主なレポート課題の例 (続き) (01/13 配布)

問 14. 集合 X が可算 (enumerable) であるとは、自然数全体の集合 $\boldsymbol{N}$ との間に全単射 $X \to \boldsymbol{N}$ が存在することをいう。また、単射 $X \to \boldsymbol{N}$ が存在するとき、X が高々可算であると言う。

(1) 高々可算集合の高々可算個の合併集合が再び高々可算であることを示せ。
(2) 高々可算集合の有限部分集合全体の成す集合が再び高々可算であることを示せ。
(3) 可算集合の部分集合全体の成す集合 (冪集合) が可算でないことを示せ。(ヒント: 対角線論法)

問 15. 有限集合 Σ を alphabet とする言語で、チューリングマシンで認識できないものが存在することを、以下の手順で示せ。

(1) チューリングマシンの厳密な定式化を記述せよ。
(2) チューリングマシンの総数が可算個であることを示せ。
(3) 有限集合 Σ を alphabet とする言語の総数が可算でないことを示せ。
(4) 有限集合 Σ を alphabet とする言語で、チューリングマシンで認識できないものが存在することを示せ。

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。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。)

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。)

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. $\Sigma = \{a, b\}$ を alphabet とする言語 $A = \{a^k b^k | k \in \boldsymbol{N}\}$ について、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 21. 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 22. 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 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. 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 25. 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。)

レポート締切: **2011 年 2 月 7 日 (月)20 時頃**まで

内容: 配布プリントのレポート問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