KYBERNETIKA ČÍSLO 2, ROČNÍK 3/1967

Poznámka k pojmu problému a řešitelnosti

PAVEL TICHÝ

Prostředky teorie částečně rekursivních funkcí je ukázáno, že pojem řešitelnosti problému navržený v [2] je neadekvátní.

S každou funkcí f je spojen tzv. *masový problém*. Jde o problém najít efektivní postup, který aplikován na libovolný prvek x definičního oboru funkce f vede po konečném počtu kroků k identifikaci předmětu $f(x)$. Je-li f matematická funkce, nazývá se každý takový postup algoritmem. Poněvadž efektivní postup lze aplikovat jen na předměty konečné povahy, lze se při studiu algoritmů omezit na funkce, jejichž definiční obor i obor hodnot je nějakou množinou nezáporných celých čísel. Pojem algoritmu byl precizován v několika na sobě nezávislých teoriích, v teorii částečně rekursivních funkcí, v teorii Turingových strojů a v teorii normálních algoritmů. Jak známo, všechny tyto teorie jsou vzájemně ekvivalentní; v tomto článku se budeme vyjadřovat v termínech první z těchto teorií, kde je pojem algoritmu ztotožněn s pojmem částečně rekursivní funkce. Symboly T_1^1, U, μ, $\cong$, $(x)_y$ a $\{e\}(x)$ mají stejný význam jako v [1]. ∂f je definiční obor funkce f. Funkci f budeme nazývat restrikcí funkce g, jestliže $\partial f \subset \partial g$ a pro každé $x \in \partial f$ platí, že $f(x) = g(x)$. Oborem hodnot všech individuálních proměnných je množina nezáporných celých čísel. Množina všech uspořádaných dvojic $\langle x, f(x) \rangle$ takových, že $x \in \partial f$ se zpravidla nazývá grafem funkce f. Místo uspořádaných dvojic čísel $\langle x, y \rangle$ budeme pracovat s čísly, která tyto dvojice efektivně representují, totiž s čísly $2^x . 3^y$. Grafem funkce f tedy nazýváme množinu $\{2^x . 3^{f(x)} \mid x \in \partial f\}$.

Masový problém, spojený s funkcí f je řešitelný, existuje-li efektivní postup, který je aplikovatelný na každé číslo x z ∂f a který, aplikován na libovolné takové číslo x vede po konečném počtu kroků k hodnotě $f(x)$ funkce f pro argument x. V termínech částečně rekursivních funkcí vystihuje tento pojem tato

Definice. Masový problém, spojený s funkcí f je *řešitelný*, je-li f restrikcí nějaké částečně rekursivní funkce.

P. Materna navrhl v [2] jiný pojem řešitelnosti. V jeho pojetí je masový problém, spojený s funkcí f, řešitelný, existuje-li efektivní postup, který aplikován na libovolný prvek množiny ∂f vede po konečném počtu kroků k identifikaci jednoho z prvků grafu funkce f, přičemž pro každý prvek u grafu funkce f existuje prvek x množiny ∂f tak, že postup, aplikován na x vede k identifikaci u. V oboru nezáporných celých čísel precizuje tento pojem tato

Definice. Masový problém, spojený s funkcí f je *M-řešitelný*, existuje-li částečně rekursivní funkce g taková, že

$$\text{(a)} \qquad \partial f \subset \partial g\,,$$

$$\text{(b)} \qquad g(\partial f) = \{2^x \,.\, 3^{f(x)} \mid x \in \partial f\}\,.$$

Je hned vidět, že je-li masový problém spojený s funkcí f řešitelný, je i M-řešitelný. Neboť je-li g částečně rekursivní funkce, jejíž existence je požadována definicí řešitelnosti, je částečně rekursivní funkce $\bar{g}(x) = 2^x \,.\, 3^{g(x)}$ funkce, vyhovující podmínkám (a) a (b) z definice M-řešitelnosti.

Avšak z M-řešitelnosti funkce f nijak bezprostředně neplyne její řešitelnost. Předpokládejme, že g má vzhledem k f vlastnosti (a) a (b) a že máme dáno nějaké $x \in \partial f$. K identifikaci hodnoty $f(x)$ stačí najít takové $y \in \partial f$, že $(g(y))_0 = x$; díky (b) takové y existuje a $(g(y))_1 = f(x)$. Avšak v důsledku toho, že nemusí nutně existovat efektivní procedura, která generuje množinu ∂f (∂f nemusí být rekursivně spočetná) není předem jasné, zda existuje efektivní postup, jak ke každému $x \in \partial f$ najít $y \in \partial f$ takové, že $(g(y))_0 = x$.

Cílem tohoto článku je ukázat, že pojem M-řešitelnosti je slabší než pojem řešitelnosti. K tomu je třeba definovat funkci f tak, že masový problém spojený s f je M-řešitelný ale nikoli řešitelný. To vede k netriviální úloze z teorie rekursivních funkcí, jejíž řešení může být zajímavé i bez vztahu k předchozí definici.

Věta. *Existuje (částečná) funkce f a rekursivní funkce g taková, že platí* (a), (b) *a f přitom není restrikcí žádné částečně rekursivní funkce.*

Důkaz. Označme $\eta(x, y, z) = 2^x \,.\, 3^y \,.\, 5^z$. Definujeme:

$$\varphi(n) = \begin{cases} 1 \text{ jestliže } (Ey)_{y<(n)_2}\, T_1^1\,((n)_0, (n)_1, y))\ \&\ U(\mu y_{y<(n)_2}\, T_1^1\,((n)_0, (n)_1, y)) = 0\,, \\ 0 \text{ v opačném případě}\,. \end{cases}$$

Vzhledem k tomu, že T_1^1 resp. U je rekursivní predikát resp. funkce a že oba operátory jsou omezeny, je φ zřejmě rekursivní funkce. Ukážeme nyní, že $(e)\,(k)\,(Ev)\,(z)\,.\,[z \geqq v \rightarrow \varphi(\eta(e, k, z)) = \varphi(\eta(e, k, v))]$. Skutečně. Předpokládejme nejprve, že

$$(*) \qquad (Ey)\, T_1^1(e\ \ k, y)\ \&\ U(\mu y T_1^1(e\ \ k, y)) = 0$$

a nechť Y je nejmenší y takové, že $T_1^1(e, k, y)$. Pak podle definice funkce φ zřejmě $\varphi(\eta(e, k, z)) = 1$ pro všechna $z \geqq Y + 1$. Nyní předpokládejme, že $(*)$ neplatí.

Pak jsou dvě možnosti: i) $(y) \neg T_1^1(e, k, y)$ nebo ii) $(Ey)\, T_1^1(e, k, y)\, \&\, U(\mu y T_1^1(e, k, y) > 0$. V případě i) zřejmě $(z)\, \varphi(\eta(e, k, z)) = z$; v případě ii) nechť Y je nejmenší y takové, že $T_1^1(e, k, y)$. Pak zřejmě $\varphi(\eta(e, k, z)) = 0$ pro všechna $z \geqq Y + 1$.

Položme: $\pi(e, k) = \mu v[(z)\,[z \geqq v \rightarrow \varphi(\eta(e, k, z)) = \varphi(\eta(e, k, v))]]$. Zřejmě:

$$(1) \qquad \varphi(\eta(e, k, \pi(e, k))) = \begin{cases} 1 \text{ jestliže } (Ey)\, T_1^1(e, k, y)\, \&\, U(\mu y T_1^1(e, k, y)) = 0\,, \\ 0 \text{ v opačném případě}\,. \end{cases}$$

Definujme:

$$w(0) = 0\,,$$

$$w(e + 1) = \eta(e, w(e), \pi(e, w(e)))\,.$$

Protože pro všechna x, y, z číslo $\eta(x, y, z)$ je větší než x, y, z, máme:

$$(2) \qquad w(e) < w(e + 1) \text{ pro všechna } e\,.$$

Definujeme dále:

$$A = \{w(e) \mid e \geqq 0\}\,,$$

$$g(n) = \begin{cases} 3^{\varphi(w(1))} & \text{jestliže} \quad n = 0\,, \\ 2^{(n)_1} \,.\, 3^{\varphi(n)} & \text{v opačném případě}\,. \end{cases}$$

Funkce g je zřejmě rekursivní.

Dokážeme, že $(k)_{k \in A}\, (En)_{n \in A}\, [(g(n))_0 = k]$. Protože $A = \{w(e) \mid e \geqq 0\}$, stačí ukázat, že $(e)\,(En)\,[n \in A\, \&\, (g(n))_0 = w(e)]$. Vezměme tedy libovolné e a položme $n = w(e + 1)$. Pak $n \in A$ a $(g(n))_0 = (g(w(e + 1)))_0 = (g(\eta(e, w(e), \pi(e, w(e)))))_0 = (2^{w(e)} \,.\, 3^{\varphi(n)})_0 = w(e)$.

Můžeme tedy definovat funkci f tak, že $\partial f = A$ a pro každé $k \in A$

$$f(k) = (g(\mu n_{n \in A}[(g(n))_0 = k]))_1\,.$$

K tomu, abychom dokázali, že f a g vyhovují podmínkám (a) a (b), budeme potřebovat následující tvrzení:

$$(3) \qquad \text{pro všechna } n_1, n_2 \in A \quad (g(n_1))_0 = (g(n_2))_0 \rightarrow (g(n_1))_1 = (g(n_2))_1\,.$$

Abychom dokázali (3), označme nejprve e_1 resp. e_2 to jediné číslo e, že $n_1 = w(e)$ resp. $n_2 = w(e)$. Máme tedy $n_1 = w(e_1)$, $n_2 = w(e)_2$. Nechť $(g(n_1))_0 = (g(n_2))_0$. Předpokládejme nejprve, že $e_1, e_2 > 0$. V důsledku (2) je pak zřejmě $n_1, n_2 > 0$. Podle definice funkce w a g máme: $w(e_1 - 1) = (w(e_1))_1 = (n_1)_1 = (g(n_1))_0 = (g(n_2))_0 = (n_2)_1 = (w(e_2))_1 = w(e_2 - 1)$. Odtud v důsledku (2) plyne $e_1 = e_2$, tedy $n_1 = n_2$, $(g(n_1))_1 = (g(n_2))_1$. Předpokládejme nyní, že jedno z čísel e_1, e_2 je rovno nule, např. $e_1 = 0$ a $e_2 > 0$. Máme $n_2 > 0$ a tedy $w(e_2 - 1) = (w(e_2))_1 = (n_2)_1 = (g(n_2))_0 = (g(n_1))_0 = (g(w(e_1)))_0 = (g(0))_0 = 0$, z čehož v důsledku (2) plyne $e_2 = 1$. Platí tedy $(g(n_1))_1 = (g(w(e_1)))_1 = (g(0))_1 = \varphi(w(1)) = (g(w(1)))_1 = (g(w(e_2)))_1 = (g(n_2))_1$. Tvrzení (3) je tedy dokázáno.

Dokážeme nyní, že

$$(4) \qquad g(A) = \{2^k \,.\, 3^{f(k)} \mid k \in A\}\,.$$

Nechť $x \in g(A)$. Podle definice funkce g pak zřejmě existuje n_1, $m \in A$ a v takové, že $x = g(n_1) = 2^m \,.\, 3^v$. Nechť $n_2 = \mu n_{n\in A}[(g(n))_0 = m]$. Podle definice funkce f máme $f(m) = (g(n_2))_1$; protože n_1, $n_2 \in A$ a $(g(n_1))_0 = (g(n_2))_0$, plyne podle (3), že $v = (g(n_1))_1 = (g(n_2))_1 = f(m)$, tedy $x \in \{2^k \,.\, 3^{f(k)} \mid k \in A\}$. Naopak, nechť $k \in A$ a $x = 2^k \,.\, 3^{f(k)}$. Nechť $n_2 = \mu n_{n\in A}[(g(n))_0 = k]$. Pak $f(k) = (g(n_2))_1$, $k = (g(n_2))_0$, $n_2 \in A$, tedy $g(n_2) = 2^{(g(n_2))_0} \,.\, 3^{(g(n_2))_1} = 2^k \,.\, 3^{f(k)} = x$. (4) je dokázáno.

Konečně dokážeme, že

$$(5) \qquad \text{pro žádné } e \text{ není } f \text{ restrikcí funkce } \{e\}\,(k) \cong U(\mu y T_1^1(e, k, y))\,.$$

Zvolme libovolné e. Je-li $e = 0$, je $f(0)$ definováno, zatímco $\{e\}\,(0)$ nikoli, neboť 0 není Gödelovým číslem žádného systému rovnic. $\partial f \subset \partial\{e\}$ tedy nemůže platit, je-li $e = 0$. Nechť tedy $e > 0$. Ukážeme, že buď funkce $\{e\}$ není definována na $w(e)$ nebo $f(w(e)) \neq \{e\}\,(w(e))$. Označme $k = w(e)$. Ukážeme nejprve, že $f(k) = \varphi(\eta(e, k, \pi(e, k))$. Nechť $N = \mu n_{n\in A}[(g(n))_0 = k]$; pak $f(k) = (g(N))_1$. Máme: $\eta(e, k, \pi(e, k)) \in A$ a $g(\eta(e, k, \pi(e, k)) = 2^k \,.\, 3^{\varphi(\eta(e,k,\pi(e,k)))}$. Protože $N \in A$ a $(g(N))_0 = (g(\eta(e, k, \pi(e, k))))_0$, plyne podle (2), že $f(k) = (g(N))_1 = (g(\eta(e, k, \pi(e, k))))_1 = \varphi(\eta(e, k, \pi,(e, k)))$. Předpokládejme nejprve, že $(Ey)\; T_1^1(e, k, y)$. Pak $\{e\}\,(k)$ je definováno a podle (1) $\{e\}\,(k) = U(\mu y T_1^1(e, k, y)) \neq \varphi(\eta(e, k, \pi(e, k))) = f(k)$ a f tedy není restrikcí funkce $\{e\}$. Nyní předpokládejme opak. Pak $\{e\}\,(k)$ není definováno, neplatí tedy $\partial f \subset \partial\{e\}$, tedy ani v tomto případě není f restrikcí funkce $\{e\}$.

(Autor je zavázán Doc. Dr. Jiřímu Bečvářovi, CSc., za několik kritických připomínek, které přispěly k přesnosti textu.)

(Došlo dne 31. března 1966.)

LITERATURA

[1] S. C. Kleene: Introduction to Metamathematics. Van Nostrand, New York/Toronto 1952.
[2] Pavel Materna: Operative Auffassung der Methode. Rozpravy ČSAV, Řada společenských věd, ročník 75, sešit 8, Praha 1965.

A Remark on the Concept of Problem and Solvability

PAVEL TICHÝ

In [2] the following definition of solvability (call it M-solvability) is suggested: The mass problem connected with a function f is M-solvable if there exists a partial recursive function g defined wherever f is defined and such that the set $\{g(x) \mid f(x)$ is defined$\}$ is the set of all ordered couples of the form $\langle y, f(y) \rangle$. In the present paper it is shown that the property of M-solvability is too weak since it does not secure for f to be a restriction of a partial recursive function (even if g is total recursive).

PhDr Pavel Tichý, CSc., Filosofická fakulta KU, Praha 1, Nám. Krasnoarmějců 2.