2022 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１２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，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．中継ノードへは，2 個ずつのパケットの組が，到着率 λ のポアソン過程に従って到着するものと仮定する．中継ノードに到着したパケットは，入力ポートを通ってバッファ内の最後尾に蓄積され，バッファ内の先頭パケットから順に 1 個ずつ出力ポートより送出される．また，あるパケットの 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 $1/\mu\ (\mu > 2\lambda)$ の指数分布に従うとする．なお，バッファサイズは無限大であると仮定する．送信途中のパケットを含めて，n 個 $(n = 0, 1, \ldots)$ のパケットが中継ノードに存在するとき，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 $n\ (n = 0, 1, \ldots)$ 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.

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

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

$$P(z) = -\frac{\mu p_0}{\lambda z^2 + \lambda z - \mu}$$

(iv) 問い（iii）の結果を利用し，p_0 を λ および μ を用いて表せ.

(v) 定常状態における，送信中のパケットも含めた中継ノード内の平均パケット数を求めよ．また，得られた結果を，到着率が 2λ でサービス率が μ である M/M/1 待ち行列モデルの定常状態における平均系内客数と比較せよ.

専門用語の英訳

中継ノード：	intermediate node
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
サービス率：	service rate
平均系内客数：	average number of customers in the system

【情報理論】 解答は，桃色の解答用紙に記入すること.

1. 離散時刻 k $(k = 0,1,\cdots)$ において 2 元記号 0 および 1 を等確率で出力する記憶のない情報源を情報源 X とする．図 1 に示すように，情報源 X にフィルタ F を接続して得られる離散時刻 k での記号を $r_k \in \{0,1\}$ とする．情報源 X・フィルタ F・通信路 C の順番で接続した伝送システム 1（図 2(a)）と，情報源 X・通信路 C・フィルタ F の順番で接続した伝送システム 2（図 2(b)）のそれぞれにおいて，r_k とは異なる記号が受信されたとき，誤りが生じたと考える．

   フィルタ F は，図 3 に示すように，1 ビット排他的論理和と 1 ビットレジスタから構成され，レジスタの初期値は 0 とする. 離散時刻 k でのフィルタ F の入力記号を $u_k \in \{0,1\}$, 出力記号を $v_k \in \{0,1\}$ とすると，$v_k = v_{k-1} \oplus u_k$ が成り立つ．ただし，$\oplus$は排他的論理和を表す．通信路 C では，図 4 に示すように，入力記号と同じ記号が出力される確率を $1-p$ とし，入力記号と異なる記号が出力される確率を p とする．ただし，$p < 0.5$ である．

   2 つの伝送システムについて以下の問いに答えよ.

(i) 伝送システム 1 において，誤りが生じる確率を求めよ.

(ii) 伝送システム 2 の各時刻において, 誤りが生じなかったときを状態 t_0 , 誤りが生じたときを状態 t_1 で表す．t_0 と t_1 の状態遷移図を示せ．遷移を表す矢印には，遷移確率も示すこと.

(iii) 伝送システム 2 において十分時間が経過したとき，誤りが生じる確率を求めよ.

(iv) 問い(i)，問い(iii)の結果を踏まえ，記号 r_k の情報を伝送するという目的に対して，伝送システム 1 と伝送システム 2 のどちらが適しているかを示し，その理由も説明せよ.

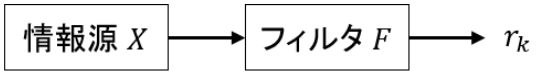

図 1：情報源 X とフィルタ F から発生する記号 r_k

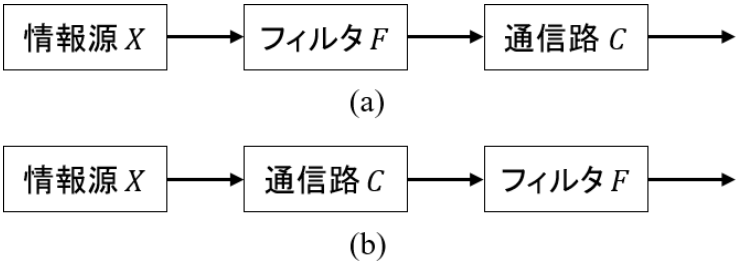

図 2：(a) 伝送システム 1 と (b) 伝送システム 2

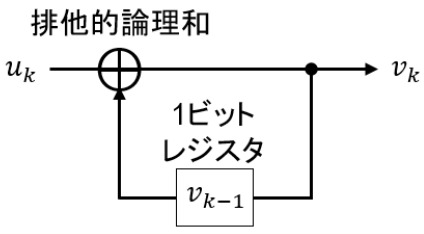

図 3：フィルタ F

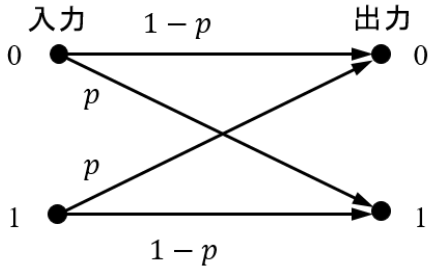

図 4：通信路 C

2. 情報記号 a，b，c，d をそれぞれ確率 $P(a)=\frac{1}{2}$，$P(b)=\frac{1}{4}$，$P(c)=\frac{1}{8}$，$P(d)=\frac{1}{8}$ で発生する記憶のない情報源について以下の問いに答えよ．解答に際して対数の計算が必要となる場合は，$\log_2 3 = 1.58$ を利用すること．

(i) 2 元瞬時符号を構成するとき，実現可能な最短平均符号長を求めよ．

(ii) 2 元ハフマン符号を構成し，その平均符号長を問い(i)で求めた最短平均符号長と比較せよ．

(iii) 3 元瞬時符号を構成するとき，実現可能な最短平均符号長を求めよ．

(iv) 3 元ハフマン符号を構成し，その平均符号長を問い(iii)で求めた最短平均符号長と比較せよ．

専門用語の英訳

排他的論理和	exclusive or
状態遷移図	state transition diagram
瞬時符号	instantaneous code
平均符号長	average code length
ハフマン符号	Huffman code

【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. 連続時間信号

$$x(t) \;=\; \frac{2}{T}\sum_{m=-\infty}^{\infty} p(t-mT) \quad \text{ただし} \quad p(t) \;=\; \begin{cases} t & (0 \leqq t < T) \\ 0 & (t < 0 \text{ または } T \leqq t) \end{cases}$$

について，以下の問いに答えよ．ただし，t は連続的な時刻を表す実数であり，m は任意の整数である．また，T は $t,\ m$ に依存しない定数であり，正の実数とする．

(i) $x(t)$ が周期信号であることを示し，その基本周期を求めよ．

(ii) $x(t)$ を図示せよ．

(iii) $x(t)$ をフーリエ級数に展開せよ．ただし，a, b, c を定数とする次の関係式

$$\int_a^b c^2 t e^{ct} dt \;=\; \Big[(ct-1)e^{ct}\Big]_a^b$$

を利用して良い．

(iv) エイリアシングを生じないように $x(t)$ をサンプリングしたい．それが可能であるならばサンプリング周波数をどのように設定すればよいかを，不可能であるならばその理由を，問い (iii) の結果に基づいて論ぜよ．

2. 入出力差分方程式

$$y[n] \;=\; x[n] \;+\; \frac{1}{6}y[n-2] \;+\; \frac{1}{3}y[n-4] \;-\; x[n-5]$$

で表される因果的な離散時間信号処理システム L について，以下の問いに答えよ．ただし，n は離散的な時刻を表す整数であり，$x[n],\ y[n]$ はそれぞれ L に対する入力信号，出力信号を表す．

(i) z 変換により定義される L の伝達関数を $H(z)$ とする．$H(z)$ を求めよ．

(ii) 問い (i) の $H(z)$ について，その極と零点を求め，図示せよ．

(iii) L の有界入力有界出力安定性を論ぜよ．

(iv) L への入力 $x[n] = \cos(\Omega_0 n)$ に対し，出力が任意の n について $y[n] = 0$ となるような Ω_0 を全て求めよ．ただし，Ω_0 は n に依存しない定数であり，$0 \leqq \Omega_0 < \pi$ を満たす．

専門用語の英訳	
連続時間信号	continuous-time signal
周期信号	periodic signal
基本周期	fundamental period
フーリエ級数	Fourier series
エイリアシング	aliasing
サンプリング	sampling
サンプリング周波数	sampling frequency
入出力差分方程式	input-output difference equation
因果的	causal
離散時間信号処理システム	discrete-time signal processing system
入力信号	input signal
出力信号	output signal
z 変換	z transform
伝達関数	transfer function
極	pole
零点	zero
有界入力有界出力安定性	bounded-input bounded-output stability

【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.

1. 計算機の命令に関する以下の文章に関して，問い(i)から(vi)に答えよ.

> 現在の大部分の計算機システムは，ノイマン型と呼ばれるアーキテクチャに基づいている．ノイマン型計算機は，実行される命令が主記憶装置にデータとして格納される点が特徴である．命令は，その種類を表す命令コード部と，対象データ（オペランド）の存在場所を指定するアドレス部からなる．
>
> 命令の設計方針として，CISC (Complex Instruction Set Computer) と RISC (Reduced Instruction Set Computer) が知られている．このうち RISC では，プロセッサの命令セットを単純化し，ロードストアアーキテクチャや固定長命令を採用することで，処理性能の向上を図っている．

(i) 下線部の方式の名称を答えよ.

(ii) オペランドの内容が主記憶にある場合, その内容は直接指定やレジスタ間接指定などのアドレス指定モードで指定できる．直接指定とレジスタ間接指定のそれぞれを，アドレス部に書かれる内容を明記したうえで,「主記憶」「アドレス」という語を用いて説明せよ.

(iii) アドレス指定モードのインデックス指定は，配列を表現するのに用いられる．この場合，命令語のアドレス部に書かれる内容と, インデックスレジスタと呼ばれるレジスタの内容が保持する情報を, それぞれ答えよ.

(iv) ロードストアアーキテクチャでは, 主記憶装置へアクセスするのはロード命令とストア命令だけである．この設計の利点について説明せよ.

(v) 固定長の命令セットを設計する際の問題に，大きい定数値の扱いがある．例えば，命令長が 32 ビットである場合，命令コード部が存在することから，32 ビットで表される定数値を一命令のオペランド部では表現できない. このことから, 一命令でそのような定数値をレジスタに代入できない. 固定長の命令セットにおいて，このような代入を行う方法を説明せよ.

(vi) RISC に基づくプロセッサで処理性能が向上する理由について，パイプライン処理の観点も含めて説明せよ.

2. 状態数が 4 ビットのアップカウンタの論理回路を設計することを考える．アップカウンタとは 1 時刻毎にその出力値が 1 ずつ増えるカウンタである．ここでは，回路の状態変数の値が 2 進数表現で回路の出力値になるとする. 具体的には, q_3, q_2, q_1, q_0 を 0 または 1 の値を取る 2 値の状態変数とし，これらの組 $q_3q_2q_1q_0$ でこのカウンタの状態を表現する．初期状態に対応する $q_3q_2q_1q_0$ の値は 0000 であり，1 時刻後における $q_3q_2q_1q_0$ の値は 0001 となる．また，$q_3q_2q_1q_0$ が 1111 となった次の時刻は初期状態に戻るものとする．この時，問い(i)から(iii)に答えよ.

(i) 現在時刻の状態変数 q_3, q_2, q_1, q_0 に対応して，次の時刻の状態を $q_3^+, q_2^+, q_1^+, q_0^+$ でそれぞれ表現することを考える．$q_3^+, q_2^+, q_1^+, q_0^+$ に関する論理関数のカルノー図を，q_3, q_2, q_1, q_0 を用いてそれぞれ書け．カルノー図の各欄は空白にせず，必ず埋めること.

(ii) 問い(i)で解答したカルノー図に基づき，$q_3^+, q_2^+, q_1^+, q_0^+$ の論理式を最小積和形でそれぞれ書け.

(iii) より一般的に，状態数が n ビットのアップカウンタの論理回路を考える．ここで，n は自然数とする．この回路の現在時刻の状態を n 個の状態変数 $q_{n-1} \dots q_1 q_0$ の組で表現する．出力値と初期状態などの設定は 4 ビットの場合と同様とする．この時，次の時刻の状態変数 $q_{n-1}^+, \dots, q_1^+, q_0^+$ の論理式を $q_{n-1}, \dots, q_1, q_0$ を用いて表現したい．ここでは，カウンタの桁上げ条件に着目する．i 桁目の状態変数 q_i^+ $(0 < i \leq n-1)$ の値が 1 をとる条件を説明し，それに基づいた q_i^+ の論理式と導出過程を示せ．補助変数を適当に定義し，用いても良い.

専門用語の英訳

ノイマン型	von Neumann architecture
命令コード	operation code
オペランド	operand
アドレス	address
プロセッサ	processor
ロードストアアーキテクチャ	load store architecture
固定長命令	fixed-length instruction
主記憶	main memory
レジスタ	register
直接指定	direct addressing
レジスタ間接指定	register indirect addressing
アドレス指定モード	addressing mode
インデックス指定	index addressing
パイプライン	pipeline
ビット	bit
アップカウンタ	up-counter
カウンタ	counter
状態変数	state variable
状態	state
カルノー図	Karnaugh map
論理関数	logical function
論理式	logical formula, logical expression
最小積和形	minimum sum-of-products form

【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. アルゴリズム A のすべての入力 x の集合を X とする．以下の (A)〜(E) の空欄の内容を答えよ．
   - アルゴリズム A がある入力 $x \in X$ を処理してその出力を得るまでに要する実行時間を，A の入力 x に関する時間計算量と言い $t(x)$ で表すとする．このとき，$\max_{x \in X} t(x)$ を A の (A) と言う．アルゴリズム A に $x \in X$ が入力される確率を $p(x)$ と表すとき，$\sum_{x \in X} p(x)t(x)$ を (B) と言う．
   - アルゴリズム A への入力 $x \in X$ の規模の大きさを表すパラメータ $n \geq 0$ が存在し，A の入力 x に関する時間計算量が $t(x) = f(n)$ なる関数 f で表されるとき，ある一定の値 $n_0 \geq 0$ と正の定数 $c > 0$, n の関数 g が存在して，任意の $n \geq n_0$ について $f(n)$ (C) $cg(n)$ が成立するならば，A の漸近時間計算量は $g(n)$ のオーダーであると言い，ランダウの記号 O を用いて $O(g(n))$ と表す．
   - アルゴリズム A が部分正当性を有するとは，任意の (D) について A が間違った出力を生じないことである．また，アルゴリズム A が完全正当性を有するとは，A が部分正当性を有することに加えて，A が有限時間で (E) しない入力 x が X に含まれないことである．

2. N 個の行列 $A_0, A_1, \ldots, A_{N-1}$ が与えられたときに，これらの行列積 $A_0A_1 \ldots A_{N-1}$ を計算する問題を考える．ここで各行列 A_i は p_i 行 p_{i+1} 列の行列であり，行列のサイズを $p_i \times p_{i+1}$ と表記することとする．また，行列積の計算順序を括弧を用いて表記することとする．例えば $(A_0(A_1A_2))$ であれば，A_1 と A_2 の積を最初に計算し，次に A_0 とその結果との積を計算する．以下の問いに答えよ．
   (i) 一般に，大きさが $p \times q$ の行列 A と大きさが $q \times r$ の行列 B の積 AB の漸近時間計算量は $O(pqr)$ である．ここで O はランダウの記号である．$N = 4$ のとき行列積 $(((A_0A_1)A_2)A_3)$ の漸近時間計算量を述べよ．
   (ii) $N = 4$ のとき $p_0 = 5, p_1 = 3, p_2 = 2, p_3 = 4, p_4 = 2$ とする．このとき，$(((A_0A_1)A_2)A_3)$ と $(A_0(A_1(A_2A_3)))$ とのどちらの漸近時間計算量が小さいか，その理由とともに述べよ．
   (iii) 行列積 $A_0A_1 \ldots A_{n-1}$, $A_nA_{n+1} \ldots A_{N-1}$ をそれぞれ漸近時間計算量が最小になる順番で計算したときの漸近時間計算量を $O(T_1), O(T_2)$ とする．このとき行列積 $((A_0A_1 \ldots A_{n-1})(A_nA_{n+1} \ldots A_{N-1}))$ の最小の漸近時間計算量を述べよ．
   (iv) プログラム 1 は行列積の最小の漸近時間計算量を動的計画法により計算するプログラムである．[1] を埋めてプログラムを完成させよ．
   (v) プログラム 1 の 20 行目で表示される `T[0][N-1]` の値を述べよ．

プログラム 1: 行列積の最小の漸近時間計算量の計算（C 言語）

```
1  #include<stdio.h>
2  #define INF 10000000
3  #define N 5
4
5  int main() {
6    int p[N+1] = {3, 5, 2, 3, 4, 3};    // 行列のサイズの配列 p_0, p_1, ..., p_N
7    int T[N][N];
8    int i, j, k, t;
9    for (i=0; i<N; ++i) T[i][i] = 0;    // 対角要素の初期化：行列1 個の場合の計算量は 0
10   for (k=2; k<=N; ++k) {              // k 個の行列積の漸近時間計算量の計算
11     for (i=0; i<N-k+1; ++i) {         // i は行列積の左端の行列のインデックス
12       T[i][i+k-1] = INF;              // 暫定の漸近時間計算量を十分大きな数で初期化
13       for (j=1; j<k; ++j) {           // j は行列積を区切る箇所のインデックス
14         // ((A_iA_{i+1} ... A_{i+j-1})(A_{i+j}A_{i+j+1} ... A_{i+k-1})) の最小の漸近時間計算量
15         t = [ 1 ] + p[i] * p[i+j] * p[i+k];
16         if (t < T[i][i+k-1]) T[i][i+k-1] = t;    // 暫定の漸近時間計算量の更新
17       }
18     }
19   }
20   printf("NumberOfOperations=%d\n", T[0][N-1]); // 行列積の最小の漸近時間計算量を表示
21 }
```

専門用語の英訳

時間計算量	time complexity
漸近時間計算量	asymptotic time complexity
ランダウの記号	Landau symbol
部分正当性	partial correctness
完全正当性	total correctness
有限時間	finite time
行列	matrix
行列積	matrix product
計算順序	calculation order
括弧	parenthesis
動的計画法	dynamic programming
暫定	temporary

【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 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 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 $(0 \leq m < n)$ 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 m 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) $p = 5, q = 11$ を用いて，公開鍵 $e = 7$ に対する秘密鍵 d を求めよ．

(ii) 問い(i)の公開鍵を用いたときの平文 $m = 3$ の暗号文 c を求めよ．

(iii) 問い(i)の公開鍵を用いたときの暗号文 $c = 5$ の平文 m を復号せよ．

(iv) RSA 公開鍵暗号化方式では，平文空間も暗号文空間も環 $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ である．平文 m と暗号文 c の関係は，写像 $\mathrm{Enc} : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ を用いて $c = \mathrm{Enc}(m)$ と書ける．ここで，$\mathrm{Enc}(m_1 \cdot m_2) = \mathrm{Enc}(m_1) \cdot \mathrm{Enc}(m_2)$ のとき Enc は乗法に関して準同型写像であるという．問い(i)の公開鍵を用いたときの平文 3 と平文 7 の暗号文 42 と 28 が与えられたとき，写像 Enc の準同型性を利用して，公開鍵 e を用いずに別の平文の暗号文を構築せよ．

(v) 直接攻撃とは，秘密鍵 d を持たない攻撃者が公開鍵だけから秘密鍵を求める攻撃である．公開鍵 $n = 65$，$e = 11$ から，直接攻撃で秘密鍵 d を求めよ．

(vi) 問い(v)で求めた秘密鍵を用いて，暗号文 $c = 11$ を復号せよ．

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
準同型写像	homomorphism
直接攻撃	direct attack