Dowodzenie poprawności programów

Wstęp do Informatyki i Programowania

Maciek Gębala

14 listopada 2024

Maciek Gehala

owodzenie poprawności programów

Niezmiennik i skończoność pętli

Poprawność programu

Na wykładzie tym zajmiemy się dwoma zagadnieniami:

- czy pętla jest poprawna?
- czy pętla zawsze kończy pracę?

Definicja: Częściowa poprawność

Mówimy, że program S jest częściowo poprawny gdy dla danych spełniających warunek P, jeśli program S kończy pracę, to jego wyniki spełniają warunek Q.

Jeśli program nie kończy pracy, to jest częściowo poprawny.

Definicja: Pełna poprawność

Mówimy, że program S jest w pełni poprawny gdy, jeśli dane spełniają warunek P, to program S kończy pracę i jego wyniki spełniają warunek Q.

Jeśli program nie kończy pracy, to nie jest w pełni poprawny.

Maciek Gębala

Dowodzenie poprawności programów

Niezmiennik i skończoność pętli

Dla pętli istnieje potencjalnie nieskończenie wiele ścieżek obliczeń.

Jak udowodnić poprawność nieskończenie wielu ścieżek obliczeń?

Dowody przez indukcję.

Rozpatrzmy następującą pętlę

- 1: while W do
- 2: S
- 3: end while

Gdzie W jest warunkiem sterującym pętli a S ciągiem instrukcji.

Maciek Gebala

owodzenie poprawności programów

Niezmiennik i skończoność pętli

Zawsze istnieje warunek P taki, że:

- 1: { zakładamy ($P \wedge W$) }
- 2: S
- $3: \{ \text{ spełnione jest } (P) \}$

to znaczy, jeśli spełniony jest warunek P oraz W, to po wykonaniu ciągu instrukcji S spełniony jest warunek P (takim warunkiem jest np. True).

Można udowodnić, że taki warunek P ma również taką własność:

- 1: { spełnione jest (P) }
- 2: while W do
- 3: *S*
- 4: end while
- 5: { spełnione jest ($P \land \neg W$) }

Warunek P o powyższej własności nazywa się niezmiennikiem pętli.

Dowodzenie poprawności progran

Notatki
Notatki
Notatki
Notatki
Notatki
Notatki
Notatki

Niezmiennik i skończoność pętli	Notatki
Nazwa niezmiennik podkreśla, że warunek ten jest zachowany	
podczas wykonywania pętli (nie zmienia się).	
Przyjmijmy, że w pętli zmieniają swoje wartości zmienne x_1, x_2, \dots, x_n	
Warunek P będziemy zapisywać jako $P(x_1, x_2, \ldots, x_n)$.	
Maciek Ogbala Dowodzenie poprawności programów	
Niezmiennik i skończoność pętli	Notatki
Aby udowodnić, że $P(x_1, x_2,, x_n)$ jest niezmiennikiem będziemy stosować indukcje :	
 w pierwszym kroku będziemy sprawdzać, czy po dojściu do pętli (a przed rozpoczęciem jej wykonywania) dane spełniają warunek 	
$P(x_1, x_2, \dots, x_n)$ (w tym celu podstawimy za zmienne x_1, x_2, \dots, x_n wartości jakie mają przy dojściu do pętli i sprawdzimy czy	
zachodzi warunek P).	
 w drugim kroku będziemy udowadniać następującą implikację: P(x₁, x₂,,x_n) \(\times W(x₁, x₂,,x_n) \) \(Q(x₁, x₂,,x_n, x'₁, x'₂,,x'_n)\) 	
$\Rightarrow P(x'_1, x'_2, \dots, x'_n) \land (x_1, x'_2, \dots, x'_n, x_1, x'_2, \dots, x'_n)$	
gdzie warunek $Q(x_1, x_2, \dots, x_n, x_1', x_2', \dots, x_n')$ wyraża zależność nowych wartości zmiennych (te z primami) od starych wartości	
(te bez primów)	
Maciek Gębala Dowodzenie poprawności programów	
Niezmiennik i skończoność pętli	Notatki
NOZIMOMIMET CHORICZONICCO PQLII	···
Przykład	
Dla ponižszej pętli 1: while W do	
2: X ← X + 1 3: Y ← Y + X	
4: end while	
warunek $Q(X, X', Y, Y')$ jest następujący $(X' = X + 1 \land Y' = Y + X')$ (zwróć uwagę, że do starej wartości Y dodawana jest nowa wartość	
X' obliczona w poprzedniej instrukcji).	
Jeśli powiedzie się dowód indukcyjny, to udowodniliśmy, że po wykonaniu pętli while nadal zachodzi warunek <i>P</i> , czyli jest on	
niezmiennikiem pętli.	
Maciek Ogbala Dowodzenie poprawności programów	
Niezmiennik i skończoność pętli	Notatki
Kluczową rolę odgrywa to, jaki warunek P będziemy dowodzić.	
Jak wcześniej wspomniano taki warunek zawsze istnieje ale warunek	
True jest bezużyteczny gdyż wszystkie wartości danych go spełniają, więc nic nie mówi on o działaniu pętli.	
Najlepiej byłoby za <i>P</i> przyjąć warunek spełniony przez jak najmniejszą liczbę danych (jak najsilniejszy), dlatego przez	
niezmiennik pętli będziemy uważać najsilniejszy warunek spośród tych, które są zachowane podczas działania pętli.	

.....

Niezmiennik i skończoność pętli Notatki Skąd wziąć taki najsilniejszy warunek? Pisząc pętlę, myślimy jak ona ma działać by uzyskać pożądany efekt i prawie zawsze wyobrażamy sobie taki niezmiennik. Dla pętli napisanych przez innych sytuacja jest bardziej skomplikowana: najlepiej prześledzić działanie pętli analizując ślad wykonania jej pierwszych kilku/kilkunastu iteracji i obserwując jak zmieniały się dane w kolejnych iteracjach można starać się odgadnąć postać niezmiennika. Po sformułowaniu warunku P należy jeszcze udowodnić indukcyjnie, że faktycznie jest to niezmiennik. Niezmiennik i skończoność pętli - przykład Notatki Przykład: iloraz całkowity W poniższym fragmencie kodu dane są wartości zmiennych całkowitoliczbowych $x\geqslant 0$ i y>0. 1: $q \leftarrow 0$ 2: *r* ← *x* 3: while $r \geqslant y$ do 4: $q \leftarrow q + 1$ 6: end while Udowodnimy, że powyższa pętla wylicza iloraz całkowity q i resztę r z dzielenia x przez y. Pokażemy indukcyjnie, że niezmiennikiem jest $P(q,r) \equiv (x = q \cdot y + r) \wedge (0 \leqslant r)$ Niezmiennik i skończoność pętli - przykład Notatki W pierwszym kroku sprawdzimy czy wartości q=0 i r=x spełniają warunek niezmiennika: $P(0,x)\equiv (x=0\cdot y+x)\wedge (0\leqslant x)\equiv (x=x)\wedge (0\leqslant x)\equiv (0\leqslant x)$ W drugim kroku pokażemy prawdziwość implikacji $P(q,r) \wedge (r \geqslant y) \wedge Q(q,q',r,r') \implies P(q',r'),$ gdzie $Q(q,q',r,r') \equiv (r'=r-y) \wedge (q'=q+1)$ Niezmiennik i skończoność pętli - przykład Notatki Założenia

 $(x=q\cdot y+r)\wedge (0\leqslant r)\wedge (r\geqslant y)\wedge (r'=r-y)\wedge (q'=q+1)$

Teza

 $(x = q' \cdot y + r') \wedge (0 \leqslant r')$

Dowód

 $x = q \cdot y + r = (q'-1) \cdot y + r = (q'-1) \cdot y + (r'+y) = q' \cdot y + r'$

 $r'=r-y\geqslant 0$

zatem nowe wartości q' i r' spełniają warunek P

Niezmiennik i skończoność pętli - przykład

Dowód

Po wyjściu z pętli zachodzi

$$P(q,r) \wedge (r < y) \equiv (x = q \cdot y + r) \wedge (0 \leqslant r < y)$$

Skończoność wykonania pętli wynika z kolejnego zmniejszania się r i dojścia do kresu dolnego mniejszego niż y.

Niezmiennik i skończoność pętli - przykład

Przykład: potęgowanie całkowite

W poniższym fragmencie kodu dane są wartości zmiennych x>0 i $n \geqslant 0$

1: *v* ← 1 2: $p \leftarrow x$ 3: $i \leftarrow n$

4: while $i \neq 0$ do

5: **if** $i \mod 2 = 0$ **then** 6:

 $p \leftarrow p \cdot p$ $i \leftarrow i/2$ 7:

8: else

9: $y \leftarrow y \cdot p$ $i \leftarrow i - 1$

10:

end if 11: 12: end while

Udowodnimy, że powyższa pętla wylicza x^n .

Pokażemy indukcyjnie, że niezmiennikiem jest $P(y, p, i) \equiv y \cdot p^i = x^n$.

Maciek Gębala Do

Niezmiennik i skończoność pętli - przykład

W pierwszym kroku sprawdzamy czy wartości y = 1, p = x i i = nspełniają warunek niezmiennika: $P(1, x, n) \equiv 1 \cdot x^n = x^n \equiv x^n = x^n$

W drugim kroku pokazujemy prawdziwość implikacji

$$P(y,p,i) \land (i \neq 0) \land Q(y,y',p,p',i,i') \implies P(y',p',i'),$$

gdzie Q(y,y',p,p',i,i') opisuje jak w jednym przebiegu pętli zmieniają się wartości zmiennych y, p oraz i.

Niezmiennik i skończoność pętli - przykład

Zmiany zmiennych zależą od parzystości wartości zmiennej i, zatem dowód będzie składał się z dwóch przypadków:

- i iest parzyste
 - założenia: $(y \cdot p^i = x^n) \wedge (i \neq 0) \wedge (y' = y) \wedge (p' = p^2) \wedge (i' = i/2)$

 - teza: $y' \cdot p'^{i'} = x^n$ dowód: $y' \cdot p'^{i'} = y \cdot (p^2)^{i/2} = y \cdot p^i = x^n$
- *i* jest nieparzyste
 - założenia:
 - Leave Hall. $(y \cdot p' = x^n) \wedge (i \neq 0) \wedge (y' = y \cdot p) \wedge (p' = p) \wedge (i' = i 1)$ teza: $y' \cdot p'^{i'} = x^n$ dowód: $y' \cdot p'^{i'} = (y \cdot p) \cdot p^{i-1} = y \cdot p^i = x^n$

Po wyjściu z pętli zachodzi warunek $P(y, p, i) \land (i = 0)$, zatem $(y \cdot p^i = x^n) \wedge (i = 0) \implies y = x^n$

Notatki
Notatki
Notatki
Hotelin
Notatkí
Notatki

Skończoność pętli

Samo udowodnienie niezmiennika nie gwarantuje, że program jest w pełni poprawny. Należy jeszcze udowodnić, że dla wszystkich poprawnych danych pętla kończy pracę.

Aby pokazać, że pętla kończy pracę należy podać wyrażenie o wartościach całkowitych ograniczonych z dołu, które przy każdej iteracji pętli maleją.

Porządek < na liczbach naturalnych jest dobrze ufundowany, gdyż nie istnieje nieskończony ciąg malejący o wartościach naturalnych.

Analogicznie można dla dowodu podać wyrażenie o wartościach całkowitych ograniczonych z góry, które przy każdej iteracji pętli rosną (wówczas maleje dystans do górnego ograniczenia).

aciek Gebala

owodzenie poprawności programów

Ciekawostka

Hipoteza Collatza (hipoteza 3n + 1)

W roku 1937 niemiecki matematyk Lothar Collatz sformułował hipotezę, że poniższy ciąg zawsze osiąga wartość 1 dla dowolnej początkowej wartości całkowitej $c_0>1$

$$c_{n+1} = \left\{ egin{array}{ll} c_n/2 & ext{gdy } c_n ext{ jest parzyste} \ 3 \cdot c_n + 1 & ext{gdy } c_n ext{ jest nieparzyste} \end{array}
ight.$$

Hipoteza pozostaje do dziś nierozstrzygnięta (sprawdzono liczby mniejsze od $5\cdot 2^{60}\approx 5.764\cdot 10^{18}).$

Maciek Gęb

owodzenie poprawności programów

Natatri
Notatki
Notatki
Notatki
Notatki
Notatki
Notatki