主なレポート課題の例（07/10 配布）

問 16. 或るデータ処理の計算量について考える。データを半分に分けてそれぞれについて処理し、それを合わせて結果を得ることが出来るが、合わせる時にデータ数に比例した計算量が必要だとする。このとき、N 個のデータに対する計算量は、$O(N \log N)$ であることを示せ。

問 17. $N \times N$ 行列の行列式を求める計算の計算量は、N について如何程か考える。但し、各成分の大きさについては考慮する必要はなく、四則演算をそれぞれ全て 1 回として数えて良いとする。（勿論、各成分の大きさも考慮しても良い。）

(1) 「全ての置換に亙って N 個の成分の積に置換の符号を掛けて足す」という明示公式を用いるとどうか。

(2) しかし上の方法は計算量が大き過ぎて適切でない。掃出し法を用いると計算量を減らすことが出来る。掃出し法による計算量は如何程か。（ヒント：多項式時間）

問 18. 十進 n 桁の整数 a, b の最大公約数 $d := \gcd(a, b)$ を互除法で計算するとき、必要な割算の回数は $O(n)$ であることを示し、O-constant を適切に評価せよ。即ち、或る定数 $C > 0$ が存在して Cn 回以内で済むことを示し、C が実際にはどの程度小さく取れるか評価せよ。（ヒント：k 回の割算を必要とする整数の組のうちの最小のものを考えよ。）

問 19. 自然数 e の二進展開を $e = e_0 + e_1 \cdot 2 + e_2 \cdot 2^2 + \cdots + e_k \cdot 2^k$ $(e_i = 0, 1)$ とする。

(1) 自然数 m, N に対し、$m^e \bmod N$ を高速に計算するアルゴリズムを記述し、何回の掛算および N で割った余りの計算で行なえるか考察せよ。

(2) そのアルゴリズムを実装せよ。

問 20. 複数テープチューリングマシンと単テープチューリングマシンとの計算量の違いについて考える。

(1) $f : \boldsymbol{N} \longrightarrow \boldsymbol{R}_{>0}$ を $f(n) \geq n$ であるような関数とする。言語 A を計算量 $O(f)$ で判定する決定性 2 テープチューリングマシンが存在するならば、言語 A を計算量 $O(f^2)$ で判定する決定性単テープチューリングマシンが存在することを示せ。

(2) 言語 A が決定性 2 テープチューリングマシンで多項式時間で判定されることと、言語 A が決定性単テープチューリングマシンで多項式時間で判定されることとは、同値である。（即ち、問題の計算量が多項式時間であることは、計算モデルとして用いるチューリングマシンが 2 テープであるか単テープであるかには依らない。）

問 21. $\Sigma = \{a, b\}$ を alphabet とする言語 $A = \{a^k b^k | k \in \boldsymbol{N}\}$ を考える。

(1) データ長 n に対し 線型時間 $O(n)$ の計算量で判定する決定性 2 テープチューリングマシンを構成せよ。

(2) データ長 n に対し n^2 より真に小さいオーダー（即ち $o(n^2)$）の計算量で判定する決定性単テープチューリングマシンを構成せよ。

問 22. 互いに素な 2 整数 a, b に対し、$ax + by = 1$ となる $x, y \in \boldsymbol{Z}$ を求めるアルゴリズム（Euclid の互除法拡張版）を実装せよ（プログラムを作成せよ）。

問 23. 多くの数値データを大きさの順に並べ替える操作（並べ替え・ソーティング）のアルゴリズムについて調べ、その計算量などについて論ぜよ。

問 24. 長桁乗算に関する高速フーリエ変換 (Fast Fourier Transform) について調べ、その計算量などについて論ぜよ。

問 25. 素数判定のアルゴリズムについて調べ、その計算量などについて論ぜよ。

問 26. 素因数分解のアルゴリズムの二次篩法 (Quadratic Sieve) について調べよ。（他のアルゴリズムでも良いが、これが原理が一番簡単。）

問 27. その他、具体的な数理問題について、それを解く効率的なアルゴリズムやその計算量、およびその実装について論ぜよ。

レポート提出について

- 締切：**2017 年 8 月 2 日 (水)20 時頃**まで
- 内容：配布プリントのレポート課題の例のような内容、及び授業に関連する内容で、授業内容の理解または発展的な取組みをアピールできるようなもの
- 分量：プリントのレポート課題を全部提出する必要はなく、問題の重さによって適宜判断して数問取り組めば良い。内容に関して意欲的な取組みを望む。