平成 30 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２２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」，「光・電波工学」，「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」，「情報セキュリティ」，及び，「制御工学」，の全部で９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．

離散時刻 $k \in \{0, 1, 2, \cdots\}$ に，2 ビットから成る 4 元記号 $u_k \in \{00, 01, 10, 11\}$ を送信機から受信機へ無線伝送することを考える．このとき，各記号の生起確率 $\Pr[u_k = 00], \Pr[u_k = 01], \Pr[u_k = 10], \Pr[u_k = 11]$ は等しく 1/4 であるものとする．送信機側では，記号時間長 T 毎に，$kT \le t < (k+1)T$ の期間，次式の信号 $s(t)$ を記号 u_k に応じて生成する．

$$s(t) = x(t)\cos(2\pi f_c t) \qquad \cdots \text{式 (1)}$$

ここで，f_c は搬送周波数，t は時刻である．（搬送波の初期位相は 0 としていることに注意せよ．）また，$x(t)$ はベースバンド信号であり，次式で与えるものとする．

$$\begin{aligned} &u_k = 00 \text{ の場合，} x(t) = -3A \\ &u_k = 01 \text{ の場合，} x(t) = -A \\ &u_k = 10 \text{ の場合，} x(t) = +A \\ &u_k = 11 \text{ の場合，} x(t) = +3A \end{aligned} \qquad \cdots \text{式 (2)}$$

ただし，A は定数である．

受信機側では，次式の信号が受信されたものとする．

$$y(t) = s(t - t_0) + n(t) \qquad \cdots \text{式 (3)}$$

ここで，t_0 は送受信機間の時刻同期誤差である．また，$n(t)$ は雑音であり，次式で与えられる．

$$n(t) = n_I(t)\cos(2\pi f_c t) - n_Q(t)\cos(2\pi f_c t) \qquad \cdots \text{式 (4)}$$

ただし，$n_I(t)$ と $n_Q(t)$ はいずれも平均が 0，分散が σ^2 のガウス分布に従い，互いに独立な確率過程に従う実数のランダム変数である．

上記を前提とし，以下の問いに答えよ．

(i) 式 (1) と (2) の規則に従う変調方式の名称を答えよ．

(ii) 式 (3) の受信信号 $y(t)$ の同期検波を行った結果得られる信号を $\tilde{x}(t)$ とする．受信機側の発振器の周波数は $f_c + f_0$ であり，搬送周波数 f_c に周波数同期誤差 f_0 ($\ll f_c$) が加わったものが搬送波として再生されているものとする．また，同期検波に利用する低域通過フィルタは理想的なものが与えられているものとする．このとき，同期検波の動作原理を説明するとともに，同期検波出力 $\tilde{x}(t)$ を数式で示せ．

(iii) 問い (ii) において，時刻同期誤差と周波数同期誤差が存在しない場合 ($t_0 = 0, f_0 = 0$) と比較して，下記の場合に同期検波出力 $\tilde{x}(t)$ が，時刻 t の変化に応じてどのような振る舞いをするか説明せよ．

- 時刻同期誤差のみがある場合 ($t_0 \neq 0, f_0 = 0$),
- 周波数同期誤差のみがある場合 ($t_0 = 0, f_0 \neq 0$)

(iv) 受信機側で得られる送信記号の判定値を $\hat{u}_k$ とする．時刻同期誤差と周波数同期誤差が存在しない理想的な状況 ($t_0 = 0, f_0 = 0$) において，しきい値を用いてどのように判定を行えばよいか説明せよ．ただし，記号の判定は最適なしきい値によりなされるものとする．

(v) 問い (iv) の判定において，

・送信機で「00」が送られたときに，受信機で「00」と判定される確率 $\Pr\left[\hat{u}_k = 00 \,|\, u_k = 00\right]$ を求めよ．ただし，次式の誤差関数あるいは誤差補関数を用いて表現せよ．

$$\mathrm{erf}(a) = \frac{2}{\sqrt{\pi}} \int_0^a \exp\left(-b^2\right) db$$

$$\mathrm{erfc}(a) = 1 - \mathrm{erf}(a) = \frac{2}{\sqrt{\pi}} \int_a^\infty \exp\left(-b^2\right) db \qquad \text{・・・式 (5)}$$

専門英語の英訳

送信機	transmitter
受信機	receiver
搬送周波数	carrier frequency
雑音	noise
同期誤差	synchronization error
ガウス分布	Gaussian distribution
確率過程	stochastic process
同期検波	coherent detection
誤差関数	error function
誤差補関数	complementary error function

【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．

下図に示すように，交換機 A，交換機 B の間に c 本 $(c \geqq 1)$ の通信リンクがある電話交換システムについて考える．交換機 A に接続している電話機より，交換機 B に接続している電話機に対して通信要求が送られるとする．一つの通信要求に対して 1 本の通信リンクが使用されるものとし，通信要求発生時に使用されていない通信リンクが存在すれば通信が開始され，全ての通信リンクが使用されていればその通信要求は棄却される．通信が終了すると，その通信のために使用されていた通信リンクは開放される．

通信要求は，到着率 λ [1/sec] $(\lambda > 0)$ のポアソン過程に従って到着し，通信時間は平均 $1/\mu$ [sec] $(\mu > 0)$ の指数分布に従うと仮定する．また，$\rho = \lambda/\mu$ とする．k 本 $(k = 0, 1, \ldots, c)$ の通信リンクが使用されているとき，この電話交換システムは状態 k にあると呼ぶ．電話交換システムが状態 k である定常状態確率を p_k とする．

以下の問いに答えよ．

(i) この電話交換システムを表す待ち行列システムをケンドールの記号を用いて表せ．

(ii) この電話交換システムの状態遷移速度図を示せ．

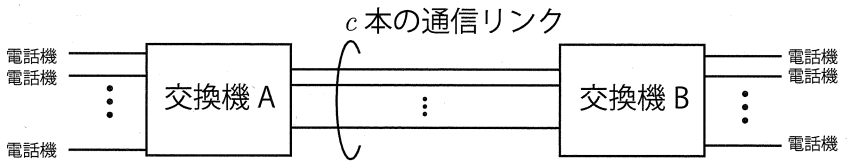
(iii) p_k が ρ，c，k を用いて次式で表されることを示せ．

$$p_k = \frac{\rho^k/k!}{\sum_{i=0}^{c} \rho^i/i!}$$

(iv) 通信リンク数が無限大であるとすると，この電話交換システムは $M/M/\infty$ 待ち行列システムで表現することができる．このとき，状態 m $(m = 0, 1, \ldots)$ である定常状態確率を q_m と表す．q_m を ρ，m を用いて表せ．

(v) p_c と q_n $(n = c, c+1, \ldots)$ には以下の関係があることを示せ．

$$p_c < \sum_{n=c}^{\infty} q_n$$



専門用語の英訳

交換機：	switch
通信リンク：	communication link
電話交換システム：	telephone switching system
電話機：	telephone
到着率:	arrival rate
ポアソン過程:	Poisson process
指数分布:	exponential distribution
定常状態確率:	steady state probability
待ち行列システム:	queueing system
ケンドールの記号:	Kendall's notation
状態遷移速度図:	state transition rate diagram

【光・電波工学】 解答は，灰色の解答用紙に記入すること．

図 1 に示すように，ビームスプリッタ（BS_1 と BS_2）とミラー（M_1 と M_2）から構成される干渉計に，パワー P_0 を有する波長 λ_0 の単一偏波光ビームを入力する．光ビームはビームスプリッタ BS_1 で 2 つの光路に分岐され，ミラー M_1 および M_2 を経て，ビームスプリッタ BS_2 で合波される．BS_2 から出力される光ビームのパワーをパワーメータ 1 とパワーメータ 2 で測定する．なお，干渉計内の 2 つの光路の長さは厳密に等しいものとする．また，ビームスプリッタおよびミラーでの偏波回転は生じない．ミラーは光ビームを全反射させ，損失は生じない．ビームスプリッタは図 2 に示す動作に従う．すなわち，入力された光ビームの複素電界振幅 E_1 および E_2 が，パワーが半分となるように分岐され，出力ポートから複素電界振幅 E_3 と E_4 の光ビームが出力される．この際，反射光については位相が 90°回転する．なお，光ビームの伝搬方向に垂直な平面における分布は考えず，伝搬によるビーム広がりや損失は生じないものとする．空間の屈折率を 1 として，以下の問いに答えよ．

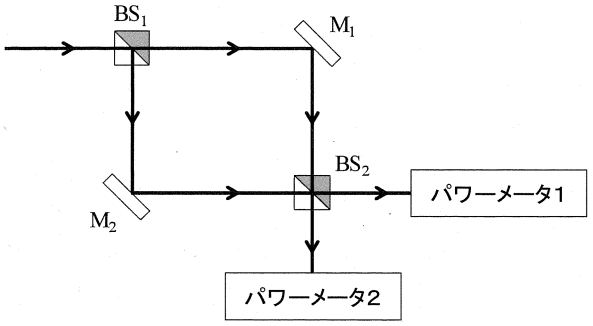


図 1

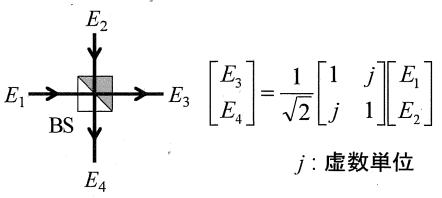


図 2

(i) パワーメータ 1 とパワーメータ 2 で測定されるパワーをそれぞれ，P_0 を用いて表せ．ただし，導出過程を示すこと．

(ii) ミラー M_2 とビームスプリッタ BS_2 の間の光路中に，図 3 に示すような屈折率 n のくさび状透明ガラスを挿入する．ただし，n は実数であり，$n > 1$ とする．ガラスの損失と表面における反射は無視し，光ビームに対するガラス表面の傾斜の影響も無視できるものとする．光路に対して垂直方向の挿入位置を制御することで，ガラス内を光ビームが伝搬する距離 L を調整できる．L が大きくなるようにガラスを徐々に挿入していくと，パワーメータ 1 とパワーメータ 2 の測定値が等しくなった．このときのガラス内を光ビームが伝搬する距離 L_0 を，λ_0 と n を用いて表せ．

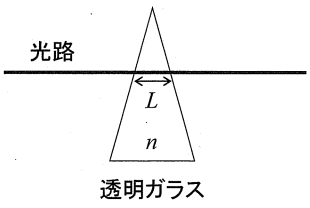


図 3

(iii) 問い(ii)において，透明ガラス内を光ビームが伝搬する距離を $L = L_0$，光ビームの波長を $\lambda_0 + \Delta\lambda$ とし

た時のパワーメータ１とパワーメータ２で測定されるパワーを，P_0，λ_0，$\Delta\lambda$を用いて表せ．なお，$\lambda_0 >> \Delta\lambda$として，必要であれば以下の近似式を用いよ．

$$(1+\Delta\lambda/\lambda_0)^{-1} \approx 1-\Delta\lambda/\lambda_0$$

(iv) 問い(ii)において，透明ガラス内を光ビームが伝搬する距離を $L(t) = L_0[2 - \cos(\Omega t)]$とゆっくり変化させた．なお，$t$ は時刻である．このときのパワーメータ１とパワーメータ２で測定されるパワーを，P_0，Ω，t を用いて表せ．なお，パワーメータの応答速度は Ω に対して十分高速である．

(v) 問い(iv)において，ビームスプリッタ BS_1 とミラーM_2 の間に，図４に示すような屈折率 n のガラスを挿入した．このガラス内を光ビームが伝搬する距離は $2L_0$ であり，ガラスの強度透過率をαとする．ただし，L_0 は問い(ii)で求めた距離，また $0 < \alpha < 1$ である．このときのパワーメータ１とパワーメータ２で測定されるパワーを，P_0，α，Ω，t を用いて表せ．

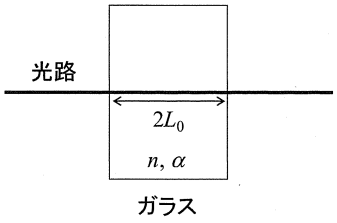


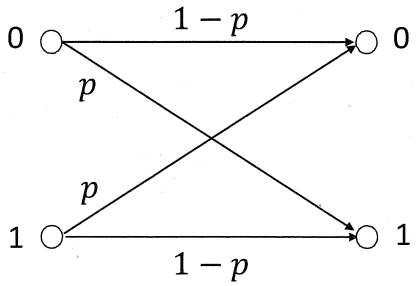
図４

専門用語の英訳

ビームスプリッタ：beam splitter
ミラー：mirror
干渉計：interferometer
パワー：power
波長：wavelength
単一偏波：single polarization
光ビーム：optical beam
光路：optical path
パワーメータ：power meter
複素電界振幅： complex amplitude
強度透過率： intensity transmittance

【情報理論】 解答は，桃色の解答用紙に記入すること．

等確率で情報ビット$x \in \{0,1\}$を出力する情報源を考える．この情報源から出力される長さkの情報ビット系列が，符号アルファベット$\{0,1\}$からなる長さnの符号語に変換されて伝送されたとき，受信側は，受信アルファベット$\{0,1\}$からなる受信語を，送信された情報ビット系列に復号する．ただし符号語は，下図に示すビット誤り率$p(0 \leq p \leq 0.5)$の2元対称通信路を通して伝送され，受信側ではpの値は未知とする．



$k = 1$のとき，情報ビット系列をN回繰り返した長さ$n = N$の符号語に変換されるとする．このような符号について問い(i)から(iii)に答えよ．

(i) 復号の際，伝送時に生じた1ビットの誤りを正しく訂正できる最小のNを求めよ．

(ii) 問い(i)のNを用いたとき，1ビットの誤りを正しく訂正する復号方法を説明せよ．また，110000010111 が受信されたとき，送信された情報ビット系列を推定せよ．

(iii) $N = 1$ 及び$N = 3$のとき，それぞれ符号化率を求め，復号誤り率をpの多項式で表せ．また，$p = 0.1$ のときの復号誤り率を求めよ．

$k = 4$のとき，情報ビット系列$(x_1x_2x_3x_4)$が，$c_1 = x_1 \oplus x_2 \oplus x_3$，$c_2 = x_2 \oplus x_3 \oplus x_4$，$c_3 = x_1 \oplus x_3 \oplus x_4$を用いて符号語$(x_1x_2x_3x_4c_1c_2c_3)$に変換されるとする．ただし，$\oplus$は排他的論理和である．このような符号について問い(iv)から(vii)に答えよ．

(iv) 伝送時に生じる誤りが何ビットまで正しく訂正可能か答えよ．

(v) 問い(iv)で答えたビット数までの誤りを正しく訂正する，検査行列を用いた復号方法を説明せよ．また，1011110 が受信されたとき，送信された情報ビット系列を推定せよ．

(vi) 符号化率を求め，復号誤り率をpの多項式で表せ．ただし，pの4次以上の項は無視してよい．この多項式を用いて，$p = 0.1$のときの復号誤り率を求めよ．

(vii) 復号した情報ビット系列におけるビット誤り率をpの多項式で表せ．ただし，pの4次以上の項は無視してよい．この多項式を用いて，$p = 0.1$のときの復号した情報ビット系列におけるビット誤り率を求めよ．

専門用語の英訳

情報源	information source
情報ビット系列	information bit sequence
アルファベット	alphabet
符号語	code word
受信語	received word
復号	decoding
ビット誤り率	bit error rate
2 元対称通信路	binary symmetric channel
符号化率	code rate
復号誤り率	decoding error rate
多項式	polynomial
排他的論理和	exclusive or
検査行列	check matrix

【信号処理】解答は，だいだい色の解答用紙に記入すること．

線形時不変な離散時間信号処理システム Q, R を図 1 のブロック線図のように構成する．ただし $x[n]$, $y[n]$ は各システムへの入力信号および出力信号であり，n は時刻を表す整数である．また，図中の $\oplus$ は加算器を，$\boxed{\mathrm{D}}$ は単位遅延器を，$\triangleright$ は係数乗算器を表し，その定義は図 2 の通りである．信号処理システム Q, R の伝達関数をそれぞれ $H^Q(z)$, $H^R(z)$ とするとき，以下の問いに答えよ．ただし，本問における伝達関数は z 変換により定義されるものとする．

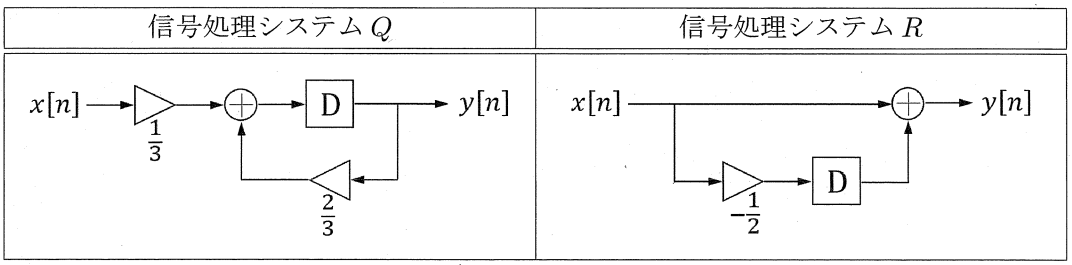


図 1: 離散時間信号処理システム Q, R のブロック線図

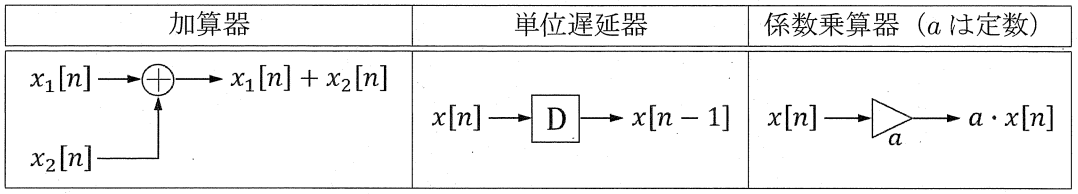


図 2: 加算器，単位遅延器，係数乗算器の定義

(i) Q および R を表す入出力差分方程式を求め，それをもとに Q, R の因果性を議論せよ．

(ii) $H^Q(z)$ および $H^R(z)$ を求めよ．

(iii) R の周波数応答を求めよ．

(iv) Q のインパルス応答を求めよ．

次に，図 1 の Q, R を用いて，線形時不変な離散時間信号処理システム L_k $(k = 0,\ 1,\ 2,\ \cdots)$ を図 3 のように再帰的に構成する．L_k の伝達関数を $H_k^L(z)$ とするとき，以下の問いに答えよ．

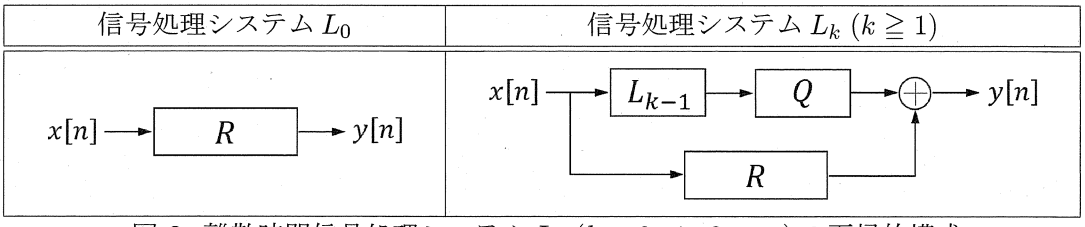


図 3: 離散時間信号処理システム L_k $(k = 0,\ 1,\ 2,\ \cdots)$ の再帰的構成

(v) $k \geqq 1$ のとき，$H^Q(z)$, $H^R(z)$, $H_{k-1}^L(z)$ を用いて $H_k^L(z)$ を表せ．

(vi) 任意の $k \geqq 0$ に対し

$$H_k^L(z) = \frac{(2z-1)\{(3z-2)^{k+1}-1\}}{6z(z-1)(3z-2)^k}$$

となることを示し，それに基づいて，$H_k^L(z)$ の極と零点を z 平面上に図示するとともに L_k の有界入力有界出力安定性を議論せよ．

専門用語の英訳	
線形時不変	linear time-invariant
離散時間信号処理システム	discrete-time signal processing system
ブロック線図	block diagram
入力信号	input signal
出力信号	output signal
加算器	adder
単位遅延器	unit delay
係数乗算器	scalar multiplier
伝達関数	transfer function
z 変換	z transform
入出力差分方程式	input-output difference equation
因果性	causality
周波数応答	frequency response
インパルス応答	impulse response
再帰的	recursive
極	pole
零点	zero
z 平面	z plane
有界入力有界出力安定性	bounded-input bounded-output stablity

【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. 10 進数整数 i ($i = 0, 1, 2, 3$) を 2 ビットの 2 進数整数 $\boldsymbol{X} = (x_1 x_0)$ に符号化するエンコーダ，および，$\boldsymbol{X}$ を i に復号化するデコーダの回路を構成することを考える（$\boldsymbol{X}$ においては，添え字の小さい方が下位ビットとする）．以下の問いに答えよ．
   ただし，回路図を答える問いにおいて，論理ゲートを表す際には図 1 に示した記号を用い，解となる回路が複数存在する場合にはその 1 つを示せばよい．

   (i) このデコーダの回路の入力は 2 進数整数 $\boldsymbol{X}$，出力は 4 ビットの y_n ($n = 0, 1, 2, 3$)とする．これらの入出力の組み合わせは，$\boldsymbol{X}$ を復号化した 10 進数整数を i としたとき，出力 y_n のうち i 番目である y_i のみが 1 となる．このデコーダの真理値表を表 1 に示す．
   このデコーダの回路図を示せ．ただし，利用可能な論理ゲートは論理積（AND），論理和（OR），論理否定（NOT）とし，各ゲートへの入力数は 2 以下とする．

   (ii) このエンコーダの回路において，符号化される 10 進数整数が i のとき，入力 y_n ($n = 0, 1, 2, 3$) において $y_i = 1$ となり，i を符号化した 2 進数整数 $\boldsymbol{X} = (x_1 x_0)$ が出力されるとする．ただし複数の y_n が 1 となるとき，優先順位が最も高い y_n を $y_i = 1$ とみなし，i を符号化した $\boldsymbol{X}$ を出力する．このような優先順位付きのエンコーダをプライオリティエンコーダと呼ぶ．ここで優先順位を y_3, y_2, y_1, y_0 の順に高い（y_3 が最も高い）としたとき，このプライオリティエンコーダの回路の真理値表，論理式の最小積和形，および回路図を示せ．ただし，利用可能な論理ゲートは否定論理積（NAND）のみとし，各ゲートへの入力数は 2 以下とする．

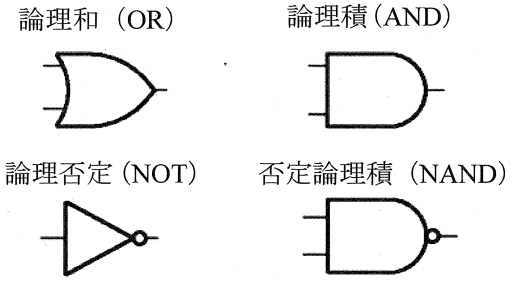


図 1：論理ゲートの凡例

表 1：デコーダの真理値表

x_1	x_0	y_3	y_2	y_1	y_0
0	0	0	0	0	1
0	1	0	0	1	0
1	0	0	1	0	0
1	1	1	0	0	0

2. ひとつの命令が 5 ステージからなる場合のパイプライン処理について考える．ここでの各ステージは，命令フェッチ（IF），命令デコード（D），オペランドフェッチ（OF），命令の実行（EX），結果の格納（S）の 5 つである．この 1 つのステージの実行時間を 1 クロックサイクルと呼ぶ．この処理系において，演算 A=B+C，つまり主記憶アドレス B の内容と主記憶アドレス C の内容を加算し，主記憶アドレス A に格納する演算を，以下の命令シーケンスにより実行する．

命令 1)　(B) → R1
命令 2)　(C) → R2
命令 3)　Add　R1, R2, R3
命令 4)　[R3] → A

ここで命令 1)は，主記憶アドレス B の内容(B)をレジスタ R1 に格納する操作を表し，命令 2)は，(C)をレジスタ R2 に格納する操作を表す．命令 3)は，R1 の内容[R1]と R2 の内容[R2]とを加算し，その結果をレジスタ R3 に格納する操作，[R1]+[R2] → R3 を表す．命令 4)は，R3 の内容[R3]を主記憶アドレス A に格納する操作を表す．なお，(・)と[・]は，それぞれメモリとレジスタの内容を表し，→は左辺の内容を右辺のアドレスに格納する操作である．このとき以下の各問いに答えよ．

(i) パイプライン処理を行わず命令を逐次的に実行した場合，上記の命令シーケンスの実行には何クロックサイクル必要か答えよ．

(ii) パイプライン処理を行った場合，制御の動作は表 2 のようになった．なおこの表では，実行開始から *n* 番目のクロックサイクルにあたる時点を CC*n* と表している．命令 4)の OF の実行を CC10 まで待つ必要がある理由について具体的に説明せよ．

(iii) パイプラインに命令を連続的に流すことができない障害(パイプラインの乱れ)が起こる原因には，構造ハザード，データハザード，制御ハザードがある．それぞれについて例を挙げて説明せよ．

(iv) データハザードを防止する方法について説明せよ．

表 2：命令パイプライン制御動作

命令	クロックサイクル（CC）											
	CC1	CC2	CC3	CC4	CC5	CC6	CC7	CC8	CC9	CC10	CC11	CC12
1)	IF	D	OF	EX	S							
2)		IF	D	OF	EX	S						
3)					IF	D	OF	EX	S			
4)						IF	D	OF			EX	S

専門用語の英訳

符号化	encode
エンコーダ	encoder
復号化	decode
デコーダ	decoder
10 進数整数	decimal integer number
2 進数整数	binary integer number
論理ゲート	logic gate
真理値表	truth table
論理式	logical formula
回路図	circuit diagram
最小積和形	minimum sum-of-products form
プライオリティエンコーダ	priority encoder
パイプライン処理	pipeline processing
ハザード	hazard
構造ハザード	structural hazard
データハザード	data hazard
制御ハザード	control hazard

【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. 図 1 は，連結無向グラフの例である．ただし，各節点内の数字は節点番号を表すものとする．隣接行列を用いてグラフを表現し，深さ優先探索により全節点を訪問する処理を行うためのプログラム A について，次の問いに答えよ．なお，プログラム A は C 言語で書かれている．

(i) 図 1 中のグラフの隣接行列を表すように，プログラム中の空欄 Q に相当する部分を記述せよ．ただし，空欄 Q は複数行にわたってよい．または，C 言語での表記に限らず，行列形式での解答でもよいものとする．

(ii) グラフを表現する代表的なデータ構造としては，隣接行列の他に，隣接リストが挙げられる．隣接行列と隣接リストを用いたグラフ表現の性質について，記憶量の観点から対比的に簡潔に述べよ．

(iii) プログラムが正しく動くように空欄 1 ～ 3 を埋めよ．また，プログラムの実行により構成される深さ優先木を図示せよ．

(iv) グラフに対する代表的な探索法としては，深さ優先探索の他に，幅優先探索が挙げられる．深さ優先探索と幅優先探索のそれぞれの長所・短所について，「メモリ効率」の点から対比的に簡潔に述べよ．

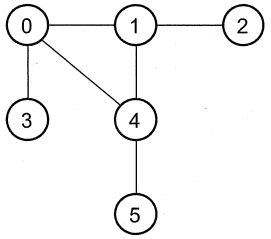


図 1　連結無向グラフの例

プログラム A

```
#define N 6

int visited[N]; // 未訪問を 0，訪問済を 1 とする

// 隣接行列
int adjacent[N][N] = Q

// 深さ優先探索
void dfs(int i) {
    visited[i] = 1 ;
    for (int j = 0; j < N; j++) {
        if (adjacent[i][j] == 1 && visited[j] == 2 )
            dfs( 3 );
    }
}

int main(void) {
    for (int i = 0; i < N; i++)
        visited[i] = 0;

    dfs(0);
    return(0);
}
```

2. 図 2 に示すネットワークにおいて，流体 1 のソースを節点 s_1，シンクを節点 t_1 とし，流体 2 のソースを節点 s_2，シンクを節点 t_2 とする．各有向辺を流れる流量は流体 1 と流体 2 の流量の合計で与えられ，各有向辺は有限な正の整数の容量を有する．各流体の各有向辺における流量は常に 0 以上の整数とする．このネットワークについて，以下の問いに答えよ．

(i) ネットワークを流体 1 のみが流れる場合，最大流最小カット定理（最大フロー最小カット定理）を用いて s_1 から t_1 への流体 1 の最大流量をその導出過程と共に示せ．

(ii) 問い (i) の s_1 から t_1 への最大流量の流体 1 の流れ（フロー）に加えて，各辺の残余容量を用いて s_2 から t_2 へ流体 2 を流す．このとき，流体 2 の流量を最大化するためには，節点 b を通る流体 1 について $b \to t_2 \to a \to t_1$ という経路よりも，なるべく直接 $b \to t_1$ という経路に多くの流量を配分した方が望ましい．この理由を最大流最小カット定理を用いて説明せよ．

(iii) 問い (ii) と同様に問い (i) で求めた s_1 から t_1 への最大流量の流体 1 の流れに加えて，各辺の残余容量を用いて s_2 から t_2 へ流体 2 を流すとき，最大流最小カット定理を用いて流体 2 の最大流量をその導出過程と共に示せ．

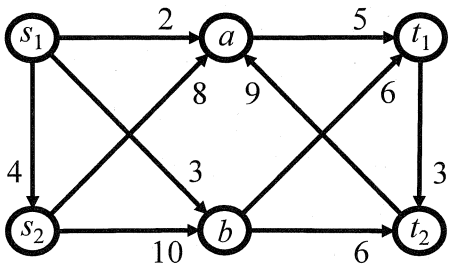


図 2　ネットワーク．各○は節点を表し，各 → は有向辺を表す．流体は各有向辺の向きにしたがって流れるものとし，隣接して付された数値はその有向辺の容量を表す．

専門用語の英訳

連結無向グラフ	connected undirected graph
節点	node
隣接行列	adjacent matrix
隣接リスト	adjacent list
深さ優先探索	depth-first search
幅優先探索	breadth-first search
有向辺	directed edge
流体	fluid
流量	flow rate
容量	capacity
残余容量	remaining capacity
ソース	source
シンク	sink
最大流量	maximum flow rate
最大流最小カット定理	max-flow min-cut theorem

【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．

G を位数 p の巡回群，g を G の生成元として以下の公開鍵暗号化方式について問い(i)-(iv)に答えよ．ただし G の群演算を・であらわし，G の任意の元 h に対して h^{-1} および自然数 a に対して h^a は多項式時間で計算可能であるとする． g は公開パラメータとする．

- 鍵生成アルゴリズム

[入力] 公開パラメータ g [出力] 秘密鍵 $sk = s$，公開鍵 $pk = g^s$

ただし s は $\{1, \ldots, p-1\}$ 上で一様ランダムに選ばれる．

- 暗号化アルゴリズム

[入力] 公開パラメータ g，平文 $m \in G$，公開鍵 pk [出力] 暗号文 $c = (g^r, m \cdot g^{sr})$

ただし r は $\{1, \ldots, p-1\}$ 上で一様ランダムに選ばれる．

- 復号アルゴリズム

[入力] 暗号文 $c = (x, y)$，秘密鍵 sk [出力] $x^{-s} \cdot y$

(i) この公開鍵暗号化方式の正当性，つまり任意の平文 $m \in G$，鍵生成アルゴリズムで生成された公開鍵 pk と秘密鍵 sk に対して，m を暗号化アルゴリズムで暗号化した暗号文 c が復号アルゴリズムで正しく m に復号されることを示せ．

(ii) この公開鍵暗号化方式の暗号文には準同型性があること，つまり秘密鍵を用いずに多項式時間で計算可能である適当な二項演算 $\circ$ を定義して，任意の二つの平文 $m_1, m_2 \in G$ の暗号文 c_1, c_2 に対して $c_1 \circ c_2$ が $m_1 \cdot m_2 \in G$ の暗号文となることを示せ．

(iii) 暗号化アルゴリズムにおいて常に同じ r を暗号化に用いると仮定する．このとき，一つの平文とその暗号文の組を手に入れた攻撃者は秘密鍵を用いずに任意の暗号文から平文を多項式時間で復号可能であることを示せ．

(iv) この公開鍵暗号化方式に対して公開鍵 pk および暗号文 c から平文 m を多項式時間計算する攻撃者が存在したと仮定すると，公開鍵暗号化方式の公開パラメータ g および任意の $a, b \in \{1, \ldots, p-1\}$ に対して，g, g^a, g^b が入力として与えられた場合に g^{ab} を求める問題が多項式時間で計算可能であることを示せ．

専門用語の英訳	
位数	order
巡回群	cyclic group
生成元	generator
公開鍵暗号化方式	public-key encryption scheme
多項式時間	polynomial time
公開パラメータ	public parameter

鍵生成アルゴリズム	key generation algorithm
公開鍵	public key
秘密鍵	secret key
暗号化アルゴリズム	encryption algorithm
復号アルゴリズム	decryption algorithm

【制御工学】解答は，白色（９番）の解答用紙に記入すること．

以下の 1.〜4. に答えよ．

1. 伝達関数 $G(s)$ が次式で表される 1 次系について，以下の問いに答えよ．

$$G(s) = \frac{1}{2s+6}$$

(i) ステップ応答の定常値を求めよ．

(ii) $G(s)$ のボード線図におけるゲイン曲線を折れ線近似したときの折点角周波数の値を求めよ．

(iii) 正弦波関数 $\sin 3t$ で表される入力に対し，定常状態での出力は $Y\sin\left(3t-\frac{\pi}{4}\right)$ と表される正弦波関数となった．Y の値を求めよ．

2. 図 1 のフィードバックシステムについて，以下の問いに答えよ．ただし，K は実数値をとるゲインである．

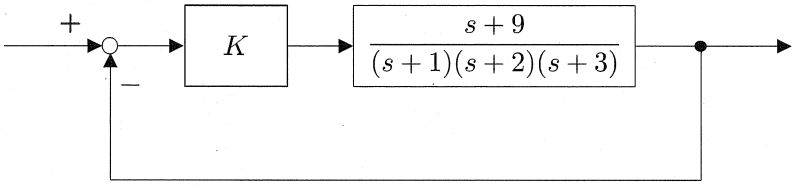


図 1

(i) K を $0 \to \infty$ と変化させたとき，虚軸と交わる根軌跡が存在する．根軌跡が虚軸と交わるときの K の値を求めよ．

(ii) 問 2. (i) において，根軌跡が虚軸と交わる点の座標をすべて求めよ．

3. 次式の状態方程式と出力方程式で与えられる線形時不変システムについて，以下の問いに答えよ．

$$\frac{d\boldsymbol{x}(t)}{dt} = \begin{bmatrix} a & 2 \\ -4 & 2 \end{bmatrix}\boldsymbol{x}(t) + \begin{bmatrix} 1 \\ 1 \end{bmatrix}u(t)$$

$$y(t) = \begin{bmatrix} 1 & 0 \end{bmatrix}\boldsymbol{x}(t)$$

ただし，a は実数値をとるパラメータであり，$\boldsymbol{x}(t) = \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix}$ は状態変数ベクトル，$u(t)$ は入力変数，$y(t)$ は出力変数とする．

(i) このシステムが可制御となるための a に関する必要十分条件を求めよ．

(ii) このシステムが任意の a の値に対して可観測となることを示せ．

(iii) $a = -1$ とする．K を正の実数値をとるゲインとし，入力 $u(t) = -Kx_2(t)$ を与えたとき，このシステムが漸近安定となるための K に関する必要十分条件を求めよ．

4. 2階常微分方程式

$$\frac{1}{2}\frac{d^2y(t)}{dt^2}+\frac{dy(t)}{dt}+2y(t)=u(t)$$

で与えられる線形時不変システムについて，以下の問いに答えよ．ただし，$u(t)$ は入力変数，$y(t)$ は出力変数とする．

(i) $x_1(t)=\dfrac{1}{2}y(t)$ と $x_2(t)=\dfrac{1}{2\sqrt{3}}\left(y(t)+\dfrac{dy(t)}{dt}\right)$ を状態変数としたとき，このシステムを表す状態空間表現

$$\frac{d\boldsymbol{x}(t)}{dt}=\boldsymbol{A}\boldsymbol{x}(t)+\boldsymbol{b}u(t)$$

$$y(t)=\boldsymbol{c}\boldsymbol{x}(t)$$

の係数行列 $\boldsymbol{A}$ と係数ベクトル $\boldsymbol{b}$，$\boldsymbol{c}$ を求めよ．ただし，$\boldsymbol{x}(t)=\begin{bmatrix}x_1(t)\\x_2(t)\end{bmatrix}$ とする．

(ii) $y(t)$ を零入力応答とすると，$y(0)=1$ かつ $y\left(\dfrac{\sqrt{3}\pi}{4}\right)=0$ となった．初期値 $x_1(0)$ と $x_2(0)$ を求めよ．ここで，つぎの結果を用いてもよい．

$$\exp\left(\begin{bmatrix}-\lambda & \omega\\ -\omega & -\lambda\end{bmatrix}t\right)=\exp(-\lambda t)\begin{bmatrix}\cos\omega t & \sin\omega t\\ -\sin\omega t & \cos\omega t\end{bmatrix}$$

ただし，λ と ω は正の実数とする．

専門用語の英訳

伝達関数	transfer function
1 次系	first order system
ステップ応答	step response
定常値	steady-state value
ボード線図	Bode diagram
ゲイン曲線	log-magnitude curve
折れ線近似	piecewise linear approximation
折点角周波数	corner angular frequency
正弦波関数	sinusoidal function
定常状態	steady state
フィードバックシステム	feedback system
虚軸	imaginary axis
根軌跡	root locus
線形時不変システム	linear time-invariant system
状態方程式	state equation
出力方程式	output equation
状態変数ベクトル	state variable vector
入力変数	input variable
出力変数	output variable
可制御	controllable
可観測	observable
漸近安定	asymptotically stable
状態空間表現	state-space description
零入力応答	zero-input response