2023 年度大学院博士前期課程入学試験

大阪大学大学院工学研究科
電気電子情報通信工学専攻

専門科目試験問題
（情報通信工学コース）

（実施時間　１４：００ ～ １６：００）

【注　意　事　項】

１．問題用紙はこの表紙や白紙を除いて１０ページある．解答開始の指示があるまで開いてはいけない．解答開始後，落丁や不鮮明な箇所等があった場合は，手を挙げて監督者にその旨を伝えること．

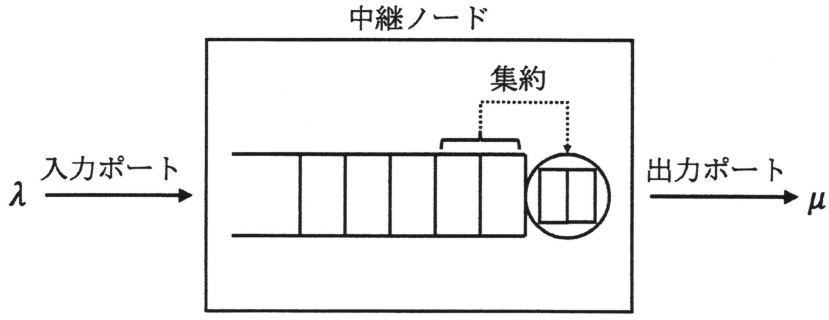
２．試験問題は，「通信ネットワーク」，「情報理論」，「信号処理」，「論理回路と計算機システム」，「データ構造とアルゴリズム」，及び，「情報セキュリティ」の全部で６題あり，この順番に綴じられている．このうち，３題を選択し解答すること．

３．解答開始前に，別紙の「専門科目試験問題選択票」に記載の注意事項も読んでおくこと．

４．問題用紙は持ち帰ってもよい．

【通信ネットワーク】解答は，黄色の解答用紙に記入すること．

以下の図に示すようなルータ等の中継ノードの性能を，待ち行列モデルを用いて評価することを考える．中継ノードは，単一の入力ポート，無限大の容量を持つ単一のバッファおよび単一の出力ポートを備えているとする．パケットは到着率 $\lambda > 0$ のポアソン過程に従って入力ポートから到着し，バッファ内の最後尾に蓄積される．その後，バッファ内の先頭から順に２個ずつのパケットの組が選ばれ，１個の新たなパケットへと集約された後，出力ポートより送出されるとする．ただし，バッファ内のパケットが１個以下の場合には，２個のパケットがバッファに蓄積されるまで，パケットの集約および送出は行われないものとする．パケットの集約にかかる時間は無視できるものとし，集約されたパケットの 1 ビット目が出力ポートより送出されてから最後のビットが送出されるまでの時間は，平均 $1/\mu\,(\mu > \lambda/2)$ の指数分布に従うとする．また，集約されたパケットを２個のパケットとして数えるとき，中継ノード内に n 個 $(n = 0, 1, \ldots)$ のパケットが存在する場合に，中継ノードは状態 n であると言うことにする．さらに，中継ノードが状態 n である定常状態確率を p_n とする．このとき，以下の問いに答えよ．



(i)　この待ち行列モデルの状態遷移速度図を示せ．ただし，$n = 0, 1, 2, 3$ における状態間の推移が分かるように示すこと．

(ii)　$p_n\,(n = 0, 1, \ldots)$ に関する平衡方程式を示せ．

(iii)　$P(z) = \sum_{n=0}^{\infty} p_n z^n$ とする．問い（ii）の結果を利用して，$P(z)$ が以下で表されることを示せ．

$$P(z) = \frac{(z+1)(p_0 + p_1 z)}{-2\rho z^2 + z + 1}$$

ただし，$\rho = \frac{\lambda}{2\mu} < 1$ とする．

(iv)　$-2\rho z^2 + z + 1 = 0$ となる z を求めよ．この結果と，$|z| < 1$ の範囲で $|P(z)| < \infty$ であることを利用し，p_1 を p_0 および ρ を用いて表せ．

(v)　問い（iii）および問い（iv）の結果を利用して，p_0 が以下で与えられることを示せ．

$$p_0 = \frac{3 - \sqrt{8\rho + 1}}{4}$$

専門用語の英訳

待ち行列モデル：	queueing model
入力ポート：	input port
バッファ：	buffer
出力ポート：	output port
到着率：	arrival rate
ポアソン過程：	Poisson process
パケット：	packet
定常状態確率：	steady state probability
指数分布：	exponential distribution
状態遷移速度図：	state transition rate diagram
平衡方程式：	balance equation

【情報理論】 解答は，桃色の解答用紙に記入すること．

図1に示すように，二つの受信器を有する通信路を考える．送信アルファベットを $X=\{0,1\}$ とし，その送信符号 0 および 1 は等確率に送信される．一方の受信アルファベットを $Y=\{0,1\}$ とし，送信符号とは異なる符号が確率 p で受信される．また，もう一方の受信アルファベットを $Z=\{0,1,E\}$ とし，二元符号 0 および 1 の他に消失符号 E が含まれる．消失符号 E が受信される確率は，各送信符号に対して e である．以下の問いに答えよ．解答には答えだけでなく，その導出過程も示すこと．なお，エントロピー，条件付きエントロピー，相互情報量の単位はビットとせよ．

(i) Y のエントロピー $H(Y)$ を求めよ．

(ii) Z のエントロピー $H(Z)$ を求めよ．

(iii) X に対する Z の条件付きエントロピー $H(Z|X)$ を求めよ．

(iv) X と Z の相互情報量 $I(X;Z)$ を求めよ．

(v) Y に対する Z の条件付きエントロピー $H(Z|Y)$ を求めよ．

(vi) Y と Z の相互情報量 $I(Y;Z)$ を求めよ．

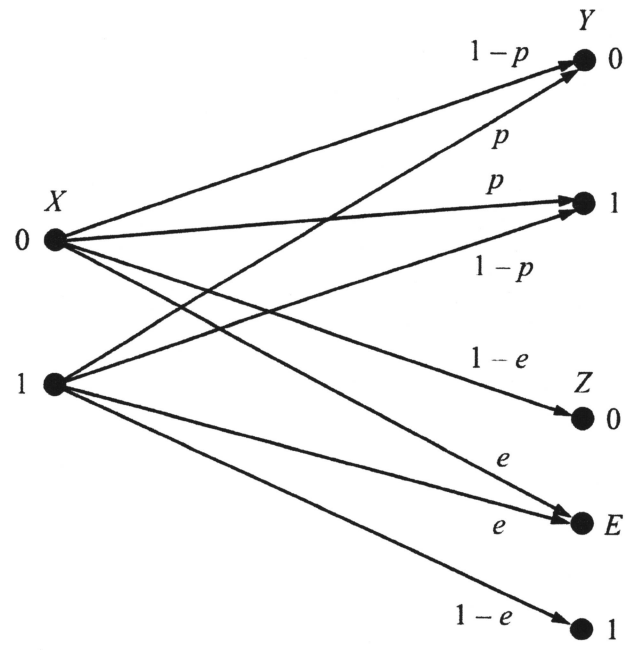


図1

専門用語の英訳

アルファベット：alphabet

エントロピー：entropy

条件付きエントロピー：conditional entropy

相互情報量：mutual information

【信号処理】 解答は，だいだい色の解答用紙に記入すること.

1. 離散時間信号 $x[n]$ （n は整数）の離散時間フーリエ変換 $X(\Omega)$ を以下のように与える．ただし，Ω は正規化角周波数であり，j は虚数単位とする.

$$X(\Omega) = \sum_{n=-\infty}^{\infty} x[n]e^{-j\Omega n}$$

以下の問いに答えよ．なお,

$$\delta[n-a] = \begin{cases} 1 & n = a \\ 0 & n \neq a \end{cases}$$

とする．ただし， a は整数である.

(i) 以下の離散時間信号 $x_1[n]$ の離散時間フーリエ変換 $X_1(\Omega)$ を求めよ．ただし，α は実数かつ $0 < \alpha < 1$ とする.

$$x_1[n] = \alpha^{n-1} \sum_{m=1}^{\infty} \delta[n-m]$$

(ii) 以下の離散時間信号 $x_2[n]$ の離散時間フーリエ変換 $X_2(\Omega)$ を求めよ．ただし，M を正の整数とする.

$$x_2[n] = \sum_{m=-M}^{M} \delta[n-m]$$

2. 周期 N の離散時間複素信号 $x[n]$ (n は整数) を 1 周期だけ取り出し，離散フーリエ変換を行うことを考える．このときの離散フーリエ変換 $X[k]$（k は整数）を以下のように与える.

$$X[k] = \sum_{n=0}^{N-1} x[n]\, {W_N}^{kn} \qquad (1)$$

なお，N を 2 のべき数，j を虚数単位とし，W_N は $W_N = e^{-j\frac{2\pi}{N}}$ で与えられる複素数とする．また，N 点の離散時間信号 $x[n]$ の離散フーリエ変換を N 点 DFT と呼ぶ.

(i) 式 (1) は以下のように行列表現できる.

$$\begin{pmatrix} X[0] \\ X[1] \\ \vdots \\ X[N-1] \end{pmatrix} = \begin{pmatrix} {W_N}^{0\cdot 0} & {W_N}^{0\cdot 1} & \cdots & {W_N}^{0\cdot(N-1)} \\ {W_N}^{1\cdot 0} & {W_N}^{1\cdot 1} & \cdots & {W_N}^{1\cdot(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ {W_N}^{(N-1)\cdot 0} & {W_N}^{(N-1)\cdot 1} & \cdots & {W_N}^{(N-1)\cdot(N-1)} \end{pmatrix} \begin{pmatrix} x[0] \\ x[1] \\ \vdots \\ x[N-1] \end{pmatrix}$$

上記の行列に基づいて，N 点 DFT を行うとする．最小の複素乗算の回数を求めよ．ここでは，${W_N}^{kn}$ は与えられているものとする．また，行列演算中に重複した複素乗算があったとしても，使いまわさずに個別に数え上げることとする.

(ii) $x[n]$ を n が偶数番目の信号 $x_e[n] = x[2n]$ と奇数番目の信号 $x_o[n] = x[2n+1]$ に分解する．それぞれの $N/2$ 点 DFT の結果を $X_e[k]$, $X_o[k]$ とする．$x[n]$ の N 点 DFT である $X[k]$ を $X_e[k]$ と $X_o[k]$ を用いて表せ．

(iii) 以下のアルゴリズムに従い，高速フーリエ変換（FFT）を行う．なお，N 点 DFT を FFT を用いて実施することをN 点 FFT と呼ぶ．

> $x[n]$ を n が偶数番目の信号と奇数番目の信号に分割し，それぞれに $N/2$ 点 DFT を行った後に，バタフライ演算を行う．これを再帰的に繰り返し，離散フーリエ変換をバタフライ演算に分解する．

このアルゴリズムを用いて，4 点 FFT をバタフライ演算に分解することを考える．再帰繰り返しの過程で現れる DFT を全てバタフライ演算に分解した場合の高速フーリエ変換をフローグラフを用いて可視化せよ．図 1 に，バタフライ演算を行うフローグラフの例を示す．例では，バタフライ演算への入力が x_1 と x_2 であり，出力が y_1 と y_2 である．フローに重みを記載することで，フローへの入力が定数倍される．ただし，値が1のフローには重みを図に記載しなくても良い．

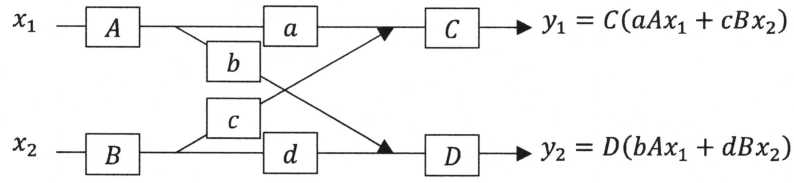


図 1

(iv) 問い (iii) で定義したアルゴリズムに従う高速フーリエ変換により N 点 FFT を行うときに必要な複素乗算回数を L_C とする．ここで，C は $C = \log_2 N$ と定義する．L_C と L_{C-1} の関係を求めよ．また，L_C を N を用いて示せ．

(v) 256 点 FFT を問い (iii) で定義したアルゴリズムに従う高速フーリエ変換を用いて実行する．演算内の 4 点 DFT は，バタフライ演算でなく，問い (i) の演算により，直接求めるとする．256 点 FFT を行うときに必要な複素乗算回数を求めよ．なお，4 点 DFT を問い (i) に基づいて計算する際に，重複した複素乗算があった場合はその結果を使いまわして良いとする．

専門用語の英訳	
離散時間信号	discrete time signal
離散時間フーリエ変換	discrete time Fourier transform
離散フーリエ変換	discrete Fourier transform
高速フーリエ変換	fast Fourier transform
バタフライ演算	butterfly computation
フローグラフ	flow graph

【論理回路と計算機システム】 解答は，水色の解答用紙に記入すること．

計算機システム内での小数の表現について，以下の各問いに答えよ．

(i) 数の固定小数点表示について具体例を用いて説明せよ．ただし表す数は正の数のみを考えればよい．

(ii) 符号を含めて 64 ビットの固定小数点表示で，Avogadro 定数 6.022×10^{23} を表現できるか．理由とともに答えよ．

(iii) 固定小数点表示で正の数を表現した場合，2^n の乗算や除算はビット列の操作で実現可能である（n は自然数）．具体的にこれらがどう実現できるかを n を用いて説明せよ．ただし，オーバーフローやアンダーフローは考えなくてよい．

(iv) 固定小数点表示と比べた際の浮動小数点表示のメリットを答えよ．

(v) 浮動小数点表示では，数は，符号，指数，仮数を用いて表現される．IEEE754 での単精度浮動小数点表示（32 ビット）では，数は，符号 1 ビット，指数部 8 ビット，仮数部 23 ビットをこの順に上位ビットから並べて表現される．このとき数 A の値は次の式で表される．

$$A = (-1)^s \ (1.m)_2 \ 2^{e-\alpha}$$

ここで，$(\ )_2$は 2 進数を表す記号であり，s は符号ビット，e は指数部が表す 10 進数である．α は指数部を常に正にするための定数（バイアス）で $\alpha = 127$ である．m は仮数部のビット列である．仮数を 2 進数で表現したうえで上式のとおりに正規化し，最上位桁の 1 を隠しビットとして除いたものが m である．

このとき，A が表現できる正の最小の数と，正の最大の数を，この 32 ビットのビット列でそれぞれ示せ．ただし，$e = 0$ および $e = 255$ は，特殊な数（ゼロ，無限大，正規化されていない数など）を表すのに使われるため，ここでは用いないこととする．ビット列は 4 桁ごとに空白で区切って書くこと．同じビット値が連続する部分は，例えば「以降は 0 が 16 桁連続する」のように，省略してその値と桁数を示せばよい．

(vi) 問い(v)で示した，正の最小の数と正の最大の数の値の範囲は，$2^p \leq A < 2^q$ で表される．p と q に入る整数をそれぞれ導出過程とともに示せ．

(vii) 10 進数値 11.8125 を，IEEE754 の単精度浮動小数点表示（32 ビット）で表せ．導出過程も示すこと．ビット列は 4 桁ごとに空白で区切って書き，同じビット値が連続する部分は，省略してその値と桁数を示せばよい．

専門用語の英訳

固定小数点	fixed point	指数	exponent
符号	sign	仮数	mantissa
乗算	multiplication	単精度	single precision
除算	division	正規化	normalization
オーバーフロー	overflow	隠しビット	hidden bit
アンダーフロー	underflow	バイアス	bias
浮動小数点	floating point		

【データ構造とアルゴリズム】　解答は，青色の解答用紙に記入すること．

1. ハッシュ表はキーと値の組を効率的に参照するためのデータ構造である．ハッシュ表を実装する方法の一つに配列と連結リストを用いる方法がある．長さ $L > 1$ の配列を用意し，配列の各セルにはそれぞれ異なる連結リストの先頭のアドレスを格納しておく．ただし，各連結リストは初期状態では空である．また，キーを 1 から L の間の整数に変換するハッシュ関数 h を用意する．キー k と値 v の組 (k, v) をハッシュ表に挿入する際には，配列の $h(k)$ 番目の連結リストに格納された値それぞれと v とを比較する．そして，連結リスト内に v と同じ値がなければ連結リストに v を挿入する．以降ではハッシュ関数 h として任意のキー k に対して確率 p_i で $h(k) = i$ $(1 \leq i \leq L)$ を返す関数を考える．ただし $p_i \geq 0, \sum_{i=1}^{L} p_i = 1$ である．以下の文章についての問い (i), (ii), (iii), (iv), (v) に答えよ．

> ハッシュ関数 h を用いて，すでにハッシュ表に相異なるランダムな T 個のキーと値の組 $\{(k_t, v_t)\}_{t=1}^{T}$ が挿入されているとする．このとき配列の i 番目の連結リストの長さの期待値は Tp_i となることがわかっている．このハッシュ表に新しくランダムなキーと値の組 (k, v) を挿入することを考える．ただし (k, v) はハッシュ表には存在しない，つまり $(k, v) \neq (k_t, v_t), \forall t$，とする．このとき (k, v) の挿入の平均時間計算量は $O(\boxed{\text{A}})$ である．ここで O はランダウの記号である．

(i) ハッシュ関数 h として任意のキーに対して等確率で 1 から L のそれぞれの値を返す関数，つまり $p_i = \frac{1}{L}, \forall i$ を考える．$\boxed{\text{A}}$ に入る式を述べよ．

(ii) ハッシュ関数 h として任意のキーに対して確率 θ で 1 を返し，2 から L のそれぞれの値を等確率で返す関数，つまり $p_i = \begin{cases} \theta & \text{if } i = 1 \\ \frac{1-\theta}{L-1} & \text{if } i \neq 1 \end{cases}$ を考える．ただし $0 \leq \theta \leq 1$ である．$\boxed{\text{A}}$ に入る式を述べよ．

(iii) 問い (i), (ii) のハッシュ関数を比較し，挿入の平均時間計算量におけるそれぞれの優劣とその理由を述べよ．

(iv) ハッシュ関数 h として一般の $p_1, p_2, \ldots, p_L$ を考える．$\boxed{\text{A}}$ に入る式を述べよ．

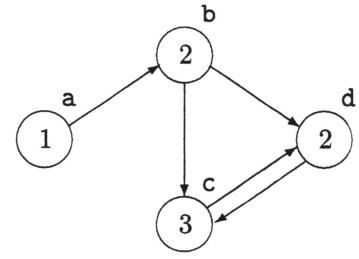
(v) $L = 2$ の場合を考える．挿入の平均時間計算量が最小となる p_1, p_2 とその導出過程を述べよ．

2. 有向グラフを表す隣接行列について，以下の問い (i), (ii), (iii) および続く問い (iv), (v) に答えよ．

$$A = \begin{array}{c} \begin{matrix} \texttt{a} & \texttt{b} & \texttt{d} & \texttt{c} \end{matrix} \\ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array} \begin{matrix} \texttt{a} \\ \texttt{b} \\ \texttt{d} \\ \texttt{c} \end{matrix}$$

行・列のアルファベットは頂点 ID を表す．

(a) 隣接行列



○は頂点，→ は有向辺，○の中の数字はラベル，
○の右上のアルファベットは頂点 ID を表す．

(b) 有向グラフ

図 1: 隣接行列と有向グラフ

図 1(a) の行列 A は，図 1(b) の有向グラフの頂点のラベルが昇順となるように行・列方向に頂点を並べた隣接行列の一例である．ただし複数の頂点が同じラベルを有する場合には，それらの頂点に対応する行と列の並び順は任意とする．隣接行列の (i, j) 要素は i 行目に対応づけられた頂点から j 列目に対応づけられた頂点へ至る有向辺が存在するときに 1，存在しないときに 0 とする．問い (i), (ii), (iii) に答えよ．

(i) 図 1(a) の行列 A 以外に，図 1(b) の有向グラフを表現し，かつ各頂点に対応する行と列が頂点のラベルについて昇順に並んだ相異なる隣接行列をすべて列挙せよ．

(ii) 図 1(b) の頂点 c のラベルを 1 に変更したグラフを図示せよ．さらに，そのグラフについて各頂点に対応する行と列が頂点のラベルについて昇順に並んだ相異なる隣接行列をすべて列挙せよ．

(iii) 図 1(b) のグラフの全頂点が同一のラベルを有する場合に，各頂点に対応する行と列が頂点のラベルについて昇順に並んだ相異なる隣接行列の総数を示せ．

一般の有向グラフを考える．有向グラフの各頂点には 1 つのラベルが与えられているとする．頂点の総数を n，ラベルの総種類数を ℓ とする．ラベル i を有する頂点の総数を n_i とすると，$n = \sum_{i=1}^{\ell} n_i$ が成立する．有向グラフの隣接行列を，各頂点に対応する行と列が頂点のラベル i について昇順に並んだ行列で表すものとする．ただし複数の頂点が同じラベルを有する場合には，それらの頂点に対応する行と列の並び順は任意とする．問い (iv), (v) に答えよ．

(iv) 相異なる隣接行列の総数が最大になる有向グラフ G_1 を考える．このとき，n_i を用いて G_1 を表す相異なる隣接行列の総数を示せ．

(v) 全頂点が同一のラベルを有する有向グラフを考える．このとき，相異なる隣接行列の総数が最大になる有向グラフを G_2 とする．n を用いて G_2 を表す相異なる隣接行列の総数を示せ．

専門用語の英訳

ハッシュ表	hash table
キーと値の組	key-value pair
配列	array
連結リスト	linked list
セル	cell
ハッシュ関数	hash function
平均時間計算量	average-case time complexity
ランダウの記号	Landau symbol
等確率	equal probability
有向グラフ	directed graph
隣接行列	adjacency matrix
頂点	vertex
有向辺	directed edge
昇順	ascending order
列挙	enumerate

【情報セキュリティ】 解答は，緑色の解答用紙に記入すること．

RSA（Rivest Shamir Adleman）公開鍵暗号方式では，異なるランダムな 2 つの素数 p, q に対し，$n = pq$ 及び $(p-1)$ と $(q-1)$ の最小公倍数 L を用いて $1 < e < L$ かつ L と互いに素な整数 e を求め，e, n を公開鍵とする．また，$ed = 1 \pmod{L}$ かつ $1 < d < L$ を満たす整数 d を生成し，これを秘密鍵とする．ここで，$ed = 1 \pmod{L}$ は $ed - 1$ が L で割り切れることを意味する．平文 $m\ (0 < m < n)$ の暗号文 c は，公開鍵 e, n を用いて，$c = m^e \pmod{n}$ により生成する．一方，暗号文 c の平文は，公開鍵 n 及び秘密鍵 d を用いて，$m' = c^d \pmod{n}$ により復号する．RSA 公開鍵暗号方式について以下の問いに答えよ．

(i) 平文 m と整数 n は互いに素なとき，RSA 公開鍵暗号方式の暗号文 $c = m^e \pmod{n}$ に対して，その復号結果 $m' = c^d \pmod{n}$ が元の平文 m と一致することを示せ．

(ii) 素数 $p = 11,\ q = 7$，及び公開鍵 $e = 23$ に対して RSA 公開鍵暗号方式の秘密鍵 d を計算せよ．

(iii) 素数 $p = 7,\ q = 13$，秘密鍵 $d = 5$ となる RSA 公開鍵暗号方式において，暗号文 $c = 8$ を復号せよ．

(iv) 2 つの公開鍵を $(n, e_1) = (91, 5)$ と $(n, e_2) = (91, 11)$ とする．同じ平文 m に対する e_1 を用いた暗号文を $c_1 = 31$ とし，e_2 を用いた暗号文を $c_2 = 73$ とする．この時，c_1 と c_2 を入手した攻撃者が秘密鍵を使わずに平文 m を復号する方法と，復号結果を示せ．ここで，$31^{-2} = 25 \pmod{91}$ であることを用いて良い．

専門用語の英訳

公開鍵暗号化方式	public-key encryption scheme
素数	prime number
最小公倍数	least common multiple
互いに素	prime to each other
公開鍵	public key
秘密鍵	secret key
復号	decryption
平文	plaintext
暗号文	ciphertext