EESTI NSV TEADUSTE AKADEEMIA TOIMETISED.
FÜÜSIKA * MATEMAATIKA
ИЗВЕСТИЯ АКАДЕМИИ НАУК ЭСТОНСКОЙ ССР. ФИЗИКА * МАТЕМАТИКА
PROCEEDINGS OF THE ACADEMY OF SCIENCES OF THE ESTONIAN SSR.
PHYSICS * MATHEMATICS

1989, 38, 2

УДК 510

Г. МИНЦ

МЕТОД ЭПСИЛОН-ПОДСТАНОВОК ДЛЯ ТЕОРИИ НАСЛЕДСТВЕННО КОНЕЧНЫХ МНОЖЕСТВ

(Представил Э. Тыугу)

1. Введение

Метод эпсилон-подстановок (ЭП) был введен Д. Гильбертом [1] в рамках его программы обоснования математики с помощью теории доказательств и нашел широкое применение [2–6]. Исходный замысел Д. Гильберта состоял в исключении инфинитарных средств (использования связанных переменных, пробегающих бесконечную совокупность) из доказательств финитных утверждений — арифметических тождеств. Позднее метод ЭП был применен для извлечения числового содержания из арифметических доказательств, в частности, оценки сложности получаемых программ [3]. Существенно, что этот метод применим к традиционным (классическим) доказательствам и в отличие от многих других методов извлечения программ, нацеленных в основном на конструктивные системы, не требует модификации. Еще одно его важное преимущество перед генценовскими методами — нечувствительность к пропозициональной структуре вывода: сложность извлекаемой программы (и скорость сходимости метода) измеряется только «глубиной вложенности» связанных переменных. При рассмотрении генценовских выводов для достижения того же эффекта приходится применять специальные приемы. Все это делает желательным обобщение метода ЭП с арифметики (для которой он был первоначально введен) на другие теории. Мы подробно рассмотрим *теорию наследственно конечных множеств* (НКМ, см., напр. [7], § 6 гл. I) и на примере нескольких ее формализаций продемонстрируем технику такого обобщения. Выбор именно этой теории обусловлен, в частности, использованием теории списков в теоретическом программировании (см., напр. [8]). Основной технический результат настоящей работы — *сходимость метода* ЭП для теории НКМ, которая доказана методом, введенным в [9]. Этот результат обобщает теорему Аккермана о сходимости метода ЭП для арифметики первого порядка (см. [1]). Большой вклад в фактическую реализацию предложенных автором соображений внес в своей дипломной работе А. Горбис; он является, по существу, соавтором настоящей статьи.

2. Теория наследственно конечных множеств

Напомним три эквивалентных (в смысле интерпретируемости) варианта этой теории в языке обычного классического исчисления предикатов с отношениями $\in$, $=$.

Первый — просто теория множеств ZFC (система Цермело—Френкеля с аксиомой выбора см. [7, 10]) без аксиомы бесконечности. Второй — (рассматривавшийся, например, А. Тарским) та же теория с отрицанием аксиомы бесконечности. Наконец, третий вариант (см. [11], начало раздела 2), который будет для нас основным и обозначается через HF — теория, содержащая константу $\varnothing$ (пустое множество), двухместную функцию * (добавление к множеству одного элемента) и (в дополнение к исчислению предикатов с равенством) следующие аксиомы.

Аксиомы теории HF.

Объемность: $\forall z(z \in x \leftrightarrow z \in y) \rightarrow x = y$.

Пустое множество: $\sim y \in \varnothing$.

Добавление одного элемента: $u \in x * y \leftrightarrow u \in x \vee u = y$.

Индукция: $A(\varnothing) \,\&\, \forall x \forall y (A(x) \,\&\, A(y) \rightarrow A(x * y)) \rightarrow \forall z A(z)$.

Стандартная модель теории HF состоит из *наследственно конечных множеств*, которые получаются из $\varnothing$ с помощью операции $*$. Напомним для дальнейшего, что *натуральные числа* в этой модели определяются как множества $\varnothing$ (число 0), $\varnothing * \varnothing$ (т. е. $\{\varnothing\}$, число 1), $1 * 1$ (т. е. $\{0, 1\}$, число 2) и т. д. При этом натуральное число $n = \{0, 1, \ldots, n-1\}$ имеет, как множество, мощность n, т. е. содержит ровно n элементов.

Другая важная модель теории HF введена В. Аккерманом. Она использует взаимно однозначную *нумерацию* $n(x)$ наследственно конечных множеств x натуральными числами, при которой элементы множества кодируются разрядами двоичного разложения

$$n(\{a, b, \ldots, c\}) = 2^{n(a)} + 2^{n(b)} + \ldots + 2^{n(c)}; \qquad n(\varnothing) = 0. \tag{1}$$

Чисто арифметическое определение получается, если ввести арифметический предикат $\in'$ соотношением $k \in' m \leftrightarrow ([m/2^k]$ нечетно). Следующее утверждение об эквивалентности рассмотренных формулировок и арифметики первого порядка хорошо известно (см., напр., [12]) и легко проверяется непосредственно.

Теорема 1. *В модели Аккермана выполнены (и даже доказуемы в арифметике первого порядка) все аксиомы* ZFC, *кроме аксиомы бесконечности (которая опровергается). После обратного перевода все арифметические аксиомы выводимы в* ZFC *без аксиомы бесконечности и в* HF.

В дальнейшем используется монотонность кодировки Аккермана (1) относительно принадлежности элемента множеству и включения множеств:

$$x \in y \rightarrow n(x) < n(y), \qquad x \subset y \,\&\, x \neq y \rightarrow n(x) < n(y). \tag{2}$$

3. Язык с эпсилон-символом

Первый шаг *гильбертовского метода* ЭП [1] — переход к эквивалентной бесквантворной формальной системе с т. н. эпсилон-символом. Кванторы исключаются из языка, куда добавляется новое правило образования термов: если A — формула, то $\varepsilon x A$ — терм (который читается «объект x, удовлетворяющий условию A»). Вхождения переменной x в этот терм — связанные. Вместо постулатов для кванторов используются логические эпсилон-аксиомы

$$A_x[t] \rightarrow A_x[\varepsilon x A], \tag{3}$$

где $A_x[t]$ или, короче, $A[t]$ — результат подстановки терма t вместо всех свободных вхождений переменной x в A (с обычными предо-

сторожностями, включая переименование связанных переменных во избежание коллизий). Кроме того, сохраняется правило подстановки терма вместо свободной предметной переменной $A/A[t]$ или, эквивалентным образом, все аксиомы понимаются как схемы аксиом. Так как некоторые из кванторных аксиом описывают вычислимые функции, для этих функций вводятся явные символы. В случае арифметики [1] — это сложение, умножение и вычитание 1 (предшествующее натуральное число). У нас используются функция $d(x, y)$, дающая элемент симметрической разности $x\Delta y$, если она непуста

$$x \neq y \to \sim (d(x, y) \in x \leftrightarrow d(x, y) \in y), \tag{4}$$

и функция $p(x, y)$, дающая множество $x - \{y\}$,

$$z \in p(x, y) \leftrightarrow z \in x \,\&\, z \neq y. \tag{5}$$

Наконец, вместо аксиом индукции вводятся математические *эпсилон-аксиомы*, выражающие, что εxA в некотором смысле минимален. В нашем случае требуется минимальность по принадлежности и по включению

$$y \in \varepsilon xA \to \sim A_x[y], \quad y \in \varepsilon xA \to \sim A_x[p(\varepsilon xA, y)]. \tag{6}$$

Обозначим через HFe теорию в языке с эпсилон-символом, *аксиомами* которой служат аксиомы исчисления высказываний с равенством, экстенсиональность в форме (4), аксиомы (5), аксиомы пустого множества и добавления, а также логические и математические эпсилон-аксиомы (3), (6) (понимаемые как схемы аксиом). Мы говорим, что (3), (6) — аксиомы для эпсилон-терма εxA. Следующий стандартный шаг метода ЭП — погружение кванторной теории в ее эпсилон-вариант.

Теорема 2. *При переводе*

$$\exists xA \mid\!\to A_x[\varepsilon xA]; \quad \forall xA \mid\!\to A_x[\varepsilon x \sim A] \tag{7}$$

все аксиомы и правила системы HF *становятся выводимыми в* HFe.

Доказательство. Аксиома $A[t] \to \exists xA$ переходит в логическую эпсилон-аксиому, кванторное правило $A/\forall xA$ переходит в применение правила подстановки $A/A[\varepsilon x \sim A]$, которое выводимо. Бескванторные аксиомы сохраняются. Аксиома экстенсиональности системы HF переходит в импликацию $(Z \in x \leftrightarrow Z \in y) \to x = y$, где Z есть $\varepsilon z \sim (z \in x \leftrightarrow z \in y)$. Она получается из логической эпсилон-аксиомы для Z и аксиомы экстенсиональности системы HF

$$(Z \in x \leftrightarrow Z \in y) \to (d(x, y) \in x \leftrightarrow d(x, y) \in y) \to x = y.$$

Наконец, рассмотрим перевод HF-аксиомы индукции

$$B[\varnothing] \,\&\, (B[X] \,\&\, B[Y] \to B[X * Y]) \to B[Z], \tag{8}$$

где $Z = \varepsilon z \sim B[z]$, $Y = \varepsilon y \sim (B[x] \,\&\, B(y) \to B(x * y))$,
$X = \varepsilon x \sim (B[x] \,\&\, B[Y] \to B[x * Y])$.

Допустим, что верна посылка импликации (8), и докажем $B[Z]$. При $Z = \varnothing$ это следует из $B[\varnothing]$. Поэтому считаем, что $Z \neq \varnothing$. Из (4) следует, что $d(Z, \varnothing) \in Z$. Вводя обозначения $y = d(Z, \varnothing)$, $x = p(Z, y)$, получаем $Z = x \ast y$, так как в силу (5)

$$u \in v \to v = p(v, u) * v. \tag{8a}$$

В силу математических ε-аксиом (6) для Z имеем $\sim\sim B[x]$ и $\sim\sim B[y]$, т. е. $B[x] \,\&\, B[y]$. В силу логических ε-аксиом для X, Y имеем из посылки (8) $B[x] \,\&\, B[y] \to B[x \ast y]$, откуда $B[x \ast y]$, т. е. $B[Z]$, что и требовалось.

4. Описание метода ЭП

Зафиксируем какую-нибудь нумерацию $n(x)$ наследственно конечных множеств x, удовлетворяющую условиям (2). Описываемый ниже аналог метода Гильберта, который мы назовем *методом ЭП* (эпсилон-подстановок) для теории НКМ (наследственно конечных множеств), состоит, по существу, в том, что значение терма εxA берется равным μxA — наименьшему в смысле нумерации n множеству x, удовлетворяющему условию A.

Применяются две меры сложности термов: степень и ранг. *Степень* терма — это обычная мера гнездности ε-символов: $\deg(t)=0$, если t не содержит ε; $\deg(f(t_1, \ldots, t_n))=\max(\deg(t_1), \ldots, \deg(t_n))$; $\deg(\varepsilon xA)=1+\max(\deg(t)$: t отличен от εxA и входит в εxA свободно). *Ранг* терма — мера гнездности по связанным вхождениям: $\mathrm{rk}(t)=0$, если t не содержит ε; $\mathrm{rk}(f(t_1, \ldots, t_n))=\max(\mathrm{rk}(t_1), \ldots, \mathrm{rk}(t_n))$; $\mathrm{rk}(\varepsilon xA)=1+\max(\mathrm{rk}(t)$: t имеет в A вхождение, содержащее x свободно).

Пример: $t=\varepsilon x(\varepsilon y(x*y=\varepsilon z(z=5)))=1$, $\deg(t)=2$, $\mathrm{rk}(t)=2$. Результат замены в эпсилон-терме t отличных от t максимальных свободных вхождений подтермов на переменные называется его *эпсилон-матрицей*. В нашем примере эпсилон-матрицей терма будет $\varepsilon x(\varepsilon y(x*y=a)=b)$. Ранг эпсилон-терма равен рангу его эпсилон-матрицы. Степень любой эпсилон-матрицы равна 1.

Пусть $\mathfrak{M}$ — некоторая система (конечный набор) ε-матриц и S — функция, сопоставляющая каждой эпсилон-матрице $M=\varepsilon xA(x, a_1, \ldots, a_l)$ из $\mathfrak{M}$ некоторую финитную l-местную функцию на НКМ, т. е. со значениями в НКМ, отличную от $\varnothing$ лишь на конечном множестве значений аргументов. Функцию S можно распространить на любые постоянные (т. е. не содержащие переменных) термы и формулы, содержащие только эпсилон-термы с матрицами из $\mathfrak{M}$. Множество $S(t)$ определяется индукцией по построению терма t с индуктивным переходом $S(\varepsilon xA(x, t_1, \ldots, t_l))=S(M)(S(t_1), \ldots, S(t_l))$, где $M=\varepsilon xA(x, a_1, \ldots, a_l)$, $S(f(t_1, \ldots, t_l))=f(S(t_1), \ldots, S(t_l))$. Истинностное значение (0,1) формулы F определяется в соответствии с обычными булевскими правилами индукцией по построению F с базисом $S(t=r)=1$, если $S(t)=S(r)$; $S(t\in r)=1$, если $S(t)\in S(r)$. Функцию S будем называть *ЭП* (эпсилон-подстановкой) для данной системы ε-матриц, если для каждой матрицы $M=\varepsilon xA(x, a_1, \ldots, a_k)$ из этой системы и каждого терма $t=\varepsilon xA(x, n_1, \ldots, n_k)$ из неравенства $S(t)\neq\varnothing$ следует, что $S(t)$ есть наименьшее в смысле нумерации n множество m, такое что $S(A(m, n_1, \ldots, n_k))=1$.

Предложенный Д. Гильбертом метод *исключения трансфинитного* (в рассматриваемом случае — эпсилон-символа) из доказательств финитных формул состоял в построении *выполняющей* ЭП для любого конечного набора постоянных эпсилон-аксиом, т. е. такой постановки S, что $S(E)=1$ для любой формулы E из рассматриваемого набора. Действительно, можно считать, что данное доказательство d не содержит свободных переменных (их можно заменить на $\varnothing$) и содержит только такие эпсилон-термы, матрицы которых участвуют в используемых эпсилон-аксиомах (остальные эпсилон-термы можно заменить на $\varnothing$). Применение выполняющей подстановки S ко всем эпсилон-термам из d не меняет последней формулы вывода, устраняет эпсилон-термы и переводит все формулы в доказуемые.

Если теперь дано доказательство d формулы F, не содержащей переменных, то применим подстановку S_d, выполняющую все эпсилон-аксиомы E, входящие в d. Сама формула F при этом не изменится, и мы получим ее доказательство, не содержащее эпсилон-символа, что и требуется.

Для построения выполняющей подстановки применим следующий *метод последовательных приближений*. Фиксируется конечный набор $\mathfrak{E}$ постоянных эпсилон-аксиом (3), (6), и список эпсилон-матриц всех эпсилон-термов из этого набора обозначается через $\mathfrak{M}$. Считается, что $\mathfrak{M}$ составлен в порядке возрастания рангов термов $\varepsilon x A$: сначала матрицы ранга 1, затем — ранга 2 и т. д.; считается, что формулы (3) выписаны в том же порядке. Исходная подстановка S_0 — нулевая: $S(M)=\varnothing$ (нулевая функция) для любой матрицы M. Если подстановка S уже определена и она не является выполняющей для $\mathfrak{E}$, то выбирается первая из рассматриваемых эпсилон-аксиом E, для которой $S(E)=0$. Пусть E — логическая эпсилон-аксиома. С использованием соответствующей эпсилон-матрицы $\varepsilon x A(x, a_1, \ldots, a_n)$ она записывается в виде $A(t, t_1, \ldots, t_n) \to A(\varepsilon x A(x, t_1, \ldots, t_n), t_1, \ldots, t_n)$. Если u^* обозначает $S(u)$, то из $S(E)=0$ получаются $S(A(t^*, t_1^*))=1$ и $S(A((\varepsilon x A(x, t_1^*)^*, t_1^*))=0$ (для простоты записи считается, что $n=1$). В *следующей ε-подстановке* S' сохраняются те же значения, что и в S для всех матриц, имеющих не больший ранг, чем рассматриваемая, «сбрасываются» на $\varnothing$ все значения матриц, имеющих больший ранг, и добавляется к оценке $S(M)$ для рассматриваемой матрицы M значение $S'(M)(t_1^*)=m$, где m — наименьшее, не превосходящее t^* НКМ такое, что $S(A(m, t_1^*))=1$. Этим завершается определение S'. Теперь $S_{i+1}=S_i'$ для $i \geqslant 0$. Математические эпсилон-аксиомы (6) рассматриваются аналогично.

5. Существование выполняющей ЭП

Все исследования ЭП в той или иной мере используют непрерывность рассматриваемых операций. Напомним соответствующие свойства, которые понадобятся при доказательстве сходимости метода ЭП.

Заметим, что этот метод можно применять к системам эпсилон-аксиом, содержащих символы произвольных функций, отображающих НКМ в НКМ.

Рассмотрим систему эпсилон-аксиом, содержащих, возможно, (свободные) переменные $\bar{f}$ для функций. Запишем такую систему в виде $\mathfrak{E}(\bar{f})$. Применение метода эпсилон-подстановок возможно только после того, как вместо переменных $\bar{f}$ будут подставлены символы конкретных функций $\bar{\varphi}$, что даст систему $\mathfrak{E}(\bar{\varphi})$.

Теорема 3. (*a*) *Для любой формулы* $A(\bar{f})$, *не содержащей индивидных переменных, для любой системы* $\bar{\varphi}$ *с подходящим числом аргументов найдется такое конечное семейство* Φ *НКМ, что для любых функций* $\bar{\psi}$, *совпадающих с* $\bar{\varphi}$ *на всех аргументах из* Φ, *верно* $A(\bar{\varphi}) \leftrightarrow A(\bar{\psi})$.

(*b*) *Для каждой системы* $\mathfrak{E}(\bar{f})$ *эпсилон-аксиом со свободными переменными* $\bar{f}$, *для любой системы функций* $\bar{\varphi}$ *с подходящим числом аргументов и любой эпсилон-подстановки* S *для системы* $\mathfrak{E}(\bar{\varphi})$ *найдется такое конечное семейство* Φ *НКМ, что для любых функций* $\bar{\psi}$, *совпадающих с* $\bar{\varphi}$ *на всех аргументах из* Φ

(*b*1) $S(A(\bar{\varphi}))=S(A(\bar{\psi}))$ *для любой эпсилон-аксиомы* A *из системы* $\mathfrak{E}$;

(*b*2) *подстановка* S', *следующая за* S, *для системы* $\mathfrak{E}(\bar{\psi})$ *та же, что и для* $\mathfrak{E}(\bar{\varphi})$.

Доказательство. При вычислении истинностного значения $A(\overline{\varphi})$ и построении следующей за S ЭП S' вычисляются значения различных функций при различных значениях аргументов. Ф — совокупность всех таких значений аргументов.

Если интересоваться только существованием выполняющей подстановки (а не сходимостью метода), то результат можно получить сравнительно просто. Приводимое ниже рассуждение, по-видимому, известно специалистам, но автор не нашел его в литературе.

Теорема 4. *Для любой конечной системы* $\mathfrak{E}$ *эпсилон-аксиом* (3), (6) *существует выполняющая ЭП* S, *являющая «срезкой» оператора минимизации: для постоянных термов* εxF *имеет место*

$$S(\varepsilon xF) \neq \varnothing \to S(\varepsilon xF) = \mu x(S(F) = 1), \tag{9}$$

где μxF *означает наименьшее в смысле нумерации* n *НКМ* x, *удовлетворяющее условию* F, *и эпсилон-символы внутри* F *понимаются так же.*

Доказательство. Подготавливая применение теоремы $3(a)$, выпишем все встречающиеся в $\mathfrak{E}$ различные эпсилон-матрицы

$$\varepsilon x_1 F_1(x_1, y_1), \ \ldots, \ \varepsilon x_n F_n(x_n, y_n)$$

или, короче,

$$\varepsilon_1(y_1), \ \ldots, \ \varepsilon_n(y_n).$$

Заменяя в $\mathfrak{E}$ матрицы $\varepsilon_1, \ldots, \varepsilon_n$ на новые свободные функциональные переменные $f_1, \ldots, f_n$ с соответствующим числом аргументов и соединяя все формулы знаком конъюнкции, получаем бескванторную формулу $A(\mathfrak{f}) = A(f_1, \ldots, f_n)$ такую, что $\&\mathfrak{E} = A(\varepsilon_1, \ldots, \varepsilon_n)$. Заметим, что подстановка $\varphi_i = \mu x_i F_i(x_i, y_i)$ вместо ε_i делает все эпсилон-аксиомы истинными. (Именно рассмотрение этих μ-операторов — основной источник неконструктивности нашего доказательства.) Таким образом, формула $A(\varphi_1, \ldots, \varphi_n)$ истинна. Остается только применить теорему $3(a)$.

6. Сходимость метода ЭП

Наша цель — доказательство следующего утверждения.

Теорема 5. *Для любой конечной системы эпсилон-формул* (2) *метод ЭП сходится, т. е. найдется* m *такое, что* S_m *— выполняющая подстановка.*

Приведенное ниже доказательство — обобщение рассуждения из [9]. Внимательный читатель заметит сходство с доказательством теоремы 4.

Будем говорить, что ЭП S_1 продолжает ЭП S (обозначение $S_1 \geqslant S$), если все ненулевые значения из S сохраняются в S_1.

Следующее утверждение обобщает известные результаты Дж. фон Неймана и В. Аккермана (см. [1], с. 107—111).

Теорема 6 (a). *Метод ЭП сходится для эпсилон-формул ранга* 1. $(б)$. *Более того, любая последовательность продолжающих друг друга ЭП* $S_1, S_2, \ldots$ *такая, что при каждом* k $S_{k+1}(t) \neq S_k(t)$ *для некоторого терма* t, *входящего в данную систему* $\mathfrak{E}$ *ε-формул ранга* 1, *содержит не более* 2^m *членов, где* m *— количество ε-термов в* $\mathfrak{E}$. *В частности, метод ЭП сходится за* 2^m *шагов.*
$(в)$ *Если* $\mathfrak{E}$ *— система эпсилон-формул ранга* 1, $S^+ \geqslant S$ *— ЭП и* $S^+(t) \neq S(t)$ *для некоторого терма* t, *входящего в* $\mathfrak{E}$, *то найдется эпсилон-терма* r, *входящий в* t *и такой, что* $S(r) = \varnothing$ *и* $S^+(r) \neq \varnothing$.

Доказательство. (*а*) следует из (*б*). Чтобы вывести (*б*) из (*в*), составим список $t_1, \ldots, t_m$ из ε-термов, входящих в $\mathfrak{E}$, в порядке возрастания (точнее, неубывания) степеней и положим

$$i_S = 2^{m-1}\delta_1 + 2^{m-2}\delta_2 + \ldots + 2\delta_{m-1} + \delta_m,$$

где $\delta_i = \operatorname{sgn}(S(t_i))$. Имеем $i_S < 2^m$. Далее, если S_{k+1} и S_k связаны так, как сказано в пункте (*б*), получим, в силу пункта (*в*), $i_{S_{k+1}} > i_{S_k}$ что и доказывает (*б*).

Осталось доказать (*в*). Применим индукцию по степени терма t. В базисе индукции $\deg(t) = 1$, поэтому из $S^+(t) \neq S(t)$ следует $t = \varepsilon x A(x, r_1, \ldots, r_k)$, причем $S(t) = \varphi(n_1, \ldots, n_k)$, $S^+(t) = \varphi^+(n_1, \ldots, n_k)$, где $n_1, \ldots, n_k$ — значения термов $r_1, \ldots, r_k$ (они не содержат ε), а φ, φ^+ — функции, сопоставленные ε-матрице $\varepsilon x A(x, a_1, \ldots, a_{k_i})$ в S, S^+. Допустим, что $\varphi(n_1, \ldots, n_k) = S(t) \neq \varnothing$. Тогда ввиду $S^+ \geqslant S$ имеем $\varphi^+(n_1, \ldots, n_k) = \varphi(n_1, \ldots, n_k)$, т. е. $S(t) = S^+(t)$ вопреки предположению. Значит, $S(t) = \varnothing$, что вместе с $S^+(t) \neq S(t)$ дает $S^+(t) \neq \varnothing$.

Индуктивный переход. В случае, когда $t = f(t_1, \ldots, t_k)$, результат сразу получается из индуктивного предположения, так как должно быть $S(t_i) \neq S^+(t_i)$ для некоторого $i \leqslant k$. Остался случай $t = \varepsilon x A(x, u)$, где $\varepsilon x A(x, a)$ — матрица терма t (для простоты записи предполагаем, что у этой матрицы всего один аргумент). Имеем $S(t) = \varphi(S(u))$, $S^+(t) = \varphi^+(S^+(u))$, где φ, φ^+ — функции, сопоставленные матрице $\varepsilon x A(x, a)$ при подстановках S, S^+. Если $S(u) \neq S^+(u)$, то применимо индуктивное предположение. Поэтому будем считать, что $S(u) = S^+(u)$, и обозначим это число через u^*. Из $\varphi(u^*) = S(t) \neq S^+(t) = \varphi^+(u^*)$ следует, как и в базисе индукции $\varphi(u^*) = \varnothing$, $\varphi^+(u^*) \neq \varnothing$, т. е. можно взять $r = t$, что и требовалось доказать.

Теорема 7. *При переходе от S к следующей подстановке S' сохраняются все ненулевые значения ε-матриц минимального имеющегося ранга.*

Предложение непосредственно следует из определения S'.

Докажем теорему 5 индукцией по рангу данной системы ε-формул. Базисом служит наша теорема 6. Предположим, что для данного r теорема доказана, и рассмотрим систему $\mathfrak{E}$ ранга $r+1$. Введем вспомогательную систему $\mathfrak{E}^+(\bar{f})$, полученную из $\mathfrak{E}$ заменой всех эпсилон-матриц минимального ранга (считаем, что он равен 1) на функциональные символы $\bar{f}$ с соответствующим числом мест и вычеркиванием эпсилон-аксиом минимального ранга. Рассмотрим также систему $\mathfrak{E}^1(\bar{g})$, полученную из $\mathfrak{E}$ заменой всех матриц M ранга больше 1 на функциональные символы $\bar{g}$ с соответствующим числом мест и вычеркиванием соответствующих им эпсилон-аксиом.

Допустим теперь (для приведения к противоречию), что метод ЭП для системы $\mathfrak{E}$ не сходится, т. е. ни одна из подстановок $S_0, S_1, S_2, \ldots$ не является выполняющей для $\mathfrak{E}$. Каждую ЭП S_i для $\mathfrak{E}$ можно представить в виде $(\bar{\varphi}_i, \bar{\psi}_i)$, где φ_i — подстановки для ε-матриц ранга 1, $\bar{\psi}_i$ — подстановки для остальных ε-матриц. При этом в силу теоремы 6 и того, что ранг системы $\mathfrak{E}^1$ равен 1, можем утверждать, что функции $\bar{\varphi}_{i+1}$ являются продолжениями функций $\bar{\varphi}_i$, т. е. из $\bar{\varphi}_i(\bar{x}) \neq \varnothing$ следует $\bar{\varphi}_{i+1}(\bar{x}) = \bar{\varphi}_i(\bar{x})$. Пусть $\bar{\varphi}$ — объединение всех $\bar{\varphi}_i$, т. е. для любой функции θ из списка $\bar{\varphi}$ значение $\theta(\bar{x})$ равно z, если для некоторого i верно $\theta_i(\bar{x}) = z \neq \varnothing$; в противном случае $\theta(\bar{x}) = \varnothing$. Применяя индуктивное предположение к системе $\mathfrak{E}^+(\bar{\varphi})$ ранга r, найдем номер h, при котором подстановка $S_h^{\bar{\varphi}}$ для системы $\mathfrak{E}^+(\bar{\varphi})$ является выполняющей. Ис-

пользуя теорему 3 ($в2$), найдем конечное семейство Φ^+ НКМ для $\mathcal{E}^+(\bar{\varphi})$ и всех подстановок $S_0^{\bar{\varphi}}, \ldots, S_h^{\bar{\varphi}}$. Затем найдем номер i_0, начиная с которого все ненулевые значения функций $\bar{\varphi}$ для аргументов из Φ^+ равны значению $\bar{\varphi}_{i_0}$.

Рассмотрим подробнее последовательность $(\bar{\varphi}_i, \bar{\psi}_i)$ для $i \geqslant i_0$. Возможны два случая.

φ-переход: $\bar{\varphi}_{i+1} = (\bar{\varphi}_i)'$, $\bar{\psi}_{i+1} = \varnothing$. $\bar{\varphi}_i$ не является выполняющей подстановкой для $\mathcal{E}^1(\bar{\psi}_i)$.

ψ-переход: $\bar{\varphi}_{i+1} = \bar{\varphi}_i$; $\bar{\psi}_{i+1} = (\bar{\psi}_i)'$. $\bar{\varphi}_i$ — выполняющая подстановка для $\mathcal{E}^1(\bar{\psi}_i)$

Пусть $h_1 = 2^{m_1}$, где m_1 — количество ε-термов в системе $\mathcal{E}^1(\bar{g})$. По теореме 4 любая последовательность соседних φ-переходов содержит не более h_1 членов. В силу выбора Φ^+, i_0 любая начинающаяся с $\varnothing$ последовательность соседних ψ-переходов $\bar{\psi}_k = \varnothing$, $\bar{\psi}_{k+1}, \ldots$ совпадает с последовательностью $\Psi = S_0^{\bar{\varphi}}, \ldots, S_h^{\bar{\varphi}}$, и потому она содержит ровно h членов. Таким образом, последовательность $(\bar{\varphi}_i, \bar{\psi}_i)$ для $i > i_0$ имеет вид

$$\Phi_1; \Psi; \Phi_2; \Psi; \ldots,$$

где Φ_i и Ψ — участки, состоящие из последовательных φ- и ψ-переходов соответственно. Считая для простоты записи, что $i_0 = 0$, мы можем представить участок $\Psi; \Phi_{i+1}$ в следующем виде:

$$(\bar{\varphi}^i, \bar{\psi}_0), (\bar{\varphi}^i, \bar{\psi}_1), \ldots, (\bar{\varphi}^i, \bar{\psi}_h); ((\bar{\varphi}^i)', \varnothing), ((\bar{\varphi}^i)'', \varnothing), \ldots, ((\bar{\varphi}^i)^{(l_i)}, \varnothing), \quad (10)$$

где $\bar{\varphi}_i$ — последняя ε-подстановка участка Φ_i.

Длина l_i участка Φ_{i+1} может быть равна единице, т. е. может быть $\bar{\varphi}^{i+1} = (\bar{\varphi}^i)'$. Ни при каком i подстановка $\bar{\varphi}^i$ не является выполняющей для $\mathcal{E}^1(\bar{\psi}_h)$, иначе φ-переход после участка ψ был бы невозможен. Это означает, что при каждом из рассмотренных значений i верно $(\bar{\varphi}^i)'(t) \neq (\bar{\varphi}^i)(t)$ для некоторого терма t, входящего в $\mathcal{E}^1(\bar{\psi}_h)$. Поскольку последовательные φ-компоненты — продолжения друг друга, то в силу части $б$ теоремы 6, примененной к $\mathcal{E}^1(\bar{\psi}_h)$, получаем, что количество φ-участков не превосходит h_1, т. е. последовательность ЭП обрывается, что и требовалось доказать.

7. Распространение на другие формулировки теории НКМ

Теорема 7 дает метод построения выполняющей ЭП для системы HFe. Проиллюстрируем обобщение этого метода и покажем, как получить выполняющую подстановку по выводу в ZFC без аксиомы бесконечности.

Напомним формулировки аксиом этой системы.

Аксиома объемности: $\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y$.

Аксиома выделения: $\exists c \forall x (x \in c \leftrightarrow (x \in a \,\&\, F(x)))$.

Аксиома объединения: $\exists u \forall x (x \in u \leftrightarrow (\exists z \in y) x \in z)$.

Аксиома степени: $\exists p \forall x (x \in p \leftrightarrow y \subset x)$.

Аксиома подстановки: $\forall xyz (F(x, y) \,\&\, F(x, z) \rightarrow y = z) \rightarrow$
$\rightarrow \exists s \forall y (y \in s \leftrightarrow (\exists x \in u) F(x, y))$.

Аксиома регулярности: $x \neq \varnothing \rightarrow (\exists y \in x)(\forall z \in y) z \notin x$.

Аксиома выбора: $\exists c (\forall y \subset x)(y \neq \varnothing \rightarrow (\exists! z \in y) \langle y, z \rangle \in c)$.

Опишем два способа получения ЭП, реализующих эти аксиомы. Под реализацией формулы $\exists x A(x)$, начинающейся с квантора существования, понимается НКМ m, такое, что выполнено $A(m)$. При этом следует помнить, что если формула A содержит кванторы, то выполнение $A(m)$ понимается в методе ЭП нестандартно: ведь области значений связанных переменных ограничиваются конечными семействами.

1) Простейший и универсальный способ

Каждая из рассматриваемых аксиом выводима в системе HF. Применяя теорему 2, получаем вывод в системе HFe. При этом формула $\exists x A(x)$ перейдет в $A^*(\varepsilon x A^*)$, где A^* — перевод формулы A. Применяя к полученному выводу метод ЭП, получаем подстановку для $\varepsilon x A^*$, которая и является искомой.

2) Введение функций, реализующих аксиомы

Этот способ позволяет выполнить некоторые экзистенциальные утверждения стандартно, а не приблизительно, как в методе ЭП. Предположим, что имеется формула $B(x)$ не содержащая связанных переменных и такая, что $A(x) \leftrightarrow B(x)$. Тогда выполнение $\exists x B(x)$ всегда стандартно, а имея $B(m)$, мы получаем и $A(m)$. Иногда проще построить $B(x)$ такую, что $B(x) \rightarrow A(x)$ и $\exists x B(x)$. Формулу $B(x)$ чаще всего получают, устраняя из $A(x)$ кванторы с помощью (скулемовских) функций. Иногда это позволяет заменить существовательную аксиому на бескванторную так, что она вообще выпадает из рассмотрения в методе ЭП. При этом существенно, чтобы все вводимые функции были вычислимы (на НКМ). Один пример такого преобразования у нас уже был: при переходе от HF к HFe в разделе 2 мы ввели функцию d, выбирающую элемент в симметрической разности двух множеств, если она непуста. Это позволило скулемизировать аксиому объемности. Аксиома выбора следует из соотношения $y \neq \varnothing \rightarrow d(y, \varnothing) \in y$: в качестве функции выбора на множестве x можно взять $\{\langle y, d(y, \varnothing)\rangle : y \subset x \,\&\, y = \varnothing\}$.

Заметим, что при переводе в эпсилон-язык можно не исключать ограниченные кванторы (вида $(\exists y \in t)$).

Действительно, все наши рассуждения, связанные с методом ЭП, проходят без изменений, если формулы с ограниченными кванторами (короче, ограниченные формулы) трактовать как бескванторные. При этом выполнение формулы $\exists x A(x)$ с ограниченной A будет стандартным.

Так обстоит дело с аксиомами объединения, степени, регулярности. Учитывая, что соответствующие скулемовские функции вычислимы на НКМ, мы можем переписать эти аксиомы в виде:

$$x \in \bigcup(y) \leftrightarrow (\exists z \in y) x \in z, \quad x \in P(y) \leftrightarrow (\forall z \in x) z \in y,$$

$$x \neq \varnothing \rightarrow (\mathrm{reg}\,(x) \in x \,\&\, (z \in \mathrm{reg}\,(x) \rightarrow z \notin x)).$$

С другой стороны, не видно, как можно было бы добиться стандартного выполнения аксиом выделения и подстановки.

Как и следовало ожидать, нельзя просто включить в рассмотрение аксиому бесконечности

$$\exists \omega (\varnothing \in \omega \,\&\, (\forall x \in \omega) x' \in \omega),$$

где x' обозначает $x \cup \{x\}$.

Эту формулу можно выполнить при любой конкретной ЭП вместо подчиненного эпсилон-терма

$$X(\omega) = \varepsilon x (x \in \omega \,\&\, x' \notin \omega).$$

Действительно, вводя обозначение $\mathrm{Prog}\,(f, z) = \varnothing \in z \,\&\, (f(z) \in z \to \to (f(z))' \in z)$, мы видим, что для любой финитной функции $S(\omega)$ можно найти НКМ Ω такое, что верно $\mathrm{Prog}(S, \Omega)$, т. е.

$$\varnothing \in \Omega \,\&\, (S(\Omega) \in \Omega \to ((S(\Omega))' \in \Omega)). \qquad (11)$$

Для этого берем натуральное положительное число n (т. е. НКМ вида $\{\varnothing, \varnothing', \varnothing'', \ldots, \varnothing^{(n-1)}\}$), удовлетворяющее условию $S(n) \neq \neq n-1$. Такое число найдется, так как $S(n) = \varnothing$, начиная с некоторого места. Условие (11) выполнено для $\Omega = n$, так как из $S(\Omega) \in \Omega$, $S(\Omega) \neq \Omega - 1$ следует, что $(S(\Omega))' \in \Omega$.

Тем не менее, наше доказательство существования выполняющей ЭП (теорема 5) не проходит, так как дополнительная эпсилон-аксиома имеет вид

$$\mathrm{Prog}\,(X, \Omega),$$

где

$$\Omega = \varepsilon\omega(\varnothing \in \omega \,\&\, (X(\omega) \in \omega \to (X(\omega))' \in \omega)),$$

но ее нельзя выполнить (при понимании $X(\omega)$ как $\mu x(x \in \omega \to x' \in \omega)$) никаким наследственно-конечным множеством в отличие от эпсилон-аксиом (3), (6) в разделе 3, которые выполняются μ-символом. По той же причине не проходит и доказательство сходимости метода ЭП (теорема 7), так как в ней используется возможность выполнить все эпсилон-аксиомы при подстановке любой (а не только финитной) функции $\bar{\varphi}$ вместо функциональной переменной. По-видимому, «наивный» метод ЭП для теории множеств просто расходится в присутствии аксиомы бесконечности.

ЛИТЕРАТУРА

1. *Гильберт Д., Бернайс П.* Основания математики. 2. Теория доказательств. М., Мир, 1980.
2. *Ackermann, W.* // Math. Ann., 1940, **117**, H 2, 162—194.
3. *Kreisel, G.* // J. Symbol. Log., 1951, **16**, 241—267.
4. *Parikh, R.* J. // Trans. Amer. Math. Soc., 1973, **177**, 29—36.
5. *Гавриленко Ю. В.* // ДАН СССР, 1984, **276**, № 1, 18—22.
6. *Божич Е. С.* // Вестн. МГУ. Мат., мех., 1985, **5**, 37—41.
7. *Коэн Дж. П.* Теория множеств и континуум-гипотеза. М., Мир, 1969.
8. *Ершов Ю. Л.* // Вычислительные системы, 1986, **114**, 3—10.
9. *Минц Г.* // Изв. АН ЭССР. Физ. Матем., 1981, **31**, № 4, 376—382.
10. Справочная книга по математической логике. Т. 2. Теория множеств. М., Мир, 1984.
11. *Takahashi, M.* // Publs Res. Inst. Math. Sci., 1977, **12**, 577—708.
12. *Wang, H.* A Survey of Mathematical Logic. Peking, Sci. Press; Amsterdam. North Holland, 1963.

Институт кибернетики
Академии наук Эстонской ССР

Поступила в редакцию
18/I 1988

G. MINTS

EPSILON-ASENDUSTE MEETOD PÄRANDLIKULT LÕPLIKE HULKADE TEOORIAS

On esitatud epsilon-asenduste meetodi püstitus ja koonduvuse tõestus pärandlikult lõplike hulkade teoorias.

G. MINTS

EPSILON-SUBSTITUTION METHOD FOR THE THEORY OF HEREDITARY FINITE SETS

The epsilon-substitution method introduced by Hilbert was later used for extracting numerical content of arithmetic proofs, and in particular for estimating the complexity of the resulting program. Essential features of the method are the applicability to classical (not necessarily intuitionistic) derivations and independence of their propositional structure: the complexity of the extracted program (and the rate of convergence of the method) depends only on the nesting of bound variables. So it is desirable to extend this method from the first-order arithmetic to other theories. We treat the theory of hereditarily finite sets in detail, and show how such extension can be made for several of its formalizations. The main technical result of this paper is the convergence of the epsilon-substitution method for the theory of hereditarily finite sets. It is established by the method given in a previous paper by the author (Proc. Acad. Sci. ESSR. Phys. Math., 1982, **31**, № 4). It also extends the Ackermann theorem on the convergence of the epsilon-substitution method for the first-order arithmetic.