Ю. В. Матиясевич, Арифметические представления перечислимых множеств с небольшим числом кванторов, *Зап. научн. сем. ЛОМИ*, 1972, том 32, 77–84

Ю.В.Матиясевич

АРИФМЕТИЧЕСКИЕ ПРЕДСТАВЛЕНИЯ ПЕРЕЧИСЛИМЫХ МНОЖЕСТВ С НЕБОЛЬШИМ ЧИСЛОМ КВАНТОРОВ

(Основные результаты доложены 17 февраля 1972 г.)

В [1] – [5] указаны различные арифметические представления перечислимых множеств натуральных чисел, содержащие небольшое число кванторов. В настоящей заметке показано, что каждое перечислимое множество $\mathfrak{M}$ натуральных чисел представимо в любом из следующих видов:

$$a \in \mathfrak{M} \Leftrightarrow \exists p \exists s \underset{i=1}{\overset{\pi}{\&}} \exists v \left[A_i(a,p,s,v) > 0\right], \tag{1}$$

$$a \in \mathfrak{M} \Leftrightarrow \exists s \underset{i=1}{\overset{\pi}{\&}} \exists p \exists v \left[B_i(a,p,s,v) > 0\right], \tag{2}$$

$$a \in \mathfrak{M} \Leftrightarrow \exists t \forall y_{\le t} \exists v \exists w \left[C(a,t,y,v,w) = 0\right]. \tag{3}$$

Здесь π – некоторое конкретное натуральное число, A_i, B_i, C – полиномы с целыми коэффициентами; строчные латинские буквы, в том числе и с индексами, здесь и ниже используются в качестве переменных для целых положительных чисел.

В построении представлений (1) – (3) мы исходим из представления множества $\mathfrak{M}$ в виде

$$a \in \mathfrak{M} \Leftrightarrow \exists z_1 \ldots \exists z_\eta \left[a = M(z_1, \ldots, z_\eta)\right]$$

где η – некоторое натуральное число, а M – полином с целыми коэффициентами (см. [6]). Пусть

$$M(z_1,\ldots,z_\eta) = \sum_{0 \le d_1+\ldots+d_\eta \le \varkappa} \mu_{d_1,\ldots,d_\eta} z_1^{d_1} \ldots z_\eta^{d_\eta}. \tag{4}$$

Определим числа $\lambda_{d_1,\ldots,d_\eta}$ с помощью тождества

$$(1+u_1+\ldots+u_\eta)^{\varkappa} = \sum_{0 \le d_1+\ldots+d_\eta \le \varkappa} \lambda_{d_1,\ldots,d_\eta} u_1^{d_1} \ldots u_\eta^{d_\eta} \tag{5}$$

и пусть λ – какое-либо положительное число, кратное всем этим числам. Определим числа $\nu_{d_1,\ldots,d_\eta}$ следующим образом:

$$\lambda_{d_1,\ldots,d_\eta} \nu_{d_1,\ldots,d_\eta} = \lambda \mu_{d_1,\ldots,d_\eta}. \tag{6}$$

Пусть $\tau = \varkappa + 1$, $\delta = \varkappa \tau^{\eta-1}$, $\sigma = 2\tau^\eta + 3$,

$$Z(q) = 1 + \sum_{i=1}^{\eta} z_i q^{\tau^{i-1}} + q^\sigma,$$

$$N(d_1,\ldots,d_\eta) = \sum_{i=1}^{\eta} d_i \tau^{i-1},$$

$$U(q) = 1 + \sum_{0 \le \alpha_1 + \ldots + \alpha_\eta \le \varkappa} v_{\alpha_1, \ldots, \alpha_\eta} q^{\delta - N(\alpha_1, \ldots, \alpha_\eta)} + q^{\sigma}.$$

Определим полиномы $R_i(z_1, \ldots, z_\eta)$ посредством тождества

$$(Z(q))^{\varkappa} U(q) = \sum_{i=0}^{\sigma\tau} R_i(z_1, \ldots, z_\eta) q^i \qquad (7)$$

Следующая лемма очевидна.

ЛЕММА 1. $R_{\sigma\tau}(z_1, \ldots, z_\eta) = 1.$

ЛЕММА 2. $R_\delta(z_1, \ldots, z_\eta) = \lambda M(z_1, \ldots, z_\eta).$

Доказательство леммы 2 основано на тождествах (5)–(7) и следующем легко проверяемом свойстве полинома N : если $0 \le \alpha_1, \ldots, \alpha_\eta, \beta_1, \ldots, \beta_\eta \le \varkappa$ и $N(\alpha_1, \ldots, \alpha_\eta) = N(\beta_1, \ldots, \beta_\eta)$, то $\alpha_1 = \beta_1, \ldots, \alpha_\eta = \beta_\eta$.

Обозначим через γ сумму абсолютных величин всех коэффициентов всех полиномов $R_0, \ldots, R_{\sigma\tau}$. Следующая лемма очевидна.

ЛЕММА 3. При $i = 0, \ldots, \sigma\tau$

$$|R_i(z_1, \ldots, z_\eta)| \le \gamma (\max\{z_1, \ldots, z_\eta\})^{\varkappa}.$$

ЛЕММА 4. Если числа $a, q, s, z_1, \ldots, z_\eta$ таковы, что $2\lambda a < q$, $s = Z(q)$ и

$$1 + 2\gamma (\max\{z_1, \ldots, z_\eta\})^{\varkappa} < q, \qquad (8)$$

то для того, чтобы $a = M(z_1, \ldots, z_\eta)$, необходимо и достаточно, чтобы существовало число v_1 такое, что

$$-q^{\delta} < 2(s^{\varkappa} U(q) - v_1 q^{\delta+1} - \lambda a q^{\delta}) < q^{\delta}. \qquad (9)$$

НЕОБХОДИМОСТЬ. Согласно тождеству (7) и леммам 1–3 можно положить

$$v_1 = \sum_{i=\delta+1}^{\sigma\tau} R_i(z_1, \ldots, z_\eta) q^{i-\delta-1}$$

ДОСТАТОЧНОСТЬ. Ясно, что существует не более одного целого числа χ такого, что

$$-q^{\delta} < 2(s^{\tau}u(q) - \chi q^{\delta}) < q^{\delta}.$$

Согласно тождеству (7) и лемме 3 таким числом χ является число

$$\sum_{i=\delta}^{\delta\tau} R_i(z_1,\dots,z_\eta)q^{i-\delta}$$

следовательно,

$$v_1 q + \lambda a = \sum_{i=\delta}^{\delta\tau} R_i(z_1,\dots,z_\eta)q^{i-\delta}$$

и

$$\lambda a \equiv R_\delta(z_1,\dots,z_\eta)(\mathrm{mod}\, q).$$

Согласно леммам 2 и 3 отсюда следует, что $a = M(z_1,\dots,z_\eta)$.

Лемма доказана.

ЛЕММА 5. Каковы бы ни были числа p, q, s, если $p < q$, то для того, чтобы существовали числа $z_1,\dots,z_\eta$, такие что $s = Z(q)$ и $\max\{z_1,\dots,z_\eta\} < p$, необходимо и достаточно, чтобы существовали числа $v_2,\dots,v_{\eta+2}$ такие, что

$$s - v_2 q = 1, \tag{10}$$

$$q^{\tau^{j-1}} < s - v_{j+2}q^{\tau^j} < pq^{\tau^{j-1}} \quad (j = 1,\dots,\eta-1), \tag{11}$$

$$q^{\tau^{\eta-1}} < s - q^{\sigma} < pq^{\tau^{\eta-1}} \tag{12}$$

НЕОБХОДИМОСТЬ. Легко проверить, что можно положить

$$v_{j+1} = \sum_{i=j+1}^{\eta} z_i q^{\tau^{i-1}-\tau^j} + q^{\sigma-\tau^j} \quad (j = 1,\dots,\eta).$$

ДОСТАТОЧНОСТЬ. Представим число s в виде

$$s = \sum_{i=0}^{\psi} \chi_i q^i,$$

где $0 \le \chi_i < q$, $i = 0,\dots,\psi$. Из (10) следует, что $\chi_0 = 1$. Из (11) получаем, что при $j = 1,\dots,\eta-1$

$$v_j q^{\tau^j} = \sum_{i=\tau^j}^{\psi} \chi_i q^i,$$

и, следовательно,

$$q^{\tau^{j-1}} < \sum_{i=0}^{\tau^j-1} \chi_i q^i < pq^{\tau^{j-1}}.$$

Из этого неравенства вытекает, что $\chi_i = 0$ при $i = \tau^{j-1}+1, \ldots, \tau^j - 1$, $0 < \chi_{\tau^{j-1}} < \rho$. Аналогично из (I2) следует, что $\chi_i = 0$ при $i = \tau^{\eta-1}+1, \ldots, \sigma-1, \sigma+1, \ldots, \psi$, $0 < \chi_{\tau^{\eta-1}} < \rho$, $\chi_\sigma = 1$. Таким образом, в качестве $z_1, \ldots, z_\eta$ можно взять соответственно $\chi_{\tau^0}, \ldots, \chi_{\tau^{\eta-1}}$. Лемма доказана.

Легко проверить, что условия (9)–(I2) эквивалентны условиям

$$q^{2\delta} - 4(s^\varkappa U(q) - v_1 q^{\delta+1} - \lambda a q^\delta)^2 > 0,$$

$$1 - (s - v_2 q - 1)^2 > 0,$$

$$(\rho-1)^2 q^{2\tau^{j-1}} - (2s - 2v_{j+2} q^{\tau^j} - (\rho+1) q^{\tau^{j-1}})^2 > 0$$

$$(j = 1, \ldots, \eta-1),$$

$$(\rho-1)^2 q^{2\tau^{\eta-1}} - (2s - 2q^\sigma - (\rho+1) q^{\tau^{\eta-1}})^2 > 0$$

соответственно. Введем следующие обозначения:

$$Q \leftrightharpoons 2(\gamma \rho^\varkappa + \lambda a),$$

$$A_1(a,\rho,s,v) \leftrightharpoons Q^{2\delta} - 4(s^\varkappa U(Q) - v Q^{\delta+1} - \lambda a Q^\delta)^2,$$

$$A_2(a,\rho,s,v) \leftrightharpoons 1 - (s - v Q - 1)^2,$$

$$A_{2+j}(a,\rho,s,v) \leftrightharpoons (\rho-1)^2 Q^{2\tau^{j-1}} - (2s - 2v Q^{\tau^j} - (\rho+1) Q^{\tau^{j-1}})^2$$

$$(j = 1, \ldots, \eta-1),$$

$$A_{\eta+2}(a,\rho,s,v) \leftrightharpoons (\rho-1)^2 Q^{2\tau^{\eta-1}} - (2s - 2Q^\sigma - (\rho+1) Q^{\tau^{\eta-1}})^2.$$

ТЕОРЕМА I. Каково бы ни было a, если

$$\exists \rho \, \exists s \, \&_{i=1}^{\eta+2} \, \exists v \, [A_i(a,\rho,s,v) > 0]$$

то $a \in \mathfrak{M}$; каково бы ни было a, если $a \in \mathfrak{M}$, то существует число ρ_0 такое, что

$$\forall \rho_{>\rho_0} \, \exists s \, [Q^\sigma < s < Q^\sigma + Q^{\tau^{\eta-1}+1} \, \&$$

$$\& \overset{\eta+2}{\underset{i=1}{\&}} \exists v [A_i(a,p,s,v)>0]].$$

ДОКАЗАТЕЛЬСТВО. Пусть числа $a, p, s, v_1, \ldots, v_{\eta+2}$ таковы, что $A_i(a,p,s,v_i)>0$ при $i=1,\ldots,\eta+2$. Положим $q=Q$. Согласно лемме 5 существуют числа $z_1,\ldots,z_\eta$ такие, что $s=Z(q)$ и $max\{z_1,\ldots,z_\eta\}<p$. Из этого неравенства следует неравенство (8) и согласно лемме 4 $a=M(z_1,\ldots,z_\eta)$, следовательно, $a\in\mathfrak{M}$. Первая часть теоремы доказана.

Пусть $a\in\mathfrak{M}$. Найдем числа $z_1,\ldots,z_\eta$ такие, что $a=M(z_1,\ldots,z_\eta)$. Положим $p_0=max\{z_1,\ldots,z_\eta\}$ и пусть $p>p_0$. Положим $q=Q$, $s=Z(q)$. Нетрудно проверить, что

$$Q^\sigma < s < Q^\sigma + Q^{\tau^{\eta-1}+1}.$$

Согласно леммам 4 и 5 существуют числа $v_1,\ldots,v_{\eta+2}$ такие, что $A_i(a,p,s,v_i)>0$ при $i=1,\ldots,\eta+2$. Теорема доказана.

Введем следующие обозначения:

$$D_1 \leftrightharpoons Q^{2\delta},$$

$$D_2 \leftrightharpoons 1,$$

$$D_{2+j} \leftrightharpoons Q^{2\tau^{j-1}+1} \qquad (j=1,\ldots,\eta),$$

$$B_j(a,p,s,v) \leftrightharpoons Q^{2\sigma-2} A_j(a,p,s,v) - D_j(s-Q^\sigma)^2 \qquad (j=1,\ldots,\eta+2).$$

ТЕОРЕМА 2. Каково бы ни было число a, для того, чтобы $a\in\mathfrak{M}$, необходимо и достаточно, чтобы

$$\exists s \overset{\eta+2}{\underset{i=1}{\&}} \exists p \exists v [B_i(a,p,s,v)>0]. \qquad (13)$$

НЕОБХОДИМОСТЬ. Пусть $a\in\mathfrak{M}$. Найдем согласно теореме I числа $p, s, v_1, \ldots, v_{\eta+2}$ такие, что $A_i(a,p,s,v_i)>0$ при $i=1,\ldots,\eta+2$ и

$$Q^\sigma < s < Q^\sigma + Q^{\tau^{\eta-1}+1}.$$

Для $i=1,\ldots,\eta+2$ имеем:

$$B_i(a,p,s,v_i) = Q^{2\sigma-2} A_i(a,p,s,v_i) - D_i(s-Q^\sigma)^2 >$$

$$> Q^{2\sigma-2} - Q^{2\tau^{\eta-1}+1} Q^{2\tau^{\eta-1}+2} \geq 0.$$

6 1410

ДОСТАТОЧНОСТЬ. Пусть числа i, a, s, ρ, v таковы, что $B_i(a,s,\rho,v) > 0$. Поскольку $D_i \geqslant A_i(a,s,\rho,v)$, то отсюда следует, что $(s - Q^\sigma)^2 < Q^{2\sigma-2}$. Далее имеем:

$$-Q^{\sigma-1} < s - Q^\sigma < Q^{\sigma-1},$$

$$(Q - \tfrac{1}{2})^2 < Q^\sigma - Q^{\sigma-1} < s < Q^\sigma + Q^{\sigma-1} < (Q + \tfrac{1}{2})^\sigma,$$

$$Q - \tfrac{1}{2} < \sqrt[\sigma]{s} < Q + \tfrac{1}{2},$$

$$\sqrt[\sigma]{s} - \tfrac{1}{2} < Q < \sqrt[\sigma]{s} + \tfrac{1}{2}$$

Таким образом, Q, а, следовательно, и ρ однозначно определяются по s, поэтому формула (13) эквивалентна формуле

$$\exists s \exists \rho \bigwedge_{i=1}^{\eta+2} \exists v [B_i(a,\rho,s,v) > 0].$$

Теперь осталось заметить, что неравенство $B_i(a,\rho,s,v) > 0$ влечет неравенство $A_i(a,\rho,s,v) > 0$ и воспользоваться теоремой I. Теорема доказана.

Обозначим через S_i выражение

$$\tfrac{1}{2}\left(\frac{t}{2^{i-1}y} + 1\right),$$

через E_i — такие полиномы с целыми коэффициентами, что

$$E_i = (2^i y)^\varkappa A_i(a, 2^{i-1}y, S_i, v),$$

$$F_i \leftrightharpoons 2^i y((y-1)tE_i - S_i - w) \quad (i = 1, \ldots, \eta+2),$$

$$G_1 \leftrightharpoons (y-1)^2 + (t - 2^{\eta+2}w)^2,$$

$$G_2 \leftrightharpoons y - (2v+1)w,$$

$$G_3 \leftrightharpoons (t - 2^{\eta+2}vy)^2 + (y - w - 1)^2,$$

$$G_4 \leftrightharpoons 2vt - y(2w+1),$$

$$C(a,t,y,v,w) \leftrightharpoons G_1 \ldots G_4 F_1 \ldots F_{\eta+2}.$$

ТЕОРЕМА 3. Каково бы ни было число a, для того, чтобы $a \in \mathfrak{M}$, необходимо и достаточно, чтобы

$$\exists t\, \forall y_{\leq t}\, \exists v\, \exists w\, [C(a,t,y,v,w)=0].$$

НЕОБХОДИМОСТЬ. Пусть $a \in \mathfrak{M}$. Найдем согласно теореме I числа $m, \rho, s, v_1, \ldots, v_{\eta+2}$ такие, что $m > \eta+2$, $\rho = 2^m$ и $A_i(a,\rho,s,v_i)>0$ при $i=1,\ldots,\eta+2$. Положим $t=(2s-1)\rho$. Пусть y — произвольное число, не превосходящее t.

Если $y=1$, то можно выбрать w так, что $G_1=0$ и, следовательно, $C(a,t,y,v,w)=0$.

Если y не является степенью числа 2, то можно выбрать v и w так, что $G_2=0$ и, следовательно, $C(a,t,y,v,w)=0$.

Если $y=2^n$, $n \leq m-\eta-2$, то можно выбрать v и w так, что $G_3=0$ и, следовательно, $C(a,t,y,v,w)=0$.

Если $y=2^n$, $n \geq m+1$, то можно выбрать w так, что $G_4=0$ и, следовательно, $C(a,t,y,v,w)=0$.

Если $y=2^{m+1-j}$, $1 \leq j \leq \eta+2$, то $2^{j-1}y=\rho$, $S_j=s$. Положим $v=v_j$. Так как $(y-1)tE_i - S_i > t-s>0$, то можно выбрать w так, что $F_j=0$ и $C(a,t,y,v,w)=0$. Этим завершается рассмотрение всех возможных значений y.

ДОСТАТОЧНОСТЬ. Пусть числа a и t таковы, что

$$\forall y_{\leq t}\, \exists v\, \exists w\, [C(a,t,y,v,w)=0].$$

Нетрудно проверить, что если $y=1$, то $G_2 \ldots G_4 F_1 \ldots F_{\eta+2} \neq 0$, следовательно, существуют такие v и w, что $G_1=0$, откуда получаем, что $2^{\eta+2} \mid t$.

Обозначим через m наибольшее число такое, что $2^m \mid t$ и положим $\rho = 2^m$, $s=(2^{-m}t+1)/2$. Докажем, что

$$\&_{i=1}^{\eta+2} \exists v\, [A_i(a,\rho,s,v)>0]. \qquad (I4)$$

Пусть i — число, не превосходящее $\eta+2$. Положим $y=2^{m+1-i}$ и найдем числа v, w такие, что $C(a,t,y,v,w)=0$. Нетрудно проверить, что в этом случае $G_1 \ldots G_4 \neq 0$ и, следовательно, найдется такое j, что $F_j=0$. Так как $F_j=0$, то S_j — число целое, а это возможно лишь в том случае, когда $2^{j-1}y=2^m$. Следовательно, $j=i$, $2^{i-1}y=\rho$, $S_j=s$ и $A_i(a,\rho,s,v)>0$. Справедливость формулы (I3) обоснована, для завершения доказательства осталось применить теорему I.

ЛИТЕРАТУРА

I. Davis M. Arithmetical problems and recursively enumerable predecates. " J. Symbol. Log.", I953, I8, № I, 33–4I (русск. перев.: "Математика", I964, 8, № 5, I5–22).

2. Robinson R.M. Arithmetical representation of recursively enumerable sets. "J. Symbol. Log.", 1956, 21, № 2, 162-186. (русск.перев.: "Математика", 1964, 8, № 5, 15-22).

3. Robinson R.M. An undecidable diophantine problem. A talk given to the IV Int.Congr. for Logic, Meth. and Phil. of Science, Bucharest, 1971.

4. Robinson R.M. Some representations of diophantine sets. " J. Symbol. Log.", в печати.

5. Matijasevič Yu. On arithmetical unsolvability of Hilbert's 10-th problem. Proc. IV Int.Congr.for Log., Meth.and Phil. of Science, в печати.

6. Матиясевич Ю.В. Диофантово представление перечислимых предикатов. "Изв.АН СССР, сер. матем.", 1971, 35, 3-30.