期末レポート課題

以下のいずれかの課題（複数可，得点は各々の問ごとに異なる）について，その解答をレポートで提出せよ．〆切は 8 月 7 日（金）昼 12:00 まで（メール `watanabe@is.titech.ac.jp` もしくは渡辺の郵便ポスト（西８号館エントランス直後の左手））

課題群１（復習課題）

以下の問題群（これまでの宿題や講義の復習となる問題群）に対し解答せよ.（注：これまでの成績が 70 点以下の人が 70 点合格を目指すための課題である．何問解いてももよいが成績が 70 点以上になった時点で採点は省略するので了承して欲しい．過去のプリントが必要な場合には，どの問題を解答したいかを指定した上で参考資料を渡辺まで請求して下さい.）

1. 定理 2.1 における定数 c_M がどのような値になるのかの見積もりを示す（考え方が十分わかる程度で十分；本当に厳密なものでなくてもよい）.（配点：〜10 点）

2. Suppose we have, for some problem P, a randomized algorithm `A` that answers correctly with prob. 1 to any positive instance (i.e., an instance for which the answer is 'yes' w.r.t. P) and answers correctly with prob. $\geq 1/2$ to any negative instance (i.e., an instance for which the answer is 'no' w.r.t. P). On the other hand, suppose that we also have an algorithm `B` that answers correctly with prob. $\geq 1/2$ to any positive instance and answers correctly with prob. 1 to any negative instance. We assume that the time complexity of both algorithms is $T(\ell)$ for instances of size ℓ. By using these two algorithms, design a randomized algorithm `C` that does not make any mistake, and Explain the time complexity of `C` (5 points).

3. $f = \Omega(g)$ を「$g = O(f)$ となること」と定義している．この意味での $f = \Omega(g)$ の定義を論理式で書き下してみよ．その上で，教科書（配布プリント）p.56 で説明している Ω-型下界との関係について述べよ.（配点：5 点）

4. ある問題 X が TIME$[\ell^2]$ に入らないことを示すには，具体的に何を示せばよいかを述べよ.（配点：5 点）

5. 決定問題とは，与えられた問題例に対して，答えが Yes もしくは No となる問題のことである．一方，もっと一般的に，何らかの条件を満たす解を求める問題を解探索問題という．一般に，解探索問題に対しては，それと似た時間計算量を持つ決定問題を定義することができる．その一例を，ある関数 f の計算で考えてみよう．

   関数 f として，任意の n に対し，$\{0,1\}^n$ から $\{0,1\}^n$ への関数を考える．つまり，$f(0110) = 1010$ というように，4 ビットも二進列を 4 ビットの二進列に対応付ける関数である．与えられた $x \in \{0,1\}^*$ に対し，この関数 f の値を求める問題が f に対する解探索問題とみなすことができる．

   この関数 f の多項式時間時間計算可能性を特徴付ける決定問題 F を定義せよ．具

体的には，$F \in \mathrm{P}$ ならば，f の値を計算することが多項式時間計算可能であることを示せるような問題が F である．そのような F を定義し，それが確かに f の多項式時間計算可能性を特徴付けていることを示せ.（配点：〜10 点）

6. 原始プログラムのコード化法を，コード長について解析できる程度，厳密に定義し，コード長を行数などから評価せよ．行数以外にコード長の評価に必要なパラメータ（定数とはできない値）は使ってもよい.（配点：〜10 点）

7. 制限レジスタ長を l としたとき，与えられた原始プログラム P の 1 ステップは $O(|P|l)$ 時間で模倣できる，とプリントでは説明されている（定理 4.1 の前）．なぜ，$|P|$ や l に比例するような時間がかかるのだろうか？説明せよ.（注：プリント中の $O(|P|l)$ は大ざっぱすぎて，実際には $O(|P|+l)$ 時間でも模倣は可能である.）（配点：5 点）

8. 仮に定理 4.1 よりよい模倣が可能で，$\mathrm{eval}(P, x, t, l)$ を $O(|P|t)$ で模倣できたとしよう（ただし，十分大きな定数で $t \geq c|x|$ の場合）．この場合，どのような階層定理を証明することができるだろうか？証明も含めて論ぜよ.（配点：〜10 点）

9. 3COLOR 問題を 3SAT 問題に多項式時間還元する方法とその正当性を示せ.（配点：〜10 点）

課題群 2（先進課題）

講義では省略した先進的なテーマについて勉強し解説して欲しい.（資料が必要だと思われるので取り組む場合には請求して下さい.）

1. 次のような問題を線形計画問題という.

   線形計画問題 LP
   入力： n 変数からなるベクトル $\mathbf{x} = (x_1, ..., x_n)$ に対する m 個の制約不等式 $A\mathbf{x} \leq \mathbf{b}$, ならびに目的関数 $c(\mathbf{x}) = \mathbf{c} \cdot \mathbf{x}$ を決めるコスト係数ベクトル $\mathbf{c}$.
   出力： $\max\{\, c(\mathbf{x}) \,:\, A\mathbf{x} \leq \mathbf{b} \,\}$.

   この問題は判定問題ではないが，それと同等（多項式時間の意味で）の難しさを持ち，クラス NP に入ることを容易に示すことのできる判定問題を定義することができる．その判定問題を示せ．また，その判定問題は coNP 問題でもある．その事実を示せ.（注：実は線形計画問題は多項式時間で計算可能である．その事実は知られていない，という想定のもとで解答せよ．なお，この問についての参考資料は自分で探すことができるはず.）（配点：〜30 点）

2. 次のグラフ同型問題 Graph Isomorphism Problem は，NP-完全かどうかがまだ確定していない問題である．もちろん，NP には入るが，実は co-AM（co-NP の乱択版クラス）にも入るため，多分 NP-完全ではないだろうと予想されている．$\mathrm{GI} \in \text{co-AM}$ であることを証明せよ.（**ヒント：**$G_1 \not\approx G_2$ のときに証拠のようなものを示せればよい．Set Lower Bound Protocol を用いる.）（配点：〜30 点）

グラフ同型問題 GI
入力： 無向グラフ $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$
質問： G_1 と G_2 が同型か？（記号では $G_1 \approx G_2$ か？）
すなわち，G_1 の頂点名を適当に並べ替えると G_2 と同じグラフになるか？

3. 講義で説明したように，多項式時間で安全な擬似乱数生成器の構成には，次の 3 つの重要な結果が使われている．そのどれでもよいので 1 つを選び，なぜ，それが成り立つのかをある程度詳しく解説せよ.（配点：〜30 点）
(1) weak one-way function ⇒ strong one-way function
(2) strong one-way function ⇒ strong pseudo random sequence generator
（注：ここでは講義で述べたように permutation を仮定してよい.）

4. 講義で説明したように，E の回路計算量下界 ⇒ BPP の脱乱択化の証明には，上記の議論に加え，worst-case hardness ⇒ average-case hardness の結果も必要となってくる．たとえば，E の問題（あるいは，もう少し簡単に #P の問題）に対して，この性質が成り立つことを解説せよ.（配点：〜30 点）

課題群３（研究課題）

チャレンジングな問題群．これが正解，というのがない場合もある．

1. 素数の（2 進数表現の）集合を PRIME と呼ぶことにする．集合 PRIME への所属判定問題は coNP 問題だが NP 問題でもあることを，我々の定義に基づいて示せ.（配点：〜30 点）

2. 現在，一般に知られている階層定理では $\mathrm{TIME}(t_1(\ell)) \subsetneq \mathrm{TIME}(t_2(\ell))$ を示すには，$t_2(\ell) \neq O(t_1(\ell)\log(t_1(\ell)))$ のような条件が必要である．しかし，限定的な計算モデルであれば，たとえば $t_2(\ell) \neq O(t_1(\ell)\log\log(t_1(\ell)))$ のような条件でも，差が示せる可能性もある．まず，現在の計算モデル（たとえば我々の原始計算機械・原始プログラムによる計算モデル）では，どこに証明の難しさがあるかを論じ，その上で，どのように制限したモデルを考えれば，より小さな差に対する階層定理定理が示せるかを述べよ.（配点：〜30 点）

3. 定理 5.2 の時間階層定理における下界を，強い意味での下界に修正した時間階層定理を証明せよ.（配点：〜30 点）

4. ○○-完全問題でおもしろい問題を選び，その問題の完全性の証明を丁寧に示せ.（配点：〜20 点）