2021 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，「通信方式」，「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７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．

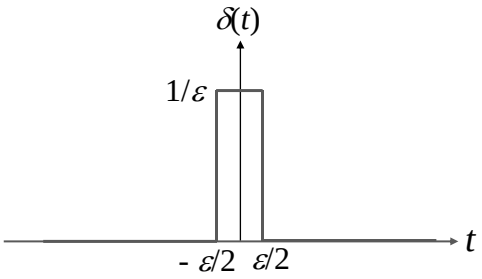
４．問題用紙は持ち帰ってもよい．

【通信方式】解答は，赤色の解答用紙に記入すること.

実時間関数 $g(t)$に対して，周期 T_s の周期インパルス列 $s(t)$でサンプリングすることを考える．$s(t)$が次式で与えられるとき，以下の問いに答えよ.

$$s(t) = \sum_{n=-\infty}^{\infty} \delta(t - nT_s)$$

ただし$\delta(t)$はディラックのデルタ関数であり，図 1 で定義されるものとする．また t は時刻，n は整数である.



ただし$\varepsilon > 0$であり，
$\varepsilon \to 0$である

図 1

(i) $\delta(t)$のフーリエ変換を導出せよ.

(ii) $s(t)$のスペクトル $S(f)$を導出すると共に，$S(f)$を図示せよ.

(iii) $g(t)$をサンプリングするとは，数学的には $g(t)$にサンプリング関数 $s(t)$を乗積することであるとするとき，サンプリングされた波形 $g_s(t)$は $g(t)$，$s(t)$を用いてどのように表されるかを示せ.

(iv) $g_s(t)$のフーリエ変換である $G_s(f)$は，$g(t)$のフーリエ変換である $G(f)$を用いてどのように表されるかを示せ. ただし $S(f)$については設問(ii)で導出した結果を用いよ.

(v) $G(f)$の形状を適当に設定し，それに対する $G_s(f)$のスペクトル形状を示せ. ただし，$G(f)$に含まれる最大周波数を f_{max} とし，スペクトルの図には f_{max} を明記すること．また $G_s(f)$を図示するにあたっては，$2f_{max} > 1/T_s$ を前提として記すこと.

専門用語の英訳

サンプリング	sampling
時間関数	time function
周期	cycle
周波数	frequency
スペクトル	spectrum
整数	integer
フーリエ変換	Fourier transform

【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，待ち行列システム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．パケットは到着率 λ のポアソン過程に従い，入力ポートより 1 つずつ中継ノードに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先着順に 1 パケットずつ出力ポートより送出される．ただし，バッファサイズは無限大とする．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 $1/\mu_1$ $(\mu_1 > \lambda)$ の指数分布に従うと仮定する．送信途中のものも含めて中継ノード内にパケットが存在する場合，中継ノードは通常状態である，と言う．

この中継ノードは，中継ノード内のパケット数が 0 になると直ちに通常状態からスタンバイ状態に移行し，さらに平均 $1/\mu_2$ $(\mu_2 > 0)$ の指数分布に従う待機時間後に，スタンバイ状態からスリープ状態へと移行する．ただし，スタンバイ状態およびスリープ状態中に中継ノードへパケットが到着した場合には，中継ノードは直ちに通常状態へ戻り，パケットの転送を開始するものとする．また，通常状態では E の電力を，スタンバイ状態では $E/2$ の電力をそれぞれ消費し，スリープ状態では電力消費はないものとする．

送信途中のパケットを含めて，n 個 $(n = 1, 2, \ldots)$ 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し，中継ノードが状態 n である定常状態確率を p_n とする．また，中継ノードのスタンバイ状態およびスリープ状態は，それぞれ状態 A および状態 B で表し，対応する定常状態確率を p_A および p_B とする．

このとき，以下の問いに答えよ．

(i)　この中継ノードを表す待ち行列システムの状態遷移速度図を示せ．

(ii)　p_n $(n = 1, 2, \ldots)$ および p_A, p_B に関する平衡方程式を示せ．

(iii)　p_n $(n = 1, 2, \ldots)$ および p_A, p_B を導出せよ．

(iv)　定常状態における，中継ノードでの平均消費電力を求めよ．

専門用語の英訳

中継ノード：	intermediate node
待ち行列システム：	queueing system
入力ポート：	input port
出力ポート：	output port
バッファ：	buffer
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
通常状態：	normal state
スタンバイ状態：	standby state
スリープ状態：	sleep state
状態遷移速度図：	state transition rate diagram
平衡方程式：	balance equation
消費電力：	energy consumption

【情報理論】 解答は，桃色の解答用紙に記入すること.

1. 立方体の各面に 1, 2, 3, 4, 5, 6 の目を有するサイコロと，表面，裏面を有するコインを同時に振ることを考える．サイコロの各目が出る確率は均等であり，コインは確率pで表，$1-p$で裏が出る．サイコロの出た目を表す確率変数をA，コインを振って表が出たら 0，裏が出たら 1 となる確率変数をBとする．XとYをそれぞれ$X=A+B$，$Y=A-B$を表す確率変数とするとき，以下の問いに答えよ．なお，エントロピー及び相互情報量の単位はビットとする．

(i) エントロピー$H(X)$，$H(Y)$を求めよ．
(ii) 条件付きエントロピー$H(B|X)$を求めよ．
(iii) 条件付きエントロピー$H(X|Y)$，$H(Y|X)$を求めよ．
(iv) 相互情報量$I(X;B)$を求めよ．
(v) 相互情報量$I(X;Y)$を求めよ．

2. 生起確率$P(c_1)=p_1$，$P(c_2)=p_2$，$P(c_3)=p_3$で情報記号c_1，c_2，c_3のいずれかを発生する記憶のない情報源を考える．以下の問いに答えよ．なお，通信路容量の単位はビットとする．また，解答には答えだけでなく，導出過程も示すこと．

(i) この情報源のエントロピーが$p_1=p_2=p_3=1/3$ のとき最大となることを証明せよ．
(ii) 各情報記号が雑音のない通信路を介して伝達されるとき，この通信路の通信路容量を求めよ．
(iii) 各情報記号が消失通信路を介して，確率ϵで消失，$1-\epsilon$で正しく伝達されるとき，この通信路の通信路容量を求めよ．

確率変数	random variable
エントロピー	entropy
相互情報量	mutual information
条件付きエントロピー	conditional entropy
生起確率	occurrence probability
情報記号	information symbol
通信路容量	channel capacity

【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. 線形かつ時不変な離散時間信号処理システム L_1, L_2 を図 1 のように縦続接続する場合を考える．縦続接続したシステム全体を L_3 とし，L_1, L_2, L_3 のインパルス応答をそれぞれ $h_1[n]$, $h_2[n]$, $h_3[n]$ とする．ただし，n は離散的な時刻を表す整数である．以下の問いに答えよ．

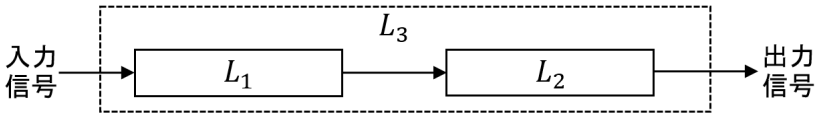


図 1: 線形時不変システムの縦続接続

(i) 一般に，離散時間における線形時不変システムが有界入力有界出力安定であるための必要十分条件を，インパルス応答 $h[n]$ を用いて答えよ．

(ii) $h_3[n]$ は $h_1[n]$ および $h_2[n]$ を用いてどのように表されるか．数式により示せ．

(iii) $h_1[n]$, $h_2[n]$ がともに問い (i) の条件を満たすとき，$h_3[n]$ もまた問い (i) の条件を満たすことを示せ．

(iv) L_1, L_2 がそれぞれ入出力差分方程式 $y[n] = x[n]-x[n-1]$ および $y[n] = x[n]+x[n-1]-y[n-2]$ により表されるとする．ただし $x[n]$, $y[n]$ は各システムに対する入力信号および出力信号を表す．L_3 の z 変換により定義される伝達関数を $H_3(z)$ とするとき，$H_3(z)$ を求め，さらに，その結果を基に L_3 の振幅特性および位相特性を求めよ．

2. 時刻を t 秒としたとき，地点 A から以下の信号 $x(t)$ を発する．

$$x(t) = \begin{cases} 0 & (t < 0) \\ 1 & (0 \leqq t \leqq 1) \\ 0 & (1 < t) \end{cases}$$

この信号は地点 A から別の地点 B まで以下のインパルス応答 $y(t)$ により伝播するものとする．

$$y(t) = \begin{cases} 0 & (t < 10) \\ 6 - 0.5t & (10 \leqq t \leqq 12) \\ 0 & (12 < t) \end{cases}$$

以下の問いに答えよ．

(i) 地点 A で発した $x(t)$ の立ち上がり部分が地点 B に初めて伝わる時刻を答えよ．

(ii) 地点 B において観測される信号 $z(t)$ を，$x(t)$ と $y(t)$ を用いた畳込み積分式で表せ．

(iii) 信号 $z(t)$ の振幅が最大になる時刻を理由と共に述べよ．

(iv) 問い (ii) の畳込み積分を計算し，信号 $z(t)$ を時刻 t の多項式で表せ．

専門用語の英訳	
線形	linear
時不変	time-invariant
離散時間信号処理システム	discrete-time signal processing system
縦続接続	cascade connection
インパルス応答	impulse response
線形時不変システム	linear and time-invariant (LTI) system
有界入力有界出力安定	bounded-input bounded-output stable
入出力差分方程式	input-output difference equation
入力信号	input signal
出力信号	output signal
z 変換	z transform
伝達関数	transfer function
振幅特性	amplitude response
位相特性	phase response
畳込み積分	convolution
多項式	polynomial

【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. 文字列パターン 101 を検出する回路を Mealy 型順序回路として実現することを考える．Mealy 型順序回路では，現在の状態と入力から出力が決定される．この回路への入力変数 x は，0 または 1 の値を取る 2 値変数とする．出力変数 z は，それまでの 3 入力が 101 である時に 1，それ以外で 0 の値を取る 2 値変数とする．入力文字の 0 と 1 は，そのまま入力変数 x の 0 と 1 に対応付けるものとする．例えば，文字列 110101 が 1 文字ずつこの回路に入力されると，対応して 000101 が 1 つずつ出力される．この時，以下の問いに答えよ．

(i) この回路の状態遷移図の一部が図 1 である．S_0 を初期状態とし S_0, S_1, S_2 の 3 状態を設定した．例えば，初期状態 S_0 で 1 がこの回路に入力されると，0 が回路から出力され，状態 S_1 に遷移する．まず解答用紙に図 1 を書き写し，これに追記して状態遷移図を完成させよ．なお，入力値と出力値の表記は凡例に従うこと．

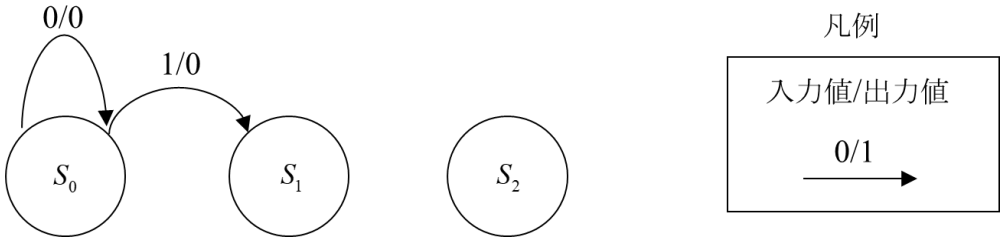


図 1　状態遷移図の一部

(ii) 問い(i)で作成した状態遷移図に従って，この回路の状態遷移表を作成する．まず，現在の状態を表現する状態変数 q_1, q_0，および，次の状態を表現する状態変数 q_1^+, q_0^+ を導入する．ここで，q_1, q_0 および q_1^+, q_0^+ はいずれも 0 または 1 の値を取る 2 値変数とする．次に，表 1 の「現在の状態」の列にある値を，$q_1 q_0$ にそれぞれ割り当てた．この時，表 1 の空欄 [1] から [12] に入る値をそれぞれ答えよ．

表 1　状態遷移表

	現在の状態 $q_1 q_0$	次の状態 $q_1^+ q_0^+$		出力 z	
		$x=0$	$x=1$	$x=0$	$x=1$
S_0	00	[1]	[4]	[7]	[10]
S_1	01	[2]	[5]	[8]	[11]
S_2	10	[3]	[6]	[9]	[12]

(iii) 問い(ii)で作成した状態遷移表に基づき，q_1^+, q_0^+ および z を q_1, q_0, x を用いて論理式で表すことを考える．まず，q_1^+, q_0^+ および z に関する論理関数のカルノー図をそれぞれ書け．ドントケアは記号 φ で示すこと．

(iv) 問い(iii)で解答したカルノー図に基づき，q_1^+, q_0^+ および z の論理式を最小積和形でそれぞれ示せ．

2. 問い 1 の回路を発展させ，入力する文字の種類を A から Z のアルファベット 26 文字に設定し，文字列パターン A[B-Z]A を検出する Mealy 型順序回路の設計を考える．ここで，記号 [B-Z] を B から Z の 25 文字のうちの任意の 1 文字を表現するものとする．この論理回路を設計するには，各アルファベットを，n 個の 0 または 1 の値を取る入力変数 $x_{n-1} \ldots x_1 x_0$ に対応づける必要がある．ただし，n は自然数とする．問い 1 と同様に，現在の状態変数 q_1, q_0 および $x_{n-1} \ldots x_1 x_0$ を用いて，次の状態変数 q_1^+, q_0^+ と出力変数 z の論理式を導きたい．この時，以下の問いに答えよ．この回路の状態遷移表は入力変数の部分を除いて表 1 と同じとすること．

(i) q_1^+, q_0^+, z を表す論理式で使う入力変数の数が最小となるように，各アルファベットと $x_{n-1} \ldots x_1 x_0$ との対応関係を工夫して設計せよ．

(ii) q_1^+, q_0^+ および z の論理式を，問い(i)において設計した入力変数と q_1, q_0 を用いた最小積和形でそれぞれ示せ．

専門用語の英訳

Mealy 型順序回路	Mealy machine
状態	state
状態変数	state variable
順序回路	sequential circuit
カルノー図	Karnaugh map
ドントケア	don’t care
状態遷移図	state transition diagram
状態遷移表	state transition table
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. n が 2 の累乗，すなわち $n = 2^{\ell}$ となる自然数 ℓ が存在するとし，S を n 個の相異なる整数から成る集合とする．S の各要素が配列 $s[i]$ $(i = 1, \ldots, n)$ に昇順で格納されている時，S から一様ランダムに取り出した整数 x が格納されている配列要素番号，すなわち $x = s[i]$ となる番号 i を探索する問題を考える．この時，以下の問いに答えよ．
   (i) $s[1]$ から $s[n]$ まで順番に $x = s[i]$ となる番号 i を探索する逐次探索を用いる場合，x と配列 $s[i]$ $(i = 1, \ldots, n)$ の比較回数の最大値と期待値を n を用いて表せ．
   (ii) 2 分探索を用いる場合，x と配列 $s[i]$ $(i = 1, \ldots, n)$ の比較回数の最大値と期待値を n を用いて表せ．なお，用いる 2 分探索の手順は以下の通りである．
      Step 1 $left = 1$ かつ $right = n$ と初期化する．
      Step 2 区間 $[left, right]$ の中央 $mid = \lfloor (left + right + 1)/2 \rfloor$ を求める．
      Step 3 もし $x < s[mid]$ であれば $right = mid - 1$ として Step 2 へ戻り，もし $x > s[mid]$ であれば $left = mid$ として Step 2 へ戻り，何れでもなければ $i = mid$ として終了する．
   ただし，$\lfloor \bullet \rfloor$ は $\bullet$ を超えない最大の整数に丸めることを表す．

2. 二分木において，指定した値 x と等しい値を持つノードが存在するか否かを判定する．ここでは木の探索方法として，**幅優先探索**，**深さ優先探索（行きがけ順）**，**深さ優先探索（帰りがけ順）**の 3 通りを考える．ただし，各ノードにおいて左の子ノードの方が右の子ノードよりも探索の優先順位が高いものとする．$x = 10$ として以下の問いに答えよ．

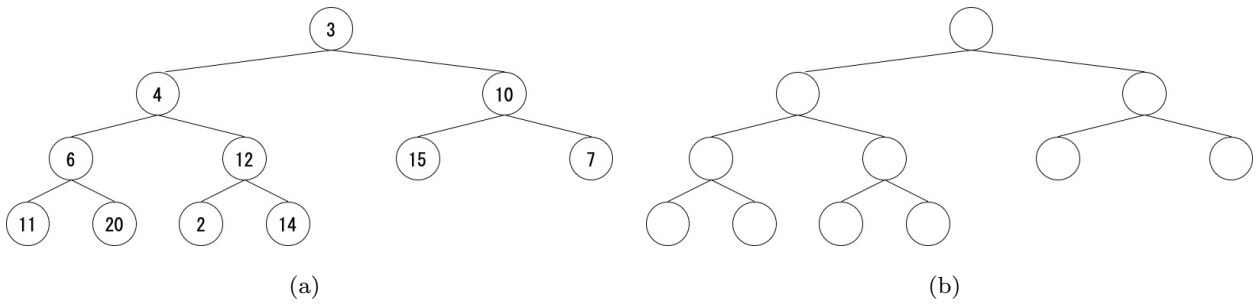


図 1: 二分木

   (i) 図 1(a) の二分木において**幅優先探索**を実行したときに，x との値の比較が行われる二分木のノードの値をその順番と共に示せ．
   (ii) 図 1(a) の二分木において**深さ優先探索（行きがけ順）**を実行したときに，x との値の比較が行われる二分木のノードの値をその順番と共に示せ．
   (iii) 図 1(a) の二分木において**深さ優先探索（帰りがけ順）**を実行したときに，x との値の比較が行われる二分木のノードの値をその順番と共に示せ．
   (iv) 図 1(b) を回答用紙に転記し，深さ優先探索（行きがけ順）による x との値の比較回数と比べて，幅優先探索による x との値の比較回数が **2 倍以上**になるように，転記した二分木の各ノードの値を埋めよ．さらにその場合に，深さ優先探索（行きがけ順），幅優先探索それぞれについて x との値の比較回数を述べよ．
   (v) 図 1(b) を回答用紙に転記し，深さ優先探索（行きがけ順）による x との値の比較回数と比べて，深さ優先探索（帰りがけ順）による x との値の比較回数が **10 倍以上**になるように，転記した二分木の各ノードの値を埋めよ．さらにその場合に，深さ優先探索（行きがけ順），深さ優先探索（帰りがけ順）それぞれについて x との値の比較回数を述べよ．

専門用語の英訳

累乗	repeated multiplication
昇順	ascending order
比較回数	number of comparisons
一様ランダム	uniform random
配列要素番号	array index number
逐次探索	sequential search
2 分探索	binary search
最大値	maximum value
期待値	expected value
二分木	binary tree
幅優先探索	breadth-first search
深さ優先探索（行きがけ順）	depth-first-search (preorder traversal)
深さ優先探索（帰りがけ順）	depth-first-search (postorder traversal)
優先順位	priority

【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．

1. RSA ディジタル署名方式では，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．一般には RSA ディジタル署名方式ではハッシュ関数を利用するが，ここではハッシュ関数を利用しない方式を考える．つまり，署名生成者は，平文 m（$1 < m < n$）と秘密鍵 d を用いて，$\sigma = m^d \pmod{n}$ により署名 σ を生成する．一方，署名検証者は，署名 σ，平文 m と公開鍵 n 及び e を用いて，$m = \sigma^e \pmod{n}$ を満たすとき，署名 σ は平文 m の正しい署名と判断する. RSA ディジタル署名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 $e = 3$ に対する秘密鍵 d を求めよ．

(ii) 問い(i)で求めた秘密鍵を用いて，平文 $m = 6$ の署名 σ を生成せよ．

(iii) 署名検証者が公開鍵 $n = 55, e = 3$ に対する平文 $m = 7$ とその署名 $\sigma = 3$ を入手したとき，署名 σ が平文 m の正しい署名であるか否かを答えよ．

2. 問い 1 で述べた RSA ディジタル署名の偽造とは，秘密鍵 d を持たない攻撃者が，平文 m^* に対する署名 σ^* を生成することを言う．ここで，公開鍵が $n = 85, e = 3$ であるとき，以下の問いに答えよ．

(i) 一般的選択平文攻撃とは，攻撃者が入手した平文と署名のペア (m, σ) を用いて，平文 $m^* \neq m$ に対する署名 σ^* を偽造することである．ここで，攻撃者が平文と署名のペア $(m, \sigma) = (8, 2)$を入手したとする．このとき，$m^* \neq m$ となる平文 m^* に対する署名 σ^* を偽造し，偽造できた平文と署名のペア (m^*, σ^*) を答えよ．なお，偽造の方法も記述せよ．

(ii) 適応的選択平文攻撃とは，攻撃者が偽造したい平文 m^* に対して，$m \neq m^*$ の任意の平文 m に対する署名 σ を入手できる状況において，平文 m^* の署名 σ^* を偽造することである．偽造したい平文を $m^* = 3$ とするとき，適応的選択平文攻撃で，平文 m^* の署名 σ^* を偽造せよ．なお，偽造の方法も記述せよ．

専門用語の英訳

ディジタル署名方式	digital signature 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
ハッシュ関数	hash function
平文	plaintext
署名	signature
偽造	forgery
一般的選択平文攻撃	generic chosen message attack
適応的選択平文攻撃	adaptive chosen message attack