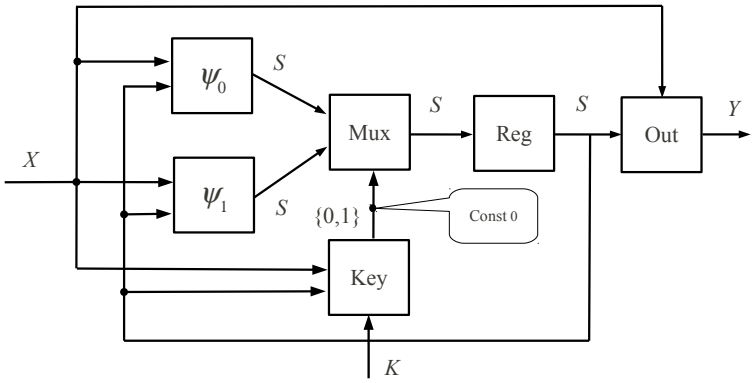


Рис. 1. Структура перестраиваемого автомата

Предполагается, что криптоаналитику о перестраиваемом автомате известно всё, кроме настройки $k \in K$ и начального состояния $s_0$ — состояния регистра Reg. В этом случае функция $\psi^{(k)}$ определяется однозначно настройкой $k$. Вместе с тем $\psi^{(k)}$ и $s_0$ однозначно определяют алгоритмы шифрования и расшифрования, поэтому атаку с угрозой раскрытия пары $(\psi^{(k)}, s_0)$ можно считать атакой с угрозой раскрытия алгоритма шифрования (расшифрования). Именно такой является описываемая далее атака аппаратного сбоя на шифр Закревского, реализуемый перестраиваемым автоматом на рис. 1.

Сначала для автомата $A_0 = (X, S, Y, \psi_0, \varphi)$ строится установочное слово $\alpha$, т. е. входное слово, наблюдая реакцию на которое, можно однозначно определить текущее состояние автомата. Далее производится воздействие на шифратор, такое, что выход компонеты Key имеет фиксированное значение 0 (Const 0 на рис. 1). Затем на шифратор подается установочное слово $\alpha$ и по реакции на него определяется текущее состояние шифратора. После этого опять производится воздействие на шифратор, которое снимает фиксацию выхода компоненты Key. Наконец, проводится простой условный эксперимент по восстановлению автомата $Z^{(k)}$, который сводится к процедуре определения неизвестного $s' = \psi^{(k)}(x, s)$ при известном $s$ и неизвестном $\psi^{(k)}$. По свойствам перестраиваемого автомата $s' \in \{\psi_0(x, s), \psi_1(x, s)\}$ и существует хотя бы один входной символ $z$, такой, что $\varphi(z, \psi_0(x, s)) \neq \varphi(z, \psi_1(x, s))$. Тогда по реакции автомата $Z^{(k)}$ на входное слово $xz$ можно однозначно идентифицировать состояние $s'$. Эта операция проделывается до тех пор, пока возможно, после чего строится входное слово, переводящее автомат $Z^{(k)}$ в известное начальное состояние некоторого нераспознанного перехода, и операция повторяется. Процесс заканчивается с определением $\psi^{(k)}(x, s)$ для всех $(x, s) \in X \times S$.

## ЛИТЕРАТУРА

1. *Панасенко С. П.* Алгоритмы шифрования. Специальный справочник. СПб.: БХВ-Петербург, 2009. 576 с.
2. *Тренькаев В. Н.* Реализация шифра Закревского на основе перестраиваемого автомата // Прикладная дискретная математика. 2010. № 3. С. 69–77.