Úvod

S používaním samočinných počítačov rôznych druhov veľmi stúpla dôležitosť rôznych algoritmov na riešenie matematických, ale aj iných úloh. Zostavujú a skúmajú sa veľké počty takýchto algoritmov. V súvislosti s tým vznikajú i rozličné všeobecné otázky o existencii algoritmov na riešenie niektorých úloh a o spôsobe ich nájdenia. Otázkami tohto druhu sa zaoberá teória algoritmov.

Objekty, s ktorými algoritmy pracujú, môžu byť najrôznejších typov (čísla, matice, tabuľky, grafy, slová, formuly, atď.). My sa však budeme zaoberať hlavne algoritmami, ktoré pracujú s prirodzenými číslami funkcií, na množine všetkých prirodzených čísel. Okrem toho sa budeme zaoberať algoritmami, ktoré pracujú so slovami, t.j. s konečnými postupnosťami znakov z nejakej konečnej množiny.

Napriek tomu, že pojem algoritmicky vypočítateľnej funkcie (na množine všetkých prirodzených čísel) je intuitívne zrejmý, nie je možné matematicky ho v úplnej všeobecnosti opísať. Môžeme však matematicky definovať rôzne špeciálne druhy algoritmickej vypočítateľnosti, a to tak, aby sme definovanými pojmami čo najlepšie vystihli všeobecný pojem algoritmickej vypočítateľnosti. Vhodnosť či nevhodnosť takýchto definícií možno posúdiť až po podrobnejšom preskúmaní vlastností definovaných pojmov. Tu zavedieme tri spresnenia pojmu algoritmickej vypočítateľnosti, a to rekurzívnosť (v kapitole 3), vypočítateľnosť na registrových strojoch (v kapitole 5) a vypočítateľnosť na Turingových strojoch (v kapitole 8). K otázke vhodnosti zavedených pojmov ako aproximácií všeobecného pojmu algoritmickej vypočítateľnosti sa vrátime v kapitole 10. (Pritom z dôvodov, ktoré postupne uvidíme, budeme radšej skúmať rôzne druhy čiastočnej vypočítateľnosti, z ktorých už príslušné druhy vypočítateľnosti dostaneme ako špeciálne prípady.)

Vo všetkých našich úvahách budeme používať abstrakciu potenciálnej uskutočniteľnosti. To znamená, že si nebudeme všímať rôzne časové, priestorové a materiálové ohraničenia, ktorým podliehajú ako skutočné samočinné počítače, tak i ľudia výpočtári. Skúmanie týchto ohraničení je zaiste veľmi dôležité, ale je lepšie najprv vybudovať jednoduchšiu a všeobecnejšiu teóriu a jej výsledky potom využiť pri rozvíjaní zložitejšej teórie, ktorá bude už skúmať i tieto ohraničenia. Z obdobných dôvodov neskúmame skutočné samočinné počítače v celej ich zložitosti, ale skúmame miesto nich registrové a Turingove stroje. Tieto stroje sú veľmi jednoduché, majú však (pri našich abstrakciách) všetky podstatné vlastnosti samočinných počítačov.

Teóriu algoritmov nebudeme rozvíjať ako formalizovanú, ba ani ako axiomatickú teóriu. Budeme ju však budovať takým spôsobom, aby ju bolo možné bez podstatných ťažkostí formalizovať, napríklad v rámci hociktorého bežného axiomatického systému teórie množín.

Ešte upozorňujeme čitateľa, že niektoré časti dôkazov mnohých viet sú ponechané do cvičení. Niekedy sú v cvičeniach vyslovované aj pomocné tvrdenia. Riešenie cvičení je preto neoddeliteľnou súčasťou štúdia skrípt.

Poznámka 1.17. Každá n-árna funkcia na množine X je aj n-árnou čiastočnou funkciou na množine X. Ak budeme chcieť zdôrazniť, že ide o n-árnu funkciu, a nie o n-árnu čiastočnú funkciu, pridáme slovo *totálna*.

Označenie 1.18. Hodnotu n-árnej čiastočnej funkcie f v bode $(x_1, \ldots, x_n)$ budeme označovať $f(x_1, \ldots, x_n)$, pre $n = 0$ prípadne iba f. To, že hodnota $f(x_1, \ldots, x_n)$ je definovaná, budeme značiť $f(x_1, \ldots, x_n)\downarrow$, to, že nie je definovaná, budeme značiť $f(x_1, \ldots, x_n)\uparrow$, prípadne $f(x_1, \ldots, x_n) = \uparrow$.

Definícia 1.19. Rovnosť medzi dvoma výrazmi chápeme takto: $A = B$ znamená, že buď sú hodnoty oboch výrazov A, B nedefinované, alebo sú obe hodnoty definované a navzájom sa rovnajú.

Definícia 1.20. (a) *Oborom definície* n-árnej čiastočnej funkcie f na množine X nazveme množinu všetkých takých $(x_1, \ldots, x_n) \in X^n$, že $f(x_1, \ldots, x_n)\downarrow$.

(b) *Oborom hodnôt* n-árnej čiastočnej funkcie f na množine X nazveme množinu všetkých takých $y \in X$, že existuje také $(x_1, \ldots, x_n) \in X^n$, že $y = f(x_1, \ldots, x_n)$.

(c) *Grafom* n-árnej čiastočnej funkcie f na množine X nazveme množinu všetkých takých $(x_1, \ldots, x_n, y) \in X^{n+1}$, že $y = f(x_1, \ldots, x_n)$.

Definícia 1.21. Množinu M budeme nazývať *reláciou* (resp. *čiastočnou funkciou*, resp. *funkciou*) na množine X, ak existuje také $n \in \mathbb{N}$, že M je n-árnou reláciou (resp. n-árnou čiastočnou funkciou, resp. n-árnou funkciou) na množine X.

Poznámka 1.22. Množina $\emptyset$ je pre každé $n \in \mathbb{N}$ n-árnou reláciou i n-árnou čiastočnou funkciou na každej množine X. Ak ale $X \neq \emptyset$, tak žiadna neprázdna množina M nemôže byť súčasne reláciou i čiastočnou funkciou na množine X, ani nemôže byť n-árnou reláciou (resp. čiastočnou funkciou) pre rôzne hodnoty n.

Definícia 1.23. Nech f, g sú čiastočné funkcie na množine X. Budeme hovoriť, že f je *zúžením* g, alebo že g je *rozšírením* f, ak $f \subseteq g$. Ak g je rozšírením f a g je totálna funkcia na X, budeme g nazývať *zúplnením* čiastočnej funkcie f na množine X.

V nasledujúcej definícii budeme predpokladať, že množina X obsahuje čísla $0, 1$; túto definíciu budeme využívať najčastejšie pre $X = \mathbb{N}$.

Definícia 1.24. (a) *Čiastočnou charakteristickou funkciou* n-árnej relácie M na množine X nazveme takú n-árnu čiastočnú funkciu f na množine X, že pre všetky $x_1, \ldots, x_n \in X$ platí:

$$f(x_1, \ldots, x_n) = \begin{cases} 0, & \text{ak } (x_1, \ldots, x_n) \in M \\ \uparrow, & \text{ak } (x_1, \ldots, x_n) \notin M \end{cases} \tag{1.24.1}$$

(b) *Charakteristickou funkciou* n-árnej relácie M na množine X nazveme takú n-árnu funkciu f na množine X, že pre všetky $x_1, \ldots, x_n \in X$ platí:

$$f(x_1, \ldots, x_n) = \begin{cases} 0, & \text{ak } (x_1, \ldots, x_n) \in M \\ 1, & \text{ak } (x_1, \ldots, x_n) \notin M \end{cases} \tag{1.24.2}$$

Poznámka 1.25. Ak budeme chcieť používať túto definíciu aj v prípade, že $0, 1 \notin X$, zvolíme miesto prvkov $0, 1$ vhodné prvky množiny X, čo však vždy dopredu výslovne uvedieme.

Niektoré výrazy používame na označovanie hodnôt funkcií (prípadne čiastočných funkcií) i na označovanie samotných týchto funkcií. Niekedy je potrebné túto nejednoznačnosť odstrániť. Aj keď uvažujeme tieto označenia len ako názvy čiastočných funkcií, zostávajú nám problémy s rozlíšením premenných a parametrov a s určením poradia premenných. Tieto ťažkosti nám pomôže odstrániť tzv. Churchova λ-notácia.

Označenie 1.26. Nech $F(x_1, \ldots, x_n)$ je výraz, ktorý pri dosadení ľubovoľných prvkov z množiny X za $x_1, \ldots, x_n$ je nedefinovaný, alebo má hodnotu z množiny X. Potom znakom

$$\lambda_X x_1 \ldots x_n F(x_1, \ldots, x_n)$$

označíme takú n-árnu čiastočnú funkciu f na množine X, že pre všetky $a_1, \ldots, a_n \in X$ platí

$$f(a_1, \ldots, a_n) = F(a_1, \ldots, a_n)$$

Pokiaľ nebude hroziť nedorozumenie, budeme index pri písmene λ vynechávať.

$\Longrightarrow$, $\Longleftrightarrow$, $\neg$ zvratom „ ... a ...“, „ ... alebo ...“, „ak ..., tak ...“, „ ... práve vtedy, keď ...“, „nie je pravda, že ...“.

Definícia 1.35. Nech $P(x)$ je unárny predikát na množine X. Potom:

(a) Výrok $(\forall x)P(x)$ je pravdivý práve vtedy, keď pre každé $a \in X$ je výrok $P(a)$ pravdivý.

(b) Výrok $(\exists x)P(x)$ je pravdivý práve vtedy, keď existuje také $a \in X$, že výrok $P(a)$ je pravdivý.

Poznámka 1.36. Podľa definície 1.35 zodpovedajú znaky $\forall$, resp. $\exists$ slovám „pre každé ...“, resp. „existuje ...“. Všimnime si, že pridanie kvantifikátora vytvorilo z unárneho predikátu výrok. Všeobecne povedané, pridanie kvantifikátora zmenšuje počet voľných premenných predikátu o jednotku. (V prípade, že niektoré pridanie kvantifikátora neznižuje počet voľných premenných, je v podstate zbytočné, lebo sa ním vytvára predikát ekvivalentný s pôvodným.)

Pri uvažovaní predikátov a ich voľných premenných vznikajú tie isté problémy ako pri uvažovaní čiastočných funkcií a ich premenných, t.j. otázka určenia poradia premenných a otázka fiktívnych premenných. Mohli by sme ich odstrániť napríklad vhodnou obdobou λ-notácie, ale nebudeme sa tým zaoberať; budeme však vždy predpokladať, že s predikátom sú už určené aj jeho voľné premenné a ich poradie.

V nasledujúcej definícii predpokladáme (obdobne ako v definícii 1.24), že $0, 1 \in X$; ak táto podmienka nebude splnená, budeme postupovať podľa poznámky 1.25.

Definícia 1.37. Nech $P(x_1, \ldots, x_n)$ je n-árny predikát na množine X.

(a) *Čiastočnou charakteristickou funkciou predikátu* $P(x_1, \ldots, x_n)$ je taká n-árna čiastočná funkcia f na množine X, že pre všetky $a_1, \ldots, a_n \in X$ platí:

$$f(a_1, \ldots, a_n) = \begin{cases} 0, & \text{ak } P(a_1, \ldots, a_n) \\ \uparrow, & \text{ak } \neg P(a_1, \ldots, a_n) \end{cases} \tag{1.37.1}$$

(b) *Charakteristická funkcia predikátu* $P(x_1, \ldots, x_n)$ je taká n-árna funkcia f na množine X, že pre všetky $a_1, \ldots, a_n \in X$ platí:

$$f(a_1, \ldots, a_n) = \begin{cases} 0, & \text{ak } P(a_1, \ldots, a_n) \\ 1, & \text{ak } \neg P(a_1, \ldots, a_n) \end{cases} \tag{1.37.2}$$

Definícia 1.38. *Oborom pravdivosti predikátu* $P(x_1, \ldots, x_n)$ na množine X nazveme množinu všetkých takých $(a_1, \ldots, a_n) \in X^n$, že platí $P(a_1, \ldots, a_n)$.

Poznámka 1.39. Charakteristická funkcia predikátu je charakteristická funkcia jeho oboru pravdivosti. Obdobnú vlastnosť má i čiastočná charakteristická funkcia predikátu.

Často sa nám vyskytne prípad, že budeme chcieť vysloviť dve vety (prípadne definície) veľmi podobného znenia, a obvykle aj s podobnými dôkazmi. V prípade, že jednu z týchto viet možno dostať z druhej vynechaním niektorých slov, budeme tieto slová dávať do zátvoriek „(...)“. Obdobne budeme postupovať i pri dôkazoch a pod.

Príklad 1.40. Definíciu 1.16 by sme teraz mohli formulovať takto: n-árnou (čiastočnou) funkciou na množine X nazveme ľubovoľné (čiastočné) zobrazenie množiny X^n do množiny X. Poznámku 1.39 by sme mohli napísať takto: (Čiastočná) charakteristická funkcia predikátu je (čiastočná) charakteristická funkcia jeho oboru pravdivosti.

Veta 2.12. Nech klon $\mathcal{M}$ čiastočných funkcií na množine $\mathbb{X}$ obsahuje všetky unárne konštantné funkcie, nech čiastočná funkcia $f(x_1, \ldots, x_n)$, $n \neq 0$, patrí do $\mathcal{M}$ a nech $a_1, \ldots, a_k \in \mathbb{X}$, $k < n$. Potom aj čiastočná funkcia g, $g(x_{k+1}, \ldots, x_n) = f(a_1, \ldots, a_k, x_{k+1}, \ldots, x_n)$ patrí do $\mathcal{M}$.

Dôkaz: Označme pre ľubovoľné $m \in \mathbb{N}$, $a \in \mathbb{X}$ symbolom K_a^m m-árnu konštantnú funkciu s hodnotou a. Podľa cvičenia 2.11 funkcie $K_{a_1}^{n-k}, \ldots, K_{a_k}^{n-k}$ patria do $\mathcal{M}$. Platí

$$g(x_{k+1}, \ldots, x_n) = f\big(K_{a_1}^{n-k}(x_{k+1}, \ldots, x_n), \ldots, K_{a_k}^{n-k}(x_{k+1}, \ldots, x_n), \\ I_1^{n-k}(x_{k+1}, \ldots, x_n), \ldots, I_{n-k}^{n-k}(x_{k+1}, \ldots, x_n)\big)$$

pre všetky $x_{k+1}, \ldots, x_n \in \mathbb{X}$, t.j.

$$g = \mathcal{S}^{n+1}\left(f, K_{a_1}^{n-k}, \ldots, K_{a_k}^{n-k}, I_1^{n-k}, \ldots, I_{n-k}^{n-k}\right)$$

a teda g patrí do $\mathcal{M}$, čo bolo treba dokázať. □

Poznámka 2.13. Podľa vety 2.12 možno za istých predpokladov „dosadzovať za premenné konštanty". Ak napríklad $\mathbb{X} = \mathbb{N}$, $\mathcal{M}$ je klon čiastočných funkcií na $\mathbb{X}$, ktorý osahuje všetky konštantné funkcie a $f(x, y) = x^y \in \mathcal{M}$, tak aj funkcie $g(x) = x^3$, $h(x) = 2^x$ patria do klonu $\mathcal{M}$.

Veta 2.14. Ak klon $\mathcal{M}$ čiastočných funkcií na $\mathbb{X}$ obsahuje všetky unárne konštantné funkcie a aspoň jednu 0-árnu funkciu, tak obsahuje všetky 0-árne funkcie na $\mathbb{X}$.

Dôkaz: Použijeme označenie z dôkazu vety 2.12. Podľa predpokladu existuje také $b \in \mathbb{X}$, že $K_b^0 \in \in \mathcal{M}$. Zoberme ľubovoľné $a \in \mathbb{X}$. Podľa predpokladu je $K_a^1 \in \mathcal{M}$, a teda aj

$$K_a^0 = \mathcal{S}^2(K_a^1, K_b^0) \in \mathcal{M} \quad \square$$

Zapíšeme teraz vety 2.8, 2.12 a 2.14 súhrnne a s použitím λ-notácie (z vety 2.8 budú zapísané dva zvlášne prípady).

Veta 2.15. Nech $\mathcal{M}$ je klon čiastočných funkcií na množine $\mathbb{X}$. Potom:

(a) Ak $n > 0$, $k_1, \ldots, k_n$ je ľubovoľné poradie prvkov $1, \ldots, n$ a $\lambda x_1 \ldots x_n f(x_1, \ldots, x_n) \in \mathcal{M}$, tak aj čiastočná funkcia $\lambda x_{k_1} \ldots x_{k_n} f(x_1, \ldots, x_n)$ patrí do $\mathcal{M}$.

(b) Ak $n > 0$, $y_1, \ldots, y_k$ sú premenné rôzne od $x_1, \ldots, x_n$ a nevyskytujúce sa vo výraze $f(x_1, \ldots, x_n)$ a $\lambda x_1 \ldots x_n f(x_1, \ldots, x_n) \in \mathcal{M}$, tak aj čiastočná funkcia

$$\lambda x_1 \ldots x_n y_1 \ldots y_k f(x_1, \ldots, x_n)$$

patrí do $\mathcal{M}$.

(c) Ak pre každé $a \in \mathbb{X}$ je $\lambda x(a) \in \mathcal{M}$, $k, n \in \mathbb{N}$, $k < n$ a ak $\lambda x_1 \ldots x_n f(x_1, \ldots, x_n) \in \mathcal{M}$, tak pre všetky $x_1, \ldots, x_k \in \mathbb{X}$ platí $\lambda x_{k+1} \ldots x_n f(x_1, \ldots, x_n) \in \mathcal{M}$.

(d) Ak pre všetky $a \in \mathbb{X}$ platí $\lambda x(a) \in \mathcal{M}$ a ak existuje také $b \in \mathbb{X}$, že $\lambda(b) \in \mathcal{M}$, tak pre každé $a \in \mathbb{X}$ platí $\lambda(a) \in \mathcal{M}$.

Čitateľ nech si sám porovná formuláciu vety 2.15 s predchádzajúcimi vetami.

Často budeme pracovať s množinou všetkých totálnych funkcií z nejakého klonu čiastočných funkcií. Pritom bude niekedy užitočná nasledujúca veta.

Veta 2.16. Nech $\mathcal{M}$ je klon čiastočných funkcií na množine $\mathbb{X}$. Potom množina $\mathcal{M}'$ všetkých totálnych funkcií klonu $\mathcal{M}$ je klonom funkcií na množine $\mathbb{X}$.

Dôkaz: $\mathcal{M}'$ zrejme obsahuje všetky projekcie na $\mathbb{X}$ a podľa tvrdenia z cvičenia 2.4 je aj množina $\mathcal{M}'$ uzavretá vzhľadom na operáciu skladania funkcií. □

Definícia 2.17. Usporiadanú trojicu funkcií C, L, R, kde C je binárna funkcia na $\mathbb{X}$ a L, R sú unárne funkcie na množine $\mathbb{X}$, nazveme *trojicou číslovacích funkcií* na množine $\mathbb{X}$, ak pre všetky x, $y \in \mathbb{X}$ platí

$$C(L(x), R(x)) = x \tag{2.17.1}$$

$$L(C(x, y)) = x, \quad R(C(x, y)) = y \tag{2.17.2}$$

Cvičenie 2.18. Dokážte, že z podmienok (2.17.1) a (2.17.2) vyplýva, že C je jednojednoznačná funkcia z množiny $\mathbb{X}^2$ na množinu $\mathbb{X}$! Pre aké množiny $\mathbb{X}$ existuje trojica číslovacích funkcií na množine $\mathbb{X}$?

Veta 2.27. Nech $\mathcal{M}_2 \subseteq \mathcal{M}_1$ sú klony čiastočných funkcií na množine $\mathbb{X}$, nech klon $\mathcal{M}_2$ obsahuje trojicu číslovacích funkcií a klon $\mathcal{M}_1$ univerzálnu čiastočnú funkciu pre množinu všetkých unárnych prvkov klonu $\mathcal{M}_2$. Potom pre každé $n \in \mathbb{N}$, $n \neq 0$ obsahuje klon $\mathcal{M}_1$ univerzálnu čiastočnú funkciu pre množinu $\mathcal{M}_2^{(n)}$ všetkých n-árnych prvkov klonu $\mathcal{M}_2$.

Dôkaz: prenechávame čitateľovi; môže pri ňom využiť poznámku 2.22. □

Poznámka 2.28. (a) Vetu 2.27 budeme najčastejšie používať v prípade $\mathcal{M}_1 = \mathcal{M}_2$.

(b) Množina $\mathcal{M}_2^{(1)}$ v tejto vete môže byť nahradená množinou $\mathcal{M}_2^{(k)}$ pre ľubovoľné $k \in \mathrm{N}$, $k \neq$ $\neq 0$.

Veta 2.29. Nech $\mathcal{M}$ je klon funkcií na množine $\mathbb{X}$ a nech obsahuje takú unárnu funkciu g, že pre všetky $x \in \mathbb{X}$ $g(x) \neq x$. Potom pre žiadne $n \in \mathbb{N}$, $n \neq 0$ neobsahuje klon $\mathcal{M}$ univerzálnu funkciu pre množinu $\mathcal{M}^{(n)}$ všetkých svojich n-árnych funkcií.

Dôkaz: Predpokladajme obrátene, že klon takú funkciu $F(t, x_1, \ldots, x_n)$ obsahuje. Potom n-árna funkcia h, $h(x_1, \ldots, x_n) = g\left(F(x_1, x_1, \ldots, x_n)\right)$ patrí do $\mathcal{M}^{(n)}$, a preto existuje také $a \in \mathbb{X}$, že pre všetky $x_1, \ldots, x_n \in \mathbb{X}$ platí $h(x_1, \ldots, x_n) = F(a, x_1, \ldots, x_n)$. Dosadením $x_1 = x_2 = \cdots = x_n = a$ dostávame jednak $h(a, \ldots, a) = g\left(F(a, a, \ldots, a)\right)$ a jednak $h(a, \ldots, a) = F(a, a, \ldots, a)$, teda pre $b = F(a, a, \ldots, a)$ dostávame $g(b) = b$, a to je spor s predpokladom o g. □

Pre veľkú dôležitosť nasledujúcej vety (a myšlienky jej dôkazu) sme najprv uviedli ako jej špeciálny prípad vetu 2.29.

Veta 2.30. Nech $\mathcal{M}$ je klon čiastočných funkcií na množine $\mathbb{X}$ a nech obsahuje takú (totálnu) unárnu funkciu g, že pre všetky $x \in \mathbb{X}$ platí $g(x) \neq x$. Nech $n \in \mathbb{N}$, $n \neq 0$. Potom žiadna univerzálna čiastočná funkcia pre množinu $\mathcal{M}^{(n)}$ všetkých n-árnych prvkov systému $\mathcal{M}$ nemá zúplnenie v klone $\mathcal{M}$.

Dôkaz: Predpokladajme obrátene, že taká $(n+1)$-árna čiastočná funkcia $H(t, x_1, \ldots, x_n)$ existuje a že nejaké jej zúplnenie $F(t, x_1, \ldots, x_n)$ patrí do klonu $\mathcal{M}$. Potom (totálna) funkcia

$$h(x_1, \ldots, x_n) = g\big(F(x_1, x_1, \ldots, x_n)\big)$$

patrí do $\mathcal{M}^{(n)}$, a teda existuje také $a \in \mathbb{X}$, že $h(x_1, \ldots, x_n) = H(a, x_1, \ldots, x_n)$. Pretože funkcia $H(a, x_1, \ldots, x_n)$ je definovaná pre všetky $x_1, \ldots, x_n \in \mathbb{X}$, pre všetky $x_1, \ldots, x_n \in \mathbb{X}$ platí $H(a, x_1, \ldots, x_n) = F(a, x_1, \ldots, x_n)$, a teda $h(x_1, \ldots, x_n) = F(a, x_1, \ldots, x_n)$. Dosadením $x_1 = \cdots = x_n = a$ dostávame $h(a, \ldots, a) = F(a, a, \ldots, a)$, a tiež $h(a, \ldots, a) = g\left(F(a, \ldots, a)\right)$, a teda pre $b = F(a, \ldots, a)$ dostávame $g(b) = b$, čo je spor. □

Poznámka 2.31. Neskôr uvidíme, že existujú klony $\mathcal{M}$ čiastočných funkcií obsahujúce funkciu g s vyššie uvedenou vlastnosťou a obsahujúce aj univerzálne čiastočné funkcie pre množiny $\mathcal{M}^{(n)}$. Podľa vety 2.30 však takéto univerzálne čiastočné funkcie nebudú mať v týchto klonoch zúplnenia. Keby sme sa pokúsili dokázať analógiu vety 2.29 pre klony čiastočných funkcií postupom použitým v jej dôkaze nedostali by sme očakávaný spor, ale iba tvrdenie, že niektorá hodnota $F(a, a, \ldots, a)$ nie je definovaná.

Klony čiastočných funkcií, s ktorými sa stretneme v ďalšom texte, budú mať obvykle všetky vlastnosti z nasledujúcej definície.

Definícia 2.32. Klon $\mathcal{M}$ (čiastočných) funkcií na množine $\mathbb{X}$ nazveme *normálnym klonom (čiastočných) funkcií na množine* $\mathbb{X}$, ak obsahuje trojicu číslovacích funkcií a ak obsahuje takú unárnu funkciu g, že pre všetky $x \in \mathbb{X}$ platí $g(x) \neq x$.

Cvičenie 2.33. Ak existuje normálny klon čiastočných funkcií na množine $\mathbb{X}$, tak je množina $\mathbb{X}$ nekonečná. Dokážte!

Cvičenie 2.34. Nech $\mathcal{M}$ je normálny klon čiastočných funkcií na množine $\mathbb{X}$ a nech $\mathcal{M}$ obsahuje univerzálnu čiastočnú funkciu pre množinu $\mathcal{M}^{(3)}$. Dokážte, že klon $\mathcal{M}$ obsahuje unárnu čiastočnú funkciu, ktorej žiadne zúplnenie nepatrí do klonu $\mathcal{M}$!

Veta 2.35. Množina všetkých (totálnych) funkcií normálneho klonu čiastočných funkcií na množine $\mathbb{X}$ je normálny klon funkcií na množine $\mathbb{X}$.

Dôkaz: je triviálny. □

Cvičenie 2.51. Rozhodnite, či platí nasledujúce tvrdenie: Ak klon funkcií na nejakej nekonečnej množine X obsahuje aspoň jednu funkciu s vlastnosťou $\forall x\big(g(x) \neq x\big)$, tak obsahuje nekonečne mnoho takýchto funkcií.

Cvičenie 2.52. Ktoré trojice číslovacích funkcií (C, L, R) majú vlastnosť $(C, L, R) = (C, R, L)$?

Cvičenie 2.53. Nech $\mathcal{M}_1$, $\mathcal{M}_2$ sú klony funkcií na tej istej množine X, a nech platí $\mathcal{M}_1^{(1)} = \mathcal{M}_2^{(1)}$. Platí potom aj $\mathcal{M}_1 = \mathcal{M}_2$?

Cvičenie 2.54. Nech $\mathcal{M}_1$, $\mathcal{M}_2$ sú normálne klony funkcií na tej istej množine X, a nech platí $\mathcal{M}_1^{(1)} = \mathcal{M}_2^{(1)}$. Platí potom aj $\mathcal{M}_1 = \mathcal{M}_2$?

Cvičenie 2.55. Nech $\mathcal{M}_1$, $\mathcal{M}_2$ sú normálne klony funkcií na tej istej množine X, a nech platí $\mathcal{M}_1^{(1)} = \mathcal{M}_2^{(1)}$. Platí potom aj $\mathcal{M}_1^{(2)} = \mathcal{M}_2^{(2)}$?

Cvičenie 2.56. Uvažujme klon funkcií na množine $\mathbb{N}$ generovaný funkciou $\lambda_{\mathbb{N}} x(2^x)$. Rozhodnite, ktoré z nasledujúcich funkcií tento klon obsahuje:

- $\lambda_{\mathbb{N}} xyz(2^{2^y})$
- $\lambda_{\mathbb{N}} xyz(4^x)$
- $\lambda_{\mathbb{N}} x(2^{x^2})$

Cvičenie 2.57. Rozhodnite, či platí nasledujúce tvrdenie: Prienik dvoch klonov funkcií na množine $\mathbb{N}$ je klon funkcií na množine $\mathbb{N}$.

Cvičenie 2.58. Rozhodnite, či platí nasledujúce tvrdenie: Zjednotenie dvoch klonov funkcií na množine $\mathbb{N}$ je klon funkcií na množine $\mathbb{N}$.

Funkcia f je *primitívne rekurzívna* , ak existuje taká konečná postupnosť funkcií $f_1, \ldots, f_n$, že platí $f_n = f$ a že pre každé $i = 1, \ldots, n$ platí

(a) $f_i = 0$ alebo $f_i = s$ alebo $f_i = I_m^n$ pre nejaké $m, n \in \mathbb{N}, 0 < m \leq n$, alebo
(b) f_i vzniká z niektorých z funkcií $f_1, \ldots, f_{i-1}$ operáciou skladania funkcií, alebo
(c) f_i vzniká z niektorých dvoch funkcií f_j, f_k, $j < i, k < i$ operáciou primitívnej rekurzie.

Takúto postupnosť by sme mohli nazvať *vytvárajúcou postupnosťou* primitívne rekurzívnej funkcie f. Inú možnosť nám poskytuje nasledujúca veta.

Veta 3.6. Množina všetkých primitívne rekurzívnych funkcií je najmenší klon funkcií, ktorý obsahuje funkcie 0, s a je uzavretý vzhľadom na operáciu primitívnej rekurzie.

Dôkaz: je zrejmý. □

Dokážeme teraz primitívnu rekurzívnosť niektorých funkcií na množine $\mathbb{N}$. Veľká väčšina konkrétnych funkcií na množine $\mathbb{N}$, ktoré sa vyskytujú v matematických úvahách, patrí medzi primitívne rekurzívne funkcie. Toto tvrdenie, samozrejme, nie je presná matematická veta, a teda nemožno ho matematicky dokázať. Aby sme však čitateľa presvedčili o jeho platnosti a súčasne dali čitateľovi možnosť predpovedať primitívnu rekurzívnosť funkcií, s ktorými sa neskôr sám stretne (a tiež aspoň principiálnu možnosť nahradiť takúto predpoveď presným dôkazom), tak:

- O niektorých aritmetických funkciách bezprostredne dokážeme, že sú primitívne rekurzívne; budeme pritom využívať ich všeobecne známe vlastnosti, ako aj vlastnosti prirodzených čísel. Označenia pre tieto funkcie väčšinou nebudeme zavádzať v samostatných definíciách (čo by bol najdôslednejší postup), ale priamo vo vetách o ich primitívnej rekurzívnosti, prípadne i v dôkazoch. Označenie funkcií sa väčšinou bude zhodovať s označovaním v [6].
- Ukážeme ďalšie operácie, ktoré zachovávajú primitívnu rekurzívnosť funkcií. Používanie týchto operácií často významne skráti a sprehľadní dôkazy primitívnej rekurzívnosti.

Bez výslovného uvádzania budeme používať nasledujúcu lemu, ktorú nechávame na rozmyslenie čitateľovi.

Lema 3.7. Funkcia, ktorá vzniká konečným počtom operácií skladania funkcií a primitívnej rekurzie z primitívne rekurzívnych funkcií, je primitívne rekurzívna.

Veta 3.8. Všetky konštantné funkcie sú primitívne rekurzívne.

Dôkaz: Nulárna funkcia 0 je primitívne rekurzívna podľa definície. Unárna funkcia $o = \lambda x(0)$ vzniká primitívnou rekurziou z funkcií $0, I_2^2$, lebo pre všetky $x \in \mathbb{N}$ platí

$$\begin{aligned} o(0) &= 0 \\ o(x+1) &= I_2^2(x, o(x)) \end{aligned} \tag{3.8.1}$$

Funkcia $\lambda x(k+1)$ vzniká skladaním funkcií $s, \lambda x(k)$:

$$\lambda x(k+1) = \mathcal{S}^2(s, \lambda x(k))$$

Tým sme indukciou dokázali, že všetky unárne konštantné funkcie sú primitívne rekurzívne. Podľa cvičenia 2.11 sú potom aj všetky n-árne ($n \neq 0$) konštantné funkcie primitívne rekurzívne a podľa vety 2.14 sú aj všetky konštanty primitívne rekurzívne. □

Cvičenie 3.9. Funkcia $\lambda x(1000)$ je primitívne rekurzívna, a teda existuje jej vytvárajúca postupnosť $f_1, \ldots, f_n$ v zmysle poznámky 3.5. Možno túto postupnosť zvoliť tak, aby bolo $n < 1000$?

Veta 3.10. Funkcie $\lambda xy(x+y)$, $\lambda xy(x.y)$, $\lambda xy(y^x)$ sú primitívne rekurzívne.

Dôkaz: Pre všetky x, $y \in \mathbb{N}$ platí

$$\begin{aligned} 0 + y &= I_1^1(y) \\ (x+1) + y &= s(I_2^3(x, x+y, y)) \end{aligned} \tag{3.10.1}$$

Poznámka 3.15. Pozor, zápis $|x - y|$ chápeme len ako celok, a nie ako zápis funkcie zloženej z funkcie $|x|$ a (na množine $\mathbb{N}$ čiastočnej) funkcie $x - y$. To sa týka aj mnohých ďalších označení, najmä tých, ktoré obsahujú znak (dolnej) celej časti „$\lfloor\ \ \rfloor$“.

Cvičenie 3.16. Dokážte presne primitívnu rekurzívnosť funkcií $\mathrm{sg}(x)$, $\overline{\mathrm{sg}}(x)$, $x \dot{-} y$ (bez využitia poznámky 3.11).

Dokážeme teraz, že operácie $\sum$ a $\prod$ sumácie a produktu dávajú z primitívne rekurzívnych funkcií znova primitívne rekurzívne funkcie.

Lema 3.17. Nech $g(y, x_1, \ldots, x_n)$ je primitívne rekurzívna funkcia. Potom aj funkcie f_1' a f_2' dané predpismi

$$f_1'(y, z, x_1, \ldots, x_n) = \sum_{i=z}^{y+z} g(i, x_1, \ldots, x_n)$$
$$f_2'(y, z, x_1, \ldots, x_n) = \prod_{i=z}^{y+z} g(i, x_1, \ldots, x_n)$$

sú primitívne rekurzívne.

Dôkaz: Platí

$$f_1'(0, z, x_1, \ldots, x_n) = g(z, x_1, \ldots, x_n),$$
$$f_1'(y+1, z, x_1, \ldots, x_n) = f_1'(y, z, x_1, \ldots, x_n) + g(y + z + 1, x_1, \ldots, x_n).$$

Teda funkcia f_1' vzniká primitívnou rekurziou z primitívne rekurzívnych funkcií, čiže je aj sama primitívne rekurzívna. Dôkaz pre funkciu f_2' je úplne analogický. □

Veta 3.18. Nech sú $g(y, x_1, \ldots, x_n)$, $h(x_1, \ldots, x_n)$, $k(x_1, \ldots, x_n)$ primitívne rekurzívne funkcie. Potom aj funkcie f_1, f_2 dané predpismi

$$f_1(x_1, \ldots, x_n) = \begin{cases} \displaystyle\sum_{i=h(x_1,\ldots,x_n)}^{k(x_1,\ldots,x_n)} g(i, x_1, \ldots, x_n), & \text{ak } h(x_1, \ldots, x_n) \le k(x_1, \ldots, x_n) \\ 0, & \text{ak } h(x_1, \ldots, x_n) > k(x_1, \ldots, x_n) \end{cases}$$

$$f_2(x_1, \ldots, x_n) = \begin{cases} \displaystyle\prod_{i=h(x_1,\ldots,x_n)}^{k(x_1,\ldots,x_n)} g(i, x_1, \ldots, x_n), & \text{ak } h(x_1, \ldots, x_n) \le k(x_1, \ldots, x_n) \\ 1, & \text{ak } h(x_1, \ldots, x_n) > k(x_1, \ldots, x_n) \end{cases}$$

sú primitívne rekurzívne.

Dôkaz: Nech f_1', f_2' sú funkcie z lemy 3.17. Označme ďalej h', k' funkcie dané predpismi

$$h'(x_1, \ldots, x_n) = h(x_1, \ldots, x_n) \dot{-} k(x_1, \ldots, x_n)$$
$$k'(x_1, \ldots, x_n) = k(x_1, \ldots, x_n) \dot{-} h(x_1, \ldots, x_n)$$

Pre všetky $x_1, \ldots, x_n \in \mathbb{N}$ platí

$$f_1(x_1, \ldots, x_n) = f_1'(k'(x_1, \ldots, x_n), h(x_1, \ldots, x_n), x_1, \ldots, x_n) . \overline{\mathrm{sg}}(h'(x_1, \ldots, x_n))$$
$$f_2(x_1, \ldots, x_n) = f_2'(k'(x_1, \ldots, x_n), h(x_1, \ldots, x_n), x_1, \ldots, x_n) . \overline{\mathrm{sg}}(h'(x_1, \ldots, x_n)) + \\ + \mathrm{sg}(h'(x_1, \ldots, x_n))$$

Tým sme vyjadrili funkcie f_1, f_2 pomocou operácie skladania funkcií a primitívne rekurzívnych funkcií, teda sme dokázali aj ich primitívnu rekurzívnosť. □

Poznámka 3.19. Aby nevzniklo nedorozumenie, napísali sme definíciu funkcií zvlášť pre prípad $h(x_1, \ldots, x_n) \le k(x_1, \ldots, x_n)$ a zvlášť pre prípad $h(x_1, \ldots, x_n) > k(x_1, \ldots, x_n)$. Ak však chceme, aby výrazy $\sum_{i=h}^{k} A_i$, $\prod_{i=h}^{k} A_i$ boli definované aj pre $h > k$, je najvhodnejšie definovať ich v tomto prípade ako rovnajúce sa 0 resp. 1. Potom nie je potrebné rozlišovať dva prípady v definíciách funkcií f_1, f_2.

Poznámka 3.27. Podľa vety 3.26 pri dôkaze primitívnej rekurzívnosti funkcie f stačí okrem vyjadrenia tvaru (3.22.1) ešte nájsť takú primitívne rekurzívnu funkciu $h(x_1, \ldots, x_n)$, že pre všetky $x_1, \ldots, x_n \in \mathbb{N}$ platí $f(x_1, \ldots, x_n) \leq h(x_1, \ldots, x_n)$.

Budeme teraz dokazovať primitívnu rekurzívnosť funkcií týkajúcich sa deliteľnosti.

Veta 3.28. Funkcia

$$\lfloor x/y \rfloor = \begin{cases} 0, & \text{ak } y = 0, \\ \text{(dolná) celá časť podielu } \frac{x}{y}, & \text{ak } y \neq 0 \end{cases} \tag{3.28.1}$$

je primitívne rekurzívna.

Dôkaz: Stačí uvážiť, že pre všetky x, $y \in \mathbb{N}$ platí

$$\lfloor x/y \rfloor = \mathrm{sg}(y).\sum_{i=1}^{x} \overline{\mathrm{sg}}(i.y \dot{-} x) \quad \square$$

Pre funkciu (3.28.1) budeme používať aj označenia $\left\lfloor \frac{x}{y} \right\rfloor$, x DIV y. Všetky tieto označenia chápeme (v zmysle poznámky 3.15) len *ako celok*.

Veta 3.29. Funkcia

$$x \text{ MOD } y = \begin{cases} \text{zvyšok pri delení } x/y, & \text{ak } y \neq 0, \\ x, & \text{ak } y = 0 \end{cases}$$

je primitívne rekurzívna.

Dôkaz: Platí x MOD $y = x \dot{-} y.\lfloor x/y \rfloor$, a teda fukcia MOD je primitívne rekurzívna, lebo vzniká skladaním z primitívne rekurzívnych funkcií. $\square$

Veta 3.30. Funkcie

$$\mathrm{div}(x, y) = \begin{cases} 1, & \text{ak } y \text{ je deliteľom } x \text{ (t.j. } y|x), \\ 0, & \text{ak } y \text{ nie je deliteľom } x \text{ (t.j. } y \not| x) \end{cases} \tag{3.30.1}$$

$$\mathrm{nd}(x) = \begin{cases} \text{počet (kladných) deliteľov } x, & \text{ak } x \neq 0, \\ 0, & \text{ak } x = 0 \end{cases} \tag{3.30.2}$$

sú primitívne rekurzívne.

Dôkaz: Veta vyplýva bezprostredne zo vzťahov

$$\mathrm{div}(x, y) = \overline{\mathrm{sg}}(x \text{ MOD } y)), \quad \mathrm{nd}(x) = \sum_{i=1}^{x} \mathrm{div}(x, i) \quad \square$$

Cvičenie 3.31. Dokážte primitívnu rekurzívnosť charakteristických funkcií množín

- $\{x \in \mathbb{N} \mid x \text{ je násobkom } 7\}$
- $\{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x^2 + y^2 \text{ je deliteľné troma}\}$
- $\{x \in \mathbb{N} \mid x \text{ je štvorcom (druhou mocninou)}\}$

Veta 3.32. Funkcie

$$\chi_p(x) = \begin{cases} 0, & \text{ak } x \text{ je prvočíslo}, \\ 1, & \text{ak } x \text{ nie je prvočíslo}, \end{cases} \tag{3.32.1}$$

$$\pi(x) = \text{počet prvočísel menších alebo rovnajúcich sa } x \tag{3.32.2}$$

sú primitívne rekurzívne.

Dôkaz: Prvočísla sú čísla, ktoré majú práve dva kladné delitele, a preto platí

$$\chi_p(x) = \mathrm{sg} \mid \mathrm{nd}(x) - 2 \mid \tag{3.32.3}$$

Nech $g_x(u)$ je ľavá strana tejto rovnice a $x > 1$ je celé číslo. (Pre $x \leq 1$ je zrejme $f(x) = 0$. Stále pokladáme u za neznámu a x za parameter.) Polynóm $g_x(u)$ má štyri imaginárne korene, a to

$$\pm\sqrt{x} - \frac{-1 \pm \mathrm{i}\sqrt{3}}{2} \cdot \sqrt[3]{x}$$

(s každou voľbou znamienok), a teda len dva reálne korene. Pretože $g_x(0) < 0$ a polynóm g_x je párneho stupňa, je jeden jeho reálny koreň kladný (a to zrejme u) a jeden záporný. Teda na intervale $(0, \infty)$ graf funkcie $g_x(u)$ pretína os u práve raz. Ďalej využívame z doterajších úvah len tento fakt; mohli sme ho dokázať aj metódami z matematickej analýzy.

Binárne funkcie

$$h_1(x,u) = u^6 + 2xu^3 + 3x^2u^2 + 6x^2u + x^2 \qquad h_2(x,u) = 3xu^4 + x^3$$

sú primitívne rekurzívne a zrejme $g_x(u) = h_1(x,u) - h_2(x,u)$. Pretože $f(x) = \lfloor u \rfloor$ je najmenšie prirodzené číslo také, že $g_x(u+1) > 0$, môžeme písať

$$f(x) = \mu_u \Big(\overline{\mathrm{sg}}\left(h_1(x,u+1) \dot{-} h_2(x,u+1)\right) = 0 \Big)$$

Na ohraničenie minimalizácie využijeme nerovnosť $f(x) \leq x$. Pre $x \leq 1$ síce niektoré z predchádzajúcich úvah neplatia, ale vzorec ľahko bezprostredne overíme.

Načrtneme ešte jeden spôsob riešenia tejto úlohy. Ľahko zistíme, že $u \in \mathbb{N}$ len vtedy, keď obe odmocniny v jeho vyjadrení sú celé čísla, teda keď x je šiestou mocninou. Tento prípad ľahko vybavíme osobitne. Ak u nie je celé, stačí nájsť dostatočne presné (racionálne) dolné a horné aproximácie pre obe odmocniny, a potom aj pre u. Ak horná a dolná aproximácia pre u majú rovnakú (dolnú) celú časť, tak je to $f(x)$. To určite nastane, ak rozdiel hornej a dolnej aproximácie je menší než vzdialenosť u od najbližšieho celého čísla. Tú môžeme zdola odhadnúť číslom $\frac{1}{M}$, kde M je horný odhad derivácie funkcie g_x (podľa u) na intervale $[u - \frac{1}{2}, u + \frac{1}{2}]$. Tento odhad využijeme na ohraničenie istej minimalizácie, alebo aj na priamejšie vyjadrenie

$$f(x) = \left(\lfloor \sqrt{4M^2x} \rfloor \dot{-} \lfloor \sqrt[3]{8M^3x} \rfloor \right) \mathrm{DIV}(2M)$$

(Za M treba dosadiť vhodnú funkciu! Vyhovuje napríklad $18x^3 + 1$. Ľahko zistíme, že vzorec platí aj pre pôvodne vylúčené prípady.) Poznamenajme ešte, že

$$f(x) = \lfloor \sqrt{x} \rfloor - \lfloor \sqrt[3]{x} \rfloor - \varepsilon_x$$

kde $\varepsilon_x \in \{0, 1\}$. Teda *približné* určenie hodnoty $f(x)$ je ľahké. (Môže byť užitočné pri výpočte M.) Ťažkosti spôsobuje až určovanie presnej hodnoty. □

Nájdeme teraz istú trojicu číslovacích funkcií na množine $\mathbb{N}$ a dokážeme ich primitívnu rekurzívnosť. Zaveďme najprv usporiadanie na množine $\mathbb{N}^2$ takto:

Definícia 3.41. Nech pre všetky $x_1, y_1, x_2, y_2 \in \mathbb{N}$ je $(x_1, y_1) \prec (x_2, y_2)$ práve vtedy, keď $x_1 + y_1 < x_2 + y_2$ alebo $x_1 + y_1 = x_2 + y_2$ a $x_1 < x_2$.

Teraz môžeme podľa tohto usporiadania zoradiť všetky prvky množiny $\mathbb{N} \times \mathbb{N}$ do prostej postupnosti

$$(0,0), \quad (0,1), \quad (1,0), \quad (0,2), \quad (1,1), \quad (2,0), \quad \ldots \tag{3.41.1}$$

a definovať:

Definícia 3.42.

$\mathrm{c}(x,y) =$ číslo člena (x,y) v postupnosti (3.41.1)

$\mathrm{l}(x) =$ prvý prvok dvojice na x-tom mieste postupnosti (3.41.1)

$\mathrm{r}(x) =$ druhý prvok dvojice na x-tom mieste postupnosti (3.41.1)

Teda

$$\begin{array}{rrrrrrrrr} \mathrm{c}(0,0) & = & 0, & \mathrm{c}(0,1) & = & 1, & \mathrm{c}(1,0) & = & 2, \quad \ldots \\ \mathrm{l}(0) & = & 0, & \mathrm{l}(1) & = & 0, & \mathrm{l}(2) & = & 1, \quad \ldots \\ \mathrm{r}(0) & = & 0, & \mathrm{r}(1) & = & 1, & \mathrm{r}(2) & = & 0, \quad \ldots \end{array}$$

Teraz môžeme definovať číslovacie funkcie c^n, $\mathrm{c}_{n,1}, \ldots, \mathrm{c}_{n,n}$ pre ľubovoľné $n \in \mathbb{N}$, $n \neq 0$.

Definícia 3.45. Pre každé $n \in \mathbb{N}$, $n \neq 0$, $i = 1, \ldots, n$ a pre všetky $x_1, \ldots, x_n$, $x \in \mathbb{N}$

$$\begin{aligned} \mathrm{c}^1(x) &= I_1^1(x) \\ \mathrm{c}_{1,1}(x) &= I_1^1(x) \end{aligned} \tag{3.45.1}$$

$$\mathrm{c}^{n+1}(x_1, \ldots, x_n, x) = \mathrm{c}(\mathrm{c}^n(x_1, \ldots, x_n), x) \tag{3.45.2}$$

$$\begin{aligned} \mathrm{c}_{n+1,i}(x) &= \mathrm{c}_{n,i}(\mathrm{l}(x)) \\ \mathrm{c}_{n+1,n+1}(x) &= \mathrm{r}(x) \end{aligned} \tag{3.45.3}$$

Veta 3.46. Funkcie z definície 3.45 sú primitívne rekurzívne.

Cvičenie 3.47. Dokážte primitívnu rekurzívnosť funkcií l, r použitím vety 3.26.

Cvičenie 3.48. Nájdite aspoň dve trojice primitívne rekurzívnych číslovacích funkcií rôzne od trojice c, l, r.

Ak si teraz uvedomíme, že pre primitívne rekurzívnu funkciu s a všetky $x \in \mathbb{N}$ platí $s(x) \neq x$, môžeme vysloviť toto zosilnenie vety 3.6:

Veta 3.49. Množina všetkých primitívne rekurzívnych funkcií je normálny klon funkcií na množine $\mathbb{N}$.

Jedným z dôsledkov tejto vety je

Veta 3.50. Pre žiadne $n \in \mathbb{N}$, $n \neq 0$ nemá množina všetkých primitívne rekurzívnych n-árnych funkcií primitívne rekurzívnu univerzálnu funkciu.

Cvičenie 3.51. Platí veta 3.50 aj bez predpokladu $n \neq 0$?

Často budeme kódovať konečnú postupnosť čísel $a_0, a_1, \ldots, a_n$ ($a_n \neq 0$) číslom $\mathrm{p}_0^{a_0} \cdot \mathrm{p}_1^{a_1} \cdots \mathrm{p}_n^{a_n}$. Pri práci s takýmito kódmi bude pre nás užitočná funkcia z nasledujúcej definície.

Definícia 3.52. Pre všetky x, $y \in \mathbb{N}$

$$x * y = \begin{cases} 0, & \text{ak } x = 0 \text{ alebo } y = 0 \\ y, & \text{ak } x = 1 \text{ a } y \neq 0 \\ \left(\prod_{i=0}^{m-1} \mathrm{p}_i^{a_i}\right) \cdot \left(\prod_{j=0}^{n-1} \mathrm{p}_{j+m}^{b_j}\right) & \text{ak } x = \prod_{i=0}^{m-1} \mathrm{p}_i^{a_i},\ a_{m-1} \neq 0,\ y = \prod_{j=0}^{n-1} \mathrm{p}_j^{b_j} \end{cases}$$

Poznámka 3.53. Čitateľ si môže sám dokázať, že tento predpis jednoznačne určuje hodnoty $x * y$.

Poznámka 3.54. Ak x je kód postupnosti $(a_0, a_1, \ldots, a_{m-1})$, $a_{m-1} \neq 0$ a y je kód postupnosti $(b_0, b_1, \ldots, b_{n-1})$, tak $x * y$ je kód postupnosti $(a_0, a_1, \ldots, a_{m-1}, b_0, b_1, \ldots, b_{n-1})$. (Všetko v uvedenom kódovaní.) Hodnoty $x * y$ pre $x = 0$, $y = 0$ nie sú dôležité.

Príklad 3.55. Kód postupnosti $(4, 1, 3)$ je $2^4.3^1.5^3 = 6000$. Kód postupnosti $(1, 2, 1)$ je $2^1.3^2.5^1 = 90$. Platí

$$6000 * 90 = (2^4.3^1.5^3) * (2^1.3^2.5^1) = (2^4.3^1.5^3).(7^1.11^2.13^1) = 6606600,$$

a to je kód postupnosti $(4, 1, 3, 1, 2, 1)$.

Cvičenie 3.56. Dokážte, že pre všetky x, y, $z \in \mathbb{N}$ platí

$$(x * y) * z = x * (y * z), \tag{3.56.1}$$

teda že $*$ je asociatívna binárna operácia na množine $\mathbb{N}$. Je táto operácia komutatívna?

Poznámka 3.57. Podľa vzťahu (3.56.1) môžeme písať výraz $x_1 * x_2 * \cdots * x_n$ bez zátvoriek.

Veta 3.58. Funkcia $\lambda xy(x * y)$ je primitívne rekurzívna.

Príklad 3.63. Dokážeme niekoľkými spôsobmi primitívnu rekurzívnosť funkcie $f(x)$ danej predpisom

$$f(0) = 0, \qquad f(1) = 1, \qquad f(x+2) = f(x+1) + f(x),$$

t.j. Fibbonaciho postupnosti.

(a) Dokážeme najprv primitívnu rekurzívnosť funkcie $g(x) = \mathrm{c}(f(x), f(x+1))$. Platí

$$\begin{aligned} g(0) &= \mathrm{c}(0,1) = 1, \\ g(x+1) &= \mathrm{c}(f(x+1), f(x+2)) = \\ &= \mathrm{c}(f(x+1), f(x+1) + f(x)) = \\ &= \mathrm{c}(\mathrm{r}(g(x)), \mathrm{r}(g(x)) + \mathrm{l}(g(x))) \end{aligned}$$

Teda funkcia g je primitívne rekurzívna, lebo vzniká operáciou primitívnej rekurzie z primitívne rekurzívnych funkcií $\lambda(1)$, $\lambda xy(\mathrm{c}(\mathrm{r}(y), \mathrm{r}(y) + \mathrm{l}(y)))$.

(b) Môžeme postupovať rovnako ako v prípade (a), len zvoliť $g(x) = 2^{f(x)} \cdot 3^{f(x+1)}$ a používať funkcie $\mathrm{ex}_0(x)$, $\mathrm{ex}_1(x)$ namiesto funkcií $\mathrm{l}(x)$, $\mathrm{r}(x)$. (Nezáleží na tom, že z týchto funkcií nemožno vytvoriť trojicu číslovacích funkcií.)

(c) Dokážeme najprv primitívnu rekurzívnosť funkcie $h(x) = \mathrm{c}^{x+1}(f(0), f(1), \ldots, f(x))$. Pre $x \in \mathbb{N}$, $x \neq 0$ platí

$$\begin{aligned} f(x) &= \mathrm{r}(h(x)), \\ f(x-1) &= \mathrm{r}(\mathrm{l}(h(x))) \\ h(x+1) &= \mathrm{c}(h(x), \mathrm{r}(h(x)) + \mathrm{r}(\mathrm{l}(h(x)))) \end{aligned}$$

Tento vzťah upravíme tak, aby platil aj pre $x = 0$:

$$h(x+1) = \mathrm{c}(h(x), \mathrm{r}(h(x)) + \mathrm{r}(\mathrm{l}(h(x)))) + \overline{\mathrm{sg}}(x)$$

Posledný vzťah spolu so vzťahom $h(0) = 0$ definuje funkciu h primitívnou rekurziou z primitívne rekurzívnych funkcií. Teda funkcia h, a potom aj funkcia $f(x) = \mathrm{r}(h(x))$ je primitívne rekurzívna.

(d) Namiesto funkcie h z bodu (c) možno použiť funkciu

$$h(x) = \mathrm{p}_0^{f(0)} \cdot \mathrm{p}_1^{f(1)} \cdots \mathrm{p}_x^{f(x)}$$

Funkcia f sa dá vyjadriť pomocou funkcie h takto:

$$f(x) = \mathrm{ex}(\mathrm{npr}(h(x)) \dot{-} 1, h(x))$$

Podrobnosti dôkazu (podobné ako v bode (c)) necháme na rozmyslenie čitateľovi.

Príklad 3.64. Dokážeme, že funkcia

$$f(x) = \text{počet štvoriek v dekadickom zápise čísla } x!$$

je primitívne rekurzívna. Cifru na i-tom mieste čísla $x!$ (počítame od konca) môžeme vyjadriť vzorcom

$$\left\lfloor \frac{x!}{10^i} \right\rfloor \text{ MOD } 10$$

(ak i je väčšie alebo rovné počtu cifier čísla $x!$, dáva tento vzorec nulu). Výraz

$$\left| \left(\left\lfloor \frac{x!}{10^i} \right\rfloor \text{ MOD } 10 \right) - 4 \right|$$

sa rovná nule práve vtedy, keď cifra na i-tom mieste čísla $x!$ je štvorka. Ak pred tento výraz napíšeme $\overline{\mathrm{sg}}$, dostaneme jednotku práve vtedy, keď i-ta cifra čísla $x!$ je štvorka, inak dostaneme nulu. Stačí teraz tieto jednotky a nuly spočítať a dostaneme hľadaný počet štvoriek. Ak ešte upravíme nájdený výraz tak, aby v ňom vystupovali len primitívne rekurzívne funkcie a odhadneme zhora počet cifier čísla $x!$ samotným číslom $x!$, dostaneme pre funkciu f vzorec

$$f(x) = \sum_{i=0}^{x!} \overline{\mathrm{sg}} \left| \left(\left\lfloor \frac{x!}{10^i} \right\rfloor \text{ MOD } 10 \right) - 4 \right|$$

označíme F_x. Ak je F_x nulárna funkcia, označme G_x konštantnú unárnu funkciu s hodnotou F_x; ak je F_x n-árna funkcia, $n \neq 0$, označme

$$G_x = \mathcal{S}^{n+1}(F_x, \mathrm{c}_{n,1}, \ldots, \mathrm{c}_{n,n}) \tag{3.67.2}$$

Postupnosť F_0, F_1, F_2, ... obsahuje všetky primitívne rekurzívne funkcie, a preto postupnosť G_0, G_1, G_2, ... obsahuje všetky unárne primitívne rekurzívne funkcie. Teraz definujeme binárnu funkciu G predpisom

$$G(x, y) = G_x(y) \tag{3.67.3}$$

Funkcia G je zrejme univerzálna funkcia pre množinu všetkých unárnych primitívne rekurzívnych funkcií. Ukážeme teraz, že je algoritmicky vypočítateľná.

Usporiadajme množinu $\mathbb{N} \times \mathbb{N}$ lexikograficky: $(x_1, y_1) \prec (x_2, y_2)$ práve vtedy, keď $x_1 < x_2$ alebo $x_1 = x_2$ a $y_1 < y_2$. Ak chceme určiť hodnotu $G(x, y)$, musíme poznať hodnoty $G(u, v)$ pre konečný (možno nulový) počet dvojíc (u, v) menších ako (x, y). (Predpokladáme, že kódovanie a dekódovanie čísel pomocou funkcií c^n, $\mathrm{c}_{n,i}$ vieme robiť priamo a že vieme tiež robiť naraz také kroky výpočtu, ktoré sme robili naraz, prípadne to o nich mlčky predpokladali, aj pri výpočte hodnôt jednej primitívne rekurzívnej funkcie.)

Zvoľme teraz efektívne nejakú postupnosť usporiadaných dvojíc prirodzených čísel

$$(x_0, y_0), \quad (x_1, y_1), \quad (x_2, y_2), \quad \ldots \tag{3.67.4}$$

ktorá obsahuje každú usporiadanú dvojicu z $\mathbb{N} \times \mathbb{N}$ nekonečne mnohokrát. Pri počítaní hodnoty $G(x, y)$ budeme postupne dopĺňať tabuľku hodnôt funkcie G tak, že budeme brať postupne dvojice (x_i, y_i) z postupnosti (3.67.4), zakaždým skontrolujeme, či sú už doplnené miesta tabuľky bezprostredne potrebné pre určenie hodnoty $G(x_i, y_i)$ a ak áno, zapíšeme ju. Dá sa ukázať, že týmto spôsobom možno určiť každú hodnotu $G(x, y)$ (t.j. že nebudeme niektoré miesto tabuľky donekonečna obchádzať). Pri zaplnení miesta pre hodnotu $G(x, y)$ výpočet skončíme. Týmto postupom môžeme určiť každú hodnotu $G(x, y)$, a teda funkcia G je algoritmicky vypočítateľná.

Cvičenie 3.68. Uveďte algoritmus na postupné zostrojovanie členov postupnosti (3.67.1); vhodne si zvoľte usporiadanie výrazov rovnakej dĺžky.

Cvičenie 3.69. Zistite, pre ktoré dvojice potrebujeme poznať hodnotu funkcie G, aby sme mohli bezprostredne určiť hodnotu $G(x, y)$, ak $V_x = \mathcal{R}(V_a, V_b)$, V_x zodpovedá n-árnej funkcii (rozlíšte prípady $\mathrm{c}_{n,1}(y) = 0$, $\mathrm{c}_{n,1}(y) \neq 0$).

Cvičenie 3.70. Riešte úlohu z predchádzajúceho cvičenia, ak $V_x = \mathcal{S}^{n+1}(V_a, V_{b_1}, \ldots, V_{b_n})$.

Cvičenie 3.71. Riešte úlohu z cvičenia 3.69 pre $V_x = 0$, $V_x = s$ a $V_x = I^n_m$.

Cvičenie 3.72. Dokážte, že všetky nájdené dvojice v predchádzajúcich troch cvičeniach sú v lexikografickom usporiadaní menšie ako dvojica (x, y).

Cvičenie 3.73. Nájdite také dve unárne primitívne rekurzívne funkcie f, g, že postupnosť

$$(f(0), g(0)), \quad (f(1), g(1)), \quad (f(2), g(2)), \quad \ldots$$

obsahuje každú usporiadanú dvojicu prirodzených čísel nekonečne mnohokrát.

Cvičenie 3.74. Ukážte, že lexikografické usporiadanie dvojíc z $\mathbb{N} \times \mathbb{N}$ je dobré usporiadanie. Potom (s použitím cvičenia 3.72) dokážte, že uvedený algoritmus pre výpočet hodnôt funkcie G dá výsledok pre všetky $x, y \in \mathbb{N}$.

Našli sme príklad algoritmicky vypočítateľnej funkcie, ktorá nie je primitívne rekurzívna. Teda vidíme, že doterajšie operácie s funkciami nestačia na to, aby sme z funkcií 0, s, I^n_m dostali všetky algoritmicky vypočítateľné funkcie. Na to je nutné použiť ešte ďalšie operácie. (Samozrejme, nie je isté, či pridaním ďalších operácií tento cieľ dosiahneme; neskôr však uvidíme, že pridanie operácie regulárnej minimalizácie (prípadne minimalizácie, ak chceme dostať i čiastočné funkcie) takmer naisto stačí.) Preto definujeme:

Definícia 3.75. Funkciu f budeme nazývať *rekurzívnou funkciou*, ak f vzniká z funkcií 0, s, I^n_m $(1 \leq m \leq n)$ konečným počtom operácií skladania funkcií, primitívnej rekurzie a regulárnej minimalizácie.

KAPITOLA 4

Množiny a predikáty

V tejto kapitole sa budeme zaoberať predikátmi na množine $\mathbb{N}$ všetkých prirodzených čísel a množinami n-tíc prirodzených čísel. Rozšírime istým spôsobom pojmy primitívnej rekurzívnosti, rekurzívnosti a čiastočnej rekurzívnosti z čiastočných funkcií na množine $\mathbb{N}$ na predikáty na množine $\mathbb{N}$ a na množine n-tíc prirodzených čísel (pritom číslo n bude rovnaké pre všetky prvky každej uvažovanej množiny). Potom preskúmame základné vlastnosti týchto pojmov. K hlbšiemu štúdiu týchto vlastností sa ešte raz vrátime po dôkaze existencie univerzálnej čiastočne rekurzívnej funkcie pre množinu $\mathcal{P}^{(1)}$ všetkých unárnych čiastočne rekurzívnych funkcií. Potom dokážeme, okrem iného, obrátenia niektorých viet tejto kapitoly. V tejto kapitole budeme používať všetky dohody z kapitoly 3 (napríklad slová „na množine $\mathbb{N}$“ budeme často vynechávať).

Pri rozširovaní pojmov rekurzívnosti a primitívnej rekurzívnosti použijeme pojem charakteristickej funkcie z kapitoly 1.

Definícia 4.1. (a) Nech $n \in \mathbb{N}$ je ľubovoľné. Množinu M n-tíc prirodzených čísel budeme nazývať *(primitívne) rekurzívnou*, ak jej charakteristická funkcia je (primitívne) rekurzívna.

(b) Množinu M prirodzených čísel budeme nazývať *(primitívne) rekurzívnou*, ak je množina M^1 (primitívne) rekurzívna.

Definícia 4.2. Nech $n \in \mathbb{N}$ je ľubovoľné. n-árny predikát $P(x_1, \ldots, x_n)$ nazveme *(primitívne) rekurzívnym*, ak jeho charakteristická funkcia je (primitívne) rekurzívna.

Poznámka 4.3. V definíciach 4.1 a 4.2 sme nevylúčili prípad $n = 0$. Tým sa stalo, že množina $\{\emptyset\}$ „všetkých 0-tíc prirodzených čísel“ je (primitívne) rekurzívna, a že pravdivý výrok a nepravdivý výrok (ako 0-árne predikáty) sú (primitívne) rekurzívne. K bodu (b), definície 4.1 pripomíname, že $\mathbb{N}^1 \neq \mathbb{N}$, t.j. „množina všetkých 1-tíc prirodzených čísel“ sa nerovná množine $\mathbb{N}$.

Poznámka 4.4. Podľa poznámky 1.39 o vzťahoch medzi predikátom, jeho charakteristickou funkciou a jeho oborom pravdivosti nemôže nám tu urobené rozšírenie pojmov dať podstatne nové metódy skúmania (primitívne) rekurzívnych funkcií. Môže nám však pomôcť pri odstraňovaní technických ťažkostí s príliš zdĺhavými dôkazmi a podobne.

Cvičenie 4.5. Dokážte, že nasledujúce množiny sú primitívne rekurzívne:

(a) prázdna množina $\emptyset$
(b) množina $\mathbb{N}^n$ pre ľubovoľné $n \in \mathbb{N}$
(c) množina všetkých párnych čísel
(d) množina všetkých nepárnych čísel
(e) množina všetkých prvočísel
(f) množina všetkých tretích mocnín prirodzených čísel
(g) množina všetkých takých (usporiadaných) dvojíc (x, y) (prirodzených) čísel, že $x = y^2$
(h) množina všetkých takých dvojíc (x, y), že x je deliteľom čísla y
(i) množina všetkých takých dvojíc (x, y), že x je násobkom čísla y
(j) množina všetkých takých trojíc (x, y, z), že x je počet núl v dekadickom zápise čísla y^z
(k) množina všetkých takých trojíc (x, y, z), že číslo x sa dá písať ako súčet y z-tých mocnín prirodzených čísel
(l) množina všetkých takých dvojíc (x, y), že číslo $x + y$ je párne

Cvičenie 4.6. Dokážte, že nasledujúce predikáty sú primitívne rekurzívne:

(a) x je párne číslo
(b) x je prvočíslo
(c) x je mocninou 2
(d) x je deliteľom y

Veta 4.12. Nech $P(x_1, \ldots, x_n, z)$ je (primitívne) rekurzívny predikát, $f(x_1, \ldots, x_n)$ je (primitívne) rekurzívna funkcia. Potom aj predikáty

$$(\exists z)\,(z \leq f(x_1, \ldots, x_n) \wedge P(x_1, \ldots, x_n, z)) \tag{4.12.1}$$

$$(\forall z)\,(z \leq f(x_1, \ldots, x_n) \implies P(x_1, \ldots, x_n, z)) \tag{4.12.2}$$

sú (primitívne) rekurzívne.

Dôkaz: Nech $\chi_P(x_1, \ldots, x_n, z)$ je charakteristická funkcia predikátu $P(x_1, \ldots, x_n, z)$. Potom funkcia $\chi(x_1, \ldots, x_n) = \prod_{i=0}^{f(x_1,\ldots,x_n)} \chi_P(x_1, \ldots, x_n, i)$ je charakteristická funkcia predikátu (4.12.1). Pretože funkcia $\chi(x_1, \ldots, x_n)$ je (primitívne) rekurzívna, je aj predikát (4.12.1) (primitívne) rekurzívny. Predikát (4.12.2) je ekvivalentný s predikátom

$$\neg\,(\exists z)\,(z \leq f(x_1, \ldots, x_n) \wedge \neg P(x_1, \ldots, x_n, z))$$

a teda je tiež (primitívne) rekurzívny podľa už dokázanej časti vety 4.12 a podľa vety 4.10. □

Dohoda 4.13. Predikáty (4.12.1) a (4.12.2) budeme skrátene zapisovať takto:

$$(\exists z \leq f(x_1, \ldots, x_n))\,P(x_1, \ldots, x_n, z) \tag{4.13.1}$$

$$(\forall z \leq f(x_1, \ldots, x_n))\,P(x_1, \ldots, x_n, z) \tag{4.13.2}$$

Výrazy $(\exists z \leq f(x_1, \ldots, x_n))$, $(\forall z \leq f(x_1, \ldots, x_n))$ budeme nazývať ohraničenými kvantifikátormi.

Veta 4.14. Ak je $P(x_1, \ldots, x_m)$ (primitívne) rekurzívny predikát,

$$f_1(y_{1,1}, \ldots, y_{1,n_1}), \ldots, f_m(y_{m,1}, \ldots, y_{m,n_m})$$

sú (primitívne) rekurzívne funkcie, tak predikát $P(f_1(y_{1,1}, \ldots, y_{1,n_1}), \ldots, f_m(y_{m,1}, \ldots, y_{m,n_m}))$ je (primitívne) rekurzívny.

Poznámka 4.15. Obdobne ako vo vete 4.10, ani tu nepredpokladáme, že premenné $y_{i,j}$, $i = 1, \ldots, m$, $j = 1, \ldots, n_i$ sú po dvoch rôzne.

Dôkaz vety 4.14: Ak je $\chi(x_1, \ldots, x_n)$ charakteristická funkcia predikátu $P(x_1, \ldots, x_n)$, tak (primitívne) rekurzívna funkcia $\chi(f_1(y_{1,1}, \ldots, y_{1,n_1}), \ldots, f_m(y_{m,1}, \ldots, y_{m,n_m}))$ je charakteristická funkcia predikátu z vety 4.14, a teda tento predikát je (primitívne) rekurzívny. □

Operácia minimalizácie, tak ako bola zavedená v definícii 3.22, dáva z čiastočnej funkcie g čiastočnú funkciu f; vo vzťahu (3.22.1) však vidíme, že čiastočná funkcia g bola vlastne použitá na vytvorenie predikátu $g(y, x_1, \ldots, x_n) = 0$, a až z neho bola vytvorená čiastočná funkcia f. Bude teda asi niekedy výhodnejšie mať možnosť tvoriť čiastočnú funkciu f priamo z predikátu. Preto definujeme:

Definícia 4.16. Nech $P(y, x_1, \ldots, x_n)$ je $(n+1)$-árny predikát. Pre ľubovoľné $x_1, \ldots, x_n \in \mathbb{N}$ označíme

$$\min_y P(y, x_1, \ldots, x_n) \tag{4.16.1}$$

také najmenšie číslo a, že platí $P(a, x_1, \ldots, x_n)$.

Poznámka 4.17. Označenia $\min_y$, μ_y majú trochu odlišný význam; pri označení μ_y nám záleží aj na tom, či príslušná funkcia je definovaná pre hodnoty menšie ako výsledok minimalizácie, kým pri označení $\min_y$ podobná otázka vôbec nemusí mať zmysel, a ak aj má, tak ju neskúmame.

Cvičenie 4.18. Nájdite takú $(n+1)$-árnu čiastočnú funkciu f, že čiastočné funkcie

$$\lambda x_1 \ldots x_n \big(\mu_y\,(f(y, x_1, \ldots, x_n) = 0)\big) \tag{4.18.1}$$

$$\lambda x_1 \ldots x_n \big(\min_y\,(f(y, x_1, \ldots, x_n) = 0)\big) \tag{4.18.2}$$

budú navzájom rôzne.

Cvičenie 4.19. Ak f je $(n+1)$-árna totálna funkcia, tak sa čiastočné funkcie (4.18.1), (4.18.2) navzájom rovnajú. Dokážte!

Uvedieme teraz dve vety o tom, kedy operátor min dáva z (primitívne) rekurzívneho predikátu (primitívne) rekurzívnu funkciu.

Definícia 4.32. (a) Nech $n \in \mathbb{N}$ je ľubovoľné, nech M je množina n-tíc prirodzených čísel a f je $(n+1)$-árna čiastočná funkcia. Budeme hovoriť, že čiastočná funkcia f je *priradená* množine M, ak pre všetky $x_1, \ldots, x_n \in \mathbb{N}$ platí

$$(x_1, \ldots, x_n) \in M \text{ práve vtedy, keď existuje } y \in \mathbb{N} \text{ také, že } f(y, x_1, \ldots, x_n) = 0 \qquad (4.32.1)$$

(b) Ak $M \subseteq \mathbb{N}$, budeme hovoriť, že f je *priradená* množine M, ak f je priradená množine M^1.

(c) Budeme hovoriť, že $(n+1)$-árna čiastočná funkcia f je *priradená* n-árnemu predikátu $P(x_1, \ldots, x_n)$, ak pre všetky $x_1, \ldots, x_n \in \mathbb{N}$ platí

$$P(x_1, \ldots, x_n) \text{ práve vtedy, keď existuje } y \in \mathbb{N} \text{ také, že } f(y, x_1, \ldots, x_n) = 0 \qquad (4.32.2)$$

Poznámka 4.33. K jednej množine, resp. jednému predikátu je priradených nekonečne mnoho čiastočných funkcií a medzi nimi aj nekonečne mnoho totálnych funkcií.

Definícia 4.34. Množinu M n-tíc prirodzených čísel, resp. množinu M prirodzených čísel nazveme *rekurzívne spočítateľnou*, ak existuje rekurzívna funkcia f priradená množine M.

Definícia 4.35. Predikát $P(x_1, \ldots, x_n)$ nazveme *rekurzívne spočítateľným*, ak existuje rekurzívna funkcia f priradená predikátu P.

Poznámka 4.36. (a) Predikát je rekurzívne spočítateľný práve vtedy, keď jeho obor pravdivosti je rekurzívne spočítateľný.

(b) Ako neskôr uvidíme, mohli by sme v definíciách 4.34, 4.35 namiesto rekurzívnej funkcie f použiť čiastočne rekurzívnu funkciu f alebo primitívne rekurzívnu funkciu f. V prvom prípade by sme dostali zdanlivo všeobecnejší pojem a v druhom zdanlivo špeciálnejší pojem; v skutočnosti by sme však dostali ekvivalentné pojmy.

Namiesto triviálnych príkladov rekurzívne spočítateľných množín a predikátov uvedieme ihneď nasledujúcu vetu.

Veta 4.37. (a) Každá rekurzívna množina je rekurzívne spočítateľná.

(b) Každý rekurzívny predikát je rekurzívne spočítateľný.

Dôkaz: Nech $M \subseteq \mathbb{N}^n$ je rekurzívna množina a $f(x_1, \ldots, x_n)$ je charakteristická funkcia. Potom f je rekurzívna, a teda aj funkcia $g(y, x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$ je rekurzívna a je to funkcia priradená k množine M. Teda množina M je rekurzívne spočítateľná. Dôkaz tvrdenia (b) je obdobný. □

Poznámka 4.38. Neskôr dokážeme, že ani jedno z tvrdení vety 4.37 sa nedá obrátiť.

Veta 4.39. Nech n je prirodzené číslo a $M_1 \subseteq \mathbb{N}^n$, $M_2 \subseteq \mathbb{N}^n$ sú rekurzívne spočítateľné množiny. Potom aj množiny $M_1 \cup M_2$, $M_1 \cap M_2$ sú rekurzívne spočítateľné.

Dôkaz: Nech $f(y, x_1, \ldots, x_n)$, $g(y, x_1, \ldots, x_n)$ sú rekurzívne funkcie priradené množinám M_1, M_2. Potom množinám $M_1 \cup M_2$, $M_1 \cap M_2$ sú priradené napríklad funkcie

$$h_1(y, x_1, \ldots, x_n) = f(y, x_1, \ldots, x_n) \,.\, g(y, x_1, \ldots, x_n) \qquad (4.39.1)$$

$$h_2(y, x_1, \ldots, x_n) = f(l(y), x_1, \ldots, x_n) + g(r(y), x_1, \ldots, x_n) \qquad (4.39.2)$$

ktoré sú samozrejme rekurzívne. Preto sú aj množiny $M_1 \cup M_2$, $M_1 \cap M_2$ rekurzívne spočítateľné.

Ukážeme podrobnejšie, že h_2 je priradená množina $M_1 \cap M_2$. Ak $h_2(y, x_1, \ldots, x_n) = 0$, tak $f(l(y), x_1, \ldots, x_n) = 0$ a $g(r(y), x_1, \ldots, x_n) = 0$, teda $(x_1, \ldots, x_n) \in M_1$, $(x_1, \ldots, x_n) \in M_2$. Obrátene, ak $(x_1, \ldots, x_n) \in M_1$, $(x_1, \ldots, x_n) \in M_2$, tak existujú u, v také, že $f(u, x_1, \ldots, x_n) = 0$, $g(v, x_1, \ldots, x_n) = 0$. Potom pre $y = c(u, v)$ platí $h_2(y, x_1, \ldots, x_n) = 0$. □

Veta 4.40. Nech m, n sú ľubovoľné prirodzené čísla a $M_1 \subseteq \mathbb{N}^m$, $M_2 \subseteq \mathbb{N}^n$ sú rekurzívne spočítateľné množiny. Potom aj množina všetkých $(m+n)$-tíc $(a_1, \ldots, a_m, a_{m+1}, \ldots, a_{m+n})$ takých, že $(a_1, \ldots, a_m) \in M_1$ a $(a_{m+1}, \ldots, a_{m+n}) \in M_2$ je rekurzívne spočítateľná. Stručnejšie povedané, kartézsky súčin rekurzívne spočítateľných množín je rekurzívne spočítateľný.

Dôkaz: Ak f_1, f_2 sú rekurzívne spočítateľné funkcie priradené množinám M_1, M_2, tak rekurzívna funkcia priradená množine $(m+n)$-tíc z vety je napríklad funkcia g daná predpisom

$$g(t, x_1, \ldots, x_m, y_1, \ldots, y_n) = f_1(l(t), x_1, \ldots, x_m) + f_2(r(t), y_1, \ldots, y_n)$$

Podrobné overenie ponechávame na čitateľa. □

Dôkaz: Nech g je $(n+2)$-árna rekurzívna funkcia priradená ku grafu n-árnej čiastočnej funkcie f. Definujme čiastočnú funkciu h predpisom

$$h(x_1, \ldots, x_n) = \mu_y (g(l(y), x_1, \ldots, x_n, r(y)) = 0) \tag{4.49.1}$$

Potom hodnota $h(x_1, \ldots, x_n)$ je definovaná práve vtedy, keď hodnota $f(x_1, \ldots, x_n)$ je definovaná. Ďalej platí

$$f(x_1, \ldots, x_n) = r(h(x_1, \ldots, x_n)) \tag{4.49.2}$$

Z týchto vyjadrení vidno, že f je čiastočne rekurzívna funkcia, čo bolo treba dokázať. □

Poznámka 4.50. Aj obrátenie vety 4.49 dokážeme v kapitole 6.

Vzhľadom na poznámku 4.36 sú vlastnosti rekurzívne spočítateľných predikátov veľmi podobné vlastnostiam rekurzívne spočítateľných množín. Preto ich uvedieme väčšinou bez dôkazov, ktoré nechávame pre čitateľa ako cvičenie. Len v prípade, keď analogická vlastnosť pre množiny nebola explicitne formulovaná (čo ale neznamená, že by sa nedala formulovať) podáme, alebo aspoň naznačíme dôkazy.

Veta 4.51. Nech $P(x_1, \ldots, x_n)$, $Q(y_1, \ldots, y_n)$ sú rekurzívne spočítateľné predikáty (pričom nežiadame, aby premenné $x_1, \ldots, x_n, y_1, \ldots, y_n$ boli po dvoch rôzne). Potom aj predikáty

$$P(x_1, \ldots, x_n) \wedge Q(y_1, \ldots, y_n)$$
$$P(x_1, \ldots, x_n) \vee Q(y_1, \ldots, y_n)$$

sú rekurzívne spočítateľné.

Veta 4.52. Ak $P(y, x_1, \ldots, x_n)$ je rekurzívne spočítateľný predikát, tak aj predikát

$$(\exists y) P(y, x_1, \ldots, x_n)$$

je rekurzívne spočítateľný.

Poznámka 4.53. Ako ukážeme neskôr, logické spojky $\Longrightarrow$, $\Longleftrightarrow$, $\neg$ nezachovávajú rekurzívnu spočítateľnosť predikátov a vo vete 4.52 nemožno písať $\forall$ namiesto $\exists$.

Veta 4.54. Nech $P(y, x_1, \ldots, x_n)$ je rekurzívne spočítateľný predikát a $f(x_1, \ldots, x_n)$ je rekurzívna funkcia. Potom aj predikáty

$$(\exists y \leq f(x_1, \ldots, x_n)) P(y, x_1, \ldots, x_n) \tag{4.54.1}$$
$$(\forall y \leq f(x_1, \ldots, x_n)) P(y, x_1, \ldots, x_n) \tag{4.54.2}$$

sú rekurzívne spočítateľné.

Dôkaz: Rekurzívna spočítateľnosť predikátu (4.54.1) bezprostredne vyplýva z viet 4.51, 4.52. Pre dôkaz (4.54.2) predpokladajme, že $g(z, y, x_1, \ldots, x_n)$ je rekurzívna funkcia, ktorá je priradená k predikátu $P(y, x_1, \ldots, x_n)$. Položme pre všetky $z, y, x_1, \ldots, x_n$

$$g_1(z, y, x_1, \ldots, x_n) = \prod_{j=0}^{z} g(j, y, x_1, \ldots, x_n)$$

Aj funkcia g_1 je rekurzívna a priradená predikátu P; navyše, ak $g_1(z_0, y, x_1, \ldots, x_n) = 0$, tak $g_1(z, y, x_1, \ldots, x_n) = 0$ pre všetky $z \geq z_0$. Teraz položme

$$h(z, x_1, \ldots, x_n) = \sum_{i=0}^{f(x_1 \ldots, x_n)} g_1(z, i, x_1, \ldots, x_n)$$

Ľahko sa overí, že h je rekurzívna funkcia priradená predikátu (4.54.2). □

Cvičenie 4.55. Dokážte rekurzívnu spočítateľnosť predikátu (4.54.1) obdobným spôsobom ako bola dokázaná rekurzívna spočítateľnosť predikátu (4.54.2).

KAPITOLA 5

Registrové stroje

V kapitole 3 sme skúmali niekoľko operácií, ktoré dávali z (čiastočne) algoritmicky vypočítateľných funkcií znova (čiastočne) algoritmicky vypočítateľné funkcie. Pritom však nebolo dopredu určené, aké kroky výpočtu možno urobiť naraz, bez ich rozkladania na ešte jednoduchšie kroky. V tejto kapitole vyjdeme naopak od veľmi elementárnych základných krokov, a to pripočítania jednotky, odčítania jednotky a podmieneného skoku podľa nuly. Ukážeme, že už tieto základné kroky stačia na výpočet hodnôt všetkých čiastočne rekurzívnych funkcií.

Prv ako uvedieme presnú matematickú definíciu registrových strojov, ktoré budeme niekedy v ďalšom texte nazývať len strojmi alebo M-strojmi, opíšeme neformálne ich činnosť. K tomuto neformálnemu opisu sa budeme i neskôr často vracať, lebo jeho použitie značne sprehľadní dôkazy; ich nahradenie presnými dôkazmi je ľahké, i keď často zdĺhavé. Registrové stroje nie sú technické alebo fyzikálne zariadenia, ale len matematické abstrakcie, ktoré však možno (s istými ohraničeniami) realizovať i technicky, dnes pravdepodobne najľahšie použitím samočinného počítača, ktorý by simuloval ich činnosť. Registrový stroj pracuje v diskrétnom čase, to znamená, že robí jednotlivé kroky v nejakej postupnosti časových okamihov, v každom okamihu z tejto postupnosti jeden krok. Má konečnú množinu vnútorných stavov, v ktorých sa môže nachádzať; jeho činnosť v istom časovom okamihu závisí od vnútorného stavu, v ktorom sa práve nachádza. Ďalej má konečne mnoho registrov R_j, do každého z ktorých môže uložiť jedno ľubovoľne veľké prirodzené číslo. (Práve táto podmienka, uloženie ľubovoľne veľkého prirodzeného čísla do jedného registra, alebo hoci aj do celej pamäti stroja, sa nedá technicky realizovať; ľahko sa však dá dosiahnuť, že počas veľmi dlhého času sa tieto ohraničenia neprejavia.) V každom kroku svojej činnosti pracuje registrový stroj s jedným svojím registrom, ktorý závisí len od momentálneho vnútorného stavu q_i stroja. Obsah tohto registra R_j stroj zmení (najviac o jednotku) a prejde do nasledujúceho vnútorného stavu q_k. Spôsob zmeny obsahu registra R_j i vnútorný stav q_k závisí od q_i a pôvodného obsahu registra R_j. Potom sa robí ďalší krok výpočtu atď., až sa stroj dostane do takého vnútorného stavu, pri ktorom je predpísané zastavenie (resp. nie je určená ďalšia činnosť). Pred začiatkom výpočtu uložíme vstupné údaje do niektorých registrov stroja a po ukončení výpočtu čítame výsledok z určeného registra.

Pristúpime teraz k matematickým definíciám vyššie spomenutých pojmov.

Definícia 5.1. (a) Symboly $q_0, q_1, q_2, \ldots$ budeme nazývať *vnútornými stavmi.* Množinu $\{q_i \mid i \in \in \mathbb{N}\}$ budeme značiť $\overline{Q}$.

(b) Symboly $R_0, R_1, R_2, \ldots$ budeme nazývať *registrami.*

Definícia 5.2. Usporiadané štvorice tvarov

$$(q_i R_j q_m q_n), \quad (q_i R_j P q_k), \quad (q_i R_j M q_k) \tag{5.2.1}$$

budeme nazývať *Minského inštrukciami*, prípadne len *inštrukciami.* (Budeme ich písať bez čiarok.)

Definícia 5.3. Konečnú množinu Minského inštrukcií, ktorá neobsahuje dve rôzne inštrukcie s rovnakým prvým prvkom, budeme nazývať *registrovým strojom.*

Definícia 5.4. Usporiadané dvojice tvaru

$$(q_i, (a_0, a_1, a_2, \ldots)), \tag{5.4.1}$$

kde q_i je vnútorný stav a $(a_0, a_1, a_2, \ldots)$ je postupnosť prirodzených čísel, ktorá má len konečne mnoho nenulových členov, budeme nazývať *stavmi registrových strojov*, prípadne len *stavmi* alebo *M-stavmi.*

Dohoda 5.5. Miesto (5.4.1) budeme používať označenie

$$(q_i; a_0, a_1, a_2, \ldots) \tag{5.5.1}$$

Definícia 5.12. (a) Konečnú postupnosť stavov $X_0, X_1, \ldots, X_n$ nazveme *výpočtom registrového stroja Z zo stavu X_0*, ak $X_i \xrightarrow{Z} X_{i+1}$ pre všetky $i = 0, 1, \ldots, n-1$ a neexistuje taký stav X_{n+1}, že $X_n \xrightarrow{Z} X_{n+1}$.

(b) Nekonečnú postupnosť stavov $X_0, X_1, \ldots, X_n, \ldots$ nazveme *výpočtom registrového stroja Z zo stavu X_0*, ak pre všetky $i = 0, 1, 2, \ldots$ platí $X_i \xrightarrow{Z} X_{i+1}$.

Definícia 5.13. (a) Nech X, Y sú stavy, Z je registrový stroj. Budeme písať $X \overset{Z}{\Longrightarrow} Y$, ak existuje taká konečná postupnosť stavov $X_0, X_1, \ldots, X_n$, že platí $X = X_0$, $Y = X_n$ a pre všetky $i = 0, 1, \ldots, n-1$ platí $X_i \xrightarrow{Z} X_{i+1}$.

(b) Budeme písať $X \overset{Z}{\longmapsto} Y$, ak $X \overset{Z}{\Longrightarrow} Y$ a neexistuje taký stav T, že $Y \xrightarrow{Z} T$.

Cvičenie 5.14. Dokážte, že pre každý registrový stroj Z a každý stav X existuje práve jeden výpočet stroja Z zo stavu X!

Cvičenie 5.15. Dokážte, že pre každý registrový stroj Z je relácia $\overset{Z}{\Longrightarrow}$ reflexívna a tranzitívna! Nájdite taký registrový stroj Z, že relácia $\overset{Z}{\Longrightarrow}$

(a) je symetrická,

(b) je slabo antisymetrická (t.j. zo vzťahov $X \overset{Z}{\Longrightarrow} Y$, $Y \overset{Z}{\Longrightarrow} X$ vyplýva $X = Y$)!

Cvičenie 5.16. Je pre nejaký stroj Z relácia $\overset{Z}{\Longrightarrow}$

(a) usporiadaním

(b) čiastočným usporiadaním množiny všetkých stavov registrových strojov?

Budeme sa teraz zaoberať možnosťou počítania hodnôt čiastočných funkcií na množine $\mathbb{N}$ na registrových strojoch. Pri počítaní hodnoty n-árnej čiastočnej funkcie f na stroji Z by sme mohli hodnoty argumentov $x_1, \ldots, x_n$ uložiť do ľubovoľných n pevne zvolených registrov a výsledok čítať po ukončení výpočtu z ľubovoľného pevne zvoleného registra (hoci aj z registra, na ktorom bola pôvodne uložená niektorá hodnota argumentu). Tieto možnosti budeme niekedy využívať pri dôkazoch. Teraz však zvolíme ukladanie argumentov a výsledku pevne; pri výpočte hodnoty n-árnej čiastočnej funkcie na stroji Z ukladáme hodnoty argumentov postupne do registrov R_1, R_2, $\ldots$, R_n a výsledok čítame z registra R_0. (Vždy predpokladáme, že stroj Z má, resp. že mu pridávame, všetky registre, ktoré potrebuje pre príslušný výpočet.) Formálne definujeme:

Definícia 5.17. Nech $n \in \mathbb{N}$, Z je registrový stroj a f je n-árna čiastočná funkcia na množine $\mathbb{N}$. Budeme hovoriť, že stroj Z *počíta* n-árnu čiastočnú funkciu f, a písať $f = \Phi^n_Z$, ak pre všetky $x_1, \ldots, x_n, y \in \mathbb{N}$ platí $f(x_1, \ldots, x_n) = y$ práve vtedy, keď existujú také čísla $b_1, \ldots, b_k \in \mathbb{N}$, že

$$(q_1; 0, x_1, \ldots, x_n) \overset{Z}{\longmapsto} (q_0; y, b_1, \ldots, b_k) \tag{5.17.1}$$

(T.j. že výpočet stroja Z zo stavu $(q_1; 0, x_1, \ldots, x_n)$ sa končí stavom $(q_0; y, b_1, \ldots, b_k)$.)

Príklad 5.18. Určíme pre registrový stroj $Z = \{(q_1 R_1 q_2 q_0), (q_2 R_1 M q_3), (q_3 R_0 P q_1)\}$ čiastočnú funkciu Φ^1_Z. Sledujme výpočet z okamžitého opísania $(q_1; y, x)$. Pre $x = 0$ má tento výpočet len dva členy, $(q_1; y, 0)$ a $(q_0; y, 0)$. Pre $x \neq 0$ a každé y platí

$$(q_1; y, x) \xrightarrow{Z} (q_2; y, x)$$

$$(q_2; y, x) \xrightarrow{Z} (q_3; y, x-1)$$

$$(q_3; y, x-1) \xrightarrow{Z} (q_1; y+1, x-1)$$

a teda

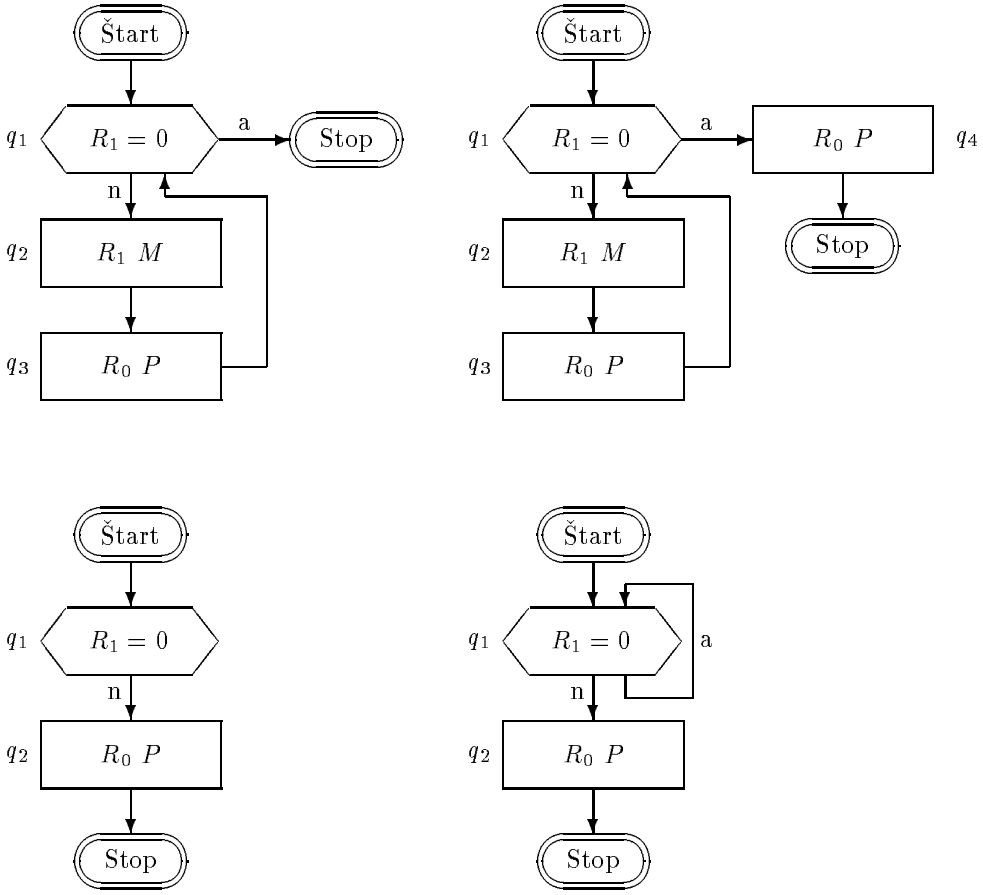
$$(q_1; y, x) \overset{Z}{\Longrightarrow} (q_1; y+1, x-1)$$

Z posledného vzťahu môžeme indukciou dokázať

$$(q_1; y, x) \overset{Z}{\Longrightarrow} (q_1; y+x, 0)$$

Podľa úvahy urobenej na začiatku potom platí

$$(q_1; y, x) \overset{Z}{\longmapsto} (q_0; y+x, 0)$$



Obr. 5.1.

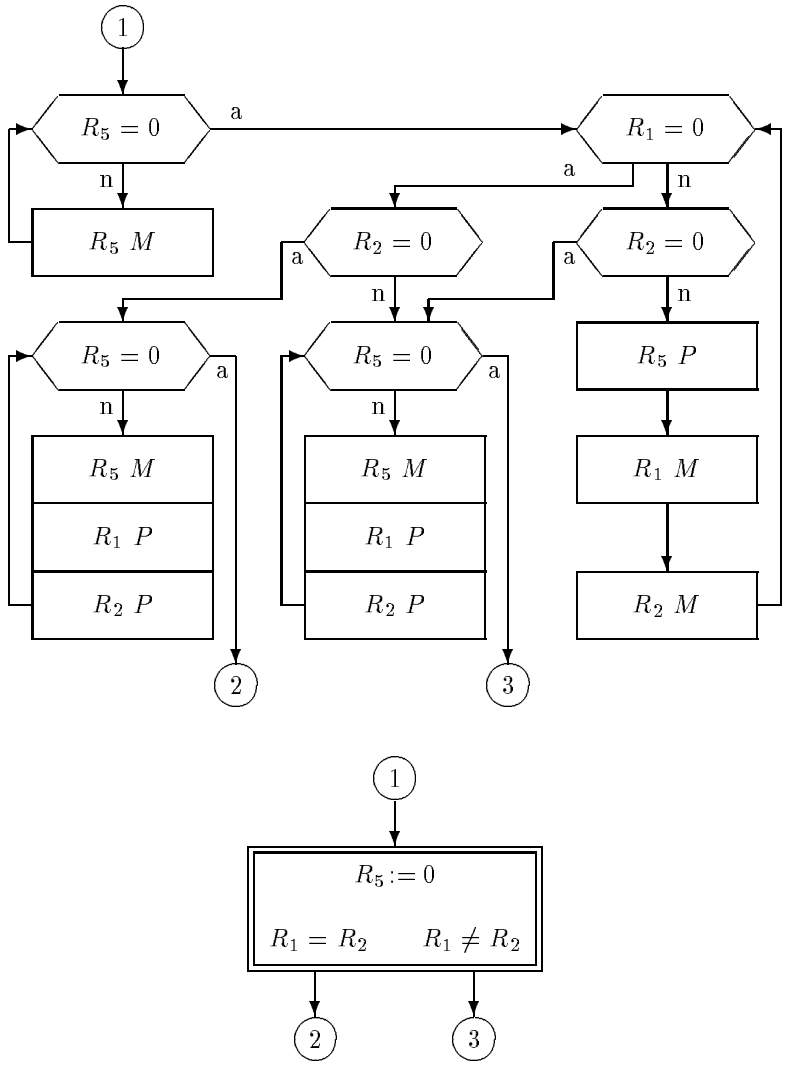
(7) K obdĺžnikom a šesťuholníkom pripíšeme vnútorné stavy, ktorými sa začínajú k nim patriace inštrukcie.

Príklad 5.27. Blokové schémy priradené podľa predchádzajúcej definície strojom z príkladov 5.18, 5.20, 5.22 sú na obrázku 5.1.

Poznámka 5.28. Registrový stroj je svojou blokovou schémou jednoznačne určený, až na vnútorné stavy rôzne od q_0 nachádzajúce sa len na tretích a štvrtých miestach jeho inštrukcií. Aby však platila i obrátená veta, museli by sme definovať blokové schémy registrových strojov napríklad ako vhodné ohodnotené orientované grafy, a tým abstrahovať od rôznych možností nakreslenia tej istej schémy.

Poznámka 5.29. Na to, aby bola určená činnosť registrového stroja (špeciálne, aby boli určené čiastočné funkcie, ktoré stroj počíta), stačí jeho bloková schéma dokonca bez dopísaných vnútorných stavov podľa bodu (7) definície 5.26. Bloková schéma je obvykle prehľadnejšia ako zápis stroja ako množiny inštrukcií. Preto je často výhodné pri konštrukcii registrového stroja najprv nakresliť jeho blokovú schému bez vyznačených vnútorných stavov, potom ich vhodne doplniť, a až nakoniec vypísať inštrukcie stroja.

Pri zostavovaní blokových schém nebudeme vždy postupovať striktne podľa definície 5.26, ale v tých prípadoch, kde to bude výhodné a kde nebude hroziť nedorozumenie, budeme pracovať s blokovými schémami voľnejšie. Niektoré časté odchýlky od definície 5.26 uvedieme teraz:



Obr. 5.2.

- $f_7(x, y) = |x - y|$

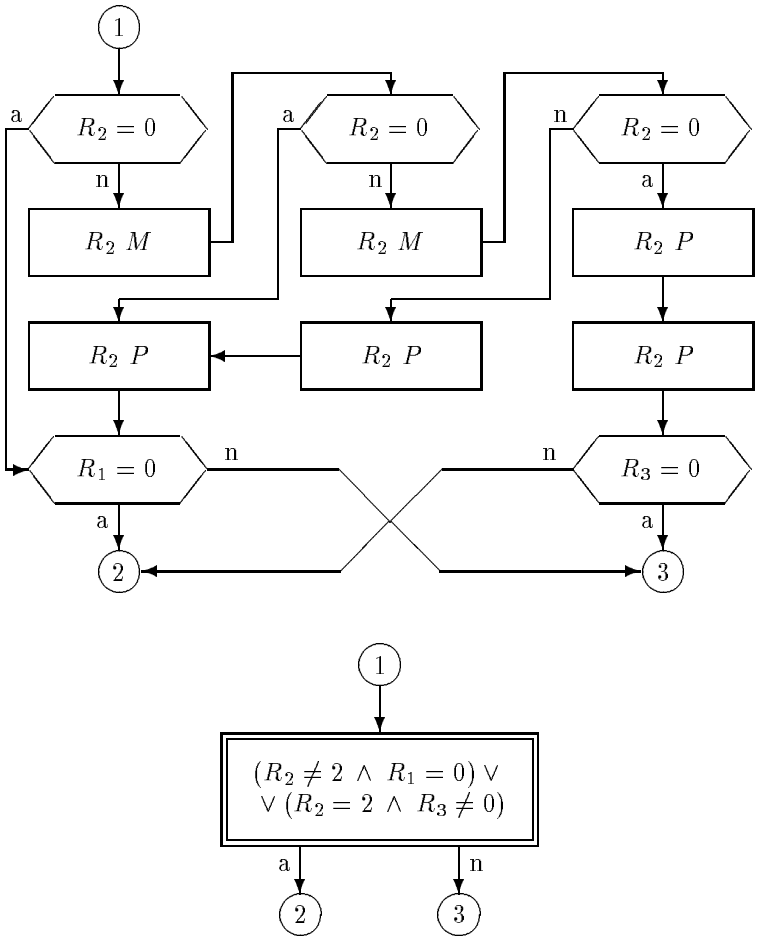
Cvičenie 5.34. Nakreslite schému registrového stroja, ktorý počíta čiastočnú charakteristickú funkciu množiny všetkých prvočísel!

Cvičenie 5.35. Vypracujte algoritmus na pripisovanie vnútorných stavov k súvislej blokovej schéme registrového stroja so začiatkovým oválom, v ktorej toto vyznačenie chýba! (Blokovú schému nazveme súvislou, ak sa môžeme ku každému jej šesťuholníku, alebo obdĺžniku dostať zo začiatkového oválu pohybom po jej šípkach, prípadne i proti ich smeru.)

Vrátime sa teraz ku skúmaniu čiastočných funkcií na množine $\mathbb{N}$ (slová „na množine $\mathbb{N}$“ budeme obvykle zasa vynechávať).

Definícia 5.36. (Čiastočnú) funkciu f nazveme *(čiastočne) vypočítateľnou na registrovom stroji*, ak existuje registrový stroj Z a také číslo n, že $f = \Phi^n_Z$.

Dohoda 5.37. Zatiaľ budeme slová „na registrovom stroji“ vynechávať. Ak bude v neskorších odsekoch potrebné odlíšenie od iných druhov (čiastočnej) vypočítateľnosti, budeme niekedy hovoriť o (čiastočnej) M-vypočítateľnosti. Obdobne ako v prípade čiastočnej rekurzívnosti budeme sa



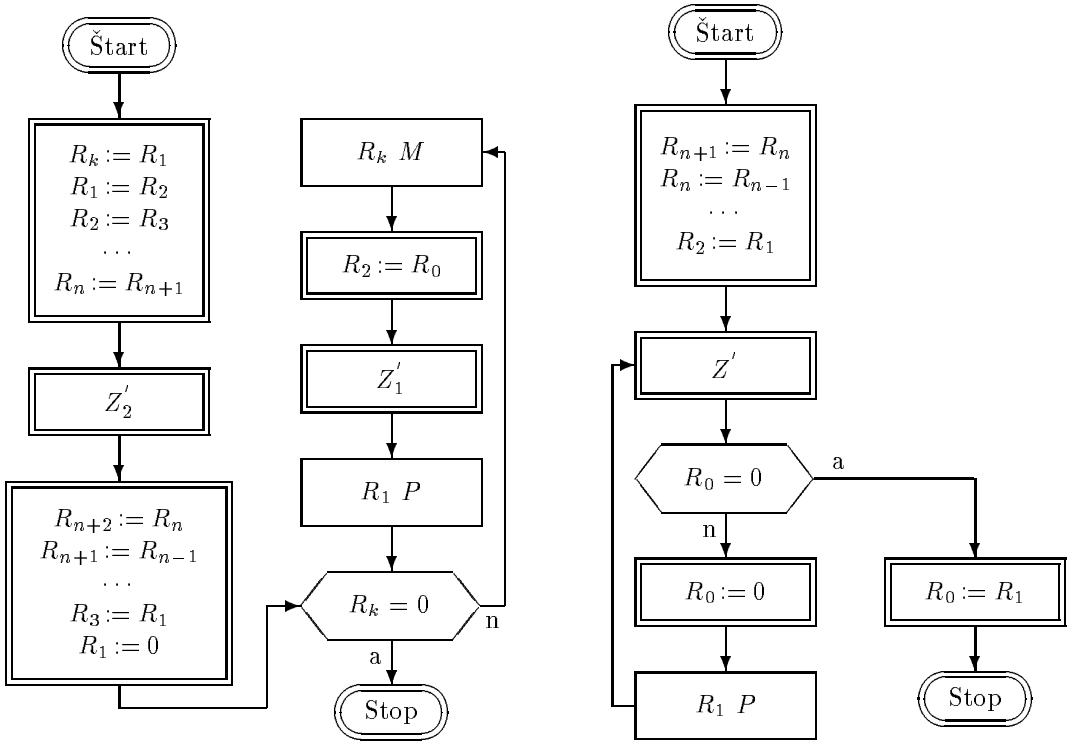
Obr. 5.4.

t taký najmenší index, že index vnútorného stavu A_t je väčší ako n. Také t zrejme existuje a príslušný vnútorný stav je q_{n+1}. Potom postupnosti $A_0, A_1, \ldots, A_t$ a $A_t, A_{t+1}, \ldots, A_s$ sú výpočty strojov Z_1', Z_2'. Vhodnou zmenou vnútorných stavov v týchto postupnostiach dostaneme z týchto výpočtov výpočty strojov Z_1, Z_2. Postupnosť $(c_0, c_1, \ldots)$ teda stačí zvoliť tak, aby platilo $A_t = (q_{n+1}; c_0, c_1, \ldots)$. Pre dôkaz druhej implikácie treba obdobným spôsobom zostaviť z výpočtov strojov Z_1, Z_2 výpočet stroja Y. □

Poznámka 5.39. Všimnime si, že sme nielen dokázali platnosť vety 5.38, ale sme i našli efektívny predpis na zostrojenie stroja Y zo strojov Z_1, Z_2. Aj od čitateľa budeme vyžadovať, aby nasledujúce cvičenia riešil, prípadne vety dokazoval obdobným spôsobom. Pritom, pravda, nemusí zakaždým vypisovať celý predpis na nájdenie požadovaného stroja, ale môže využívať výsledky predchádzajúcich dôkazov a cvičení.

Poznámka 5.40. Podľa vety 5.38 stačí namiesto hľadania jedného zložitého stroja hľadať jednoduchšie stroje pre jednotlivé etapy výpočtu. Blokovú schému tohto zložitého stroja dostaneme z blokových schém jednoduchších strojov vynechaním začiatkových a koncových oválov (okrem začiatkového oválu stroja pre prvú etapu a koncového oválu stroja pre poslednú etapu výpočtu) a vhodným zapojením takto uvoľnených šípok.

Príklad 5.41. Stroj Z pozostávajúci z inštrukcií $(q_1 R_1 q_2 q_5)$, $(q_2 R_1 M q_3)$, $(q_3 R_0 P q_4)$, $(q_4 R_2 q_6 q_0)$, $(q_5 R_0 M q_7)$, $(q_6 R_0 M q_7)$, $(q_7 R_1 P q_5)$ má vlastnosť, že pre všetky $x \in \mathbb{N}$ platí $(q_1; 0, x, 0) \overset{Z}{\Longmapsto} (q_0; 0, x, x)$.



OBR. 5.5.

Dôkaz: Pripomeňme najprv, že pre čiastočnú funkciu Φ_Y^{n+1} platí:

$$\Phi_Y^{n+1}(0, x_1, \ldots, x_n) = \Phi_{Z_2}^n(x_1, \ldots, x_n)$$
$$\Phi_Y^{n+1}(y+1, x_1, \ldots, x_n) = \Phi_{Z_1}^{n+2}(y, \Phi_Y^{n+1}(y, x_1, \ldots, x_n), x_1, \ldots, x_n)$$

Stroje Z_1, Z_2 prerobíme podľa vety 5.43 na stroje Z_1', Z_2', ktoré budú počítať tie isté čiastočné funkcie $\Phi_{Z_1}^{n+2}$, $\Phi_{Z_2}^n$, a ktoré budú okrem toho zachovávať argumenty. Nech k je najmenší index registra, ktorý nepoužíva ani jeden zo strojov Z_1', Z_2'. Potom stroj Y s blokovou schémou na obrázku 5.5(a) má vo vete požadovanú vlastnosť. Vnútorné stavy v tejto blokovaj schéme doplníme (po eliminácii dvojitých obdĺžnikov) podľa cvičenia 5.35 . (Ak by táto bloková schéma nebola súvislá, čo by sa mohlo stať, keby blokové schémy strojov Z_1, Z_2 neboli súvislé, vezmeme tú jej časť, ktorá obsahuje začiatkový ovál.) Potom už môžeme vypísať inštrukcie stroja Y; pokiaľ by neboli blokovou schémou určené vnútorné stavy na tretích a štvrtých miestach niektorých inštrukcií, zvolíme ich tak, aby sa rovnali vnútornému stavu na prvom mieste inštrukcie. □

Cvičenie 5.52. Opíšte konštrukciu stroja Y z vety 5.51 (prípadne iného, ako je uvedený v jej dôkaze) spôsobom použitým v príkladoch 5.44 a 5.49!

Z vety 5.51, vety 5.48 a príkladu 5.20 vyplývajú nasledujúce dve vety:

Veta 5.53. Každá primitívne rekurzívna funkcia je vypočítateľná na registrovom stroji.

Veta 5.54. Množina všetkých (čiastočne) vypočítateľných funkcií je normálny klon (čiastočných) funkcií na množine $\mathbb{N}$.

Teraz sa budeme zaoberať operáciou minimalizácie.

KAPITOLA 6

Ekvivalentnosť M-vypočítateľnosti a rekurzívnosti

V tejto kapitole dokážeme ekvivalentnosť (čiastočnej) vypočítateľnosti na registrových strojoch a (čiastočnej) rekurzívnosti; písmenom M budeme vyznačovať, že zavádzané označenie, resp. termín sa týka registrových strojov. V priebehu tohto dôkazu nájdeme čiastočne rekurzívne univerzálne čiastočné funkcie pre množiny všetkých n-árnych čiastočne rekurzívnych funkcií. Tieto výsledky využijeme na dôkaz niektorých ďalších vlastností (čiastočne) rekurzívnych funkcií a rekurzívne spočítateľných množín a predikátov. Sformulujeme problém zastavenia pre M-stroje a dokážeme jeho rekurzívnu neriešiteľnosť (podľa kapitoly 10 to znamená algoritmickú neriešiteľnosť, bez ohľadu na použitý typ algoritmov).

Na dosiahnutie týchto výsledkov najprv musíme očíslovať všetky M-stroje, ich stavy a výpočty. Číslo objektu X budeme označovať $\mathrm{num}(X)$ bez ohľadu na to, o objekt akého druhu ide. (V čísle objektu nebude vyznačený jeho druh. Teda napríklad nejaký M-stroj a nejaký stav M-stroja môžu mať rovnaké číslo. Avšak rôzne objekty rovnakého druhu musia mať rôzne čísla.)

Definícia 6.1. (a) *Číslom inštrukcie* $(q_i R_j q_m q_n)$ nazveme číslo $\mathrm{p}_i^{2\,\mathrm{c}^3(j,m,n)+2}$

(b) *Číslom inštrukcie* $(q_i R_j P q_k)$ nazveme číslo $\mathrm{p}_i^{4\mathrm{c}(j,k)+3}$

(c) *Číslom inštrukcie* $(q_i R_j M q_k)$ nazveme číslo $\mathrm{p}_i^{4\mathrm{c}(j,k)+1}$

(d) *Číslom registrového stroja* nazveme súčin čísel všetkých jeho inštrukcií.

Číslo inštrukcie je vždy mocninou prvočísla. Príslušné prvočíslo určuje vnútorný stav, v ktorom sa inštrukcia používa, exponent určuje činnosť pri tomto vnútornom stave. Pretože tento exponent je vždy kladný, a pretože registrový stroj neobsahuje rôzne inštrukcie s rovnakým prvým prvkom, možno číslo M-stroja tvoriť ako súčin čísel jeho inštrukcií. Ľahko sa tiež overí nasledujúca veta.

Veta 6.2. Každé kladné celé číslo je číslom práve jedného M-stroja.

Cvičenie 6.3. (a) Určte čísla inštrukcií $(q_2 R_2 q_3 q_4)$, $(q_2 R_0 P q_0)$, $(q_1 R_1 M q_1)$.

(b) Určte inštrukcie, ktorých čísla sú 6561, 16, 8192.

Cvičenie 6.4. (a) Určte M-stroj, ktorého číslo je 196196000000.

(b) Určte číslo niektorého M-stroja, ktorý počíta funkciu $x + y$. (Mocniny neroznásobujte.)

Označenie 6.5. Ak k je číslom M-stroja Z, budeme čiastočnú funkciu Φ_Z^n označovať aj symbolom Φ_k^n. Ak k nebude číslom stroja, budeme klásť $\Phi_k^n = \emptyset$ (t.j. nikde nedefinovanej čiastočnej funkcii).

Poznámka 6.6. Takéto označovanie smieme použiť, pokiaľ uvažujeme a číslujeme len jeden druh strojov.

Definícia 6.7. Pre každé $n \in \mathbb{N}$ definujeme $(n+1)$-árnu čiastočnú funkciu muniv^{n+1} predpisom:

$$\mathrm{muniv}^{n+1}(y, x_1, \ldots, x_n) = \Phi_y^n(x_1, \ldots, x_n) \tag{6.7.1}$$

pre všetky $y, x_1, \ldots, x_n \in \mathbb{N}$.

Z vety 6.2 a z toho, že $\Phi_0^n = \emptyset = \Phi_1^n$ bezprostredne vyplýva

Veta 6.8. Pre každé $n \in \mathbb{N}$ je čiastočná funkcia muniv^{n+1} univerzálna čiastočná funkcia pre množinu všetkých n-árnych čiastočne M-vypočítatelných funkcií.

Teraz sa budeme snažiť dokázať, že čiastočné funkcie muniv^{n+1} sú čiastočne rekurzívne. Na to očíslujeme stavy a výpočty M-strojov a zavedieme niektoré špeciálne, v podstate jednoúčelové, označenia.

Definícia 6.9. (a) *Číslom stavu* $(q_i; a_0, a_1, \ldots, a_n)$ nazveme číslo $2^i \cdot 3^{a_0} \cdot 5^{a_1} \cdots \mathrm{p}_{n+1}^{a_n}$.

Primitívna rekurzívnosť funkcie mobs vyplýva z vyjadrenia (ktoré zoberieme ďalej ako definíciu)

$$\mathrm{mobs}(y) = \mathrm{ex}\left(1, \mathrm{ex}(\mathrm{npr}(y) \dot{-} 1, y)\right) \tag{6.13.3}$$

Teda: berie sa exponent posledného člena v rozklade y na prvočinitele, ten sa znova rozloží na prvočinitele a berie sa exponent prvočísla $\mathrm{p}_1 = 3$.

Primitívna rekurzívnoť funkcií $\mathrm{mvýp}^{n+2}$ bezprostredne vyplýva z primitívnej rekurzívnosti predikátov $\mathrm{Mvýp}^{n+2}$. □

Veta 6.14. Pre každé $n \in \mathbb{N}$ a pre všetky $y, x_1, \ldots, x_n$ platí

$$\mathrm{muniv}^{n+1}(z, x_1, \ldots, x_n) = \mathrm{mobs}\left(\mu_y(\mathrm{mvýp}^{n+2}(y, z, x_1, \ldots, x_n) = 0)\right) \tag{6.14.1}$$

Dôkaz: je triviálny. Z tejto vety však vyplývajú rôzne dôsledky, ktoré budeme v ďalšom skúmať. Odteraz niekedy budeme vynechávať horné indexy v označeniach muniv^{n+1}, $\mathrm{mvýp}^{n+2}$, ak budú zrejmé z kontextu; tak je to napr. vždy, keď sa vypisujú aj argumenty. □

Veta 6.15. Pre každé $n \in \mathbb{N}$ je funkcia muniv^{n+1} čiastočne rekurzívna univerzálna čiastočná funkcia pre množinu všetkých n-árnych čiastočne rekurzívnych funkcií.

Dôkaz: Čiastočná rekurzívnosť čiastočnej funkcie muniv^{n+1} vyplýva bezprostredne z vyjadrenia (6.14.1). Potom zrejme pre každé $n \in \mathbb{N}$ je čiastočná funkcia

$$f(x_1, \ldots, x_n) = \mathrm{muniv}(a, x_1, \ldots, x_n) \tag{6.15.1}$$

čiastočne rekurzívna. Nech, obrátene, $f(x_1, \ldots, x_n)$ je n-árna čiastočne rekurzívna funkcia. Potom podľa vety 5.56 je f čiastočne M-vypočítateľná, t.j. existuje M-stroj Z taký, že $f = \Phi_Z^n$. Ak za a zvolíme číslo stroja Z, tak bude platiť (6.15.1). □

Pre dôkaz nasledujúcej vety použijeme nasledujúce označenie; definované funkcie sú zrejme primitívne rekurzívne.

Definícia 6.16. Pre každé $a, n \in \mathbb{N}$ označíme mvp_a^{n+1} tú funkciu, pre ktorú platí:

$$\mathrm{mvp}_a^{n+1}(y, x_1, \ldots, x_n) = \mathrm{mvýp}^{n+2}(y, a, x_1, \ldots, x_n) \tag{6.16.1}$$

pre všetky $y, x_1, \ldots, x_n$.

Veta 6.17. (Čiastočná) funkcia f je (čiastočne) rekurzívna práve vtedy, keď je (čiastočne) M-vypočítateľná.

Dôkaz: Znenie so slovami v zátvorkách dostávame bezprostredne z viet 6.8 a 6.15. Pre znenie bez týchto slov uvažujeme (totálnu) n-árnu funkciu f. Ak je funkcia f rekurzívna, tak $f = \Phi_Z^n$ pre nejaký M-stroj Z a f je M-vypočítateľná. Obrátene, ak f je M-vypočítateľná, tak existuje také a, pre ktoré platí (6.15.1), a potom aj

$$f(x_1, \ldots, x_n) = \mathrm{mobs}\left(\mu_y(\mathrm{mvp}_a^{n+1}(y, x_1, \ldots, x_n) = 0)\right) \tag{6.17.1}$$

Funkciu f sme teda vyjadrili pomocou skladania rekurzívnych funkcií a regulárnej minimalizácie. Teda f je rekurzívna funkcia, čo bolo treba dokázať. □

Dôsledok 6.18. Množina všetkých rekurzívnych funkcií sa rovná množine všetkých totálnych čiastočne rekurzívnych funkcií.

Z dvoch ekvivalentných pojmov vo vete 6.17 budeme odteraz častejšie používať vo vetách pojem (čiastočnej) rekurzívnosti. Z vety 6.15 a z viet 2.30, 3.80 vyplýva

Veta 6.19. Pre žiadne $n \in \mathbb{N}$, $n \neq 0$ nemá čiastočná funkcia muniv^{n+1} rekurzívne zúplnenie.

Veta 6.20. Nech $n \in \mathbb{N}$, $n \neq 0$. Potom

(a) čiastočná funkcia $\mathrm{sg}\left(\mathrm{muniv}^{n+1}(y, x_1, \ldots, x_n)\right)$ nemá rekurzívne zúplnenie
(b) obor definície čiastočnej funkcie muniv^{n+1} nie je rekurzívna množina
(c) predikát $(\exists y)(\mathrm{mvýp}^{n+2}(y, z, x_1, \ldots, x_n) = 0)$ nie je rekurzívny
(d) predikát $(\forall y)(\mathrm{mvýp}^{n+2}(y, z, x_1, \ldots, x_n) > 0)$ nie je rekurzívne spočítateľný

Poznámka 6.21. Veta 6.20 dáva príklady na to, že pojem rekurzívnej spočítateľnosti a pojem rekurzívnosti nie sú ekvivalentné.

Cvičenie 6.35. Možno v predchádzajúcom cvičení nahradiť rekurzívny predikát $P(x_1, \ldots, x_n)$ rekurzívne spočítateľným predikátom $P(x_1, \ldots, x_n)$?

Cvičenie 6.36. Každá neprázdna rekurzívne spočítateľná podmnožina množiny $\mathbb{N}$ je množinou hodnôt nejakej primitívne rekurzívnej funkcie. Dokážte!

Cvičenie 6.37. Pre každú n-árnu čiastočne rekurzívnu funkciu f existuje unárna primitívne rekurzívna funkcia g a n-árna čiastočne rekurzívna funkcia h s primitívne rekurzívnym grafom tak, že $f(x_1, \ldots, x_n) = g(h(x_1, \ldots, x_n))$ pre všetky $x_1, \ldots, x_n \in \mathbb{N}$. Dokážte! (Návod: Vyjdite z vyjadrenia (6.23.1).)

Cvičenie 6.38. Ak obor definície čiastočne rekurzívnej funkcie f je rekurzívna množina, tak čiastočná funkcia f má rekurzívne zúplnenie. Dokážte!

Teraz sa budeme zaoberať pojmom tzv. m-redukovateľnosti a niektorým pojmom z nej odvodeným; študovalo sa už mnoho pojmov redukovateľnosti a na odlíšenie od iných druhov používame písmeno m (ktoré však tentokrát nemá pripomínať meno Minsky; napr. ruský termín z [6] je mnogosvodimosť, v skratke m-svodimosť). Tieto pojmy zavádzame pre množiny prirodzených čísel; odteraz až do konca kapitoly 6 bude „množina“ znamenať množinu prirodzených čísel, pokiaľ výslovne neuvedieme inak.

Definícia 6.39. (a) Budeme hovoriť, že množina A je *m-redukovateľná* k množine B a písať $A \leq_m B$, ak existuje rekurzívna funkcia f taká, že pre všetky $x \in \mathbb{N}$ platí $x \in A \iff \Rightarrow f(x) \in B$.

(b) Budeme hovoriť, že množiny A, B sú *m-ekvivalentné* a písať $A \equiv_m B$, ak $A \leq_m B$ a súčasne $B \leq_m A$.

Cvičenie 6.40. (a) Relácia $\leq_m$ je kváziusporiadanie (t.j. je tranzitívna a reflexívna) množiny $\mathcal{P}(\mathbb{N})$ všetkých podmnožín množiny $\mathbb{N}$ a relácia $\equiv_m$ je ekvivalencia na množine $\mathcal{P}(\mathbb{N})$.

(b) Množiny $\{\emptyset\}$, $\{\mathbb{N}\}$ a množina všetkých ostatných rekurzívnych množín z $\mathcal{P}(\mathbb{N})$ sú triedami ekvivalencie $\equiv_m$.

(c) Všetky triedy ekvivalencie $\equiv_m$ okrem $\{\emptyset\}$, $\{\mathbb{N}\}$ sú nekonečné spočítateľné.

Dokážte tieto tvrdenia!

Poznámka 6.41. Predstavme si, že by sme mali nejaké zariadenie, ktoré by pre nejakú (vo všeobecnosti nerekurzívnu) množinu A mohlo pre každé prirodzené číslo x rozhodnúť, či platí $x \in A$ alebo či platí $x \notin A$. Takéto hypotetické zariadenie sa niekedy nazýva orákulum pre množinu A. Potom, ak platí $B \leq_m A$, a ak poznáme M-stroj Z taký, že $x \in B \iff \Phi_Z^n(x) \in A$, mohli by sme z orákula pre A a zo stroja Z zostrojiť orákulum pre B. Teda problém, či $x \in A$, sa redukuje na problém, či $x \in B$. V tom je idea definície 6.39.

Podľa cvičenia 6.40 je m-redukovateľnosť medzi rekurzívnymi množinami v podstate triviálna. Avšak v prípade rekurzívne spočítateľných množín je už situácia zaujímavejšia.

Definícia 6.42. Množinu A nazveme *kreatívnou*, ak je rekurzívne spočítateľná a ak každá rekurzívne spočítateľná množina je m-redukovateľná k A.

Kreatívne množiny sú teda v zmysle m-redukovateľnosti najzložitejšie medzi rekurzívne spočítateľnými množinami. Najprv vyriešime otázku, či kreatívne množiny vôbec existujú; kladnú odpoveď dáva nasledujúca veta.

Veta 6.43. Množina

$$K = \{\mathrm{c}(y, x) \mid (y, x) \in \mathrm{Dom}(\mathrm{muniv}^2)\} \tag{6.43.1}$$

je kreatívna.

Dôkaz: Množina K je rekurzívne spočítateľná, pretože je oborom definície čiastočne rekurzívnej funkcie $g(x) = \mathrm{muniv}^2(\mathrm{l}(x), \mathrm{r}(x))$. Nech teraz A je rekurzívne spočítateľná množina, a nech $\mathrm{mvp}_a^1(x)$ je jej čiastočná charakteristická funkcia. Uvažujme rekurzívnu funkciu $f(x) = \mathrm{c}(a, x)$. Pre každé $x \in \mathbb{N}$ platí $x \in A$ vtedy a len vtedy, keď $\mathrm{mvp}_a^1(x)$ je definované, t.j. keď $\mathrm{muniv}^2(a, x)$ je definované, t.j. keď $g(f(x))$ je definované, t.j. keď $f(x) \in K$, čo bolo treba dokázať. □

Kreatívnosť množín sa najčastejšie dokazuje pomocou nasledujúcej takmer zrejmej lemy; uvádzame aj ukážku jej použitia.

Cvičenie 6.53. Pre každé $i \in \mathbb{N}$ definujme

$$M_i = \{\mathrm{c}(y,x) \mid \mathrm{muniv}^2(y,x) = i\} \tag{6.53.1}$$

Dokážte, že pre $i \neq j$ sú množiny M_i, M_j disjunktné a rekurzívne neoddeliteľné.

Definícia 6.54. Množinu A nazveme *prostou*, ak A je rekurzívne spočítateľná, jej komplement $\mathbb{N} \setminus A$ je nekonečný a $\mathbb{N} \setminus A$ neobsahuje žiadnu nekonečnú rekurzívne spočítateľnú množinu.

Veta 6.55. Prostá množina A nie je rekurzívna a nie je kreatívna.

Dôkaz: Ak je A rekurzívna, tak $\mathbb{N} \setminus A$ je tiež rekurzívna, teda keď je $\mathbb{N} \setminus A$ nekonečná, obsahuje sama seba ako nekonečnú rekurzívne spočítateľnú podmnožinu. Nech teraz M_0, M_1 sú rekurzívne neoddeliteľné rekurzívne spočítateľné a navzájom disjunktné a nech $M_0 \leq_m A$. Nech f je taká rekurzívna funkcia, že $x \in M_0 \iff f(x) \in A$. Uvažujme množinu $A_1 = \{f(x) \mid x \in M_1\}$. Táto množina je rekurzívne spočítateľná a disjunktná s A, teda musí byť konečná. Teda množiny $\mathbb{N} \setminus A_1$, A_1 sú rekurzívne. Položme teraz

$$M_0' = \{x \mid f(x) \in \mathbb{N} \setminus A_1\}, \qquad M_1' = \{x \mid f(x) \in A_1\}$$

Množiny M_0', M_1' sú rekurzívne spočítateľné a disjunktné, $M_0' \cup M_1' = \mathbb{N}$. Preto podľa Postovej vety 4.44 sú rekurzívne. Pritom $M_0 \subseteq M_0'$, $M_1 \subseteq \mathbb{N} \setminus M_0'$, a to je spor s rekurzívnou neoddeliteľnosťou M_0, M_1. □

Cvičenie 6.56. Dokážte podrobne, že množiny M_0', M_1' sú rekurzívne spočítateľné.

Aby sme dokázali, že existujú aj iné rekurzívne spočítateľné množiny než rekurzívne a kreatívne, zostane dokázať nasledujúcu vetu.

Veta 6.57. Obor hodnôt A čiastočnej funkcie

$$f(y) = \mathrm{r}\left(\mu_z(\mathrm{mvýp}^3(y, \mathrm{l}(z), \mathrm{r}(z)) + (2y \dot{-} \mathrm{r}(z)) = 0)\right) \tag{6.57.1}$$

je prostá množina.

Dôkaz: Čiastočná funkcia f je čiastočne rekurzívna, a teda A je rekurzívne spočítateľná. Pre číslo z nájdené minimalizáciou k danému y platí

$$f(y) = \mathrm{r}(z), \quad \mathrm{r}(z) \geq 2y \tag{6.57.2}$$

Teda $f(y) \geq 2y$, pokiaľ je $f(y)$ definovaná. Preto A obsahuje najviac n prvkov menších než $2n$, a teda $\mathbb{N} \setminus A$ je nekonečná množina. Ďalej platí

$$\mathrm{mvýp}^3(y, \mathrm{l}(z), \mathrm{r}(z)) = 0 \tag{6.57.3}$$

teda $\mathrm{l}(z)$ je číslo výpočtu M-stroja s číslom y pre vstup $\mathrm{r}(z)$, a teda $f(y) = \mathrm{r}(z)$ je z oboru definície čiastočnej funkcie Φ_y^1.

Nech teraz B je nekonečná rekuzívne spočítateľná množina a Φ_y^1 jej čiastočná charakteristická funkcia. Zoberme ľubovoľné $x \in B$, $x \geq 2y$. Výpočet stroja s číslom y pre vstup x je konečný; nech u je jeho číslo. Potom pre $z = \mathrm{c}(u,x)$ platí (6.57.2) aj $\mathrm{r}(z) \geq 2y$, teda $f(y)$ je definované. (Minimalizácia (6.57.1) však môže dať inú, menšiu, hodnotu pre z než $\mathrm{c}(u,x)$, a $f(y)$ môže vyjsť aj väčšie než x.) Potom $f(y) \in A \cap B$, teda B nie je podmnožinou $\mathbb{N} \setminus A$, čo bolo treba dokázať. □

Cvičenie 6.58. (a) Ak je A prostá množina, $B \subseteq \mathbb{N}$ a množiny $A \setminus B$, $B \setminus A$ sú konečné, tak aj B je prostá množina. Dokážte!

(b) Dokážte analogické tvrdenia pre rekurzívne spočítateľné množiny a pre rekurzívne množiny.

Cvičenie 6.59. Ak A je prostá množina, B je nekonečná rekurzívne spočítateľná množina, tak $A \cap B$ je nerekurzívna rekurzívne spočítateľná množina. Dokážte!

Na záver tejto kapitoly sa zmienime o problémoch zastavenia pre registrové stroje. Na to prijmeme nasledujúcu definíciu; diskusiu o jej zmysle odkladáme do kapitoly 10. Tu len bez zdôvodnenia poznávame, že zavádzané pojmy rekurzívnej riešiteľnosti, resp. neriešiteľnosti veľmi presne zodpovedajú intuitívnym pojmom algoritmickej riešiteľnosti, resp. neriešiteľnosti. Formálnu definíciu hromadného problému tiež odkladáme, a to do kapitoly 7. Zatiaľ nám stačí vedieť, že hromadný problém reprezentuje množinu otázok rovnakého typu, ktoré dostávame z jednej „schémy otázok“ voľbou parametrov.

a potom prečítať exponenty n prvočísel počnúc od $5 = \mathrm{p}_2$ v týchto nepárnych prvkoch. Formulou to môžeme vyjadriť napríklad takto:

$$(x_1, \ldots, x_n) \in A \iff (\exists y)\big(y \in X \ \wedge\ \mathrm{ex}_0(y) = 0 \ \wedge\ x_1 = \mathrm{ex}_2(y) \ \wedge\ \cdots \ \wedge\ x_n = \mathrm{ex}_{n+1}(y)\big) \quad \square$$

Definícia 7.1. (a) Symbolom $\overline{A}$ označíme množinu všetkých prvkov postupnosti

$$a_0, a_1, a_2, a_3, \ldots \tag{7.1.1}$$

(b) Konečné neprázdne podmnožiny množiny $\overline{A}$ budeme nazývať *abecedami*.

Poznámka 7.2. Predpokladáme, že postupnosť (7.1.1) je prostá. Nebudeme potrebovať voliť ju konkrétnejšie, keby sme to však chceli, môžeme zvoliť napríklad $a_i = \{\{i\}, \{i+1\}\}$ pre všetky $i \in \mathbb{N}$. Ak sme zvolili prirodzené čísla podľa poznámky 1.5, sú množiny $\overline{A}$, $\mathbb{N}$, $\overline{A}^1$, $\mathbb{N}^1$, $\overline{A}^2$, $\mathbb{N}^2$, ... po dvoch disjunktné.

Dohoda 7.3. Budeme navzájom stotožňovať symboly B a a_0, symboly O a a_1 a symboly I a a_2.

Definícia 7.4. (a) Konečné postupnosti prvkov množiny $\overline{A}$ nazývame *slovami*. Ak $A \subseteq \overline{A}$ je abeceda a všetky členy slova w patria do A, budeme w nazývať slovom v abecede A. Slová budeme písať bez zátvoriek a čiarok.

(b) *Dĺžkou* slova w nazveme počet členov postupnosti w. Dĺžku slova w budeme označovať $|w|$.

(c) Slovo dĺžky 0 budeme označovať ε a nazývať *prázdnym slovom*. (Takéto slovo existuje práve jedno.)

(d) *Množinu všetkých slov* v abecede A budeme označovať A^*. *Množinu všetkých neprázdnych slov* v abecede A budeme označovať A^+.

Poznámka 7.5. Označenia z bodu (d) definície 7.4 sú len špeciálnymi prípadmi všeobecnejšieho označenia, ktoré zavedieme nižšie.

Definícia 7.6. (a) *Zreťazením slov* $x = a_{i_1}a_{i_2}\ldots a_{i_m}$, $y = a_{j_1}a_{j_2}\ldots a_{j_n}$ nazveme slovo

$$z = a_{i_1}a_{i_2}\ldots a_{i_m}a_{j_1}a_{j_2}\ldots a_{j_n}$$

Zreťazenie slov x, y budeme označovať xy.

(b) *Zreťazením množín slov* A, B nazveme množinu $C = \{xy \mid x \in A, y \in B\}$ všetkých slov, ktoré vzniknú zreťazením slova z množiny A a slova z množiny B. Zreťazenie množín A, B budeme označovať AB.

Dohoda 7.7. Pokiaľ nebude hroziť nedorozumenie, budeme slová dĺžky 1 označovať rovnako ako ich prvky a jednoprvkové množiny slov rovnako ako tieto slová.

Cvičenie 7.8. Dokážte, že operácia zreťazenia slov je asociatívna, t.j. že pre každé tri slová x, y, z platí

$$(xy)z = x(yz) \tag{7.8.1}$$

Je operácia zreťazenia komutatívna?

Cvičenie 7.9. Dokážte, že operácia zreťazenia množín slov je asociatívna, t.j. že pre každé tri množiny slov A, B, C platí

$$(AB)C = A(BC) \tag{7.9.1}$$

Je táto operácia komutatívna?

Cvičenie 7.10. Tvorí množina

- všetkých slov,
- všetkých množín slov,
- všetkých slov v abecede A,
- všetkých množín slov v abecede A

voľný monoid (t.j. voľnú pologrupu s jednotkovým prvkom)?

Z operácie zreťazenia utvoríme teraz operáciu mocniny slov a množín slov, operáciu iterácie $*$ a operáciu $+$. Upozorňujeme, že mocnina množiny slov sa označuje rovnako ako kartézska mocnina, ale ide o úplne rozličné pojmy; v prípadoch, keď nebude z kontextu zrejmé, o ktorý význam tohto označenia ide, budeme musieť určiť správny význam slovami.

V nasledujúcej definícii zavádzame pojem hromadnej úlohy. Tento pojem zodpovedá pojmu množiny úloh rovnakého typu. Podľa úvah na začiatku tejto kapitoly bude vstupným údajom pre úlohu slovo v nejakej abecede A_1, výsledkom bude slovo v nejakej vo všeobecnosti inej abecede A_2. Ak ešte vezmeme do úvahy, že obvykle nie každé slovo v abecede A_1 má zmysel ako vstupný údaj a že nie vždy má úloha riešenie, aj keď majú vstupné údaje zmysel, vidíme, že je vhodná nasledujúca definícia:

Definícia 7.19. Usporiadanú štvoricu tvaru

$$\mathcal{H} = (A_1, A_2, Z, \varkappa) \tag{7.19.1}$$

kde A_1, a A_2 sú abecedy, Z je množina slov v abecede A_1 a $\varkappa$ je čiastočné zobrazenie množiny Z do množiny A_2^*, budeme označovať *hromadnou úlohou*. Abecedu A_1 budeme nazývať *vstupnou abecedou*, abecedu A_2 budeme nazývať *výstupnou abecedou* a množinu Z *oborom* hromadnej úlohy $\mathcal{H}$. Čiastočné zobrazenie $\varkappa$ budeme označovať czb($\mathcal{H}$) a budeme o ňom hovoriť, že je čiastočným zobrazením z hromadnej úlohy $\mathcal{H}$.

Poznámka 7.20. Najdôležitejšou zložkou hromadnej úlohy (7.19.1) je zrejme čiastočné zobrazenie a prípadne ešte obor Z hromadnej úlohy. Tým nie je určená vstupná ani výstupná abeceda, ale to zvyčajne nebude potrebné. Obvykle potom zvolíme tieto abecedy najmenšie možné (v zmysle množinovej inklúzie).

Príklad 7.21. Uvedieme, ako možno chápať základné aritmetické operácie na prirozených číslach (daných v dekadickom zápise) ako hromadné úlohy. Označme C množinu $\{0, 1, \ldots, 9\}$ všetkých dekadických cifier. Potom množina všetkých dekadických zápisov prirodzených čísiel sa dá písať v tvare $D = \{0\} \cup (C \setminus \{0\})\, C^*$. Na označovanie sčítania, odčítania, násobenia a delenia použijeme v uvedenom poradí znaky „+“, „−“, „×“, „:“. Vstupnými abecedami budú množiny $C \cup \{X\}$, kde X je znova znak príslušnej operácie (tentokrát je však použitý podľa dohody 7.7 pre jednoprvkové slovo; neskôr budeme podľa tej istej dohody vynechávať v podobných označeniach aj zátvorky $\{\}$). Výstupnou abecedou je vo všetkých štyroch prípadoch množina C. Definícia čiastočných zobrazení $\varkappa_1$, $\varkappa_2$, $\varkappa_3$, $\varkappa_4$ v hromadných úlohách zodpovedajúcich v uvedenom poradí sčítaniu, odčítaniu, násobeniu a deleniu, je zrejmá. Platí napríklad $\varkappa_1(23+34) = 57$, $\varkappa_2(23-11) = 12$, $\varkappa_3(23 \times 21) = 483$, $\varkappa_4(24 : 2) = 12$; naproti tomu $\varkappa_2(23-34)$ a $\varkappa_4(23 : 34)$ nie sú definované. Zátvorky „(“, „)“ sú tu len pomocnými symbolmi a nepatria do vstupných ani výstupných abecied.

Príklad 7.22. Ak by sme chceli sčítanie viacerých prirodzených čísiel v dekadickom zápise chápať ako hromadnú úlohu, mohli by sme za vstupnú abecedu tejto hromadnej úlohy zvoliť množinu $C \cup \{+\}$, za výslednú abecedu množinu C a za obor množinu $Z = (D\{+\})^* D$. (Množiny C, D sú tie isté ako v predchádzajúcom prípade.) Keby sme sa chceli vyhnúť „súčtom s jediným sčítancom“, zvolili by sme $Z = (D\{+\})^+ D$. Definícia čiastočného zobrazenia z tejto hromadnej úlohy je iste čitateľovi zrejmá.

Príklad 7.23. Hromadnú úlohu zodpovedajúcu vykonaniu jednej základnej aritmetickej operácie na prirodzených číslach daných v dekadickom zápise dostamene tak, že hromadné úlohy z príkladu 7.21 po zložkách množinove zjednotíme.

Cvičenie 7.24. Aká je nutná a postačujúca podmienka na hromadné úlohy $(A_1, A_2, Z, \varkappa)$, $(A_1', A_2', Z', \varkappa')$, aby aj usporiadaná štvorica

$$(A_1 \cup A_1', A_2 \cup A_2', Z \cup Z', \varkappa \cup \varkappa')$$

bola hromadnou úlohou?

Hromadné úlohy, v ktorých ide len o rozhodnutie o pravdivosti jedného výroku z nejakej množiny výrokov, nazývame častejšie hromadnými problémami. Pri formálnom poňatí podľa definície 7.19 budú čiastočné zobrazenia z takýchto úloh nadobúdať iba dve hodnoty, z ktorých jedna zodpovedá pravdivosti skúmaného výroku a druhá jeho nepravdivosti. Vstupným údajom nemusí byť zápis celého výroku, ale stačí zapisovať jeho meniacu sa časť.

Príklad 7.25. Zisťovaniu párnosti (resp. nepárnosti) prirodzeného čísla podľa jeho dekadického zápisu zodpovedá hromadná úloha so vstupnou abecedou C, výstupnou abecedou O, I a oborom

pre všetky $w_2 \in U_2$, $w_1 \in U_1$.

Cvičenie 7.30. (a) Nájdite kód niektorého M-stroja, ktorý počíta funkciu $x + y$. (Porovnajte namáhavosť tejto úlohy a úlohy z cvičenia 6.4(b).)

(b) Nájdite kódy všetkých členov výpočtu stroja z bodu (a) zo stavu $(q_1; 0, 1, 1)$.

(c) Navrhnite nejaký jednoduchý spôsob kódovania konečných postupností M-stavov s použitím kódov týchto stavov podľa bodu (c) definície 7.26.

Vhodnými zariadeniami na skúmanie a riešenie hromadných úloh (bez prechodu k číselným funkciám) sú Turingove stroje. Tie však budeme definovať a skúmať až v nasledujúcej kapitole. V informatike sa uvažuje mnoho iných typov zariadení (rôznej sily) na rozpoznávanie množín slov (teda: formálnych jazykov). Čitateľ sa veľmi pravdepodobne už stretol s niektorými z nich. Najjednoduchšie sú konečné automaty, ktoré rozpoznávajú tzv. regulárne množiny. My tieto množiny zavedieme iným (ale tiež známym spôsobom). Regulárne množiny sú dôležité napríklad pri štúdiu otázok týkajúcich sa programovacích jazykov, i keď samotné programovacie jazyky sú spravidla zložitejšie. Obory hromadných úloh (tretie zložky štvoríc (7.19.1)) spravidla sú regulárne množiny.

Definícia 7.31. Množinu slov nazveme *regulárnou* množinou, ak vzniká z konečných množín slov konečným počtom operácií zreťazenia, iterácie a množinového zjednotenia.

Poznámka 7.32. (a) Slová „konečným počtom operácií“ by sme mohli eliminovať spôsobom uvedeným v poznámke 3.5.

(b) O voľbe písmen, z ktorých sa skladajú slová, platí aj v tejto kapitole všetko, na čom sme sa dohodli v predchádzajúcej kapitole.

(c) Z definície 7.31 bezprostredne vyplýva, že ak sú A, B regulárne množiny, sú aj AB, $A \cup B$ a A^* regulárne množiny.

Poznámka 7.33. Každá regulárna množina M je množina slov v nejakej abecede A. Takúto abecedu môžeme dostať napríklad zo všetkých písmen všetkých slov tých konečných množín, z ktorých vzniká napríklad množina M podľa definície 7.31 (ak by takto vznikla prázdna množina, môžeme položiť $A = \{a_0\}$). Obvykle sa definujú regulárne množiny v nejakej abecede A. My to nemusíme robiť, lebo sme si dopredu zvolili množinu písmen $\overline{A}$.

Príklad 7.34. Množiny z príkladu 7.15 sú regulárne množiny.

Cvičenie 7.35. Dokážte, že zrkadlový obraz regulárnej množiny je regulárna množina!

Cvičenie 7.36. Ak M je regulárna množina, je aj M^+ regulárna množina. Dokážte!

Cvičenie 7.37. Dokážte, že nasledujúce množiny slov sú regulárne:

(a) množina M_1 všetkých slov v abecede $\{O, I\}$, ktoré obsahujú aspoň dve I,

(b) množina M_2 všetkých slov v abecede $\{O, I\}$, ktoré obsahujú dve I za sebou,

(c) množina M_3 všetkých slov v abecede $\{O, I\}$, ktoré obsahujú práve dve I,

(d) množiny $\{O, I\}^* \setminus M_1$, $\{O, I\}^* \setminus M_2$, $\{O, I\}^* \setminus M_3$.

Cvičenie 7.38. Dokážte, že množina všetkých dekadických zápisov prirodzených čísel deliteľných 1250-mi je regulárna! (Predpokladáme pritom, že dekadické cifry sú stotožnené s nejakými prvkami množiny $\overline{A}$.)

Cvičenie 7.39. Dokážte, že nasledujúce množiny sú regulárne:

(a) množina všetkých dekadických zápisov prirodzených čísel deliteľných 9-mi

(b) množina všetkých dekadických zápisov prirodzených čísel, ktoré pri delení 9-mi dávajú zvyšok 4, 5 alebo 6

(c) množina všetkých dekadických zápisov prirodzených čísel, ktoré pri delení 7-mi dávajú zvyšok 3

(d) množina všetkých slov v abecede $\{O, I, B\}$, ktoré obsahujú párny počet O a nepárny počet I

(e) množina všetkých slov v abecede $\{O, I, B\}$, ktoré neobsahujú dve B za sebou

(f) množina všetkých slov v abecede $\{O, I, B\}$, v ktorých je počet I deliteľný 5-mi

Dohoda 8.6. Na označenie T-stavov budeme používať aj také postupnosti (8.5.1), ktoré nespĺňajú podmienky $i_1 \neq 0, i_n \neq 0$. V takomto prípade však budeme (8.5.1) pokladať za označenie stavu, ktorý vznikne z tejto postupnosti vynechaním všetkých B (t.j. a_0 podľa dohody 7.3) na začiatku a na konci. Bude teda platiť napríklad $a_0a_1a_0q_4a_2a_0 = a_1a_0q_4a_2$, t.j. $BOBq_4IB = OBq_4I$ podľa dohody 7.3.

Poznámka 8.7. Vnútorné stavy q_i nestotožňujeme so žiadnymi symbolmi a_i, a preto (8.5.1) nie je v rámci našej definície slovom. Napriek tomu však budeme pre stavy používať obdobné označenia ako pre slová.

Definícia 8.8. Nech X_1, X_2 sú T-stavy, T je Turingov stroj. Budeme písať

$$X_1 \xrightarrow{T} X_2 \tag{8.8.1}$$

ak existujú také slová v, w a také čísla i, j, k, m, $n \in \mathbb{N}$, že platí

(a) $X_1 = vq_ia_jw$, $X_2 = vq_na_mw$ a $(q_ia_ja_mNq_n) \in T$ alebo
(b) $X_1 = vq_ia_jw$, $X_2 = va_mq_nw$ a $(q_ia_ja_mPq_n) \in T$ alebo
(c) $X_1 = va_kq_ia_jw$, $X_2 = vq_na_ka_mw$ a $(q_ia_ja_mLq_n) \in T$.

Poznámka 8.9. V neformálnom chápaní (8.8.1) znamená, že stav X_2 vzniká zo stavu X_1 jedným krokom výpočtu Turingovho stroja T. Body (a), (b), (c) zodpovedajú v tomto poradí prípadom, že sa pri tomto kroku výpočtu čítacia a zapisovacia hlava nepohne, že sa pohne doprava a že sa pohne doľava.

Neformálne chápanie Turingových strojov budeme často používať aj neskôr pre jeho prehľadnosť. Predpokladáme však, že čitateľ si ho v prípade potreby sám prepracuje na opis v rámci formálnych definícií.

Poznámka 8.10. Ku každému Turingovmu stroju T a každému T-stavu X_1 existuje najviac jeden taký T-stav X_2, že platí $X_1 \xrightarrow{T} X_2$.

Dohoda 8.11. Ak nebude hroziť nedorozumenie, budeme z označenia (8.8.1) vynechávať T.

Príklad 8.12. Nech $T = \{(q_1OIPq_1), (q_1IOPq_1), (q_1BBLq_2), (q_2OOLq_2), (q_2IILq_2), (q_2BBPq_3), (q_3OONq_0), (q_3IINq_0)\}$. Podľa definície 8.4 je T Turingov stroj. Podľa definície 8.8 platí napríklad:

$$q_1OIIO \xrightarrow{T} Iq_1IIO \qquad IOq_2OI \xrightarrow{T} Iq_2OOI$$
$$Iq_1IIO \xrightarrow{T} IOq_1IO \qquad Iq_2OOI \xrightarrow{T} q_2IOOI$$
$$IOq_1IO \xrightarrow{T} IOOq_1O \qquad q_2IOOI \xrightarrow{T} q_2BIOOI$$
$$IOOq_1O \xrightarrow{T} IOOIq_1 \qquad q_2BIOOI \xrightarrow{T} q_3IOOI$$
$$IOOIq_1 \xrightarrow{T} IOOq_2I \qquad q_3IOOI \xrightarrow{T} q_0IOOI$$
$$IOOq_2I \xrightarrow{T} IOq_2OI$$

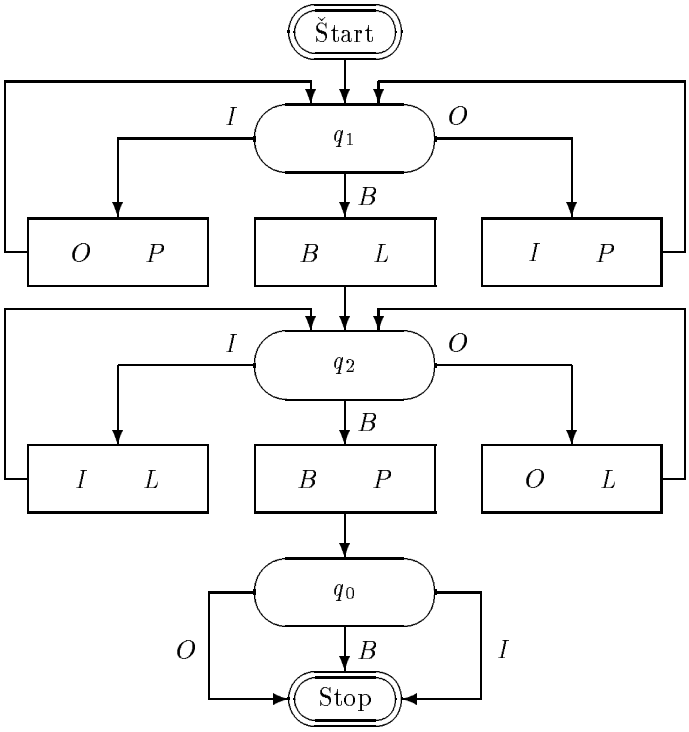
Definícia 8.13. (a) Konečnú postupnosť T-stavov $X_0, X_1, \ldots, X_n$ nazveme *výpočtom Turingovho stroja T zo stavu X_0*, ak $X_i \xrightarrow{T} X_{i+1}$ pre všetky $i = 0, 1, \ldots, n-1$ a neexistuje taký stav X_{n+1}, že $X_n \xrightarrow{T} X_{n+1}$.

(b) Nekonečnú postupnosť T-stavov $X_0, X_1, X_2, \ldots$ nazveme *výpočtom Turingovho stroja T zo stavu X_0*, ak pre všetky $i = 0, 1, 2, \ldots$ platí $X_i \xrightarrow{T} X_{i+1}$.

Definícia 8.14. (a) Nech X, Y sú T-stavy, T je Turingov stroj. Budeme písať $X \overset{T}{\Longrightarrow} Y$, ak existuje taká konečná postupnosť T-stavov $X_0, X_1, \ldots, X_n$, že platí $X = X_0$, $Y = X_n$ a pre všetky $i = 0, 1, \ldots, n-1$ platí $X_i \xrightarrow{T} X_{i+1}$.

(b) Budeme písať $X \overset{T}{\Longmapsto} Y$, ak $X \overset{T}{\Longrightarrow} Y$ a neexistuje taký stav Z, že $Y \xrightarrow{T} Z$.

Príklad 8.15. Nech T je stroj z príkladu 8.12. Potom q_1OIIO, Iq_1IIO, IOq_1IO, $IOOq_1O$, $IOOIq_1$, $IOOq_2I$, IOq_2OI, Iq_2OOI, q_2IOOI, q_2BIOOI, q_3IOOI, q_0IOOI je výpočet stroja T



Obr. 8.2.

Definícia 8.20. Nech T je Turingov stroj a A je jeho abeceda. Symbolom Rez_T označíme také čiastočné zobrazenie množiny A^* do množiny A^*, že pre všetky v, $w \in A^*$ platí $\mathrm{Rez}_T(v) = w$ práve vtedy, keď $q_1 v \overset{T}{\Longmapsto} q_0 w$.

Poznámka 8.21. Pre $v \in A^*$ môže byť $\mathrm{Rez}_T(v)$ nedefinované z niektorého z nasledujúcich dôvodov:

(a) výpočet stroja T zo stavu $q_1 v$ je nekonečný (v ďalších bodoch už predpokladáme konečnosť tohto výpočtu),
(b) výpočet stroja T zo stavu $q_1 v$ sa končí členom s vnútorným stavom rôznym od q_0,
(c) políčka pásky s obsahom rôznym od B (ďalej: neprázdne políčka) netvoria súvislý úsek pásky po ukončení výpočtu zo stavu $q_1 v$,
(d) po ukončení výpočtu zo stavu $q_1 v$ nie je čítacia a zapisovacia hlava pri ľavom krajnom políčku úseku neprázdnych políčok pásky.

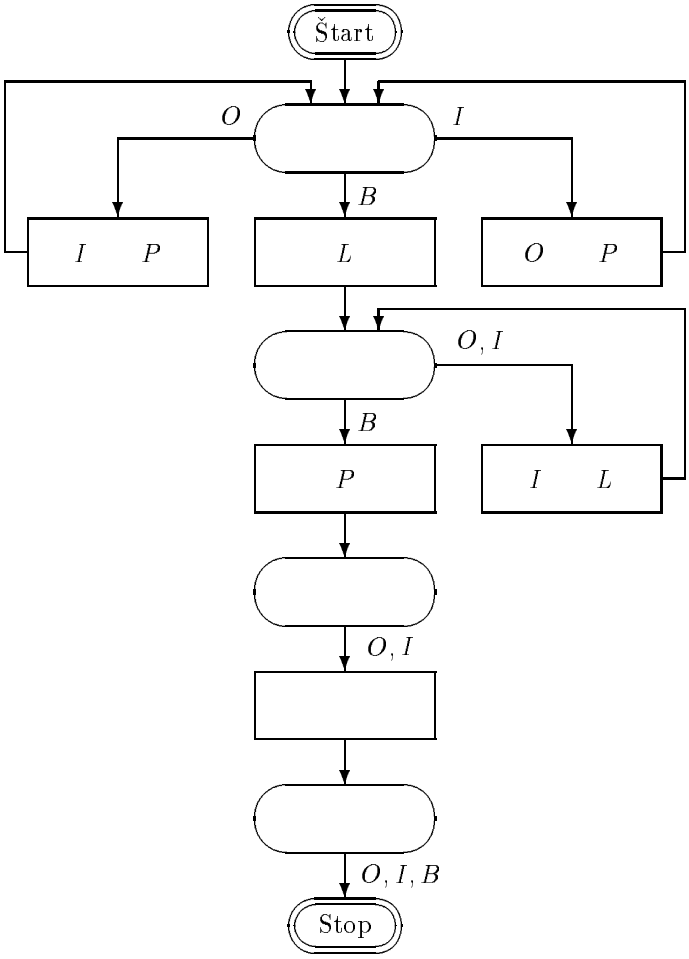
V kapitole 7 sme ukázali, ako možno chápať niektoré triedy úloh rovnakého typu ako hromadné úlohy, avšak nezaoberali sme sa otázkou algoritmickej riešiteľnosti hromadných úloh. Kvôli preskúmaniu tohto problému teraz definujeme:

Definícia 8.22. (a) Budeme hovoriť že Turingov stroj T *rieši* hromadnú úlohu $(A_1, A_2, Z, \varkappa)$, ak A_1, A_2 sú podmožiny abecedy stroja T a pre všetky $v \in Z$ platí $\mathrm{Rez}_T(v) = \varkappa(v)$.

(b) Budeme hovoriť, že hromadná úloha $\mathcal{H}$ je *riešiteľná Turingovým strojom* (alebo: *T-strojovo riešiteľná*), ak existuje Turingov stroj, ktorý ju rieši.

Poznámka 8.23. Z podmienky $\mathrm{Rez}_T(v) = \varkappa(v)$ v definícii 8.22 nevyplýva $\mathrm{Rez}_T = \varkappa$, lebo tieto čiastočné zobrazenia nemusia mať rovnaký obor definície; zobrazenie Rez_T je však vždy rozšírením zobrazenia $\varkappa$.

Pre číselné čiastočné funkcie definujeme:



Obr. 8.4.

I, O vzájomne zamenené. Tento stroj teda rieši hromadnú úlohu $\big(\{O,I\},\{O,I\},\{O,I\}^*,\varkappa\big)$, kde $\varkappa$ je zobrazenie, ktoré každému slovu v abecede $\{O,I\}$ priraďuje jeho „negatív".

Príklad 8.28. Nech $T = \{(q_1OILq_2),(q_2BOPq_3),(q_3IIPq_3),(q_3OILq_4),(q_4IOPq_5),(q_5OOLq_5),(q_5IILq_5),(q_5BBPq_0)\}$. Pre tento stroj T platí napríklad: $q_1OIIOIOIO \xrightarrow{T} q_2BIIIOIOIO \xrightarrow{T} Oq_3IIIOIOIO \xrightarrow{T} \cdots \xrightarrow{T} OIIIq_3OIOIO \xrightarrow{T} OIIq_4IIIOIO \xrightarrow{T} OIIOq_5IIOIO \xrightarrow{T} \cdots \xrightarrow{T} q_5OIIOIIOIO \xrightarrow{T} q_5BOIIOIIOIO \xrightarrow{T} q_0OIIOIIOIO$. Všeobecnejšie, pre každé $n \in \mathbb{N}, n \geq 2$ a všetky $k_1, \ldots, k_n$ platí

$$\mathrm{Rez}_T(OI^{k_1}OI^{k_2}O\ldots OI^{k_n}O) = OI^{k_1}OI^{k_2+1}OI^{k_3}O\ldots OI^{k_n}O$$

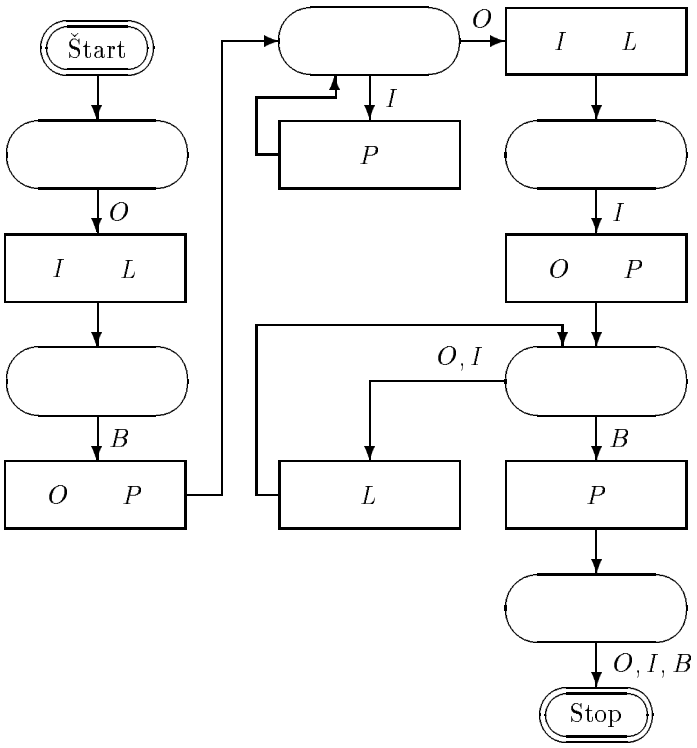
Teda tento stroj rieši hromadnú úlohu $\mathcal{H} = (\{O,I\},\{O,I\},O\{O,I\}^*O,\varkappa)$, kde $\varkappa$ je dané vzorcom:

$$\varkappa\big(OI^{k_1}OI^{k_2}OI^{k_3}O\ldots OI^{k_n}O\big) = OI^{k_1}OI^{k_2+1}OI^{k_3}O\ldots OI^{k_n}O$$

Cvičenie 8.29. Nájdite Turingov stroj, ktorý bude riešiť hromadnú úlohu $\mathcal{H} = (\{O,I\},\{O,I\}, O\{O,I\}^*O,\varkappa)$, kde $\varkappa$ je dané vzorcom:

$$\varkappa\big(OI^{k_1}OI^{k_2}OI^{k_3}O\ldots OI^{k_n}O\big) = OI^{k_1}OI^{k_2-1}OI^{k_3}O\ldots OI^{k_n}O, \quad (n \geq 2, k_1,\ldots,k_n \in \mathbb{N})$$

Aby sme mohli ľahšie hľadať Turingove stroje na riešenie hromadných úloh, prípadne na počítanie čiastočných funkcií, zavedieme pre ne blokové schémy obdobným spôsobom ako pre M-stroje.



Obr. 8.6.

Dohoda 8.32. (a) V blokovej schéme T-stroja sa nemusia vyznačovať vnútorné stavy.

(b) V obdĺžnikoch v blokovej schéme možno vynechávať symbol N.

(c) V obdĺžnikoch blokovej schémy T-stroja možno vynechávať symbol $a_i \in \overline{A}$, ak je rovnaký ako symbol pri začiatku šípky smerujúcej do tohto obdĺžnika.

(d) Ak sa v blokovej schéme vyskytlo (prípadne po zjednodušení podľa bodov (b), (c)) niekoľko obdĺžnikov, do ktorých sú vpísané rovnaké symboly a z ktorých vedú šípky k tomu istému krúžku, možno tieto obdĺžniky nahradzovať jediným obdĺžnikom (do ktorého potom bude smerovať viac šípok).

(e) Miesto viacerých šípok smerujúcich od niektorého krúžku k niektorému obdĺžniku (alebo koncovému oválu) možno kresliť jedinú šípku, k začiatku ktorej pripíšeme všetky symboly, ktoré boli pripísané k začiatku jednotlivých nahradzovaných šípok.

Príklad 8.33. Zjednodušené blokové schémy T-strojov z príkladov 8.12, 8.27 a 8.28 sú na obrázku 8.4, 8.5 a 8.6.

Poznámka 8.34. Pri zostrojovaní nejakého Turingovho stroja T je obvykle vhodné začať neformálnym opisom jeho činnosti, k tomuto opisu zostaviť zjednodušenú blokovú schému, z nej úplnú blokovú schému a až nakoniec vypísať inštrukcie stroja T.

Príklad 8.35. Nech $\mathcal{H} = \big(\{O,I\}, \{O,I\}, \{O,I\}^*, \varkappa\big)$, kde $\varkappa$ je zobrazenie množiny $\{O,I\}^*$ do $\{O,I\}^*$ dané vzorcom

$$\varkappa(w) = \begin{cases} O, & \text{ak } w^R \neq w \\ I, & \text{ak } w^R = w \end{cases}$$

Nájdeme Turingov stroj T, ktorý rieši túto hromadnú úlohu. Stroj bude pracovať tak, že prečíta prvé písmeno slova w, nahradí ho symbolom B, ale „zapamätá“ si ho. Potom vyhľadá posledný symbol slova w a porovná ho so zapamätaným prvým symbolom. Ak sa tieto symboly zhodujú,

že stroj T obsahuje tri inštrukcie, ktoré majú na prvom mieste q_2, a to (q_2OOPq_2), (q_2IIPq_2), (q_2BBLq_4).

Poznámka 8.36. Jedna z možností ako prehľadne napísať inštrukcie nejakého stroja T, je použitie tabuľky. Do záhlavia jej riadkov vpíšeme vnútorné stavy nachádzajúce sa aspoň v jednej inštrukcii stroja T na prvom mieste, do záhlavia stĺpcov vpíšeme symboly, ktoré sa nachádzajú na druhých miestach inštrukcií stroja T. Do jednotlivých okienok tabuľky potom vpisujeme posledné tri prvky inštrukcie stroja T, ktorej prvé dva prvky sú v záhlaví príslušného riadku a stĺpca. Pritom budeme niekedy vynechávať tretí prvok, ak sa zhoduje s druhým, štvrtý, ak sa rovná N a piaty, ak sa zhoduje s prvým, nikdy však všetky tri súčasne. Do okienok, ktorým nepatrí žiadna inštrukcia, vpíšeme pomlčku alebo ich necháme prázdne. Takúto tabuľku budeme nazývať *tabuľkou stroja* T.

Príklad 8.37. Tabuľka stroja T z príkladu 8.35 je:

	B			O			I		
q_1	I	N	q_0	B	P	q_2	B	P	q_3
q_2		L	q_4		P			P	
q_3		L	q_5		P			P	
q_4	I		q_0	B	L	q_6	B	L	q_7
q_5	I		q_0	B	L	q_7	B	L	q_6
q_6		P	q_1		L			L	
q_7	O		q_0	B	L		B	L	

Cvičenie 8.38. Nakreslite schému a zostavte tabuľku Turingovho stroja, ktorý rieši hromadnú úlohu $\mathcal{H} = (\{O, I\}, \{O, I\}, \{O, I\}^*, \varkappa)$, kde $\varkappa$ je zobrazenie množiny $\{O, I\}^*$ do $\{O, I\}^*$ dané predpisom:

(a) $\varkappa(w) = \begin{cases} w^R, & \text{ak } w \text{ je slovo párnej dĺžky} \\ w, & \text{ak } w \text{ je slovo nepárnej dĺžky} \end{cases}$

(b) $\varkappa(w) = \begin{cases} O, & \text{ak slovo } w \text{ obsahuje viac „}O\text{“ ako „}I\text{“} \\ I, & \text{ak slovo } w \text{ obsahuje viac „}I\text{“ ako „}O\text{“} \\ \varepsilon, & \text{v ostatných prípadoch} \end{cases}$

(c) $\varkappa(w) = ww$, pre každé $w \in \{O, I\}^*$

(d) $\varkappa(w) = w^R w$, pre každé slovo $w \in \{O, I\}^*$

(e) $\varkappa(w) = \begin{cases} I^n, & \text{ak slovo } w \text{ obsahuje presne o } n \text{ viac „}I\text{“ ako „}O\text{“} \\ O^n, & \text{ak slovo } w \text{ obsahuje presne o } n \text{ viac „}O\text{“ ako „}I\text{“} \end{cases}$

Odteraz budeme pod úlohou „nájsť Turingov stroj“ rozumieť úlohu „nakresliť blokovú schému alebo zostaviť tabuľku Turingovho stroja“.

Cvičenie 8.39. Nech $A_1 \subseteq \overline{A} \backslash \{B\}$ je konečná množina a $X \subseteq {A_1}^*$ je regulárna množina. Dokážte, že existuje Turingov stroj, ktorý rieši hromadnú úlohu $(A_1, \{O, I\}, A_1^*, \varkappa)$, kde

(a) $\varkappa(w) = \begin{cases} 0, & \text{ak } w \in X \\ 1, & \text{ak } w \notin X \end{cases}$

(b) $\varkappa(w) = \begin{cases} w, & \text{ak } w \in X \\ \varepsilon, & \text{ak } w \notin X \end{cases}$

Cvičenie 8.40. Nájdite taký Turingov stroj, aby pre ľubovoľné slovo $w \in \{O, I\}^*$ platilo

$$\mathrm{Rez}_T(w) = OwOwO$$

Cvičenie 8.41. Nájdite taký Turingov stroj T, že pre všetky $x, y \in \mathbb{N}$

- $\Phi_T^1(x) = 2x$
- $\Phi_T^2(x, y) = x \cdot y$
- $\Phi_T^2(x, y) = \lfloor x/y \rfloor$

Turingov stroj T' má nasledujúcu vlastnosť: Ak m je prirodzené číslo väčšie alebo rovnajúce sa najväčšiemu indexu registrov R_i v inštrukciách M-stroja Z', tak pre všetky $r_0, r_1, \ldots, r_m$, $s_0, s_1, \ldots, s_m \in \mathbb{N}$ a všetky $q_i, q_j \in (Q \setminus \{q_0, q_1\}) \cup \{q_u, q_v\}$ platí

$$(q_i; r_0, r_1, \ldots, r_m) \overset{Z'}{\Longmapsto} (q_j; s_0, s_1, \ldots, s_m) \tag{8.45.6}$$

práve vtedy, keď

$$q_i \operatorname{Slv}(r_0, r_1, \ldots, r_m) \overset{T'}{\Longmapsto} q_j \operatorname{Slv}(s_0, s_1, \ldots, s_m) \tag{8.45.7}$$

Nech teraz m' je maximálny index registra v M-inštrukciách stroja Z (ak $Z = \emptyset$, položíme $m' = 0$) a $m = \max(m', n)$. Nájdime také T-stroje T_1, T_2, že

(1) T_1 obsahuje jedinú inštrukciu začínajúcu sa q_1 a jedinú inštrukciu končiacu sa q_u. T_2 obsahuje jedinú inštrukciu začínajúcu sa q_v a jedinú inštrukciu končiacu sa q_0. Okrem týchto výnimiek neobsahujú inštrukcie strojov T_1, T_2, T' žiadne rovnaké vnútorné stavy.

(2) pre všetky $k_0, k_1, \ldots, k_n \in \mathbb{N}$ platí

$$q_1 \operatorname{Slv}(k_1, \ldots, k_n) \overset{T_1}{\Longmapsto} q_u \operatorname{Slv}(0, k_1, \ldots, k_n, \underbrace{0, \ldots, 0}_{m-n})$$

(3) pre každé $r \in \mathbb{N}$, a $k_0, k_1, \ldots, k_r \in \mathbb{N}$

$$q_v \operatorname{Slv}(k_0, k_1, \ldots, k_r) \overset{T_2}{\Longmapsto} q_0 \operatorname{Slv}(k_0) \tag{8.45.8}$$

Teraz už môžeme vytvoriť stroj T:

$$T = T' \cup T_1 \cup T_2 \tag{8.45.9}$$

Dôkaz rovnosti $\Phi_Z^n = \Phi_T^n$ prenechávame čitateľovi ako cvičenie. □

Cvičenie 8.46. (a) Nakreslite blokové schémy strojov T_X pre $X = (q_i S_j P q_k)$, $X = (q_i S_j M q_k)$ a $X = (q_i S_j q_r q_s)$. (Samozrejme, úplne ich nakresliť možno len pre pevne zvolené j; urobte to aspoň pre $j \leq 2$.) V blokových schémach nevyznačujte vnútorné stavy okrem q_i, q_j, q_r, q_s.

(b) Udajte nejaký algoritmus na také doplňovanie vnútorných stavov v ľubovoľnej množine blokových schém z bodu a, ktoré zodpovedajú nejakému registrovému stroju Z, aby boli splnené podmienky z dôkazu vety 8.45!

(c) Dokážte, že množina T' zo vzťahu (8.45.5) je T-stroj!

(d) Dokážte, že (8.45.6) práve vtedy, keď (8.45.7)!

Cvičenie 8.47. (a) Pre pevne zvolené m nakreslite blokovú schému stroju T_1 z dôkazu vety 8.45! Nakreslite blokovú schému stroja T_2 z dôkazu vety 8.45! (V blokových schémach nevyznačujte vnútorné stavy okrem q_0, q_1, q_u, q_v.)

(b) Udajte algoritmus, ktorým možno prípustným spôsobom doplniť vnútorné stavy do blokových schém strojov T_1, T_2, ak je daný stroj T a blokové schémy z bodu (a).

(c) Dokážte, že množina T zo vzťahu (8.45.9) je Turingov stroj!

KAPITOLA 9

Ekvivalentnosť rekurzívnosti a T-vypočítateľnosti

V tejto kapitole dokážeme, že každá (čiastočne) T-vypočítateľná funkcia je (čiastočne) rekurzívna, čím dokončíme dôkaz vzájomnej ekvivalentnosti troch spresnení pojmu algoritmickej vypočítateľnosti. Potom rozšírime pojem rekurzívnosti a príbuzné pojmy na množiny slov, resp. čiastočné funkcie na množinách slov.

Definícia 9.1. (a) *Číslom T-inštrukcie* $(q_i a_j a_k L q_m)$ nazveme číslo $\mathrm{p}_{\mathrm{c}(i,j)}^{3\,\mathrm{c}(k,m)+1}$

(b) *Číslom T-inštrukcie* $(q_i a_j a_k N q_m)$ nazveme číslo $\mathrm{p}_{\mathrm{c}(i,j)}^{3\,\mathrm{c}(k,m)+2}$

(c) *Číslom T-inštrukcie* $(q_i a_j a_k P q_m)$ nazveme číslo $\mathrm{p}_{\mathrm{c}(i,j)}^{3\,\mathrm{c}(k,m)+3}$

(d) *Číslom Turingovho stroja* nazveme súčin čísel všetkých jeho inštrukcií.

Cvičenie 9.2. (a) Nájdite čísla T-inštrukcií $(q_1 a_3 a_4 L q_3)$, $(q_2 BIN q_3)$, $(q_2 OOP q_1)$.

(b) Nájdite T-inštrukcie, ktorých čísla sú 1048576, 16807, 15625, 361201.

(c) Nájdite číslo Turingovho stroja $\{(q_1 OIL q_2)\}$.

(d) Nájdite Turingov stroj, ktorého číslo je 27027000.

Poznámka 9.3. Turingov stroj s jedinou T-inštrukciou má rovnaké číslo ako táto inštrukcia. Aj ďalej sa bude vyskytovať prípad, že to isté číslo je číslom viacerých objektov; to nám však nebude prekážať, pokiaľ tieto objekty budú „rôznych druhov“, t.j. z rôznych množín, ktorých objekty číslujeme. Budeme len vyžadovať, aby rôzne objekty „rovnakého druhu“ mali rôzne čísla.

Cvičenie 9.4. (a) Zistite, ktoré prirodzené čísla sú číslami T-strojov!

(b) Nech n_1, n_2 sú čísla T-strojov T_1, T_2. Ak sú n_1, n_2 nesúdeliteľné, potom $T_1 \cup T_2$ je Turingov stroj. Dokážte!

Definícia 9.5. (a) *Číslom T-stavu* $a_{i_0} a_{i_1} \dots a_{i_{k-1}} q_j a_{i_{k+1}} \dots a_{i_n}$, $i_0 \neq 0$, $i_n \neq 0$ budeme nazývať číslo

$$2^{2i_0} \cdot 3^{2i_1} \cdots \mathrm{p}_{k-1}^{2i_{k-1}} \cdot \mathrm{p}_k^{2j+1} \cdot \mathrm{p}_{k+1}^{2i_{k+1}} \cdots \mathrm{p}_n^{2i_n}$$

(b) *Číslom konečnej postupnosti T-stavov* (špeciálne číslom výpočtu) $(X_0, X_1, \dots, X_n)$ budeme nazývať číslo

$$2^{\mathrm{n}(X_0)} \cdot 3^{\mathrm{n}(X_1)} \cdots \mathrm{p}_n^{\mathrm{n}(X_n)}$$

kde $\mathrm{n}(X_i)$ znamená číslo stavu X_i.

Príklad 9.6. Číslo stavu $OIOq_2IOI$ je $2^2 \cdot 3^4 \cdot 5^2 \cdot 7^5 \cdot 11^4 \cdot 13^2 \cdot 17^4$. Číslo stavu $q_1 BBIOI$ je $2^3 \cdot 7^4 \cdot 11^2 \cdot 13^4$. Číslo stavu $IOIBBq_3$ je $2^4 \cdot 3^2 \cdot 5^4 \cdot 13^7$.

Cvičenie 9.7. Určte, koľkociferné sú čísla T-stavov v príklade 9.6 v dekadickom zápise!

Cvičenie 9.8. Rozhodnite, či existujú T-stavy, ktorých čísla sú 3125000000, 999999, 171717 a ak áno, napíšte ich!

Cvičenie 9.9. Napíšte číslo konečnej postupnosti T-stavov ($q_1 0110$, $q_2 \mathrm{B}1110$, $q_0 01110$) a odhadnite počet jeho dekadických cifier!

V nasledujúcej definícií zavedieme niekoľko predikátov a funkcií.

Definícia 9.10. (a) $\mathrm{Tstv}(x)$ bude znamenať „existuje T-stav s číslom x“, inými slovami „x je číslom nejakého T-stavu“.

(b) $\mathrm{Prech}(x, y, z)$ bude znamenať „existujú také T-stavy X, Y s číslami x, y a taký T-stroj Z s číslom z, že $X \xrightarrow{Z} Y$“.

(c) $\mathrm{Tvýp}(x, y, z)$ bude znamenať „x je číslo výpočtu T-stroja číslo y zo stavu číslo z“.

(d) $\mathrm{Tvýp}_0(x, y, z)$ bude znamenať „$\mathrm{Tvýp}(x, y, z)$ a posledný člen vo výpočte číslo x sa začína vnútorným stavom q_0“.

Cvičenie 9.14. (a) Dokážte, že platí

$$\begin{aligned}\mathrm{Tvýp}(x,y,z) \iff \big((\forall i \le x)(\mathrm{ex}_{i+1}(x) \neq 0 \implies \\ \implies \mathrm{Prech}(\mathrm{ex}_i(x), \mathrm{ex}_{i+1}(x), y)) \wedge \\ \wedge\ x > 1 \wedge \mathrm{ex}_0(x) = z \wedge \\ \wedge\ \neg(\exists t \le x^z)\,\mathrm{Prech}(\mathrm{ex}(\mathrm{npr}(x) \dot{-} 1, x), t, y)\big)\end{aligned} \tag{9.14.1}$$

$$\begin{aligned}\mathrm{Tvýp}_0(x,y,z) \iff \mathrm{Tvýp}(x,y,z) \wedge \\ \wedge\ (\exists u \le x)\big(\mathrm{ex}(\mathrm{npr}(x), x) = 2 \cdot 3^2 \cdot \left(\prod_{i=0}^{n-1} p_{i+2}^4\right) \cdot p_u^2\big)\end{aligned} \tag{9.14.2}$$

(b) Dokážte, že predikáty Tvýp, $\mathrm{Tvýp}_0$ sú primitívne rekurzívne!
(c) Dokážte, že funkcia $\mathrm{tvýp}_0$ je primitívne rekurzívna!

Cvičenie 9.15. (a) Dokážte, že pre funkciu tobs platí

$$\mathrm{tobs}(x) = \left(\overline{\mathrm{sg}} \sum_{i=0}^{\mathrm{npr}(x)} \left| 1 - \sum_{j=0}^{x} \mathrm{ex}_j(\mathrm{ex}_i(x)) \ \mathrm{MOD}\ 2 \right| \right) \cdot \sum_{i=0}^{x} \overline{\mathrm{sg}}\,\big|4 - \mathrm{ex}_i\left(\mathrm{ex}(\mathrm{npr}(x), x)\right)\big| \tag{9.15.1}$$

(b) Dokážte, že funkcia tobs je primitívne rekurzívna!

Cvičenie 9.16. (a) Dokážte, že pre každé $n \in \mathbb{N}$ platí pre funkciu tvst^n vzorec:

$$\mathrm{tvst}^n(x_1,\ldots,x_n) = 2^3 * 2^2 * \left(\prod_{i=0}^{x_1-1} p_i^4\right) * 2^2 * \left(\prod_{i=0}^{x_2-1} \mathrm{p}_i^4\right) * \cdots * 2^2 * \left(\prod_{i=0}^{x_n-1} \mathrm{p}_i^4\right) * 2^2 \tag{9.16.1}$$

(b) Dokážte, že pre každé $n \in \mathbb{N}$ je funkcia tvst^n primitívne rekurzívna!

Teraz už môžeme pristúpiť ku konštrukcii univerzálnej čiastočnej funkcie pre množinu všetkých n-árnych čiastočne rekurzívnych funkcií.

Definícia 9.17. Pre každé $n \in \mathbb{N}$ definujme funkciu $\mathrm{tvýp}^{n+2}$ a čiastočnú funkciu Tun^{n+1} vzorcami:

$$\mathrm{tvýp}^{n+2}(x,y,x_1,\ldots,x_n) = \mathrm{tvýp}_0(x,y,\mathrm{tvst}^n(x_1,\ldots,x_n)) \tag{9.17.1}$$

$$\mathrm{Tun}^{n+1}(y,x_1,\ldots,x_n) = \mathrm{tobs}\left(\mu_x(\mathrm{tvýp}^{n+2}(x,y,x_1,\ldots,x_n) = 0)\right) \tag{9.17.2}$$

Cvičenie 9.18. Dokážte, že pre každé $n \in \mathbb{N}$ je $\mathrm{tvýp}^{n+2}$ primitívne rekurzívna funkcia a Tun^{n+1} čiastočne rekurzívna funkcia!

Cvičenie 9.19. (a) Ak y je číslo Turingovho stroja T, $u, x_1, \ldots, x_n \in \mathbb{N}$ tak $\Phi^n{}_T(x_1,\ldots,x_n) = u$ práve vtedy, keď $\mathrm{Tun}^{n+1}(y,x_1,\ldots,x_n) = u$. Dokážte!
(b) Pre $y = 0$ a všetky $x_1, \ldots, x_n \in \mathbb{N}$ platí:

$$\mathrm{Tun}^{n+1}(0,x_1,\ldots,x_n) = \mathrm{Tun}^{n+1}(1,x_1,\ldots,x_n) = \uparrow$$

Dokážte!

Z cvičenia 9.19 vyplýva

Veta 9.20. Pre každé $n \in \mathbb{N}$ je čiastočná funkcia Tun^{n+1} univerzálna čiastočná funkcia pre množinu všetkých n-árnych čiastočne T-vypočítateľných funkcií.

Pretože Tun^{n+1} je čiastočne rekurzívna funkcia, sú všetky čiastočne T-vypočítateľné funkcie čiastočne rekurzívne. Odtiaľto a z viet 6.17, 8.53 a 8.54 vyplýva nasledujúci veľmi dôležitý výsledok.

Veta 9.21. Pre každú (čiastočnú) funkciu f na množine $\mathbb{N}$ sú následujúce podmienky ekvivalentné:
(a) f je (čiastočne) M-vypočítateľná;
(b) f je (čiastočne) T-vypočítateľná;
(c) f je (čiastočne) rekurzívna.

Veta 9.31. Nech f je prosté zobrazenie množiny $\mathbb{N}$ na množinu $\mathbb{N}$ a nech X, Y sú také S-množiny, že

$$Y = \{a_{f(i_1)}a_{f(i_2)}\dots a_{f(i_n)} \mid a_{i_1}a_{i_2}\dots a_{i_n} \in X\} \tag{9.31.1}$$

Potom

(a) S-množina X je (primitívne) rekurzívna práve vtedy, keď S-množina Y je (primitívne) rekurzívna.

(b) S-množina X je rekurzívne spočítateľná práve vtedy, keď S-množina Y je rekurzívne spočítateľná.

Dôkaz: Existuje taká konečná podmnožina $A = \{a_1, a_2, \dots, a_n\}$ množiny $\overline{A}$, že $X \subseteq A^*$, $Y \subseteq A^*$. Nech h je také ľubovoľné zobrazenie množiny $\{1, 2, \dots, n\}$ na seba, že $h(i) = f(i)$, ak $1 \leq i \leq n$ a $f(i) \leq n$. Takéto zobrazenie zrejme existuje. Definujme teraz funkciu g:

$$g(x) = \begin{cases} x, & \text{ak } x > n \text{ alebo } x = 0 \\ h(x), & \text{ak } x \leq n \text{ a } x \neq 0 \end{cases}$$

Funkcia g je zrejme primitívne rekurzívna a okrem toho v (9.31.1) môžeme písať g miesto f. Teraz už ľahko vyjadríme charakteristickú funkciu χ_X množiny $\mathrm{Num}(X)$ pomocou charakteristickej funkcie χ_Y množiny $\mathrm{Num}\,(Y)$ a obrátene takým spôsobom, aby sa pri týchto vyjadreniach zachovala (primitívna) rekurzívnosť. Pre bod (b) treba analogicky použiť čiastočné charakteristické funkcie množín $\mathrm{Num}(X)$, $\mathrm{Num}(Y)$ a všímať si ich čiastočnú rekurzívnosť. □

Poznámka 9.32. Na začiatku kapitoly 7 sme uviedli, že niekedy budeme zostavovať slová aj z iných symbolov ako z prvkov množiny $\overline{A}$, ale že budeme tieto symboly považovať za stotožnené s niektorými symbolmi množiny $\overline{A}$. Pritom spôsob stotožnenia sme vo všeobecnosti neuviedli. Veta 9.31 ukazuje, že pre množiny slov zostavených z konečne mnohých symbolov nie je spôsob stotožnenia zložitý, pokiaľ sa zaujímame o primitívnu rekurzívnosť, rekurzívnosť alebo rekurzívnu spočítateľnosť. Preto budeme tieto pojmy v príkladoch a cvičeniach používať i pre také množiny slov.

Cvičenie 9.33. Každá regulárna množina je primitívne rekurzívna. Dokážte!

Cvičenie 9.34. Dokážte, že ternárny predikát $\mathrm{Zr}(x, y, z)$ na množine $\mathbb{N}$, znamenajúci „existujú také slová w_1, w_2, že $x = \mathrm{num}(w_1)$, $y = \mathrm{num}(w_2)$, $z = \mathrm{num}(w_1w_2)$“, je primitívne rekurzívny!

Cvičenie 9.35. (a) Ak X, Y sú (primitívne) rekurzívne S-množiny tak aj XY, X^R, X^*, X^+ sú (primitívne) rekurzívne S-množiny. Dokážte!

(b) Ak X, Y sú rekurzívne spočítateľné S-množiny, tak aj XY, X^*, X^+, X^R sú rekurzívne spočítateľné S-množiny. Dokážte!

Poznámka 9.36. Rekurzívne spočítateľné S-množiny sa niekedy v literatúre nazývajú aj jazykmi typu 0.

Definícia 9.37. Čiastočné zobrazenie $\varkappa$ množiny všetkých slov do množiny všetkých slov budeme nazývať *S-zobrazením*, ak existujú také S-množiny X, Y, že $\varkappa$ je čiastočným zobrazením S-množiny X do S-množiny Y.

Poznámka 9.38. Slovo „čiastočným“ v predchádzajúcej definícii sme zrejme mohli vynechať. Niekedy budeme hovoriť „čiastočné S-zobrazenie $\varkappa$“ miesto „S-zobrazenie“, zvlášť vtedy, keď budeme súčasne hovoriť o nejakých takých konkrétnych S-množinách X, Y, že $\varkappa$ bude čiastočným zobrazením X do Y, ale nie zobrazením X do Y.

Definícia 9.39. Budeme hovoriť, že unárna čiastočná funkcia f na množine $\mathbb{N}$ je *číselná čiastočná funkcia priradená S-zobrazeniu $\varkappa$*, a písať $f = \mathrm{Num}(\varkappa)$, ak pre všetky $x, y \in \mathbb{N}$ platí $f(x) = y$ práve vtedy, keď existujú také slová w_1, w_2, že $x = \mathrm{num}(w_1)$, $y = \mathrm{num}(w_2)$ a $\varkappa(w_1) = w_2$.

Príklad 9.40. Nech $\varkappa = \{\langle OI, IO\rangle, \langle OOO, II\rangle, \langle IO, \varepsilon\rangle, \langle \varepsilon, III\rangle\}$ a $f = \mathrm{Num}(\varkappa)$. Potom $f(324) = 144$, $f(900) = 12396$, $f(144) = 1$, $f(1) = 81000$ a $f(x) = \uparrow$ pre ostatné $x \in \mathbb{N}$.

Cvičenie 9.41. Dokážte, že pre žiadne S-zobrazenie $\varkappa$ nie je $\mathrm{Num}(\varkappa)$ totálna funkcia!

Cvičenie 9.48. (a) Dokážte, že existujú také primitívne rekurzívne funkcie f, g, že pre všetky slová x platí

$$f(\mathrm{num}(q_1x)) = \mathrm{num}(x), \qquad g(\mathrm{num}(x)) = \mathrm{num}(q_0x)$$

(b) Dokážte, že pre každý Turingov stroj T je Rez_T čiastočne rekurzívne S-zobrazenie.

Z cvičenia 9.48 a poznámky 8.23 vyplýva:

Veta 9.49. Ak je hromadná úloha $\mathcal{H} = (A_1, A_2, Z, \varkappa)$ riešiteľná Turingovým strojom, tak existuje také čiastočne rekurzívne S-zobrazenie $\varkappa_1$, že pre všetky $x \in Z$ platí $\varkappa(x) = \varkappa_1(x)$.

Teraz sa budeme snažiť dokázať obrátenie tejto vety.

Cvičenie 9.50. Nech $n \in \mathbb{N}$, $n \neq 0$, $A = \{a_1, a_2, \ldots, a_n\}$.

(a) Dokážte, že existuje taký Turingov stroj T_1, že pre všetky slová $a_{k_1}a_{k_2}\ldots a_{k_j} \in A^*$ platí

$$q_1a_{k_1}a_{k_2}\ldots a_{k_j} \overset{T_1}{\Longmapsto} q_0\,\mathrm{Slv}(2k_1, 2k_2, \ldots, 2k_j) \tag{9.50.1}$$

(b) Dokážte, že existuje taký Turingov stroj T_2, že pre všetky $j \in \mathbb{N}$ a všetky $k_1, k_2, \ldots, k_j \in \mathbb{N}$ platí

$$q_1\,\mathrm{Slv}(k_1, k_2, \ldots, k_j) \overset{T_2}{\Longmapsto} q_0\,\mathrm{Slv}(k_1 * k_2 * \cdots * k_j) \tag{9.50.2}$$

(c) Dokážte, že existuje taký Turingov stroj T_3, že pre všetky $w \in A^*$ platí

$$q_1w \overset{T_3}{\Longmapsto} q_0OI^{\mathrm{num}(w)}O \tag{9.50.3}$$

(d) Dokážte, že existuje taký Turingov stroj T_4, že pre všetky $x \in \mathbb{N}$ platí

$$q_1OI^xO \overset{T_4}{\Longmapsto} q_0\,\mathrm{Slv}\left(\mathrm{ex}_0(x), \mathrm{ex}_1(x), \ldots, \mathrm{ex}_{\mathrm{npr}(x) \dot{-} 1}(x)\right) \tag{9.50.4}$$

(e) Dokážte, že existuje taký Turingov stroj T_5, že pre všetky $j \in \mathbb{N}$ a všetky $k_1, k_2, \ldots, k_j \in \mathbb{N}$, $1 \leq k_i \leq n$ pre $i = 1, 2, \ldots, j$, platí

$$q_1\,\mathrm{Slv}(2k_1, 2k_2, \ldots, 2k_j) \overset{T_5}{\Longmapsto} q_0a_{k_1}a_{k_2}\ldots a_{k_j} \tag{9.50.5}$$

(f) Dokážte, že existuje taký Turingov stroj T_6, že pre každé slovo $w \in A^*$ platí

$$q_1OI^{\mathrm{num}(w)}O \overset{T_6}{\Longmapsto} q_0w \tag{9.50.6}$$

Veta 9.51. Ku každému čiastočne rekurzívnemu S-zobrazeniu $\varkappa$ existuje taký Turingov stroj T, že $\varkappa = \mathrm{Rez_T}$.

Dôkaz: Označme $A = \{a_1, \ldots, a_n\}$, kde $n \neq 0$ je také najmenšie prirodzené číslo, že $\varkappa$ je čiastočné zobrazenie množiny A do A. Pretože zobrazenie $\varkappa$ je čiastočne rekurzívne, existuje taký Turingov stroj T', že $\mathrm{Num}(\varkappa) = \Phi^1_{T'}$, teda pre všetky w z oboru definície zobrazenia $\varkappa$ platí

$$q_1OI^{\mathrm{num}(w)}O \overset{T'}{\Longmapsto} q_0OI^{\mathrm{num}(\varkappa(w))}O \tag{9.51.1}$$

Budeme ďalej predpokladať, že pre ostatné slová w je výpočet stroja T' zo stavu $q_1OI^{\mathrm{num}(w)}O$ nekonečný. Nech T_3, T_6 sú T-stroje z cvičenia 9.50. Zo strojov T_3, T_6, T' sa už ľahko dá zostaviť taký stroj T, že pre všetky slová w z oboru definície zobrazenia $\varkappa$ platí

$$q_1w \overset{T}{\Longrightarrow} q_2OI^{\mathrm{num}(w)}O \overset{T}{\Longrightarrow} q_3OI^{\mathrm{num}(\varkappa(w))}O \overset{T}{\Longrightarrow} q_0w \quad \square$$

Cvičenie 9.52. Opíšte, ako treba zmeniť Turingove stroje T_3, T_6, T' na také Turingove stroje T_3', T'', T_6', aby sme v dôkaze vety 9.51 mohli použiť $T = T_3' \cup T'' \cup T_6'$!

Teraz už môžeme dokázať obrátenie vety 9.49. K čiastočne rekurzívnemu zobrazeniu $\varkappa_1$ existuje taký Turingov stroj T, že $\varkappa_1 = \mathrm{Rez_T}$, a teda pre všetky $x \in Z$ platí $\varkappa_1(x) = \mathrm{Rez_T}(x)$. Ľahko možno zariadiť, aby abeceda stroja T obsahovala všetky prvky množín A_1, A_2. Potom Turingov stroj T rieši hromadnú úlohu $\mathcal{H}$, a teda táto hromadná úloha je T-strojove riešiteľná.

Vyslovíme teraz vetu 9.49 spolu s jej obrátením.

KAPITOLA 10

Churchova téza

Cieľom teórie algoritmov je skúmať algoritmy a algoritmicky (čiastočne) vypočítateľné funkcie (napríklad na množine $\mathbb{N}$, ale aj na iných množinách). Pojem algoritmu nie je pravdepodobne možné úplne všeobecne definovať, a to je dôvod, prečo sme skúmali iba isté špeciálne triedy algoritmov. Uvedieme však aspoň základné črty algoritmov, ktoré formuloval A. A. Markov (pozri [6], str. 10–11).

10.1. Diskrétnosť algoritmu: Algoritmus je proces postupného zostrojovania veličín, ktorý postupuje v diskrétnom čase tak, že v počiatočnom časovom okamihu je daný konečný systém veličín a systém veličín v niektorom okamihu (okrem počiatočného) vzniká zo systému veličín v predchádzajúcom okamihu podľa istého zákona (programu).

10.2. Determinističnosť algoritmu: Systém veličín v ľubovoľnom (nie počiatočnom) okamihu je jednoznačne určený systémom veličín v predchádzajúcom okamihu.

10.3. Elementárnosť krokov algoritmu: Pravidlo, podľa ktorého vzniká nasledujúci systém veličín z predchádzajúceho, musí byť jednoduché.

10.4. Rezultatívnosť algoritmu: Ak z daného systému veličín už nemožno dostať podľa príslušného pravidla nasledujúci systém, musí byť určené, čo treba pokladať za výsledok algoritmu.

10.5. Hromadnosť algoritmu: Počiatočný systém veličín sa môže vyberať z nejakej (potenciálne) nekonečnej množiny.

Na vysvetlenie týchto rysov algoritmu poznamenajme, že pojem „veličina“ netreba chápať len ako číslo, ale že to môže byť aj slovo v nejakej abecede alebo aj objekt iného druhu, s ktorým algoritmus pracuje.

Elementárnosť krokov je veľmi relatívny pojem; to, čo sa pokladá za elementárny krok v jednom algoritme, nemusí byť elementárnym krokom v inom algoritme. Napríklad aritmetické operácie s racionálnymi číslami pokladáme obvykle za elementárne kroky pri riešení sústav lineárnych rovníc s racionálnymi koeficientmi. Pritom na vykonávanie týchto operácií používame iné algoritmy, ktorých elementárnymi krokmi niekedy bývajú algoritmy pre aritmetické operácie s prirodzenými číslami, a na vykonávanie týchto operácií máme ďalšie algoritmy.

K pojmu hromadnosti poznamenajme, že z praktického hľadiska sú dôležité aj prípady, keď algoritmus možno aplikovať len na konečný, ale veľmi veľký počet vstupných systémov veličín. V takýchto prípadoch je v teórii vhodnejšie abstrahovať od konečnosti množiny vstupných systémov veličín. Algoritmy založené na princípe prebratia všetkých možností bývajú tu totiž prakticky bezcenné.

My sme sa zaoberali hlavne algoritmami na počítanie čiastočných funkcií na množine $\mathbb{N}$ a preskúmali sme tieto tri spresnenia pojmu algoritmicky (čiastočne) vypočítateľných funkcií:

- (čiastočne) rekurzívne funkcie
- (čiastočne) M-vypočítateľné funkcie
- (čiastočne) T-vypočítateľné funkcie

Vzhľadom na to, že vo všetkých troch prípadoch ide o spresnenie toho istého pojmu, neprekvapuje nás, že tieto tri pojmy majú mnoho spoločných vlastností. Videli sme však, že tieto pojmy majú spoločné dokonca všetky vlastnosti, že sú ekvivalentné (pozri vetu 9.21). Matematici preskúmali mnoho ďalších spresnení pojmu algoritmicky (čiastočne) vypočítateľných funkcií, a vo všetkých prípadoch sa ukázalo, že tieto pojmy sú ekvivalentné s našimi troma pojmami. To viedlo rôznych matematikov k vysloveniu nasledujúcej hypotézy:

10.6. Churchova téza: Systém všetkých algoritmicky (čiastočne) vypočítateľných funkcií na množine $\mathbb{N}$ je totožný so systémom všetkých (čiastočne) rekurzívnych funkcií (na množine $\mathbb{N}$).

1. polož $x = 0$ a prejde k bodu 2;
2. urobí x krokov algoritmu A pre usporiadanú n-ticu s číslom $q(x)$, ak práca algoritmu A neskončí skôr. Ak vyšla odpoveď „áno“, vydá B ako výsledok usporiadanú n-ticu s číslom $q(x)$. Potom prejde k bodu 3;
3. zväčší x o jednotku a prejde k bodu 2.

Obrátene, nech B je algoritmus z 10.10. Hľadajme algoritmus A z 10.8(d). V tomto prípade stačí zrejme porovnávať výsledky, ktoré vydáva algoritmus B, s n-ticou $x_1, \ldots, x_n$, a ak niekedy nastane rovnosť, ukončiť prácu a vydať odpoveď „áno“. Teraz už môžeme veľmi jednoducho zdôvodniť vetu 4.44.

Ak sú množiny M, $\mathbb{N}^n \setminus M$ rekurzívne spočítateľné, existujú algoritmy A, B, ktoré generujú množiny M, $\mathbb{N}^n \setminus M$. Utvorme teraz algoritmus C, ktorý bude pre danú n-ticu $(x_1, \ldots, x_n) \in M$ robiť striedavo jeden krok algoritmu A a jeden krok algoritmu B, a v prípade, že niektorý z algoritmov A, B dá výsledok, porovná ho s n-ticou $(x_1, \ldots, x_n)$. Ak vyjde rovnosť, práca algoritmu C sa skončí, a C vydá výsledok „áno“, resp. „nie“ podľa toho, či nastala rovnosť s niektorým výsledkom algoritmu A, resp. B. Poznamenajme, že dôkaz vety 4.44 sa v podstate zakladal na tejto myšlienke.

Cvičenie 10.11. Ukážte, že generujúci algoritmus možno upraviť tak, aby nedával viackrát ten istý výsledok!

Cvičenie 10.12. Zdôvodnite pomocou Churchovej tézy vety:

(a) Množina $M \subseteq \mathbb{N}$ je rekurzívne spočítateľná práve vtedy, keď je množinou hodnôt čiastočne rekurzívnej funkcie.

(b) Neprázdna množina $M \subseteq \mathbb{N}$ je rekurzívne spočítateľná práve vtedy, keď je množinou hodnôt rekurzívnej funkcie.

(c) Nekonečná množina $M \subseteq \mathbb{N}$ je rekurzívne spočítateľná práve vtedy, keď je množinou hodnôt prostej rekurzívnej funkcie.

(d) Neprázdna množina $M \subseteq \mathbb{N}$ je rekurzívna práve vtedy, keď je množinou hodnôt neklesajúcej rekurzívnej funkcie.

(e) Nekonečná množina $M \subseteq \mathbb{N}$ je rekurzívna práve vtedy, keď je množinou hodnôt rastúcej rekurzívnej funkcie.

Cvičenie 10.13. Dokážte vety z predchádzajúceho cvičenia!

Na záver poznamenajme, že tak ako sme použili Churchovu tézu pre podmnožiny množín $\mathbb{N}$ a $\mathbb{N}^n$ a pre čiastočné funkcie na $\mathbb{N}$, mohli by sme ju použiť, prípadne s malými a z definícií zrejmými modifikáciami, aj pre S-množiny a S-zobrazenia. Tým sa však nebudeme podrobnejšie zaoberať. Pojmy primitívnej rekurzívnosti či už množín alebo funkcií však nie je možné pomocou Churchovej tézy jednoducho charakterizovať.

Nejde tak veľmi o to, že číslo 1 má dva dekadické rozvoje, ale o to, že ešte neznáme číslice vždy môžu spôsobiť to, že výsledok je väčší než 1 i to, že je menší než 1. Pritom ľahko skonštruujeme zariadenie, ktoré dáva ľubovoľne krátke intervaly obsahujúce výsledok.

Teraz začneme postupovať formálnejšie. Pritom spôsob, ktorý použijeme, sa bude podobať na intervalový v tej jeho podstatnej vlastnosti, že sa vždy pripúšťajú odchýlky aproximácií na obe strany. V ďalšom bude pre nás výhodné rozšíriť pojem (primitívnej) rekurzívnosti na postupnosti racionálnych (špeciálne, celých) čísel a na niektoré postupnosti intervalov.

Definícia 11.2. Postupnosť racionálnych čísel $(c_0, c_1, c_2, \dots)$ budeme nazývať *(primitívne) rekurzívnou*, ak existujú unárne (primitívne) rekurzívne funkcie f, g, h také, že pre všetky $x \in \mathbb{N}$ platí

$$c_x = \frac{(-1)^{f(x)} \cdot g(x)}{h(x)}$$

Postupnosť otvorených (alebo uzavretých) intervalov s racionálnymi koncami nazveme *(primitívne) rekurzívnou*, ak postupnosť ľavých i postupnosť pravých koncových bodov týchto intervalov je (primitívne) rekurzívna.

Ak by sme chceli (primitívnu) rekurzívnosť zaviesť i pre postupnosti intervalov všetkých štyroch typov (ale zasa s racionálnymi koncami), museli by sme pridať príslušnú podmienku na striedanie typov intervalov.

Pre reprezentáciu reálnych čísel budeme používať postupnosti celých čísel, t.j. funkcie s oborom definície $\mathbb{N}$ a s oborom hodnôt $\mathbb{Z}$. Budeme ich chápať ako postupnosti čitateľov vhodných cauchyovských postupností; pritom ich postupnosť menovateľov $(1, 1, 2, 3, 4, \dots)$ bude stále rovnaká (vyhli sme sa menovateľu 0). Namiesto každej takejto funkcie f by sme mohli použiť dvojicu (g, h) funkcií na množine $\mathbb{N}$ takých, že pre všetky $x \in \mathbb{N}$ platí

$$f(x) = (-1)^{g(x)} \cdot h(x) \qquad \text{a} \qquad g(x) \leq \min(1, h(x)) \tag{11.2.1}$$

Druhá podmienka je tu len kvôli jednoznačnosti g. Neformálne povedané, g tu určuje znamienko a h absolútnu hodnotu; nulu uvažujeme len so znamienkom plus. (Iná možnosť by bola obmedziť sa najprv len na nezáporné rekurzívne reálne čísla; podľa cvičenia 11.11 by to nebolo podstatné obmedzenie.)

Definícia 11.3. Budeme hovoriť, že funkcia $f\colon \mathbb{N} \to \mathbb{Z}$ *reprezentuje reálne číslo* α, ak pre všetky $x \in \mathbb{N}$ platí

$$|\alpha x - f(x)| < 1 \tag{11.3.1}$$

Všimnime si, že (11.3.1) znamená, že (pre $x \neq 0$) číslo $\frac{f(x)}{x}$ aproximuje α s chybou menšou než $\frac{1}{x}$. Ak poznáme hodnoty $f(1)$, $f(2)$, $\dots$, $f(k)$, tak vieme, že

$$\max\left\{\frac{f(x)-1}{x} \;\middle|\; 1 \leq x \leq k\right\} < \alpha < \min\left\{\frac{f(x)+1}{x} \;\middle|\; 1 \leq x \leq k\right\}$$

Cvičenie 11.4. Dokážte (alebo vyvráťte) nasledujúce tvrdenia:

(a) Každé reálne číslo je reprezentované aspoň jednou funkciou $f\colon \mathbb{N} \to \mathbb{Z}$.
(b) Každá funkcia $f\colon \mathbb{N} \to \mathbb{Z}$ reprezentuje najviac jedno reálne číslo.
(c) Každé celé číslo α je reprezentované práve jednou funkciou $f\colon \mathbb{N} \to \mathbb{Z}$.
(d) Ak je reálne číslo α reprezentované práve jednou funkciou $f\colon \mathbb{N} \to \mathbb{Z}$, tak $\alpha \in \mathbb{Z}$.

Cvičenie 11.5. Nahraďme číslo 1 v nerovnosti (11.3.1)

- číslom 2
- číslom $\frac{2}{3}$
- číslom $\frac{1}{3}$
- číslom $\frac{1}{2}$

Ktoré z tvrdení predchádzajúceho cvičenia budú platiť v jednotlivých prípadoch? Zmení sa niektorá odpoveď, ak ešte nahradíme znak „$<$“ znakom „$\leq$“?

Teda h reprezentuje $\alpha+\beta$. Úvahy pre rozdiel sú skoro rovnaké; možno tiež využiť cvičenie 11.11. Pre súčin položíme $M = 2+\max\big(|f(1)|,|g(1)|\big)$ a definujeme

$$h(x) = \left\lfloor \frac{f(4Mx)\cdot g(4Mx)}{16M^2x} + \frac{1}{2} \right\rfloor \quad \text{pre } x>0 \quad \text{a} \quad h(0)=0.$$

Odhad pre $x=0$ je triviálny a pre $x>0$ platí

$$\begin{aligned} |\alpha\beta\cdot x - h(x)| &= \frac{1}{2} + \left|\alpha\beta\cdot x - \frac{f(4Mx)\cdot g(4Mx)}{16M^2x}\right| = \\ &= \frac{1}{2} + \frac{1}{4M}\left|\alpha\cdot\big(\beta\cdot 4Mx - g(4Mx)\big) + \frac{g(4Mx)}{4Mx}\cdot\big(\alpha\cdot 4Mx - f(4Mx)\big)\right| < \\ &< \frac{1}{2} + \frac{1}{4M}\big(|\alpha|\cdot 1 + (|\beta|+1)\cdot 1\big) \le 1 \end{aligned}$$

Namiesto podielu stačí uvažovať prevrátenú hodnotu, a to len ku kladnému rekurzívnemu reálnemu číslu α. Potrebujeme ho odhadnúť zdola kladným racionálnym číslom. Na to nájdeme najmenšie c také, že $f(c)\ge 2$; potom vieme, že $\alpha > \frac{1}{c}$. Dokážeme, že funkcia $h(x) = \left\lfloor \frac{x\cdot(2c^2x+c)}{f(2c^2x+c)} + \frac{1}{2}\right\rfloor$ reprezentuje číslo $\frac{1}{\alpha}$. Skutočne, pre každé $x>0$ platí

$$\begin{aligned} \left|\frac{x}{\alpha} - h(x)\right| &\le \frac{1}{2} + \left|\frac{x}{\alpha} - \frac{x\cdot(2c^2x+c)}{f(2c^2x+c)}\right| = \frac{1}{2} + x\cdot\left|\frac{1}{\alpha} - \frac{2c^2x+c}{f(2c^2x+c)}\right| = \\ &= \frac{1}{2} + x\cdot\frac{\big|f(2c^2x+c) - \alpha\cdot(2c^2x+c)\big|}{\alpha\cdot f(2c^2x+c)} < \\ &< \frac{1}{2} + x\cdot\frac{1}{\alpha\cdot f(2c^2x+c)} < \frac{1}{2} + \frac{x}{\alpha\cdot 2cx} < \frac{1}{2} + \frac{x}{2x} = 1 \quad \square \end{aligned}$$

Nazvime *p-adickým rozvojom* čísla $\alpha\ge 0$ funkciu f takú, že pre každé $n>0$ je $f(n)$ n-tá číslica p-adického rozvoja čísla α (za „p-adickou“ bodkou). V prípade nejednoznačnosti rozvoja dáme prednosť nekonečne mnohým nulám. Pre určitosť ešte definujeme $f(0) = \lfloor \alpha x\rfloor$.

Veta 11.14. Pre nezáporné reálne číslo α a celé $p>1$ sú nasledujúce podmienky ekvivalentné:

(a) α je rekurzívne reálne číslo;
(b) funkcia $\lfloor \alpha x\rfloor$ je rekurzívna;
(c) p-adický rozvoj čísla α je rekurzívny.

Dôkaz: Dôkazy implikácií (b) $\Longrightarrow$ (c), (c) $\Longrightarrow$ (a) sú ľahké a prenechávame ich čitateľovi. Pre implikáciu (a) $\Longrightarrow$ (b) rozlíšme prípady α racionálne a α iracionálne. Pre α racionálne (b) zrejme platí: o funkcii $\lfloor \alpha x\rfloor$ vieme, že je rekurzívna (dokonca primitívne rekurzívna).

Nech teraz α je iracionálne, a nech rekurzívna funkcia f reprezentuje číslo α. Ak chceme vypočítať $\lfloor \alpha x\rfloor$ pre $x>0$, uvedomme si najprv, že pre každé $y>0$ platí $|\alpha xy - f(xy)|<1$, a preto

$$\frac{f(xy)-1}{y} < \alpha x < \frac{f(xy)+1}{y} \tag{11.14.1}$$

Číslo αx nie je celé. Zvoľme y tak, že vzdialenosť αx od najbližšieho celého čísla je väčšia než $\frac{1}{y}$. Potom oba krajné výrazy v (11.14.1) majú rovnakú celú časť; je to potom aj celá časť stredného výrazu. Teda rekurzívnosť funkcie $\lfloor \alpha x\rfloor$ môžeme dokázať tak, že najprv nadefinujeme pomocnú funkciu

$$h(x) = \mu_y\left(\left\lfloor \frac{f(xy)-1}{y+\overline{\mathrm{sg}}(y)}\right\rfloor = \left\lfloor \frac{f(xy)+1}{y+\overline{\mathrm{sg}}(y)}\right\rfloor\right)$$

Podľa vyššie urobených úvah je táto minimalizácia regulárna. (Členy $\overline{\mathrm{sg}}(y)$ v menovateľoch len zabraňujú deleniu nulou. Striktne vzaté, mali by sme výraz vpravo ešte trochu upraviť.) Potom využijeme vyjadrenie

$$\lfloor \alpha x\rfloor = \left\lfloor \frac{f\big(x\cdot h(x)\big)}{h(x)}\right\rfloor \quad \square$$

Dôkaz: Môžeme postupovať rovnako ako vyššie, ale s funkciou h, ktorej obor hodnôt je rekurzívna, no nie primitívne rekurzívna množina. Tu je dôležité, že vo vyjadrení (11.19.2) sa nepoužíva minimalizácia. □

Prechodom k opačným číslam by sme dostali obdobné príklady klesajúcich postupností. Vzhľadom na vetu 11.19 je zaujímavé nasledujúce tvrdenie. Dôkaz nie je ťažký a prenechávame ho čitateľovi.

Veta 11.21. Pre ľubovoľné reálne číslo α sú ekvivalentné nasledujúce podmienky:

(a) α je rekurzívne reálne číslo;
(b) α je limitou rastúcej rekurzívnej postupnosti racionálnych čísel a súčasne limitou klesajúcej rekurzívnej postupnosti racionálnych čísel;
(c) α je limitou rastúcej primitívne rekurzívnej postupnosti racionálnych čísel a súčasne limitou klesajúcej primitívne rekurzívnej postupnosti racionálnych čísel;
(d) α patrí do prieniku (primitívne) rekurzívnej postupnosti intervalov s racionálnymi koncami, ktorých dĺžky konvergujú k nule.

V poslednom bode vety nezáleží na type uvažovaných intervalov. Ale len pre postupnosti uzavretých a do seba zapadajúcich intervalov je zaručená neprázdnosť podobných prienikov.

Cvičenie 11.22. Nájdite postupnosť do seba zapadajúcich

(a) otvorených
(b) zľava otvorených, sprava uzavretých
(c) zľava uzavretých, sprava otvorených

intervalov (s racionálnymi koncami), ktorej prienik je prázdny.

Poznámka 11.23. Všimnime si, že vo vete 11.21 aj primitívne rekurzívne postupnosti racionálnych čísel alebo intervalov charakterizujú rekurzívne (a nie primitívne rekurzívne) reálne čísla. Na charakterizáciu primitívne rekurzívnych reálnych čísel by bolo treba vhodne vziať do úvahy aj rýchlosť konvergencie vzhľadom k veľkosti príslušných menovateľov.

Teraz sa budeme zaoberať niektorými algoritmickými problémami pre rekurzívne reálne čísla. Aby sme to mohli robiť, musíme ich nejako konečne reprezentovať. Priradíme rekurzívne reálne čísla (niektorým) registrovým strojom. (Častý je trochu abstraktnejší prístup, keď sa rekurzívne reálne čísla vhodným spôsobom priradia niektorým prirodzeným číslam. My by sme sa k istému takémuto spôsobu najľahšie dostali cez číslovanie registrových strojov.) Pretože registrové stroje nemôžu bezprostredne počítať so zápornými celými číslami, necháme ich istým spôsobom počítať dve funkcie g, h na $\mathbb{N}$, ktoré kódujú jednu funkciu $f\colon \mathbb{N} \to \mathbb{Z}$. (Zvolili sme jednu z mnohých, v podstate rovnocenných možností.) Dôkazy budeme len naznačovať, a to s využitím Churchovej tézy.

Definícia 11.24. Budeme hovoriť, že registrový stroj Z *reprezentuje reálne číslo* α, ak existuje funkcia $f\colon \mathbb{N} \to \mathbb{Z}$, ktorá reprezentuje α a unárne funkcie g, h na $\mathbb{N}$ také, že pre každé $x \in \mathbb{N}$ platí (11.2.1) a

$$(q_1; 0, x) \overset{Z}{\Longrightarrow} (q_0; h(x), x, g(x), b_1, \ldots, b_k)$$

pre nejaké $k \in \mathbb{N}$ a $b_1, \ldots, b_k \in \mathbb{N}$.

Ľubovoľné reálne číslo je rekurzívne práve vtedy, keď je reprezentované nejakým registrovým strojom; tento stroj nie je jednoznačne určený. Nie každý registrový stroj reprezentuje nejaké reálne číslo, ale ak áno, toto číslo je zrejme jednoznačne určené.

Veta 11.25. K daným dvom registrovým strojom Z_1, Z_2 možno zostrojiť registrové stroje Z_3, Z_4, Z_5, Z_6, že platí: Ak Z_1, Z_2 reprezentujú reálne čísla α, β, tak Z_3, Z_4, Z_5 po rade reprezentujú $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$; ak navyše $\beta \neq 0$, tak Z_6 reprezentuje $\frac{\alpha}{\beta}$.

Veta 11.26. Existujú primitívne rekurzívne funkcie h_3, h_4, h_5, h_6 také, že ak vo vete 11.25 sú Z_1, Z_2 registrové stroje s číslami u, v, tak za Z_3, Z_4, Z_5, Z_6 možno zobrať registrové stroje s číslami $h_3(u, v)$, $h_4(u, v)$, $h_5(u, v)$, $h_6(u, v)$.

Dôkaz: Pre obe vety v podstate stačí sledovať dôkaz vety 11.13. (Netreba žiadne špeciálne konštrukcie, stačí „nekaziť úmyselne“.) □

Na záver tejto kapitoly ešte zrejmým spôsobom rozšírime uvažované pojmy i na komplexné čísla.

Definícia 11.33. Komplexné číslo budeme nazývať *(primitívne) rekurzívnym*, ak obe jeho zložky sú (primitívne) rekurzívne.

Veta 11.34. Množina všetkých (primitívne) rekurzívnych komplexných čísel tvorí algebraicky uzavreté pole (špeciálne, obsahuje všetky algebraické čísla). Je tiež uzavretá vzhľadom na operáciu umocňovania, logaritmus, goniometrické a cyklometrické funkcie.

Pre dôkaz možno využiť bežné metódy numerického riešenia algebraických rovníc, resp. výpočtu hodnôt uvedených funkcií. Zoznam funkcií by bolo možné podstatne rozšíriť, napríklad o hodnoty integrálov. (Poznamenajme, že pri uzavretosti na čiastočnú funkciu uvažujeme len jej definované hodnoty. Pre „mnohohodnotové“ analytické funkcie možno brať všetky ich hodnoty.)

je vstupný vnútorný stav niektorej jeho skupiny inštrukcií, tak $F(x,i) = 3j + k$, kde $0 \leq k \leq 2$, určuje typ skupiny a j je index výstupného vnútorného stavu (ak sú dva, tak nižší).

Čítač inštrukcií počíta hodnotu $F(x,i)$, kde x je číslo simulovaného stroja (uložené v R_1) a i je obsah R_4 (prípadne zväčšený o 1). Počíta tak, že $x+1$ postupne delí číslami $1, 2, 3, \ldots$ (pričom počíta len zvyšok, nie podiel) a vždy, keď narazí na nenulový zvyšok, zmenší obsah registra R_4. Deliteľ sa uchováva ako súčet obsahov registrov R_5, R_6, číslo stroja ako súčet obsahov registrov R_1, R_7. (Delenec je $x+1$, hoci sa uchováva x.) Vnútorné stavy q_7 až q_{12} (a celé zodpovedajúce inštrukcie) zodpovedajú jednému odčítaniu deliteľa od delenca, vnútorné stavy q_4 až q_6 obnove deliteľa v R_6, pri vstupe cez šípku zľava zväčšeniu deliteľa o 1. Vnútorné stavy q_1 až q_3 slúžia na presun obsahu z R_1 do R_7.

Pri výstupe z čítača inštrukcií je obsah R_6 nenulový; aby nenarušil nový priebeh cyklu, je vynulovaný inštrukciou začínajúcou q_{34}; môžeme predpokladať, že obsah R_6 je menší než číslo simulovaného stroja.

Poznámka 12.2. Inštrukcie začínajúce q_{33} a q_{34} v stroji U_{34} sú vlastne zbytočné. Mohli by sme ich vynechať (a nahradiť q_{33} symbolom q_{16} v inštrukcii začínajúcej q_{14}), a dostali by sme univerzálny registrový stroj s 32 inštrukciami. Ale dôkaz by vyžadoval veľmi špeciálnu voľbu simulovaných strojov a oveľa silnejšie vety o rozdelení prvočísel.

Teraz pristúpime k vybraným technickým detailom. Okrem nich by bolo treba ešte podrobne overiť ďalšie pomerne triviálne, ale tiež dôležité tvrdenia o činnosti stroja U_{34}; nie je problém so žiadnym z nich, ale je ich veľa. Preto by často pomohla i počítačová simulácia, aj keď sama samozrejme nestačí.

Najprv dokážeme potrebnú kódovaciu vlastnosť funkcie F. Nech $\mathrm{nond}(x,i)$ označuje i-ty kladný nedeliteľ čísla x. Pripomíname, že potom pre kladné x, i platí

$$F(x,i) = (x+1) \text{ MOD } \mathrm{nond}(x+1,i)$$

(Teraz nie je dôležité, ako nadefinujeme hodnoty pre $x = 0$ alebo $i = 0$).

Definícia 12.3. *F-číslom* konečnej postupnosti $(a_1, a_2, \ldots, a_k)$ kladných celých čísel nazveme každé $x \in \mathbb{N}$ také, že

$$F(x,i) = a_i \quad \text{pre všetky } i = 1, 2, \ldots, k. \tag{12.3.1}$$

Veta 12.4. Každá konečná postupnosť kladných celých čísel má aspoň jedno F-číslo.

Dôkaz: Využijeme známy fakt z teórie čísel, že počet prvočísel medzi n a $2n$ rastie do nekonečna s rastúcim n. Možno ho ľahko odvodiť z asymptotického vzorca $\pi(x) \approx \frac{x}{\ln(x)}$.

Nech $a_1, a_2, \ldots, a_k$ sú kladné celé čísla. Zvoľme k prvočísel $p_1 < p_2 < \cdots < p_k$ takých, že $p_k < 2p_1$ a $p_i > a_i$ pre všetky $i = 1, \ldots, k$. Číslo x môžeme nájsť ako riešenie nasledujúcej sústavy kongruencií

$$\begin{aligned} &x + 1 \equiv a_i \pmod{p_i} && \text{pre } i = 1, \ldots, k \\ &x + 1 \equiv 0 \pmod{p^e}, \text{ kde } e = \lfloor \ln p_k / \ln p \rfloor && \text{pre všetky ostatné prvočísla } p < p_k \end{aligned}$$

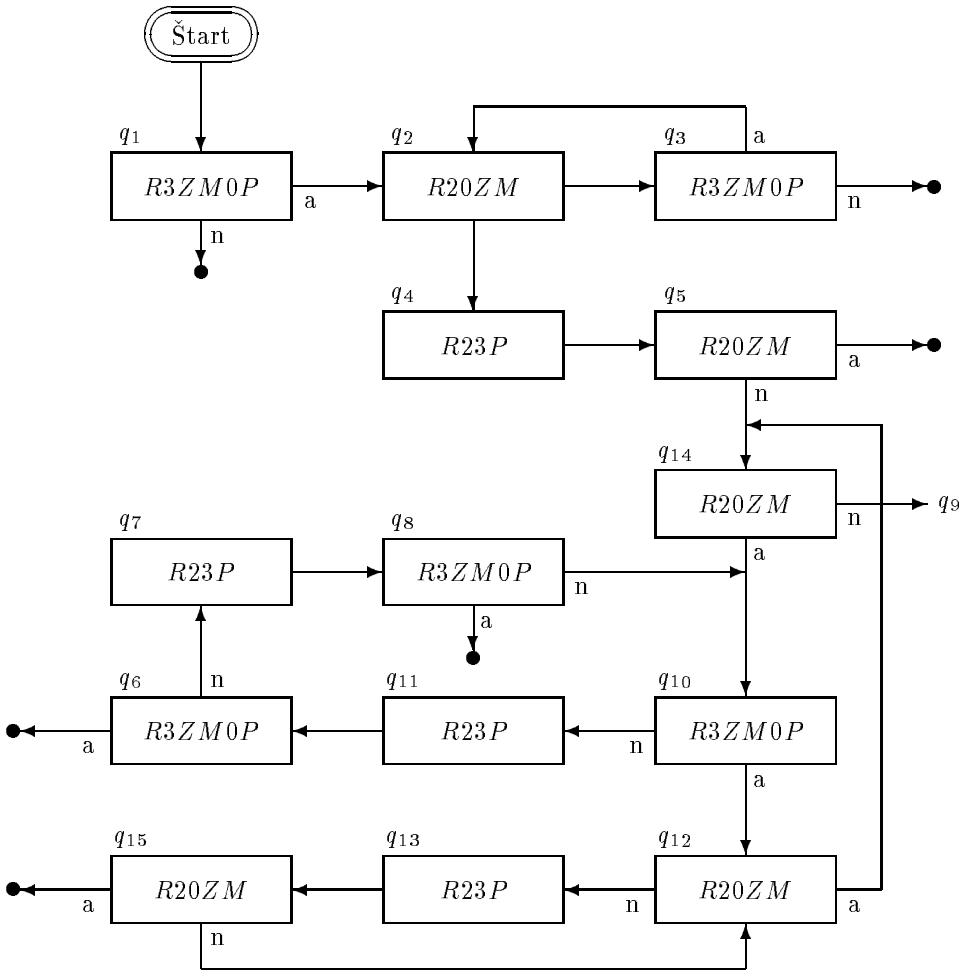
Moduly tejto sústavy kongruencií sú po dvoch nesúdeliteľné, a preto podľa čínskej zvyškovej vety je táto sústava riešiteľná. Vezmime nejaké jej kladné riešenie x.

Podľa druhej časti sústavy (a nerovnosti $p_1 < p_2 < \cdots < p_k$) jediné kladné nedelitele čísla $x+1$ menšie alebo rovné p_k sú $p_1, \ldots, p_k$. Podľa prvej časti sústavy sú to naozaj nedelitele $x+1$, a preto platí $\mathrm{nond}(x+1,i) = p_i$ pre všetky $1 \leq i \leq k$; potom zrejme $F(x,i) = (x+1) \text{ MOD } p_i = a_i$. □

Upozorňujeme, že F-číslo konečnej postupnosti nie je určené jednoznačne. (Situácia je podobná ako pri Gödelovskom kódovaní: číslo nejakej postupnosti je aj číslom každého jej začiatočného úseku.)

Cvičenie 12.5. Nájdite aspoň dve F-čísla pre každú z konečných postupností

- $(2, 4, 6)$
- $(6, 4, 2)$
- $(2, 3, 4, 5, 6, 7)$



Obr. 12.2. Blok pre prvú etapu.

Teraz nadefinujeme tzv. *R3a*-stroje. V ich označení *R3* pripomína, že pracujú s troma registrami. Písmeno *a* zasa pripomína, že sa používajú špeciálne inštrukcie a nejde teda len o obmedzenie počtu registrov v pôvodnej definícii registrových strojov.

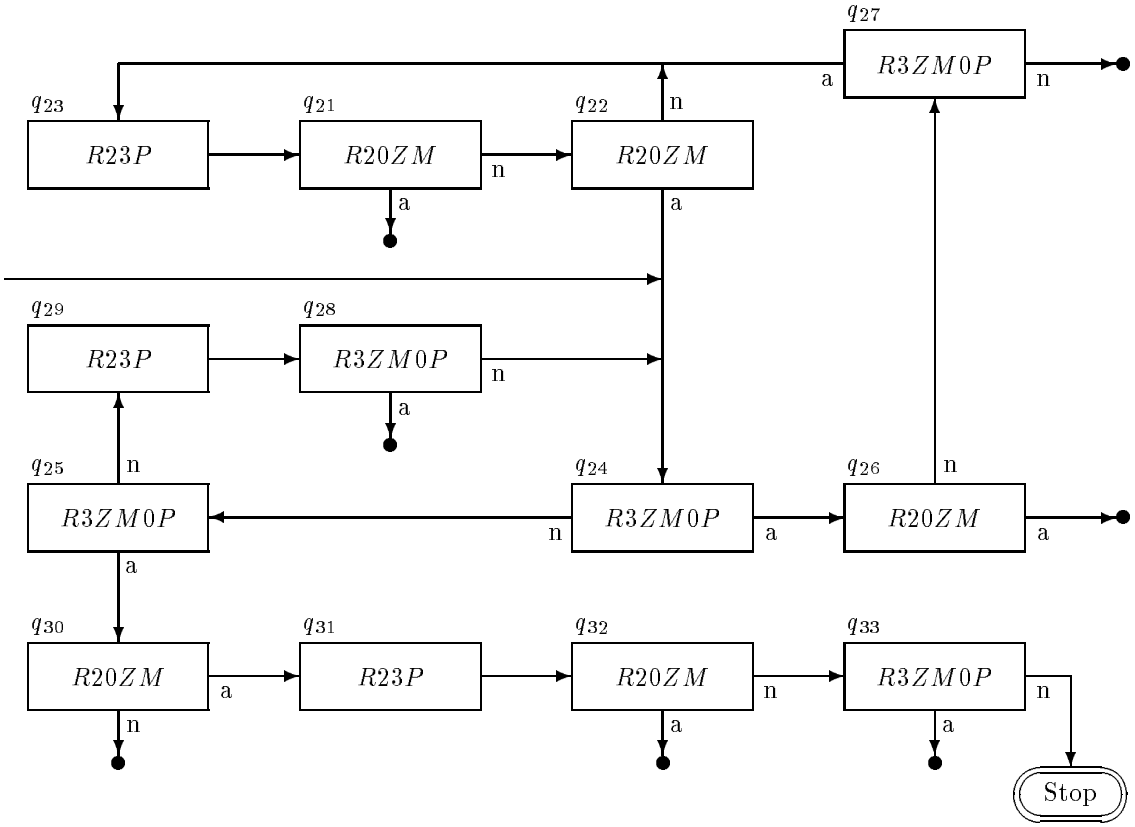
Definícia 12.6. *R3a-stroj* je konečná množina X usporiadaných trojíc alebo štvoríc (nazývaných ďalej inštrukciami) tvaru

$$(q_j, \mathsf{R20ZM}, q_k, q_{k+1}), \qquad (q_j, \mathsf{R3ZM0P}, q_k, q_{k+1}), \qquad (q_j, \mathsf{R23P}, q_k),$$

$j, k \in \mathbb{N}$, ktorá neobsahuje dve rôzne štvorice s rovnakým prvým prvkom a ktorá spĺňa nasledujúce podmienky:

(1) q_0 nie je na prvom mieste žiadnej inštrukcie;
(2) ak q_j, $j \neq 0$ je na treťom alebo štvrtom mieste nejakej inštrukcie z X, tak je aj na prvom mieste nejakej inštrukcie z X;
(3) žiadna inštrukcia nie je tvaru $(q_j, \mathsf{R20ZM}, q_0, q_1)$.

Samozrejme by sme teraz mali pre tieto stroje nadefinovať výpočty, nimi počítané funkcie atď. Namiesto toho len povieme, že majú zodpovedať špeciálnym registrovým strojom spomínaným vyššie. Tomu mnemotechnicky zodpovedajú i symboly na druhých miestach inštrukcií (budeme ich používať takmer výhradne v blokových schémach). Posledná podmienka je potrebná preto, lebo pri už spomenutom očíslovaní strojov pomocou funkcie F by jej mal zodpovedať nulový zvyšok.

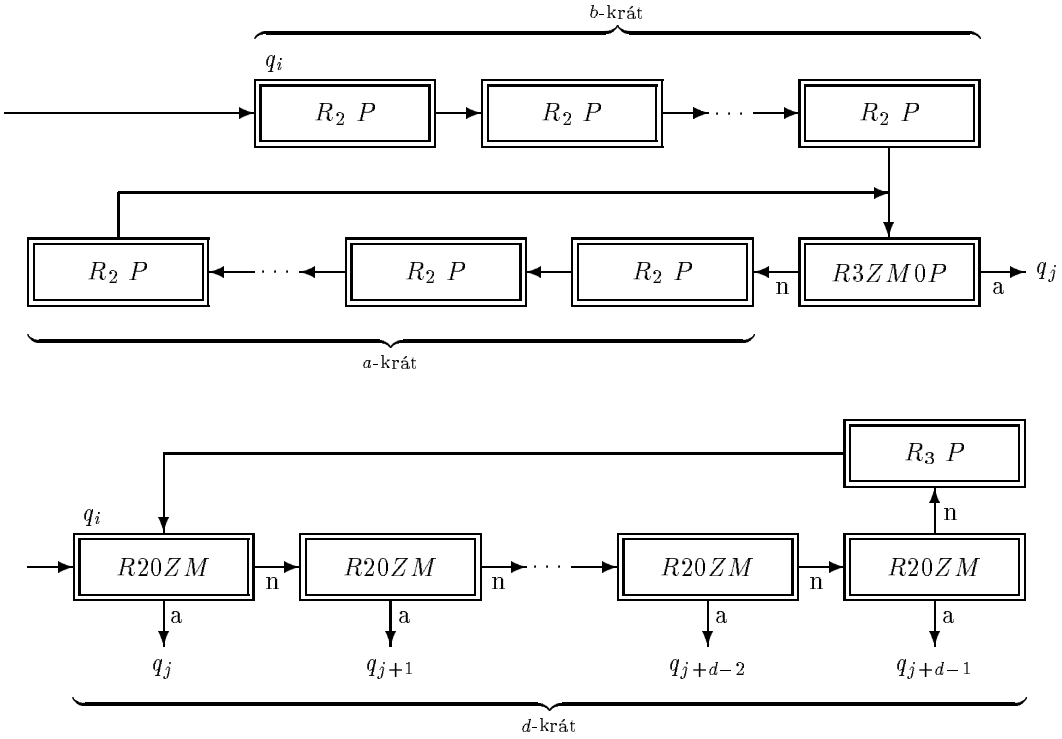


Obr. 12.4. Blok pre dekódovanie.

0: $(q_{24}; 0, 99, 0, 4)$
1: $(q_{25}; 0, 99, 0, 3)$
2: $(q_{29}; 0, 99, 0, 2)$
3: $(q_{28}; 0, 99, 1, 3)$
4: $(q_{24}; 0, 99, 1, 2)$
5: $(q_{25}; 0, 99, 1, 1)$
6: $(q_{29}; 0, 99, 1, 0)$
7: $(q_{28}; 0, 99, 2, 1)$
8: $(q_{24}; 0, 99, 2, 0)$
9: $(q_{26}; 1, 99, 2, 0)$
10: $(q_{27}; 1, 99, 1, 0)$
11: $(q_{23}; 2, 99, 1, 0)$
12: $(q_{21}; 2, 99, 2, 1)$
13: $(q_{22}; 2, 99, 1, 1)$
14: $(q_{23}; 2, 99, 0, 1)$
15: $(q_{21}; 2, 99, 1, 2)$
16: $(q_{22}; 2, 99, 0, 2)$
17: $(q_{24}; 1, 99, 0, 2)$
18: $(q_{25}; 1, 99, 0, 1)$
19: $(q_{29}; 1, 99, 0, 0)$
20: $(q_{28}; 1, 99, 1, 1)$
21: $(q_{24}; 1, 99, 1, 0)$
22: $(q_{26}; 2, 99, 1, 0)$
23: $(q_{27}; 2, 99, 0, 0)$
24: $(q_{23}; 3, 99, 0, 0)$
25: $(q_{21}; 3, 99, 1, 1)$
26: $(q_{22}; 3, 99, 0, 1)$
27: $(q_{24}; 2, 99, 0, 1)$
28: $(q_{25}; 2, 99, 0, 0)$
29: $(q_{30}; 3, 99, 0, 0)$
30: $(q_{31}; 2, 99, 0, 0)$
31: $(q_{32}; 2, 99, 1, 1)$
32: $(q_{33}; 2, 99, 0, 1)$
33: $(q_0;\ 2, 99, 0, 0)$

Obr. 12.5. Ukážka výpočtu bloku pre dekódovanie.

nám umožňuje meniť vnútorný stav. Jej použitie vidno v poslednom príklade; rozdiel oproti pôvodnej inštrukcii v definícii 12.6 je v tom, že nemusí platiť $n = m + 1$. (Ľahko zistíme, že táto makroinštrukcia zodpovedá siedmim $R3a$-inštrukciám a až 22 inštrukciám špeciálnych registrových strojov spomínaných v popise činnosti U_{34}. Nemáme však žiaden silný dôvod snažiť sa tento počet znížiť.) Preto odteraz možno blokové schémy (pre druhú etapu) kresliť bez špeciálneho sledovania vnútorných stavov. □



Obr. 12.7. Makroinštrukcie $R3a$-strojov (pokračovanie).

Register