Лекция 13: Алгоритмично неразрешими проблеми

4.2.5 Ефективно изброяване (номериране) на полуразрешимите множества

Да напомним две означения, които въведохме по-рано: при фиксирани $n \geq 1$ и $a \in \mathbb{N}$, с $W_a^{(n)}$ ще означаваме дефиниционната област на функцията $\varphi_a^{(n)}$, а с $E_a^{(n)}$ — множеството от нейните стойности:

$$W_a^{(n)} = Dom(\varphi_a^{(n)}) \stackrel{\text{деф}}{=} \{ \bar{x} \mid !\varphi_a^{(n)}(\bar{x}) \}$$

$$E_a^{(n)} = Range(\varphi_a^{(n)}) \stackrel{\text{деф}}{=} \{ y \mid \exists \bar{x} \in \mathbb{N}^n \colon \varphi_a^{(n)}(\bar{x}) \simeq y \}.$$

От първото НДУ за полуразрешимост (*Твърдение* 4.8) знаем, че едно множество $A \subseteq \mathbb{N}^n$ е полуразрешимо тогава и само тогава, когато съществува изчислима функция f, такава че $A = Dom(f)$. Оттук:

$$A \subseteq \mathbb{N}^n \text{ е полуразрешимо} \iff \exists a\ A = Dom(\varphi_a^{(n)}) \iff \exists a\ A = W_a^{(n)}.$$

Тогава е ясно, че редицата

$$W_0^{(n)},\ W_1^{(n)},\ \dots\ , W_a^{(n)},\ \dots$$

се състои от всички полуразрешими подмножества на $\mathbb{N}^n$. Ще я наричаме *ефективно изброяване* (номериране) на полуразрешимите множества.

Ако $A = W_a^{(n)}$, то числото a ще наричаме *индекс* (или номер) на A. Понеже всяка изчислима функция има безброй много индекси, то и всяко полуразрешимо множество ще има безброй много индекси. (Всъщност дори изчислимите функции да имаха само по един индекс, полуразрешимите множества пак щяха да имат безброй много индекси, защото е ясно, че безброй много изчислими функции имат един и същи домейн).

При $n = 1$ ще пишем за по-кратко

$$W_a = Dom(\varphi_a) \quad \text{и} \quad E_a = Range(\varphi_a).$$

Множеството $K \stackrel{\text{деф}}{=} \{x \mid !\varphi_x(x)\}$ можем да препишем чрез W_a по следния начин:

$$K = \{ x \mid x \in W_x \}.$$

Тогава $\overline{K} = \{ x \mid x \notin W_x \}$ и сега вече и без теоремата на Пост се вижда защо $\overline{K}$ не може да е полуразрешимо — защото по дефиниция

$$x \in \overline{K} \iff x \notin W_x,$$

и значи $\overline{K}$ и W_x се различават в точката x. С други думи, $\overline{K} \neq W_x$ за всяко x, следователно $\overline{K}$ не е полуразрешимо.

От *Твърдение* 4.12 знаем, че обединението на две, а оттук и на краен брой полуразрешими множества, е полуразрешимо. Когато имаме безкраен брой такива множества, обединението им вече може и да не е такова. Най-простият контрапример е да вземем някакво "сложно" множество $D = \{x_0,\ x_1,\ \dots\}$ и да разгледаме едноелементните множества $A_n = \{x_n\}$ за $n = 0, 1, \dots$. Всяко такова A_n е крайно, и значи — полуразрешимо, докато обединението на тези множества, което е точно D, вече не е полуразрешимо.

Проблемът в горния пример е, че съвкупността от индексите на множествата A_n е много сложна. Когато, обаче, обединяваме множества, чийто индекси са от някое полуразрешимо множество, това обединение със сигурност ще е полуразрешимо. Да се убедим:

Задача 4.28. Нека $A \subseteq \mathbb{N}$ е полуразрешимо. Докажете, че е полуразрешимо и множеството

$$B \ = \ \bigcup_{a \in A} W_a.$$

Решение. По определение

$$\begin{aligned} x \in B \iff & \exists a\ (a \in A\ \&\ x \in W_a) \iff \exists a(a \in A\ \&\ !\Phi_1(a,x)) \\ \iff & \exists a\ (a \in A\ \&\ (a,x) \in Dom(\Phi_1)) \\ \iff & \exists a\ (a,x) \in (A \times \mathbb{N}) \cap Dom(\Phi_1). \end{aligned}$$

Тъй като множеството $(A \times \mathbb{N}) \cap Dom(\Phi_1)$ е полуразрешимо, то ще е полуразрешимо и множеството B, съгласно теоремата за проекцията. $\square$

Знаем, че всяко полуразрешимо $A \subseteq \mathbb{N}$ има индекс, т.е. можем да си го мислим във вида $A = W_b$ за някое b. Това ни дава възможност да обобщим горната задача по следния начин:

Задача 4.29. Докажете, че е полуразрешимо множеството

$$B^* \ = \ \{\ (b,x) \mid x \in \bigcup_{a \in W_b} W_a\ \}.$$

Решение. По определение

$$\begin{aligned} (b,x) \in B^* \iff & \exists a(a \in W_b\ \&\ x \in W_a) \iff \exists a(!\varphi_b(a)\ \&\ !\varphi_a(x)) \\ \iff & \exists a\ !(\varphi_b(a) + \varphi_a(x)) \iff \exists a\ !(\ \underbrace{\Phi_1(b,a) + \Phi_1(a,x)}_{f(a,b,x)}\ ). \end{aligned}$$

Понеже f е изчислима, то множеството $C = Dom(f)$ ще е полуразрешимо. Оттук по теоремата за проекцията ще е полуразрешимо и B^*.

$\square$

Всички твърдения за полуразрешими множества, които доказахме в предишния раздел, имат и своите "равномерни" версии. Доказателствата им се основават на S^m_n-теоремата.

Да разгледаме, например, равномерната версия на твърдението, че обединение и сечение на полуразрешими множества е полуразрешимо (*Твърдение* 4.12). Тя ще изглежда така:

Задача 4.30. Докажете, че съществуват рекурсивни функции cut и uni, такива че за всяко a и b:

$$W_{cut(a,b)} \; = \; W_a \cap W_b \quad \text{и} \quad W_{uni(a,b)} \; = \; W_a \cup W_b.$$

Решение. Първо да решим задачата за сечението. Искаме да конструираме изчислима функция $f(a,b,x)$, която е такава, че след прилагане на S^m_n-теоремата към нея и намиране на функция $cut(a,b)$, такава че $\varphi_{cut(a,b)}(x) \simeq f(a,b,x)$, да се окаже, че $cut(a,b)$ търсената, т.е. за нея е изпълнено $W_{cut(a,b)} \; = \; W_a \cap W_b$.

За целта можем да вземем следната функция f:

$$f(a,b,x) \simeq \varphi_a(x) + \varphi_b(x).$$

Тя е изчислима, защото можем да я препишем чрез универсалната функция като $f(a,b,x) \simeq \Phi_1(a,x) + \Phi_1(b,x)$. Прилагаме към нея S^m_n-теоремата и получаваме, че за някоя (примитивно) рекурсивна функция $cut(a,b)$ ще е изпълнено $\varphi_{cut(a,b)}(x) \simeq f(a,b,x)$, или все едно:

$$\varphi_{cut(a,b)}(x) \simeq \varphi_a(x) + \varphi_b(x).$$

Оттук получаваме, че за произволни a, b и x:

$$x \in W_{cut(a,b)} \iff !\varphi_{cut(a,b)}(x) \iff !\varphi_a(x) \;\&\; !\varphi_b(x) \iff x \in W_a \cap W_b,$$

и следователно $W_{cut(a,b)} \; = \; W_a \cap W_b$.

При обединението на W_a и W_b нещата са по-сложни (знаем го още от "неравномерната" версия на това твърдение). Затова тръгваме отдалече — с полуразрешимото множество $U \; = \; Dom(\Phi_1)$. За него съществува рекурсивна функция ρ, такава че за всяко a и x:

$$(a,x) \in U \iff \exists t \; \rho(a,x,t) = 0.$$

Тогава

$$\begin{aligned} x \in W_a \cup W_b &\iff x \in W_a \;\vee\; x \in W_b \iff (a,x) \in U \;\vee\; (b,x) \in U \\ &\iff \exists t \; \rho(a,x,t) = 0 \;\vee\; \exists t \; \rho(b,x,t) = 0 \\ &\iff \exists t \; \rho(a,x,t).\rho(b,x,t) = 0 \iff \,! \underbrace{\mu t[\rho(a,x,t).\rho(b,x,t) = 0]}_{f(a,b,x)}. \end{aligned}$$

Към изчислимата функция $f(a,b,x) \simeq \mu t[\rho(a,x,t).\rho(b,x,t) = 0]$ прилагаме S^m_n-теоремата и получаваме, че съществува (отново примитивно) рекурсивна функция $uni(a,b)$, такава че

$$\varphi_{uni(a,b)}(x) \simeq f(a,b,x).$$

Тогава за всяко a, b и x ще е изпълнено:

$$x \in W_a \cup W_b \iff !f(a,b,x) \iff !\varphi_{uni(a,b)}(x) \iff x \in W_{uni(a,b)},$$

което означава, че функцията uni има исканото свойство. $\square$

Да докажем и равномерната версия на *Твърдение* 4.15, което казваше, че образът и първообразът на полуразрешимо множество чрез изчислима функция също е полуразрешимо множество.

Задача 4.31. Докажете, че съществуват рекурсивни функции im и $preim$, такива че за всяко a и b е изпълнено:

1) $W_{preim(a,b)} = \varphi_a^{-1}(W_b)$;

2) $W_{im(a,b)} = \varphi_a(W_b)$.

Решение. 1) За първообраза на W_b чрез φ_a имаме:

$$x \in \varphi_a^{-1}(W_b) \iff !\varphi_a(x) \,\&\, \varphi_a(x) \in W_b \iff !\varphi_b(\varphi_a(x)) \iff !\underbrace{\Phi_1(b, \Phi_1(a,x))}_{f(a,b,x)}$$

за всяко a, b и x. Функцията f е изчислима и по S^m_n-теоремата ще съществува примитивно рекурсивна функция $preim(a,b)$, такава че

$$\varphi_{preim(a,b)}(x) \simeq f(a,b,x).$$

Тогава за всяко a, b и x ще е изпълнено:

$$x \in \varphi_a^{-1}(W_b) \iff !f(a,b,x) \iff !\varphi_{preim(a,b)}(x) \iff x \in W_{preim(a,b)},$$

и значи функцията $preim$ е търсената.

2) За образа $\varphi_a(W_b)$ разсъждаваме така:

$$\begin{aligned} y \in \varphi_a(W_b) &\iff \exists x(x \in W_b \,\&\, \varphi_a(x) \simeq y) \\ &\iff \exists x(\mathcal{O}(\Phi_1(b,x)) \simeq 0 \,\&\, |(\Phi_1(a,x) - y| \simeq 0) \\ &\iff \exists x(\underbrace{\mathcal{O}(\Phi_1(b,x)) + |(\Phi_1(a,x) - y| \simeq 0}_{\{(a,b,y,x) \ \mid \ (a,b,x,y) \in A\}}). \end{aligned}$$

Функцията $\mathcal{O}(\Phi_1(b,x)) + |(\Phi_1(a,x) - y|$ е изчислима и следователно множеството A, което сме дефинирали по-горе, ще е полуразрешимо. Сега по теоремата за проекцията ще е полуразрешимо и множеството $A^* = \exists x A = \{(a,b,y) \mid \exists x(a,b,x,y) \in A\ \}$. Тогава ще е изчислима полухарактеристичната функция C_{A^*} на това множество и значи по S_n^m-теоремата ще съществува примитивно рекурсивна функция $im(a,b)$, такава че

$$\varphi_{im(a,b)}(y) \simeq C_{A^*}(a,b,y).$$

Така ще имаме, че за всяко a, b и y:

$$\begin{aligned} y \in \varphi_a(W_b) &\iff \exists x\ (a,b,y,x) \in A \iff (a,b,y) \in A^* \\ &\iff\ !C_{A^*}(a,b,y) \iff\ !\varphi_{im(a,b)}(y) \iff y \in W_{im(a,b)} \end{aligned}$$

и следователно $\varphi_a(W_b) = W_{im(a,b)}$. □

В *Задача* 4.25 показахме, че теоремата на Пост не може да се обобщи за безкраен брой непресичащи се полуразрешими подмножества на $\mathbb{N}^n$. При определени условия, обаче, че тя продължава да е вярна за безкраен брой множества $A_0, A_1, \ldots$. Това, което е необходимо, е редицата от тези множества да е *ефективна*. Какво означава това?

Нека $A_0, A_1, \ldots$ е редица от полуразрешими подмножества на $\mathbb{N}^k$. Казваме, че тази редица е *ефективна*, ако съществува рекурсивна функция h, такава че за всяко n:

$$A_n \ = \ W^{(k)}_{h(n)}.$$

Функцията h ще наричаме *индексна функция* за тази редица.

Задача 4.32. Нека $A_0, A_1, \ldots$ е ефективна редица от непресичащи се полуразрешими подмножества на $\mathbb{N}^k$, такива че $A_0 \cup A_1 \cup \cdots = \mathbb{N}^k$. Докажете, че всяко от тези множества е разрешимо.

Решение. За произволно n ще покажем, че допълнението $\overline{A_n}$ на множеството A_n е полуразрешимо. И тъй като и A_n е полуразрешимо, по теоремата на Пост ще следва, че A_n е разрешимо.

Нека h е индексната функция на дадената редица. Тогава за произволно $\bar{x} \in \mathbb{N}^k$ ще е изпълнено:

$$\begin{aligned} \bar{x} \in \overline{A_n} &\iff \exists m(m \neq n \ \&\ \bar{x} \in A_m) \iff \exists m(m \neq n \ \&\ \bar{x} \in W^{(k)}_{h(m)}) \\ &\iff \exists m(\chi_{\neq}(m,n) = 0 \ \&\ \mathcal{O}(\varphi^{(k)}_{h(m)}(\bar{x})) \simeq 0) \\ &\iff \exists m(\underbrace{\chi_{\neq}(m,n) + \mathcal{O}(\Phi_k(h(m),\bar{x}))}_{f(m,n,\bar{x})} \simeq 0). \end{aligned}$$

Функцията f е изчислима, следователно множеството $A = \{(m,n,\bar{x}) \mid f(m,n,\bar{x}) \simeq 0\}$ ще е полуразрешимо, откъдето по теоремата за проекцията и $\overline{A_n}$ ще е полуразрешимо. □

Задача 4.33. Докажете, че една редица $A_0, A_1, \ldots$ от полуразрешими подмножества на $\mathbb{N}^k$ е ефективна тогава и само тогава, когато множеството

$$U \;=\; \{(n, \bar{x}) \mid \bar{x} \in A_n\}$$

е полуразрешимо.

Забележка. Множеството U се явява *универсално множество* за множествата от редицата $\{A_n\}_n$.

Решение. В правата посока: нека h е рекурсивна функция, такава че за всяко n: $A_n = W^{(k)}_{h(n)}$. Тогава

$$(n, \bar{x}) \in U \stackrel{\text{деф}}{\Longleftrightarrow} \bar{x} \in A_n \iff \bar{x} \in W^{(k)}_{h(n)} \iff !\varphi^{(k)}_{h(n)}(\bar{x}) \iff !\Phi_k(h(n), \bar{x}).$$

Понеже функцията $\lambda n, \bar{x}.\Phi_k(h(n), \bar{x})$ е изчислима, то множеството U е полуразрешимо.

Обратно, ако горното множество U е полуразрешимо, то полухарактеристичната му функция $C_U(n, \bar{x})$ е изчислима. Прилагаме към нея S^m_n-теоремата и получаваме, че за някоя рекурсивна функция h ще е изпълнено:

$$\varphi^{(k)}_{h(n)}(\bar{x}) \simeq C_U(n, \bar{x}).$$

Тогава за всяко n и $\bar{x} \in \mathbb{N}^k$ ще имаме:

$$\bar{x} \in A_n \iff (n, \bar{x}) \in U \iff !C_U(n, \bar{x}) \iff !\varphi^{(k)}_{h(n)}(\bar{x}) \iff \bar{x} \in W^{(k)}_{h(n)},$$

и следователно редицата $A_0, A_1, \ldots$ е ефективна. $\square$

От *Задача* 4.17 знаем, че едно множество $A \subseteq \mathbb{N}$ е полуразрешимо тогава и само тогава, когато $A = Range(f)$ за някоя едноместна изчислима функция f, откъдето:

$$A \subseteq \mathbb{N} \text{ е полуразрешимо} \iff \exists a\ A = E_a.$$

С други думи, множеството $A \subseteq \mathbb{N}$ е полуразрешимо точно когато е от вида E_a за някое a. Така получаваме друг начин за индексиране на полуразрешимите множества от естествени числа. Да видим, че между двете системи за индексиране има равномерен преход:

Задача 4.34. Докажете, че съществуват примитивно рекурсивни функции α и β, такива че за всяко a:

а) $W_{\alpha(a)} = E_a$

б) $E_{\beta(a)} = W_a$.

Решение. а) Ще ни трябва изчислима функция $f(a,x)$, такава че $Dom(\lambda x.f(a,x))$ да е точно E_a. Да вземем например

$$f(a,x) \simeq \begin{cases} 0, & \text{ако } x \in E_a \\ \neg!, & \text{иначе.} \end{cases}$$

Всъщност f е полухарактеристична функция на множеството $A = \{(a,x) \mid x \in E_a\}$. Да се убедим, че A е полуразрешимо. Имаме

$$(a,x) \in A \iff \exists y\ \varphi_a(y) \simeq x \iff \exists y\, \underbrace{|\Phi_1(a,y) - x| \simeq 0}_{g(a,x,y)}.$$

Функцията g е изчислима, значи множеството $B = \{(a,x,y) | g(a,x,y) \simeq 0\}$ ще е е полуразрешимо, откъдето по теоремата за проекцията и A ще е полуразрешимо. Тогава $f = C_A$ е изчислима. По S^m_n-теоремата ще съществува примитивно рекурсивна функция α, такава че

$$\varphi_{\alpha(a)}(x) \simeq f(a,x),$$

откъдето получаваме, че за всяко a и x:

$$x \in W_{\alpha(a)} \iff !\varphi_{\alpha(a)}(x) \iff$$

$$x \in W_{\alpha(a)} \iff !f(a,x) \iff x \in E_a.$$

Следователно $W_{\alpha(a)} = E_a$ за всяко a.

б) Ще ни е нужна изчислима функция $f(a,x)$, която този път трябва да е такава, че $Range(\lambda x.f(a,x))$ да е W_a. Един начин да изберем f е следният:

$$f(a,x) \simeq \begin{cases} x, & \text{ако } x \in W_a \\ \neg!, & \text{иначе.} \end{cases}$$

Условието $x \in W_a$ от нейната дефиниция е еквивалентно на $(a,x) \in Dom(\Phi_1)$, което е полуразрешимо, и значи съгласно *Следствие* 4.5, функцията f е изчислима. Сега отново от S^m_n-теоремата ще имаме, че за някоя примитивно рекурсивна функция β ще е изпълнено:

$$\varphi_{\beta(a)}(x) \simeq g(a,x).$$

Оттук за всяко a и y ще имаме

$$\begin{aligned} y \in E_{\beta(a)} &\iff \exists x\ \varphi_{\beta(a)}(x) \simeq y \iff \exists x\ g(a,x) \simeq y \\ &\iff \exists x\ (y = x\ \&\ x \in W_a) \iff y \in W_a, \end{aligned}$$

и значи $E_{\beta(a)} = W_a$ за всяко a. □

Задача 4.35. (Задача за ЕК) Нека $A \subseteq \mathbb{N}$ и $R \subseteq \mathbb{N}^2$ са полуразрешими множества. С индукция по n дефинираме следната редица от подмножества на $\mathbb{N}$:

$$A_0 = A, \quad A_{n+1} = \{\ x \mid \exists y((x, y) \in R \ \&\ y \in A_n\ \}.$$

Докажете, че:

а) всяко от множествата A_n е полуразрешимо;

б) редицата $A_0,\ A_1,\ \ldots$ е ефективна.

4.3 Алгоритмично неразрешими проблеми

4.3.1 m-сводимост

За да можем да сравняваме алгоритмичната сложност на *масови проблеми*, които ще представяме с множества от естествени числа, въвеждаме следната релация между две числови множества A и B:

Определение 4.5. Нека $A \subseteq \mathbb{N}$ и $B \subseteq \mathbb{N}$. Ще казваме, че A е *m-сводимо* към B (и ще пишем $A \leqslant_m B$), ако съществува рекурсивна функция f, такава че за всяко $x \in \mathbb{N}$ е в сила еквивалентността:

$$x \in A \iff f(x) \in B.$$

Забележка. Терминът е m-сводимост, защото функцията f в общия случай е "**m**any-to-one" (т.е. неинективна), откъдето идва и името на сводимостта. Когато f е "one-to-one" (инективна), говорим за 1-сводимост, която се означава с $\leqslant_1$. Тъй като за нашите цели ще ни е нужна само m-сводимостта, ще я наричаме просто *сводимост* и съответно ще пишем $A \leqslant B$ вместо $A \leqslant_m B$.

Когато искаме да означим, че f е тази функция, която свежда A към B, ще пишем

$$A \underset{f}{\leqslant} B.$$

Ясно е, че ако $A \underset{f}{\leqslant} B$, то и $\bar{A} \underset{f}{\leqslant} \bar{B}$. Да споменем също, че ако $A \underset{f}{\leqslant} B$, то всъщност $A = f^{-1}(B)$, т.е. A е първообразът на B чрез f.

Ако $A \underset{f}{\leqslant} B$, то очевидно

$$\chi_A = \chi_B \circ f \quad \text{и} \quad C_A = C_B \circ f.$$

Оттук следва, че ако B е разрешимо (полуразрешимо), то и A ще е разрешимо (полуразрешимо). С други думи, ако имаме разрешаваща (полуразрешаваща) процедура за B, то ще имаме подобна процедура и за A. В този смисъл, ако $A \leqslant B$, то множеството A е алгоритмично *по-просто* от множеството B, което обяснява и означението $\leqslant$.

Една от типичните задачи в този раздел ще бъде да показваме, че дадено множество *не* е разрешимо или полуразрешимо. За тази цел ще използваме горното наблюдението, взето в контрапозиция. Понеже ще го цитираме често, да го формулираме като отделно твърдение:

Твърдение 4.18. Нека $A \leqslant B$. Тогава ако A не е разрешимо (полуразрешимо), то и B не е разрешимо (полуразрешимо).

От *Твърдение* 4.7 и *Задача* 4.23 знаем, че множеството $K = \{\, x \mid !\varphi_x(x) \,\}$ не е разрешимо, а допълнението му $\overline{K}$ не е полуразрешимо. K и $\overline{K}$ ще бъдат еталонни множества за нас. Ако за някое множество A успеем да покажем, че $K \leqslant A$, това ще означава, че A не е разрешимо, а ако стигнем до неравенството $\overline{K} \leqslant A$, то A няма да е полуразрешимо.

Твърдение 4.19. Релацията $\leqslant$ е рефлексивна и транзитивна.

Доказателство. Рефлексивност: ясно е, че A се свежда към себе си чрез функцията $\lambda x.x$.

Транзитивност: нека $A \underset{f}{\leqslant} B$ и $B \underset{g}{\leqslant} C$. Тогава за всяко $x \in \mathbb{N}$:

$$x \in A \iff f(x) \in B \iff g(f(x)) \in C.$$

Така получаваме, че A се свежда към C чрез функцията $g \circ f$. □

Да отбележим, че релацията $\leqslant$ не е антисиметрична. По-надолу ще имаме много примери на *различни* множества A и B, такива че $A \leqslant B$ и $B \leqslant A$. Ако искате да имате контрапример още сега, вземете например множествата $\mathbb{N}$ и $\mathbb{N}^+$. За всяко x ще са в сила еквивалентностите

$$x \in \mathbb{N} \iff \mathcal{S}(x) \in \mathbb{N}^+ \quad \text{и} \quad x \in \mathbb{N}^+ \iff x \dot{-} 1 \in \mathbb{N},$$

които ни дават $\mathbb{N} \leqslant \mathbb{N}^+$ и $\mathbb{N}^+ \leqslant \mathbb{N}$. В същото време $\mathbb{N} \neq \mathbb{N}^+$.

Определението за сводимост се обобщава по един съвсем естествен начин и за подмножества на *произволни* декартови степени на $\mathbb{N}$:

Определение 4.6. Нека $A \subseteq \mathbb{N}^n$ и $B \subseteq \mathbb{N}^k$. Ще казваме, че A е *сводимо* към B (и отново ще пишем $A \leqslant B$), ако съществуват рекурсивни функции $f_1, \dots, f_k$, такива че за всяко $\bar{x} \in \mathbb{N}^n$ е изпълнено:

$$\bar{x} \in A \iff (f_1(\bar{x}), \dots, f_k(\bar{x})) \in B.$$

От тази еквивалентност веднага получаваме, че за всяко $\bar{x}$:

$$\chi_A(\bar{x}) = \chi_B(f_1(\bar{x}), \dots, f_k(\bar{x})) \quad \text{и} \quad C_A(\bar{x}) \simeq C_B(f_1(\bar{x}), \dots, f_k(\bar{x})),$$

откъдето

$$\chi_A = \chi_B(f_1, \dots, f_k) \quad \text{и} \quad C_A = C_B(f_1, \dots, f_k).$$

Следователно *Твърдение* 4.18 остава вярно и за случая на произволни множества A и B. *Твърдение* 4.19 също продължава да е вярно (убедете се сами).

Да напомним дефиницията и на множеството U, което въведохме по-рано:

$$U \;=\; \{(a,x) \mid x \in W_a\} \;=\; \{(a,x) \mid !\Phi_1(a,x)\}.$$

Множеството U е дефиниционна област на най-сложната изчислима функция — универсалната функция Φ_1, поради което очакваме да е най-сложното полуразрешимо множество. Да се убедим:

Твърдение 4.20. Всяко полуразрешимо множество $A \subseteq \mathbb{N}$ е сводимо към U.

Решение. Щом $A \subseteq \mathbb{N}$ е полуразрешимо, то $A = W_a$ за някое a. Но тогава за всяко $x \in \mathbb{N}$ ще имаме, че

$$x \in W_a \iff (\underbrace{a}_{f_1(x)}, \underbrace{x}_{f_2(x)}) \in U.$$

Следователно A е сводимо към U чрез функциите $f_1 = \lambda x.a$ и $f_2 = \lambda x.x$, които очевидно са рекурсивни. □

Множеството U се явява *универсално* множество за всички полуразрешими подмножества на $\mathbb{N}$.

От горното твърдение следва, в частност, че и $K \leqslant U$, защото $K \subseteq \mathbb{N}$ е полуразрешимо. Оказва се, че е вярно и обратното неравенство $U \leqslant K$. Ще го получим като следствие от твърдението по-долу, според което и K е най-сложното сред полуразрешимите подмножества на $\mathbb{N}$.

Твърдение 4.21. Всяко полуразрешимо $A \subseteq \mathbb{N}$ се свежда към K.

Доказателство. Да дефинираме функцията f като

$$f(a,x) \simeq \begin{cases} 0, & \text{ако } a \in A \\ \neg!, & \text{иначе.} \end{cases}$$

Тя е изчислима, защото A е полуразрешимо ($f(a,x) \simeq C_A(a)$). Тогава по S^m_n-теоремата ще съществува рекурсивна функция h, такава че за всяко a и x: $\varphi_{h(a)}(x) \simeq f(a,x)$, с други думи, за всяко $a, x \in \mathbb{N}$:

$$\varphi_{h(a)}(x) \simeq \begin{cases} 0, & \text{ако } a \in A \\ \neg!, & \text{иначе.} \end{cases}$$

$\varphi_{h(a)}$ можем да препишем и така:

$$\varphi_{h(a)} = \begin{cases} \mathcal{O}, & \text{ако } a \in A \\ \emptyset^{(1)}, & \text{иначе.} \end{cases}$$

Твърдим, че A се свежда към K чрез функцията h. Наистина, за всяко $a \in \mathbb{N}$ имаме:

$$a \in A \iff \varphi_{h(a)} = \mathcal{O} \iff !\varphi_{h(a)}(h(a)) \stackrel{\text{деф}}{\iff} h(a) \in K.$$

$\square$

От релацията $\leqslant$ стандартно въвеждаме *еквивалентност* на две множества A и B:

$$A \equiv B \stackrel{\text{деф}}{\iff} A \leqslant B \ \& \ B \leqslant A.$$

Ясно е, че тази релация е релация на еквивалентност (тя очевидно е симетрична, а от *Твърдение* 4.19 се вижда, че е и рефлексивна и транзитивна).

Задача 4.36. (Задача за ЕК) Разглеждаме релацията $\equiv$ върху множеството $\mathcal{R}$ на всички разрешими подмножества на $\mathbb{N}$. Опишете получените класове на еквивалентност.

По-горе лесно съобразихме, че $\mathbb{N} \equiv \mathbb{N}^+$. Ето и първият ни не толкова очевиден пример за двойка еквивалентни множества — множеството K и универсалното множество U.

Задача 4.37. Докажете, че $U \equiv K$.

Решение. Като следствие от *Твърдение* 4.20 получихме, че $K \leqslant U$. За да съобразим обратното, да разгледаме следното множество $\hat{U}$, което има същата сложност като U, но вече е подмножество на $\mathbb{N}$:

$$\hat{U} \stackrel{\text{деф}}{=} \{\ \Pi(a, x) \mid (a, x) \in U\ \}.$$

Ясно е, че U е полуразрешимо и следователно $\hat{U} \leqslant K$, съгласно *Твърдение* 4.21. Освен това имаме, че $U \leqslant \hat{U}$, което се вижда от еквивалентността:

$$(a, x) \in U \iff \Pi(a, x) \in \hat{U}.$$

Сега вече от $U \leqslant \hat{U}$ и $\hat{U} \leqslant K$ по транзитивност достигаме до неравенството $U \leqslant K$, което заедно с обратното $K \leqslant U$ ни дава $U \equiv K$. $\square$

4.3.2 Неразрешимост на стоп-проблема за МНР

За едно множество $A \subseteq \mathbb{N}^n$ ще казваме, че е *неразрешимо*, ако то не е разрешимо.

При фиксирано $n \geq 1$ да положим:

$$HP_n \stackrel{\text{деф}}{=} \{(a, x_1, \ldots, x_n) \mid P_a \text{ спира върху } (x_1, \ldots, x_n)\}.$$

Теорема 4.2. (Стоп-проблемът за МНР е неразрешим) Нека $n \geq 1$. Множеството $HP_n = \{ (a, x_1, \ldots, x_n) \mid P_a \text{ спира върху } (x_1, \ldots, x_n) \}$ не е разрешимо.

Доказателство. Най-напред ще се спрем на случая $n = 1$. В този случай HP_1 е всъщност множеството, което по-горе означихме с U, и за което видяхме (*Задача* 4.23), че $K \leqslant U$. И понеже K не е разрешимо, то и U не може да е разрешимо, съгласно *Твърдение* 4.18.

Нека сега $n \geq 1$ е произволно. Ще покажем, че $HP_1 \leqslant HP_n$, откъдето ще следва, че и общият стоп-проблем не е неразрешим.

Да разгледаме функцията

$$f(a, x_1, \ldots, x_n) \stackrel{\text{деф}}{\simeq} \varphi_a(x_1).$$

Тя е изчислима и следователно за някоя рекурсивна функция h, съгласно S^m_n-теоремата, ще е изпълнено

$$\varphi^{(n)}_{h(a)}(x_1, \ldots, x_n) \simeq f(a, x_1, \ldots, x_n), \text{ т.е. } \quad \varphi^{(n)}_{h(a)}(x_1, \ldots, x_n) \simeq \varphi_a(x_1)$$

за всяко $a \in \mathbb{N}, \bar{x} \in \mathbb{N}^n$. При $x_1 = \cdots = x_n = x$ ще имаме

$$\varphi^{(n)}_{h(a)}(\underbrace{x, \ldots, x}_{n \text{ пъти}}) \simeq \varphi_a(x),$$

откъдето в частност

$$!\varphi_a(x) \iff !\varphi^{(n)}_{h(a)}(\underbrace{x, \ldots, x}_{n \text{ пъти}}).$$

Преписана чрез HP_1 и HP_n, горната еквивалентност изглежда така:

$$(a, x) \in HP_1 \iff (h(a), \underbrace{x, \ldots, x}_{n \text{ пъти}}) \in HP_n.$$

Тя е в сила за всяко a и x, и значи $HP_1 \leqslant HP_n$. □

Да отбележим, че множеството HP_n все пак е полуразрешимо, защото

$$HP_n = \{(a, \bar{x}) \mid P_a \text{ спира върху } \bar{x}\} = \{(a, \bar{x}) \mid !\Phi_n(a, \bar{x})\}.$$

Това означава, че стоп-проблемът за МНР е полуразрешим.

Да означим с RHP_n (от *restricted halting problem*) следното множество:

$$RHP_n \stackrel{\text{деф}}{=} \{(a,\bar{x},t) \mid P_a \text{ спира върху } \bar{x} \text{ за } \leq\ t \text{ стъпки}\}.$$

Твърдение 4.22. (Ограниченият стоп-проблем за МНР е разрешим) За всяко $n \geq 1$ множеството RHP_n е разрешимо.

Доказателство. Най-напред да си припомним, че съгласно определението за код на програма, ако $P_a\colon I_0,\dots,I_k$, то номерът k на последния оператор на P_a е $lh(a)$.

Разполагаме и с примитивно рекурсивна функция $Q_n(a,\bar{x},t)$, която дава кода на конфигурацията на стъпка t от работата на P_a върху $\bar{x}$. Тогава очевидно

$$P_a \text{ спира върху } \bar{x} \text{ за } \leq\ t \text{ стъпки} \iff (Q_n(a,\bar{x},t))_0 > lh(a),$$

или все едно

$$(a,\bar{x},t) \in RHP_n \iff (Q_n(a,\bar{x},t))_0 > lh(a).$$

Следователно множеството RHP_n е разрешимо. □

4.3.3 Теорема на Райс-Успенски

Оттук нататък основната ни задача ще бъде да изследваме *семантичните* свойства на програмите от нашия изчислителен модел и да ги класифицираме в зависимост от тяхната сложност — разрешими, полуразрешими, неразрешими, неполуразрешими и пр. Ще разглеждаме само програми с една входна променлива, тъй като всички резултати, които са или не са в сила за тези програми, съответно ще са или няма да са в сила и за програмите с n входни променливи.

Ще ни интересуват т.нар. *масови* проблеми, т.е. задачи, отнасящи се до *безкрайни* съвкупности от обекти — функции, множества, програми. Разбира се, това, че даден проблем е алгоритмично неразрешим, съвсем не означава, че в някои *частни случаи* той не може да бъде разрешен. Алгоритмичната неразрешимост означава, че няма *общ метод*, който да работи за *всички* случаи.

Например, ако се интересуваме от проблема дали произволна програма P_a спира за всеки вход x, в някои конкретни случаи бихме могли да си отговаряме на този въпрос — например, ако в програмата няма цикли, е ясно, че тя ще завършва винаги. Това, което ни интересува, е дали съществува алгоритъм, който работи при *всеки* конкретен случай.

Да напомним, че с $\mathcal{C}_1$ означаваме съвкупността от всички едноместни изчислими функции, т.е.

$$\mathcal{C}_1 \;=\; \{\varphi_0,\ \varphi_1,\ \dots\}.$$

Да разглеждаме някакво *семантично* свойства на програмите за МНР с една входна променлива означава да разглеждаме свойство на *функциите*, които тези програми пресмятат, т.е. свойство на функциите от класа $\mathcal{C}_1$. Всяко такова свойство може да се зададе със съответно множество $\mathcal{A} \subseteq \mathcal{C}_1$ — това е множеството от всички функции, имащи това свойство. Следователно проблемът дали една функция от $\mathcal{C}_1$ има свойството P е еквивалентен на проблема дали тази функция принадлежи на множеството $\mathcal{A} = \{f \mid f$ има свойството $P\}$. Формално този проблем ще записваме така:

$$\text{"}\varphi_a \in \mathcal{A}?\text{"}$$

Например проблемът дали P_a завършва за всяко x е точно проблемът дали φ_a е тотална, или все едно — дали φ_a принадлежи на класа

$$\mathcal{A}_{tot} = \{f \mid f \text{ е тотална и изчислима}\}.$$

Следователно проблемът дали P_a завършва за всяко x може да се запише така: "$\varphi_a \in \mathcal{A}_{tot}$?".

Друг пример е *проблемът за коректността*, т.е. дали програмата P_a пресмята конкретна функция f_0. Имаме

$$P_a \text{ пресмята } f_0 \iff \varphi_a = f_0 \iff \varphi_a \in \mathcal{A}_0 \stackrel{\text{деф}}{=} \{f_0\}.$$

Значи проблемът за коректността може да се запише като проблема дали "$\varphi_a \in \mathcal{A}_0$?".

Нека $\mathcal{A} \subseteq \mathcal{C}_1$. *Индексното множество $I_{\mathcal{A}}$ на $\mathcal{A}$* дефинираме по следния начин:

$$I_{\mathcal{A}} \;=\; \{\ a \mid \varphi_a \in \mathcal{A}\ \}.$$

С други думи, в $I_{\mathcal{A}}$ влизат всевъзможните индекси на всяка функция от $\mathcal{A}$. Да отбележим, че $I_{\mathcal{A}}$ вече е множество от *числа*. Това ни дава възможност да говорим за *сложност* на проблема "$\varphi_a \in \mathcal{A}$?", като разглеждаме сложността на индексното му множество $I_{\mathcal{A}}$.

Определение 4.7. Ще казваме, че проблемът "$\varphi_a \in \mathcal{A}$?" *е разрешим (полуразрешим, неразрешим)*, ако индексното му множество $I_{\mathcal{A}}$ е разрешимо (полуразрешимо, неразрешимо).

Ще казваме, че един проблем от вида "$\varphi_a \in \mathcal{A}$?" е *нетривиален*, ако има поне една функция, която е в $\mathcal{A}$, и поне една извън $\mathcal{A}$, с други думи, ако $\emptyset \subsetneqq \mathcal{A} \subsetneqq \mathcal{C}_1$. Следващата теорема показва, че всеки нетривиален проблем "$\varphi_a \in \mathcal{A}$?" е неразрешим.

Теорема 4.3. (Теорема на Райс-Успенски) Нека $\emptyset \subsetneqq \mathcal{A} \subsetneqq \mathcal{C}_1$. Тогава проблемът "$\varphi_a \in \mathcal{A}$?" е неразрешим.

Доказателство. По-краткото (но и по-малко информативно) доказателство минава през втората теорема за рекурсия.

Да допуснем, че проблемът "$\varphi_a \in \mathcal{A}$?" е разрешим, т.е. множеството $I_{\mathcal{A}} = \{a \mid \varphi_a \in \mathcal{A}\}$ е разрешимо. Да фиксираме два индекса b и c, такива че $\varphi_b \in \mathcal{A}$ и $\varphi_c \notin \mathcal{A}$, и да разгледаме функцията

$$h(a) = \begin{cases} c, & \text{ако } \varphi_a \in \mathcal{A} \\ b, & \text{ако } \varphi_a \notin \mathcal{A}. \end{cases}$$

Условието $\varphi_a \in \mathcal{A}$ е еквивалентно на $a \in I_{\mathcal{A}}$, което е разрешимо по допускане, и значи h е рекурсивна функция. Тогава ще съществува индекс a, такъв че

$$\varphi_a \;=\; \varphi_{h(a)}. \tag{4.2}$$

Да разгледаме двете възможности за стойностите на $h(a)$:

1 сл.: $h(a) = b$, което означава, че $\varphi_a \notin \mathcal{A}$. Тогава от равенството (4.2) ще имаме $\varphi_a = \varphi_b$ и следователно $\varphi_a \in \mathcal{A}$ — противоречие.

2 сл.: $h(a) = c$, което съгласно дефиницията на h означава, че $\varphi_a \in \mathcal{A}$. Тогава отново от (4.2) ще имаме $\varphi_a = \varphi_c$, и понеже $\varphi_c \notin \mathcal{A}$, то и $\varphi_a \notin \mathcal{A}$ — пак противоречие, което показва, че допускането ни, че проблемът "$\varphi_a \in \mathcal{A}$?" е разрешим, е погрешно.

Друг начин да покажем, че проблемът "$\varphi_a \in \mathcal{A}$?" е неразрешим, е чрез *свеждане*. По-точно, ще покажем, че $K \leqslant I_{\mathcal{A}}$, откъдето не само ще следва, че множеството $I_{\mathcal{A}}$ е неразрешимо, но това неравенство ще ни казва още, че сложността на $I_{\mathcal{A}}$ е над тази на K. В частност, ако $I_{\mathcal{A}}$ е полуразрешимо, то ще е със сложността на K.

Без ограничение на общността можем да си мислим, че $\emptyset^{(1)} \notin \mathcal{A}$, защото ако не е така, можем да разгледаме проблема "$\varphi_a \in \overline{\mathcal{A}}$?" и за него да покажем, че не е разрешим. Тогава множеството $I_{\overline{\mathcal{A}}}$ няма да е разрешимо, откъдето и $I_{\mathcal{A}}$, като негово допълнение, също няма да е разрешимо.

Нека отново приемем, че b е индекс на функция от класа $\mathcal{A}$, т.е. $b \in I_{\mathcal{A}}$. Да дефинираме функцията f по следния начин:

$$f(a,x) \simeq \begin{cases} \varphi_b(x), & \text{ако } a \in K \\ \neg!, & \text{иначе.} \end{cases}$$

Тази функция очевидно е изчислима, и значи към нея можем да приложим S^m_n-теоремата. Така ще получим, че има рекурсивна функция h, такава че за всяко a и x, $\varphi_{h(a)}(x) \simeq f(a, x)$. Оттук веднага

$$\varphi_{h(a)} = \begin{cases} \varphi_b, & \text{ако } a \in K \\ \emptyset^{(1)}, & \text{иначе.} \end{cases}$$

Като имаме предвид, че $\varphi_b \neq \emptyset^{(1)}$, лесно съобразяваме, че

$$a \in K \iff \varphi_{h(a)} \in \mathcal{A} \iff h(a) \in I_{\mathcal{A}},$$

което означава, че $K \underset{h}{\leqslant} I_{\mathcal{A}}$. И тъй като K не е разрешимо, по *Твърдение* 4.18 и $I_{\mathcal{A}}$ няма да е разрешимо. □

Да отбележим, че двата случая, които се изключват от теоремата на Райс-Успенски — $\mathcal{A} = \emptyset$ и $\mathcal{A} = \mathcal{C}_1$, са тривиално разрешими, защото индексните им множества са $\emptyset$ и $\mathbb{N}$.

Да предположим, че индексното множество $I_{\mathcal{A}}$ на даден проблем е полуразрешимо. От *Задача* 4.23 имаме, че тогава $I_{\mathcal{A}} \leqslant K$. В доказателството по-горе получихме и обратното свеждане $K \leqslant I_{\mathcal{A}}$. Това означава, че $I_{\mathcal{A}} \equiv K$, с други думи, ако се случи един проблем от вида "$\varphi_a \in \mathcal{A}$?" да е полуразрешим, то той е със сложността на K. Ясно е също, че индексните множества на всички такива полуразрешими проблеми ще бъдат еквивалентни помежду си, защото всички те са еквивалентни на K.

От доказателството на теоремата на Райс-Успенски (по втория начин) се вижда още едно полезно следствие:

Следствие 4.6. Нека класът от функции $\mathcal{A} \subsetneqq \mathcal{C}_1$ е такъв, че $\emptyset^{(1)} \in \mathcal{A}$. Тогава проблемът "$\varphi_a \in \mathcal{A}$?" не е полуразрешим.

Доказателство. Разглеждаме допълнителния проблем "$\varphi_a \in \overline{\mathcal{A}}$?". Той очевидно е непразен (защото $\emptyset^{(1)} \in \mathcal{A}$), а също и $\overline{\mathcal{A}} \neq \mathcal{C}_1$ (защото $\mathcal{A} \subsetneqq \mathcal{C}_1$). За него имаме още, че $\emptyset^{(1)} \notin \overline{\mathcal{A}}$ и следователно $K \leqslant I_{\overline{\mathcal{A}}}$. Тогава $\overline{K} \leqslant I_{\mathcal{A}}$ (тъй като $I_{\mathcal{A}} = \mathbb{N} \setminus I_{\overline{\mathcal{A}}}$). И понеже $\overline{K}$ не е полуразрешимо, то и $I_{\mathcal{A}}$ няма да е полуразрешимо. □

Като директно приложение на теоремата на Райс-Успенски да си дадем сметка, че са неразрешими следните проблеми:

Задача 4.38. Докажете, че следните проблеми са неразрешими:

1) *Проблемът за тоталността*: дали програмата P_a завършва за всяко x, т.е. проблемът "φ_a е тотална?"

2) *Проблемът за ограничената тоталност*: дали P_a завършва за всяко $x \leq c$, където c е фиксирано, или формално "$\forall x_{x \leq c}\ !\varphi_a(x)$?"

3) Проблемът дали програмата P_a спира при безкрайно много входове, те дали "$Dom(\varphi_a)$ е безкрайно?"

4) Проблемът за коректността, т.е. дали програмата P_a пресмята фиксирана функция f_0, или все едно "$\varphi_a = f_0$?"

5) Проблемът дали P_a пресмята примитивно рекурсивна функция, или все едно "$\varphi_a \in \mathcal{PR}_1$?", където $\mathcal{PR}_1$ е класът на всички едноместни примитивно рекурсивни функции.

Решение. Единственото, което трябва да съобразим е, че всички тези проблеми са нетривиални, което е очевадно $\ddot\smile$. Тогава по теоремата на Райс-Успенски те автоматично ще бъдат неразрешими. □

Задача 4.39. Докажете, че следните проблеми не са полуразрешими:

1) "φ_a е крайна функция?"

2) "φ_a не е тотална?"

3) "$\varphi_a = \emptyset^{(1)}$?"

4) $c \in \mathbb{N}$, "$\exists x_{x \le c}\ \neg!\varphi_a(x)$?".

Решение. Лесно се съобразява, че всеки от тези проблеми е в сила за никъде недефинираната функция $\emptyset^{(1)}$. Освен това никой от тях не е валиден *за всяка* функция. Тогава съгласно *Следствие* 4.6 никой от тях не е полуразрешим. □

Да припомним, че програмите P_a и P_b са еквивалентни ($P_a \approx P_b$), ако пресмятат една и съща функция, т.е. ако $\varphi_a = \varphi_b$. Индексното множество на проблема "$\varphi_a = \varphi_b$?" е множеството $E = \{(a,b) \mid \varphi_a = \varphi_b\}$.

Твърдение 4.23. (Проблемът за еквивалентността на МНР програмите не е полуразрешим) Множеството

$$E = \{(a,b) \mid \varphi_a = \varphi_b\}$$

не е полуразрешимо.

Доказателство. Да допуснем, че E е полуразрешимо. Твърдим, че тогава ще бъде полуразрешимо и множеството

$$E_0 = \{a \mid \varphi_a = \emptyset^{(1)}\}.$$

Това звучи правдоподобно, защото проблемът "$\varphi_a = \emptyset^{(1)}$?" е частен случай на проблема "$\varphi_a = \varphi_b$?", но да го съобразим все пак: наистина, $C_{E_0}(a) \simeq C_E(a, b_0)$, където b_0 е фиксиран индекс на $\emptyset^{(1)}$, следователно C_{E_0} също е изчислима, и значи E_0 е полуразрешимо. Но E_0 е индексното множество на проблема "$\varphi_a = \emptyset^{(1)}$?", който не е полуразрешим, съгласно *Задача* 4.39 — противоречие. Следователно E не е полуразрешимо. $\square$

Сега ще дефинираме две понятия за коректност на програма. За тях ще покажем, че проблемът за коректността не е дори полуразрешим.

Нека P е произволна програма с една входна променлива, а $I(x)$ и $O(x, y)$ са съответно някакво *входно* и някакво *изходно условие* за P (или *спецификация* за P).

Казваме, че програмата P е *частично коректна* относно дадената спецификация $I \,/\, O$, ако е вярно, че за всеки вход x, такъв че входното условие $I(x)$ е в сила, *ако* програмата спре върху x с резултат y, то този резултат ще е коректен, т.е ще е изпълнено изходното условие $O(x, y)$.

Функцията f, която тази програма пресмята, очевидно ще удовлетворява свойството $P_{p.c.}(f)$, което се дефинира по следния начин:

$$P_{p.c.}(f) \iff \forall x(\ I(x)\ \&\ !f(x) \implies O(x, f(x))\ ).$$

Програмата P е *тотално коректна*, ако при всеки коректен вход тя *задължително* завършва и резултатът отново е коректен, разбира се. Тогава за функцията f, която тя пресмята, ще е изпълнено свойството $P_{t.c.}$, където

$$P_{t.c.}(f) \iff \forall x(\ I(x) \implies !f(x)\ \&\ O(x, f(x))\ ).$$

Задача 4.40. Докажете, че всеки нетривиален проблем за частична коректност на МНР програмите не е полуразрешим.

Решение. Да фиксираме някаква спецификация $I \,/\, O$ и нека

$$\mathcal{A}_{p.c.} \ = \ \{f \mid f \text{ е изчислима } \&\ P_{p.c.}(f)\}.$$

Тогава P_a е частично коректна относно $I \,/\, O$ точно когато $\varphi_a \in \mathcal{A}_{p.c.}$.

При смислена спецификация със сигурност проблемът "$\varphi_a \in \mathcal{A}_{p.c.}$?" ще е нетривиален. Пример за тривиален проблем е да кажем този с входно условие $I(x) \overset{\text{деф}}{\iff} x = x + 1$. Това условие е тъждествената *лъжа*, и следователно свойството свойствата $P_{p.c.}(f)$ и $P_{t.c.}(f)$ ще са в сила за всяка функция f, т.е. ще имаме $\mathcal{A}_{p.c.} = \mathcal{C}_1$ и $\mathcal{A}_{t.c.} = \mathcal{C}_1$.

Лесно се вижда, свойството $P_{p.c.}$ е в сила за $\emptyset^{(1)}$. Следователно ако $\mathcal{A}_{p.c.} \neq \mathcal{C}_1$, проблемът за частичната коректност няма да е полуразрешим, съгласно *Следствие* 4.6. $\square$

Проблемът за тоталната коректност също не е полуразрешим, но това ще следва от един по-общ критерий за неполуразрешимост, който предстои да докажем — теоремата на Райс-Шапиро.

Задача 4.40 показва, че не може да се съществува универсална програма-верификатор, която да проверява дали всяка МНР програма е коректна относно дадена спецификация.

4.3.4 Теорема на Райс-Шапиро

Вече се убедихме, че всеки нетривиален проблем от вида "$\varphi_a \in \mathcal{A}$?" е неразрешим. Сега да видим, че съществуват поне *полуразрешими* проблеми от този тип. Следващата задача ще ни подскаже, че тези проблеми трябва да отговарят на едно специфично условие.

Задача 4.41. Докажете, че проблемът "φ_a не е инективна?" е полуразрешим.

Решение. По определение една *частична* функция $f : \mathbb{N} \longrightarrow \mathbb{N}$ е инективна, ако е изпълнено условието:

$$\forall x \forall y (x \neq y \ \& \ !f(x) \ \& \ !f(y) \implies f(x) \neq f(y)).$$

Тогава

$$\begin{aligned} \varphi_a \text{ не е инективна } &\iff \exists x \exists y \exists z (x \neq y \ \& \ \varphi_a(x) \simeq z \ \& \ \varphi_a(y) \simeq z) \\ &\iff \exists x \exists y \exists z \underbrace{\chi_{\neq}(x,y) + |\Phi_1(a,x) - z| + |\Phi_1(a,y) - z|}_{f(a,x,y,z)} \simeq 0 \end{aligned}$$

f е изчислима, значи множеството $A = \{(a,x,y,z) \mid f(a,x,y,z) \simeq 0\}$ е полуразрешимо, а оттам по теоремата за проекцията (приложена трикратно) ще е полуразрешимо и множеството $I = \{a \mid \varphi_a \text{ не е инективна}\}$. Следователно проблемът "φ_a не е инективна?" е полуразрешим. □

Следващата теорема ни дава *необходимо* (но недостатъчно) условие един проблем от типа "$\varphi_a \in \mathcal{A}$?" да е полуразрешим. Затова няма как да я използваме, за да доказваме, че даден проблем е полуразрешим. Но това няма да бъде и нашата цел; ние ще я прилагаме с контрапозиция, за да показваме, че даден проблем *не* е полуразрешим.

Теорема 4.4. **(Теорема на Райс-Шапиро)** Нека проблемът "$\varphi_a \in \mathcal{A}$?" е полуразрешим. Тогава за всяка функция $f \in \mathcal{C}_1$ е в сила еквивалентността:

$$f \in \mathcal{A} \iff \exists \theta (\theta \text{ е крайна } \& \ \theta \subseteq f \ \& \ \theta \in \mathcal{A}). \tag{4.3}$$

Тази теорема остава без доказателство, защото не остана време за него :(.
Все пак го оставям в записките, за тези, които искат да се уверят във верността на теоремата. :)

Доказателство. Условието (4.3) ни казва, че за да е полуразрешим даден проблем "$\varphi_a \in \mathcal{A}$?", той трябва да се локализира до някоя крайна част θ от функцията $f \in \mathcal{A}$.

Да вземем за пример свойството "неинективност" от *Задача* 4.41. За да не е инективна една функция f, е достатъчно да има две различни точки x и y от дефиниционната ѝ област, за които $f(x) = f(y)$. Значи в качеството на $\theta \subseteq f$ можем да вземем функцията θ, която е дефинирана само в тези две точки.

Най-напред да се заемем с правата посока на еквивалентността (4.3). За целта да фиксираме изчислима функция $f \in \mathcal{A}$ и да допуснем, че условието в дясната страна на (4.3) не е изпълнено. Това означава, че за всяка крайна $\theta \subseteq f$ ще е вярно, че $\theta \notin \mathcal{A}$. Да видим, че тогава $\overline{K} \leqslant I_{\mathcal{A}}$, което ще противоречи на полуразрешимостта на $I_{\mathcal{A}}$.

От третото НДУ за полуразрешимост (*Твърдение* 4.10), приложено за полуразрешимото множество K, ще съществува рекурсивна функция ρ, такава че за всяко a:

$$a \in K \iff \exists t\ \rho(a,t) = 0. \tag{4.4}$$

Чрез тази функция ρ дефинираме функцията g по следния начин:

$$g(a,x) \simeq \begin{cases} f(x), & \text{ако } \forall t \leq x\ \rho(a,t) > 0 \\ \neg!, & \text{ако } \exists t \leq x\ \rho(a,t) = 0. \end{cases}$$

Тъй като f е изчислима, а условието $\forall t \leq x\ \rho(a,t) > 0$ е разрешимо, то и g ще е изчислима. S^m_n-теоремата, приложена към нея, ще ни даде рекурсивна функция h, такава че за всяко a и x,

$$\varphi_{h(a)}(x) \simeq g(a,x). \tag{4.5}$$

Нашата цел ще бъде да покажем, че $\overline{K}$ се свежда към $I_{\mathcal{A}}$ чрез горната функция h (т.е. $a \in \overline{K} \iff h(a) \in I_{\mathcal{A}}$).
Да разгледаме най-напред случая $a \in \overline{K}$. Тогава от (4.4) ще имаме, че $\forall t\ \rho(a,t) > 0$. Но това означава, че $g(a,x) \simeq f(x)$ за всяко x. Тогава според (4.5) ще имаме, че

$$\varphi_{h(a)}(x) \simeq f(x)$$

за всяко x и значи $\varphi_{h(a)} = f$. Но съгласно нашия избор, $f \in \mathcal{A}$, с други думи, $\varphi_{h(a)} \in \mathcal{A}$ и значи $h(a) \in I_{\mathcal{A}}$. Така получихме, че

$$a \in \overline{K} \implies h(a) \in I_{\mathcal{A}}. \tag{4.6}$$

Нека сега $a \in K$. Тогава от (4.4) ще имаме, че $\rho(a,t) = 0$ за някое t. Нека t_0 е първото с това свойство. Лесно се вижда, че

$$\varphi_{h(a)}(x) \simeq g(a,x) \simeq \begin{cases} f(x), & \text{ако } x < t_0 \\ \neg!, & \text{иначе.} \end{cases}$$

Следователно в този случай $\varphi_{h(a)}$ е крайна и очевидно $\varphi_{h(a)} \subseteq f$. Но по допускане никоя такава функция не може да е в класа $\mathcal{A}$, т.е. имаме $\varphi_{h(a)} \notin \mathcal{A}$ и съответно — $h(a) \notin I_{\mathcal{A}}$. Така стигнахме до импликацията

$$a \in K \implies h(a) \notin I_{\mathcal{A}},$$

която заедно с обратната ѝ импликация (4.6) ни дава общо $a \in \overline{K} \iff h(a) \in I_{\mathcal{A}}$. Това означава, че $\overline{K} \underset{h}{\leqslant} I_{\mathcal{A}}$ — противоречие с факта, че $I_{\mathcal{A}}$ е полуразрешимо.

Сега да проверим и обратната посока на еквивалентността (4.3). Нека за изчислимата функция f е вярно, че съществува крайна функция θ, такава че $\theta \subseteq f$ и $\theta \in \mathcal{A}$. Да допуснем, че $f \notin \mathcal{A}$. Целта ни е отново да стигнем до свеждането $\overline{K} \leqslant I_{\mathcal{A}}$, което ще ни даде търсеното противоречие.

Сега дефинираме функцията g както следва:

$$g(a,x) \simeq \begin{cases} f(x), & \text{ако } x \in Dom(\theta) \ \vee \ a \in K \\ \neg!, & \text{иначе.} \end{cases}$$

Да означим с A множеството $\{(a,x) \mid x \in Dom(\theta) \ \vee \ a \in K\}$ от дефиницията на g. Тогава

$$(a,x) \in A \iff x \in Dom(\theta) \vee a \in K \iff (a,x) \in (\mathbb{N} \times Dom(\theta)) \cup (K \times \mathbb{N}).$$

Така $A = (\mathbb{N} \times Dom(\theta)) \cup (K \times \mathbb{N})$ и значи A е полуразрешимо, следователно g е изчислима. Отново прилагаме S^m_n-теоремата и получаваме, че има рекурсивна функция h, такава че за всяко a и x:

$$\varphi_{h(a)}(x) \simeq g(a,x).$$

Ако $a \in K$, тогава за всяко x, $g(a,x) \overset{\text{деф}}{\simeq} f(x)$, което според горното равенство означава, че за всяко x, $\varphi_{h(a)}(x) \simeq f(x)$, т.е. $\varphi_{h(a)} = f \notin \mathcal{A}$. Тогава $h(a) \notin I_{\mathcal{A}}$, или дотук проверихме, че

$$a \in K \implies h(a) \notin I_{\mathcal{A}}.$$

Нека сега $a \notin K$. Тогава от дефиницията на g ще имаме:

$$\varphi_{h(a)}(x) \simeq g(a,x) \simeq \begin{cases} f(x), & \text{ако } x \in Dom(\theta) \\ \neg!, & \text{иначе.} \end{cases}$$

Понеже $\theta \subseteq f$, излезе, че в този случай $\varphi_{h(a)} = \theta$, като $\theta \in \mathcal{A}$, т.е. получихме, че $\varphi_{h(a)} \in \mathcal{A}$ и съответно — $h(a) \in I_{\mathcal{A}}$. Така проверихме импликацията $a \in \overline{K} \implies h(a) \in I_{\mathcal{A}}$, която заедно с обратната импликация от по-горе, ни дава общо $a \in \overline{K} \iff h(a) \in I_{\mathcal{A}}$ и търсеното противоречие. □

От тази теорема на момента получаваме, че проблемът за тоталността не е полуразрешим, защото няма крайни функции, за които той да е в сила:

Задача 4.42. Докажете, че проблемът "$\varphi_a \in \mathcal{A}_{tot}$?" не е полуразрешим.

Решение. Ако допуснем, че е полуразрешим, то трябва да е изпълнено условието (4.3). Но няма крайна функция, която принадлежи на $\mathcal{A}_{tot}$, и значи допускането ни е погрешно. □

От теоремата на Райс-Шапиро получаваме следното удобно за използване ДУ за неполуразрешимост:

Следствие 4.7. Нека проблемът "$\varphi_a \in \mathcal{A}$?" е полуразрешим. Тогава класът $\mathcal{A}$ е затворен нагоре, т.е. за всяка $f, g \in \mathcal{C}_1$ е в сила импликацията:

$$f \in \mathcal{A} \;\&\; f \subseteq g \implies g \in \mathcal{A}.$$

Доказателство. Нека $f \in \mathcal{A}$. Тогава от еквивалентността (4.3), прочетена в правата посока, ще имаме, че за някоя крайна функция $\theta \subseteq f$ ще е вярно, че $\theta \in \mathcal{A}$. Сега ако $f \subseteq g$, по транзитивността на $\subseteq$ получаваме, че $\theta \subseteq g$, и оттук отново чрез (4.3), но този път приложена в обратната посока, достигаме до $g \in \mathcal{A}$. □

Оттук лесно се вижда как теоремата на Райс-Успенски следва леко от теоремата на Райс-Шапиро:

Задача 4.43. Изведете теоремата на Райс-Успенски като следствие на теоремата на Райс-Шапиро.

Решение. Нека $\emptyset \subsetneqq \mathcal{A} \subsetneqq \mathcal{C}_1$ и да приемем, че проблемът "$\varphi_a \in \mathcal{A}$?" е разрешим. Тогава и двата проблема — "$\varphi_a \in \mathcal{A}$?" и "$\varphi_a \in \overline{\mathcal{A}}$?" ще са полуразрешими. Разглеждаме поотделно двата случая:

1 сл.: $\emptyset^{(1)} \in \mathcal{A}$. Тъй като за всяка функция $g \in \mathcal{C}_1$ е вярно, че $\emptyset^{(1)} \subseteq g$, то от горното следствие веднага следва, че $\mathcal{A} = \mathcal{C}_1$, което противоречи на условието $\mathcal{A} \subsetneqq \mathcal{C}_1$.

2 сл.: $\emptyset^{(1)} \notin \mathcal{A}$. Но тогава $\emptyset^{(1)} \in \overline{\mathcal{A}}$ и разсъждавайки както в сл. 1, ще получим, че $\overline{\mathcal{A}} = \mathcal{C}_1$, откъдето $\mathcal{A} = \emptyset$ — отново противоречие с условието.

Следователно допускането ни, че проблемът "$\varphi_a \in \mathcal{A}$?" е разрешим, е било погрешно. □

От това следствие с контрапозиция получаваме, че ако $\mathcal{A}$ не е затворен нагоре, то проблемът "$\varphi_a \in \mathcal{A}$?" не е полуразрешим. Така можем да покажем, че не са полуразрешими редица проблеми.

Задача 4.44. Нека f_0 е фиксирана едноместна изчислима функция. Докажете, че проблемът "$\varphi_a = f_0$?" не е полуразрешим.

Решение. Този проблем можем да разпишем като "$\varphi_a \in \mathcal{A}$?", където $\mathcal{A} = \{f_0\}$. Да видим, че той не е полуразрешим. Ще разгледаме следните два случая за f_0:

1 сл.: f_0 е крайна. Тогава според горното *Следствие* 4.7, класът $\mathcal{A}$ трябва да е затворен нагоре, а той очевидно не е — противоречие.

2 сл.: f_0 не е крайна. Тогава според (4.3) класът $\mathcal{A}$ трябва да съдържа крайна функция, а той очевидно не съдържа такава — отново противоречие. $\square$

Видяхме, че проблемът "$\varphi_a = f_0$?" не е полуразрешим. Дали това ще бъде вярно и за допълнителния проблем "$\varphi_a \neq f_0$?"? Оказва се, че не е.

Задача 4.45. Има ли изчислима функция f_0, за която проблемът "$\varphi_a \neq f_0$?" да е полуразрешим?

Решение. Нека $\mathcal{A} = \{f \mid f \neq f_0\}$. Тогава

$$\varphi_a \neq f_0 \iff \varphi_a \in \mathcal{A}$$

и можем да разсъждаваме за $\mathcal{A}$.

Ако f_0 не е $\emptyset^{(1)}$, то $\emptyset^{(1)} \in \mathcal{A}$ и следователно проблемът "$\varphi_a \neq f_0$?" няма да е полуразрешим, съгласно *Следствие* 4.6.

Ако $f_0 = \emptyset^{(1)}$, се оказва, че проблемът "$\varphi_a \neq f_0$?" , т.е "$\varphi_a \neq \emptyset^{(1)}$?", вече е полуразрешим. Наистина, в този случай ще имаме, че за произволно a:

$$a \in I_{\mathcal{A}} \iff \varphi_a \neq \emptyset^{(1)} \iff \exists x \, !\varphi_a(x) \iff \exists x \, !\Phi_1(a, x)$$

и значи $I_{\mathcal{A}}$ е полуразрешимо множество. $\square$