

Универзитет у Београду
Математички факултет

Семинарски рад
Теорија израчунљивости

Примитивно рекурзивне функције

Грујић Александар
Октобар 2009.

ДЕФИНИЦИЈА ПО СЛУЧАЈУ

Теорема 1. Нека су $h_0, \dots, h_m$ примитивно рекурзивне функције аргумента $\bar{x} = (x_1, \dots, x_k)$ и $A_0, \dots, A_m$ примитивно рекурзивни предикати такви да за сваку k -торку $\bar{x}$ важи само један од њих. Тада је функција

$$f(\bar{x}) = \begin{cases} h_0(\bar{x}), & \text{ако важи } A_0(\bar{x}) \\ \vdots \\ h_m(\bar{x}), & \text{ако важи } A_m(\bar{x}) \end{cases}$$

примитивно рекурзивна и кажемо да је она дефинисана по случају.

Доказ. Функција f се може записати у облику

$$f(\bar{x}) = \sum_{i=0}^m h_i(\bar{x}) \cdot C_{A_i}(\bar{x}),$$

па је примитивно рекурзивна. □

Овакав начин задавања функције срећемо код дефинисања функције експлицитним задавањем вриједности за првих l природних бројева, а у преосталим случајевима користећи неку другу ПР функцију.

ОГРАНИЧЕНА КВАНТИФИКАЦИЈА

Дефиниција 1. Нека је k природан број и R $k + 1$ -арни предикат. *Ограничена егзистенцијална квантификација* предиката R је $k + 1$ -арни предикат Q за који важи

$$Q(\bar{x}, m) \Leftrightarrow (\exists i \leq m) R(\bar{x}, i), \quad 0 \leq i \in \mathbb{N}$$

Ограничена универзална квантификација предиката R је $k + 1$ -арни предикат Q за који важи

$$Q(\bar{x}, m) \Leftrightarrow (\forall i \leq m) R(\bar{x}, i), \quad 0 \leq i \in \mathbb{N}$$

Теорема 2. *Ако је R примитивно рекурзивни предикат арности $k+1$, тада су и предикати ограничене егзистенцијалне и универзалне квантификације за R примитивно рекурзивни.*

Доказ. Карактеристична функција предиката ограничене универзалне квантификације је

$$C_{\forall}(\bar{x}, m) = \prod_{i \leq m} C_R(\bar{x}, i),$$

а како је она примитивно рекурзивна (ограничени производ је ПР) и предикат ограничене универзалне квантификације је такав.

Даље је

$$(\exists i \leq m) R(\bar{x}, i) \Leftrightarrow \neg(\forall i \leq m) \neg R(\bar{x}, i),$$

па карактеристичну функцију предиката ограничене егзистенцијалне квантификације можемо записати у облику

$$C_{\exists}(\bar{x}, m) = \div \left(\prod_{i \leq m} (\div (C_R(\bar{x}, i), 1)), 1 \right),$$

па је и он примитивно рекурзиван (на основу тога што су карактеристична функција ограниченог производа и функција монус ПР). □

Примјер 1. Нека предикат $непарно(n)$ важи ако и само ако је n непаран број. Он је ПР јер

$$непарно(n) \Leftrightarrow n \text{ је непаран } \Leftrightarrow (\exists m \leq n)(n = 2 \cdot m + 1).$$

Примјер 2. Слично, за предикат $парно(n)$ имамо

$$парно(n) \Leftrightarrow n \text{ је паран } \Leftrightarrow (\exists m \leq n)(n = 2 \cdot m).$$

Примјер 3. Нека предикат $\div(m, n)$ важи ако и само ако m дијели n без остатка. Како је

$$\div(m, n) \Leftrightarrow (\exists k \leq n)(n = k \cdot m),$$

предикат $\div(m, n)$ је ПР.

Примјер 4. Предикат $prost(n)$ је ПР, јер важи ако и само ако важи $(1 < n) \wedge \left((\forall m \leq n) \left((m = 1) \vee (m = n) \vee (\neg \div(m, n)) \right) \right)$.

Напомена 1. Могли смо такође писати

$$prost(x) = \begin{cases} 1 & \text{ако је } D(x) = 2 \\ 0 & \text{иначе} \end{cases}, \text{ гдје је } D(x) = \sum_{y \leq x} \div(y, x),$$

а затим искористити функцију $\overline{\text{sgn}}$, па бисмо имали $prost(x) = \overline{\text{sgn}}(|D(x) - 2|)$.

ОГРАНИЧЕНА МИНИМИЗАЦИЈА

Дефиниција 2. Нека је $k \in \mathbb{N}$ и R предикат арности $k + 1$. *Ограничена минимизација* за предикат R је функција $f(\bar{x}, n)$ арности $k + 1$, дефинисана са

$$(\mu p \leq n) R(\bar{x}, p) = \begin{cases} \text{најмањи } p \leq n, p \in \mathbb{N}, \\ \text{такав да } R(\bar{x}, p) \text{ важи,} & \text{ако такав постоји} \\ 0 & \text{иначе} \end{cases}$$

Напомена 2. Постоји и оператор неограничене минимизације или само μ -оператор који се дефинише на следећи начин

$$(\mu y) (f(\bar{x}, y) = 0) = \begin{cases} \text{најмањи } z \text{ такав да је } f(\bar{x}, z) = 0 \text{ и} \\ (\forall y < z) f(\bar{x}, y) \text{ је дефинисано,} & \text{ако постоји такво } y \\ \text{недефинисано} & \text{иначе} \end{cases}$$

Напомена 3. С обзиром на претходну дефиницију, μ -оператор се још зове и *оператор претраге*, јер се за дату функцију $f(\bar{x}, y)$ *тражи најмање* y такво да је она нула.

Теорема 3. Нека је k природан број и R примитивно рекурзивни предикат арности $k+1$. Тада је ограничена минимизација за предикат R примитивно рекурзивна функција.

Доказ. Функција

$$h(p, n, \bar{x}) = \begin{cases} p & \text{ако } (\exists i \leq n) R(\bar{x}, i) \\ n+1 & \text{ако } R(\bar{x}, n+1) \wedge \neg(\exists i \leq n) R(\bar{x}, i) \\ 0 & \text{ако није } (\exists i \leq n+1) R(\bar{x}, i) \end{cases}$$

је ПР јер је дефинисана по случају ПР предикатима и функцијама. Примитивном рекурзијом се може дефинисати и функција $(\mu p \leq n) R(\bar{x}, p)$:

$$\begin{aligned} (\mu p \leq n) R(\bar{x}, p) &= 0 \\ (\mu p \leq n+1) R(\bar{x}, p) &= h((\mu p \leq n) R(\bar{x}, p), n, \bar{x}) \end{aligned}$$

Вриједност функције је минимално $p \leq n$ за које важи $R(\bar{x}, p)$, ако такво постоји одн. $n+1$ ако такво p не постоји, а важи $R(\bar{x}, n+1)$, одн. 0 ако ни за једно $p \leq n+1$ није $R(\bar{x}, p)$. Како је h ПР, таква је и функција ограничене минимизације $(\mu p \leq n) R(\bar{x}, p)$. $\square$

Примјер 5. Дефинишимо функцију $p(n)$ као вриједност n -тог простог броја. Посматрајмо функцију $h(n, x) = (\mu x \leq (!n + 1))((n < x) \wedge \text{prost}(x))$. Функцију $p(n)$ можемо дефинисати као

$$p(0) = 2$$

$$p(n + 1) = h(p(n), n), \text{ па је она ПР.}$$

Примјер 6. Нека је $[x]_n =$ степен n -тог простог броја у факторизацији броја x . Она је ПР јер је

$$[x]_n = (\mu y \leq x) \left(\neg \div (p(n)^{y+1}, x) \right)$$

Примјер 7. Функција $duzina(x)$, дефинисана са

$$duzina(x) = \text{редни број најмањег простог броја чији је степен у факторизацији броја } x \text{ једнак } 0,$$

је такође ПР, јер је $duzina(x) = (\mu n \leq x) ([x]_n = 0)$.

Нпр. ако је низ простих бројева дефинисан са $p(0) = 2, p(1) = 3, p(2) = 5, \dots$ тада је $duzina(660) = 3$, јер је $660 = 2^2 \cdot 3 \cdot 5 \cdot 11$, одакле видимо да број 7 има степен једнак 0, па из претходног низа добијамо да је његов редни број 3.

ГЕДЕЛИЗАЦИЈА

Кодирање омогућава придруживање природних бројева објектима, који су у нашем случају функције или програми, у циљу да се испитивање тих објеката сведе на испитивање њихових слика помоћу аритметике. Овакав поступак дозвољава да се функција одн. њена слика одн. код јавља као сопствени аргумент.

Услови:

- не постоје два објекта са истим придруженим бројем,
- број сваког објекта рачуна се у коначном броју корака,
- за дати природан број може се у коначном броју корака провјерити да ли је он број неког објекта и наћи тај објекат, ако постоји.

Ако је $gb : \mathcal{T} \rightarrow \mathbb{N}$ претходни услови заправо значе

- ако је $gb(P_1) = gb(P_2)$ тада је $P_1 = P_2$,
- gb је ефективно израчунљива,
- gb^{-1} је ефективно израчунљива.

Описани поступак кодирања зове се геделизација, а кôд придружен објекту Геделов број. Ако су испуњени наведени услови, тврђења и докази не зависе од начина кодирања.

У даљим одјељцима биће детаљно описан поступак кодирања парцијално рекурзивних функција. У том поступку значајни су прости бројеви и јединственост приказа сваког броја у облику производа степена простих бројева. Од помоћних функција користићемо:

- $p(n)$ n -ти прост број,
- $[x]_n$ степен n -тог простог броја у факторизацији броја x ,
- $duzina(x)$ дужина факторизације броја x .

за које је раније показано да су рекурзивне.

Ако имамо низ бројева $(a_0, a_1, \dots, a_n)$, такав низ кодирамо изразом:

$$gb(a_0, a_1, \dots, a_n) = p(0)^{a_0+1} \cdot p(1)^{a_1+1} \cdot \dots \cdot p(n)^{a_n+1}.$$

Притом усвајамо договор:

- за кодирање броја a_i (i -то мјесто у низу) користимо облик $p(i)^{a_i+1}$,
- за декодирање користимо функцију $(x)_i = \div(1, [x]_i) = [x]_n - 1$,
- $(\forall x)$ x кодира низ дужине $duzina(x)$, а x за које је $duzina(x) = 0$ кодира празну ријеч.

Нпр. за $x = 756 = 2^2 \cdot 3^3 \cdot 7 = p(0)^2 \cdot p(1)^3 \cdot p(3)$, $duzina(756) = 2$, одн. x кодира $((x)_0, (x)_1) = (1, 2)$. Како је $gb(1, 2) = 108$, видимо да различити бројеви могу представљати исти низ, али се различити низови увијек кодирају различитим бројевима.

ИЗРАЧУНЉИВЕ И ПРИМИТИВНО РЕКУРЗИВНЕ ФУНКЦИЈЕ

Када знамо како можемо кодирати ПР функције, могуће је замислити интуитивно израчунљиву тоталну функцију која није примитивно рекурзивна.

Посматрајмо ПР функције и неко њихово набрајање $f_0, f_1, f_2, \dots$. Дефинишимо функцију $g(x) = f_x(x) + 1$. Иако је $g(x)$ тотална и израчунљива, она није ПР. Ако претпоставимо да јесте, тада постоји индекс k за који према дефиницији функције имамо да важи $f_k(k) = g(k) = f_k(k) + 1$, што је контрадикција. Описани поступак назива се дијагонализација или Канторов дијагонални поступак.

Напомена 4 (Опис дијагоналног поступка). Претпоставимо да је низ $\xi_0, \xi_1, \xi_2, \dots$ набрајање неких објеката (функција, скупова природних бројева). Тада можемо конструисати објекат ξ истог типа који се разликује од сваког ξ_n , тако да нам важи да се ξ и ξ_n разликују у n . *Разликовање* зависи од примјене, одн. од врсте објекта, нпр. за функције се ради о домену, или о дефинисаности у некој тачки, док се код скупова говори о припадности.

Примјер 8 (Акерманова функција). Акерманова функција је примјер израчунљиве функције која није примитивно рекурзивна. Она заправо показује да је скуп примитивно рекурзивних функција строги подскуп скупа рекурзивних функција. Носи име по Вилхелму Акерману, који ју је дефинисао 1928. године:

$$A(0, n, k) = n + k$$

$$A(1, n, 0) = 0$$

$$A(2, n, 0) = 1$$

$$A(m + 1, n, 0) = n, \text{ за } m > 1.$$

$$A(m + 1, n, k + 1) = A(m, n, A(m + 1, n, k)), \text{ за } k \geq 0.$$

Ова функција је интуитивно израчунљива, нпр. за њу се може написати програм на неком програмском језику или на Тјуринговој машини. Може се показати да дијагонала Акерманове функције $f(n) = A(n, n, n)$ расте брже од сваке унарне примитивно рекурзивне функције, па да ни Акерманова функција није примитивно рекурзивна.

Слично важи и за функцију дефинисану са

$$A'(0, n) = n + 1$$

$$A'(m + 1, 0) = A'(m, 1)$$

$$A'(m + 1, n + 1) = A'(m, A'(m + 1, n)).$$

Напомена 5. Као што је већ речено, Акерманова функција расте веома брзо. Нпр. $A(4, 2)$ је број са 19729 цифара. Због своје веома дубоке рекурзије, може се користити као тест способности преводиоца да оптимизује рекурзију. Прва таква употреба 1971. године.

Напомена 6. Као што Акерманова функција расте изузетно брзо, тако и њена инверзна функција, у ознаци $\alpha(n)$ расте изузетно споро. Јавља се у изразима за временску сложеност неких алгоритама.