Poprawność

Czy program P jest poprawny, skoro

1. ~~udało się go sprzedać 2 mln użytkowników~~
2. ~~był w użyciu przez dwa lata i prawie nie było uzasadnionych skarg ze strony klientów~~
3. ~~został przetestowany na dużej ilości losowych danych i~~
   - ~~w 36.1% przypadków dał wyniki, o których wiemy, że są poprawne~~
   - ~~w 63.3% przypadków dał wyniki, w których nie znaleźliśmy błędu, ale nie wiemy, jaka powinna być prawidłowa odpowiedź~~
   - ~~zaledwie w 0.6% przypadków dał wyniki na pewno błędne~~
4. autorzy programu są głęboko przekonani o jego poprawności i potrafili przekonać o niej sceptyków spoza firmy
5. do jego sporządzenia zatrudniono najlepszych dostępnych fachowców, w czasie pracy stosowano ostre reżimy technologiczne, a ostateczny produkt długo sprawdzali zupełnie inni fachowcy zainteresowani materialnie w znalezieniu błędu

---

4: dowodzenie poprawności
5: formalne metody programowania

Reguły wnioskowania dla poprawności częściowej

Logika Hoare'a

$\{p_0\}\, c\, \{p_1\}$ — instrukcja c jest *częściowo poprawna* wzgl. formuł p_0 i p_1:

$$\{p_0\}\, c\, \{p_1\} \overset{\text{def}}{\iff}$$
$$\forall_s\ s \text{ spełnia } p_0\ \&\ c \text{ przeprowadza } s \text{ w } s' \Rightarrow s' \text{ spełnia } p_1$$

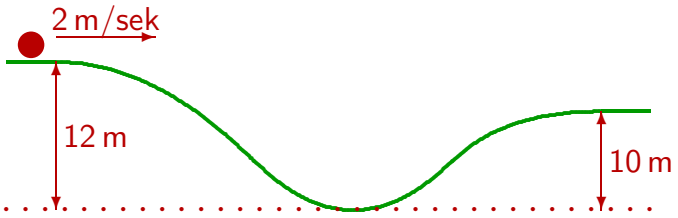
czyli: *jeśli* dane s spełniają p_0 *i* c zatrzymuje się na s z wynikiem s' *to* wyniki s' spełniają p_1

czyli: c nie daje błędnych wyników (ale może nie dać żadnych)

Przykład:

$\{\text{fałsz}\}\, c\, \{p\}$ — zawsze prawda
$\{p_0\}$ WHILE true DO $c\, \{p_1\}$ — zawsze prawda
$\{p\}\, c\, \{\text{fałsz}\}$ — prawda jeśli c zapętla się na danych spełniających p
$\{x+1=1\}\, x := x+1\, \{x=1\}$ — prawda
$\{x=0\}\, x := x+1\, \{x=1\}$ — prawda

Niezmienniki spoza informatyki



energia $=$ energia kinetyczna $+$ energia potencjalna $= \frac{mv^2}{2} + mgh$
— jest stała.

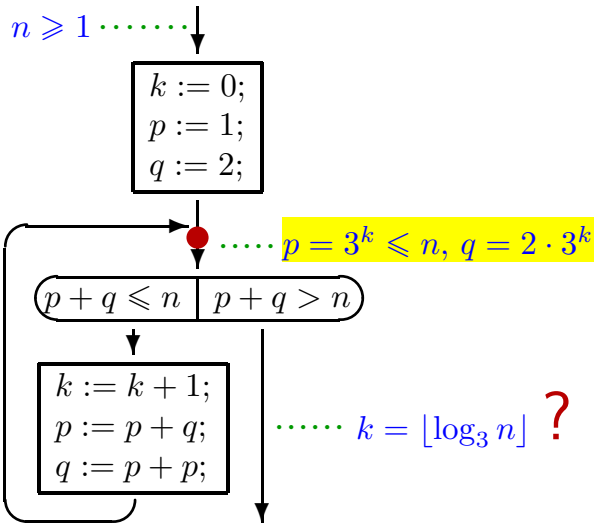
$$\frac{2^2}{2} + 12 \cdot g = \frac{v^2}{2} + 10 \cdot g \qquad v = \sqrt{4 + 4 \cdot g}$$

Reguły wnioskowania dla poprawności częściowej

Metoda niezmienników

k	0	1	2	3	4	$\cdots$
p	1	3	9	27	81	$\cdots$
q	2	6	18	54	162	$\cdots$

z $3^k \leqslant n < 3^{k+1}$
wynika $k = \lfloor \log_3 n \rfloor$



formuła jest spełniona za pierwszym wejściem do ●

jeśli formuła jest spełniona w ●, to będzie spełniona za następną bytnością w ●

---

formuła jest *zawsze* spełniona w ●

Reguły wnioskowania dla poprawności częściowej

Logika Hoare'a

Wprowadzanie instr. pustej:

$$\frac{}{\{p\}\ \{p\}}$$

Wprowadzanie przypisania:

$$\frac{}{\{p(t)\}\, x := t\, \{p(x)\}}$$

Wprowadzanie złożenia:

$$\frac{\{p_0\}\, c_1\, \{p_1\} \quad \{p_1\}\, c_2\, \{p_2\}}{\{p_0\}\, c_1; c_2\, \{p_2\}}$$

Wprowadzanie instr. warunkowej:

$$\frac{\{p_0\ \&\ b\}\, c_1\, \{p_1\} \quad \{p_0\ \&\ \neg b\}\, c_2\, \{p_1\}}{\{p_0\}\, \mathsf{IF}\ b\ \mathsf{THEN}\ c_1\ \mathsf{ELSE}\ c_2\, \{p_1\}}$$

Wprowadzanie pętli:

$$\frac{\{p\ \&\ b\}\, c\, \{p\}}{\{p\}\, \mathsf{WHILE}\ b\ \mathsf{DO}\ c\, \{p\ \&\ \neg b\}}$$

Konsekwencja:

$$\frac{p_0' \Rightarrow p_0 \qquad \{p_0\}\, c\, \{p_1\} \qquad p_1 \Rightarrow p_1'}{\{p_0'\}\, c\, \{p_1'\}}$$