ным решением. Располагая такими условиями, можно для нахождения решения задачи предложить следующий алгоритм поиска с возвращением (по дереву).

Алгоритм моделирует процесс перехода из корня дерева в искомый лист путем выполнения серии подъемов и спусков, осуществляемых при определенных условиях. Подъем – это перемещение из достигнутой вершины i-го яруса в смежную вершину $(i+1)$-го яруса для $i<k$, а спуск – возвращение из текущей вершины i-го яруса в смежную вершину $(i-1)$-го яруса для $i>0$. Подъем может выполняться только в вершину, в которую до этого еще не поднимались. В отсутствие таковой или, если достигнутая вершина не может быть частичным решением задачи, осуществляется спуск. По достижению вершины дерева, являющейся квазиполным решением задачи, алгоритм останавливается. Ниже дается строгое описание данного алгоритма. В нем через $\alpha[i]$ и $\alpha]_i$ обозначены соответственно i-я компонента и префикс длины i вектора α.

1. (Начальная установка) $\alpha:=\lambda$, $i:=0$, $z(\alpha)=y$.

2. $i=i+1$ и

3. (Подъем).

3.1. $\alpha:=\alpha 0$, и если α не может быть частичным решением, то п. 3.2, иначе – п. 2.

3.2. $\alpha:=\alpha 1$, $z(\alpha):=z(\alpha)\oplus g_i$, и если α не может быть частичным решением, то п. 4, в противном случае, если α – квазиполное, то п. 5, иначе п. 2.

4. (Спуск) $z(\alpha):=z(\alpha)\oplus g_i$, $i:=i-1$, $\alpha:=\alpha]_i$, и если $\alpha[i]=1$, то п. 4, иначе $\alpha:=\alpha]_{i-1}$ и п. 3.2.

5. Вектор $\alpha 0^{k-i}$ есть решение.

Сформулируем условия, при которых булев вектор $\alpha=a_1a_2\ldots a_i$ для $i<k$ не может быть частичным решением задачи. Вычислим вектор $z(\alpha)=z_1z_2\ldots z_n$. Пусть матрица H получена из G вычеркиванием первых i строк и t_0 обозначает количество таких r в $\{1, 2,\ldots, n\}$, что $z_r=1$ и r-й столбец матрицы H состоит из одних нулей (является нулевым). Разобьем множество всех ненулевых столбцов матрицы H на классы одинаковых столбцов. Пусть число классов равно m, и s-й из них, $s=1, 2,\ldots, m$, состоит из столбцов с номерами $r_1,\ldots,r_p$. Обозначим t_{s0} и t_{s1} количество нулей и единиц соответственно среди компонент вектора $z(\alpha)$, имеющих номера $r_1,\ldots, r_p$. Пусть, наконец, t_s есть наименьшее из t_{s0} и t_{s1}, а t' равно сумме всех t_s, $s=1,\ldots, m$.

Теорема. Вектор α не может быть частичным решением задачи, если $t_0+t'>t$.

Утверждение справедливо, так как в противном случае вектор e в уравнении (1) должен иметь вес больше t.

ЛИТЕРАТУРА

1. *Сидельников В.М.* Открытое шифрование на основе двоичных кодов Рида-Маллера // Дискретная математика. 1994. Вып. 2.
2. *Сидельников В.М., Шестаков С.О.* О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона // Дискретная математика. 1992. Вып. 3.
3. *Брикелл Э.Ф., Одлижко Э.М.* Криптоанализ: Обзор новейших результатов // ТИИЭР. 1998. № 5.
4. *Радюк Л.Е., Терпугов А.Ф.* Теория вероятностей и случайных процессов. Томск: Изд-во Том. ун-та, 1988.
5. *Аснис И.Л., Федоренко С.В., Шабунов К.Б.* Краткий обзор криптосистем с открытым ключом // Защита информации. 1994. № 2.
6. *Агибалов Г.П.* Адекватные модели полурешеток, функций и автоматов на полурешетках // Вестник ТГУ. 2000. № 271.

Статья представлена кафедрой защиты информации и криптографии факультета прикладной математики и кибернетики Томского государственного университета, поступила в научную редакцию 1 марта 2000 г.

УДК 519.7

Г.П. Агибалов

АДЕКВАТНЫЕ МОДЕЛИ ПОЛУРЕШЕТОК, ФУНКЦИЙ И АВТОМАТОВ НА ПОЛУРЕШЕТКАХ

Работа выполнена при финансовой поддержке РФФИ, грант № 98-01-00288

Определяются понятия адекватной модели и ее точности для конечной верхней полурешетки, для функции и автомата на таких полурешетках и для полурешеточно упорядоченной алгебры. В этих определениях элементами адекватной модели полурешетки служат все наибольшие элементы смежных классов некоторой конгруэнции, которая, в свою очередь, характеризует точность модели. Изучаются свойства и даются методы построения адекватных моделей для полурешеток, функций и автоматов на них.

Введение

Важнейшими характеристиками всякой математической модели являются ее адекватность и степень точности. В случае дискретных моделей первая понимается как безошибочность в том смысле, что результат адекватного моделирования всегда содержит в себе истинное значение моделируемой величины, а вторая – как степень неопределенности этого результата [1]. Для управляющих систем на конечных верхних полурешетках удается формализовать эти понятия, а утверждения о них сделать доказательными [2]. Это достигается определением адекватной модели на полурешетках, составленных из наибольших элементов смежных классов полурешеток заданной системы по некоторым конгруэнциям, которыми и характеризуется степень точности модели.

В данной работе понятия адекватной модели и ее точности определяются для полурешеток, функций и автоматов на полурешетках и для полурешеточно упорядоченных алгебр. Указан метод построения адекватных моделей для полурешеток подмножеств и интервалов с точностью до эквивалентности на множестве минимальных элементов полурешетки. Показано, что свойства монотонности и квазимонотонности функции на полурешетках передаются любой ее адекватной модели, а свойство аддитивности – лишь модели, точность которой сохраняется данной функцией. Установлено, что адекватная модель суперпозиции монотонных функций реализует суперпозицию их адекватных моделей и совпадает с ней в случае сохранения функциями точностей их моделей. В терминах стабильных троек конгруэнций охарактеризованы всевозможные адекватные модели произвольного конечного автомата на полурешетках. Показано, что свойства аддитивности, монотонности и квазимонотонности автомата на полурешетках сохраняются в его адекватных моделях.

Эти результаты находят широкое применение в адекватном моделировании дискретных управ[illegible] их систем с различной степенью точности и в синтезе их логической структуры на базе БИС с заданным динамическим поведением [2].

Всюду далее под полурешеткой подразумевается конечная верхняя полурешетка, т.е. конечное частично упорядоченное множество, в котором любые два элемента a и b имеют точную верхнюю грань, называемую их *суммой* и обозначаемую $a+b$. В ней обязательно есть наибольший и минимальные элементы. Последние называются *точками* полурешетки.

Адекватные модели полурешеток

Пусть S – полурешетка со сложением + и σ – конгруэнция на ней. Каждый смежный класс A в S/σ является подполурешеткой в S [2], и в нем есть наибольший элемент $\sup A$. Смежные классы A и B как элементы фактор-полурешетки S/σ и элементы в них, в том числе наибольшие, как элементы полурешетки S, связаны между собой соотношением:

$$A \le B \Leftrightarrow \sup A \le \sup B \Leftrightarrow \exists a \in A \exists b \in B (a \le b).$$

Пусть далее $S\uparrow\sigma=\{\sup A: A \in S^{\sigma}\}$. Определим на $S\uparrow\sigma$ сложение $\oplus$ как $a \oplus b = \sup[a+b]_{\sigma}$. Вместе с $\oplus$ множество $S\uparrow\sigma$ является полурешеткой, гомоморфной полурешетке S и изоморфной полурешетке S/σ, и называется *адекватной моделью полурешетки S с точностью* σ.

Множество $\tilde{M}$ всех непустых подмножеств конечного множества M, рассматриваемое вместе с отношением включения, является полурешеткой. Для любой эквивалентности R на M определяется эквивалентность $\tilde{R}$ на $\tilde{M}$ как $A \tilde{R} B \Leftrightarrow \forall a \in A \exists b \in B (aRb) \& \forall b \in B \exists a \in A (aRb)$. Это есть конгруэнция на полурешетке $\tilde{M}$. Пусть $\{R\}$ обозначает подполурешетку в $\tilde{M}$, порожденную смежными классами эквивалентности R.

Теорема 1. $\{R\} = \tilde{M} \uparrow \tilde{R}$.

Доказательство. Между непустыми подмножествами A смежных классов эквивалентности R, элементами B полурешетки $\{R\}$ и смежными классами C эквивалентности $\tilde{R}$ можно установить взаимно однозначное соответствие, при котором для соответствующих A, B, C справедливо следующее: B есть объединение смежных классов в A; C состоит из всех таких подмножеств в M, которые пересекаются с каждым смежным классом в A и не пересекаются с другими смежными классами эквивалентности R; наибольший элемент в C совпадает с B. Таким образом, множества $\{R\}$ и $\tilde{M} \uparrow \tilde{R}$ равны. Суммы в полурешетках $\{R\}$ и $\tilde{M} \uparrow \tilde{R}$ совпадают с объединением и потому одинаковы. Теорема доказана.

В случае, когда $\tilde{M}$ есть декартово произведение множеств, те его непустые подмножества, которые сами являются декартовыми произведениями множеств, называются *интервалами* на $\tilde{M}$. Пусть в этом случае $\hat{M}$ – множество всех интервалов на $\tilde{M}$; $<R> = \hat{M} \cap \{R\}$; $\hat{R}$ – минимальная конгруэнция на $\hat{M}$ такая, что для любого смежного класса A эквивалентности R существует смежный класс конгруэнции $\hat{R}$, содержащий в качестве элементов все одноэлементные подмножества в A.

Теорема 2. $<R> = \hat{M} \uparrow \{R\}$.

Доказательство. По определению элементами полурешетки $<R>$ являются объединения смежных классов эквивалентности R, совпадающие с суммами всех своих элементов, рассматриваемых как элементы полурешетки $\hat{M}$, а смежные классы конгруэнции $\hat{R}$ состоят из всевозможных сумм элементов в таких объединениях. Таким образом, элементы в $<R>$ суть наибольшие элементы в смежных классах $\hat{R}$. Теорема доказана.

Пусть отношение $\rho \subseteq \{R\}^2$ определено как $U \rho V \Leftrightarrow h(U)=h(V)$, где $h(P)$ для $P \subseteq M$ – наименьший интервал в $<R>$, для которого $P \subseteq h(P)$. По определению отображение $h: \{R\}^2 \to <R>$ является гомоморфизмом полурешеток и отношение ρ – его ядерной конгруэнцией. Поэтому полурешетки $<R>$ и $\{R\}/\rho$ изоморфны и верна следующая теорема.

Теорема 3. $<R> = \{R\} \uparrow \rho$.

Следствие 1. $\hat{M}$ является адекватной моделью $\tilde{M}$.

Следствие 2. Адекватные модели $\hat{M}$ являются адекватными моделями $\tilde{M}$.

Следствие 3. *$<R>$ есть адекватная модель $\tilde{M}$.*

Полурешетка S называется *точечной*, если каждый элемент в ней равен сумме некоторых ее точек. Так, полурешетки $\tilde{M}, \hat{M}$ и $\{R\}$ – точечные.

Теорема 4. Полурешетка <R> точечная, если каждый смежный класс эквивалентности R является элементом $\hat{M}$.

В этом случае минимальными элементами полурешетки $<R>$ являются все смежные классы эквивалентности R и только они, а всякий другой ее элемент, будучи интервалом и одновременно объединением некоторых минимальных элементов, равен сумме последних. Этим теорема доказана.

Адекватные модели функций

Имеются в виду функции на полурешетках, т.е. отображения полурешеток в полурешетки. Области определения и значений функции f обозначаются D_f и V_f соответственно. Есть четыре замечательных класса функций на полурешетках [2] – аддитивные, точечные, монотонные и квазимонотонные. Функция *точечная*, если на любом элементе области определения ее значение равно сумме значений на точках последней, содержащихся в данном элементе. Функция называется *аддитивной*, если она является гомоморфизмом полурешеток. Функция f *монотонная*, если $a \le b \Rightarrow f(a) \le f(b)$. Функция g *реализует* функцию f, если $D_f \subseteq D_g$ и $g(a) \le f(a)$ для всех a в D_f. Функция называется *квазимонотонной*, если она реализуется монотонной функцией. Класс квазимонотонных функций является собственным подмножеством множества всех функций на полурешетках, монотонные функции образуют собственное подмножество в классе квазимонотонных функций, а аддитивные и точечные – собственные подмножества в классе монотонных функций. Классы аддитивных и точечных функций пересекаются, но не совпадают. Они не замкнуты относительно суперпозиции, но суперпозиции аддитивных или точечных

функций обязательно монотонные. Данные классы замечательны тем, что функции на полурешетках простейших компонент современных интегральных микросхем (транзисторов, вентилей, ключей) являются аддитивными и точечными. Схемы из таких компонент имеют монотонные функции на полурешетках и реализуют квазимонотонные функции. Понятие квазимонотонности является, таким образом, формальным эквивалентом понятия физической реализуемости. Конструктивные тесты квазимонотонности известны [2, 3]. Один такой тест, применяемый ниже, имеет следующую форму.

Тест квазимонотонности. Функция f квазимонотонна, если и только если для любого подмножества $A \subseteq D_f$, имеющего нижнюю грань в D_f, подмножество $f(A) \subseteq V_f$ имеет нижнюю грань в V_f.

Функция g называется *адекватной моделью функции f с точностью* (σ,ρ), если σ и ρ суть конгруэнции на полурешетках D_f и V_f соответственно, $D_g = D_f\uparrow\sigma$, $V_g = V_f\uparrow\rho$ и $g(a) = \sup[f(a)]_\rho$ для всех a в D_g. Функция f *сохраняет пару* (σ,ρ), если $a \sigma\ b \Rightarrow f(a) \rho f(b)$.

Теорема 5. Пусть g – адекватная модель f с точностью (σ,ρ). Тогда справедливы следующие утверждения.

(1) Если функция f монотонная или квазимонотонная, то функция g также монотонная или квазимонотонная соответственно.

(2) Если функция f сохраняет (σ, ρ) и аддитивна, то функция g также аддитивна.

(3) Пусть $f = f_0(f_1, \ldots, f_m)$, функция g_0 есть адекватная модель функции f_0 с точностью (δ, ρ), функция g_i для $i=1, \ldots, m$ есть адекватная модель функции f_i с точностью (σ,δ_i), $\delta = \delta_1 \times \ldots \times \delta_m$ и $h = g_0(g_1,\ldots,g_m)$. Тогда если функция f_0 монотонная, то $g \le h$; если же функция f_0 сохраняет (δ, ρ), то $g = h$.

Доказательство. Пусть $a \in D_g$ и $b \in D_g$.

(1) Если функция f монотонная и $a \le b$, то $f(a) \le f(b)$, $[f(a)]_\rho \le [f(b)]_\rho$, $\sup[f(a)]_\rho \le \sup[f(b)]_\rho$ и $g(a) \le g(b)$, т.е. функция g монотонная.

Если $\varphi(a) \le f(a)$ и адекватная модель функции φ с точностью (σ,ρ) есть ψ, то $[\varphi(a)]_\rho \le [f(a)]_\rho$, $\sup[\varphi(a)]_\rho \le \sup[f(a)]_\rho$ и $\psi(a) \le g(a)$, что ввиду утверждения для монотонности доказывает квазимонотонность g при условии квазимонотонности f.

(2) Пусть f сохраняет пару (σ, ρ). Тогда для любого $x \in D_f$ ввиду $x \sigma \sup[x]_\sigma$ имеет место $f(x) \rho f(\sup[x]_\square)$ и, следовательно, $\sup[f(x)]_\rho = \sup[f(\sup[x]_\sigma)]_\rho$. В этом случае если $f(a+b) = f(a) + f(b)$, то можно записать $g(a \oplus b) = \sup[f(a \oplus b)]_\rho = \sup[f(\sup[a]_\sigma \oplus \sup[b]_\sigma)]_\rho = \sup[f(\sup[a+b]_\sigma)]_\rho = \sup[f(a+b)]_\rho = \sup([f(a)]_\rho + [f(b)]_\rho) = \sup[f(a)]_\rho \oplus \sup[f(b)]_\rho = g(a) \oplus g(b)$, т.е. из аддитивности f следует аддитивность g.

(3) По условию $g(a) = \sup[f(a)]_\delta$, для всех $i=1, \ldots, m$. Отсюда $f_1(a) \ldots f_m(a) \le g_1(a) \ldots g_m(a) = \sup[f_1(a) \ldots f_m(a)]_\delta \in D_{f_0}\uparrow\delta$. Поэтому, во-первых, $(f_1(a) \ldots f_m(a))(\delta g_1(a) \ldots g_m(a))$, во-вторых, $\sup[f_0(g_1(a) \ldots g_m(a))]_\rho = g_0(g_1(a) \ldots g_m(a)) = h(a)$. С другой стороны, $g(a) = \sup[f(a)]_\rho = \sup[f_0(f_1(a) \ldots f_m(a))]_\rho$.

Если функция f_0 монотонная, то $\sup[f_0(f_1(a) \ldots f_m(a))]_\rho \le \sup[f_0(g_1(a) \ldots g_m(a))]_\rho$, т.е. $g(a) \le h(a)$.

Если же f_0 сохраняет пару (δ,ρ), то

$$f_0(f_1(a) \ldots f_m(a)) \rho f_0(g_1(a) \ldots g_m(a)),$$

$\sup[f_0(g_1(a) \ldots g_m(a))]_\rho = g_0(g_1(a) \ldots g_m(a))$, т.е. $g(a) = h(a)$.

Теорема доказана.

Утверждение (3) теоремы допускает следующую интерпретацию: заменив в какой-либо функциональной схеме функции элементов их адекватными моделями, получим схему, функция которой реализуется адекватной моделью функции прежней схемы, если функции элементов монотонные, и совпадает с ней, если функции элементов сохраняют точности их моделей.

В [2] приведены примеры функций на полурешетках, показывающие, что свойства точечности и аддитивности функции в ее адекватной модели могут теряться, причем точечность может теряться даже тогда, когда точность модели сохраняется функцией.

Адекватные модели автоматов

Конечный автомат $S = (X, Q, Y, \psi, \varphi)$, где X – входной и Y – выходной алфавиты; Q – множество состояний; ψ – функция переходов; $\psi: X \times Q \to Q$, и φ – функция выходов, $\varphi: X \times Q \to Y$; называется *автоматом на полурешетках*, если в нем X, Q и Y суть полурешетки. Всюду далее под автоматом подразумевается именно автомат на полурешетках. Автомат называется *аддитивным*, *монотонным* или *квазимонотонным*, если соответственно таковы его функции переходов и выходов. Автомат $L = (U, P, V, \lambda, \delta)$ называется *гомоморфным образом*, или *моделью* автомата S, если существуют эпиморфизмы полурешеток $h_1: X \to U$, $h_2: Q \to P$, $h_3: Y \to V$, такие, что для всех xq в $X \times Q$ $h_2\psi(x,q) = \lambda(h_1x, h_2q)$; $h_3\varphi(x,q) = \delta(h_1x, h_2q)$; в этом случае $h_1h_2h_3$ называется *гомоморфизмом S на L*. Гомоморфизм $h_1h_2h_3$ называется *изоморфизмом*, если h_1, h_2, h_3 суть изоморфизмы полурешеток. Автоматы *изоморфны*, если существует изоморфизм одного из них на другой.

Теорема 6. Любая модель аддитивного, монотонного или квазимонотонного автомата является соответственно аддитивным, монотонным или квазимонотонным автоматом.

Доказательство. Для доказательства теоремы достаточно показать, что если не квазимонотонный, не монотонный или не аддитивный автомат является моделью автомата S, то автомат S также не квазимонотонный, не монотонный или не аддитивный соответственно. Для этого, в свою очередь, достаточно убедиться в том, что если функция λ или функция δ автомата L не квазимонотонна (не монотонна или не аддитивна) и автомат S гомоморфно отображается на L, то функция ψ или соответственно функция φ автомата S также не квазимонотонна (не монотонна или не аддитивна соответственно). Сделаем это для функции переходов, для функций выходов рассуждения аналогичны.

Пусть далее $h_1h_2h_3$ есть гомоморфизм S на L и функция λ не квазимонотонна. Тогда по тесту квазимонотонности существует подмножество $A = \{u_1p_1, \ldots, u_mp_m\} \subseteq U \times P$, имеющее нижнюю грань в $U \times P$, такое, что подмножество $\lambda(A) \subseteq P$ не имеет нижней грани в P. Определим $x_i = \sup h_1^{-1}(u_i)$ и $q_i = \sup h_2^{-1}(p_i)$ для $i=1, \ldots, m$ и $B = \{x_1q_1, \ldots, x_mq_m\} \subseteq X \times Q$. Входные символы $u_1, \ldots, u_m$ имеют общую нижнюю грань в U, состояния $p_1, \ldots, p_m$ имеют общую нижнюю грань в P, поэтому входные символы $x_1, \ldots, x_m$ имеют общую нижнюю грань в X, состояния $q_1, \ldots, q_m$ – общую нижнюю грань в Q, а подмножество B –

нижнюю грань в $X\times Q$. Из соотношений гомоморфности, связывающих L и S, следует $\lambda(A)=h_2\psi(B)$, поэтому $h_2\psi(B)$ не имеет нижней грани в P. Если же допустить, что функция ψ квазимонотонна, то по тесту квазимонотонности подмножество $\psi(B)\subseteq Q$ будет иметь нижнюю грань в Q, а подмножество $h_2\psi(B)\subseteq P$, поскольку h_2 – гомоморфизм Q на P, – нижнюю грань в P. Следовательно, функция ψ не квазимонотонна.

Пусть теперь функция λ не монотонна, т.е. существуют u_1p_1 и u_2p_2 в $U\times P$ такие, что $u_1p_1\le u_2p_2$ и не $\lambda(u_1p_1)\le\lambda(u_2p_2)$. Определим $x_i=\sup h_1^{-1}(u_i)$ и $q_i=\sup h_2^{-1}(p_i)$ для $i=1, 2$. Из $u_1p_1\le u_2p_2$ следует $x_1q_1\le x_2q_2$. Кроме того, $h_2\psi(x_1,q_1)=\lambda(u_1p_1)$ и $h_2\psi(x_2,q_2)=\lambda(u_2p_2)$, поэтому не $h_2\psi(x_1,q_1)\le h_2\psi(x_2,q_2)$ и, следовательно, не $\psi(x_1,q_1)\le\psi(x_2,q_2)$, т.е. функция ψ не монотонна.

Пусть теперь функция λ не аддитивна, т.е. существуют u_1p_1 и u_2p_2 в $U\times P$ такие, что $\lambda(u_1p_1+u_2p_2)\ne\lambda(u_1p_1)+\lambda(u_2p_2)$. В этом случае для любых $x_i\in h_1^{-1}(u_i)$ и $q_i\in h_2^{-1}(p_i)$ для $i=1, 2$ можно записать

$$h_2\psi(x_1q_1+x_2q_2)=h_2\psi(x_1+x_2,q_1+q_2)=\lambda(h_1x_1+h_1x_2,h_2q_1+h_2q_2)=$$
$$=\lambda(u_1p_1+u_2p_2)\ne\lambda(u_1p_1)+\lambda(u_2p_2)=h_2\psi(x_1,q_1)+h_2\psi(x_2,q_2)=$$
$$=h_2(\psi(x_1,q_1)+\psi(x_2,q_2)),$$

откуда

$$\psi(x_1q_1+x_2q_2)\ne\psi(x_1,q_1)+\psi(x_2,q_2),$$

т.е. функция ψ не аддитивна. Теорема доказана.

Для автомата S и конгруэнций α, β, γ на его полурешетках X, Q, Y соответственно определяется автомат $S\uparrow\alpha\beta\gamma=(X\uparrow\alpha,Q\uparrow\beta,Y\uparrow\gamma,\psi',\varphi')$, в котором ψ' и φ' являются адекватными моделями функций ψ и φ с точностями $(\alpha\times\beta,\beta)$ и $(\alpha\times\beta,\gamma)$ соответственно. Если он является моделью автомата S, то он называется *адекватной моделью автомата S с точностью* $\alpha\beta\gamma$. Тройка конгруэнций α, β, γ *стабильна в автомате* S, если пара $(\alpha\times\beta,\beta)$ сохраняется функцией ψ, а пара $(\alpha\times\beta,\gamma)$ – функцией φ.

Теорема 7. Если тройка конгруэнций $\alpha\beta\gamma$ стабильна в автомате S, то автомат $S\uparrow\alpha\beta\gamma$ является моделью автомата S и, следовательно, его адекватной моделью. Обратно, если автомат L является моделью автомата S, то существует стабильная в S тройка конгруэнций $\alpha\beta\gamma$ такая, что L и $S\uparrow\alpha\beta\gamma$ изоморфны и, следовательно, L изоморфен адекватной модели S с точностью $\alpha\beta\gamma$.

Доказательство. Пусть отображения $h_1:X\to X\uparrow\alpha$, $h_2:Q\to Q\uparrow\beta$, $h_3:Y\to Y\uparrow\gamma$ – канонические гомоморфизмы полурешеток, т.е. $h_1(x)=\sup[x]_\alpha$, $h_2(q)=\sup[q]_\beta$, $h_3(y)=\sup[y]_\gamma$. Пусть $xq\in X\times Q$, $x'=\sup[x]_\alpha$, $q'=\sup[q]_\beta$. Тогда $h_1(x')=x'=h_1(x)$, $x'\alpha x$, $h_2(q')=q'=h_2(q)$, $q'\beta q$ и в силу стабильности тройки $\alpha\beta\gamma$ в S будем иметь $\psi(x,q)\beta\psi(x',q')$ и $\varphi(x,q)\gamma\varphi(x',q')$, поэтому

$$\psi'(x',q')=\sup[\psi(x',q')]_\beta=\sup[\psi(x,q)]_\beta$$

и $\varphi'(x',q')=\sup[\varphi(x',q')]_\gamma=\sup[\varphi(x,q)]_\gamma$, откуда по определению h_2 и h_3 следует $h_2\psi(x,q)=\psi'(x',q')=\psi'(h_1x,h_2q)$ и $h_3\varphi(x,q)=\varphi'(x',q')=\varphi'(h_1x,h_2q)$. Таким образом, $h_1h_2h_3$ есть гомоморфизм S на $S\uparrow\alpha\beta\gamma$. Этим доказано, что $S\uparrow\alpha\beta\gamma$ является моделью S.

Для доказательства второго предложения теоремы рассмотрим произвольный гомоморфизм $h_1h_2h_3$ автомата S на автомат L. Пусть α, β и γ являются ядерными конгруэнциями эпиморфизмов $h_1:X\to U$, $h_2:Q\to P$ и $h_3:Y\to V$ соответственно. Тогда если $a\alpha b$ и $p\beta q$, то $h_1(a)=h_1(b)$ и $h_2(p)=h_2(q)$, в силу чего $\lambda(h_1a,h_2p)=\lambda(h_1b,h_2q)=h_2\psi(a,p)=h_2\psi(b,q)$ и $\delta(h_1a,h_2p)=\delta(h_1b,h_2q)=h_3\varphi(a,p)=h_3\varphi(b,q)$, поэтому $\psi(a,p)\beta\psi(b,q)$ и $\varphi(a,p)\gamma\varphi(b,q)$, т.е. тройка конгруэнций $\alpha\beta\gamma$ стабильна в S. Определим изоморфизмы полурешеток $g_1:X\uparrow\alpha\to U$, $g_2:Q\uparrow\beta\to P$, $g_3:Y\uparrow\gamma\to V$ как $g_1(x)=h_1(x)$, $g_2(q)=h_2(q)$, $g_3(y)=h_3(y)$. Пусть ψ' – функция переходов и φ' – функция выходов автомата $S\uparrow\alpha\beta\gamma$. Тогда

$$\psi'(x,q)=\sup[\psi(x,q)]_\beta \text{ и } \varphi'(x,q)=\sup[\varphi(x,q)]_\gamma,$$

поэтому $\psi'(x,q)\beta\psi(x,q)$ и $\varphi'(x,q)\gamma\varphi(x,q)$, откуда по определению β и γ следует $h_2\psi'(x,q)=h_2\psi(x,q)=\lambda(h_1x,h_2q)$ и $h_3\varphi'(x,q)=\varphi(x,q)=\delta(h_1x,h_2q)$, в силу чего по определению g_1, g_2 и g_3 имеет место $g_2\psi'(x,q)=\lambda(g_1x,g_2q)$ и $g_3\varphi'(x,q)=\delta(g_1x,g_2q)$. Таким образом, $g_1g_2g_3$ есть изоморфизм $S\uparrow\alpha\beta\gamma$ на L. Теорема доказана.

В силу этой теоремы все модели любого автомата на полурешутках с точностью до изоморфизма исчерпываются его адекватными моделями; последние, в свою очередь, полностью характеризуются в терминах стабильных троек конгруэнций на полурешетках автомата.

Из теоремы 7 и предложения (2) теоремы 5 следует также, что адекватные модели аддитивных автоматов аддитивны.

Адекватные модели полурешеточно упорядоченных алгебр

Если A – полурешетка и Ω – множество некоторых конечно-местных операций на множестве A, монотонных относительно порядка в полурешетке A, то пара (A, Ω) называется *полурешеточно упорядоченной алгеброй*. В этом случае, если ρ – конгруэнция на A, ω – произвольная n-местная операция в Ω, ω_ρ – ее адекватная модель с точностью (ρ^n, ρ) и $\Omega_\rho=\{\omega_\rho:\omega\in\Omega\}$, то пара $(A\uparrow\rho, \Omega_\rho)$ является также полурешеточно упорядоченной алгеброй и называется *адекватной моделью алгебры* (A, Ω) *с точностью* ρ.

Адекватные модели полурешеточно упорядоченных алгебр применяются в адекватном моделировании с различной степенью точности интегральных схем логического управления. Примеры этого можно найти в [2].

ЛИТЕРАТУРА

1. *Агибалов Г.П., Буланов В.А., Липский В.Б., Румянцев Б.Ф.* Логическое проектирование переключательных автоматов. Томск: Изд-во Том. ун-та, 1983. 154 с.
2. *Агибалов Г.П.* Дискретные автоматы на полурешетках. Томск: Изд-во Том. ун-та, 1993. 227 с.
3. *Агибалов Г.П.* Квазимонотонные функции и их минимизация // Кибернетика. 1989. № 2. С. 111–113.

Статья поступила в научную редакцию 21 февраля 2000 г.