

Algoritmusok tervezése és elemzése

2012. 03. 14.

Dijkstra-féle leggyengébbelőfeltétel-kalkulus (weakest precondition):

$[P] C [Q] \ll \Rightarrow P \exists \text{wp}(C, Q)$, ahol $\exists$ az implikációt jelenti és $\text{wp}(C, Q)$ egy formula.

$\text{wp}(C, \perp) = \perp$ (A csoda kizárásának elve)

Műveleti tulajdonságok:

$\text{wp}(\text{skip}, Q) = Q$

$\text{wp}(X:=E, Q) = Q_E^X$

$\text{wp}(C_1; C_2, Q) = \text{wp}(C_1, \text{wp}(C_2, Q))$ (kompozíciós szabály)

$\text{wp}(\text{while } B \text{ do } C \text{ od}, Q) = \exists i \geq 0. P_i$, ahol P_i annak leggyengébb előfeltétele, amely mellett a ciklus pontosan i lépés után befejeződik és teljesül Q .

$P_0 = \neg B \wedge Q$

$P_{i+1} = B \wedge \text{wp}(C, P_i), i \geq 0$

Feladatmegoldás:

$\text{wp}(Y:=0; \text{while } X>0 \text{ do } X:=X-1; Y:=Y+2X+1 \text{ od}, Y=Z) = (\text{kompozíciós szabályt alkalmazva}) =$
 $= \text{wp}(Y:=0, \text{wp}(\text{while } X>0 \text{ do } X:=X-1; Y:=Y+2X+1 \text{ od}, Y=Z)) = \exists i \geq 0. P_i = *^1$

A kapott wp formulán belül ott található egy **ciklus wp**-je, amelyet a műveleti tulajdonságok alapján meg kell oldalnunk. Ezért az eredmény megoldása előtt meg kell határoznunk a kékkel kiemelt formula eredményét. Ahogy régen, most is C jelöli a ciklusmagot, illetve a wp második paramétere Q -t.

$P_0 = X \leq 0 \wedge Y=Z$

$P_1 = X>0 \wedge \text{wp}(C, X \leq 0 \wedge Y=Z) = X>0 \wedge \text{wp}(X:=X-1; Y:=Y+2X+1, X \leq 0 \wedge Y=Z) = (\text{komp. szabály}) =$
 $= X>0 \wedge \text{wp}(X:=X-1; \text{wp}(Y:=Y+2X+1, X \leq 0 \wedge Y=Z)) = *^2$

A kékkel kiemelt wp egy **értékadást** jelöl. A formula egyszerűsítése érdekében be kell helyettesítenünk a wp első paraméterét a második paraméterként megjelenő formulába. Azaz a kékkel jelölt részt leegyszerűsítjük a következőre: $X \leq 0 \wedge Y+2X+1=Z$

$*^2 = X>0 \wedge \text{wp}(X:=X-1; X \leq 0 \wedge Y+2X+1=Z) = X>0 \wedge (X-1) \leq 0 \wedge Y+2(X-1)+1=Z = *^3$

Ebben a lépésben ismételten egy értékadással egyszerűsítettük a formulát. Mint látható, már nem tudunk különösebb műveletet kifejteni, azonban a formula egyszerűsítésére talán még van lehetőségünk. Próbáljuk először egyszerűbb alakban felírni, hogy X értéke mi lehet. Az $(X-1) \leq 0$ formulát átírhatjuk úgy, hogy $X \leq 1$. Azonban X -re van egy másik kikötés és, miszerint $X>0$. Mivel X csak egész szám lehet, így logikusan következik, hogy $X=1$. Ha X -et behelyettesítjük a formula többi részébe, akkor $Y+2(X-1)+1=Z$ -ből $Y+1=Z$ lesz.

$*^3 = X=1 \wedge Y+1=Z$ (ez lesz P_1)

$P_2 = X>0 \wedge \text{wp}(C, X=1 \wedge Y+1=Z) = X>0 \wedge \text{wp}(X:=X-1; Y:=Y+2X+1, X=1 \wedge Y+1=Z) = (\text{komp. szab.}) =$
 $= X>0 \wedge \text{wp}(X:=X-1, \text{wp}(Y:=Y+2X+1, X=1 \wedge Y+1=Z)) = (\text{értékadás szabály}) =$

$$= X > 0 \wedge \text{wp}(X := X - 1, X = 1 \wedge (Y + 2X + 1) + 1 = Z) = X > 0 \wedge \text{wp}(X := X - 1, X = 1 \wedge Y + 4 = Z) = *^4$$

A fenti műveletnél is látható, hogy érdemes a lehető leghamarabb elvégezni az egyszerűsítéseket, mert később könnyebb lesz velük számolni. Jelen esetben láthatjuk, hogy a wp második paraméterén belül (a kékkel jelölt rész) a formulában szerepel egy $X=1$ tag. Ha ezt behelyettesítjük az $(Y+2X+1)+1=Z$ formulába, akkor $Y+4=Z$ -t kapunk.

$$*^4 = X > 0 \wedge (X-1)=1 \wedge Y+4=Z = *^5$$

Ismét elértük azt a részt, amikor már műveleti tulajdonság nem alkalmazható. Következzék tehát a formula egyszerűsítése. Az $(X-1)=1$ formula átírható $X=2$ -re. Ennek következtében $X > 0$ mindig igaz lesz, tehát a konjunkció ezen része elhagyható a formulából. Így előáll a végleges alakja P_2 -nek.

$$*^5 = X=2 \wedge Y+4=Z \text{ (ez lesz } P_2)$$

Feladatunk, hogy addig írjuk fel a $P_1, P_2, \dots$ formulákat, mígnem használható kifejezést tudunk felírni bármely P_i -re. Jelen esetben P_0, P_1 és P_2 ismeretében egész jó közelítést kaptunk, hogy megadjuk a minden i -re teljesülő kifejezést.

Állítás:

$$P_i = X=i \wedge Y+i^2=Z, i > 0$$

Bizonyítás teljes indukcióval:

P_0, P_1 és P_2 esetén igaz.

$$\begin{aligned} P_{i+1} &= X > 0 \wedge \text{wp}(C, P_i) = (\text{gyors felírás}) = X > 0 \wedge \text{wp}(X := X - 1, \text{wp}(Y := Y + 2X + 1, X = i \wedge Y + i^2 = Z)) = \\ &= X > 0 \wedge \text{wp}(X := X - 1, X = i \wedge (Y + 2X + 1) + i^2 = Z) = (\text{átírás}) = X > 0 \wedge \text{wp}(X := X - 1, X = i \wedge Y + 2i + 1 + i^2 = Z) = \\ &= X > 0 \wedge \text{wp}(X := X - 1, X = i \wedge Y + (i+1)^2 = Z) = (\text{értékkadás}) = X > 0 \wedge (X-1) = i \wedge Y + (i+1)^2 = Z = *^6 \end{aligned}$$

P_{i+1} kiszámításakor az átírás résznél X helyére behelyettesíthettük i -t, hiszen a formulában volt egy $X=i$ kifejezés. X -et azonban tovább egyszerűsíthetjük, hiszen többször is szerepel a formulában. Az $X-1=i$ formula átírható $X=i+1$ alakúra, amelyből következik, hogy $X > 0$, hiszen i nem lehet negatív szám ($P_0, P_1, P_2, \dots$ indexek miatt belátható), így az $X > 0$ formula konjunkciója elhagyható.

$$*^6 = X = i + 1 \wedge Y + (i + 1)^2 = Z \quad \text{Ez pontosan illeszkedik a felírt sablonra!}$$

Igen ám, de ezzel még nem vagyunk készek. Fel kell írni a ciklus eredményét jelentő kifejezést, majd az eredeti wp formulát tovább egyszerűsíteni.

$$\begin{aligned} *^1 &= P_0 \vee (\exists i \geq 0 . P_i) = (\text{behelyettesítünk}) = (X \leq 0 \wedge Y = Z) \vee (\exists i > 0 . X = i \wedge Y + i^2 = Z) = \\ &= (X \leq 0 \wedge Y = Z) \vee [(\exists i > 0 . X = i \wedge Y + X^2 = Z)] = (X \leq 0 \wedge Y = Z) \vee (X > 0 \wedge Y + X^2 = Z) \end{aligned}$$

Az előbb látott lépésekben i helyére beírtuk X -et, hiszen $X=i$. A $\exists i > 0 . X=i$ kifejezés tulajdonképpen felesleges, helyette egyszerűbb azt írni, hogy $X > 0$.

Visszatérve az eredeti formulához:

$$\begin{aligned} \text{wp}(Y := 0; \text{while } X > 0 \text{ do } X := X - 1; Y := Y + 2X + 1 \text{ od, } Y = Z) &= \text{wp}(Y := 0, (X \leq 0 \wedge Y = Z) \vee (X > 0 \wedge Y + X^2 = Z)) = \\ &= (\text{értékkadás}) = (X \leq 0 \wedge 0 = Z) \vee (X > 0 \wedge 0 + X^2 = Z) \quad \leftarrow \text{Ez lesz a megoldás!} \end{aligned}$$

Egy másik feladatmegoldás:

$\text{wp}(\text{while } X > 0 \text{ do } X := X - Y; Y := 1 - Y \text{ od, } T) = \exists i > 0 . P_i$, ahol

$$P_0 = X \leq 0 \wedge \top$$

$$P_1 = X > 0 \wedge \text{wp}(C, X \leq 0) = X > 0 \wedge \text{wp}(X := X - Y; Y := 1 - Y, X \leq 0) = X > 0 \wedge \text{wp}(X := X - Y, \text{wp}(Y := 1 - Y, X \leq 0)) = \\ = X > 0 \wedge (X - Y) \leq 0 = 0 < X \leq Y$$

$$P_2 = X > 0 \wedge \text{wp}(X := X - Y; Y := 1 - Y, 0 < X \leq Y) = X > 0 \wedge \text{wp}(X := X - Y, \text{wp}(Y := 1 - Y, 0 < X \leq Y)) = \\ = X > 0 \wedge \text{wp}(X := X - Y, 0 < X \leq (1 - Y)) = X > 0 \wedge 0 < (X - Y) \leq (1 - Y) = X > 0 \wedge Y < X \leq 1 = X = 1 \wedge Y < 1$$

$$P_3 = X > 0 \wedge \text{wp}(X := X - Y; Y := 1 - Y, X = 1 \wedge Y < 1) = X > 0 \wedge \text{wp}(X := X - Y, \text{wp}(Y := 1 - Y, X = 1 \wedge Y < 1)) = \\ = X > 0 \wedge \text{wp}(X := X - Y, X = 1 \wedge (1 - Y) < 1) = X > 0 \wedge \text{wp}(X := X - Y, X = 1 \wedge 0 < Y) = X > 0 \wedge (X - Y) = 1 \wedge 0 < Y) = \\ = \cancel{X > 0} \wedge X = Y + 1 \wedge 0 < Y = (Y \text{ nagyobb, mint } 0 \text{ és így } X \text{ is, ezért egyszerűsíthető}) = X = Y + 1 \wedge 0 < Y$$

$$P_4 = X > 0 \wedge \text{wp}(X := X - Y, \text{wp}(Y := 1 - Y, X = Y + 1 \wedge 0 < Y)) = X > 0 \wedge \text{wp}(X := X - Y, X = (1 - Y) + 1 \wedge 0 < (1 - Y)) = \\ = X > 0 \wedge \text{wp}(X := X - Y, X = (1 - Y) + 1 \wedge Y < 1) = X > 0 \wedge \text{wp}(X := X - Y, X + Y = 2 \wedge Y < 1) = \\ = X > 0 \wedge \text{wp}(X := X - Y, X + Y = 2 \wedge Y < 1) = X > 0 \wedge (X - Y) + Y = 2 \wedge Y < 1 = \cancel{X > 0} \wedge X = 2 \wedge Y < 1 = X = 2 \wedge Y < 1$$

$$P_5 = X > 0 \wedge \text{wp}(X := X - Y, \text{wp}(Y := 1 - Y, X = 2 \wedge Y < 1)) = X > 0 \wedge \text{wp}(X := X - Y, X = 2 \wedge (1 - Y) < 1) = \\ = X > 0 \wedge \text{wp}(X := X - Y, X = 2 \wedge 0 < Y) = X > 0 \wedge (X - Y) = 2 \wedge 0 < Y = \cancel{X > 0} \wedge X = Y + 2 \wedge 0 < Y = \\ = (Y \text{ nagyobb, mint } 0 \text{ és így } X \text{ is, ezért egyszerűsíthető}) = X = Y + 2 \wedge 0 < Y$$

Állítás:

$$P_{2k} = X = k \wedge Y < 1$$

A P_0 és P_1 eseteket elkülönítettük a többitől.

$$P_{2k+1} = X = Y + k \wedge 0 < Y$$

Egészen P_5 -ig felírtuk a P -ket, hogy jó kifejezést adjunk.

Bizonyítás:

Kifejteni már nem volt idő.

Feladatmegoldás befejezése:

$$\exists i > 0 . P_i = P_0 \vee P_1 \vee (\exists k > 0 . P_{2k}) \vee (\exists k > 0 . P_{2k+1}) = (X \leq 0) \vee (0 < X \leq Y) \vee (\exists k > 0 . X = k \wedge Y < 1) \\ \vee (\exists k > 0 . X = Y + k \wedge 0 < Y) = (\text{Néhány egyszerűsítés}) =$$

Ahogy már korábban is tettük, az egzisztenciálisan kvantált változók értékeinek átadását egy másik változónak nem tekintjük túl egyszerűnek, ezért egyszerűsítjük őket. A kékkel jelölt kifejezésben jól látható, hogy k egy olyan pozitív egész, amelyet átadjuk X értékéül. Tehát X egy pozitív egész. Elég, ha csak ezt írjuk le, azaz $X > 0$. A narancssárgával jelölt kifejezést is felírhatjuk kvantormentesen. A lényeg, hogy olyan alakúra írjuk fel, hogy k magában szerepeljen az egyik oldalon. Tehát $X - Y = k$. A k -ról tudjuk, hogy nagyobb, mint 0. Tehát $X - Y > 0$ lesz a megfelelő kifejezés, amellyel helyettesítjük a régit.

$$= (X \leq 0) \vee (0 < X \leq Y) \vee (X > 0 \wedge Y < 1) \vee (X - Y > 0 \wedge 0 < Y) = X \leq 0 \vee (0 < X \wedge (X \leq Y \vee Y \leq 0 \vee (X > Y \wedge 0 < Y))) = T$$

Az utolsó lépésben annyira leegyszerűsítjük a formulát, hogy tulajdonképpen észrevevessük, hogy azonosan igaz kifejezést kapunk. Ez az azonosan igaz kifejezés lesz a feladat megoldása.

Az utolsó lépés részletezve:

$$X \leq Y \vee Y \leq 0 \vee (X > Y \wedge 0 < Y) \cong A \vee B \vee (\neg A \wedge \neg B) = (A \vee B) \vee \neg(A \vee B) = T$$

$$X \leq 0 \vee 0 < X \wedge \top = X \leq 0 \vee X > 0 = T$$