

問題 I

以下の部分正当性が成立するための必要十分条件を, A と B を用いた論理式で表せ.

$$\{A\} \text{if } X > 0 \text{ then } Y := X + Y \text{ else skip } \{B\}$$

まず, 再弱事前条件 $wp(\text{if } X > 0 \text{ then } Y := X + Y \text{ else skip }, B)$ を計算する.

$$\begin{aligned} wp(\text{if } X > 0 \text{ then } Y := X + Y \text{ else skip }, B) &\equiv (X > 0 \wedge wp(Y := X + Y, B)) \vee (\neg(X > 0) \wedge wp(\text{skip}, B)) \\ &\equiv (X > 0 \wedge [X + Y/Y]B) \vee (\neg(X > 0) \wedge B) \end{aligned}$$

よって, $\{A\} \text{if } X > 0 \text{ then } Y := X + Y \text{ else skip } \{B\}$ が成り立つための必要十分条件は

$A \Rightarrow wp(\text{if } X > 0 \text{ then } Y := X + Y \text{ else skip }, B)$, すなわち

$$A \Rightarrow (X > 0 \wedge [X + Y/Y]B) \vee (\neg(X > 0) \wedge B)$$

問題 II

以下の注釈つきプログラム c を考える.

while $\{X > 0 \wedge Y > 0 \wedge gcd(X, Y) = gcd(m, n)\}$ **not** $(X = Y)$ **do**
 if $X \leq Y$ **then** $Y := Y - X$ **else** $X := X - Y$

$\{X = m > 0 \wedge Y = n > 0\}c\{X = gcd(m, n)\}$ の検証条件 (すなわち $vc(X = m > 0 \wedge Y = n > 0, c, X = gcd(m, n))$) を計算せよ.

$$I \equiv X > 0 \wedge Y > 0 \wedge gcd(X, Y) = gcd(m, n)$$

$$c_0 \equiv \text{if } X \leq Y \text{ then } Y := Y - X \text{ else } X := X - Y$$

とすると,

まず

$$wp2(Y := Y - X, I) \equiv ([Y - X/Y]I, \text{true})$$

$$wp2(X := X - Y, I) \equiv ([X - Y/X]I, \text{true})$$

より,

$$wp2(c_0, I) \equiv (([Y - X/Y]I \wedge X \leq Y) \vee ([X - Y/X]I \wedge \neg X \leq Y), \text{true})$$

よって,

$$\begin{aligned} wp2(c, X = gcd(m, n)) &\equiv \\ &(I, \\ &(I \wedge \neg(X = Y) \Rightarrow (([Y - X/Y]I \wedge X \leq Y) \vee ([X - Y/X]I \wedge \neg X \leq Y))) \\ &\wedge (I \wedge \neg\neg(X = Y) \Rightarrow X = gcd(m, n))) \end{aligned}$$

したがって, 検証条件 $vc(X = m > 0 \wedge Y = n > 0, c, X = gcd(m, n))$ は,

$$\begin{aligned} &((X = m > 0 \wedge Y = n > 0) \Rightarrow I) \\ &\wedge ((I \wedge \neg(X = Y)) \Rightarrow (([Y - X/Y]I \wedge X \leq Y) \vee ([X - Y/X]I \wedge \neg X \leq Y))) \\ &\wedge (I \wedge \neg\neg(X = Y) \Rightarrow X = gcd(m, n)) \end{aligned}$$

解説 検証条件の計算式に従って忠実に計算するだけ.