2020 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１６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」，及び，「情報セキュリティ」の全部で８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.

OOK (On-Off Keying) は，$nT \le t < (n+1)T$ の時間区間で n 番目の情報ビット $b_n = 1$ を送信するときには $A\cos(2\pi f_c t + \phi)$ なる信号を送信し，$b_n = 0$ を送信するときには信号を送信しない（$A = 0$）変調方式であり，OOK で変調された信号 $s_{\mathrm{OOK}}(t)$は次式で与えられる.

$$s_{\mathrm{OOK}}(t) = \begin{cases} A\cos(2\pi f_c t + \phi), & b_n = 1 \\ 0, & b_n = 0 \end{cases} \tag{1}$$

ここで A は信号の振幅，f_c は搬送周波数，t は時間，T は情報ビットの送信周期，ϕは搬送波の初期位相である．受信機においては，式 (1) の信号に，加法性白色ガウス雑音である $n(t) = n_I(t)\cos(2\pi f_c t + \phi) - n_Q(t)\sin(2\pi f_c t + \phi)$ が加算された信号が受信されるものとする．さらに，誤り訂正符号は適用されておらず，受信機では，タイミング同期，周波数同期は完全に動作しているものとする．このとき，以下の問いに答えよ.

i) $b_n = 1$ と $b_n = 0$ それぞれの場合において受信機で受信される受信信号 $r(t)$を数式で表記せよ.

ii) 受信機において同期検波を用いるとき，同期検波器の構成を，図を用いて説明し，さらに $b_n = 1$ と $b_n = 0$ それぞれの場合における検波器出力を数式で表記せよ.

iii) $n_I(t), n_Q(t)$ はいずれも平均 0, 分散σ^2 で互いに独立したガウス分布に従うランダム変数であり，その確率密度関数は次式に従うものとする.

$$p(n_I) = \frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{n_I^2}{2\sigma^2}\right),\ p(n_Q) = \frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{n_Q^2}{2\sigma^2}\right) \tag{2}$$

このとき，$n(t)$の分散を導出せよ.

iv) 受信信号の信号電力対雑音電力比を導出せよ.

v) 同期検波において，雑音が全くない場合に $b_n = 1$ が送信された場合の受信信号の値と，雑音が全くない場合に $b_n = 0$ が送信された場合の受信信号の値の平均値を判定しきい値とする．受信信号が判定しきい値未満であれば $b_n = 0$，受信信号が判定しきい値以上であれば $b_n = 1$ が送信されたと判定するものとする．$b_n = 1$ が送信された場合に判定誤りが発生する確率を導出せよ．ただし次式を利用してよい.

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt,\quad \mathrm{erfc}(x) = 1 - \mathrm{erf}(x) \tag{3}$$

誤り訂正符号	error correction code
位相	phase
加法性白色ガウス雑音	additive white Gaussian noise
受信機	receiver
受信信号	received signal
信号対雑音電力比	signal to noise power ratio
振幅	amplitude
送信周期	transmission cycle
同期検波	coherent detection
搬送周波数	carrier frequency
判定しきい値	decision threshold
変調方式	modulation scheme

【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.

N 個（$N \geq 3$）の無線端末を収容可能な無線基地局を考える. 時間軸はスロットに分割されており，各スロットの終了時点において確率 a （$0 < a < 1$） で新たな無線端末が 1 個到着し, 確率 $1-a$ で到着がないとする．ただし，スロットの開始時点において既に無線基地局へ収容されている無線端末が N 個であった場合，新たに到着した無線端末は収容されることなく棄却されると仮定する．無線基地局に収容されている各無線端末は他の端末とは独立に，スロット毎に確率 q （$0 < q < 1$）で 1 パケットを送信し，確率 $1-q$ で送信を行わないとする．各スロットにおいてパケット送信を行った無線端末が 1 つの場合にはパケット送信は成功し，送信が成功した無線端末はそのスロットの終了時点で基地局から離脱する. 一方, パケット送信を行った無線端末が複数の場合には，パケットの衝突が発生することでパケット送信は失敗し，無線端末の離脱は発生しないとする.

各スロットの開始時点において無線基地局に収容されている無線端末数が n （$0 \leq n \leq N$） である定常状態確率を p_n で表すとき，以下の問いに答えよ.

(i) あるスロットの開始時点において，無線基地局に収容されている無線端末が n 個 （$1 \leq n \leq N$）であったとする.

(a) パケットの衝突が発生することなく, 無線基地局に収容されているいずれかの無線端末のパケット送信が成功し, このスロットにおいて無線端末の離脱が発生する確率 q_n を求めよ.

(b) 新たな無線端末の到着がないと仮定したとき, 無線端末の離脱が発生するまでに必要な平均スロット数を求めよ.

(ii) p_{n+1}, p_n および p_{n-1} （$1 \leq n \leq N-1$） の関係を a, q_n $(1 \leq n \leq N-1)$ を用いて表せ. ただし，$n = 1$，$2 \leq n \leq N-2$，$n = N-1$ の 3 つの場合についてそれぞれ表すこと.

(iii) $a_n^* = a(1-q_n)$, $q_n^* = (1-a)q_n$ $(1 \leq n \leq N-1)$ とおく．このとき，p_N を p_0 と a_n^*, q_n^* および a, q_N を用いて表せ.

(iv) p_0 が以下で表されることを示せ.

$$p_0 = \left[1 + \frac{a}{q(1-a)} + \sum_{n=2}^{N-1} D_n + (1-a)D_N\right]^{-1}$$

ただし，D_n $(2 \leq n \leq N)$ は以下で与えられる.

$$D_n = \left(\frac{a}{q(1-a)}\right)^n \frac{\prod_{m=1}^{n-1}(1-mq(1-q)^{m-1})}{n!(1-q)^{\frac{n(n-1)}{2}}}$$

専門用語の英訳

無線端末：	wireless terminal
基地局：	base station
時間軸：	time axis
スロット：	slot
確率：	probability
衝突：	collision
パケット：	packet
定常状態確率：	steady state probability
平均：	mean

【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 BS1 と BS2，全反射ミラー M1 と M2 から構成される干渉計に，直線偏波・単一周波数光ビームを入力する．光ビームはビームスプリッタ BS1 で２つに分岐され，一方はミラー M1 と M2 を含む光路１を伝搬し，一方は空間のみの光路２を伝搬した後，ビームスプリッタ BS2 で合波される．ここでは，光路２に対して光路１は十分長いものとする．BS2 で合波された光ビームのパワーをパワーメータで測定する．なお，ビームスプリッタ BS1 および BS2 では，入力光ビームのパワーが半分になるように分岐される．ビームスプリッタおよびミラーでの損失は無視でき，ビームスプリッタとミラーでの偏波回転は生じないものとする．また，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無視できるものとする．空間の屈折率を 1 として，以下の問いに答えよ．なお，答えだけでなく導出過程を示すこと.

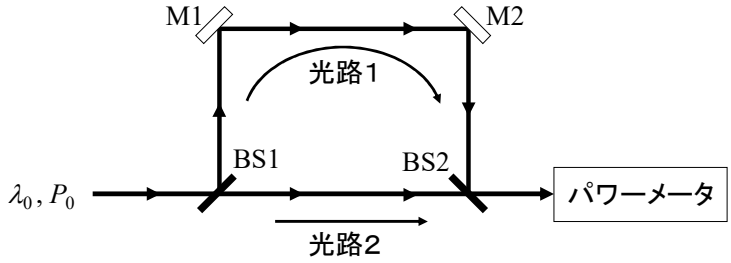

図1

(i) 波長 λ_0 およびパワー P_0 の光ビームを干渉計に入力し，パワーメータの測定値が P_0 となるように，干渉計内の光路長を厳密に調整した．このときの，BS1 で分岐された２つの光ビームが，それぞれ光路１および光路２を伝搬し BS2 で合波されるまでに生じる位相変化量の差 $\Delta\phi_1$ を求めよ.

(ii) 波長 λ_0 およびパワー P_0 の光ビームを干渉計に入力し，パワーメータの測定値が P_0 の半分になるように，干渉計内の光路長を厳密に調整した．このときの，BS1 で分岐された２つの光ビームが，それぞれ光路１および光路２を伝搬し BS2 で合波されるまでに生じる位相変化量の差 $\Delta\phi_2$ を求めよ．ただし，光ビームの波長を λ_0 から徐々に長波長側に変化させるとパワーメータの測定値が大きくなることとする.

(iii) 問い(ii)の干渉計の状態で，M1 と M2 の間に減衰板を挿入した．この減衰板では入力光ビームのパワーの半分が透過する．また，簡単のために減衰板の屈折率を 1 とみなす．この干渉計に波長 λ_0 およびパワー P_0 の光ビームを入力したときのパワーメータの測定値を求めよ.

(iv) 問い(ii)の干渉計の状態において， M1 と M2 の間の光路中に，屈折率が n で厚さが L の均一な透明ガラス板を光路に垂直に挿入した．この干渉計に波長 λ_0 およびパワー P_0 の光ビームを入力すると，パワーメータの測定値が P_0 となった．このときのガラス板厚 L を求めよ．なお，ガラスの損失と表面における反射は無視できるものとする.

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
直線偏波：linear polarization
単一周波数：single frequency
光ビーム：optical beam
光路：optical path
パワーメータ：power meter
波長：wavelength
パワー：power

【情報理論】 解答は，桃色の解答用紙に記入すること.

1. 入力アルファベット $A=\{a,b,c,d\}$ の 1 記号が入力されると出力アルファベット $B=\{a,b,c,d\}$ の 1 記号を出力する通信路 T を考える．入力，出力を表す確率変数 X，Y の結合確率分布が表 1 のように与えられるとき，以下の問いに答えよ.

表 1：結合確率分布 $P_{XY}(x,y)$

$P_{XY}(x,y)$		X			
		a	b	c	d
Y	a	$\frac{1}{8}$	$\frac{1}{8}$	0	$\frac{1}{4}$
	b	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{8}$	0
	c	$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{16}$	0
	d	$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{16}$	0

(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 $H(X|Y)$，$H(Y|X)$ を求めよ.

(iii) 相互情報量 $I(X;Y)$ を求めよ.

(iv) 通信路の性質は本来，入出力の条件付き確率分布 $P_{Y|X}(\mathrm{y}|x)$ で表され，通信路 T の性質を表す $P_{Y|X}(\mathrm{y}|x)$ は表 1 より求められる．通信路 T の通信路容量 C_T を求めよ．また，C_T を実現する X の確率分布 $P_X(x)$ を求めよ．なお，X の確率分布を $P_X(a)=p_1$，$P_X(b)=p_2$，$P_X(c)=p_3$，$P_X(d)=1-(p_1+p_2+p_3)$などとして考えるとよい.

2. 情報源記号 0，1 をそれぞれ確率0.9，0.1で発生する記憶のない 2 元情報源に関して，以下の問いに答えよ.

(i) 情報源記号を 2 個ずつまとめた情報源系列に対し 2 元ハフマン符号化を行う場合の符号化則，及び 1 情報源記号あたりの平均符号長を求めよ.

(ii) 長さ 3 までの連続した 0 をまとめた情報源系列 1，01，001，000 に対し 2 元ハフマン符号化を行う場合の符号化則，及び 1 情報源記号あたりの平均符号長を求めよ.

(iii) 問い(i)，問い(ii)のいずれの符号化が効率的か説明せよ.

専門用語の英訳

通信路	channel
確率変数	random variable
結合確率分布	joint probability distribution
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
通信路容量	channel capacity
情報源記号	source symbol
記憶のない 2 元情報源	memoryless binary source
ハフマン符号化	Huffman coding
符号化則	coding rule
平均符号長	average code length

【信号処理】解答は，だいだい色の解答用紙に記入すること．

図 1 のブロックダイアグラムに示すように，信号処理システム S, L, H を縦続接続する．S は，図 2 に示すように，連続時間信号 $x(t)$ から間隔 T 秒で一様サンプリングを行い離散時間信号 $x[n]$ を得るシステムであり，このとき，量子化は含まないものとする．L は，$x[n]$ を入力として離散時間信号 $y[n]$ を出力するシステムである．H は，サンプリング定理に従って $y[n]$ から連続時間信号 $y(t)$ を復元するシステムである．ただし，t は連続的な時刻を表す実数，n は離散的な時刻を表す整数である．

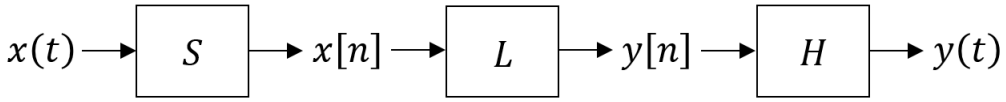

図 1: 対象とする信号処理システムのブロックダイアグラム

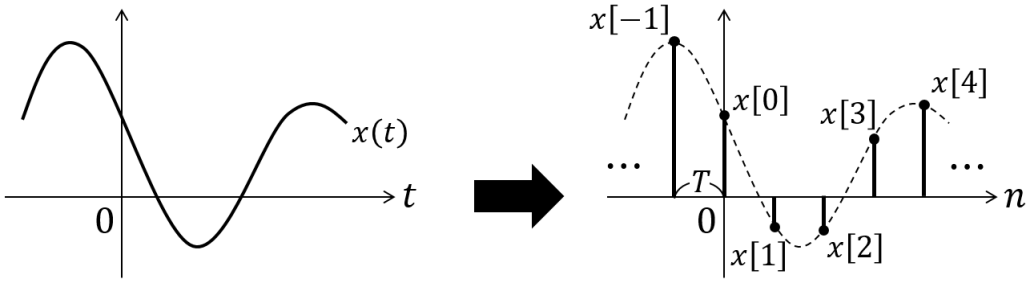

図 2: システム S による連続時間信号 $x(t)$ の一様サンプリング

(i) L が恒等システム，すなわち $y[n] = L[x[n]] = x[n]$ とする．また，$x(t)$ は $x(t) = \cos(400\pi t)$ で表される正弦波であるとする．このとき，以下の問いに答えよ．

(a) 正弦波 $x(t)$ の基本周期および周波数を求めよ．

(b) $x(t)$ からエイリアシングなしに $x[n]$ が得られるためには T がどのような条件を満たす必要があるか，数式を用いて答えよ．

(c) $T = 0.004$ のとき，$y[n]$ を具体的な数式で表せ．

(d) $T = 0.004$ のとき，$y(t)$ は何 Hz の正弦波となるか，理由とともに答えよ．

(ii) L における入力 $x[n]$ と出力 $y[n]$ が次の関係式を満たすものとする．

$$y[n] \;=\; (1-a)x[n] \;+\; ay[n-1]$$

ここで a は $0 < a < 1$ を満たす実数の定数である．また，$x(t)$ は

$$x(t) = u\left(t + \frac{T}{2}\right) - u\left(t - \frac{T}{2}\right), \quad \text{ただし } u(t) \;=\; \begin{cases} 1 & (t \geqq 0) \\ 0 & (t < 0) \end{cases}$$

で表される信号とする．このとき，以下の問いに答えよ．

(a) $x(t)$ および $x[n]$ を図示せよ．

(b) L の伝達関数を求めよ．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．

(c) 問い (b) で求めた伝達関数をもとに，L の有界入力有界出力安定性を論ぜよ．

(d) $y[n]$ を具体的な数式で表せ．

専門用語の英訳	
ブロックダイアグラム	block diagram
信号処理システム	signal processing system
縦続接続	cascade connection
連続時間信号	continuous-time signal
一様サンプリング	uniform sampling
離散時間信号	discrete-time signal
量子化	quantization
サンプリング定理	Sampling Theorem
恒等システム	identity system
正弦波	sinusoidal wave
基本周期	fundamental period
周波数	frequency
エイリアシング	aliasing
伝達関数	transfer function
z 変換	z transform
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.

n ビットの 2 つの 2 進整数 $\boldsymbol{X} = (x_{n-1}\ x_{n-2}\ \ldots\ x_0)$ と $\boldsymbol{Y} = (y_{n-1}\ y_{n-2}\ \ldots\ y_0)$ を加算し，その結果として n ビットの 2 進整数 $\boldsymbol{S} = (s_{n-1}\ s_{n-2}\ \ldots\ s_0)$ を得る回路を構成することを考える．つまり，$\boldsymbol{S} = \boldsymbol{X} + \boldsymbol{Y}$ である．このとき以下の各問いに答えよ．2 進数表現においては添え字が小さい方を下位桁とする．また，i ビット目の加算（$0 \leq i < n$）において，加算すべき入力を x_i，y_i，出力するそれらの和を s_i，下位桁からの桁上げ入力を c_i，上位桁への桁上げ出力を c_{i+1} とする．c_0 は $c_0 = 0$ としてよい．論理ゲート（AND, OR, NOT）の入力数に制限はなく，一つの論理ゲートの遅延時間はその入力数によらず全て T であるとする．

(i) 全加算器とは，加算すべき 2 つの 2 進数 1 ビットと下位桁からの桁上げを入力とし，和と上位桁への桁上げを出力する加算回路である．i ビット目の加算を行う全加算器 FA_i は，図 1 に示すように 3 入力 2 出力の回路である．この全加算器 FA_i の真理値表と，2 つの出力 s_i および c_{i+1} の論理式の最小積和形を示せ.

(ii) 問い(i)で求めた最小積和形に基づき設計した全加算器 FA_i において，入力の x_i，y_i，c_i が確定した後，s_i および c_{i+1} を得るのにかかる時間を，それぞれ T を用いて表せ.

(iii) 全加算器 FA_i を直列に接続した n ビットのリプル桁上げ加算器を考える．つまり，FA_i の桁上げ出力 c_{i+1} を，次の上位桁の全加算器 FA_{i+1} の桁上げ入力に接続する．このリプル桁上げ加算器において，$\boldsymbol{X}$，$\boldsymbol{Y}$ の値が確定した後，最上位桁の全加算器 FA_{n-1} の出力 s_{n-1} を得るまでに要する演算時間を示せ．また，この演算時間の n に関するオーダーを示せ.

(iv) 桁上げ出力の計算時間を短縮するために，桁上げ先見加算器を構成する．桁上げ先見加算器とは，各桁の桁上げ出力を直接論理回路で構成した回路である．これを構成するために i ビット目の全加算器 FA_i の桁上げ出力 c_{i+1} を，$g_i(x_i, y_i) + p_i(x_i, y_i)\ c_i$ の形で表すことを考える．ここで $g_i(x_i, y_i)$ と $p_i(x_i, y_i)$ はいずれも論理式であり，x_i と y_i を入力として時間 T で計算できるように構成する．この $g_i(x_i, y_i)$ と $p_i(x_i, y_i)$ の論理式を示せ.

(v) 問い(iv)の $g_i(x_i, y_i)$ と $p_i(x_i, y_i)$ を用いて桁上げ先見加算器を構成した場合，$g_i(x_i, y_i)$，$p_i(x_i, y_i)$ の値が確定した後，i ビット目の桁上げ出力 c_{i+1} を得るまでに要する時間を，T を用いて示せ.

(vi) 問い(v)のように桁上げ先見加算器を構成した場合に，$\boldsymbol{X}$，$\boldsymbol{Y}$ が確定した後，$\boldsymbol{S}$ を得るのに要する時間を，T を用いて表せ.

(vii) 符号付き 2 進整数の加算を考える．負の数は 2 の補数で表現し，$\boldsymbol{X}$，$\boldsymbol{Y}$，$\boldsymbol{S}$ の最上位桁が符号を，残りの桁が数値を表すとする．この場合，減算は負の数の加算で実現できる．このとき $\boldsymbol{X}$ と $\boldsymbol{Y}$ の加算においてオーバーフローが生じる条件を，$\boldsymbol{X}$，$\boldsymbol{Y}$，$\boldsymbol{S}$ の符号に着目して説明せよ．オーバーフローとは，加算の結果が数値を表す桁で表現できる範囲を超えることにより，正しい演算結果が得られないことを指す．さらに，この条件を $\boldsymbol{X}$，$\boldsymbol{Y}$，$\boldsymbol{S}$ に含まれるビットを用いた論理式で表せ.

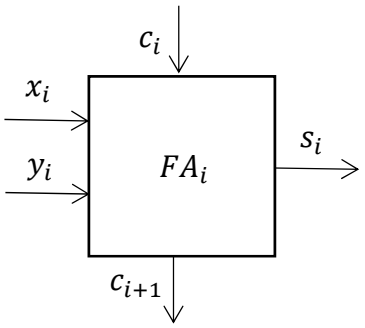

図 1　i ビット目の全加算器

専門用語の英訳

2 進整数	binary integer
加算	addition
論理ゲート	logic gate
遅延時間	delay time
全加算器	full adder
真理値表	truth table
論理式	logical formula
最小積和形	minimum sum-of-products form
リプル桁上げ加算器	ripple-carry adder
最上位桁	most significant bit
桁上げ先見加算器	carry-lookahead adder
符号	sign
2 の補数	two's complement
オーバーフロー	overflow

【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. ヒープは，何らかの整数が付与された要素の集合から，最大整数を持つ要素を効率良く取り出すことができる木構造である．n 個の要素から成る集合 $\mathbf{S} = \{i | i = 1, \ldots, n\}$ について，要素 i に付与された整数を $I[i]$ と表す． 配列 $\mathbf{X}[k]$ $(k = 1, \ldots, n)$ を用いて，$\mathbf{S}$ から以下の 4 つの規則に従ってヒープを構成する．

   規則 1 $\mathbf{X}[1]$ をヒープの根とする．
   規則 2 $2k \leq n$ ならば，$\mathbf{X}[k]$ の左の子を $\mathbf{X}[2k]$ とする．さもなければ，$\mathbf{X}[k]$ の左の子は存在しない．
   規則 3 $\boxed{\text{(A)}} \leq n$ ならば，$\mathbf{X}[k]$ の右の子を $\mathbf{X}[\boxed{\text{(A)}}]$ とする．さもなければ，$\mathbf{X}[k]$ の右の子は存在しない．
   規則 4 各配列要素 $\mathbf{X}[k]$ $(k = 1, \ldots, n)$ に，$I[i]$ $(i = 1, \ldots, n)$ を 1 つずつ格納する．この時，何れの親子同士についても，$I[i] \boxed{\text{(B)}} I[j]$ となるように $\mathbf{X}[k] = I[i]$，$\mathbf{X}[2k] = I[j]$（または $\mathbf{X}[\boxed{\text{(A)}}] = I[j]$）と格納する．

   この時，以下の問いに答えよ．

   (i) $\boxed{\text{(A)}}$ に入る数式と $\boxed{\text{(B)}}$ に入る不等号を答えよ．

   (ii) 図 1 は上記規則に従って，9 個の要素からなる $\mathbf{S}$ について，各要素の整数を $\mathbf{X}[k]$ $(k = 1, \ldots, 9)$ に格納したヒープを表す．四角の上の数字は $\mathbf{X}[k]$ の要素番号 $k = 1, \ldots, 9$ を，四角の中の数字は $I[i]$ $(i = 1, \ldots, 9)$ を表す．さらに $I[10] = 69$ を 10 番目の配列要素 $\mathbf{X}[10]$ として追加し，最少回数の親子同士の交換を行って新たなヒープを構成する．得られるヒープを配列 $\mathbf{X}[k]$ $(k = 1, \ldots, 10)$ を用いて図示せよ．

k	1	2	3	4	5	6	7	8	9
$\mathbf{X}$	78	28	65	18	24	55	12	5	8

図 1 整数を持つ 9 個の要素からなる集合 $\mathbf{S}$ を 9 個の要素からなる配列 $\mathbf{X}$ に格納したヒープ

   (iii) 図 2 は図 1 の $\mathbf{X}[k]$ $(k = 1, \ldots, 9)$ によって構成されるヒープから，最大整数を持つ最初の要素 $\mathbf{X}[1] = 78$ を削除し，$\mathbf{X}[1]$ に最後の要素 $\mathbf{X}[9] = 8$ を移動した配列 $\mathbf{X}$ を表す．この配列から，最少回数の親子同士の交換を行って新たなヒープを構成する．得られるヒープを配列 $\mathbf{X}[k]$ $(k = 1, \ldots, 8)$ を用いて図示せよ．

k	1	2	3	4	5	6	7	8
$\mathbf{X}$	8	28	65	18	24	55	12	5

図 2 図 1 のヒープから先頭の最大整数を削除し最後の要素を先頭に移動した配列 $\mathbf{X}$

2. キューとスタックに関する以下の問いに答えよ．
   (i) キューとスタックの違いを説明せよ．
   (ii) キューに既に格納されている要素数を N とし，さらにそれに対してある期間内に合計で n 回の要素の追加と取り出しが行われるとする．ただし，$N \gg n$ である．n 回の内で追加の回数を k $(0 \leq k \leq n)$ とした時，k が以下の二項分布

$$P(k) = \frac{n!}{k!(n-k)!} p^k (1-p)^{n-k}$$

   に従うとする．ここでは特に要素が追加される確率 p が取り出される確率 $1-p$ より大きい $(p > 0.5)$ とする．この時，n 回の追加または取り出しによるキューに格納される要素数の増分 m の期待値と標準偏差を求めよ．また，スタックについてはどうか説明せよ．
   (iii) n が大きく問 (ii) の二項分布が正規分布で近似可能である場合，いま考えている期間内にキューやスタックの長さが成長しても，十分な確率ですべての要素を格納可能な配列長をその理由と共に論ぜよ．

専門用語の英訳

ヒープ	heap
キュー	queue
配列	array
根	root
格納	store
親子同士	parent-child relationship
二項分布	binomial distribution
期待値	expectation
標準偏差	standard deviation

【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 公開鍵暗号化方式では，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，$ed = 1 \pmod{L}$ となる $1<d<L$ 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 （ただし，$1<m<n$）は，公開鍵 e, n を用いて，$c = m^e \pmod{n}$ により暗号文 c に暗号化される．一方，暗号文 c は，公開鍵 n 及び秘密鍵 d を用いて，$m = c^d \pmod{n}$ により平文 m に復号される．RSA 公開鍵暗号化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) (i)の鍵を用いて，平文 $m = 3$ を暗号化した暗号文 c を求めよ．

(iii) $c = m^e \pmod{n}$ をバイナリ法で計算する場合の計算量は，法 n の剰余乗算の回数とする．ここで法 n の剰余乗算とは，$1 \leqq a, b<n$ となる a, b に対して，$ab \pmod{n}$の計算を意味し，$a = b$ のとき，乗算といい，$a \neq b$ のとき，2 乗算という．1 回の剰余乗算の計算時間を乗算，2 乗算ともに M で表すとき，暗号化にかかる計算時間を M で表せ．ただし，e の大きさは 1021 ビットとし，e の最上位ビットは 1，最上位ビット以外の各ビットは 1/2 の確率で 1 になると考える．

(iv) RSA 暗号では高速化のために，e の大きさを押さえることが行われる．e の大きさを 63 ビットとしたときの暗号化にかかる計算時間を求め，(iii)と比べて計算時間が何%削減されるか求めよ．ただし，e の最上位ビットは 1，最上位ビット以外の各ビットは 1/2 の確率で 1 になると考える．

2. 暗号では素数が重要となる．素数の生成について，以下の問いに答えよ．

(i) $5^{7-1} = 1 \pmod{7}$となることを示せ．

(ii) p が素数ならば，p と互いに素な正整数 a に対して $a^{p-1} = 1 \pmod{p}$ となることを示せ．

(iii) (ii)の命題の逆を記述せよ．

(iv) 命題の逆は真とは限らない．(iii)を利用して，正整数 p が与えられたとき，p が素数であるかどうか判定するアルゴリズムを記述せよ．ただし，(iii)が偽となる確率を T とし，正整数 k に対して，確率 $1 - T^k$ で，アルゴリズムは素数であると判定する．

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
平文	plaintext
暗号文	ciphertext
バイナリ法	binary exponentiation
計算量	computational complexity
剰余乗算	modulo multiplication
乗算	multiplication
2 乗算	square
命題	proposition
逆	converse