

# Algoritmusok tervezése és elemzése

2012. 02. 15.

Parciális Hoare-kalkulus

Alaphalmazok:  $V^*$ ,  $Z$

```
{ T } Y := X; Z := λ; while Y ≠ λ do Z := f(Y)Z; Y := t(Y) od;
    while Z ≠ λ do
    if f(Y) = f(Z) then Z := t(Z) else Y := f(Z)Y fi
    od { Y = red(X) }
```

Értelmezzük az algoritmus működését és írjuk fel az egyes változók tartalmát a ciklusok alatt.

| X      | Y      | Z      |                                         |
|--------|--------|--------|-----------------------------------------|
| aabccc | aabccc | λ      | Határozzuk meg az első ciklus ciklus-   |
|        | abccc  | a      | invariánsát (manuálisan kell!).         |
|        | bccc   | aa     | Keresünk egy olyan kifejezést, amely    |
|        | ccc    | baa    | minden lépésben felírható a változókra. |
|        | cc     | cbaa   |                                         |
|        | c      | ccbaa  | $P = Y^{-1}Z = X^{-1}$                  |
|        | λ      | cccbaa | P minden lépésben teljesül.             |

| Y         | Z             |                                                                    |
|-----------|---------------|--------------------------------------------------------------------|
| <u>λ</u>  | <u>cccbaa</u> | Határozzuk meg a második ciklus-invariánst.                        |
| c         | ccbaa         | Keresünk egy olyan kifejezést, amely minden lépésben               |
| c         | cbaa          | felírható a változókra.                                            |
| <u>c</u>  | <u>baa</u>    |                                                                    |
| bc        | baa           | $P = \text{red}(Z^{-1}Y) = \text{red}(X) \wedge Y = \text{red}(Y)$ |
| <u>bc</u> | <u>aa</u>     |                                                                    |
| abc       | aa            | Ha a bal oldali kifejezésben $Z^{-1}$ és Y nem lenne a zárójelen   |
| abc       | a             | belül, előfordulhatna, hogy $Z^{-1}$ és Y redukált alakjában       |
| abc       | λ             | ugyanaz a betű külön-külön szerepelne és ezek összefűzött          |
|           |               | alakja már nem lenne redukált.                                     |

A jobb oldali kifejezésben az  $Y = \text{red}(Y)$  kifejezés a feltétel erősítésére szolgál, azaz garantáljuk, hogy Y minden esetben redukált kifejezést tartalmaz (globálisan helyes formula).

## Dekorációs feladat:

- $\{ T \}$
- $\{ X^{-1} = X^{-1} \}$
- $Y := X;$
- $\{ Y^{-1} = X^{-1} \}$

3.  $Z := \lambda;$

16.  $\{ Y^{-1} Z = X^{-1} \}$  // A while feletti sorba a P-t írjuk (ciklus invariáns)

4. while  $Y \neq \lambda$  do

17.  $\{ Y^{-1} Z = X^{-1} \wedge Y \neq \lambda \}$  // A while alatti sorba a „ $P \wedge B$ ”-t írjuk (B = feltétel)

31.  $\{ \underline{t(Y)^{-1} f(Y) Z = X^{-1}} \}$

5.  $Z := f(Y) Z;$

30.  $\{ \underline{t(Y)^{-1} Z = X^{-1}} \}$

6.  $Y := t(Y);$

18.  $\{ Y^{-1} Z = X^{-1} \}$  // od feletti sorba: P

7. od;

19.  $\{ Y^{-1} Z = X^{-1} \wedge Y = \lambda \}$  // od alatti sorba:  $(P \wedge \neg B)$

20.  $\{ \text{red}(Z^{-1} Y) = \text{red}(X) \wedge Y = \text{red}(Y) \}$  // while feletti sorba: P (ciklus invariáns)

8. while  $Z \neq \lambda$  do

21.  $\{ \text{red}(Z^{-1} Y) = \text{red}(X) \wedge Y = \text{red}(Y) \wedge Z \neq \lambda \}$  // while alatti sorba:  $P \wedge B$  (B = feltétel)

9. if  $f(Y) = f(Z)$  then **Az IF-nek saját P-je van, amely a hozzá tartozó while alatti formula.**  
**Azaz P alakja az IF-en belül:**  $\text{red}(Z^{-1} Y) = \text{red}(X) \wedge Y = \text{red}(Y) \wedge Z \neq \lambda$

24.  $\{ \text{red}(Z^{-1} Y) = \text{red}(X) \wedge Y = \text{red}(Y) \wedge Z \neq \lambda \wedge f(Y) = f(Z) \}$  //  $P \wedge B$ , ahol B az IF feltétele

29.  $\{ \underline{\text{red}(t(Z)^{-1} Y) = \text{red}(X) \wedge Y = \text{red}(Y)} \}$

10.  $Z := t(Z);$

25.  $\{ \text{red}(Z^{-1} Y) = \text{red}(X) \wedge Y = \text{red}(Y) \}$  // else feletti sorba: Q (lejjebb infó)

11. else

26.  $\{ \text{red}(Z^{-1} Y) = \text{red}(X) \wedge Y = \text{red}(Y) \wedge Z \neq \lambda \wedge f(Y) \neq f(Z) \}$  // else alatti sorba:  $P \wedge \neg B$

28.  $\{ \underline{\text{red}(Z^{-1} f(Z) Y) = \text{red}(X) \wedge f(Z) = \text{red}(f(Z) Y)} \}$

12.  $Y := f(Z) Y;$

27.  $\{ \text{red}(Z^{-1} Y) = \text{red}(X) \wedge Y = \text{red}(Y) \}$  // fi feletti sorba: Q (itt van alatta az infó)

13. fi **Az IF-nek megadunk egy Q formulát, amely a hozzá tartozó fi alatti formula.**

22.  $\{ \text{red}(Z^{-1} Y) = \text{red}(X) \wedge Y = \text{red}(Y) \}$  // od fölötti sorba:  $P \Rightarrow Q$  (fi alatti)

14. od

23.  $\{ \text{red}(Z^{-1} Y) = \text{red}(X) \wedge Y = \text{red}(Y) \wedge Z = \lambda \}$  // od alatti sorba:  $(P \wedge \neg B)$

15.  $\{ Y = \text{red}(X) \}$

A while és a do részeknél a felső, ill. alsó sorokba a ciklushoz hozzá tartozó ciklus-invariánst kell írni! Az aláhúzott formulákat alulról felfelé határozzuk meg az alattuk álló formulákból.

Az (1,33), (17,31), (19,20), (24,29), (26,28) és (23,15) számpárokkal jelölt sorok között implikáció áll fenn, amelyet a gépelt jegyzet hátrányai miatt nem jelöltem a sorok elején.

### Bináris hatványozás:

$$Y^X = \begin{cases} 1, & \text{ha } X = 0 \\ Y * Y^{X-1}, & \text{ha } X > 0, \text{ Dom} = \mathbb{Z} \text{ (egész számok halmaza)} \\ w, & \text{ha } X < 1 \end{cases}$$

{ T } X := 1; Y := m; Z := n; while Z ≠ 0 do

2 | Z = osztója –e?

if 2 | Z then Y := Y<sup>2</sup>; Z := Z/2 else X := XY; Z := Z-1 fi

Z/2 = lefelé kerekített osztás

od { X = m<sup>n</sup> }

| m | n  | X               | Y               | Z  |
|---|----|-----------------|-----------------|----|
| 2 | 36 | 1               | 2               | 36 |
|   |    | 1               | 2 <sup>2</sup>  | 18 |
|   |    | 1               | 2 <sup>4</sup>  | 9  |
|   |    | 2 <sup>4</sup>  | 2 <sup>4</sup>  | 8  |
|   |    | 2 <sup>4</sup>  | 2 <sup>8</sup>  | 4  |
|   |    | 2 <sup>4</sup>  | 2 <sup>16</sup> | 2  |
|   |    | 2 <sup>4</sup>  | 2 <sup>32</sup> | 1  |
|   |    | 2 <sup>36</sup> | 2 <sup>32</sup> | 0  |

Határozzuk meg a ciklus-invariánst.

Melyik az a kifejezés, amely minden lépésben teljesül?

$$P = X * Y^Z = m^n$$

Megjegyezném, hogy már korábban is írtam:  
P meghatározása nem automatizálható!

### Dekoráció:

1. { T }

29. { m<sup>n</sup> = m<sup>n</sup> ∨ n < 0 }

// n ≥ 0

2. X := 1

**A „Z < 0” formulát** a ciklus-invariáns erősítéséhez

28. { Xm<sup>n</sup> = m<sup>n</sup> ∨ n < 0 }

vezettük be, hogy az algoritmusunk totálisan helyes legyen.

3. Y := m;

27. { XY<sup>n</sup> = m<sup>n</sup> ∨ n < 0 }

4. Z := n;

16. { XY<sup>Z</sup> = m<sup>n</sup> ∨ Z < 0 }

// while feletti sorba: P

5. while Z ≠ 0 do

17. { ( XY<sup>Z</sup> = m<sup>n</sup> ∨ Z < 0 ) ∧ Z ≠ 0 }

// while alatti sorban: P ∧ B

6. if 2 | Z then

20. { ( XY<sup>Z</sup> = m<sup>n</sup> ∨ Z < 0 ) ∧ Z ≠ 0 ∧ 2 | Z }

// if alatti sorban: P ∧ B (ahol P a while alatti sor)

26. { (X(Y<sup>Z</sup>)<sup>Z/2</sup> = m<sup>n</sup>) ∨ (Z/2 < 0) }

7. Y := Y<sup>2</sup>;

25. { XY<sup>Z/2</sup> = m<sup>n</sup> ∨ (Z/2 < 0) }

8. Z := Z/2;

9.  $\{XY^Z = m^n \vee Z < 0\}$  // else feletti sorban: Q (od fölötti sorból jön)
10. else
21.  $\{ (XY^Z = m^n \vee Z < 0) \wedge Z \neq 0 \wedge 2+Z \}$  // else alatti sorban:  $P \wedge \neg B$  (+ = nem osztója)
24.  $\{ \underline{XY^{Z-1} = m^n \vee (Z-1 < 0)} \}$
11.  $X := XY;$
23.  $\{ \underline{XY^{Z-1} = m^n \vee (Z-1 < 0)} \}$
12.  $Z := Z-1;$
22.  $\{XY^Z = m^n \vee Z < 0\}$  // fi feletti sorban: Q
13. fi
18.  $\{XY^Z = m^n \vee Z < 0\}$  // od feletti sorban:  $P \Rightarrow Q$  (fi alatti)
14. od
19.  $\{ (XY^Z = m^n \vee (Z < 0)) \wedge (Z = 0) \}$  // od alatti sorban:  $P \wedge \neg B$
15.  $\{X = m^n\}$

Az (1,29), (20,26), (21,24) és (19,15) számpárokkal jelölt sorok között implikáció áll fenn, amelyet a gépelt jegyzet hátrányai miatt nem jelöltem a sorok elején.