宿題 #10

以下の問いについて解答せよ．〆切は次回（7 月 17 日）の授業終了後（授業前にメールで解答しても構わない）．

課題内容：

1. チェルノフ上界（下記）を証明せよ.（配点：5 点）

【チェルノフ Chernoff の不等式】
任意の ε（ただし $0 < \varepsilon < 1$）に対し，

$$\begin{aligned} \Pr[\ X > (1+\varepsilon)\mu\ ] &\leq \exp(-\mu\varepsilon^2/3) = \exp(-np\varepsilon^2/3), \\ \Pr[\ X < (1-\varepsilon)\mu\ ] &\leq \exp(-\mu\varepsilon^2/2) = \exp(-np\varepsilon^2/2). \end{aligned}$$

期末レポート課題（予告）

以下のいずれかの課題（複数可，得点は各々の課題ごとにことなる）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））

1. これまでの宿題の中の問題群（来週リスト配布）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.）

2. ○○-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）

3. 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．GI $\in$ 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．講義でも少しふれた Set Lower Bound Protocol を用いてよい；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？

4. 講義で説明したように，E の回路計算量下界 $\Rightarrow$ BPP の脱乱択化の証明は，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．

(1) computationally hard problem $\Rightarrow$ weak one-way function

(2) weak one-way function $\Rightarrow$ strong one-way function
(3) strong one-way function $\Rightarrow$ strong pseudo random sequence generator

5. その他