EESTI NSV TEADUSTE AKADEEMIA TOIMETISED. 31. KÖIDE
FÜÜSIKA * MATEMAATIKA. 1982, NR. 4

ИЗВЕСТИЯ АКАДЕМИИ НАУК ЭСТОНСКОЙ ССР. ТОМ 31
ФИЗИКА * МАТЕМАТИКА. 1982, № 4

УДК 510.652

Г. МИНЦ

УПРОЩЕННОЕ ДОКАЗАТЕЛЬСТВО НЕПРОТИВОРЕЧИВОСТИ АРИФМЕТИКИ

(Представил Е. Тыугу)

В настоящей работе приводится новое доказательство теоремы Аккермана [1] о сходимости *метода ε-подстановок* для арифметики. Постановка задачи излагается в разделе 1, доказательство — в разделе 2. Идея метода была предложена Д. Гильбертом в рамках его программы обоснования математики посредством исключения трансфинитных высказываний (содержащих кванторы $\forall$, $\exists$ по бесконечным совокупностям) из доказательств числовых равенств. В доказательстве В. Аккермана использовались минимальные (в некотором точном смысле) конструктивные средства, достаточные для его целей, — индукция до конструктивного ординала ε_0. Оно содержит довольно изощренную комбинаторику — даже упрощенное его изложение в Приложении VB [2] достаточно громоздко. Приводимое ниже доказательство удается значительно упростить в комбинаторном отношении за счет использования (нефинитного) понятия непрерывного функционала.

1. Язык *системы* $\mathcal{A}$, формализующей классическую арифметику первого порядка, содержит константу 0, переменные для натуральных чисел (обозначаемые через x, x_1, y, y_1 ...), символы примитивно рекурсивных функций, включая $+$, $\cdot$, $'$ (функция следования или прибавления 1), δ (вычитание 1 из положительных чисел), символ равенства $=$, символ ε и (свободные) переменные для функций (обозначаемые через f, g, h, f_1, g_1, h_1, ...). *Термы* строятся из 0 и переменных с помощью символов для функций [напр., $\delta(0' \cdot g(x))$], а также с помощью *ε-символа*: если A — формула (см. ниже), x — переменная, то εxA — терм, который трактуется ниже как наименьшее число x, удовлетворяющее условию A. Формулы строятся из равенств термов с помощью пропозициональных связок &, $\rightarrow$, $\neg$ без кванторов.

Постулаты системы $\mathcal{A}$ — тавтологии классического исчисления высказываний, бескванторные аксиомы Пеано, определяющие равенства для имеющихся примитивно рекурсивных функций [напр., $t+0=t$, $t+r'=(t+r)'$], аксиома $t\neq 0\rightarrow t=(\delta(t))'$, аксиома равенства

$$t=r\rightarrow (A(t)\rightarrow A(r)), \tag{1}$$

правило modus ponens $A, A\rightarrow B/B$, правило подстановки $A(x)/A(t)$ для любого терма t, а также ε-аксиомы

$$A(t)\rightarrow A(\varepsilon xA), \quad A(t)\rightarrow \varepsilon xA\neq t'. \tag{2}$$

Обычная формализация исчисления предикатов и арифметики погружается в рассматриваемую с помощью определений

$$\exists xA(x) \leftrightharpoons A(\varepsilon xA), \quad \forall xA(x) \leftrightharpoons A(\varepsilon x\neg A). \tag{3}$$

При этом формула $A(t)\rightarrow \exists xA(x)$ переходит в первую из ε-аксиом (2), а перевод аксиомы индукции на наш язык получается с помощью другой.

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

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

Пусть $\mathfrak{M}$ — некоторая система (конечный набор) ε-матриц и S — функция, сопоставляющая каждой ε-матрице $M\colon = \varepsilon xA(x, a_1, \dots, a_l)$ из $\mathfrak{M}$ некоторую финитную l-местную арифметическую функцию, т. е. функцию из ω^l в ω, отличную от нуля лишь на конечном отрезке. Функцию S можно распространить на любые постоянные (т. е. не содержащие переменных) термы и формулы системы $\mathcal{A}$, содержащие только ε-термы с матрицами из $\mathfrak{M}$. Число $S(t)$ определяется индукцией по построению терма t с индуктивным переходом $S(\varepsilon xA(x, t_1, \dots, t_l)) =$ $= S(M)(S(t_1), \dots, S(t_l))$, где $M\colon = \varepsilon xA(x, a_1, \dots, a_l)$, $S(f(t_1, \dots, t_l)) =$ $= f(S(t_1), \dots, S(t_l))$. *Истинностное значение* (0,1) формулы F определяется в соответствии с обычными булевскими правилами индукцией по построению F с базисом $S(t = r) := 1$, если $S(t) = S(r)$. Функцию S будем называть *ε-подстановкой для* данной *системы* ε-матриц, если для каждой матрицы $M\colon = \varepsilon xA(x, a_1, \dots, a_k)$ из этой системы и каждого терма $t\colon = \varepsilon xA(x, n_1, \dots, n_k)$ из неравенства $S(t) \neq 0$ следует, что $S(t)$ есть наименьшее число n такое, что $S(A(n, n_1, \dots, n_k)) = 1$.

Предложенный Д. Гильбертом метод исключения трансфинитного (в рассматриваемом случае — ε-символа) из доказательств постоянных равенств $t = r$ в системе $\mathcal{A}$, не содержащих ε, состоял в построении *выполняющей* ε-подстановки *для* любого *конечного набора постоянных ε-формул* (2), т. е. такой подстановки S, что $S(E) = 1$ для любой формулы E из рассматриваемого набора. Действительно, можно считать, что данное доказательство d не содержит переменных (их можно заменить на 0) и содержит только такие ε-термы, матрицы которых участвуют в используемых формулах (2) (остальные ε-термы можно заменить на 0). Применение выполняющей подстановки S ко всем ε-термам из d не меняет последней формулы вывода, устраняет ε-термы и переводит все формулы в доказуемые.

Д. Гильберт предложил для построения выполняющей подстановки *метод последовательных приближений*, который, после уточнения Дж. фон Нейманом и В. Аккерманом, формулируется следующим образом. Фиксируется конечный набор $\mathfrak{E}$ постоянных ε-формул (2) и список ε-матриц всех ε-термов из этого набора обозначается через $\mathfrak{M}$. Считается, что $\mathfrak{M}$ составлен в порядке возрастания рангов термов εxA: сначала матрицы ранга 1, затем — ранга 2 и т. д.; считается, что формулы (2) выписаны в том же порядке. Исходная подстановка S_0 — нулевая: $S(M) = 0$ (нулевая функция) для любой матрицы M. Если подстановка S уже определена и она не является выполняющей для $\mathfrak{E}$, то выбирается первая из рассматриваемых формул E вида (2), для которой $S(E) = 0$. Пусть E имеет вид первой из формул (2). С использованием соответствующей ε-матрицы $\varepsilon xA(x, a_1, \dots, a_n)$ она записывается в виде $A(t, t_1, \dots, t_n) \to A(\varepsilon xA(x, t_1, \dots, t_n), t_1, \dots, t_n)$. Если u^* обозначает $S(u)$, то из $S(E) = 0$ получается $S(A(t^*, t_1^*)) = 1$ 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 0 все значения матриц, имеющих больший ранг, и добавляется к оценке $S(M)$ для рассматриваемой матрицы M значение $S'(M)(t_1^*) = n$, где n — наименьшее, не превосходящее t^* натуральное число такое, что $S(A(n, t_1^*)) = 1$. Этим завершается определение S'. Теперь $S_{i+1} = S'_i$ для $i \geqslant 0$. Случай второй из формул (2) трактуется аналогично.

Теорема Аккермана ([1]). *Для любой конечной системы ε-формул* (2) *метод ε-подстановок сходится, т. е. найдется n такое, что S_n — выполняющая подстановка.*

Будем говорить, что ε-подстановка S_1 *продолжает* ε-подстановку S (обозначение $S_1 \succeq S$), если все ненулевые значения из S сохраняются в S_1.

2. Значительным достижением школы Гильберта в «до гёделевский» период было доказательство следующей теоремы, первая часть которой принадлежит Дж. фон Нейману, а вторая обобщает доказательство Аккермана, изложенное в [2] (с. 107—111).

Теорема. А. *Метод ε-подстановок сходится для ε-формул ранга* 1.

Б. *Более того, любая последовательность продолжающих друг друга ε-подстановок $S_1, S_2, \ldots$ такая, что при каждом i $S_{i+1}(t) \neq S_i(t)$ для некоторого терма t, входящего в данную систему $\mathcal{E}$ ε-формул ранга* 1, *содержит не более 2^m членов, где m — количество ε-термов в $\mathcal{E}$. В частности, метод ε-подстановок сходится за 2^m шагов.*

В. *Если $\mathcal{E}$ — система ε-формул ранга* 1, *$S^+ \succeq S$ — ε-подстановки и $S^+(t) \neq S(t)$ для некоторого терма t, входящего в $\mathcal{E}$, то найдется ε-терм r, входящий в t и такой, что $S(r) = 0$ и $S^+(r) > 0$.*

Доказательство. А следует из Б. Чтобы вывести Б из В, составим список $t_1, \ldots, t_m$ из ε-термов, входящих в $\mathcal{E}$, 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 $\delta_i = \mathrm{sgn}(S(t_i))$. Имеем $i_S < 2^m$. Далее, если S_{i+1} и S_i связаны так, как сказано в пункте Б, получим, в силу пункта В, $i_{S_{i+1}} > i_{S_i}$, 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 $S(t) = \varphi(n_1, \ldots, n_k)$, $S^+(t) = \varphi^+(n_1, \ldots$ $\ldots, n_k)$, где $n_1, \ldots, n_k$ — числовые значения термов $r_1, \ldots, r_k$ (они не содержат ε), а φ, φ^+ — функции, сопоставленные ε-матрице $\varepsilon x A(x, a_1, \ldots$ $\ldots, a_k)$ в S, S^+. Допустим, что $\varphi(n_1, \ldots, n_k) = S(t) > 0$. Тогда ввиду $S^+ \succeq S$ имеем $\varphi^+(n_1, \ldots, n_k) = \varphi(n_1, \ldots, n_k)$, т. е. $S(t) = S^+(t)$ вопреки предположению. Значит, $S(t) = 0$, что вместе с $S^+(t) \neq S(t)$ дает $S^+(t) > 0$.

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 $\varphi(u^*) = S(t) \neq \neq S^+(t) = \varphi^+(u^*)$ следует, как и в базисе индукции, $\varphi(u^*) = 0$, $\varphi^+(u^*) > 0$, т. е. можно взять $r := t$, что и требовалось доказать.

Сформулируем хорошо известное *свойство непрерывности* метода ε-подстановок. Рассмотрим систему ε-формул (2), содержащих, возможно, (свободные) переменные $\bar{f}$ для функций. Будем записывать такую систему в виде $\mathcal{E}(\bar{f})$. Применение метода ε-подстановок возможно только после того, как вместо переменных $\bar{f}$ будут подставлены символы конкретных функций $\bar{\varphi}$, что даст систему $\mathcal{E}(\bar{\varphi})$.

Предложение 1. *Для каждой системы $\mathcal{E}(\bar{f})$ ε-формул вида* (2) *со свободными переменными $\bar{f}$, для любой системы $\bar{\varphi}$ с подходящим числом аргументов и любой ε-подстановки S для системы $\mathcal{E}(\bar{\varphi})$ найдется число N такое, что подстановка S', следующая за S, будет одна и та же для системы $\mathcal{E}(\bar{\psi})$ при любых функциях ψ, совпадающих с $\bar{\varphi}$ на всех аргументах, не превосходящих N.*

Доказательство. При построении S' для $\mathcal{E}(\bar{\varphi})$ вычисляются значения различных функций при различных значениях аргументов. Искомое N — это максимальное значение аргумента.

Предложение 2. *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 Аккермана* индукцией по рангу системы ε-формул (2). Базисом служит наша теорема. Предположим, что для данного r теорема доказана, и рассмотрим систему $\mathcal{E}$ ранга $r+1$. Введем вспомогательную систему $\mathcal{E}^+(\bar{f})$, полученную из $\mathcal{E}$ заменой всех ε-матриц M минимального ранга (считаем, что он равен 1) на функциональные символы $\bar{f}$ с соответствующим числом мест. Рассмотрим также систему $\mathcal{E}^1(\bar{g})$, полученную из $\mathcal{E}$ заменой всех матриц M ранга больше 1 на функциональные символы $\bar{g}$ с соответствующим числом мест.

Допустим теперь (для приведения к противоречию), что метод ε-подстановок для системы $\mathcal{E}$ не сходится, т. е. ни одна из подстановок $S_0, S_1, S_2, \ldots$ не является выполняющей для $\mathcal{E}$. Каждую ε-подстановку S_i для $\mathcal{E}$ можно представить в виде $(\bar{\varphi}_i, \bar{\psi}_i)$, где $\bar{\varphi}_i$ — подстановки для ε-матриц ранга 1, $\bar{\psi}_i$ — подстановки для остальных ε-матриц. При этом в силу предложения 2 и того, что ранг системы $\mathcal{E}^1$ равен 1, можем утверждать, что функции $\bar{\varphi}_{i+1}$ являются продолжениями функций $\bar{\varphi}_i$, т. е. из $\bar{\varphi}_i(\bar{x}) \neq 0$ 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 $n+1$, если для некоторого i верно $\theta_i(\bar{x}) = n+1$; в противном случае $\theta(\bar{x}) = 0$. Применяя индуктивное предположение к системе $\mathcal{E}^+(\bar{\varphi})$ ранга r, найдем номер h, при котором подстановка $S_h^{\bar{\varphi}}$ для системы $\mathcal{E}^+(\bar{\varphi})$ является выполняющей. Используя предложение 1, найдем натуральное число N для $\mathcal{E}^+(\bar{\varphi})$ и всех подстановок $S_0^{\bar{\varphi}}, \ldots, S_h^{\bar{\varphi}}$. Затем найдем номер i_N, начиная с которого все ненулевые значения функций $\bar{\varphi}$ для аргументов, не превосходящих N, равны значению $\bar{\varphi}_i$.

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

φ-переход: $\bar{\varphi}_{i+1} = \bar{\varphi}'_i$, $\bar{\psi}_{i+1} = 0$; $\bar{\varphi}_i$ не является выполняющей подстановкой для $\mathcal{E}^1(\bar{\psi}_i)$.

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

Пусть $h_1=2^{m_1}$, где m_1 — количество ε-термов в системе $\mathcal{E}^1(\bar\psi)$. По теореме 1 любая последовательность соседних φ-переходов содержит не более h_1 членов. В силу выбора N, i_N любая начинающаяся с 0 последовательность соседних $\bar\psi$-переходов $\bar{\bar\psi}_k=0$, $\bar\psi_{k+1}, \ldots$ — это начальный отрезок последовательности $S^{\bar\varphi}_0, \ldots, S^{\bar\varphi}_h$, и потому он содержит не более h членов. Таким образом, последовательность $(\bar\varphi_i, \bar\psi_i)$ для $i \geqslant i_N$ имеет вид

$$\Phi_1, \Psi_1, \Phi_2, \Psi_2, \ldots, \tag{4}$$

где Φ_j и Ψ_j — участки, состоящие из последовательных φ- и ψ-переходов соответственно. Считая, для простоты записи, что $i_N=0$, можем представить участок (Ψ_i, Φ_{i+1}) в следующем виде:

$$(\bar\varphi^i, \bar\psi_1),\ (\bar\varphi^i, \bar\psi_2),\ \ldots,\ (\bar\varphi^i, \bar\psi_{k_i});\ (\bar\varphi^{i'}, 0),\ (\bar\varphi^{i''}, 0),\ \ldots,\ (\bar\varphi^{i(l_i)}, 0). \tag{5}$$

Здесь функции $\bar\psi_1, \bar\psi_2, \ldots$ — одни и те же на всех участках Ψ_i, различно только их количество $k_i \leqslant h$. Длина l_i участка Φ_{i+1} может быть равна единице, т. е. может быть $\bar\varphi^{i+1}=\bar\varphi^{i'}$. Предположим, что одно и то же число k встретилось в качестве k_i в (5) для нескольких, скажем, q_k значений i (не обязательно последовательных). Обозначим $\bar\psi_k$ через $\bar\psi$. Ни при каком i подстановка $\bar\varphi^i$ не является выполняющей для $\mathcal{E}^1(\bar\psi)$, иначе φ-переход после участка Ψ_i 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 $\mathcal{E}^1(\bar\psi)$. Поскольку последовательные φ-компоненты — продолжения друг друга, то в силу части Б теоремы, примененной к $\mathcal{E}^1(\bar\psi)$, получаем $q_k \leqslant h_1$. А из $k \leqslant h$ следует, что имеется не более hh_1 участков, т. е. последовательность ε-подстановок обрывается, что и требовалось доказать.

Замечание. Из определения ε-подстановки следует, что выполняющая ε-подстановка для данной системы ε-формул выполняет также формулы $\varepsilon x A(x) \neq 0 \rightarrow A(\varepsilon x A)$ и $\varepsilon x A \neq 0 \rightarrow (t < \varepsilon x A \rightarrow \neg A(t))$ с термами $\varepsilon x A$, для которых вообще написаны ε-формулы. Это позволяет учесть дополнительную гильбертовскую аксиому $\forall x(A \leftrightarrow B) \rightarrow \varepsilon x A = \varepsilon x B$.

ЛИТЕРАТУРА

1. Ackermann, W., Math. Ann., 117, Hf. 2, 162—194 (1940).
2. Hilbert, D., Bernays, P., Grundlagen der Mathematik, 2, Springer Verlag, Berlin—Heidelberg—New York, 1968.

Институт кибернетики
Академии наук Эстонской ССР

Поступила в редакцию
23/II 1982

G. MINTS

ARITMEETIKA MITTEVASTURÄÄKIVUSE LIHTSUSTATUD TÕESTUS

Artiklis on esitatud uus tõestus Hilberti ε-asenduste meetodi koonduvust käsitleva Ackermanni teoreemi rakendatavusest aritmeetikas. Tõestuse lihtsus on saavutatud pideva (transfiniitse) funktsionaali mõiste kasutamise teel.

G. MINTS

SIMPLIFIED CONSISTENCY PROOF FOR ARITHMETIC

Hilbert's ε-substitution method was devised to achieve the main aim of Hilbert's program — elimination of transfinite sentences from derivations of finite ones. Satisfying ε-substitution for given derivation is a kind of (local) finite model satisfying all axioms from the given formal derivation. ε-substitution method is a successive approximation method for generating new ε-substitutions (finite models) until a satisfying one is achieved. In 1939 W. Ackermann proved that the method converges, and that the process eventually stops after the finite number of steps, producing a satisfying substitution. His proof contained a lot of combinatorial lemmas and induction on the ordinal ε-zero. We present a new convergence proof where combinatorial details are simplified by introducing the non-finite notion of a continuous functional of type 1. Combinatorial part of the proof is contained in the following slight extension of a theorem by J. von Neumann.

Theorem. *Let $\mathfrak{S}$ be a system of ε-formulas of rank 1, let S and S^+ be ε-substitutions for (ε-matrices occurring in) $\mathfrak{S}$ such that every non-zero value from S is preserved in S^+, and the value of some term t occurring in $\mathfrak{S}$ is different under S and S^+. Then there is an ε-term r occurring in t such that the value of t is* 0 *under S but different from* 0 *under S^+.*

This implies that the ε-substitution method converges for ε-formulas of rank 1 in no more than 2^m steps, where m is the total number of ε-terms in the system $\mathfrak{S}$. Convergence in a general case is proved by induction on the rank (nesting of variable occurrences bound by different ε-symbols) and uses continuous dependence of the solution of parameters.

Proposition. *For any system $\mathfrak{S}(f)$ of ε-formulas with the free function variable f, for any arithmetic function $\bar{f}$ and ε-substitution S for the system $\mathfrak{S}(\bar{f})$, there is a natural number N such that the ε-substitution S' which is the successor of S is the same for any system $\mathfrak{S}(\bar{g})$ for any function $\bar{g}$ which has the same values as $\bar{f}$ for all arguments not exceeding N.*

Since the satisfying substitution changes ε-symbols into (local) least-number operators, it is possible to satisfy also Hilbert's additional axiom: $\forall x(A \leftrightarrow B) \rightarrow \varepsilon x A = \varepsilon x B$.