Časopis pro pěstování matematiky

Ladislav Rieger

Ke Kleeneho normální formě strojově vyčíslitelných funkcí

Časopis pro pěstování matematiky, Vol. 88 (1963), No. 3, 349--363

Persistent URL: http://dml.cz/dmlcz/117467

Časopis pro pěstování matematiky, roč. 88 (1963), Praha

KE KLEENEHO NORMÁLNÍ FORMĚ STROJOVĚ VYČÍSLITELNÝCH FUNKCÍ

LADISLAV RIEGER, Praha

(Došlo dne 22. ledna 1962)

V článku je podáno krátké odvození známé tzv. Kleeneho normální formy strojově vyčíslitelných funkcí s nezápornými celočíselnými argumenty a hodnotami (dále jen „funkcí") ve smyslu Turingově.[1])

1. TURINGŮV POČÍTAČ S PÁSKOU OHRANIČENOU DO LEVA

1.1. Turingův počítač M si představujeme jako ideálně primitivní[2]) ale zároveň co do rozsahu paměti neomezený samočinný počítač. Jeho dvě podstatné části jsou:

a) Doleva ohraničená[3]) a doprava neohraničená páska (obr. 1), rozdělená na jednotlivá políčka (buňky); páska zastává úlohu paměti, ale také je místem vstupu i výstupu Turingova počítače.

b) Konečný automat $\mathscr{A}_M$ opatřený pohyblivou snímací a zapisující hlavou. $\mathscr{A}_M$ je

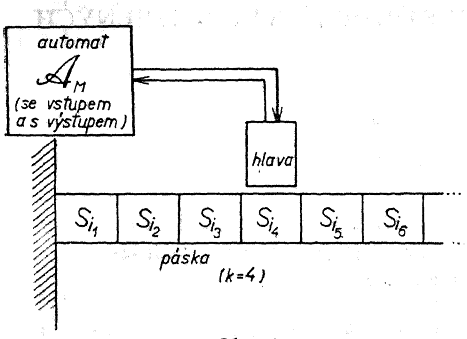
[1]) Na rozdíl od běžných odvození neužívá se tu symbolického aparátu a pojmů z matematické logiky a počet pomocných definic je co možno malý. „Číslo" znamená vždy celé nezáporné („přirozené") číslo.

[2]) Realizovat technicky samočinný počítač s neomezeným rozsahem paměti prozatím nelze; avšak sestrojit prakticky zařízení se „značně dlouhou" páskou a fungující podle schématu práce Turingova stroje není zásadním technickým problémem; takové zařízení by však nebylo schopno ničeho jiného, než čeho jsou schopny běžné elektronické samočinné počítače a navíc by bylo asi poměrně pomalé a drahé, takže (pokud je autorovi známo) dosud žádný počítač Turingova typu nebyl prakticky vyzkoušen. Je tedy Turingův počítač asi takovou idealizovanou schematizací skutečných počítačů jakou je např. matematické kyvadlo vzhledem k praktickým kyvadlům). Přitom je v případě Turingova počítače, jak se zdá, idealizace skutečnosti bližší než v případě matematického kyvadla jakožto „hmotného bodu zavěšeného na tuhé bezvážné niti". Smysl co největšího zjednodušení jednotlivých početních kroků Turingova stroje je teoreticko-matematický. Dovoluje totiž studovat početní procesy v jejich „čisté" formě — a např. v numerickém počítání není vázán na žádnou číselnou soustavu.

[3]) V tomto bodě se nepodstatně odchylujeme od běžného (a v podstatě již od A. M. TURINGA [1] z r. 1936 pocházejícího) pojetí, v němž se předpokládá páska na obě strany neohraničená. Snadno lze dokázat (viz M. DAVIS [1], str. 26—27), že náš formálně zjednodušující předpoklad ohraničenosti pásky vlevo není na újmu schopností Turingových strojů.

jakousi operační jednotkou stroje M. Hlava automatu $\mathscr{A}_M$ se nalézá (v matematické idealizaci „vždy“, ve skutečnosti by to bylo „až na zanedbatelně malé intervaly přechodu“) nad jediným políčkem pásky.

1.2. Dále k **určení stroje** M patří pevný konečný počet $i_M + 1$ ($i_M > 0$) tzv. symbolů pásky, jež označme jako $S_0, S_1, \ldots, S_{i_M}$; jsou to zpravidla číslice a pomocné (instrukční) symboly; na každém políčku pásky může být zapsán nejvýše jeden symbol.



Obr. 1.

Je však formálně výhodné prohlásit i prázdné políčko za „obsazené prázdným“ symbolem S_0; psáváme proto názorně $S_0 = \square$. Dále je teoreticky vhodné (srov. pozn. [2]) užít jen jednoho symbolu, řekněme S_1, k zapisování čísel; píšeme proto $S_1 = |$. Pak totiž často blok $m + 1$ za sebou na pásce zanesených čárek prostě pokládáme za záznam čísla m, jestliže je blok z obou stran oddělen prázdným políčkem.

Posloupnost $S_{i_1}, S_{i_2}, S_{i_3}, \ldots$ všech symbolů zanesených v daném okamžiku na pásce nazýváme *nápisem*; omezujeme se na fakticky konečné ale tzv. formálně neomezené nápisy, tj. $S_{i_l} = \square$ (tj. $i_l = 0$) pro všechna l dostatečně vysoká.

1.3. K určení stroje M konečně patří pevný konečný počet $j_M + 1$ ($j_M > 0$) tzv. jeho vnitřních stavů, tj. stavů konečného automatu $\mathscr{A}_M$, jež označme $q_0, q_1, \ldots, q_j, \ldots, q_{j_M}$.

1.4. Vlastní práce stroje M je pak složena z kroků, z nichž každý je uskutečněním těchto činností:

Automat $\mathscr{A}_M$ ve svém stavu q_j (= j-tý vnitřní stav stroje) „přečte“ (z políčka, nad nímž právě je jeho hlava) symbol S_i (může ovšem být také $i = 0$, tj. $S_i = \square$ – políčko je prázdné). Pak pod výlučným určujícím vlivem uspořádané dvojice q_j, S_i:

a) automat $\mathscr{A}_M$ přejde do nového (vnitřního) stavu q_{j^*} (nevylučuje se $q_j = q_{j^*}$, tj. $j = j^*$ – vnitřní stav stroje se nemění);

b) zároveň automat $\mathscr{A}_M$ „přepíše“ (pomocí své hlavy) na právě sejmutém políčku symbol S_i v nový symbol S_{i^*} (opět se nevylučuje $i = i^*$, tj. $S_i = S_{i^*}$; rozumí se, že v případě $i^* = 0$ se symbol S_i „vymaže“);

c) nato $\mathscr{A}_M$ posune svoji hlavu do nové polohy, a to nejvýše o jedno políčko pásky, tj. buďto zůstane stát, anebo se posune nad sousední pravé políčko, anebo nad sousední levé políčko, pokud je to možné; když by však hlava byla nad prvým políčkem pásky, pak automat $\mathscr{A}_M$ vykoná „vysunutí pásky ze zásobníku“ doprava o jedno políčko, namísto v tomto případě neproveditelného posuvu hlavy doleva (která tedy bude opět nad prvním políčkem pásky). Je běžné (a pro některé účely formálně výhodné a přitom to neomezuje schopnosti Turingových strojů) vyloučit kroky, při nichž by docházelo jak k faktickému přepsání čteného symbolu (tj. $S_i \neq S_{i*}$) tak i k vysunutí pásky. Tento zjednodušující předpoklad budeme v dalším činit všude.

Provedením popsaného kroku přechází stroj M ze svého tzv. celkového stavu, tj. z posloupnosti $\alpha = \{q_j, k, S_{i_1}, S_{i_2}, \ldots\}$, do svého následujícího celkového stavu

$$\alpha^* = \{q_{j^*}, k^*, S_{i_1*}, S_{i_2*}, \ldots\}, \quad \text{kde} \quad q_j; k; S_{i_1}, S_{i_2}, \ldots$$

po řadě jsou: daný vnitřní stav; daná poloha hlavy; daný nápis, tj. S_{i_n} je symbol na n-tém políčku a hlava čte právě symbol S_{i_k}; obdobně je tomu pro následující vnitřní stav q_{j^*}, následující polohu hlavy k^* (kde $|k - k^*| \leqq 1$) a pro následující nápis $S_{i_1*}, S_{i_2*}, \ldots$ Stav α^* je tedy ve smyslu sub a), b), c) jednoznačně určen stavem α, tj. lze psát $\alpha^* = \Phi_M(\alpha)$, kde Φ_M je tzv. pracovní funkce stroje M, tj. jisté zobrazení množiny všech celkových stavů stroje M do sebe.

Jestliže stroj M byl spuštěn v celkovém svém stavu α, pak v t-tém taktu práce dosáhne celkového stavu $\beta = \Psi_M(t, \alpha)$, kde Ψ_M je tzv. (časová) iterace pracovní funkce stroje M, tj. je to jisté zobrazení množiny jistých uspořádaných dvojic („čas t“, v čase t dosažený celkový stav α) do množiny celkových stavů, dané touto rekurencí:

$$\Psi_M(0, \alpha) = \alpha, \quad \Psi_M(t + 1, \alpha) = \Phi_M(\Psi_M(t, \alpha)).$$

1.5. Explicitní definice pracovní funkce Turingova stroje instrukcemi. Abychom ve smyslu 1.4 definovali pracovní funkci Φ_M stroje M matematicky explicitně, uvažme, že pracovní kroky stroje M jsou sub a), b), c) vlastně udány trojicí funkcí J_M, I_M, π_M, definovaných vesměs na konečném oboru všech uspořádaných dvojic (j, i), kde $j = 0, \ldots, j_M$; $i = 0, \ldots, i_M$, a to takto: $j^* = J_M(j, i_k)$ je index nového vnitřního stavu, $i_k^* = I_M(j, i_k)$ je index nově zapsaného symbolu na právě přečteném k-tém políčku $(k > 0)$, pokud nedojde k vysunutí pásky; v tomto výjimečném případě je ovšem $i_1^* = 0$ a $i_k^* = i_{k-1}$ pro $k > 1$; a konečně $\pi_M(j, i_k) = 0; 1; 2$ znamená po řadě: setrvání hlavy na starém místě; posuv o políčko doprava; posuv o políčko doleva (pokud je možný) a jinak vysunutí pásky. Konečně je, jak se snadno přesvědčíme,

$$k^* = (k + \pi_M(j, i_k)) \dot{-} 3[\pi_M(j, i_k)/2]\ ^{4})$$

pokud je $k \neq 1$, nebo $\pi_M(j, i_1) \neq 2$; jestliže naopak je výjimečně $k = 1$, $\pi_M(j, i_1) = 2$ (tj. dojde k vysunutí pásky), pak je $k = k^* = 1$ jako nová poloha hlavy, podle 1.4 sub c).

Každou trojici hodnot funkcí

$$J_M(j, i), \quad I_M(j, i), \quad \pi_M(j, i)$$

pro danou hodnotu argumentu (j, i) nazveme instrukcí; speciálně

$$J_M(j, i) = j, \quad I_M(j, i) = i, \quad \pi_M(j, i) = 0$$

je tzv. identická instrukce; právě a jen taková patrně vede k faktickému zastavení stroje $(\alpha = \alpha^* = \Phi_M(\alpha))$. Celou trojici funkcí J_M, I_M, π_M nazveme souhrnem instrukcí, či

---

[4]) $x \dot{-} y = x - y$ pro $x \geqq y$; jinak $x \dot{-} y = 0$; $[x/y]$ pro $y \neq 0$ je celá část z x/y.

prostě programem daného Turingova stroje M; je třeba v tomto smyslu Turingův stroj pokládat za stroj jednoúčelový (s pevným programem, zabudovaným v konstrukci stroje samého). V odst. 2.5 uvedeme, v jakém smyslu lze jistého Turingova stroje užít jako universálního počítače.

1.6. Pojem algoritmického řešení hromadné matematické úlohy, ať jde o počítání čistě numerické anebo o počítání čistě symbolické anebo o početní proces smíšený z obou, je každému matematikovi intuitivně dobře znám.

Až dosud se nenašel příklad matematického resp. matematicko-logického algoritmického řešení hromadné úlohy, které by se nedalo při vhodné formulaci provést na nějakém Turingově stroji. Možno tedy přijmout předpoklad (hypotezu), že hromadná úloha je zásadně algoritmicky řešitelná tehdy a jen tehdy, dá-li se řešit na nějakém Turingově stroji.

Tato hypoteza nese po svém objeviteli název Turingova teze. Není to matematická poučka, ani axiom, nýbrž výraz přesvědčení, že intuitivní, ale nematematický pojem algoritmického řešení je vskutku pojmem řešení na Turingově stroji (matematicky přesně) vystižen.

1.7. Vyčíslování funkce na Turingově stroji. Nebudeme se však blíže zabývat precizací obecného pojmu řešení hromadné úlohy na Turingově stroji a obrátíme se k speciálnímu užití Turingova stroje k výpočtu numerické hodnoty $y = f(x_1, \ldots, x_n)$ funkce f pro numerickou n-tici hodnot $x_1, \ldots, x_n$, přičemž zásadně připouštíme funkce, které nejsou definovány všude.

Definice 1. Řekneme, že funkce f je vyčíslitelná na Turingově stroji M, jestliže platí: Nechť $\alpha_{x_1,\ldots,x_n} = \{q_0, 1, \underbrace{|\ldots|}_{x_1+1} \square \underbrace{|\ldots|}_{x_2+1} \square \ldots \square \underbrace{|\ldots|}_{x_n+1} \square\, \square \ldots\}$ je počáteční celkový stav stroje M vzájemně jednoznačně odpovídající numericky zadané n-tici čísel $x_1, x_2, \ldots, x_n$. Pak funkce f je pro argumenty $x_1, x_2, \ldots, x_n$ definována a nabývá hodnoty $y = f(x_1, x_2, \ldots, x_n)$ tehdy a jen tehdy, když existuje takt t práce stroje M takový, že je

a) $\Psi_M(t + 1, \alpha_{x_1,\ldots,x_n}) = \Psi_M(t, \alpha_{x_1,\ldots,x_n}) = \beta$, tj. stroj M se fakticky zastaví v (celkovém) stavu β, byv spuštěn ve stavu $\alpha_{x_1,\ldots,x_n}$,

b) celkový počet čárek zanesený na pásce ve stavu β je právě číslo $y = f(x_1, \ldots, x_n)$.[5])

(Tedy stroj M se nezastaví nikdy, je-li spuštěn ve stavu $\alpha_{x_1,\ldots,x_2}$ takovém, že funkce f pro hodnoty $x_1, \ldots, x_n$ není definována.)

Ve shodě s Turingovou tezí až dosud všechny známé celočíselné funkce celistvých argumentů, pro něž je udán nějaký efektivní vyčíslovací proces (vedoucí k hodnotě funkce tehdy a jen tehdy, když je definována), se ukázaly být vyčíslitelné na vhodném Turingově stroji.

[5]) Zřejmě je $y \leqq t$. Pro účely případného dalšího zpracování hodnot y bylo by třeba na Turingově stroji zvláštními symboly ohraničit záznam čísla y na pásce.

V následující druhé (a hlavní) části tohoto článku podáme stručné odvození známého uniformního Kleeneho vyjádření všech strojově vyčíslitelných funkcí daného počtu argumentů. Viz věta B.

2. NORMÁLNÍ KLEENEHO FORMA STROJOVĚ VYČÍSLITELNÝCH FUNKCÍ A UNIVERSÁLNÍ TURINGŮV POČÍTAČ

2.1. Třída primitivně rekursivních funkcí. Připomeňme nejprve definici třídy primitivně rekursivních funkcí. Je to nejmenší třída funkcí všude definovaných, která splňuje tyto požadavky:

1. patří do ní sčítání a násobení (jako dvouargumentové funkce);

2. patří do ní všechny konstantní funkce a všechny tzv. diagonální funkce, tj. funkce mající za hodnotu určitý ze svých argumentů (speciálně identická funkce);

3. je uzavřena vůči operaci superpozice (tvoření složené funkce);

4. je uzavřena vůči operaci tzv. primitivní rekurence, tj.: jestliže do této třídy patří $n + 2$-argumentová funkce h a n-argumentová funkce g, pak do této třídy patří i $n + 1$-argumentová funkce f, splňující rekursivní identity

$$f(0, x_1, \ldots, x_n) = g(x_1, \ldots, x_n)\,,$$
$$f(x + 1, x_1, \ldots, x_n) = h(x, f(x, x_1, \ldots, x_n), x_1, \ldots, x_n)\,.$$

Primitivně rekursivními jsou všechny běžné číselně teoretické funkce (některých budeme užívat aniž bychom to o nich dokazovali). Jsou to především: funkce f, kde $f(n) = p_n$ je podle velikosti n-té prvočíslo ($p_0 = 2$, $p_1 = 3, \ldots$), dále funkce exp, kde píšeme $\exp(i, n) = \exp_i(n)$, což je exponent i-tého prvočísla v rozkladu čísla $n \neq 0$ na součin mocnin prvočísel (pozor: $\exp_i(n) = 0$ se nevylučuje). Dále jsou to funkce běžným způsobem z těchto sestrojené, anebo takové, jejichž primitivní rekursivnost je dostatečně zřejmá.

2.2. Vzájemně jednoznačné očíslování uspořádaných číselných dvojic. Z mnoha způsobů jak primitivně rekursivně vzájemně jednoznačně očíslovat uspořádané dvojice (u, v) přirozených čísel (mezi něž důsledně počítáme nulu) užijeme známého uspořádání uspořádaných dvojic podle stoupajícího součtu $u + v$ a v případě stejných součtů podle rostoucího prvního sčítance. Pak je pořadové číslo r (včetně $r = 0$) uspořádané dvojice (u, v) dáno funkcí μ, kde

$$\mu(u, v) = r = (0 + 1 + \ldots + (u + v)) + u =$$
$$= [(u + v)(u + v + 1)/2] + u\,.$$

Obráceně, každé číslo r je takto pořadovým číslem určité uspořádané dvojice (u, v) a to, položíme-li

$$\nu(r) = \max_n ([n(n + 1)/2] \leqq r)\,,$$

potom je patrně

$$u = \kappa(r) = r - \nu(r)\,, \quad v = \lambda(r) = 2\nu(r) - r\,.$$

Ježto zřejmě je

$$\nu(r) = \sum_{k=0}^{r} \operatorname{sg}(r \dot{-} [k(k+1)/2])$$

(kde $\operatorname{sg}(x) = 1$ pro $x > 0$, $\operatorname{sg}(0) = 0$ udává patrně primitivně rekursivní funkci sg), je i funkce ν a tím i funkce κ a funkce λ primitivně rekursivní. Platí ovšem $r = \mu(\kappa(r), \lambda(r))$ identicky. Krom toho se snadno lze přesvědčit, že funkce η roste v prvním argumentu (když $u_1 < u_2$ pak $\mu(u_1, v) < \mu(u_2, v)$ pro každé v).

2.3. Aritmetizace pracovní funkce Turingova počítače a její iterace. Půjde nyní o to očíslovat vzájemně jednoznačně celkové stavy $\alpha, \beta, \ldots$ daného Turingova stroje čísly $|\alpha|, |\beta|, \ldots$ a udat primitivně rekursivní jednoargumentovou funkci φ_M tak, aby platilo $|\beta| = \varphi_M(|\alpha|)$ tehdy a jen tehdy když $\beta = \Phi_M(\alpha)$ (pro jakékoli celkové stavy α, β daného stroje M). Je-li tedy $\alpha = \{q_j, k, S_{i_1}, S_{i_2}, \ldots\}$ $(k > 0)$ celkový stav stroje, nejprve položme

$$|\alpha| = 2^{\mu(j,k-1)} 3^{i_1} 5^{i_2} \ldots p_m^{i_m}\,,$$

kde číslo $m = m_\alpha$ je jednoznačně určeno stavem α, jako první takové číslo $m \geqq k$, že platí $i_n = 0$ pro každé $n > m$. Číslo $|\alpha|$ je možno podle běžné terminologie nazvat Gödelovým číslem celkového stavu α (stroje M). Je zřejmé, že toto číslo je určeno jednoznačně pro každý celkový stav, a navíc je i stanoven (číslem m_α) jednoznačně určitý jeho (normovaný) zápis jako součin mocnin prvočísel; přitom z triviálních mocnin prvočísel s nulovým exponentem (které se běžně vynechávají a jejichž připouštění bez dalšího stanovení by činilo konečný zápis čísla jako součinu mocnin prvočísel nekonečně mnohoznačným) píšeme přesně ty, které umožňují zachytit vnitřní stav a polohu hlavy — a potřebnou konečnou část pásky (s příslušnými symboly resp. prázdnými políčky). Stejně tak patrně i obráceně, každé kladné číslo u lze jednoznačně považovat v tomto smyslu za číslo určitého celkového stavu jistého (nikoli jediného) Turingova stroje; přitom číslo m (určující ve shora uvedeném smyslu zápis rozkladu čísla u v součin mocnin prvočísel) je dáno pomocí čísla

$$k = \lambda(\exp_0(u)) + 1\,.$$

Úmluva. Zaveďme ještě tyto dvě primitivně rekursivní funkce, využívajíce 1.5 shora:

$$J(u) = \kappa(\exp_0(u))\,, \quad K(u) = \lambda(\exp_0(u)) + 1\,.$$

Dále položme

$$\tilde{J}_M(u) = J_M(J(u), \exp_{K(u)}(u))\,, \quad \tilde{I}_M(u) = I_M(J(u), \exp_{K(u)}(u))\,,$$

$$\tilde{K}_M(u) = K(u) + \pi_M(J(u), \exp_{K(u)}(u) \dot{-} 3[\pi_M(J(u), \exp_{K(u)}(u))/2]$$

pro $u > 0$, jestliže $u = (\alpha)$ je Gödelovo číslo celkového stavu α stroje M.

Lemma 1. *Budiž M daný Turingův stroj s instrukcemi danými uspořádanou trojicí funkcí J_M, I_M, π_M podle 1.5 shora. Pišme $\overline{\mathrm{sg}}\,(x) = 1 \dot{-} \mathrm{sg}\,(x)$. Položme*

$$(*) \qquad \varphi_M(u) = [u/2^{\exp_0(u)}\, p_{K(u)}^{\exp_{K(u)}(u)}]\, 2^{\mu(\tilde{J}_M(u), \tilde{K}_M(u) \dot{-} 1)}\, p_{K(u)}^{\tilde{I}_M(u)}\, \mathrm{sg}\,(\tilde{K}_M(u)) +$$
$$+ \overline{\mathrm{sg}}\,(\tilde{K}_M(u))\, 2^{\mu(\tilde{J}_M(u), 0)} \prod_{n=0}^{u} p_{n+1}^{\exp_n(u)} .$$

Pak funkce φ_M je definována (alespoň) pro všechna Gödelova čísla celkových stavů stroje M a rovnost $\Phi_M(\alpha) = \beta$ platí pro dva celkové stavy Turingova stroje M tehdy a jen tehdy, když je $\varphi_M(|\alpha|) = |\beta|$.

Poznámka. Funkce φ_M, tzv. aritmetická pracovní funkce stroje M, by se stala (jak lze snadno ukázat) primitivně rekursivní, kdybychom ji vhodně rozšířili i na ta čísla u, která nejsou Gödelovými čísly celkových stavů stroje M (to jsou vedle nuly přesně ta u pro něž neplatí $\kappa(\exp_0(u)) \leqq j_M$, $\exp_i(u) \leqq i_M$ (pro $i = 1, 2, 3, \ldots$). Stačilo by prostě dodefinovat $\varphi_M(u) = 0$ pro tato čísla. Srov. níže, ve větě B.

Důkaz. (I) Budiž předně

$$\Phi_M(\alpha) = \beta\,, \quad \text{tj.} \quad \alpha^* = \beta = \{q_{j^*}, k^*, S_{i_1^*}, S_{i_2^*}, \ldots\}\,,$$
$$\alpha = \{q_j, k, S_{i_1}, S_{i_2}, \ldots\}\,.$$

Pak sestrojení čísel $j^*, k^*; i_1^*, i_2^*, \ldots$ jako čísel určených čísly j, k, i_k podle 1.4 a 1.5 a sestrojení příslušných Gödelových čísel $|\alpha|, |\alpha^*|$ celkových stavů α, α^* (za pomoci 2.2 a 2.3) přímo ukáže, že je vskutku $\varphi_M(|\alpha|) = |\alpha^*|$.

(II) Buďtež obráceně $u = |\alpha|$, $v = |\beta|$ dvě Gödelova čísla celkových stavů α, β stroje M a nechť $\varphi_M(u) = v$; pak

$$\kappa(\exp_0(u)) \leqq j_M\,, \quad \exp_n(u) \leqq i_M \quad (\text{pro } n = 1, 2, \ldots)$$

a podobně pro v namístě u.

Tedy $\alpha = \{q_j, k, S_{i_1}, S_{i_2}, \ldots\}$, kde $j = y(|\alpha|)$, $0 < k = K(|\alpha|)$, $i_n = \exp_n(|\alpha|)$ pro $n = 1, 2, \ldots$; podobně pro β namístě α.

Snadno se lze přesvědčit, že ve smyslu 1.4, 1.5 a 2.3 vskutku platí

$$\beta = \alpha^* = \{q_{j^*}, k^*, S_{i_1^*}, S_{i_2^*}, \ldots\}\,.$$

Jestliže totiž je $\tilde{K}_M(|\alpha|) > 0$, pak podle (*) je

$$y(v) = \tilde{y}_M(|\alpha|) = j^*\,, \quad K(v) = \tilde{K}_M(|\alpha|) = k^*\,,$$
$$i_n^* = i_n \quad \text{pro} \quad n \neq k = K(|\alpha|) \quad \text{a} \quad i_k^* = \tilde{I}_M(|\alpha|)\,.$$

Jestliže naopak $K_M(|\alpha|) = 0$, pak podle (*) je opět

$$y(v) = \tilde{y}_M(|\alpha|) = j^*$$

a přitom $k^* = 1 = k$, $i_1^* = 0$ a $i_{n-s}^* = i_n$ pro $n = 2, 3, \ldots$

Je tedy vždy $\varphi_M(|\alpha|)$ vskutku Gödelovým číslem celkového stavu α^* bezprostředně následujícího ze stavu α.

2.4. Tvar funkce vyčíslitelné na Turingově stroji. Nejprve uveďme tato lemmata:

Lemma 2. *Funkce σ daná rovností $\sigma(x_1, \ldots, x_n) = |\alpha_{x_1,\ldots,x_n}|$ je primitivně rekursivní.*

Důkaz. Jest

$$|\alpha_{x_1,\ldots,x_n}| = 3 \,.\, 5 \ldots p_{x_1+1} \cdot p_{x_1+3} \cdots p_{x_1+x_2+3} \cdot p_{x_1+x_2+5} \cdots p_{x_1+x_2+x_3+5} \cdot$$

$$\cdot\, p_{x_1+x_2+x_3+7} \cdots p_{x_1+x_2+x_3+x_4+7} \ldots p_{x_1+x_2+\ldots+x_{n-1}+2n-1} \ldots p_{x_1+x_2+\ldots+x_{n-1}+x_n+2n-1}$$

ve smyslu definice 1. Položme tedy

$$\varrho(k, x_1, \ldots, x_n) = \left(\sum_{s=1}^{k} x_s\right) + 2k$$

pro $1 \leqq k \leqq n$ (pro $k > n$ a $k = 0$ může být hodnota funkce ϱ dána libovolně, např. $= 0$). Snadno nahlédneme, že ϱ je primitivně rekursivní funkce. Potom lze psát

$$|\alpha_{x_1,\ldots,x_n}| = \left[\prod_{r=1}^{x_1+\ldots+x_n+2n} p_r \Big/ \prod_{k=1}^{n} p_{\varrho(k,x_1,\ldots,x_n)}\right],$$

z čehož je primitivní rekursivnost funkce σ zřejmá.

Lemma 3. *Položme*

$$\psi_M(0, x_1, \ldots, x_n) = |\alpha_{x_1,\ldots,x_n}|\,, \quad \psi_M(t + 1, x_1, \ldots, x_n) = \varphi_M(\psi_M(t, x_1, \ldots, x_n))\,.$$

Pak ψ_M je primitivně rekursivní funkce a platí $\psi_M(t, x_1, \ldots, x_n) = w$ tehdy a jen tehdy, když

$$\psi_M(t, \alpha_{x_1,\ldots,x_n}) = \beta \quad \text{a} \quad |\beta| = w\,.$$

Důkaz je zřejmý z lemmat 1 a 2, jakož i z definice funkce Ψ_M v 1.4.

Lemma 4. *Je-li β (celkový) stav libovolného Turingova stroje, pak označme na chvíli jako $\langle\beta\rangle$ celkový počet čárek na pásce za stavu β. Pro libovolné $v > 0$ položme*

$$\eta(v) = \sum_{k=1}^{v} \overline{\mathrm{sg}}\,(|\exp_k(v) - 1|)$$

a dodejme pro formální úplnost, že $\eta(0) = 0$. Pak η je primitivně rekursivní funkce a platí $\langle\beta\rangle = \eta(|\beta|)$.

Důkaz je podle 2.3 zřejmý, uvážíme-li, že je-li

$$\beta = \{q_j, k, S_{i_1}, S_{i_2}, \ldots\}\,, \quad \text{pak} \quad S_{i_n} = |$$

čili $i_n = 1$ tehdy a jen tehdy, když $\exp_n(|\beta|) = 1$ (pro $n = 1, 2, \ldots$).

Věta A. *Nechť f je n-argumentová funkce vyčíslitelná na Turingově stroji M. Potom platí rovnost*

$$(A)\qquad f(x_1, \ldots, x_n) = \eta(\psi_M(\min_t(|\psi_M(t+1, x_1, \ldots, x_n) - \psi_M(t, x_1, \ldots, x_n)| = \\ = 0), x_1, \ldots, x_n))$$

a to vždy, když f je pro $x_1, \ldots, x_n$ definována; když f není pro $x_1, \ldots, x_n$ definována, pak nemá smysl ani pravá strana rovnosti (A).

Tj. slovy a poněkud méně určitě: Každá strojově vyčíslitelná funkce se dá složit ze dvou primitivně rekursivních funkcí superpozicí pomocí jednoho užití operace minima.

D ů k a z je zřejmý z lemmat 1, 2, 3, 4 podle definice 1; stačí si uvědomit, že operace $\min_t(\ldots = 0)$ užitá na pravé straně rovnosti (A) má vskutku smysl tehdy a jen tehdy, když funkce f je definována.

Jde nyní o to vyvodit z téměř triviální věty (A) Kleeneho universální normální formu vyčíslitelné funkce. (Toto je také jediný náš krok, který není zcela nasnadě a který není obvyklý.) K tomu cíli uvedeme tuto definici:

Definice 2. a) Je-li Turingův stroj M po celkovém počtu t taktů své práce v (celkovém) svém stavu β, pak uspořádanou dvojici (t, β) nazveme jeho (okamžitým) časovým stavem. Je tedy časový stav stroje údajem, sestávajícím jednak z (celkového) stavu, v němž se právě stroj nachází, jednak z doby, po kterou je „spuštěn".

b) Je přirozené očíslovat vzájemně jednoznačně časové stavy (t, β) čísly $|(t, \beta)| = s$ tak, že ve smyslu 2.2 položíme $|(t, \beta)| = \mu(t, |\beta|)$; pak obráceně, je-li s číslem časového stavu stroje M, udává $\lambda(s) = |\beta|$ stav, v němž se právě M nachází, a $\kappa(s) = t$ počet taktů, po který stroj „běží". Přesně řečeno, vlastnost čísla s „býti číslem časového stavu stroje M" znamená totéž, co splnění obou rovností

$$\beta = \Psi_M((\kappa(s), \alpha)\,, \quad |\beta| = \lambda(s)$$

při vhodném celkovém výchozím stavu α stroje M.

Zřejmě k jednomu a témuž celkovému stavu β může příslušet v uvedeném smyslu mnoho časových stavů s. Zvláště, je-li β koncový stav stroje, pak každý s, kde $\lambda(s) = |\beta|$ a $\kappa(s)$ je dostatečně veliké — přísluší k β.

Věta B⁺. *Budiž f n-argumentová funkce vyčíslitelná na Turingově stroji M. Položme ve smyslu lemmat* 1, 3 *a* 4

$$\xi_M(s, x_1, \ldots, x_n) = |\lambda(s) - \varphi_M(\lambda(s))| + |\lambda(s) - \psi_M(\kappa(s), x_1, \ldots, x_n)|\,,$$
$$U(u) = \eta(\lambda(u)) \quad \textit{pro libovolná} \quad s, x_1, \ldots, x_n, u\,.$$

Potom platí rovnost

$$(B^+)\qquad f(x_1, \ldots, x_n) = U(\min_s(\xi_M(s, x_1, \ldots, x_n) = 0))$$

a to vždy, když funkce f je pro čísla $x_1, \ldots, x_n$ definována; není-li tomu tak, ani pravá strana rovnosti (B^+) *není definována. Funkce U a ξ_M jsou primitivně rekursivní.*

Důkaz. Primitivní rekursivnost funkcí U a ξ_M je zřejmá. Podle definice je $\xi_M(s, x_1, \ldots, x_n) = 0$ tehdy a jen tehdy, když jednak platí $\lambda(s) = \varphi_M(\lambda(s))$ a jednak platí $\lambda(s) = \psi_M(\kappa(s), x_1, \ldots, x_n)$.

Druhá rovnost však znamená podle lemmatu 3 a definice 2, že s je číslem časového stavu stroje příslušným k celkovému stavu β (o Gödelově čísle $|\beta| = \lambda(s)$), do něhož se stroj M dostává po $\kappa(s)$ taktech, jestliže byl spuštěn ve stavu $\alpha_{x_1, \ldots, x_n}$ (ve smyslu definice 1 a lemmatu 2). První rovnost pak znamená, že stroj se v celkovém stavu β (o čísle $|\beta| = \lambda(s)$) zastaví, tj. tento stav se dále jen opakuje.

Podle 2.2 se číslo $s = \mu(t, |\beta|)$ zvětší, když se zvětší číslo $t = \kappa(s)$. Tedy číslo

$$\bar{s} = \min_s (\xi_M(s, x_1, \ldots, x_n) = 0)$$

je právě takové, že $\bar{t} = \kappa(\bar{s})$ je onen nejmenší počet taktů, po němž dojde k zastavení stroje, spuštěného ve stavu $\alpha_{x_1, \ldots, x_n}$; čili je

$$\kappa(\bar{s}) = \min_t (|\psi_M(t + 1, x_1, \ldots, x_n) - \psi_M(t, x_1, \ldots, x_n)| = 0)\,.$$

Ježto $\psi_M(\kappa(\bar{s}), x_1, \ldots, x_n) = \lambda(\bar{s})$, je podle definice 1, rovnosti (A) a lemmatu 4 shora číslo $U(\bar{s}) = \eta(\lambda(\bar{s}))$ vskutku hodnotou funkce f pro dané hodnoty argumentů $x_1, \ldots, x_n$, tj. platí (B^+).

Obráceně je vidět, že číslo $\min_s (\xi_M(s, x_1, \ldots, x_n) = 0)$ neexistuje právě tehdy, když by se stroj nikdy nezastavil, byv spuštěn ve stavu $\alpha_{x_1, \ldots, x_n}$. Tím je věta B^+ (a tedy v podstatě již i Kleeneho normální forma) odvozena; zbývá jen nahradit závislost definice funkce ξ_M na volbě Turingova počítače M primitivně rekursivní závislostí na vhodném číselném parametru z; přesněji řečeno, zbývá nalézt primitivně rekursivní $(n + 2)$-argumentovou funkci τ a takové očíslování Turingových strojů (resp. jejich programů) M čísly z_M, aby platilo

$$\tau(z_M, s, x_1, \ldots, x_n) = \xi_M(s, x_1, \ldots, x_n)$$

pro všechna $s, x_1, \ldots, x_n$ a pro všechna M.

K tomuto cíli proveďme jistou vhodnou a formálně zjednodušující modifikaci každého ze strojů M:

Je-li totiž $\mu(j_M, i_M) = r_M$, pak se může stát, že některé uspořádané dvojice (j, i) neudávají vnitřní stav stroje M a číslo některého ze symbolů jeho pásky, ačkoli je $\mu(j, i) \leqq r_M$ (tj. stává se, že je $j > j_M$ nebo $i > i_M$ a přitom $\mu(j, i) \leqq \mu(j_M, i_M)$). Je proto vhodné formálně modifikovat stroj M ve stroji M^* tím, že:

a) připojíme tolik vnitřních stavů (o číslech j, kde $j_M < j \leqq j_{M^*}$) a tolik nových symbolů pásky (o číslech i, kde $i_M < i \leqq i_{M^*}$), aby bylo splněno $\mu(j, i) \leqq \mu(j_M, i_M)$;

b) přitom každá nová instrukce (pro přidaný vnitřní stav, nebo pro přidaný symbol) je identická (zatímco staré instrukce stroje M platí i pro stroj M^*).

Snadno nahlédneme, že nový stroj M^* bude vyčíslovat funkci f vyčíslitelnou na stroji M přesně stejným způsobem jako daný stroj M; přitom M^* jistě neupotřebí více instrukcí, nežli jsou ony udané dvojicemi (j, i) o číslech $\mu(j, i) = 0, 1, \ldots, r_M$, takže můžeme na tato čísla dvojic omezit argumenty nových funkcí J_M^*, I_M^*, π_M^*.

Nyní již můžeme potřebnou část programu stroje M^*, tj. trojici funkcí J_M^*, I_M^*, π_M^* (s právě udaným omezením argumentů na dvojice (j, i) o číslech $0, 1, \ldots, r_M$) pohodlně zaznamenat jediným číslem z_M takto:

Položme pro $r = 0, 1, \ldots, r_M$ nejprve

$$\omega_M(r) = 2^{J_M*(\kappa(r),\lambda(r))+1} \cdot 3^{J_M*(\kappa(r),\lambda(r))+1} \cdot 5^{\pi_M*(\kappa(r),\lambda(r))+1}$$

jako číslo r-té instrukce, tj. číslo uspořádané trojice hodnot funkcí J_M^*, I_M^*, π_M^* pro r-tou hodnotu jejich společného argumentu – číselnou dvojici $(\kappa(r), \lambda(r)) = (j, i)$.

Pak definujme

$$z_M = 2^{\omega_M(0)}\ 3^{\omega_M(1)}\ 5^{\omega_M(2)} \ldots p_{r_M}^{\omega_M(r_M)} = \prod_{l=0}^{r_M} p_l^{\omega_M(l)}$$

jako tzv. Gödelovo číslo Turingova stroje M.

Nechť obráceně je dáno číslo $z = z_M$ nějakého Turingova stroje M. Pak toto číslo má následující vlastnosti:

(1) když $\exp_s(z) > 0$ a $s^* < s$, pak $\exp_{s^*}(z) > 0$,

(2) označíme-li jako $d(z)$ délku prvočíselného rozkladu čísla čili počet prvočíselných dělitelů čísla z, pak pro $r = 0, 1, \ldots, d(z_M) - 1$, platí $1 \leqq \exp_0(\exp_r(z_M))$, $1 \leqq \exp_1(\exp_r(z_M))$, $1 \leqq \exp_2(\exp_r(z_M)) \leqq 3$, $\exp_v(\exp_r(z_M) = 0$ když $v > 2$. Pak můžeme psát pro všechny uspořádané dvojice (j, i), kde $\mu(j, i) \leqq r_M = \mu(j_M, i_M)$:

$J_M^*(j, i) = \exp_0(\exp_{\mu(j,i)}(z_M)) - 1\,,\quad I_M^*(j, i) = \exp_1(\exp_{\mu(j,i)}(z_M)) - 1\,,$

$\pi_M^*(j, i) = \exp_2(\exp_{\mu(j,i)}(z_M)) - 1\,.$

Položme tedy

$J(z, j, i) = \exp_0(\exp_{\mu(j,i)}(z)) - 1\,,\quad I(z, j, i) = \exp_1(\exp_{\mu(j,i)}(z)) - 1\,,$

$\pi(z, j, i) = \exp_2(\exp_{\mu(j,i)}(z)) - 1\,,$

jestliže číslo z splňuje podmínky (1) a (2) shora a přitom pro j, i je $\mu(j, i) < d(z)$; pro ostatní uspořádané trojice (z, j, i) můžeme funkce J, I, π definovat třebas nulovou hodnotou.

Snadno pak nahlédneme, že funkce J, I, π jsou primitivně rekursivní a že platí

$$J(z_M, j, i) = J_M(j, i)\,,\quad I(z_M, j, i) = I_M(j, i)\,,\quad \pi(z_M, j, i) = \pi_M(j, i)$$

pro všechny uspořádané dvojice (j, i), kde $0 \leqq j \leqq j_M$, $0 \leqq i \leqq i_M$ a pro libovolný Turingův stroj M.

Nahraďme konečně v úmluvě před lemmatem 1 důsledně funkční znaky $J_M(.,.)$; $I_M(.,.)$, $\pi_M(.,.)$ po řadě odpovídajícími funkčními znaky $J(z,.,.)$, $I(z,.,.)$, $\pi(z,.,.)$ a přepišme v tomto smyslu i definiční rovnost (*) v lemmatu 1. (Explicitní vypsání takto obdržené rovnosti si můžeme ušetřit; je tvaru $\varphi(z, u) = \ldots$, kde pravá strana vypadá formálně úplně stejně jako pravá strana rovnosti (*), až na to, že jen index M u symbolů pomocných funkcí $\tilde{J}_M$, $\tilde{I}_M$, $\tilde{\pi}_M$ bychom přepsali v dodatečný argument z, kladený na prvé místo za příslušné funkční znaky $\tilde{J}$, $\tilde{I}$, $\tilde{\pi}$.)

Tím jsme definovali primitivně rekursivní funkci φ o dvojici argumentů (z, u) takovou, že platí $\varphi(z_M, u) = \varphi_M(u)$ pro každé u a každé M.

Přepišme dále v právě uvedeném smyslu důsledně i primitivní rekurenci z lemmatu 3. Obdržíme tak $(n + 2)$-argumentovou funkci ψ (primitivně rekursivní) splňující identity

$$\psi(0, z, x_1, \ldots, x_n) = |\alpha_{x_1, \ldots, x_n}|,$$
$$\psi(t + 1, z, x_1, \ldots, x_n) = \varphi(z, \psi(t, z, x_1, \ldots, x_n)).$$

Zřejmě bude $\psi(t, z_M, x_1, \ldots, x_n) = \psi_M(t, x_1, \ldots, x_n)$

pro každé $t, x_1, \ldots, x_n$ a každé M. Konečně i definici funkce ξ_M ve větě B^+ přepišme stejným způsobem; obdržíme tak primitivně rekursivní funkci ξ, kde

$$\xi(z, s, x_1, \ldots, x_n) = |\lambda(s) - \varphi(z, \lambda(s)| + |\lambda(s) - \psi(\kappa(s), z, x_1, \ldots, x_n)|,$$

pro kterou platí

$$\xi(z_M, s, x_1, \ldots, x_n) = \xi_M(s, x_1, \ldots, x_n) \text{ pro všechna } s, x_1, \ldots, x_n \text{ a každé } M.$$

Tím je z věty B^+ odvozena základní

Věta B. (*O Kleeneho normální uniformizaci vyčíslitelných funkcí.*) *Primitivně rekursivní funkce o $n + 2$-argumentech ξ a jednoargumentová primitivně rekursivní funkce U z věty* B^+ *mají tuto vlastnost:*

Ke každé strojově vyčíslitelné funkci f o n argumentech existuje číslo z takové, že platí

$$f(x_1, \ldots, x_n) = U\left(\min_s \left(\xi(z, s, x_1, \ldots, x_n) = 0\right)\right)$$

a to pro všechny hodnoty $x_1, \ldots, x_n$, pro něž je funkce f definována; navíc funkce f je definována jen pro takové hodnoty $x_1, \ldots, x_n$, pro něž i pravá strana má smysl, tj. pro něž existuje číslo s takové, že $\xi(z, s, x_1, \ldots, x_n) = 0$.

Poznámka. Čtenář seznámený se základy teorie Turingových strojů si uvědomí, že přes naprostou formální shodu právě uvedené normální formy vyčíslitelné funkce a dobře známé Kleeneho formy má tato forma v našem odvození poněkud odlišnou interpretaci parametru s. Úlohu „důležitých" hodnot tohoto parametru běžně hraje tzv. číslo výpočtu (number of computation, viz M. Davis [1], str. 57, 58), tj. číslo celé konečné posloupnosti stavů, jimiž prošel uvažovaný Turingův stroj, než skončil výpočet; v naší interpretaci jsou to čísla časového stavu stroje ve smyslu definice 2 shora.

2.5. Universální Turingův stroj. Zbývá několika slovy připomenout hlavní smysl věty B (který je v běžné i v právě uvedené interpretaci stejný). Funkce ξ z věty B je definována pro všechny hodnoty $z, s, x_1, \ldots, x_n$, tj. i tehdy, když z není číslem Turingova stroje. Proto např. dvouargumentová funkce g udaná rovností

$$(^{**}) \qquad g(z, x) = U(\min_s (\xi(z, s, x_1, \ldots, x_n) = 0))$$

$$\text{kde } x_i = \exp_{i-1}(x) \ (i = 1, 2, \ldots, n_x),\ n_x = \max_m (\exp_m(x) > 0)\,,$$

je definována pro všechny hodnoty argumentů z, x takové, že existuje s, pro něž je $\xi(z, s, \exp_0, (x), \exp_1(x), \ldots, \exp_{n_x-1}(x)) = 0$.

Ze základů teorie Turingových strojů (viz M. Davis [1], str. 42) plyne, že funkce g sama patří mezi strojově vyčíslitelné funkce; existuje tedy Turingův stroj Mg, který vyčísluje hodnoty funkce g právě tam, kde funkce g je definována. Dokonce by bylo z uvedeného explicitního vyjádření funkce g možno sestavit pevný (ale dosti složitý) program stroje Mg. Stroj Mg je v tom smyslu universální, že zafixujeme-li hodnotu prvého argumentu číslem z_M (programu) Turingova stroje, vyčíslujícího libovolně předepsanou n-argumentovou funkci f, pak zřejmým způsobem pro hodnotu („kód" argumentu) $x = 2^{x_1}3^{x_2} \ldots p_{n-1}^{x_n}$ obdržíme hodnotu $f(x_1, \ldots, x_n) = g(z_M, x)$ funkce f všude, kde je tato vyčíslitelna strojem M. Jakoby tedy stroj Mg byl opatřen „programujícím programem", který po zanesení čísla z_M libovolného Turingova stroje M na pásku stroje Mg zařídí, že stroj Mg vykoná vyčíslovací práci daného stroje M (při uvedeném „kódu" x argumentu $(x_1, \ldots, x_n)$.

Na základě toho, co bylo právě řečeno, je již snadné ukázat prostý (a v podstatě dobře známý) příklad hromadné strojově neřešitelné úlohy. Je to tzv. úloha o zastavení daného Turingova stroje, které můžeme dát ve smyslu Turingovy teze význam úlohy o „konvergenci" daného algoritmu při daném zadání; tato úloha zní takto:

Jest rozhodnout (předpovědět), zda Turingův počítač M o Gödelově čísle z_M se zastaví či nezastaví, jestliže byl spuštěn v daném (celkovém) stavu α.

Proveďme jednoduchý důkaz algoritmické (strojové) neřešitelnosti této úlohy. Označme jako $\mathfrak{J}$ („irreflexivita") onu číselnou vlastnost, kterou mají právě a jen ta čísla z_M strojů M, jež se nezastaví byvše spuštěny právě ve stavu α_{z_M} (odpovídajícím ve smyslu definice 1 záznamu čísla samotného stroje M).

Pak tedy ve smyslu věty B platí pro vlastnost $\mathfrak{J}$ charakteristická nutná a postačující podmínka:

[*] *Číslo z má vlastnost $\mathfrak{J}$ tehdy a jen tehdy, když z je číslem nějakého Turingova stroje a když neexistuje číslo s (tj. číslo časového stavu) tak, že $\xi(z, s, z) = 0$.*

Nechť nyní, oproti tomu co máme dokázat, existuje Turingův stroj $\overline{M}$, který naši úlohu řeší. Můžeme bez újmy obecnosti předpokládat, že to činí následujícím způsobem: Stroj $\overline{M}$ byv spuštěn ve stavu α_{z_M} se vždy po konečném počtu kroků zastaví a to ve stavu $\{q_T, 1, S, \square, \square, \ldots\}$, kde $S = |$ anebo $S = \square$ podle toho, zda z_M má či nemá vlastnost $\mathfrak{J}$. (T je pevné číslo.)

Pozměňme poněkud stroj $\overline{M}$ ve stroj $\widetilde{M}$ takový, že namísto identické instrukce $J_{\overline{M}}(T, 0) = T$, $I_{\overline{M}}(T, 0) = 0 = \pi_{\overline{M}}(T, 0)$ vedoucí k fixaci celkového stavu $\{q_T, 1,$

$\square, \square, \square, \ldots\}$ stroje $\overline{M}$ dáme instrukci zaručující neustálý posuv hlavy doprava, tj. napsanou identickou instrukci nahradíme instrukcí

$$J_{\tilde{M}}(T, 0) = T, \quad I_{\tilde{M}}(T, 0) = 0, \quad \pi_{\tilde{M}}(T, 0) = 1$$

a ostatní instrukce ponecháme beze změny. Potom podle podané definice stroje $\tilde{M}$ bude platit (opět s ohledem na větu B):

[**] *Číslo z má vlastnost $\mathfrak{F}$ tehdy a jen tehdy, když z je číslem nějakého Turingova stroje a když existuje číslo $\bar{s}$ (časového stavu stroje $\tilde{M}$) takové, že $\xi(z_{\tilde{M}}, \bar{s}, z) = 0$.*

Dosadíme-li však v podmínce [**] za z právě číslo $z_{\tilde{M}}$, dostáváme se okamžitě do sporu s podmínkou [*], tj. dostáváme výsledek „$z_{\tilde{M}}$ má vlastnost $\mathfrak{F}$ tehdy a jen tehdy, když $z_{\tilde{M}}$ nemá vlastnost $\mathfrak{F}$“.

Proto stroj $\overline{M}$ řešící shora danou úlohu o zastavení nemůže existovat.

Logický obrat, jímž se dokázala neřešitelnost úlohy o zastavení, je známý tzv. diagonální postup; sama úloha má ovšem význam jen teoretický a důkaz její strojové neřešitelnosti je prostý. Obtížnost důkazů strojové neřešitelnosti matematicky významnějších úloh (jako např. problému ekvivalence slov v teorii grup nebo problému faktorizovatelnosti čtvercových regulárních celočíselných matic (viz P. S. Novikov [5] nebo A. I. Markov [2], [3]) spočívá ve složitosti a nenázornosti redukce takových úloh na právě uvedenou úlohu o zastavení.

Literatura

[1] *M. Davis*: Computability and Unsolvability. McGraw-Hill. New York 1958. (V této monografii je vybraná bibliografie, zejména prací západních odborníků.)

[2] *А. А. Марков:* Об одной неразрешимой проблеме, касающейся матриц. Dokl. A. N. SSSR, 1951, T. *78*, No 6, 1089–1092.

[3] *А. А. Марков:* Теория алгорифмов. Trudy mat. inst. V. A. Steklova, *XLII*, Moskva 1954. (V této monografii je representativní výběr bibliografických údajů do r. 1953.)

[4] *A. M. Turing*: On Computable Numbers, with an Application to the Entscheidungsproblem. Proc. Lond. Math. Soc. ser. 2, vol. *42*, pp. 230–265 (1963–1937); Correction, ibid. vol. *43*, pp. 544–546 (1937).

[5] *П. С. Новиков:* Об алгорифмической неразрешимости проблемы слов в теории групп. Trudy mat. inst. im V. A. Steklova, *XLIV*, Moskva 1955.

Резюме

О НОРМАЛЬНОЙ ФОРМЕ КЛИНИ ДЛЯ ВЫЧИСЛИМЫХ ФУНКЦИЙ

ЛАДИСЛАВ РИГЕР (Ladislav Rieger), Прага

Известная нормальная форма Клини для частично вычислимых функций выводится непосредственно из арифметизации работы машины Тюринга; некоторое упрощение (по сравнению с овыкновенным путем) при этом получается применением операции минимума не к числу вычисления (по Геделю, см. M. DAVIS [1], п. 57—8) но к т.н. числу временного состояния; этим числом для данной машины Тюринга M разумеется натуральное число упорядоченной пары $(t, |\alpha|)$ натуральных чисел (в некоторой нумерации) где t обозначает число шагов машины, которым она может ползоваться, чтобы осуществить состояние α, числом Геделя которого является $|\alpha|$. Кроме того в статье приводится изложение понятия машины Тюринга с односторонней лентой.

CONCERNING KLEENE'S NORMAL FORM FOR COMPUTABLE FUNCTIONS

LADISLAV RIEGER, Praha

The well known Kleene's normal form of a Turing-computable function (= partial recursive function) is shortly inferred. Instead of the usual Gödel numbers of a computation (cf. e.g. M. DAVIS [1], pp. 57—58) as values of the minimized parameter, the so-called time-state numbers of a Turing machine are used, yielding explicit and relatively simple expression for Turing-computable functions in Kleene's normal form; a time-state number of a Turing machine M is a number of any ordered couple $(t, |\alpha|)$ of naturals (in a suitable numbering) where t is the number of steps of M from some initial state to the "present" state α whose Gödel number is $|\alpha|$. An exposition of the notion of Turing machine with a one-sided tape as well as the diagonal argument for recursive unsolvability of the "halting-problem" are also given.