

Поняття алгоритму.

Алгоритм Евкліда (визначення НСД).

Вхід. p и q , додатні цілі числа.

Вихід. g , НСД чисел p і q .

Метод. 1. Знайти r , остачу від ділення p на q .

2. Якщо $r = 0$, покласти $g = q$ і зупинитись.

Інакше, покласти $p = q$, $q = r$ і перейти на 1.

Алгоритм - всюди визначений, якщо він зупиняється на всіх входах, тобто на всіх значеннях вхідних даних.

Приклад 1. **Вхід.** p і q , додатні цілі числа.
Вихід. g , сума чисел p і q .

Метод. Покласти $g = p + q$ і зупинитись.

Алгоритм - частковий, якщо він не зупиняється на деяких входах.

Приклад 2. **Вхід.** p - довільне ціле число.
Вихід. p .

Метод. 1. Якщо $p = 0$, то перейти на 1.
Інакше - зупинитись.

При $p = 0$ алгоритм не зупиняється.

Загальні риси алгоритмів

1. *Дискретність*. В процесі виконання алгоритму із початкової скінченної системи величин та величин, знайдених в попередні моменти часу послідовно (в дискретному часі) будується система величин по деякому закону (програмі).

2. *Елементарність*. Закон повинен бути простим.

3. *Детермінованість*. Система величин,

які одержуються в якийсь момент часу однозначно визначається системою величин, одержаних в попередні моменти часу.

4. *Результативність*. Якщо спосіб одержання величини не дає результату, то повинно бути вказано, що вважати результатом алгоритму.

5. *Масовість*. Початкова система величин (вхід алгоритму) може вибиратись із потенційно нескінченної множини.

Алгоритм, визначений загальними рисами 1-5 називається *інтуїтивним* поняттям алгоритму.

Такому інтуїтивному поняттю алгоритму задовольняє наступне: алгоритм – це скінченна множина правил (програма), яка дозволяє кожному елементу x із деякої нескінченної області (області визначення алгоритму) ставити у відповідність скінченну послідовність елементів $\langle x_0, x_1, \dots, x_k \rangle$ (процес обчис-

лень) так, що кожний наступний елемент x_{i+1} будується за попереднім елементом x_i застосуванням до нього деякого елементарного правила (крок алгоритму), а застосування правила до елемента x_k уже неможливе.

В цьому випадку елемент x_k вважається результатом застосування алгоритму до елемента x .

Отже, алгоритм – це скінченна послідовність правил «конструктивного» перетворення вхідних даних у вихідні.

Якщо алгоритм зупиняється через скінченну кількість кроків (скінченна кількість застосувань правил перетворення), то говорять, що алгоритм визначений на вхідних даних, в іншому випадку – коли алгоритм працює нескінченно довго – говорять, що алгоритм невизначений на вхідних даних.

Приклад 3. Необхідно знайти алгоритм, який дозволяє для кожної четвірки цілих чисел a, b, c, d вияснити, існують чи ні цілі числа x, y , які задовольняють рівнянню

$$ax^2 + bxy + cy^2 = d.$$

Такий алгоритм був побудований.

Приклад 4 (Проблема відповідностей Поста). Нехай $(x, y) \subseteq \Sigma^* \times \Sigma^*$ - скінченна множина пар непустих слів в алфавіті Σ .

Проблема. Чи існує скінченна послідов-

ність пар $(x_1, y_1), \dots, (x_n, y_n)$ (не обов'язково різних) таких, що $x_1 x_2 \dots x_n = y_1 y_2 \dots y_n$. Така послідовність називається розв'язуючою.

Приклад 5. Нехай $\{(abbb, b), (a, aab), (ba, b)\}$ – скінченна множина пар в алфавіті Σ . Тоді послідовність $(a, aab), (a, aab), (ba, b), (abbb, b)$ - розв'язуюча так, як

$$(a)(a)(ba)(abbb) = (aab)(aab)(b)(b).$$

Скінченна множина $\{(ab, aba), (aba, baa), (baa, aa)\}$ пар в цьому ж алфавіті розв'язуючих послідовностей не має.

Побудувати алгоритм, який розв'язує цю проблему неможливо. Але для цього потрібно довести неіснування алгоритму.

Як це зробити? Для цього треба точно знати, що таке алгоритм, тобто мати якесь математичне поняття, еквівалентне поняттю алгоритму.

Розв'язання задачі точного визначення алгоритму було одержано в роботах Гільберта, Геделя, Чьорча, Кліні, Поста, Т'юрінга.

Для цього розглядалися функції $f:\mathbb{N}\rightarrow\mathbb{N}$ і клас функцій, які обчислюються алгоритмами ототожнювався з класом спеціально побудованих функцій – рекурсивних (таке ототожнення або гіпотеза відома під назвою тези Чьорча).

Алгоритмічна обчислюваність функцій означає існування алгоритму, який знаходить їх значення (у випадку визначеності функцій) і працює нескінченно довго в іншому.

Тези Чьорча достатньо, щоб доводити нерозв'язність алгоритмічних проблем. Тому, що питання про алгоритмічну обчислюваність функцій еквівалентне питанню про її рекурсивність. Поняття рекурсивної функції – математично точне. Тому можна безпосередньо доводити, що функція, яка розв'язує задачу не може бути рекурсивною.

Поняття примітивно рекурсивної, частково рекурсивної та рекурсивної функцій. Алгебри рекурсивних функцій.

Розглянемо спосіб опису алгоритмічно обчислюваних функцій, що ґрунтується на породженні таких функцій за допомогою певних обчислюваних операцій із так званих базових функцій.

Надалі під функцією будемо розуміти функцію натуральних аргументів і значень.

Базовими функціями називаються найпростіші функції $o(x) = 0$, $s(x) = x+1$ та функції-селектори $I_m^n(x_1, \dots, x_n) = x^m$, де $n \geq m \geq 1$.

Всі базові функції всюди визначені.

Основними обчислювальними операціями будуть операції суперпозиції S^{n+1} , примітивної рекурсії R та мінімізації M .

Операція суперпозиції S^{n+1} дозволяє із n -арної функції $g(x_1, \dots, x_n)$ та n функцій $g_1(x_1, \dots, x_m)$, \dots , $g_n(x_1, \dots, x_m)$, однакової арності ут-

ворити функцію

$$f(x_1, \dots, x_m) = g(g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m)).$$

Таку функцію позначають $S^{n+1}(g, g_1, \dots, g_n)$.

Операція примітивної рекурсії R дозволяє із n -арної функції g та $n+2$ -арної функції h утворити $n+1$ -арну функцію f за допомогою наступних співвідношень:

$$f(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n)$$

$$f(x_1, \dots, x_n, y+1) = h(x_1, \dots, x_n, y, f(x_1, \dots, x_n, y))$$

Таку функцію позначають $R(g, h)$.

Операція мінімізації M дозволяє із n -арної функції g утворити n -арну функцію f , що задається співвідношенням:

$$f(x_1, \dots, x_n) = \mu_y (g(x_1, \dots, x_{n-1}, y) = x_n).$$

Тобто, значення функції $f(x_1, \dots, x_n)$ дорівнює найменшому y для якого $g(x_1, \dots, x_{n-1}, y) = x_n$.

Значення функції $f(x_1, \dots, x_n)$ вважається невизначеним у випадках: 1) для всіх y значення $g(x_1, \dots, x_{n-1}, y) \neq x_n$; 2) для всіх $y < t$ значення $g(x_1, \dots, x_{n-1}, y)$ визначене і $\neq x_n$, а

значення $g(x_1, \dots, x_{n-1}, t)$ невизначене; 3)

значення $g(x_1, \dots, x_{n-1}, 0)$ невизначене.

Таку функцію позначають $M(g)$.

Функцію, яку можна одержати з базових функцій за допомогою скінченної кількості застосувань операцій суперпозиції та примітивної рекурсії, називають *примітивно рекурсивною функцією* (скорочено ПРФ).

Функцію, яку можна одержати з базових функцій за допомогою скінченної кількості застосувань операцій суперпозиції, примітивної рекурсії та мінімізації, називають *частково рекурсивною функцією* (скорочено ЧРФ).

Всюди визначену ЧРФ називають *рекурсивною функцією* (скорочено РФ).

Із визначень ПРФ, ЧРФ, РФ маємо такі співвідношення між класами функцій:

$$\text{ПРФ} \subseteq \text{РФ} \subseteq \text{ЧРФ}.$$

Приклад 6. За визначенням, функції $o(x) = 0$, $s(x) = x+1$, $I_m^n(x_1, \dots, x_n) = x^m$, де $n \geq m \geq 1$ – примітивно рекурсивні.

Для n -місної функції $o^n(x_1, \dots, x_n) = 0$

маємо

$$o^n(x_1, \dots, x_n) = S^2(o, I_1^n(x_1, \dots, x_n))$$

і тому функція o^n - примітивно рекурсивна.

Зрозуміло, що існують алгоритми для обчислення значень базових функцій $o(x) = 0$, $s(x) = x+1$, $I_m^n(x_1, \dots, x_n) = x_m$.

При цьому конструктивне перетворення вхідних даних функції $f(x_1, \dots, x_n)$ в результаті означає, що для будь-яких натуральних чисел x_1, \dots, x_n вхідне слово $1^{x_1}\# \dots \# 1^{x_n}$ перетворюється в слово $1^{f(x_1, \dots, x_n)}$, якщо $f(x_1, \dots, x_n)$ визначене і працює нескінченно довго, якщо $f(x_1, \dots, x_n)$ не визначене ($1^{x_i} - x_i$ одиниць).

Так, обчислення функції $o(x)$ зводиться до витирання вихідного слова, обчислення функції $s(x)$ до дописування одиниці до вхідного слова, обчислення $I_m^n(x_1, \dots, x_n)$ до стирання всіх вхідних компонент, крім m -ї.

Оператори суперпозиції, примітивної рекурсії та мінімізації теж породжують алгоритмічно обчислювані функції із алгоритмічно обчислюваних функцій.

Дійсно, у випадку суперпозиції, якщо ми можемо обчислювати значення функцій g, g_1, \dots, g_n , то значення їх суперпозиції $f(a_1, \dots, a_m)$

можна обчислити за допомогою наступного алгоритму $S^{n+1}(g, g_1, \dots, g_n)$: знаходимо числа $b_1 = g_1(a_1, \dots, a_m), \dots, b_n = g_n(a_1, \dots, a_m)$, $b = g(b_1, \dots, b_n)$.

Останнє i є значенням суперпозиції .

У випадку примітивної рекурсії, якщо ми можемо обчислювати значення функцій g , h , то значення функції $f(a_1, \dots, a_n, m+1)$ може бути обчислене за допомогою наступного алгоритму $\mathbf{R}(g, h)$: послідовно знаходимо числа $b_0 = g(a_1, \dots, a_n)$, $b_1 = h(a_1, \dots, a_n, 0, b_0)$, $b_2 = h(a_1, \dots, a_n, 1, b_1)$, \dots , $b_{m+1} = h(a_1, \dots, a_n, m, b_m)$. Число b_{m+1} буде значенням функції f в точці $(a_1, \dots, a_n, m+1)$.

У випадку операції мінімізації, якщо ми можемо обчислювати значення функції g , то значення функції $f(a_1, \dots, a_n)$ може бути обчислене за допомогою наступного алгоритму $\mathbf{M}(g)$: послідовно обчислюємо значення $g(a_1, \dots, a_n, 0)$, $g(a_1, \dots, a_n, 1)$, \dots .

Найменше значення a , для якого

$$g(a_1, \dots, a_n, a) = 0$$

і є значенням функції f в точці (a_1, \dots, a_n) .

Характеристичною функцією χ_A множини натуральних чисел A називається одномісна функція, рівна 0 в точках множини A і рівна 1 в точках, які не належать A .

Частковою характеристичною функцією множини натуральних чисел A називається одномісна функція, рівна 0 в точках множини A і не визначена в точках, які не належать A .

Множина натуральних чисел A називається примітивно рекурсивною, якщо її характеристична функція примітивно рекурсивна.

Множина натуральних чисел A називається частково рекурсивною, якщо її характеристична функція частково рекурсивна.

Зрозуміло, що кожна примітивно рекурсивна функція є частково рекурсивною (за визначенням).

Звідси випливає, що кожна примітивно рекурсивна множина є частково рекурсивною.

Теза Черча. *Клас алгоритмічно обчислюваних числових функцій співпадає з класом всіх частково рекурсивних функцій.*

Нехай $\chi(x)$ – характеристична функція множини натуральних чисел A .

Тоді функція $\chi_{\bar{A}}(x) = 0 - \chi(x)$ – часткова характеристична функція множини \bar{A} .

Теорема. Нехай $f(x)$ – примітивно рекурсивна функція, A – примітивно рекурсивна множина. Тоді часткова функція $f_{\bar{A}}(x) = f(x)$, якщо $x \in A$ і невизначена, якщо $x \notin A$ є частково рекурсивною.

Доведення. Легко бачити, що $f_{\text{ч}}(x) = f(x) + \chi_{\text{ч}}(x)$. Так як $\chi_{\text{ч}}(x)$ – частково рекурсивна, то $f_{\text{ч}}(x)$ – частково рекурсивна.

Теорема дозволяє будувати приклади частково рекурсивних функцій (при умові, що операції “+”, “-” не виводять із класу ЧРФ).

Всюди визначені частково рекурсивні функції називаються *загальнорекурсивними*.

Деякі примітивно рекурсивні функції

1.
$$\text{sg}(x) = \begin{cases} 0, & x = 0 \\ 1, & x > 0 \end{cases}$$

2.
$$\overline{\text{sg}}(x) = \begin{cases} 1, & x = 0 \\ 0, & x > 0 \end{cases}$$

3.
$$x \boxminus y = \begin{cases} x - y, & x \geq y \\ 0, & x < y \end{cases}$$

Властивості ПР функцій

Теорема 1 (про сумування). Нехай n -місна функція g примітивно рекурсивна. Тоді n -місна функція f , яка визначається рівністю

$$f(x_1, \dots, x_n) = \sum_{i=0}^{x_n} g(x_1, \dots, x_{n-1}, i),$$

теж примітивно рекурсивна.

Доведення. Із рівності випливають спів-
відношення:

$$\begin{aligned} f(x_1, \dots, x_{n-1}, 0) &= g(x_1, \dots, x_{n-1}, 0), \\ f(x_1, \dots, x_{n-1}, y+1) &= \\ &f(x_1, \dots, x_{n-1}, y) + g(x_1, \dots, x_{n-1}, y+1). \end{aligned}$$

Але функції

$g(x_1, \dots, x_{n-1}, 0)$ та

$$h(x_1, \dots, x_{n-1}, y, z) = z + g(x_1, \dots, x_{n-1}, y+1)$$

ПР функції.

Дійсно,

$$g(x_1, \dots, x_{n-1}, 0)$$

є суперпозицією $g(x_1, \dots, x_n)$ та, наприклад, $I_1^{n-1}(x_1, \dots, x_{n-1}), \dots, I_{n-1}^{n-1}(x_1, \dots, x_{n-1}), O^{n-1}(x_1, \dots, x_{n-1})$.

Функції $q_1(x_1, \dots, x_{n-1}, y, z) = z = I_{n+1}^{n+1}(x_1, \dots, x_{n-1}, y, z)$,

$q_2(x_1, \dots, x_{n-1}, y, z) = g(x_1, \dots, x_{n-1}, y+1) = g(I_1^n(x_1, \dots, x_n), \dots, I_{n-1}^n(x_1, \dots, x_n), s(I_n^n(x_1, \dots, x_{n-1}, y)))$.

Тому $h(x_1, \dots, x_{n-1}, y, z) = S(+, q_1, q_2)$ і, отже, є ПР функцією. Звідси f – ПР функція, як така, що виникає за схемою примітивної рекурсії із g та h .

Наслідок 1. Якщо n -місна функція g примітивно рекурсивна, то $n+1$ -місна функція f , яка визначається схемою

$$f(x_1, \dots, x_{n-1}, y, z) = \begin{cases} \sum_{i=y}^z g(x_1, \dots, x_{n-1}, i), & \text{якщо } y \leq z; \\ 0, & \text{якщо } y > z, \end{cases}$$

також ПР функція.

Дійсно, функція f задовольняє співвідношенню

$$f(x_1, \dots, x_{n-1}, y, z) = \left(\sum_{i=0}^z g(x_1, \dots, x_{n-1}, i) \div \sum_{i=0}^y g(x_1, \dots, x_{n-1}, i) \right) + g(x_1, \dots, x_{n-1}, y) \overline{sg}(y \div z).$$

Функції \div та \overline{sg} - ПР. В силу попередньої теореми та того, що $f = S(+, q_1, q_2)$, де

$$q_1 = S(\div, \sum_{i=0}^z g(x_1, \dots, x_{n-1}, i), \sum_{i=0}^y g(x_1, \dots, x_{n-1}, i)),$$

$q_2 = S(\times, g(x_1, \dots, x_{n-1}, y), \overline{sg}(y \div z))$ функція f – ПР функція.

Наслідок 2. Якщо g, h, k – ПР функції, то функція f^* , що визначається співвідношенням

$$f^*(x_1, \dots, x_n) = \begin{cases} \sum_{i=h(x_1, \dots, x_n)}^{k(x_1, \dots, x_n)} g(x_1, \dots, x_{n-1}, i), & \text{якщо} \\ h(x_1, \dots, x_n) \leq k(x_1, \dots, x_n); \\ 0, & \text{якщо } h(x_1, \dots, x_n) > k(x_1, \dots, x_n) \end{cases}$$

також ПР функція.

Ця функція є суперпозицією функції f з наслідка 1, функцій селекторів та функцій h, k ($f^*(x_1, \dots, x_n) = f(x_1, \dots, x_{n-1}, h, k)$).

Теорема 2 (про множення). Нехай n -місна функція g примітивно рекурсивна. Тоді n -місна функція f , яка визначається рівністю

$$f(x_1, \dots, x_n) = \prod_{i=0}^{x_n} g(x_1, \dots, x_{n-1}, i),$$

теж примітивно рекурсивна.

Говорять, що функція f в теоремі 1 виникає з функції g операцією сумування, а функція f в теоремі 2 виникає з функції g операцією множення.

Кускове задання функції

Нехай задані функції $f_i(x_1, \dots, x_n)$, $i=1, \dots, k+1$ та умови $P_j(x_1, \dots, x_n)$, $j=1, \dots, k$, які для будь-якого набору чисел x_1, \dots, x_n можуть приймати значення 0 або 1.

Для доведення достатньо зауважити, що функцію f можна представити у вигляді

$$f = f_1 \overline{\text{sg}} \alpha_1 + \dots + f_k \overline{\text{sg}} \alpha_k + f_{k+1} \text{sg} (\alpha_1 \dots \alpha_k),$$

де $\overline{\text{sg}} = 1$, якщо $x=0$, $\overline{\text{sg}} = 0$, якщо $x > 0$ – ПР функція.

В теоремі 3 розглянуто типовий випадок, коли умова P_i має вигляд $\alpha_i=0$. Так як умови вигляду

$$\alpha_i=\beta_i, \alpha_i\leq\beta_i, \alpha_i<\beta_i \quad \text{рівносильні,}$$

відповідно, умовам

$$|\alpha_i-\beta_i|=0, \alpha_i\div\beta_i=0, (\beta_i\div\alpha_i)=0,$$

то теорема 3 залишається справедливою і в тому разі, коли в кусковій схемі рівності $\alpha_i=0$ замінюються іншими умовами, де α_i, β_i – ПР функції.

Розглянемо рівняння

$$g(x_1, \dots, x_n, y) = 0,$$

ліва частина якого є всюди визначена функція. Припустимо, що для кожного набору значень x_1, \dots, x_n це рівняння має єдиний розв'язок y . Тоді цей розв'язок буде однозначною всюди визначеною функцією від x_1, \dots, x_n . Чи буде ця функція примітивно рекурсивною, якщо функція g є ПР функцією від x_1, \dots, x_n, y ? В загальному випадку відповідь

на це питання негативна. Але справедлива наступна теорема.

Теорема 4 (про мажоруючі неявні функції). Нехай $g(x_1, \dots, x_n, y)$, $\alpha(x_1, \dots, x_n)$ - такі ПР функції, що рівняння $g(x_1, \dots, x_n, y) = 0$ для кожних x_1, \dots, x_n має хоча б один розв'язок і

$$\mu_y(g(x_1, \dots, x_n, y) = 0) \leq \alpha(x_1, \dots, x_n) \quad (*)$$

для будь-яких x_1, \dots, x_n . Тоді функція

$$f(x_1, \dots, x_n) = \mu_y(g(x_1, \dots, x_n, y) = 0)$$

також ПР функція.

Доведення. Фіксуємо які-небудь значення x_1, \dots, x_n і нехай

$$a = \mu_y(g(x_1, \dots, x_n, y) = 0).$$

Розглянемо послідовність добутків

$$g(x_1, \dots, x_n, 0)g(x_1, \dots, x_n, 1) \dots g(x_1, \dots, x_n, i) \\ (i = 0, 1, 2, \dots).$$

Так як $y=a$ є найменший розв'язок рівняння $g(x_1, \dots, x_n, y) = 0$, то перші a членів цієї послідовності не рівні нулю, а інші містять рівний 0 співмножник $g(x_1, \dots, x_n, a)$ і тому рівні

нулю. Враховуючи обмеження (*), будемо мати

$$a = \sum_{i=0}^{\alpha(x_1, \dots, x_n)} \text{sg}(g(x_1, \dots, x_n, 0) \dots g(x_1, \dots, x_n, i)).$$

Введемо ПР функцію

$$h(x_1, \dots, x_n, z) = \prod_{i=0}^z g(x_1, \dots, x_n, i).$$

Тоді

$$f(x_1, \dots, x_n) = \sum_{i=0}^{\alpha(x_1, \dots, x_n)} \text{sg}(h(x_1, \dots, x_n, i)).$$

Звідси випливає, що функція f ПР функція.

Примітивна рекурсивність деяких арифметичних функцій

Нехай $f(x,y) = [x/y]$ – частка від ділення x на y , а $g(x,y) = \text{rest}(x,y)$ – остача від ділення x на y .

Для того, щоб введені функції були всюди визначені, покладемо

$$[x/0] = x, \text{rest}(x,0) = x \text{ для всіх } x.$$

Зрозуміло, що так визначені функції зв'язані тотожністю $\text{rest}(x,y) = x \div (y \times [x/y])$.

Тому, із того, що функція $[x/y]$ – ПР функція, буде випливати, що $\text{rest}(x,y)$ – ПР функція ($\text{rest}(x,y) = \div(x, y \times [x/y]) = \div(I_1^2(x,y), \times(y, [x/y])) = \div(I_1^2(x,y), \times(I_2^2(x,y), [x/y]))$).

Твердження. Функція $f(x,y) = [x/y]$ – ПР функція.

Дійсно, $x = y \times [x/y] + \text{rest}(x,y)$. Тому при $y > 0$ виконуються співвідношення

$$y \times [x/y] \leq x = y \times [x/y] + \text{rest}(x,y) < ([x/y] + 1) \times y.$$

Звідси видно, що $[x/y]$ дорівнює числу нулів в послідовності

$$1y \div x, 2y \div x, \dots, [x/y]y \div x, \dots, xy \div x.$$

Тому для $y > 0$ маємо формулу

$$[x/y] = \sum_{j=0}^x \overline{\text{sg}}(iy \div x).$$

Ця формула буде вірною і при $y=0$. Так як функція $\overline{\text{sg}}(iy \div x)$ ПР функція, то за теоремою про суму функція $[x/y]$, а разом з нею і функція $\text{rest}(x,y)$ ПР функції.

Нехай $\text{div}(x,y) = 1$, якщо $\text{rest}(x,y) = 0$,
 $\text{div}(x,y) = 0$, якщо $\text{rest}(x,y) \neq 0$.

Очевидне співвідношення

$$\text{div}(x,y) = \overline{\text{sgrest}(x,y)}$$

показує, що функція div - ПР функція.

Нехай

$$\text{nd}(x) = \sum_{i=0}^x \text{div}(x,i).$$

При $x > 0$ число $\text{nd}(x)$ співпадає з числом різних дільників числа x . Крім того, функція nd – ПР функція.

Введемо для простих чисел 2, 3, 5, 7, ...
позначення $p_0 = 2, p_1 = 3, \dots$. Таким чином, p_n –
це $(n+1)$ просте число.

Позначимо через $\chi_p(n)$ функцію таку, що
 $\chi_p(n) = 0$ для n простого і $\chi_p(n) = 1$ для n не-
простого.

Так як прості числа і тільки вони мають
рівно 2 дільника, то

$$\chi_p(x) = \text{sg}|nd(x)-2|$$

а, отже, $\chi_p(x)$ – ПР функція.

Функція $\pi(x)$, яка дорівнює числу простих чисел, що не перевищують x задається формулою

$$\pi(x) = \sum_{i=0}^x \overline{\text{sg}} \chi_p(i)$$

і тому є ПР функцією.

Із визначення функції $\pi(x)$ безпосередньо випливає, що

$$\pi(p_n) = n+1,$$

$$\pi(x) < n+1, \text{ якщо } x < p_n.$$

Звідси видно, що $x = p_n$ є мінімальний розв'язок рівняння $\pi(x) = n+1$. Тому

$$p_n = p(n) = \mu_x(|\pi(x) - (n+1)| = 0).$$

Функція $|\pi(x) - (n+1)|$ - ПР функція. В силу теореми про мажоруючі неявні функції для доведення того, що функція $p(n)$ – ПР функція, достатньо знайти ПР функцію $\alpha(n)$ таку, що для всіх n виконується $p_n \leq \alpha(n)$. За функцію $\alpha(n)$ можна взяти 2^{2^n} . Отже $p(x)$ ПР функція.

Рекурсія 2-го рівня

Нехай $\alpha_1(x), \dots, \alpha_s(x)$ – всюди визначені функції, які для всіх значень x задовольняють умовам

$$\alpha_i(x+1) \leq x \quad (i=1, \dots, s).$$

Говорять, що функція $f(x_1, \dots, x_{n+1})$ одержується із функцій $g(x_1, \dots, x_n)$, $h(x_1, \dots, x_n, y, z_1, \dots, z_s)$ та допоміжних функцій $\alpha_1, \dots, \alpha_s$ рекурсією 2-го рівня, якщо для всіх значень змінних x_1, \dots, x_n, y

$$f(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n),$$

$$f(x_1, \dots, x_n, y+1) = h(x_1, \dots, x_n, y,$$

$$f(x_1, \dots, x_n, \alpha_1(y+1)), \dots, f(x_1, \dots, x_n, \alpha_s(y+1)))$$

Теорема. Функція $f(x_1, \dots, x_{n+1})$ може бути одержана з функцій g, h, α_i (схема рекурсії 2-го рівня) та найпростіших функцій операціями підстановки та примітивної рекурсії, а отже є ПР функцією.

Приклад. Послідовність Фібоначчі.

$$F(0)=0, F(1)=1, F(n+2) = F(n) + F(n+1) .$$

Або $F(0) = 0$,

$$F(n+1) = F(n) + F(n \div 1) + \overline{sg} n.$$

Звідси видно, що $F(n)$ одержується рекурсією 2-го рівня з функції

$h(y, z_1, z_2) = \overline{sg} y + z_1 + z_2$ та допоміжних функцій

$$\alpha_1(y) = y \div 1, \alpha_2(y) = y \div 2.$$

Отже, $F(n)$ – ПР функція.

(Чому $(y+1) \div 2 = y \div 1$?)

Нумерації пар і n-ок чисел

Ми розглядали функції виду

$$f: \mathbb{N} \times \mathbb{N} \times \dots \times \mathbb{N} \rightarrow \mathbb{N}$$

і доводили їх примітивну рекурсивність.

Розглянемо функцію виду

$$f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N},$$

наприклад таку $f(\langle x, y \rangle) = \langle x, y \rangle$.

Як показати, що вона буде алгоритмічно обчислюваною?.

Можна розглянути дві функції

$$f_1(\langle x, y \rangle) = x, f_2(\langle x, y \rangle) = y.$$

Такі функції, як відомо є ПР функціями
($f_1(\langle x, y \rangle) = I^2_1(x, y)$, $f_2(\langle x, y \rangle) = I^2_2(x, y)$).

Отже, функція $f(\langle x, y \rangle) = \langle x, y \rangle$ може бути алгоритмічно обчислюваною (покомпонентно). Аналогічно у випадку функції

$$f(\langle x, y \rangle) = \langle g(x), h(y) \rangle$$

де g, h – ПР функції.

Інший випадок. Нехай функція $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ така, що існує бієкція $g: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, причому, g – ПР функція. Розглянемо функцію $h: \mathbb{N} \rightarrow \mathbb{N}$ таку, що

$$h(x) = y \Leftrightarrow f(g^{-1}(x)) = g^{-1}(y).$$

Якщо функція h алгоритмічно обчислювана, то такою ж буде і функція f . Дійсно, для того, щоб обчислити значення функції f в точці $\langle x, y \rangle$, обчислимо значення функції h в точці $z = g(\langle x, y \rangle)$. Покладемо $f(\langle x, y \rangle) = g^{-1}(h(z))$.

Дійсно, якщо $f(\langle x, y \rangle) = \langle x', y' \rangle$, то
 $h(g(\langle x, y \rangle)) = g(\langle x', y' \rangle) (f(g^{-1}(g(\langle x, y \rangle))) =$
 $f(\langle x, y \rangle) = \langle x', y' \rangle = g^{-1}(g(\langle x', y' \rangle))$). Тобто,
наведеним вище способом, ми обчислюємо
значення функції f в точці $\langle x, y \rangle$.

Таким чином, бієкція між n -ми натуральних чисел дозволяє зводити питання про алгоритмічну обчислюваність функцій на одних структурах (n -ках) до питання про алгоритмічну обчислюваність на інших n -ках.

Одну із таких бієкцій між \mathbb{N} та $\mathbb{N} \times \mathbb{N}$ можна задати наступним чином. Всі пари натуральних чисел розташуємо в послідовність $\langle 0,0 \rangle, \langle 0,1 \rangle, \langle 1,0 \rangle, \langle 0,2 \rangle, \langle 1,1 \rangle, \langle 2,0 \rangle, \langle 0,3 \rangle, \dots$ тобто, впорядкуємо всі пари так, що пара $\langle x,y \rangle$ йде раніше за пару $\langle u,v \rangle$ якщо $x+y < u+v$, або якщо $x+y = u+v$ і $x < u$.

Бієкцію задаємо співвідношенням

$$\langle x,y \rangle \leftrightarrow n,$$

де n – номер пари в цій послідовності.

Така бієкція називається нумерацією Кантора пар чисел і позначається $c(x,y)$, тобто $c(x,y)$ – це номер пари $\langle x,y \rangle$ в послідовності Кантора.

Лівий та правий елементи пари $\langle x,y \rangle$ з номером n визначають функції $l(n)$ і $r(n)$, які називаються лівою та правою координатними функціями.

Теорема. Функції $c(x,y)$, $l(n)$, $r(n)$ – ПР функції.

Доведення. Пара $\langle x,y \rangle$ знаходиться у відрізку $\langle 0, x+y \rangle$, $\langle 1, x+y-1 \rangle$, ..., $\langle x,y \rangle$, ..., $\langle x+y, 0 \rangle$ на x -му місці після пари $\langle 0, x+y \rangle$. Перед парою $\langle 0, x+y \rangle$ в послідовності Кантора знаходяться $x+y$ відрізків, що містять $1+2+\dots+(x+y)$ пар. Тому $c(x,y) = \frac{(x+y)(x+y+1)}{2} + x = \frac{((x+y)^2 + 3x + y)}{2}$.

Для функції $l(n)$ враховуючи, що $c(x,y) = n$ із останньої формули будемо мати

$$2n = (x+y)^2 + 3x + y \text{ або}$$

$$8n+1 = (2x+2y+1)^2 + 8x = (2x+2y+3)^2 - 8y - 8 .$$

Звідси випливає, що

$$2x+2y+1 \leq [\sqrt{8n+1}] < 2x+2y+3 \text{ або}$$

$$x+y+1 \leq ([\sqrt{8n+1}]+1)/2 < x+y+2 .$$

Таким чином, $x+y+1 = ([\sqrt{8n+1}]+1)/2$.

З формули для $c(x,y)$ будемо мати

$$l(n) = x = n \div 1/2 [([\sqrt{8n+1}]+1)/2] [([\sqrt{8n+1}]\div 1)/2].$$

Таким чином, $\mathbf{c}(x,y)$ та $\mathbf{l}(n)$ – ПР функції.

Аналогічно для $\mathbf{r}(n)$ оскільки

$$\mathbf{r}(n) = y = (x+y+1) \div (x+1) = [([\sqrt{8n+1}] + 1) / 2] \div (x+1) = [([\sqrt{8n+1}] + 1) / 2] \div (\mathbf{l}(n) + 1).$$

Зауваження. Крім того, що функції $\mathbf{c}(x,y)$, $\mathbf{l}(n)$, $\mathbf{r}(n)$ – ПР функції, їх можна одержати з елементарних арифметичних функцій $+$, \div , \times , $[\sqrt{\quad}]$, $[/2]$ за допомогою операції суперпозиції.

Зазначимо також, що із визначення функцій $\mathbf{c}(x,y)$, $\mathbf{l}(n)$, $\mathbf{r}(n)$ випливають наступні

співвідношення

$$\mathbf{c}(\mathbf{l}(n), \mathbf{r}(n)) = n, \mathbf{l}(\mathbf{c}(x, y)) = x, \mathbf{r}(\mathbf{c}(x, y)) = y.$$

З допомогою нумерації пар чисел можна одержати нумерацію трійок, четвірок і т. д. натуральних чисел. Для цього вводяться наступні функції

$$\mathbf{c}^3(x_1, x_2, x_3) = \mathbf{c}(\mathbf{c}(x_1, x_2), x_3)$$

.....

$$\mathbf{c}^{n+1}(x_1, x_2, \dots, x_{n+1}) = \mathbf{c}^n(\mathbf{c}(x_1, x_2), x_3, \dots, x_{n+1})$$

За визначенням, число $c^n(x_1, x_2, \dots, x_n)$ називається канторовим номером n -ки $\langle x_1, x_2, \dots, x_n \rangle$.

Якщо $c^n(x_1, x_2, \dots, x_n) = x$, то із тотожностей для $c(x, y)$, $l(n)$, $r(n)$, $c^i(x_1, x_2, \dots, x_i)$ одержимо:
 $x_n = r(x)$, $x_{n-1} = rl(x)$, \dots , $x_2 = rl\dots l(x)$, $x_1 = ll\dots l(x)$.

Ввівши позначення $c_{nn}(x)$, \dots , $c_{n1}(x)$ для правих частин вищеприведених рівностей, одержимо:

одержимо $\mathbf{c}^n(c_{n1}(x), \dots, c_{nn}(x)) = x$,

$$c_{ni}(\mathbf{c}^n(x_1, x_2, \dots, x_n)) = x_i \quad (i=1, \dots, n).$$

Це аналоги канторової нумерації для n -ок чисел.

Введемо функцію

$$\Gamma(x, y) = \mathbf{rest}(l(x), 1 + (y+1)r(x)).$$

Функція Геделя

Функція Геделя $\Gamma(x, y)$ дозволяє генерувати довільні скінченні послідовності натуральних чисел згідно наступній властивості цієї функції: для будь-яких чисел $a_0, \dots, a_n \in \mathbb{N}$ існує x таке, що $\Gamma(x, i) = a_i$, $i = 0, \dots, n$.

Числа $q, p \in \mathbb{N}^+$ взаємно прості, якщо їх найбільший спільний дільник дорівнює 1.

Числа p_1, \dots, p_s називаються попарно простими, якщо будь-які два з них взаємно прості.

Лема. Для будь-яких взаємно простих чисел q, p має місце наступне співвідношення: $\{\text{rest}(pi, q) \mid i = 0, \dots, q-1\} = \{0, \dots, q-1\}$.

Доведення. Для будь-якого числа x маємо $0 \leq \text{rest}(x, q) \leq q-1$. Тому достатньо показати, що для будь-яких $0 \leq i < j \leq q-1$ виконується нерівність $\text{rest}(pi, q) \neq \text{rest}(pj, q)$. Допустимо протилежне. Тоді $pj - pi$ ділиться на q . Тобто p ділиться на q . Але p і q – взаємно прості і $q \neq 1$. Інакше – суперечність ($j-i \leq q-1$).

Теорема (китайська теорема про остачі).

Для будь-яких попарно простих чисел p_1, \dots, p_s і натуральних чисел a_1, \dots, a_s таких, що $a_i < p_i$, $i=1, \dots, s$ існує натуральне число $M < p_1 \times \dots \times p_s$ таке, що $\text{rest}(M, p_i) = a_i$ для всіх $i = 1, \dots, s$.

Доведення (індукцією по s).

1. Нехай $s=2$. За попередньою лемою існують числа $n < p_1$, $m < p_2$ такі, що $\text{rest}(p_1 m, p_2) = a_2$, $\text{rest}(p_2 n, p_1) = a_1$. Нехай $M' = p_1 m + p_2 n$ і $M_0 = \text{rest}(M', p_1 p_2)$. Тоді M_0 – шукане бо, $M_0 < p_1 p_2$ і

$\text{rest}(M_0, p_1) = a_1, \text{rest}(M_0, p_2) = a_2$ ($M' = kp_1p_2 + M_0$
для деякого k , а отже $\text{rest}(M_0, p_1) = \text{rest}(M' -$
 $kp_1p_2, p_1) = \text{rest}(M', p_1) = \text{rest}(p_2n, p_1) = a_1$).

Зауваження. Рівності для остач впливають із співвідношень $[x + y/z] = x + [y/z], [x - y/z] = x - [y/z], [(xz + y)/z] = x + [y/z]$.

2. Нехай твердження леми вірне для $s \leq m$.

Покажемо, що воно вірне і для $s = m + 1$.

Маємо натуральні a_1, \dots, a_{s+1} та попарно прості p_1, \dots, p_{s+1} такі, що $a_i < p_i, i = 1, \dots, s + 1$.

Покладемо, $p'_1 = p_1 p_2$, $p'_i = p_{i+1}$, $a'_1 = M_0$, $a'_i = a_{i+1}$, $i=2, \dots, s$. Тоді $p'_1 \dots p'_s$ попарно прості та $a'_i < p'_i$ для всіх $i=1, \dots, s$. Тому за припущенням індукції знайдеться натуральне M таке, що $M < p'_1 \dots p'_s$ та $\text{rest}(M, p'_i) = a'_i$ для всіх $i=1, \dots, s$. Звідси маємо $M < p_1 \dots p_{s+1}$, $\text{rest}(M, p_i) = a_i$ для всіх $i=3, \dots, s+1$ та $\text{rest}(M, p_1 p_2) = M_0$. Остання рівність означає, що $M = \beta p_1 p_2 + M_0$ для деякого β . Звідси маємо $\text{rest}(M, p_1) = \text{rest}(M_0, p_1) = a_1$, $\text{rest}(M, p_2) = \text{rest}(M_0, p_2) = a_2$.

Теорема. Для будь-якої послідовності a_0, \dots, a_n натуральних чисел існує число $x \in \mathbb{N}$ таке, що $\Gamma(x, i) = a_i$, $i = 0, 1, \dots, n$.

Доведення. Нехай R таке число, що числа $1 + (i+1)R$, $i=0, \dots, n$ попарно прості і $a_i < 1 + (i+1)R$ для всіх $i=0, \dots, n$. Тоді за попередньою теоремою існує число L таке, що $\text{rest}(L, 1 + (i+1)R) = a_i$ для всіх $i=0, \dots, n$. Покладемо $x = \mathbf{c}(L, R)$. Тоді $\Gamma(x, i) = \text{rest}(\mathbf{l}(x), 1 + (i+1)\mathbf{r}(x)) = \text{rest}(\mathbf{l}(\mathbf{c}(L, R)), 1 + (i+1)\mathbf{r}(\mathbf{c}(L, R))) = \text{rest}(L,$

$1+(i+1)R) = a_i$ для всіх $i=0, \dots, n$ і теорема доведена. Залишилось знайти число R . Таким числом є число $R = (1+n+a_0+\dots+a_n)!$. Дійсно, $a_i < 1+(i+1)R$ для всіх $i=0, \dots, n$. Крім того числа $1+(i+1)R$ будуть попарно простими.

Справді, припустимо супротивне: існує просте $q > 1$ таке, що для деяких i, j таких, що $j > i$, $1+(i+1)R$ та $1+(j+1)R$ діляться на q . Але $j-i \leq n$, тому $j-i$ входить як множник в число R . Тому R ділиться на q , а отже $R = \gamma q$.

Звідси $1+(i+1)R = 1+(i+1) \gamma q$ та $1+(j+1)R = 1+(j+1) \gamma q$ не діляться на q , а це суперечить припущенню. Теорему доведено.

Функція Геделя разом з деякими іншими функціями утворює розширення множини базових функцій, яке дозволяє промоделювати операцію примітивної рекурсії.

Теорема (про моделювання примітивної рекурсії). Якщо функція виникає за схемою примітивної рекурсії із функцій g, h , то вона може бути одержана із функцій $g, h, \Gamma(x, y), \overline{sg}, x+y, x \div y, x \times y$ та найпростіших функцій скінченною кількістю застосувань операцій суперпозиції та мінімізації.

Доведення. Доводимо для випадку, коли f – функція двох змінних (В загальному випадку доведення аналогічне). За схемою

примітивної рекурсії маємо:

$$f(x, 0) = g(x)$$

$$f(x, 1) = h(x, 0, f(x, 0)) \quad (1)$$

.....

$$f(x, y) = h(x, y-1, f(x, y-1))$$

За основною властивістю функції Гьоделя

існує таке t , що

$$\Gamma(t, 0) = f(x, 0)$$

.....

$$\Gamma(t, y) = f(x, y)$$

(2)

Враховуючи (1) перепишемо (2) в вигляді

$$\Gamma(t, 0) = g(x)$$

$$\Gamma(t, 1) = h(x, 0, \Gamma(t, 0)) \quad (3)$$

.....

$$\Gamma(t, y) = h(x, y-1, \Gamma(t, y-1))$$

Згідно з (3) для всіх $u = 0, \dots, y-1$ виконується

$\Gamma(t, u+1) = h(x, u, \Gamma(t, u))$. Тому $\mu_u (y=u \text{ або } \Gamma(t, u+1) \neq h(x, u, \Gamma(t, u))) = y$. Отже (3) рівносильне

$$(4): \Gamma(t, 0) = g(x)$$

$$y = \mu_u (|y=u| \quad \overline{\text{sg}} \quad |\Gamma(t, u+1) - h(x, u, \Gamma(t, u))| = 0)$$

Позначивши $\mu_u(|y = u| \text{ sgn} |\Gamma(t, u+1) - h(x, u, \Gamma(t, u))| = 0)$ як $F(x, y, t)$ одержимо, що система (4) рівносильна рівнянню (5):

$$|\Gamma(t, 0) - g(x)| + |y - F(x, y, t)| = 0.$$

За основною властивістю функції Гьоделя система (3), а отже і рівняння (5) має розв'язок t для всіх x, y . Тому існує мінімальний розв'язок

$$t = \mu_z(|\Gamma(z, 0) - g(x)| + |y - F(x, y, z)| = 0).$$

Позначивши таке t як $\phi(x, y)$ маємо:

$f(x,y) = \Gamma(t,y) = \Gamma(\phi(x,y),y)$. Теорему

ДОВЕДЕНО.