

問題 I

関係 $(c, \sigma) \longrightarrow^* (c', \sigma')$ を用いて以下の性質を論理式で表せ. (Σ は状態の集合, すなわち $\mathbf{Var} \rightarrow$ とする.)

(a) 初期状態での変数 X の値が正であれば, プログラム c の実行は停止する.

$$\forall \sigma \in \Sigma. (\sigma(X) > 0 \Rightarrow \exists \sigma' \in \Sigma. (c, \sigma) \longrightarrow^* (\mathbf{skip}, \sigma'))$$

(b) 初期状態での変数 X の値が正であれば, プログラム c の実行は停止し, 停止時の Y の値は, 初期状態での X の値よりも大きい.

$$\forall \sigma \in \Sigma. (\sigma(X) > 0 \Rightarrow \exists \sigma' \in \Sigma. (c, \sigma) \longrightarrow^* (\mathbf{skip}, \sigma') \wedge \sigma'(Y) > \sigma(X))$$

(c) どんな初期状態でも, プログラム c_1 の実行が停止するならば, 同じ初期状態のもとでプログラム c_2 も停止する.

$$\forall \sigma \in \Sigma. ((\exists \sigma' \in \Sigma. (c_1, \sigma) \longrightarrow^* (\mathbf{skip}, \sigma')) \Rightarrow \exists \sigma' \in \Sigma. (c_2, \sigma) \longrightarrow^* (\mathbf{skip}, \sigma'))$$

注: 限量子 ($\forall, \exists$) の使い方に注意すること. 例えば最後の問題の答を

$$\forall \sigma \in \Sigma. \exists \sigma' \in \Sigma. ((c_1, \sigma) \longrightarrow^* (\mathbf{skip}, \sigma') \Rightarrow (c_2, \sigma) \longrightarrow^* (\mathbf{skip}, \sigma'))$$

とすると全然違う意味になる.

問題 II

次のプログラム c を考える.

```
R := 1;
while 1 ≤ N do (R := R × N; N := N − 1)
```

以下は,

$$\forall n \in \mathbf{N}. \forall \sigma \in \Sigma. (\sigma(N) = n \geq 0 \Rightarrow \exists \sigma' \in \Sigma. ((c, \sigma) \longrightarrow^* (\mathbf{skip}, \sigma') \wedge \sigma'(R) = n!))$$

すなわち, 「 N の値が 0 以上である初期状態のもとで c を実行したら, 実行が停止し, 停止時の R の値は N の初期値の階乗である」ことの証明である.

空白部分を埋めて証明を完成させよ.

証明 while $1 \leq N$ do $(R := R \times N; N := N - 1)$ の部分を c_1 とすると $(c, \sigma) \longrightarrow^* (c_1, \sigma\{R \mapsto 1\})$ が成り立つ. 従って, 与えられた命題を証明するためには

$$\forall n \in \mathbf{N}. \forall \sigma \in \Sigma. (\sigma(N) = n \geq 0 \wedge \sigma(R) = 1 \Rightarrow \exists \sigma' \in \Sigma. ((c_1, \sigma) \longrightarrow^* (\mathbf{skip}, \sigma') \wedge \sigma'(R) = n!))$$

を示せばよい. そのためには, これをさらに一般化して得られる次の命題 (A) を n に関する数学的帰納法により証明すれば十分である.

$$\forall n \in \mathbf{N}. \forall \sigma \in \Sigma. (\sigma(N) = n \geq 0 \Rightarrow \exists \sigma' \in \Sigma. ((c_1, \sigma) \longrightarrow^* (\mathbf{skip}, \sigma') \wedge \sigma'(R) = \sigma(R) \times n!))$$

(i) $n = 0$ のとき.

$$\begin{aligned} (c_1, \sigma) &\longrightarrow (\text{if } 1 \leq N \text{ then } (R := R \times N; N := N - 1); c_1 \text{ else skip}, \sigma) \\ &\longrightarrow^* (\text{if } \boxed{\text{false}} \text{ then } (R := R \times N; N := N - 1); c_1 \text{ else skip}, \sigma) \\ &\longrightarrow (\text{skip}, \sigma) \end{aligned}$$

従って, $\sigma' = \boxed{\sigma}$ とおくと, $(c_1, \sigma) \longrightarrow^* (\text{skip}, \sigma') \wedge \sigma'(R) = \sigma(R) \times n!$ が成り立つ.

(ii) $n > 0$ のとき.

$\sigma(R) = r$ とおくと,

$$\begin{aligned} (c_1, \sigma) &\longrightarrow (\text{if } 1 \leq N \text{ then } (R := R \times N; N := N - 1); c_1 \text{ else skip}, \sigma) \\ &\longrightarrow^* (\text{if } \boxed{\text{true}} \text{ then } (R := R \times N; N := N - 1); c_1 \text{ else skip}, \sigma) \\ &\longrightarrow ((R := R \times N; N := N - 1); c_1, \sigma) \\ &\longrightarrow^* ((N := N - 1); c_1, \sigma\{R \mapsto r \times n\}) \\ &\longrightarrow^* (c_1, \sigma_1) \quad \cdots(1) \end{aligned}$$

ただし, $\sigma_1 = \{R \mapsto r \times n, N \mapsto \boxed{n - 1}\}$.

帰納法の仮定より, ある σ' が存在して,

$$(c_1, \sigma_1) \longrightarrow^* (\text{skip}, \sigma') \quad \cdots(2)$$

$$\sigma'(R) = \sigma_1(R) \times (\sigma_1(N))! \quad \cdots(3)$$

が成り立つ. (1) および (2) より, $(c_1, \sigma) \longrightarrow^* (\text{skip}, \sigma')$ が成り立ち, (3) より

$$\sigma'(R) = (r \times n) \times \boxed{(n - 1)!} = \sigma(R) \times n!$$

が成り立つ.

以上より, 命題 (A) が示された.

□

問題 III

次のプログラムについて以下の問に答えよ. ただし, m, n は正の整数であるとする.

$M := m; N := n; R := 1; X := 1;$
while $X \leq N$ **do** $(R := R \times M; X := X + 1)$

(i) 上のプログラムが停止する理由を述べよ.

解答例 1:

プログラムに含まれる唯一の while 文が停止することを言えばよい. while 文の本体 ($R := R \times M; X := X + 1$) を実行するたびに N は変化せず, X は1ずつ増加する. したがって, $N - X$ は, $N - X \geq -1$ の範囲で単調に減少するので, 上のプログラム中の while 文は必ず停止する.

解答例 2: while 文の本体 ($R := R \times M; X := X + 1$) を実行するたびに N は変化せず, X は 1 ずつ増加する. したがって, ループの条件判定時の X の値が, well-founded relation $\{(x, y) \mid y < x \leq n + 1\}$ に関して単調減少する. ゆえに, while 文は必ず停止し, プログラム全体も停止する.

(ii) while 文の条件判定時に常に成り立つ性質（ループ不変条件）を述べよ。

$$R = m^{X-1} \wedge X \leq N + 1 \wedge N = n$$

(iii) (ii) の結果を用いて、プログラムの停止状態における R の値が m^n であることを示せ.

(ii) より, 停止時には,

$$R = m^{X-1} \quad \cdots (1)$$

$$X \leq N + 1 \quad \cdots(2)$$

$$N = n \quad \cdots (3)$$

が成り立つ.

また、停止時には while の条件は偽なので、

$$X > N \quad \cdots (4)$$

が成り立つ.

(2), (3), (4) より, $X = N + 1 = n + 1$. ゆえに, (1) より, $R = m^{n+1-1} = m^n$ が成り立つ.