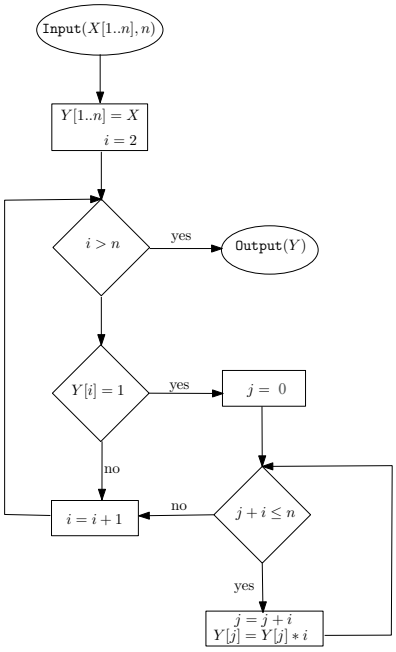
Генерално контролно по СЕП, спец. Информатика, 13.06.21



Задача 1. *Да се докаже, че програмата, представена чрез гораната блок-схема, е частично коректна относно входно условие:*

$$I(X,n) \iff \forall 1 \leq i \leq n(X[i] = 1)$$

и изходно условие:

$$O(X,n,Y) \iff \forall 1 \leq i \leq n(Y[i] = Y[Y[i]]).$$

Задача 2. *Нека* $\Gamma : \mathcal{F}^1 \longrightarrow \mathcal{F}^1$ *е операторът, зададен чрез равенството:*

$$\Gamma(f)(x) \simeq \begin{cases} x+1, & \text{ако } x < 2 \\ \sum_{i=f(x-2)}^{f(x-1)} f(i), & \text{ако } x \geq 2. \end{cases}$$

1. *Да се докаже, че* Γ *е компактен.*
2. *Да се докаже, че ако* f_Γ *е най-малката неподвижна точка на оператора* Γ*, то:*

$$\forall x \in \mathbb{N}(!f_\Gamma(x) \implies f_\Gamma(x) \text{ е число от редицата на Фибоначи}).$$

Забележка: Има се предвид следната дефиниция на редицата $\{a_n\}_{n\in\mathbb{N}}$ на Фибоначи:

$$a_0 = 0, \quad a_1 = 1, \quad a_{n+2} = a_{n+1} + a_n.$$

Задача 3. *Нека* R *е следната рекурсивна програма:*

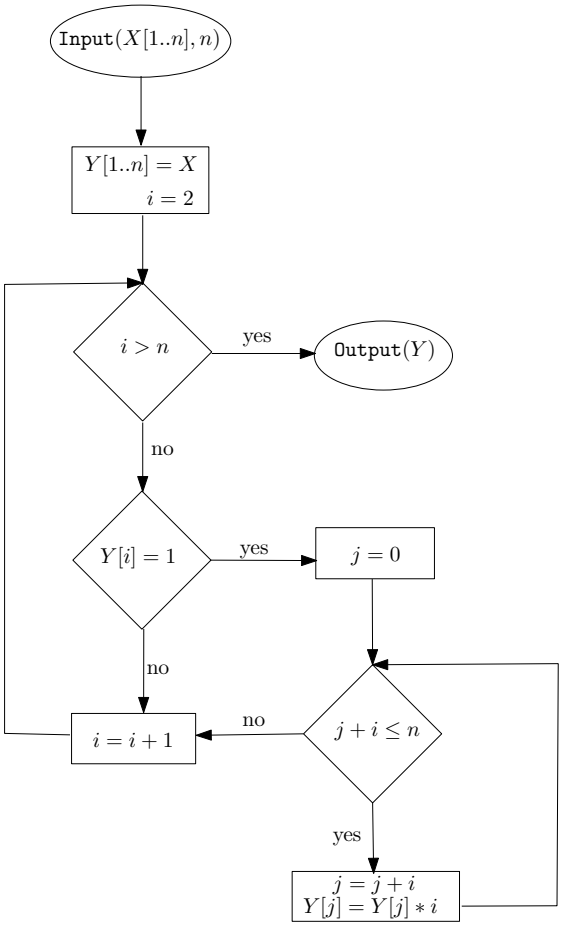
$F(X,Y,Y)$ `where`
$F(X,Y,Z) =$ `if` $Y > X$ `then` 0 `else` $F(X, Y * Z, Z) + G(X,Y)$
$G(X,Y) =$ `if` $X < Y$ `then` 0 `else` $1 + G(X - Y, Y)$

Да се докаже, че:

$$\forall n,p \in \mathbb{N}((!D_V(R)(n,p) \text{ и } p \text{ е просто }) \implies p^{D_V(R)(n,p)} \mid n! \text{ и } p^{D_V(R)(n,p)+1} \nmid n!).$$

По-долу следват решенията:

Решения на задачите:



Фигура 1:

Задача 1. Да се докаже, че програмата, представена чрез блок-схемата на фигура 1 е частично коректна, относно входно условие:

$$I(X, n) \iff \forall 1 \leq i \leq n(X[i] = 1)$$

и изходно условие:

$$O(X, n, Y) \iff \forall 1 \leq i \leq n(Y[i] = Y[Y[i]]).$$

Решение. *Самото* решение е технически просто, но преди да пристъпим към него, трябва да си отговорим на няколко въпроса в контекста на входното условие.

1. Какво прави тази програма?
2. Какво общо има това с изходното условие?
3. Как го прави?

Да започнем с първия въпрос. Какво прави тази програма? Първоначално всички елементи на Y са единици и лесно се вижда, че те само могат на нараства. Да видим кога това се

случва. Би трябвало да е ясно, че вътрешният цикъл обхожда точно онези индекси j, които са кратни на i. Така че, ако $Y[j]$ се увеличи, тоест се умножи по нещо, то това ще бъде с делител на j. Сега, ако j има делител по-малък от j и по-голям от 1, то $Y[j]$ ще нарасне преди външния цикъл да увеличи i на j. С други думи, ако j не е просто, то тестът $Y[j] = 1$ ще е отрицателен. Обратно, ако j е просто, то $Y[j]$ няма да нарасне преди външния цикъл да увеличи i до j и съответно тестът $Y[j] = 1$ ще бъде положителен[1].

Като знаем горното разсъждение, вече може да разгадаем и вътрешния цикъл. Поточно, $Y[j]$ ще бъде увеличавано точно на онези стъпки i, за които i е прост делител на j. Следователно, ако $j = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ е каноничното разлагане на j, за $Y[j]$ в края на изпълнението на програмата очакваме да бъде:

$$Y[j] = \prod_{s=1}^{k} p_s,$$

или казано с думи, $Y[j]$ е произведението на простите делители на j.

С това общо взето разбрахме какво прави програмата и сме готови да видим и отговора на втория въпрос. Какво общо има $Y[j] = \prod_{s=1}^{k} p_s$ с изходното условие? Ако си спомним, че $j = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, то $Y[j]$ и j имат едни и същи прости делители и следователно от интерпретацията на горното условие получаваме, че $Y[Y[j]] = Y[j]$.

На идейно ниво, горните разсъждения решават задачата. Останалото е въпрос на техника, да отговорим на въпроса: Как програмата прави това, което видяхме? Тук отговорът също не е сложен, защото циклите са монотонни, а ние вече разгадахме кога се задейства вътрешния цикъл. По-конкретно:

1. преди стъпка i на външния цикъл, всяко $Y[\ell]$ е произведението на простите делители на ℓ, които са по-малки от i:

$$Y[\ell] = \prod_{p<i \text{ и } p \text{ просто и } p|\ell} p.$$

2. преди стъпка j на вътрешния цикъл горното условие се изфинява като, разбира се трябва да отбележим, че i е просто и:

$$Y[\ell] = \begin{cases} \prod_{p\leq i \text{ и } p \text{ просто и } p|\ell} p \text{ ако } \ell \leq j \\ \prod_{p<i \text{ и } p \text{ просто и } p|\ell} p \text{ ако } \ell > j. \end{cases}$$

Сега сме готови да пристъпим към *самото* решение, което представлява обличането на горните разсъждения във формализма на метода на индуктивните твърдения.

Да въведем следното означение:

$$P(Y,i,\ell) \iff Y[\ell] = \prod_{p<i \text{ и } p \text{ просто и } p|\ell} p.$$

Сега дефинираме по един инвариант за всеки от двата цикъла:

1. за условието $i > n$ дефинираме $L(X,n,Y,i)$:

$$i \leq n+1 \& \forall 1 \leq \ell \leq n(P(Y,i,\ell))$$

[1] Всъщност, по-опитните сигурно ще разпознаят приликата между тази програма и решетото на Ератостен.

2. за условието $j + i \leq n$ дефинираме $M(X, n, Y, i, j)$:

$$\begin{aligned} i \leq n \quad \& \quad (i \text{ е просто }) \quad \& \quad i|j \quad \& \quad j \leq n + i \quad \& \\ \forall 1 \leq \ell \leq \max(j, n)(P(Y, i+1, \ell)) \quad \& \quad \forall j < \ell \leq n(P(Y, i, \ell)). \end{aligned}$$

Преминаваме към верификацията, като предполагаме[2], че $n \geq 1$:

1. $I(X, n) \& i = 2 \& Y = X \Rightarrow L(X, n, Y, i)$. Тъй като няма прости числа по-малки от 2, то $P(Y, 2, \ell)$ е вярно, защото $Y[\ell] = X[\ell] = 1$. Също така, доколкото $n \geq 1$, то $i = 2 \leq n+1$. С това проверихме, че $I(X, n) \& i = 2 \& Y = X \Rightarrow L(X, n, Y, i)$.

2. $L(X, n, Y, i) \& i \not> n \Rightarrow O(X, n, Y)$. Тъй като $L(X, n, Y, i)$, то $i \leq n + 1$. Сега от $i \not> n$ получаваме, че $i = n + 1$. Сега е ясно, че ако $\ell \leq n$ и $p|\ell$, то $p < i + 1 = n + 1$. Поради това:

$$P(Y, i, \ell) \iff Y[\ell] = \prod_{p<i=n+1 \text{ и } p \text{ просто и } p|\ell} p \iff Y[\ell] = \prod_{p \text{ просто и } p|\ell} p.$$

   От $L(X, n, Y, i)$, $P(Y, i, \ell)$ е вярно за всяко $\ell \leq n$. Следователно $Y[\ell]$ има същите прости делители като ℓ и очевидно $1 \leq Y[\ell] \leq \ell$. Следователно от $L(X, n, Y, i)$ получаваме, че и $P(Y, i, Y[\ell])$ е вярно, тоест:

$$Y[Y[\ell]] = \prod_{p<i=n+1 \text{ и } p \text{ просто и } p|Y[\ell]} p \iff Y[Y[\ell]] = \prod_{p \text{ просто и } p|Y[\ell]} p,$$

   но тъй като простите делители на $Y[\ell]$ и ℓ са едни и същи, то последното е еквивалентно на:

$$Y[Y[\ell]] = \prod_{p \text{ просто и } p|Y[\ell]} p = \prod_{p \text{ просто и } p|\ell} p = Y[\ell].$$

3. $L(X, n, Y, i) \& i \not> n \& Y[i] \& i' = i + 1 \neq 1 \Rightarrow L(X, n, Y, i')$. Първо, тъй като $i \not> n$, то $i \leq n$ и следователно $i' = i + 1 \leq n + 1$. После, тъй като $Y[i] \neq 1$, то от $P(Y, i, i)$ имаме, че i има прост делител по-малък от i, тоест i не е просто. Следователно простите числа по-малки от i са точно простите числа по-малки от $i + 1 = i'$. Това означава, че:

$$\begin{aligned} P(Y, i, \ell) \iff Y[\ell] = \prod_{p<i \text{ и } p \text{ просто и } p|\ell} p \iff Y[\ell] = \prod_{p<i+1 \text{ и } p \text{ просто и } p|\ell} p \\ \iff P(Y, i+1, \ell) = P(Y, i', \ell). \end{aligned}$$

   Оттук директно получаваме, че $L(X, n, Y, i')$.

4. $L(X, n, Y, i) \& i \not> n \& Y[i] = 1 \& j = 0 \Rightarrow M(X, n, Y, i, j)$. Подред:

   (а) $i \not> n$, следователно $i \leq n$.

   (б) $Y[i] = 1$, тогава от $P(Y, i, i)$, получаваме, че $Y[i]$ няма прости делители по-малки от i, следователно i е просто.

   (в) $j = 0$, $i \leq n$, следователно $0 + i \leq n + i$.

   (г) $i|0$, следователно $i|j$.

   (д) $j = 0$, така че $\forall 1 \leq \ell \leq j(P(Y, i + 1, \ell))$ е изпълнено по тривиални съображения.

[2] Случаят $n = 0$ е тривиален. При него изходното условие е изпълнено по тривиални причини.

(е) $L(X,n,Y,i)$ е в сила, така че $\forall 1 \leq \ell \leq n(P(Y,i,\ell))$, което е еквивалентно на $\forall 0 < \ell \leq n(P(Y,i,\ell))$. С оглед на това, че $j = 0$, получаваме и последното условие от $M(X,n,Y,i,j) = M(X,n,Y,i,0)$.

5. $M(X,n,Y,i,j)\&j + i \leq n\&j' = j + i\&Y'[j'] = Y[j'] * i \Rightarrow M(X,n,Y',i,j')$. Отново подред:

   (а) $i \leq n$, следва от $M(X,n,Y,i,j)$.

   (б) i е просто, следва от $M(X,n,Y,i,j)$.

   (в) $i|j$ и $j' = i + j$, следователно $i|j'$.

   (г) $i + j \leq n$, следователно $j' \leq n$, откъдето $i + j' \leq n + i$.

   (д) Това, че $P(Y',i+1,\ell)$ е изпълнено за $\ell \leq j$ следва от $M(X,n,Y,i,j)$. Сега, ако $j < \ell < i+j = j'$, тъй като $i|j$, то $i \not| \ell$ и следователно $P(Y',i+1,\ell) \iff P(Y,i,\ell)$. Тъй като $P(Y,i,\ell)$ е вярно от $M(X,n,Y,i,j)$, то вярно е и $P(Y,i+1,\ell)$. Накрая $P(Y',i+1,j')$ също е вярно, защото:

   $$P(Y,i,j') \Rightarrow Y'[j'] = Y[j'] * i = i \prod_{p<i \text{ и } p \text{ просто и } p|j'} p = \prod_{p \leq i \text{ и } p \text{ просто и } p|j'} p \Rightarrow P(Y',i+1,j').$$

   Тук използвахме, че i е просто.

   (е) За $\ell > j'$, очевидно $P(Y,i,\ell) \iff P(Y',i,\ell)$. Следователно $M(X,n,Y',i,j')$.

6. $M(X,n,Y,i,j)\&j + i \not\leq n\&i' = i + 1 \Rightarrow L(X,n,Y,i')$. Тъй като $i \leq n$, то $i + 1 \leq n + 1$. Сега за всяко $\ell \leq \max(j,n)$ имаме, че:

   $$P(Y,i+1,\ell), \text{ тоест } P(Y,i',\ell).$$

   Накрая, ако $n \geq \ell > j$, то тъй като $j + i > n$ и $i|j$, то ℓ не се дели на i и поради това:

   $$P(Y,i,\ell) \iff P(Y,i+1,\ell), \text{ което е същото като } P(Y,i',\ell).$$

   С това и тази стъпка е завършена, а с това и доказателството.

□

Задача 2. Нека $\Gamma\colon\ \mathcal{F}_1 \longrightarrow \mathcal{F}_1$ е операторът, зададен чрез равенството:

$$\Gamma(f)(x) \ \simeq \ \begin{cases} x+1, & \text{ако } \ x<2 \\ \sum_{i=f(x-2)}^{f(x-1)} \ f(i), & \text{ако } \ x \geq 2. \end{cases}$$

1) Да се докаже, че Γ е компактен.

2) Да се докаже, че ако f_Γ е най-малката неподвижна точка на оператора Γ, то:

$$\forall x \in \mathbb{N}\ (!f_\Gamma(x) \implies f_\Gamma(x) \text{ е число от редицата на Фибоначи}).$$

Забележка: Има се предвид следната дефиниция на редицата $\{a_n\}_n$ на Фибоначи:

$$a_0 = 0, \quad a_1 = 1$$
$$a_{n+2} = a_{n+1} + a_n.$$

Решение. Дефиницията на оператора Γ се разбира така:

$$\Gamma(f)(x) \simeq \begin{cases} x+1, & \text{ако } \ x<2 \\ \sum_{i=f(x-2)}^{f(x-1)} \ f(i), & \text{ако } \ x \geq 2 \ \& \ !f(x-2) \ \& \ !f(x-1) \ \& \ f(x-2) \leq f(x-1) \\ \neg!, & \text{в останалите случаи.} \end{cases}$$

1) Да покажем, че този оператор е компактен. Най-напред ще съобразим, че Γ е монотонен. За целта да вземем две функции f и g от $\mathcal{F}_1$, такива, че $f \subseteq g$. Трябва да покажем, че $\Gamma(f) \subseteq \Gamma(g)$.

Наистина, нека $x, y \in \mathbb{N}$ са такива че $\Gamma(f)(x) \simeq y$. Искаме да покажем, че и $\Gamma(g)(x) \simeq y$.

1 сл. $x < 2$. Тогава $\Gamma(f)(x) \overset{\text{деф } \Gamma}{=} x+1 = y$, така че и $\Gamma(g)(x) = x+1 = y$.

2 сл. $x \geq 2$. Ние приехме, че $\Gamma(f)(x) \simeq y$, което съгласно дефиницията на Γ означава, че $!f(x-2)\ \&\ !f(x-1)\ \&\ f(x-2) \leq f(x-1)$ и

$$\sum_{i=f(x-2)}^{f(x-1)} f(i) \simeq \ y.$$

В частност, $f(i)$ ще е дефинирана за всяко $i = f(x-2), \ldots, f(x-1)$. Понеже $f \subseteq g$, то и $g(i)$ ще е дефинирана за всяко такова i и освен това

$$g(i) \simeq f(i) \ \text{ за всяко } \ i = f(x-2), \ \ldots \ , f(x-1).$$

Разбира се, ще имаме също, че $g(x-2) \simeq f(x-2)$ и $g(x-1) \simeq f(x-1)$. Лесно се вижда, че в такъв случай $\Gamma(g)(x) \simeq \sum_{i=g(x-2)}^{g(x-1)} g(i)$, откъдето

$$\Gamma(g)(x) \ \simeq \sum_{i=g(x-2)}^{g(x-1)} g(i) \simeq \sum_{i=f(x-2)}^{f(x-1)} f(i) \simeq \ y.$$

Тъй като x и y бяха произволни, от казаното по-горе можем да заключим, че $\Gamma(f) \subseteq \Gamma(g)$.

Сега нека $\Gamma(f)(x) \simeq y$ за някои x и y. Ще покажем, че

$$\exists\theta\ (\theta \subseteq f\ \&\ \theta \text{ е крайна } \&\ \Gamma(\theta)(x) \simeq y). \tag{1}$$

Отново разглеждаме двата случая от дефиницията на Γ:
1 сл. $x < 2$. Тук $\Gamma(f)(x)$ не зависи от f, така че за $\theta = \emptyset^{(1)}$ условието (1) очевидно ще е в сила.
2 сл. $x \geq 2$. По-горе видяхме, че $\Gamma(f)(x) \simeq y$ в този случай влече $!f(x-2)$ & $!f(x-1)$ & $f(x-2) \leq f(x-1)$ и $\sum_{i=f(x-2)}^{f(x-1)} f(i) \simeq y$.
Да означим $k = f(x-2)$, $n = f(x-1)$ и да положим

$$\theta := f \restriction \{x-2, x-1, k, k+1, \ldots, n\}.$$

Ясно е, че тази θ е крайна функция и $\theta \subseteq f$. Понеже f е дефинирана във всички точки от множеството $\{x-2, x-1, k, k+1, \ldots, n\}$, то и θ ще е дефинирана в тези точки и ще има същите стойности като f. Но тогава

$$\Gamma(\theta)(x) \overset{\text{деф } \Gamma}{\simeq} \sum_{i=\theta(x-2)}^{\theta(x-1)} \theta(i) \simeq \sum_{i=f(x-2)}^{f(x-1)} f(i) \simeq y.$$

Така проверихме, че условието (1) е изпълнено за произволни x и y, което завършва доказателството за компактността на оператора Γ.

2) Нека f е произволна неподвижна точка на Γ, т.е. за нея е изпълнено:

$$f(x) \simeq \begin{cases} x+1, & \text{ако } x < 2 \\ \sum_{i=f(x-2)}^{f(x-1)} f(i), & \text{ако } x \geq 2. \end{cases} \tag{2}$$

Виждаме, че при $x = 2$ за тази f ще имаме:

$$f(2) \overset{(2)}{\simeq} \Gamma(f)(2) \overset{\text{деф } \Gamma}{\simeq} \sum_{i=f(0)}^{f(1)} f(i) \overset{(2)}{\simeq} \sum_{i=1}^{2} f(i) \simeq f(1) + f(2).$$

С други думи, за f трябва да е изпълнено $f(2) \simeq f(1)+f(2)$. Тази "лоша" рекурсия ни подсказва, че най-вероятно $f_\Gamma(2)$ няма да е дефинирана, а оттук няма да са дефинирани и $f_\Gamma(x)$ за всяко $x \geq 2$. Но да се убедим формално, че това е така, като приложим теоремата на Кнастер-Тарски, според която

$$f_\Gamma = \bigcup_n \Gamma^n(\emptyset^{(1)}).$$

Да означим $f_n := \Gamma^n(\emptyset^{(1)})$. Като използваме рекурентната схема

$$\begin{aligned} f_0 &= \emptyset^{(1)} \\ f_{n+1} &= \Gamma(f_n), \end{aligned}$$

съобразяваме, че

$$f_1(x) \simeq \Gamma(\emptyset^{(1)})(x) \overset{\text{деф } \Gamma}{\simeq} \begin{cases} x+1, & \text{ако } x < 2 \\ \neg!, & \text{ако } x \geq 2. \end{cases} \tag{3}$$

Оттук за $f_2 = \Gamma(f_1)$ ще получим:

$$f_2(x) \simeq \begin{cases} x+1, & \text{ако } x < 2 \\ \sum_{i=f_1(x-2)}^{f_1(x-1)} f_1(i), & \text{ако } x \geq 2. \end{cases} \overset{(3)}{\simeq} \begin{cases} x+1, & \text{ако } x < 2 \\ \sum_{i=1}^{2} f_1(i), & \text{ако } x = 2 \\ \neg!, & \text{ако } x > 2 \end{cases} \overset{(3)}{\simeq} \begin{cases} x+1, & \text{ако } x < 2 \\ f_1(1) + \underbrace{f_1(2)}_{\neg!}, & \text{ако } x = 2 \\ \neg!, & \text{ако } x > 2, \end{cases}$$

или начисто:

$$f_2(x) \simeq \begin{cases} x+1, & \text{ако } x < 2 \\ \neg!, & \text{ако } x \geq 2. \end{cases}$$

Получихме че двете апроксимации f_1 и f_2 са равни, откъдето, както знаем, следва, че $f_\Gamma = f_1$, т.е.

$$f_\Gamma(x) \simeq \begin{cases} x+1, & \text{ако } x < 2 \\ \neg!, & \text{ако } x \geq 2. \end{cases}$$

Но тази функция очевидно удовлетворява условието от подточка **2)**. $\square$

Задача 3. Нека R е следната рекурсивна програма:

$F(X,Y,Y)$, `where`
$F(X,Y,Z) =$ `if` $Y > X$ `then` 0 `else` $F(X,Y*Z,Z) + G(X,Y)$
$G(X,Y) =$ `if` $X < Y$ `then` 0 `else` $1 + G(X-Y,Y)$

Да се докаже, че:

$$\forall n,p \in \mathbb{N}(!D_V(R)(n,p) \text{ и } p \text{ просто } \Rightarrow p^{D_V(R)(n,p)} | n! \text{ и } p^{D_V(R)(n,p)+1} \not| n!).$$

Решение. Отново процедираме като в първата задача, тоест първо ще анализираме задачата и ще я решим на идейно ниво, а после ще изложим формалната верификация. Основните въпроси са същите:

1. Какво прави програмата?
2. Какво общо има това с условието, което трябва да верифицираме?
3. Как програмата го прави?

В тази ситуация, за разлика от горната задача, първият и последният въпрос са по-прозаични. Това че втората функция, $G(X,Y)$, не съдържа косвена рекурсия, ни помага да я "разгадаем" сравнително лесно. Тя добавя толкова единички, колкото пъти Y се съдържа в X. С това може да си мислим за функцията[3]:

$$g(x,y) \simeq \left\lfloor \frac{x}{y} \right\rfloor .$$

Знаейки, какво прави функцията G, функцията F също става достъпна. Тя събира стойности(те) на $g(x,yz^k)$:

$$f(x,y,z) \simeq \left\lfloor \frac{x}{y} \right\rfloor + \left\lfloor \frac{x}{yz^2} \right\rfloor + \ldots \left\lfloor \frac{x}{yz^k} \right\rfloor \ldots .$$

Човек, разбира се, си задава въпрос докога събираме. Програмата дава ясен отговор на този въпрос: *докато* $yz^k \leq x$. От математическа гледна точка, обаче, това не е толкова важно, защото, ако $y \neq 0$ и $z > 1$, то след като настъпи условието $yz^k > x$, всички събираеми $\left\lfloor \frac{x}{yz^k} \right\rfloor$ стават нула, тоест безкрайната сума не представлява проблем[4].

С горните разсъждение, задачата се свежда до следното:

$$\text{ако } M = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \text{ то } p^M | n! \text{ и } p^{M+1} \not| n!.$$

Казано с думи, M е степента на p в каноничното разлагане на $n!$. Може да разсъждаваме така:

1. Нека с $\alpha(k)$ означим степента на p в каноничното разлагане на k. ($\alpha(k) = 0$, ако p не дели k.)
2. Тогава искаме да покажем, че $M = \alpha(n!)$.

[3] По-наблюдателните сигурно ще забележат, че горното неформално разсъждение, макар и вярно, крие "клопка". Поради това дефинираната функция не е тотална!

[4] Разбира се, такива разсъждения може да правим в мета езика и ще бъдем далеч по-прецизни, когато стигнем до самото решение.

3. Но тъй като $n! = 1.2.\ldots.n$, то:

$$\alpha(n!) = \alpha(1) + \alpha(2) + \ldots \alpha(n) = \sum_{k=1}^{n} \alpha(k).$$

4. Сега да забележим, че $\alpha(k) \geq \alpha$, точно когато$p^{\alpha}|k$. Но числата, които са по-малки или равни на n и се делят на p^{α} са точно:

$$\left\lfloor \frac{n}{p^{\alpha}} \right\rfloor.$$

5. Сега "броим":

$$\alpha(n!) = \sum_{k=1}^{n} \alpha(k) = \sum_{k=1}^{n} \sum_{\alpha=1}^{\alpha(k)} 1 = \sum_{\alpha=1}^{\infty} \sum_{\substack{1 \leq k \leq n \\ \alpha(k) \geq \alpha}} 1 = \sum_{\alpha=1}^{\infty} \left\lfloor \frac{n}{p^{\alpha}} \right\rfloor = M.$$

Поради горните разсъждения, остава да покажем, че за $D_V(R)$ е в сила, че:

$$\forall n, m \in \mathbb{N}(!D_V(R)(n,m) \text{ и } m > 1 \Rightarrow D_V(R)(n,m) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{m^k} \right\rfloor).$$

Може да направим това, като формализираме горните разсъждения например използвайки индукционното правило на Скот:

1. За всяко от уравненията в програмата R дефинираме по един оператор, съответно:

$$\Gamma : \mathcal{F}_3 \times \mathcal{F}_2 \to \mathcal{F}_3 \quad \text{и} \quad \Delta : \mathcal{F}_3 \times \mathcal{F}_2 \to \mathcal{F}_2$$

$$\Gamma(f,g)(x,y,z) \simeq \begin{cases} 0, \text{ ако } y > x \\ f(x,yz,z) + g(x,y), \text{ иначе,} \end{cases} \qquad \Delta(f,g)(x,y) \simeq \begin{cases} 0, \text{ ако } x < y \\ g(x-y,y), \text{ иначе.} \end{cases}$$

2. Знаем, че $(\Gamma, \Delta) : \mathcal{F}_3 \times \mathcal{F}_2 \to \mathcal{F}_3 \times \mathcal{F}_2$ е непрекъснат оператор от областта на Скот $(\mathcal{F}_3 \times \mathcal{F}_2, \subseteq, (\emptyset^{(3)}, \emptyset^{(2)}))$ и съответно от теоремата на Кнастер-Тарски има най-малка неподвижна точка (f^*, g^*). При това:

$$D_V(R)(n,m) \simeq f^*(n,m,m).$$

3. Сега за всяко от двете наблюдения, които направихме в началото, формулираме по едно свойство от тип частична коректност, като спокойно може да ги формулираме така, че да избегнем, ако желаем, случаите при $m = 0, 1$:

$$P : \mathcal{F}_3 \times \mathcal{F}_2 \to \{true, false\} \text{ и } Q : \mathcal{F}_3 \times \mathcal{F}_2 \to \{true, false\}$$

$$P(f,g) \leftrightarrow \forall n, m, r \in \mathbb{N}(!f(n,m,r) \& m > 1 \& r > 1 \Rightarrow f(n,m,r) = \sum_{k=0}^{\infty} \left\lfloor \frac{n}{mr^k} \right\rfloor)$$

$$Q(f,g) \leftrightarrow \forall n, m \in \mathbb{N}(!g(n,m) \& m > 0 \Rightarrow g(n,m) = \left\lfloor \frac{n}{m} \right\rfloor).$$

4. Тъй като P и Q са от тип частична коректност, то те са непрекъснати. Следователно и тяхната конюнкция:

$$R(f,g) \leftrightarrow P(f,g) \& Q(f,g)$$

също е непрекъснато.

5. Ще докажем, че (Γ, Δ) и R удовлетворяват предпоставките на правилото на Скот:

   (а) (Γ, Δ) е непрекъснат оператор в $(\mathcal{F}_3 \times \mathcal{F}_2, \subseteq, (\emptyset^{(3)}, \emptyset^{(2)}))$. От общи съображения, вж. по-горе.

   (б) R е непрекъснато, вж. по-горе.

   (в) $R(\emptyset^{(2)}, \emptyset^{(3)})$. Тъй като P и Q са от тип частична коректност, то $P(\emptyset^{(2)}, \emptyset^{(3)})$ и $Q(\emptyset^{(2)}, \emptyset^{(3)})$ са удовлетворени по тривиални съображения. Следователно $R(\emptyset^{(2)}, \emptyset^{(3)}) = true$.

   (г) $R(f, g) \Rightarrow R((\Gamma, \Delta)(f, g))$. Нека $R(f, g)$ и $f' = \Gamma(f, g)$ и $g' = \Delta(f, g)$. Ще покажем, че и $R(f', g')$.

      i. $P(f', g')$. Нека $f'(n, m, r)$ е дефинирано и $m, r > 1$. Тогава:

         - $n < m$. Следователно, от една страна, $f'(n, m, r) = \Gamma(f, g)(n, m, r) = 0$. От друга, $n < m$ и тъй като $r > 1$, то и $n < mr^k$ за $k \geq 0$. Следователно $\left\lfloor \frac{n}{mr^k} \right\rfloor = 0$ за $k \geq 0$, откъдето и:

$$f'(n, m, r) = 0 = \sum_{k=0}^{\infty} \left\lfloor \frac{n}{mr^k} \right\rfloor.$$

         - $n \geq m$. Тогава:

$$f'(n, m, r) = \Gamma(f, g)(n, m, r) \simeq f(n, m * r, r) + g(n, m).$$

           Тъй като лявата страна е дефинирана, то дефинирана е и дясната страна. Следователно $!f(n, m * r, r)$ и $!g(n, m)$. Тъй като $m, r > 1$, то $m * r > 1$ и от $P(f, g)$ заключаваме, че:

$$f(n, mr, r) = \sum_{k=0}^{\infty} \left\lfloor \frac{n}{mrr^k} \right\rfloor = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{mr^k} \right\rfloor.$$

           Също така от това, че $!g(n, m)$ и $m > 1$, то от $Q(f, g)$ получаваме, че:

$$g(n, m) = \left\lfloor \frac{n}{m} \right\rfloor.$$

           Сега е ясно, че:

$$f'(n, m, r) = f(n, m * r, r) + g(n, m) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{mr^k} \right\rfloor + \left\lfloor \frac{n}{m} \right\rfloor = \sum_{k=0}^{\infty} \left\lfloor \frac{n}{mr^k} \right\rfloor.$$

         С това $P(f', g')$ е доказано.

      ii. $Q(f', g')$. Нека $g'(n, m)$ е дефинирано и $m > 1$. Тогава:

         - $n < m$. Тогава от една страна $g'(n, m) = \Delta(f, g)(n, m) = 0$. От друга, тъй като $n < m$, то $\left\lfloor \frac{n}{m} \right\rfloor = 0$.
         - $n \geq m$. Тогава:

$$g'(n, m) = \Delta(f, g)(n, m) \simeq g(n - m, m) + 1.$$

           Тъй като лявата страна е дефинирана, то има смисъл и дясната страна. Тъй като $m > 1$, то от $Q(f, g)$ получаваме, че:

$$g(n - m, m) = \left\lfloor \frac{n - m}{m} \right\rfloor = \left\lfloor \frac{n}{m} - 1 \right\rfloor = \left\lfloor \frac{n}{m} \right\rfloor - 1.$$

Сега е ясно, че:

$$g'(n,m) = \Delta(f,g)(n,m) \simeq g(n-m,m)+1 = \left\lfloor \frac{n}{m} \right\rfloor - 1 + 1 = \left\lfloor \frac{n}{m} \right\rfloor .$$

С това установихме, че $Q(f',g')$ също е вярно.

(д) От правилото на Скот заключаваме, че $R(f^*,g^*)$, където (f^*,g^*) беше най-малката неподвижна точка на (Γ,Δ).

6. За нас е важно, че $P(f^*,g^*)$, тоест:

$$\forall n,m,r \in \mathbb{N}(!f^*(n,m,r) \& m>1 \& r>1 \Rightarrow f^*(n,m,r) = \sum_{k=0}^{\infty} \left\lfloor \frac{n}{mr^k} \right\rfloor .$$

Оттук получаваме, че ако p е просто, в частност $p>1$, и $!f^*(n,p,p)$, то:

$$f^*(n,m,r) = \sum_{k=0}^{\infty} \left\lfloor \frac{n}{p.p^k} \right\rfloor = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

С това доказателството е завършено, защото последното означава, че:

$$\forall n,p \in \mathbb{N}(!D_V(R)(n,p) \& p \text{ е просто} \Rightarrow D_V(R)(n,p) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor).$$

□