С. П. Ковалев, Алгебраический подход к проектированию распределенных вычислительных систем, *Сиб. журн. индустр. матем.*, 2007, том 10, номер 2, 70–84

Сибирский журнал
индустриальной математики
Апрель–июнь, 2007. Том X, № 2(30)

УДК 519.68

АЛГЕБРАИЧЕСКИЙ ПОДХОД К ПРОЕКТИРОВАНИЮ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

С. П. Ковалев

Дается алгебраическое описание класса конечных моделей вычислений, реализуемых в современных компьютерах, и правил сборки из них крупномасштабных распределенных вычислительных систем класса Grid. Доказано, что адекватным математическим средством моделирования компьютерных вычислений служит аппарат полупримальных алгебр, клоны операций которых состоят из всех функций, сохраняющих совокупность их подалгебр. Найдены штрихи Шеффера в клонах операций полупримальных алгебр. Указан критерий возможности привлекать технику доказательства конечнозначных логик для верификации моделей вычислений. Предложено обобщение понятия гомоморфизма, превращающее класс полупримальных алгебр в категорию, которая служит формальным определением дисциплины проектирования распределенных вычислительных систем.

Введение

Выполнение значительных объемов арифметических вычислений является традиционной сферой приложения компьютерных технологий. Вычислительные задачи формулируются на абстрактном математическом языке, поэтому при проектировании автоматизированных систем для их решения естественным образом задействуются формальные математические методы инженерии программного обеспечения. Такие методы позволяют создавать формальные спецификации и модели архитектуры систем и далее преобразовывать их в программы с последующей верификацией (доказательством правильности). При этом удается гарантировать корректность получаемых результатов, привлекая аппарат алгебры, логики и дискретной математики.

Отправным пунктом для применения формальных методов служит представление вычислительной задачи в виде совокупности операций, выполняемых над числовыми данными различной природы (натуральными, вещественными числами и т. д.). Действие каждой операции задается как функция на множестве возможных значений данных. Множества значений вместе с правилами выполнения операций образуют абстрактные типы данных (АТД), описываемые на математическом языке (в общем случае многосортными) алгебрами [1, 2]. Различным фрагментам задачи сопоставляются компоненты вычислительной системы, отвечающие за выполнение определенных наборов операций. В ходе функционирования системы данные передаются для обработки между экземплярами компонентов, выбор которых при решении сложных задач приходится осуществлять динамически исходя из текущих профилей их загрузки. Крупномасштабные распределенные вычислительные системы с динамическим развертыванием задач известны под общим названием Grid [3]. На математическом языке динамика функционирования многокомпонентных систем описывается с привлечением аппарата мутирующих (эволюционных) алгебр [4], известных также как машины абстрактных состояний (МАС). В рамках этого аппарата подходящая алгебра сопоставляется каждому состоянию каждого компонента и вводится специальный метаязык для описания правил перехода

между состояниями. Формальное описание и анализ механизма динамического развертывания, применяемого в Grid-системах, при помощи техники MAC приведено в работе [5].

Программная реализация вычислительной системы заключается в переводе алгебраической спецификации на язык программирования, поддерживаемый целевой аппаратной платформой. При этом возникает ряд сложностей, связанных с невозможностью точного воспроизведения свойств математических объектов средствами современных компьютеров. Так, любой элемент данных может иметь лишь конечное количество различных значений, определяемое объемом доступных ресурсов памяти. Поэтому стандартные модели арифметики, обладающие бесконечными основными множествами, остаются сугубо абстрактными типами данных, не реализуемыми на практике. Существуют различные способы построения моделей вычислений — (односортных) конечных алгебр, в той или иной степени «аппроксимирующих» поведение требуемых АТД и реализуемых в программно-аппаратных средствах. Различные модели вычислений оптимизируются по различным критериям эффективности, поэтому они часто плохо совмещаются друг с другом, и при организации обмена данными приходится реализовывать сложные процедуры согласования значений. Систематический подход к построению и анализу моделей вычислений предложен в [6].

Возникающие здесь алгебраические конструкции изучены значительно слабее, чем их абстрактные оригиналы. Применяются методы дискретной математики [7], с их помощью наиболее хорошо исследованы операции над представлениями чисел в двоичной системе счисления с фиксированным количеством разрядов. Однако такое представление не всегда оптимально, особенно при кодировании числовых значений в целях передачи между компонентами вычислительной системы. Поэтому при проектировании вычислительных систем требуется единое алгебраическое описание класса практически полезных моделей вычислений и правил сборки из них распределенных систем с динамическим развертыванием. Это описание не должно зависеть от правил представления числовых значений.

Такое описание предложено в настоящей работе. Естественным критерием практической полезности модели вычислений, определяющим границы класса рассматриваемых конечных алгебр, является возможность управления потоком вычислений путем проверки равенства значения элемента данных любому из поддерживаемых чисел. Доказывается, что этот критерий выделяет так называемые полупримальные (semi-primal) алгебры, однозначно характеризующиеся совокупностью своих подалгебр. Также доказывается, что он эквивалентен наличию (достаточно большого объема) адресуемой памяти, в которой можно хранить массивы данных. Любой из этих признаков является характерным для PAM-машины — классической модели вычислительного устройства общего назначения, исходя из возможностей которого специфицируются и анализируются вычислительные алгоритмы [8]. Для проектирования многокомпонентных вычислительных систем, (динамически) развертываемых на разнородных реализациях PAM-машины, применяется формализация подхода на основе контрактов, данная при помощи аппарата MAC [9].

Основные сведения о полупримальных алгебрах приводятся в разделе 1. Разд. 2 посвящен функциональным свойствам полупримальных алгебр: базисам, штрихам Шеффера, алгебраическим представлениям многозначных логик. В разд. 3 дается формальное доказательство пригодности полупримальных алгебр в качестве моделей архитектуры распределенных вычислительных систем, при этом используется аппарат теории категорий. В заключении намечены направления дальнейших исследований в области алгебраического подхода к проектированию распределенных вычислительных систем.

1. Класс полупримальных алгебр

Пусть $\mathfrak{A}$ — конечная алгебра, будем обозначать через $\operatorname{Sub}\mathfrak{A}$ совокупность всех подалгебр $\mathfrak{A}$. Следуя часто используемому соглашению (см, например, [10]), мы полагаем по определению, что $\emptyset \in \operatorname{Sub}\mathfrak{A}$ для любой алгебры $\mathfrak{A}$, в том числе если среди ее термов имеются константы. Это соглашение является существенным при изучении структурных свойств совокупности подалгебр. Именно, обозначим через SetSL_{01} множество всех нижних полурешеток множеств, частично упорядоченных включением, содержащих пустое множество и конечный наибольший элемент. В силу теоремы Биркгофа — Фринка Sub является отображением класса всех конечных алгебр на SetSL_{01}. Подчеркнем, что для целей настоящей работы $\operatorname{Sub}\mathfrak{A}$ рассматривается как нижняя полурешетка, несмотря на наличие на ней решеточной структуры. В дальнейшем мы определим на SetSL_{01} структуру категории такую, что сужение отображения Sub на интересующий нас класс алгебр будет расширено до функтора.

Пусть $S \in \mathrm{SetSL}_{01}$. Введем обозначение $\cup S \rightleftharpoons \bigcup\limits_{A\in S} A$, $\operatorname{Mt} S \rightleftharpoons \bigcap\limits_{A\in S\setminus\{\emptyset\}} A$. Будем называть нижнюю полурешетку S главной, если множество $\operatorname{Mt} S$ непусто, так что оно является единственным атомом S. Через $S[X]$ будем обозначать наименьшее множество из S, содержащее множество $X \subseteq \cup S$. Преобразование $X \mapsto S[X]$ является замыканием на $2^{\cup S}$ с областью значений S. Если $S = \operatorname{Sub}\mathfrak{A}$ для некоторой алгебры $\mathfrak{A}$, то $S[X]$ — подалгебра $\mathfrak{A}$, порожденная X (для непустого X). Далее, через $\operatorname{Sub}_{0,1} S$ будем обозначать семейство нижних подполурешеток S, принадлежащих SetSL_{01}. Всякое такое семейство является решеткой относительно теоретико-множественного включения, обладающей нулем $\{\emptyset, \cup S\}$ и единицей S.

Для непустой конечной алгебры $\mathfrak{A}$ будем обозначать через $|\mathfrak{A}|$ ее основное множество, через $\operatorname{Clo}\mathfrak{A}$ — семейство всех ее термальных операций, которое является клоном — классом функций на конечном множестве $|\mathfrak{A}|$, замкнутым относительно суперпозиции и содержащим все функции-селекторы I^j_k, где $I^j_k(x_1, \ldots, x_k) = x_j$. Совокупность всех клонов, состоящих из функций на множестве A, обозначим через $\mathcal{K}_A$. Эта совокупность является решеткой относительно теоретико-множественного включения. Решетка обладает нулем (это минимальный клон I_A, состоящий из всех селекторных функций), единицей (это полный клон P_A, состоящий из всех функций на множестве A), а также дуальными атомами (максимальными клонами), их семейство полностью описано в [11]. Выделим также клон констант, состоящий из селекторов и всех функций-констант из A. Клон из $\mathcal{K}_A$ называется функционально (или слабо) полным, если его объединение с клоном констант образует P_A. Ясно, что с точки зрения компьютерной реализации арифметики только функционально полные клоны представляют интерес. Достаточным условием функциональной полноты является наличие в клоне тернарного дискриминатора — операции, определяемой следующим образом:

$$d(x, y, z) \rightleftharpoons \begin{cases} z, & x = y, \\ x, & x \neq y. \end{cases}$$

Хорошо известно, что каждый клон состоит из всех функций, сохраняющих некоторое семейство отношений. Клон, состоящий из функций, сохраняющих семейство отношений R, обозначается $\operatorname{Pol} R$. Например, в дальнейшем нам встретятся клоны вида $\mathrm{M}^\rho_A \rightleftharpoons \operatorname{Pol}\{\rho\}$, где ρ — отношение эквивалентности на множестве A. Каждый такой клон совпадает с P_A, если ρ тривиально (т. е. совпадает с равенством либо с $A \times A$). В противном случае он является максимальным в решетке $\mathcal{K}_A$ и не является функционально полным. Отношение ρ является единственной конгруэнцией алгебры, клон операций которой совпадает с M^ρ_A. В связи с этим для произвольной алгебры возникает задача

нахождения ее обеднений и обогащений, имеющих конгруэнцию ρ. Решение этой задачи порождает следующие конструкции.

Определение 1. Пусть $\mathfrak{A}$ — конечная алгебра, ρ — отношение эквивалентности на $|\mathfrak{A}|$. Конгруэнц-проекцией алгебры $\mathfrak{A}$ на ρ называется алгебра $\mathfrak{A}(\rho)$ с основным множеством $|\mathfrak{A}|$ и клоном операций $\operatorname{Clo}\mathfrak{A} \cap \mathrm{M}^{\rho}_{|\mathfrak{A}|}$. Конгруэнц-расширением алгебры $\mathfrak{A}$ по ρ называется конгруэнц-проекция на ρ любой алгебры, обладающей совокупностью подалгебр $\operatorname{Sub}\mathfrak{A} \cap \{\rho(X) \mid X \subseteq |\mathfrak{A}|\}$. Класс всех конгруэнц-расширений алгебры $\mathfrak{A}$ по ρ обозначается через $\rho(\mathfrak{A})$.

Обозначим через $\operatorname{Clo}_k\mathfrak{A}$ совокупность всех k-местных операций из $\operatorname{Clo}\mathfrak{A}$. Разбиение $\operatorname{Clo}\mathfrak{A} = \bigcup\limits_{k\geq 0} \operatorname{Clo}_k\mathfrak{A}$ позволяет рассматривать $\operatorname{Clo}\mathfrak{A}$ как счетносортную алгебру. В связи с этим рассматриваются гомоморфизмы клонов: отображения, которые сохраняют арность операций, переводят селекторы I^j_k в I^j_k и суперпозиции в суперпозиции. Отметим, что если $\operatorname{Clo}_0\mathfrak{A}$ непусто (т. е. $\operatorname{Clo}\mathfrak{A}$ содержит функции-константы), то $\operatorname{Sub}\mathfrak{A}$ является главной нижней полурешеткой. В этом случае мы будем называть алгебру $\mathfrak{A}$ главной. Для удобства описания главных алгебр введем обозначение $\operatorname{Mt}\mathfrak{A} \rightleftharpoons \operatorname{Mt}\operatorname{Sub}\mathfrak{A}$.

Для построения семейств алгебр, характеризующихся различными свойствами, традиционно используются такие конструкции, как гомоморфизмы, прямые и свободные произведения, фактор-алгебры. Для целей настоящей работы необходимо привлечь следующие дополнительные конструкции.

Определение 2. n-й матричной степенью конечной алгебры $\mathfrak{A}$ называется алгебра $\mathfrak{A}^{[n]}$ с основным множеством $|\mathfrak{A}|^n$ и клоном операций $\bigcup\limits_{k\geq 0}\{(t_1,\ldots,t_n) \mid t_i \in \operatorname{Clo}_{kn}\mathfrak{A},\ i=1,\ldots,n\}$.

Определение 3. Пусть $\mathfrak{A}$ — конечная алгебра. Унарный терм $t \in \operatorname{Clo}_1\mathfrak{A}$ называется идемпотентным, если $t(t(x)) = t(x)$ для всякого $x \in |\mathfrak{A}|$. Термальной проекцией алгебры $\mathfrak{A}$ на идемпотентный терм t называется алгебра $\mathfrak{A}(t)$ с основным множеством $t(|\mathfrak{A}|)$ и клоном операций $\{t \circ s \restriction_{t(|\mathfrak{A}|)} \mid s \in \operatorname{Clo}\mathfrak{A}\}$.

В математике эти операции используются при изучении категорной эквивалентности многообразий алгебр [10]. Они также играют важную роль в прикладных задачах построения моделей компьютерных вычислений, например с их помощью строится поразрядное разложение машинных представлений чисел [6].

В настоящей работе рассматриваются конечные алгебры $\mathfrak{A}$, для которых $\operatorname{Clo}\mathfrak{A} = \operatorname{Pol}\operatorname{Sub}\mathfrak{A}$. Такие алгебры называются полупримальными (semiprimal) [12], мы будем называть их клоны операций также полупримальными. Из универсальной алгебры известны следующие свойства полупримальных алгебр.

Предложение 1. *Пусть $\mathfrak{A}$ — полупримальная алгебра. Тогда*:

(i) $\mathfrak{A}$ *проста*;

(ii) $\mathfrak{A}$ *не имеет нетождественных автоморфизмов*;

(iii) $\mathfrak{A}$ *является квазипримальной* (*т. е. содержит тернарный дискриминатор*);

(iv) $\operatorname{Clo}\mathfrak{A}$ *функционально полон*;

(v) $\operatorname{Mt}\mathfrak{A}$ *является ее центроидом* (*множеством значений констант, содержащихся в клоне ее операций*);

(vi) $\operatorname{Clo}\mathfrak{A}$ *изоморфен клону операций полупримальной алгебры $\mathfrak{B}$ тогда и только тогда, когда существует биекция $\varphi\colon |\mathfrak{A}| \to |\mathfrak{B}|$, индуцирующая биекцию $\varphi^+\colon \operatorname{Sub}\mathfrak{A} \to \operatorname{Sub}\mathfrak{B}$*;

(vii) *всякая подалгебра $\mathfrak{A}$ является полупримальной алгеброй*;

(viii) *если $\mathfrak{A}$ неодноэлементна и $\mathfrak{B}$ также неодноэлементная полупримальная алгебра, то прямое произведение $\mathfrak{A} \times \mathfrak{B}$ не является полупримальной алгеброй*;

(ix) *неодноэлементный гомоморфный образ алгебры* $\mathfrak{A}$ *изоморфен ей*;

(x) *для всякого отношения эквивалентности* $\rho \subseteq |\mathfrak{A}| \times |\mathfrak{A}|$ *фактор-алгебра* $\mathfrak{A}(\rho)/\rho$ *является полупримальной алгеброй, обладающей совокупностью подалгебр* $\{\cap W \mid W \subseteq \{\rho(A)/\rho \mid A \in \operatorname{Sub}\mathfrak{A}\}\}$;

(xi) $\mathfrak{A}^{[n]}$ *является полупримальной алгеброй, обладающей совокупностью подалгебр* $\{A^n \mid A \in \operatorname{Sub}\mathfrak{A}\} \cong \operatorname{Sub}\mathfrak{A}$;

(xii) *для всякого идемпотентного терма* $t \in \operatorname{Clo}_1\mathfrak{A}$ *термальная проекция* $\mathfrak{A}(t)$ *является полупримальной алгеброй, обладающей совокупностью подалгебр* $\{t(A) \mid A \in \operatorname{Sub}\mathfrak{A}\} = \{A \cap t(|\mathfrak{A}|) \mid A \in \operatorname{Sub}\mathfrak{A}\}$.

Если $|\operatorname{Sub}\mathfrak{A}| = 1$, то $\operatorname{Sub}\mathfrak{A} = \{\emptyset\}$, так что $\mathfrak{A}$ — тривиальная (пустая) алгебра. Если $|\operatorname{Sub}\mathfrak{A}| = 2$, т. е. $\operatorname{Sub}\mathfrak{A} = \{\emptyset, |\mathfrak{A}|\}$, то $\operatorname{Pol}\operatorname{Sub}\mathfrak{A} = \mathrm{P}_{|\mathfrak{A}|}$ (в этом случае алгебра $\mathfrak{A}$ называется примальной). Если $|\operatorname{Sub}\mathfrak{A}| = 3$, т. е. $\operatorname{Sub}\mathfrak{A} = \{\emptyset, X, |\mathfrak{A}|\}$, где $\emptyset \subset X \subset |\mathfrak{A}|$, то клон $\operatorname{Pol}\operatorname{Sub}\mathfrak{A}$ обозначается через $\mathrm{C}^X_{|\mathfrak{A}|}$; он является максимальным. Для нашего рассмотрения важную роль играет также случай $\operatorname{Sub}\mathfrak{A} = 2^{|\mathfrak{A}|}$ (для непустой алгебры $\mathfrak{A}$). Здесь $\operatorname{Pol}\operatorname{Sub}\mathfrak{A} = \mathrm{C}_{|\mathfrak{A}|}$, где через C_A обозначается клон всех функций на множестве A, значение которых на каждом наборе аргументов равно одному из них. Этот случай является предельным: для всякой полупримальной алгебры $\mathfrak{A}$ имеет место соотношение $\mathrm{C}_{|\mathfrak{A}|} \subseteq \operatorname{Clo}\mathfrak{A}$. Как мы увидим далее, это свойство является характеристическим для полупримальных алгебр и, по сути, определяет их пригодность в качестве формальных моделей вычислительных систем, реализуемых на базе современных цифровых компьютеров.

Используя технику представления решеток, можно строить полупримальные алгебры с произвольными полурешетками подалгебр, принадлежащими SetSL_{01}. Конструкция, обладающая значительной степенью общности, выглядит следующим образом. Пусть X — решетка, A — такое конечное частично упорядоченное множество, что: (i) $X \subseteq A$; (ii) на A задан частичный порядок, сужение которого на X совпадает с решеточным; (iii) единица решетки X является максимальным элементом A. Рассмотрим алгебру $\mathfrak{L}^X_A$ с основным множеством A и клоном операций $\operatorname{Pol}\{\{y \in A \mid y \leq x\} \mid x \in X\}$. Она является главной полупримальной алгеброй, причем $\operatorname{Sub}\mathfrak{L}^X_A \setminus \{\emptyset\} \cong X$, $\operatorname{Mt}\mathfrak{L}^X_A = \{y \in A \mid y \leqslant 0_X\}$.

Возьмем в качестве X множество $D(n)$ делителей некоторого натурального числа $n > 1$, а в качестве A — начальный отрезок неотрицательных целых чисел $[0, n]$, частично упорядоченный отношением, обратным к отношению делимости. Этот порядок превращает $D(n)$ в решетку с нулем n и единицей 1. Соответствующая полупримальная алгебра L_{n+1} изоморфна алгебраическому представлению $(n+1)$-значной логики Лукасевича с истинностным значением n (этот факт известен как критерий Мак-Нотона, см. [13]). Приложению аппарата логики Лукасевича к задачам моделирования компьютерной арифметики посвящена работа [14].

Первым результатом настоящей работы является критерий изоморфизма нижних полурешеток подалгебр полупримальных алгебр, формулируемый следующим образом.

Предложение 2. *Пусть* $\mathfrak{A}_1$ *и* $\mathfrak{A}_2$ *— полупримальные алгебры. Для того чтобы* $\operatorname{Sub}\mathfrak{A}_1$ *была изоморфна* $\operatorname{Sub}\mathfrak{A}_2$*, необходимо и достаточно, чтобы существовали такие идемпотентные термы* $t_i \in \operatorname{Clo}_1\mathfrak{A}_i$, $i = 1, 2$, *что* $\operatorname{Sub}\mathfrak{A}_i[t_i(A)] = A$ *для всякого* $A \in \operatorname{Sub}\mathfrak{A}_i$ *и, кроме того,* $\mathfrak{A}_1(t_1) \cong \mathfrak{A}_2(t_2)$.

Доказательство. С одной стороны, если требуемые t_i существуют, то преобразование $X \mapsto \operatorname{Sub}\mathfrak{A}_i[X]$ задает изоморфизм между $\operatorname{Sub}\mathfrak{A}_i(t_i)$ и $\operatorname{Sub}\mathfrak{A}_i$, поэтому $\operatorname{Sub}\mathfrak{A}_1 \cong \operatorname{Sub}\mathfrak{A}_2$. С другой стороны, пусть $\operatorname{Sub}\mathfrak{A}_1 \cong \operatorname{Sub}\mathfrak{A}_2$. Обозначим через Ξ_i совокупность неприводимых элементов нижней полурешетки

$\operatorname{Sub}\mathfrak{A}_i$. (Напомним, что элемент X называется неприводимым, если существует такой Y, что $X \cap Y \neq X$ и $X \cap Z = Y \cap Z$ для всякого Z такого, что $X \cap Z \neq X$.) Определим отображение $\xi_i \colon \Xi_i \to |\mathfrak{A}_i|$, выбирая $\xi_i(X)$ таким, что $\operatorname{Sub}\mathfrak{A}_i[\{\xi_i(X)\}] = X$ (существование $\xi_i(X)$ следует из неприводимости X). Построим термы $t_i \in \operatorname{Clo}_1\mathfrak{A}_i$, полагая $t_i(x) = x$, если $x \in \xi_i(\Xi_i)$, и $t_i(x) = \xi_i(A)$ для произвольного атома $A \subseteq \operatorname{Sub}\mathfrak{A}_i[\{x\}]$ в противном случае. Термы t_i удовлетворяют условию предложения, поскольку изоморфизм между $\operatorname{Sub}\mathfrak{A}_1$ и $\operatorname{Sub}\mathfrak{A}_2$ индуцирует биекцию между множествами $\xi_1(\Xi_1)$ и $\xi_2(\Xi_2)$, задающую изоморфизм между $\mathfrak{A}_1(t_1)$ и $\mathfrak{A}_2(t_2)$ в силу утверждения (vi) предложения 1. $\square$

Покажем теперь, что любая алгебра $\mathfrak{A}$, клон операций которой содержит $\mathrm{C}_{|\mathfrak{A}|}$, является полупримальной. Имеет место

Лемма 1. *Пусть* $S \in \mathrm{SetSL}_{01}$, $f \colon (\cup S)^k \to \cup S$. *Объединение полупримального клона* $\operatorname{Pol} S$ *с функцией* f *образует полупримальный клон* $\operatorname{Pol}(S \cap \operatorname{Sub}\langle \cup S, f\rangle)$.

Доказательство. Положим $F = S \setminus \operatorname{Sub}\langle \cup S, f\rangle$, $j = |F|$, в доказательстве нуждается случай $j > 0$. Ясно, что и все операции из $\operatorname{Pol} S$, и функция f сохраняют любое множество из $S \setminus F$. Нужно показать, что всякую операцию из $\operatorname{Pol}(S \setminus F)$ можно представить суперпозицией функции f и операций из $\operatorname{Pol} S$. Мы обобщим классическое доказательство максимальности клонов C^X_A, приведенное в [15]. Зафиксируем произвольную нумерацию элементов F — биективное отображение $\iota \colon F \to [1, j]$. Для каждого $i \in [1, j]$ выберем набор $\big(z^i_1, \dots, z^i_k\big) \in F^k_i$ такой, что $f\big(z^i_1, \dots, z^i_k\big) \notin F_i$. Пусть $g \in \operatorname{Pol}(S \setminus F)$ — произвольная m-местная функция, считаем $m > 0$ (т. е. рассматриваем константы как одноместные функции с фиктивным аргументом). Рассмотрим функцию $h_g \colon \cup S^{m+j} \to \cup S$, определенную следующим образом:

$$h_g(x_1, \dots, x_m, y_1, \dots, y_j) \rightleftharpoons \begin{cases} y_1, & S[\{x_1, \dots, x_m\}] \in F, \quad y_i \neq f\big(z^i_1, \dots, z^i_k\big), \\ & \text{где } i = \iota(S[\{x_1, \dots, x_m\}]); \\ g(x_1, \dots, x_m) & \text{иначе.} \end{cases}$$

Легко проверить, что $h_g \in \operatorname{Pol} S$. Для всякого $z \in \cup S$, $(x_1, \dots, x_m) \in \cup S^m$ положим

$$c_z(x_1, \dots, x_m) \rightleftharpoons \begin{cases} z, & z \in S[\{x_1, \dots, x_m\}]; \\ x_1 & \text{иначе,} \end{cases}$$

так что $c_z \in \operatorname{Pol} S$. Имеет место равенство

$$g(x_1, \dots, x_m) = h_g(x_1, \dots, x_m, f(c_{z^1_1}(x_1, \dots, x_m), \dots, c_{z^1_k}(x_1, \dots, x_m)), \dots, \\ f(c_{z^j_1}(x_1, \dots, x_m), \dots, c_{z^j_k}(x_1, \dots, x_m))). \quad \square$$

Отсюда следует основной результат настоящего раздела.

Теорема 1. *Пусть* A *— непустое конечное множество. Отображение* Sub *задает дуальный изоморфизм* $[\mathrm{C}_A, \mathrm{P}_A] \cong^D \operatorname{Sub}_{0,1} 2^A$.

Доказательство. Ввиду леммы 1 достаточно показать, что если $S \subset T$, то $\operatorname{Pol} S \supset \operatorname{Pol} T$ для произвольных $S, T \in \mathrm{SetSL}_{01}$ таких, что $\cup S = \cup T = A$. Действительно, пусть $Q \in T \setminus S$, зафиксируем некоторый $a \in S[Q] \setminus Q$. Определим $|Q|$-местную операцию q на A, полагая

$$q(x_1, \dots, x_{|Q|}) \rightleftharpoons \begin{cases} a, & \{x_1, \dots, x_{|Q|}\} = Q; \\ x_1 & \text{иначе.} \end{cases}$$

Непосредственно проверяется, что $q \in \operatorname{Pol} S \setminus \operatorname{Pol} T$. $\square$

Следствие 1. *Конечная алгебра* $\mathfrak{A}$ *является полупримальной тогда и только тогда, когда ее клон операций содержит* $\mathrm{C}_{|\mathfrak{A}|}$.

Отметим, что если нижняя полурешетка S является главной (например, если $S = \operatorname{Sub} \mathrm{L}_{n+1}$, где L_{n+1} — логика Лукасевича), то интервал $[\operatorname{Pol} S, \mathrm{P}_{\cup S}]$ дуально изоморфен решетке всех нижних подполурешеток нижней полурешетки $S \setminus \{\emptyset, \cup S\}$. Характеризация решетки всех нижних подполурешеток нижней полурешетки приводится в [16, 17].

2. Функциональные свойства полупримальных клонов

Для удобства задания термальных операций полупримальных алгебр будем считать, что их основные множества пронумерованы начальными отрезками неотрицательных целых чисел $E_{n+1} \rightleftharpoons [0, n]$, причем в целях исключения тривиальных случаев полагаем $n > 0$. Соответственно, определенные выше клоны, имеющие обозначения вида K_A (например, C_A), будут обозначаться как K_{n+1}.

Для всякого $i \in E_{n+1}$ определим на E_{n+1} операцию

$$\mathrm{If}^i(x, y, z) \rightleftharpoons \begin{cases} y, & x = i, \\ z, & x \neq i. \end{cases}$$

Для всякого $X \subseteq E_{n+1}$ обозначим $\mathrm{IFS}^X_{n+1} \rightleftharpoons \{\mathrm{If}^i \mid i \in X\}$. Имеет место

Теорема 2. (i) *Если* $|X| = n+1$, *то система функций* IFS^X_{n+1} *полна в* C_{n+1}.

(ii) *Если* $|X| = n$, *то* IFS^X_{n+1} *образует базис в* C_{n+1}.

(iii) *Если* $0 < |X| < n$, *то* IFS^X_{n+1} *образует базис в клоне, который не является функционально полным.*

Доказательство. Любая функция If^i принадлежит C_{n+1}, поскольку ее значение всегда совпадает со значением одного из аргументов. Далее, выберем произвольную k-местную операцию $t \in \mathrm{C}_{n+1}$. Определим отображение $\bar{t}\colon E^k_{n+1} \to \{1, \dots, k\}$, полагая $\bar{t}(x_1, \dots, x_k)$ равным индексу первого из таких аргументов из набора $(x_1, \dots, x_k)$, значение которых равно $t(x_1, \dots, x_k)$. Имеет место соотношение

$$\begin{aligned} t(x_1, \dots, x_k) = \mathrm{If}^0(x_1, \dots, \mathrm{If}^0(x_k, x_{\bar{t}(0,\dots,0,0)}, \dots, \\ \mathrm{If}^{n-1}(x_k, x_{\bar{t}(0,\dots,0,n-1)}, x_{\bar{t}(0,\dots,0,n)}) \dots) \dots, \\ \mathrm{If}^n(x_1, \dots, \mathrm{If}^0(x_k, x_{\bar{t}(n,\dots,n,0)}, \dots, \\ \mathrm{If}^{n-1}(x_k, x_{\bar{t}(n,\dots,n,n-1)}, x_{\bar{t}(n,\dots,n,n)}) \dots) \dots)). \end{aligned}$$

Далее, для всякого $j \in E_{n+1}$ имеем

$$\mathrm{If}^j(x, y, z) = \mathrm{If}^0(x, z, \dots, \mathrm{If}^{j-1}(x, z, \mathrm{If}^{j+1}(x, z, \dots, \mathrm{If}^n(x, z, y) \dots)) \dots).$$

Таким образом, система IFS^X_{n+1}, где $X = E_{n+1} \setminus \{j\}$, полна в C_{n+1}. Ее независимость следует из того, что для всякого непустого $Y \subset X$ система функций IFS^Y_{n+1} сохраняет нетривиальное отношение эквивалентности на E_{n+1}, отождествляющее друг с другом все элементы множества $E_{n+1} \setminus Y$ и попарно различающее все остальные значения. □

Отметим, что отсюда получается прямое доказательство функциональной полноты клона операций любой полупримальной алгебры (утверждение (iv) предложения 1). Действительно, произвольную k-местную функцию $t \in \mathrm{P}_{n+1}$

можно представить суперпозицией функций If^i, аналогичной приведенной в доказательстве теоремы 2 с заменой термов $x_{\bar{t}(a_1,\dots,a_k)}$ константами $t(a_1,\dots,a_k)$. По аналогии с ДНФ такое представление можно назвать If-*нормальной формой*. Из его существования вытекает даже функциональная полнота клона операций любой квазипримальной алгебры, поскольку $\mathrm{If}^i(x,y,z) = d(d(x,i,y),d(x,i,z),z)$, где d — тернарный дискриминатор.

Определим $(n+2)$-местную операцию CASE, полагая

$$\mathrm{CASE}(x_0,\dots,x_{n+1}) \rightleftharpoons \mathrm{If}^0(x_{n+1},x_0,\mathrm{If}^1(x_{n+1},x_1,\dots,\mathrm{If}^{n-1}(x_{n+1},x_{n-1},x_n)\dots)).$$

Предложение 3. *Функция* CASE *является штрихом Шеффера в* C_{n+1}.

Доказательство. $\mathrm{If}^i(x,y,z) = \mathrm{CASE}(\dots,y,\dots,x)$, где y находится на i-м месте, а на месте каждого из пропущенных аргументов находится z. □

Перейдем от C_{n+1} к произвольным полупримальным клонам. Выберем полурешетку $S \in \mathrm{SetSL}_{01}$ такую, что $\cup S = E_{n+1}$. Положим

$$F^S(x_0,\dots,x_{n+1}) \rightleftharpoons \begin{cases} c, & x_0 = \dots = x_{n+1} = c,\ \{c\} \in S; \\ \max(\{x_0,\dots,x_{n+1}\} \setminus \{x_{n+1}\}), & \\ \qquad |\{x_0,\dots,x_{n+1}\}| > 1, & \\ \qquad \{x_0,\dots,x_{n+1}\} \in S; & \\ \max(S[\{x_0,\dots,x_{n+1}\}] \setminus \{x_0,\dots,x_{n+1}\}) & \\ \qquad \text{в остальных случаях}, & \end{cases}$$

$$F^S_{\mathrm{CASE}}(x_0,\dots,x_{n+2}) \rightleftharpoons \begin{cases} F^S(x_0,\dots,x_{n+1}), & x_{n+2} = x_{n+1}; \\ \mathrm{CASE}(x_0,\dots,x_{n+1}), & x_{n+2} \neq x_{n+1}. \end{cases}$$

Предложение 4. *Функция* F^S_{CASE} *является штрихом Шеффера в* $\mathrm{Pol}\, S$.

Доказательство. Имеем

$$F^S(x_0,\dots,x_{n+1}) = F^S_{\mathrm{CASE}}(x_0,\dots,x_{n+1},x_{n+1}),$$
$$\mathrm{CASE}(x_0,\dots,x_{n+1}) = F^S_{\mathrm{CASE}}(x_0,\dots,x_{n+1},F^S(x_0,\dots,x_{n+1})).$$

Искомое утверждение следует из предложения 3 и теоремы 1, поскольку F^S сохраняет все множества из S и только их. □

Функциональные свойства клонов операций конечных алгебр изучаются, в частности, в связи с возможностью алгебраического представления конечнозначных пропозициональных логик. Такое представление имеет форму логической матрицы [13] — алгебраической системы вида $\mathfrak{M} \rightleftharpoons \langle V, f_1,\dots,f_l,\mathcal{D}\rangle$, где V — основное множество, $f_1,\dots,f_l$ — функциональные символы, $\mathcal{D}$ — одноместный предикатный символ. Элементам основного множества соответствуют логические значения, а функциональным символам — логические связки (операции), поэтому термы матрицы представляют собой логические формулы. Если логическая формула $f(x_1,\dots,x_k)$ такова, что $\mathfrak{M} \models \forall x_1 \dots \forall x_k \mathcal{D}(f(x_1,\dots,x_k))$, то она называется тавтологией данной логической матрицы, так что предикат $\mathcal{D}$ определяет подмножество логических значений, которые трактуются как истинные. Таким образом, строятся матричные представления пропозициональных логик — множеств тавтологий в языке, состоящем из имен переменных и связок. Интерес представляют нетривиальные логики, тавтологии которых образуют непустые собственные подмножества множества всех предложений языка.

Для одной и той же логики возможны эквивалентные матричные представления с различными наборами связок такие, что любая связка одного представления выражается через связки другого. Эти матрицы характеризуются

тем свойством, что они имеют одинаковые клоны операций. Вместе с тем не всякий клон может быть клоном операций матрицы некоторой нетривиальной логики. Кроме того, в ряде случаев возможно представление логической матрицы в виде алгебры, т. е. задание предиката $\mathcal{D}$ равенством. Дадим строгое определение этих свойств и исследуем их выполнимость для полупримальных алгебр.

Определение 4. Матричным обогащением конечной алгебры $\mathfrak{A}$ называется ее обогащение $\mathfrak{A}^{\mathcal{D}}$ одноместным предикатным символом $\mathcal{D}$ такое, что выполняются следующие условия:

(i) $\mathfrak{A}^{\mathcal{D}} \models \exists x \neg \mathcal{D}(x)$;

(ii) существуют такие число $k \geq 0$ и терм $f \in \mathrm{Clo}_k \mathfrak{A}$, что $\mathfrak{A}^{\mathcal{D}} \models \forall x_1 \ldots \forall x_k \mathcal{D}(f(x_1, \ldots, x_k))$;

(iii) существуют такие одноместные термы $t, u \in \mathrm{Clo}_1 \mathfrak{A}$, что $\mathfrak{A}^{\mathcal{D}} \models \forall x(\mathcal{D}(x) \Leftrightarrow t(x) = u(x))$.

Предложение 5. *Матричное обогащение полупримальной алгебры $\mathfrak{A}$ существует тогда и только тогда, когда существует элемент $x \in |\mathfrak{A}|$ такой, что $\{x\} \notin \mathrm{Sub}\,\mathfrak{A}$.*

Доказательство. Обозначим через A множество всех атомов нижней полурешетки $\mathrm{Sub}\,\mathfrak{A}$, положим $a = n + 1 - |A|$. Занумеруем $|\mathfrak{A}|$ числами от нуля до подходящего n (включительно) так, чтобы в интервал $[a, n]$ попало по одному элементу каждого атома. Если $a = 0$, то любое одноэлементное подмножество основного множества алгебры $\mathfrak{A}$ является ее подалгеброй, поэтому условия (i) и (ii) определения 4 не могут быть одновременно выполнены. В противном случае произвольно выберем число $d \in [1, a]$ и построим одноместную операцию v на E_{n+1} следующим образом:

$$v(x) \rightleftharpoons \begin{cases} x, & x \geq d, \\ \max(\mathrm{Sub}\,\mathfrak{A}[\{x\}] \cap [a, n]), & x < d. \end{cases}$$

Тогда $v \in \mathrm{Clo}_1 \mathfrak{A}$, $v(|\mathfrak{A}|) = [d, n]$ и равенство $v(x) = x$ определяет одноместный предикат, интерпретируемый интервалом $[d, n]$. $\square$

Отметим, что условия предложения 5 выполняются, если $\mathfrak{A}$ является главной полупримальной алгеброй. Любое ее матричное обогащение определяет такую логику, среди истинностных значений которой присутствуют элементы множества $\mathrm{Mt}\,\mathfrak{A}$.

Полученные результаты имеют прозрачное содержательное истолкование в контексте разработки распределенных вычислительных систем. Именно, функции If^i и CASE хорошо знакомы программистам — это условные операторы вида `if x = i then y else z` и легко реализуемый через них оператор выбора с вариантами. Теорема 2 показывает, что C_{n+1} является минимальным набором операций, содержащим достаточное количество условных операторов, чтобы различать все реализуемые значения числовых данных. Согласно предложению 3 этот набор можно построить, используя только операцию выбора значения, явно заданного для каждого возможного значения аргумента. Поэтому C_{n+1} естественно назвать табличной моделью вычислений, это самая бедная модель, позволяющая строить практически полезные вычислительные компоненты. На практике к ней прибегают в условиях наличия большого объема памяти и высокой сложности реализуемого алгоритма арифметических вычислений.

Из теорем 1 и 2 вытекает, что критерием пригодности алгебры в качестве формальной модели вычислений является ее принадлежность классу полупримальных алгебр. Предложение 4 утверждает, что любую такую модель можно построить из единственной операции (правда, достаточно большой арности). Наконец, предложение 5 определяет критерий наличия возможности

использовать технику доказательства конечнозначных логик для верификации вычислительных компонентов. Так, в приложениях возникают матрицы $(n+1)$-значных логик, обладающих единственным истинностным значением n, которое отвечает арифметическому переполнению [6]. Для обработки появления этого значения (флага) в ходе вычислений применяется условный оператор If^n, реализуемый в любом вычислительном компоненте.

Отметим, что операции CASE можно придать другое толкование. А именно, она реализует понятие одномерного массива — функции, определенной на множестве индексов (адресов), совпадающем с множеством реализуемых чисел. Мы видим, что для всякой конечной модели вычислений наличие адресуемой памяти достаточного объема эквивалентно наличию различающего множества условных операторов. Любой из этих признаков характеризует PAM-машину.

3. Категория вычислительных систем

Дадим формальную характеризацию полупримальных алгебр как моделей архитектуры распределенных вычислительных систем. С этой целью сконструируем из них категорию, определяющую формальное описание процесса реализации системы путем сборки из отдельных компонентов. Мы будем следовать работе [18], в которой такие описания названы формальными дисциплинами проектирования (architecture schools) и предложены правила их построения.

Определение 5 [18]. Формальной дисциплиной проектирования с категорией сигнатур SIG называется тройка $\langle \text{c-DESC}, \text{Conf}, \text{r-DESC}\rangle$, где:

c-DESC — категория формальных моделей компонентов и их композиций;

Conf — класс диаграмм в c-DESC, описывающих допустимые конфигурации систем;

r-DESC — категория трансформаций компонентов;

SIG — образ категории c-DESC относительно некоторого сигнатурного функтора sig.

При этом выполняются следующие условия:

(i) любая диаграмма из класса Conf имеет копредел;

(ii) $|\text{c-DESC}| = |\text{r-DESC}|$;

(iii) если объекты A и B изоморфны в c-DESC, то они изоморфны в r-DESC;

(iv) функтор sig унивалентен (т. е. инъективен на каждом $\mathrm{Mor}(A, B)$);

(v) функтор sig сохраняет копределы диаграмм из класса Conf;

(vi) функтор sig обладает левым сопряженным;

(vii) если диаграммы d_1 и d_2 таковы, что $(d_1; \mathrm{sig}) = (d_2; \mathrm{sig})$, то $d_1 \in \text{Conf}$ тогда и только тогда, когда $d_2 \in \text{Conf}$;

(viii) для всякой диаграммы $d\colon I \to \text{c-DESC}$ и семейства морфизмов $\phi = \{\varphi_i \mid \varphi_i \in \mathrm{Mor}(\text{r-DESC}), \mathrm{dom}\,\varphi_i = d_i,\ i \in I\}$, если $d \in \text{Conf}$, то $(d;\phi) \in \text{Conf}$ и существует $\psi \in \mathrm{Mor}(\text{r-DESC})$ такой, что $\mathrm{colim}(d;\phi) = \psi(\mathrm{colim}\, d)$.

Условия этого определения формализуют в языке теории категорий те общесистемные ограничения, в рамках которых работают проектировщики многокомпонентных программных систем. Процессам реализации компонентов отвечают трансформационные преобразования одних моделей в другие, а актам сборки сложных систем из их совокупностей (конфигураций) — построение копределов. Спецификации допустимых правил соединения компонентов в систему образуют их сигнатуры. Для каждой сигнатуры гарантируется наличие хотя бы одной реализации — образа относительно функтора, левого сопряженного к сигнатурному.

Нас интересует частный случай, когда объектами категории SIG являются контракты — формальные спецификации интерфейсов компонентов, однозначно определяющие их поведение при композиции [9]. Контракты полностью отделяют интерфейс от реализации в том смысле, что трансформациями являются в точности такие модификации компонента, которые сохраняют его

контракт. Применение контрактов является обязательным при разработке систем с динамическим развертыванием, результат работы которых не должен зависеть от выбора конкретного экземпляра компонента, реализующего требуемую функцию. Эффект от проектирования, основанного на контрактах, описывается следующим легко проверяемым утверждением.

Предложение 6. *Пусть категории* c-DESC, r-DESC, SIG *и класс* Conf *диаграмм в* c-DESC *таковы, что*:
(i) *любая диаграмма из класса* Conf *имеет копредел*;
(ii) *категория* r-DESC *состоит из всех объектов* c-DESC *и всех изоморфизмов* c-DESC;
(iii) *существует функтор* $\mathrm{sig}\colon$ c-DESC $\to$ SIG, *сюръективный на объектах и биективный на морфизмах*;
(iv) *класс* Conf *является абстрактным* (*замкнутым относительно изоморфизмов диаграмм*).
Тогда $\langle$c-DESC, Conf, r-DESC$\rangle$ *является формальной дисциплиной проектирования с категорией сигнатур* SIG.

Согласно результатам предыдущих разделов, при построении формальной дисциплины проектирования вычислительных систем исходным материалом служат полупримальные алгебры. Однако в силу утверждения (ix) предложения 1 традиционное понятие гомоморфизма между ними является слишком бедным для построения содержательной категории моделей вычислений, поэтому требуется обобщить его. Для этого мы вводим следующие конструкции.

Определение 6. Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — алгебры (необязательно полупримальные). Отображение $\varphi\colon |\mathfrak{A}| \to |\mathfrak{B}|$ называется субнепрерывным, если $\varphi^{-1}(X) \in \operatorname{Sub}\mathfrak{A}$ для любого $X \in \operatorname{Sub}\mathfrak{B}$. Отображение φ называется главным, если $\varphi(\operatorname{Mt}\mathfrak{A}) \subseteq \operatorname{Mt}\mathfrak{B}$.

Роль этих понятий иллюстрируется следующими примерами.

Предложение 7. *Отображение* $\varphi\colon |\mathfrak{A}| \to |\mathfrak{B}|$ *является главным и субнепрерывным, если выполняется хотя бы одно из следующих условий*:
(i) $\varphi = \varphi_1 \circ \varphi_2$, *где* $\varphi_1\colon |\mathfrak{A}| \to |\mathfrak{C}|$ *и* $\varphi_2\colon |\mathfrak{C}| \to |\mathfrak{B}|$ — *главные субнепрерывные отображения*;
(ii) *алгебры* $\mathfrak{A}$ *и* $\mathfrak{B}$ *имеют одинаковую сигнатуру,* φ — *гомоморфизм между ними*;
(iii) $\operatorname{Sub}\mathfrak{A} = 2^{|\mathfrak{A}|}$;
(iv) $\varphi(|\mathfrak{A}|) \subseteq B$ *либо* $\varphi(|\mathfrak{A}|) \cap B = \emptyset$ *для всякого* $B \in \operatorname{Sub}\mathfrak{B}$;
(v) $\{X \cap \varphi(|\mathfrak{A}|) \mid X \in \operatorname{Sub}\mathfrak{B}\} \subseteq \{\varphi(A) \mid A \in \operatorname{Sub}\mathfrak{A}\}$, $\operatorname{Mt}\mathfrak{A} = \emptyset$ *либо* $\operatorname{Mt}\mathfrak{B} \cap \varphi(|\mathfrak{A}|) \neq \emptyset$, φ *инъективно*;
(vi) $\operatorname{Sub}\mathfrak{B} = \operatorname{Sub}\mathfrak{C}/\rho$ *для некоторого* $\mathfrak{C} \in \rho(\mathfrak{A})$, $\varphi\colon a \mapsto \rho(\{a\})$, *где* ρ — *отношение эквивалентности на* $|\mathfrak{A}|$;
(vii) $\mathfrak{A} \cong \prod_{i\in I}\mathfrak{A}_i$, $\mathfrak{B} = \mathfrak{A}_j$, $\varphi\colon a \mapsto a_j$ *для некоторого* $j \in I$ (*здесь* $\mathfrak{A}$ *и различные* $\mathfrak{A}_i$ *имеют, вообще говоря, различные сигнатуры*);
(viii) $\mathfrak{B} \cong \mathfrak{A}^{[n]}$, $\varphi\colon a \mapsto (\varphi_1(a), \ldots, \varphi_n(a))$, *где* $\varphi_i\colon |\mathfrak{A}| \to |\mathfrak{A}|$ — *главные субнепрерывные отображения для всех* $i = 1, \ldots, n$.

Этот набор примеров является в определенном смысле исчерпывающим, как показывает

Предложение 8. *Отображение основных множеств алгебр является главным и субнепрерывным тогда и только тогда, когда оно раскладывается в композицию двух отображений, одно из которых удовлетворяет условию* (vi) *предложения 7, а второе — условию* (v).

Доказательство. Достаточность непосредственно следует из предложения 7, докажем необходимость. Пусть $\varphi\colon |\mathfrak{A}| \to |\mathfrak{B}|$ — главное субнепрерывное отображение. Выберем произвольную алгебру $\mathfrak{C} \in (\ker\varphi)(\mathfrak{A})$. Ее

фактор-алгебра $\mathfrak{C}/\ker\varphi$ обладает основным множеством $|\mathfrak{A}|/\ker\varphi$. Разложение φ в композицию сюръекции $\varphi_1\colon |\mathfrak{A}| \to |\mathfrak{C}/\ker\varphi|$ и инъекции $\varphi_2\colon |\mathfrak{C}/\ker\varphi| \to |\mathfrak{B}|$ удовлетворяет условиям предложения. $\square$

Интуитивно ясно, что свойство субнепрерывности отображения должно обеспечивать определенную степень согласованности между алгебраическими структурами его области и кообласти. При описании этой согласованности будем говорить, что отображение $\varphi\colon |\mathfrak{A}| \to |\mathfrak{B}|$ индуцирует гомоморфизм клонов $\varphi^*\colon \operatorname{Clo}\mathfrak{A} \to \operatorname{Clo}\mathfrak{B}$, если выполняется соотношение

$$\varphi t(x_1,\dots,x_k) = (\varphi^* t)(\varphi x_1,\dots,\varphi x_k) \text{ для всех } (x_1,\dots,x_k) \in |\mathfrak{A}|^k,$$
$$t \in \operatorname{Clo}_k\mathfrak{A}, \quad k \geq 0.$$

При этом все операции из $\varphi^*(\operatorname{Clo}\mathfrak{A})$ сохраняют множество $\varphi(|\mathfrak{A}|)$, поэтому можно рассматривать алгебру-образ $\varphi\mathfrak{A}$, обладающую основным множеством $\varphi(|\mathfrak{A}|)$ и клоном операций $\{\varphi^* t \restriction_{\varphi(|\mathfrak{A}|)} \mid t \in \operatorname{Clo}\mathfrak{A}\}$.

Ясно, что отображение φ может индуцировать гомоморфизм клонов только при условии, что отношение эквивалентности $\ker\varphi$ является конгруэнцией в $\mathfrak{A}$. Поэтому «наиболее близким» к гомоморфизму является отображение, индуцирующее гомоморфизм клонов, определенный на конгруэнц-проекции своей области на свое ядро. Для полупримальных алгебр таковыми оказываются в точности главные субнепрерывные отображения, как показывает

Предложение 9. *Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — полупримальные алгебры. Отображение $\varphi\colon |\mathfrak{A}| \to |\mathfrak{B}|$ индуцирует гомоморфизм клона $\operatorname{Clo}\mathfrak{A}(\ker\varphi)$ в клон $\operatorname{Clo}\mathfrak{B}$ тогда и только тогда, когда оно является главным субнепрерывным отображением основного множества алгебры $\mathfrak{A}(\ker\varphi)$ в основное множество алгебры $\mathfrak{B}$. При этом $\varphi\mathfrak{A}(\ker\varphi)$ является полупримальной алгеброй.*

Доказательство. Предположим сначала, что отображение $\varphi\colon |\mathfrak{A}(\ker\varphi)| \to |\mathfrak{B}|$ является главным и субнепрерывным. Прежде всего для всякого $c \in \operatorname{Clo}_0\mathfrak{A}$ положим $\varphi^* c = \varphi c \in \operatorname{Clo}_0\mathfrak{B}$. (Такое определение корректно, поскольку φ является главным и $\operatorname{Mt}\mathfrak{A}(\ker\varphi) = \operatorname{Mt}\mathfrak{A}$.) Далее, определим отображение $\varphi^{-1}\colon |\mathfrak{B}| \to |\mathfrak{A}|$, полагая $\varphi^{-1}y$ равным произвольному элементу множества $\varphi^{-1}(\{y\})$ для всякого $y \in \varphi(|\mathfrak{A}|)$ и произвольному элементу $v \in \varphi(|\mathfrak{A}|)$ для всех остальных $y \in |\mathfrak{B}|$. Кроме того, зафиксируем какой-либо линейный порядок на $|\mathfrak{A}|$. Выберем операцию $t \in \operatorname{Clo}_k\mathfrak{A}(\ker\varphi)$, $k > 0$, обозначим через $\operatorname{supp} t$ множество индексов всех ее существенных переменных. Для всякого набора $(y_1,\dots,y_k) \in |\mathfrak{B}|^k$ положим

$$\varphi^* t(y_1,\dots,y_k) \rightleftharpoons \begin{cases} \varphi t(\varphi^{-1}y_1,\dots,\varphi^{-1}y_k), & \bigcup\limits_{j\in\operatorname{supp} t}\{y_j\} \subseteq \varphi(|\mathfrak{A}|), \\ \max\Big(\bigcup\limits_{j\in\operatorname{supp} t}\{y_j\} \setminus \varphi(|\mathfrak{A}|)\Big) & \text{иначе.} \end{cases}$$

Поскольку φ субнепрерывно, $\varphi^* t$ сохраняет любую подалгебру $\mathfrak{B}$. Непосредственно проверяется, что φ^* является гомоморфизмом клонов, индуцированным отображением φ.

Пусть теперь отображение $\varphi\colon |\mathfrak{A}(\ker\varphi)| \to |\mathfrak{B}|$ не является субнепрерывным. Тогда существует такое $B \in \operatorname{Sub}\mathfrak{B}$, что $Q = \varphi^{-1}(B) \notin \operatorname{Sub}\mathfrak{A}(\ker\varphi)$. Поэтому можно зафиксировать некоторое $a \in \mathfrak{A}(\ker\varphi)(Q) \setminus Q$. Определим на $|\mathfrak{A}|$ $|Q|$-местную операцию q следующим образом:

$$q(x_1,\dots,x_{|Q|}) \rightleftharpoons \begin{cases} a, & \varphi(\{x_1,\dots,x_{|Q|}\}) = \varphi(Q), \\ x_1 & \text{иначе.} \end{cases}$$

Тогда $q \in \operatorname{Clo}\mathfrak{A}$ (поскольку если бы существовало такое множество $X \in \operatorname{Sub}\mathfrak{A}$, что $\varphi(X) = \varphi(Q)$, то было бы $Q = (\ker\varphi)(X) \in \operatorname{Sub}\mathfrak{A}(\ker\varphi)$, что противоречит выбору Q), а также $q \in \mathrm{M}_{|\mathfrak{A}|}^{\ker\varphi}$. Однако для всякого гомоморфизма клонов $\varphi^*\colon \operatorname{Clo}\mathfrak{A}(\ker\varphi) \to \operatorname{Clo}\mathfrak{B}$ и для всякого такого набора $(x_1, \dots, x_{|Q|})$, что $\{x_1, \dots, x_{|Q|}\} = Q$, имеет место соотношение $(\varphi^* q)(\varphi x_1, \dots, \varphi x_{|Q|}) \in B$, однако $\varphi q(x_1, \dots, x_{|Q|}) = \varphi a \notin B$.

Если же отображение $\varphi\colon |\mathfrak{A}(\ker\varphi)| \to |\mathfrak{B}|$ является субнепрерывным, но не главным, то обязательно $\operatorname{Mt}\mathfrak{B} = \emptyset$ и $\operatorname{Mt}\mathfrak{A} \neq \emptyset$. Поэтому не существует отображения клона $\operatorname{Clo}\mathfrak{A}(\ker\varphi)$ в клон $\operatorname{Clo}\mathfrak{B}$, переводящего 0-местные операции в 0-местные операции.

Осталось рассмотреть алгебру $\varphi\mathfrak{A}(\ker\varphi)$. Положим $\Phi = \{\varphi(X) \mid X \in \operatorname{Sub}\mathfrak{A}\}$. Имеем $\Phi \subseteq \operatorname{Sub}\varphi\mathfrak{A}(\ker\varphi)$, поэтому $\operatorname{Clo}\varphi\mathfrak{A}(\ker\varphi) \subseteq \operatorname{Pol}\Phi$. Чтобы доказать справедливость обратного включения, выберем произвольную k-местную операцию t^*, $k \geq 0$, на $\varphi(|\mathfrak{A}|)$, сохраняющую все множества из Φ. Рассмотрим k-местную операцию t на $|\mathfrak{A}|$, определенную согласно правилу $t(x_1, \dots, x_k) = \varphi^{-1}t^*(\varphi x_1, \dots, \varphi x_k)$ для всех $(x_1, \dots, x_k) \in |\mathfrak{A}|^k$. Тогда (при любом выборе отображения φ^{-1}) t сохраняет любую подалгебру $\mathfrak{A}$ и отношение эквивалентности $\ker\varphi$, и $\varphi^* t \restriction_{\varphi(|\mathfrak{A}|)} = t^*$ для всякого гомоморфизма клонов φ^*, индуцированного отображением φ. Поэтому $\operatorname{Clo}\varphi\mathfrak{A}(\ker\varphi) = \operatorname{Pol}\Phi$, так что $\varphi\mathfrak{A}(\ker\varphi)$ является полупримальной алгеброй. □

Исходя из этих соображений мы строим основную категорию формальных моделей вычислительных систем следующим образом.

Определение 7. Категорией вычислительных систем называется категория c-CS, объектами которой служат полупримальные алгебры, а морфизмами — главные субнепрерывные отображения их основных множеств.

Отметим, что в силу предложения 8 каждый морфизм в категории c-CS раскладывается в композицию эпиморфизма и мономорфизма. Правда, это разложение в общем случае не единственно (даже с точностью до изоморфизма), поскольку не всякое главное субнепрерывное биективное отображение основных множеств полупримальных алгебр является изоморфизмом (ср. утверждение (vi) предложения 1).

В качестве класса конфигураций выберем класс всех конечных диаграмм в c-CS, обозначим его через Δ(c-CS). Такой выбор оправдывается следующим фактом.

Предложение 10. *Любая конечная диаграмма в* c-CS *имеет копредел.*

Доказательство. Нужно проверить существование амальгам в c-CS. Прежде всего определим прямую сумму $\bigoplus\limits_{i\in I}\mathfrak{A}_i$ конечного семейства полупримальных алгебр $\mathfrak{A}_i$, $i \in I$. Положим $|\bigoplus\limits_{i\in I}\mathfrak{A}_i| = \bigoplus\limits_{i\in I}|\mathfrak{A}_i|$, $\operatorname{Sub}\bigoplus\limits_{i\in I}\mathfrak{A}_i = \{\emptyset\} \cup \{\bigoplus\limits_{i\in I}(\mathfrak{A}_i \cup \operatorname{Mt}\mathfrak{A}_i) \mid \mathfrak{A}_i \in \operatorname{Sub}\mathfrak{A}_i\}$. Тогда $\operatorname{Mt}\bigoplus\limits_{i\in I}\mathfrak{A}_i = \bigoplus\limits_{i\in I}\operatorname{Mt}\mathfrak{A}_i$, поэтому естественные вложения $\iota_i\colon |\mathfrak{A}_i| \to |\bigoplus\limits_{i\in I}\mathfrak{A}_i|$ являются главными (и, очевидно, субнепрерывными). Легко проверить, что $\bigoplus\limits_{i\in I}\mathfrak{A}_i$ действительно является копределом диаграммы в c-CS, состоящей из объектов $\mathfrak{A}_i$ и не содержащей морфизмов.

Далее, рассмотрим диаграмму Δ вида $\mathfrak{A}_1 \leftarrow \mathfrak{B} \rightarrow \mathfrak{A}_2$ с главными субнепрерывными отображениями $\varphi_i\colon |\mathfrak{B}| \to |\mathfrak{A}_i|$. Пусть ρ_Δ — отношение эквивалентности на $|\mathfrak{A}_1 \oplus \mathfrak{A}_2|$, получающееся путем рефлексивного транзитивного замыкания из отношения $\{\langle\varphi_1(x), \varphi_2(x)\rangle \mid x \in |\mathfrak{B}|\}$. В классе алгебр $\{\mathfrak{C}/\rho_\Delta \mid \mathfrak{C} \in \rho_\Delta(\mathfrak{A}_1 \oplus \mathfrak{A}_2)\}$ имеется (единственная с точностью до изоморфизма) полупримальная алгебра, обозначим ее $\mathfrak{C}_\Delta$. Отображения $\iota_i \circ \rho_\Delta\colon |\mathfrak{A}_i| \to |\mathfrak{C}_\Delta|$ являются

главными и субнепрерывными в силу предложения 7, и $\varphi_1 \circ \iota_1 \circ \rho_\Delta = \varphi_2 \circ \iota_2 \circ \rho_\Delta$. Легко видеть, что $\mathfrak{C}_\Delta$ является копределом диаграммы Δ. $\square$

Естественным кандидатом на роль категории сигнатур согласно теореме 1 является образ c-CS относительно функтора, индуцированного отображением Sub. Обозначим эту категорию через SSL, положим $|\,\mathrm{SSL}\,| = \mathrm{SetSL}_{01}$. Морфизм $\varphi\colon S \to T$ в категории SSL — это отображение $\varphi\colon \bigcup S \to \bigcup T$ такое, что $\varphi^{-1}(X) \in S$ для любого $X \in T$ и, кроме того, $\varphi(\mathrm{Mt}\, S) \subseteq \mathrm{Mt}\, T$. Сигнатурный функтор сопоставляет полупримальной алгебре $\mathfrak{A}$ полурешетку $\mathrm{Sub}\,\mathfrak{A}$, а на морфизмах действует тождественно. Отметим, что любой морфизм $\varphi \in \mathrm{Mor(SSL)}$ индуцирует гомоморфизм нижних полурешеток $\varphi^{-1}\colon \mathrm{codom}\,\varphi \to \mathrm{dom}\,\varphi$. Иначе говоря, существует контравариантный функтор из SSL в категорию конечных нижних полурешеток и их гомоморфизмов, сюръективный на объектах.

Наконец, в качестве категории трансформаций согласно принципам контрактного проектирования следует выбрать категорию r-CS, состоящую из всех полупримальных алгебр и их изоморфизмов в категории c-CS.

Из определений и полученных выше результатов вытекает справедливость следующего утверждения.

Теорема 3. *Тройка* $\langle \text{c-CS}, \Delta(\text{c-CS}), \text{r-CS}\rangle$ *является формальной дисциплиной проектирования с категорией сигнатур* SSL.

Содержательное толкование этой теоремы таково. Совокупность числовых множеств, сохраняемых операциями, реализованными в вычислительном компоненте, выступает в качестве его контракта. Композиция компонентов сводится к согласованию этих множеств путем фиксации правил кодирования и декодирования чисел при обмене данными между компонентами, совместимых с максимально возможным количеством операций. При этом в силу предложения 8 каждое такое согласование раскладывается на два: неизбыточное (оно не содержит незадействованных «мусорных» кодов) и различающее (оно сопоставляет различным значениям различные коды). Согласно предложению 10 композиционные возможности компонентов ничем не ограничены, любая согласованная конфигурация распределенной вычислительной системы является допустимой. Кроме того, никакие трансформации компонентов не могут изменить совокупность сохраняемых множеств. Поэтому реализация компонента сводится к выбору набора операций, порождающего клон, однозначно определяемый контрактом.

Заключение

В настоящей работе намечены общие контуры единого алгебраического языка, предназначенного для анализа и проектирования распределенных вычислительных систем. Выделен класс алгебр, способных служить формальными спецификациями практически полезных компьютерных моделей вычислений. Предложен формальный подход к проектированию протоколов обмена данными между вычислительными компонентами, реализованными согласно таким спецификациям. При этом использованы (элементарные) методы универсальной алгебры, конечнозначной логики, теории категорий. Применение этого аппарата во всей его мощности позволило бы выявить ряд фундаментальных свойств моделей вычислений, способных оказать значительное влияние на ключевые проектные решения в области распределенных вычислений и Grid-технологий. Например, согласно теореме 1 оценка возможности обогащения заданной модели вычислений требует характеризации решеток вида $\mathrm{Sub}_{0,1}\, S$, где S — нижняя полурешетка с нулем и единицей.

Другие направления дальнейших исследований по тематике работы связаны с анализом конкретных моделей вычислений, более или менее широко применяющихся на практике. В первую очередь обстоятельного алгебраического анализа требуют различные системы поразрядного представления чисел, включая системы с основанием, отличным от 2, системы остаточных классов

и т. д. Для многих алгоритмов и нетрадиционных вычислительных устройств необходимы нестандартные модели вычислений, разработка которых в настоящее время ведется бессистемно, и результат часто зависит только от удачи конкретного исследователя. Систематический подход, основанный на современной алгебраической технике, позволит повысить эффективность решения таких задач.

ЛИТЕРАТУРА

1. *Ehrig H., Mahr B.* Fundamentals of Algebraic Specification. V. 1. Berlin: Springer-Verl., 1985.
2. *Ehrig H., Mahr B.* Fundamentals of Algebraic Specification. V. 2. Berlin: Springer-Verl., 1990.
3. *Grid Computing:* Making the Global Infrastructure a Reality. N. Y.: Wiley & Sons, 2003.
4. *Gurevich Y.* Evolving Algebras 1993: Lipari Guide // Specification and Validation Methods. Oxford: Univ. Press, 1995. P. 9–36.
5. *Németh Z., Sunderam V.* Characterizing Grids: attributes, definitions and formalisms // J. Grid Computing. 2003. V. 1. P. 9–23.
6. *Ковалев С. П.* Аналитические модели машинной арифметики // Сиб. журн. индустр. математики. 2003. Т. 6, № 3. С. 88–102.
7. *Дискретная математика* и математические вопросы кибернетики. Т. I. М.: Наука, 1974.
8. *Ахо А. В., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. М.: Мир, 1979.
9. *Barnett M., Schulte W.* Runtime verification of .NET contracts // J. Systems and Software. 2003. N 65(3). P. 199–208.
10. *Bergman C., Berman J.* Morita equivalence of almost-primal clones // J. Pure Appl. Algebra. 1996. V. 108. P. 175–201.
11. *Rosenberg I. G.* Completeness properties of multiple-valued logic algebras // Computer science and multiple-valued logic. Amsterdam: North Holland, 1977. P. 144–186.
12. *Foster A. L., Pixley A. F.* Semi-categorical algebras I. Semi-primal algebras // Math. Z. 1964. V. 83. P. 147–169.
13. *Карпенко А. С.* Логики Лукасевича и простые числа. М.: Наука, 2000.
14. *Ковалев С. П.* Логика Лукасевича как архитектурная модель арифметики // Сиб. журн. индустр. математики. 2003. Т. 6, № 4. С. 32–50.
15. *Яблонский С. В., Гаврилов Г. П., Набебин А. А.* Предполные классы в многозначных логиках. М.: изд. МЭИ, 1997.
16. *Libkin L., Muchnik I.* The lattice of subsemilattices of a semilattice // Algebra Universalis. 1994. V. 31. P. 252–255.
17. *Шеврин Л. Н., Овсянников А. Я.* Полугруппы и их полугрупповые решетки. Ч. 2. Решеточные изоморфизмы. Свердловск: Изд-во Урал. ун-та, 1991.
18. *Fiadeiro J. L., Lopes A., Wermelinger M.* A mathematical semantics for architectural connectors // Lecture Notes in Computer Sci. 2003. V. 2793. P. 190–234.

г. Новосибирск
Институт вычислительных технологий СО РАН
E-mail: kovalyov@nsc.ru

Статья поступила 15 июня 2006 г.