平成 31 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１５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．

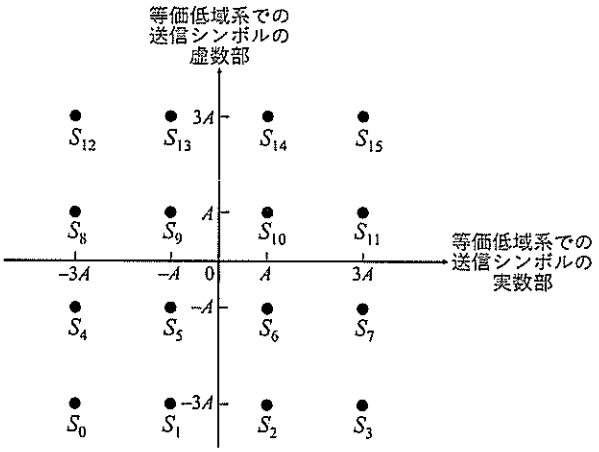
3．解答開始前に，別紙の「専門科目試験問題選択票」に記載の注意事項も読んでおくこと．

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．

16QAM (Quadrature Amplitude Modulation) は，図に示されるように，振幅と位相が異なり，かつ直交座標上で等間隔に配置された 16 個のシンボルを用いて，1 シンボル当たり 4 ビットの情報を伝送できる変調方式である．その受信信号の時間領域表現 $y(t)$は，次式で表されるものとする．

$$y(t)=\mathrm{Re}\left[u(t)e^{j2\pi f_c t}\right]+n(t)$$



16QAM のシンボル配置

ここで Re[x]は x の実数成分を表す関数，$u(t)$は被変調信号の等価低域系表現であり，$u(t)$の実数成分は $u_I(t)$, 虚数成分は $u_Q(t)$で表されるものとする．なお図における A は任意の正の定数である．また，f_c は搬送周波数，t は時刻，$n(t)$は加法性白色ガウス雑音とする．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，送信時に適用される，4 ビット系列を 1 シンボルにマッピングするビットマッピング則に対応させて，復調されたシンボルから 4 ビットの系列が再生されるものとするとき，以下の問いに答えよ．ただし，送信機で生成される 16 個のシンボルの生起確率はそれぞれ 1/16 であるものとする．

(i) 図に示される 16QAM のシンボル配置において，送信されたシンボルと受信機で判定されたシンボルが異なるときシンボル誤りが発生し，同様に，送信されたビットと受信機で判定されたビットが異なるとき，ビット誤りが発生したとする．16QAM の場合のシンボル誤りのほとんどは，最も近接しているシンボルへの誤りであるという前提が成立するものとする．ビット誤り率を最小化するためには，送信機におけるシンボルへのビットマッピング処理において上記の特徴をどのように利用すればよいかを説明せよ．

(ii) 図に示される 16QAM の信号点配置においては，それぞれのシンボルのシンボル誤りの発生確率（シンボル誤り率）はシンボルによって異なり，それらはシンボル誤り率に応じて複数のグループに分けることができる．そのグループの数を示すとともに，各グループの特徴を説明せよ．また各グループには，どの送信シンボルが属するかを，図に示される S_0〜S_{15} を用いて示せ．

(iii) 16QAM のシンボル誤り率の導出に際しては，最も近接しているシンボルへの誤りだけを考慮するという近似が適用可能という前提のもとで，問い(i)における「ビット誤りを最小化する手段」を各シンボルへのビットマッピング手法として適用した場合の，16QAM の平均ビット誤り率を導出せよ．ただしシンボル i から最も近接している隣接シンボル j に誤るシンボル誤り率は $P_{16\mathrm{QAM}}(i\to j)$で与えられるものとする．

専門用語の英訳

振幅	amplitude
位相	phase
時間領域表現	time-domain representation
情報	information
送信信号	transmitted signal
受信信号	received signal
送信機	transmitter
受信機	receiver
直交座標	orthogonal coordinate
変調	modulation
復調	demodulation
被変調信号	modulated signal
実数成分	real component
虚部成分	imaginary component
等価低域系	equivalent lowpass system
搬送周波数	carrier frequency
加法性白色ガウス雑音	additive white Gaussian noise
誤り訂正符号	error correction code
マッピング則	mapping rule
生起確率	probability of occurrence
シンボル誤り率	symbol error rate
ビット誤り率	bit error rate

【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 個の無線端末を収容している基地局を考える．ただし $N \geq 2$ である．時間軸はスロットに分割されており，各無線端末は各スロットにおいて高々 1 パケットを基地局へ送信できる．各スロットにおいて，パケット送信を行った無線端末が一つの場合，そのパケット送信は成功するが，複数の場合には衝突が発生し，パケット送信は失敗すると仮定する．各端末は送信すべきパケットを常に保持していると仮定して以下の問いに答えよ．

(i) 各端末は，他の端末とは独立に，スロット毎に確率 p でパケットを送信し，確率 $1-p$ でパケットを送信しないと仮定する．ただし $0 < p < 1$.

  (a) ある特定の端末のスループット θ_1（パケット／スロット）を求めよ．

  (b) スループット θ_1 が最大となる p の値 p^* を求めよ．

(ii) 連続する M 個 $(M \geq 2)$ のスロットをフレームと呼ぶ．すなわち，k 番目 $(k = 1, 2, \ldots)$ のフレームは $(k-1)M+1$ 番目から kM 番目のスロットで構成される．各端末は，各フレームごとに，他の端末とは独立に，同じ確率 $1/M$ で一つのスロットを選択し，パケットを送信すると仮定する．

  (a) ある特定の端末のスループット θ_2（パケット／スロット）を求めよ．

  (b) スループット θ_2 が最大となる M の値 M^* を求めよ．

(iii) p^* を用いた前問 (i) のシステムと M^* を用いた前問 (ii) のシステムにおける性能の違いを端末側の視点から議論せよ．

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
パケット：	packet
確率：	probability
スループット：	throughput
フレーム：	frame

【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）とミラー（M_1 と M_2）から構成される干渉計に，波長λ_0の水平直線偏波・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 BS で２つに分岐され，ミラーM_1およびM_2が配置された光路１および光路２を経て，再度ビームスプリッタ BS で合波される．そして，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．図２に示すように，ビームスプリッタでは，入射された光ビームのパワーの R 倍が反射され，T 倍が透過される．ビームスプリッタおよびミラーでの損失は無視できるものとする．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．

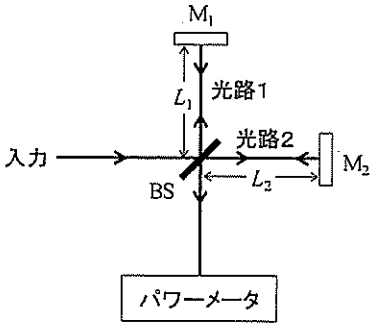


図１

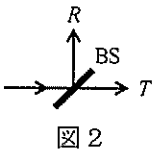


図２

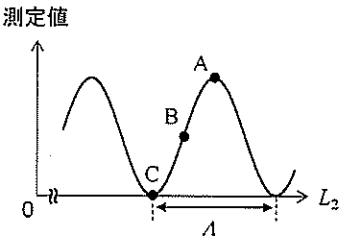


図３

光路２におけるビームスプリッタ BS とミラーM_2の間の距離を L_2 とする．今，光路２と並行な方向にミラーM_2を動かし L_2 を変化させると，図３に示すように，測定値が正弦的に変化する．

(i) 図３における周期Λを，λ_0 を用いて表せ．その理由も示せ．

(ii) 光路１におけるビームスプリッタ BS とミラーM_1の間の距離を L_1 とする．L_1 と L_2 が正確に等しいとき，パワーメータの測定値は図３における A，B，C のどの点と等しくなるかを答えよ．また，その理由も示せ．

(iii) 今，パワーメータの測定値が図３における点 B にあるとする．このとき，光ビームの波長を長波長側に連続的に微調した場合，測定値は大きくなるか小さくなるかを答えよ．また，その理由も示せ．

(iv) 測定のピーク値（図３の点 A における値）が最大となるビームスプリッタ BS の分岐比 R と T を示せ．その理由も説明すること．

(v) 図１に示す干渉計の工学応用例を挙げよ．

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
波長：wavelength
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：power
パワーメータ：power meter

【情報理論】 解答は，桃色の解答用紙に記入すること．

1. 生成多項式$G(z)=1+z+z^3$を用いて，4 個の情報ビット$x_0,x_1,x_2,x_3\in\{0,1\}$からなる情報語$(x_0,x_1,x_2,x_3)$（ただし，多項式表現では，2 を法とする加算と乗算を用いて，$X(z)=x_0+x_1z+x_2z^2+x_3z^3$と表される）を符号化する巡回符号を考える．この巡回符号では，多項式$X(z)z^3$を$G(z)$で割った剰余多項式$R(z)$を用いて符号多項式 $W(z)=X(z)z^3+R(z)$を求め，$W(z)$の 0 次から 6 次の項の係数を次数の低いものから並べたビット系列を符号語とする．この巡回符号について以下の問いに答えよ．

(i) 符号化率を求めよ．

(ii) 情報語(1,1,0,0)の符号語を求めよ．

(iii) この巡回符号で生成された符号語に対し，伝送路で 1 ビット以下の誤りが加わり，(1,0,1,0,0,1,1)が受信された．このとき，受信語に誤りがあるか判定し，誤りがあればその位置を示せ．

(iv) (1,0,1,0,0,1,1)が受信されたとき，2 ビットのバースト誤りのみが発生するとして，誤りの位置を求めよ．

(v) この巡回符号は連続する何ビット以下のバースト誤りを検出できるか，その理由と共に答えよ．ただし，bビットのバースト誤りは$1e_1e_2\cdots e_{b-2}1$（$e_i\in\{0,1\}$）と表されるものとする．

2. 図 1 に示す符号器により生成される畳み込み符号を考える．この符号器は 1 入力ビットを記憶するレジスタM_1，M_2，排他的論理和演算を行う 2 を法とする加算器⊕，及び並直列変換器により構成される．この符号器は，時点i（$i=1,2,\cdots$）において情報ビットx_i（$x_i\in\{0,1\}$）が入力されたとき，時点$i-1$及び$i-2$に入力された情報ビットx_{i-1}，x_{i-2}がレジスタに記憶されており，x_i，x_{i-1}，x_{i-2}の加算により得られる 2 つのビットw_{i1}，w_{i2}（w_{i1}，$w_{i2}\in\{0,1\}$）を出力する．その後，レジスタに記憶する情報ビットを 1 段ずつシフトする．この符号器により生成される畳み込み符号について以下の問いに答えよ．ただし，レジスタの初期値は 0 とする．

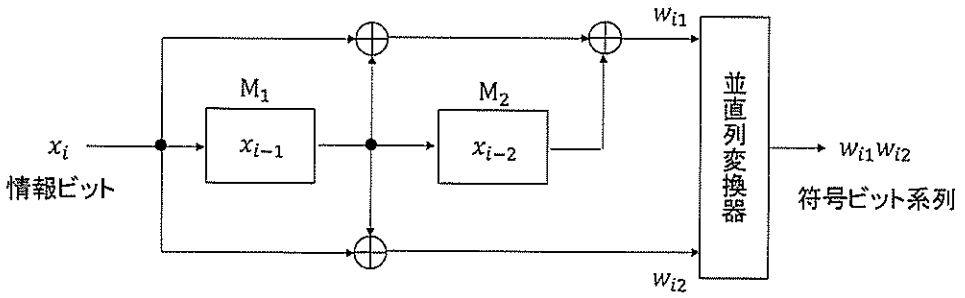


図 1：畳み込み符号器

(i) この符号器の符号化率，及び拘束長を求めよ．

(ii) 情報ビット系列 1011 が入力されたとき得られる符号ビット系列を求めよ．

(iii) レジスタM_1，M_2に記憶されたビットx_{i-1}，x_{i-2}の値に応じて符号器の状態を$S(x_{i-1}x_{i-2})$と表すとき，符号器の状態遷移図を，符号器に入力される情報ビットx_i，符号器から出力される符号ビット系列$w_{i1}w_{i2}$と共に示せ．

専門用語の英訳

生成多項式	generator polynomial
情報ビット	information bit
情報語	information word
多項式表現	polynomial representation
2 を法とする	modulo-two
巡回符号	cyclic code
剰余多項式	residual polynomial
符号多項式	code polynomial
係数	coefficient
符号語	codeword
符号化率	code rate
受信語	received word
バースト誤り	burst error
畳み込み符号	convolutional code
レジスタ	register
排他的論理和演算	exclusive OR operation
加算器	adder
並直列変換器	parallel to serial converter
拘束長	constraint length
状態遷移図	.state transition diagram

【信号処理】解答は，だいだい色の解答用紙に記入すること．

入力信号 $x[n]$ を処理し出力信号 $y[n]$（n は時刻を表す整数）を生成する離散時間信号処理システム L

$$y[n] = L[\, x[n] \,] \tag{1}$$

を考える．以下の問いに答えよ．

(i) 離散時間信号処理システムにおける線形性の定義を数式を用いて述べよ．また，線形なシステムとそうでないシステムの具体例を一つずつ挙げ，各々が定義を満たすこと，または満たさないことを示せ．

(ii) 離散時間信号処理システムにおける時不変性の定義を数式を用いて述べよ．また，時不変なシステムとそうでないシステムの具体例を一つずつ挙げ，各々が定義を満たすこと，または満たさないことを示せ．

以下の問いでは，システム L が線形かつ時不変であるとして答えよ．

(iii) システム L では，そのインパルス応答 $h[n]$ と入力信号 $x[n]$ の畳込みにより出力信号 $y[n]$ が与えられること，すなわち

$$y[n] \;=\; h[n] * x[n] \;\triangleq\; \sum_{k=-\infty}^{\infty} h[n-k]x[k]$$

となること（$*$ は畳込み演算記号）を，式 (1) より導出せよ．

(iv) システム L のインパルス応答，周波数応答，伝達関数について，各々の定義や性質を数式を交えて説明せよ．また，これらの相互関係を詳しく説明せよ．

専門用語の英訳	
入力信号	input signal
出力信号	output signal
離散時間信号処理システム	discrete-time signal processing system
線形	linear
時不変	time-invariant
インパルス応答	impulse response
畳込み	convolution
周波数応答	frequency response
伝達関数	transfer function

【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. 非負の2進整数 $X = (x_N x_{N-1} \ldots x_k x_{k-1} \ldots x_1 x_0)$ と $Y = (y_N y_{N-1} \ldots y_k y_{k-1} \ldots y_1 y_0)$ を比較する比較器の回路を構成することを考える（N, k は $1 \leq k \leq N$ を満たす整数とし，X, Y においては添え字の小さい方が下位ビットとする）．この比較器の出力 z_N は，$X < Y$ のとき $z_N = 1$，$X \geq Y$ のとき $z_N = 0$ になるとする．この比較器を構成するにあたり，X と Y の $k+1$ 桁目まで，すなわち，$(x_k x_{k-1} \ldots x_1 x_0)$ と $(y_k y_{k-1} \ldots y_1 y_0)$ の比較結果 z_k を出力する1ビット比較器（CMP）の回路を用いることを考える．この回路の入力は図1に示すように，X と Y の k 桁目までの比較結果 z_{k-1} および，x_k, y_k とする．
このとき，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は，論理ゲートを表す際には図2に示した記号を用い，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．また，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1ビット比較器（CMP）の出力 z_k を，$x_k < y_k$，$x_k > y_k$，$x_k = y_k$ の場合にわけて，$0, 1, z_{k-1}$ を用いて表せ．
   (ii) この1ビット比較器（CMP）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．
   (iii) 問い(ii)で設計した1ビット比較器（CMP）の回路を用いて，X および Y を比較した結果 z_N を出力する比較器の回路図を示せ．なお，この比較器の回路の入力は，X および Y の各ビット（$x_N, x_{N-1}, \ldots x_1, x_0$ および $y_N, y_{N-1}, \ldots y_1, y_0$）とする．ただし，問い(ii)で設計した1ビット比較器（CMP）の回路は図1で示した記号を用いて表すこと．

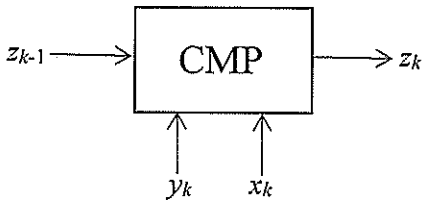


図1：1ビット比較器（CMP）の記号

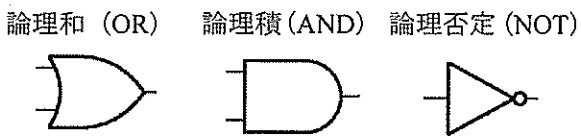


図2：論理ゲートの凡例

2. 固定小数点表示での数の表現に関する以下の各問いに答えよ．ビット列の最上位桁を符号桁（正を0，負を1）とし，小数点位置は最下位桁の右側とする．負の数の表現には2の補数表現を用いる．2の補数とは n 桁の2進整数 X に対して $2^n - X$ である．
   (i) 8ビットで表現できる数の範囲を10進数で示せ．
   (ii) 多くの計算機では負の数を表現するのに，1の補数表現ではなく，2の補数表現が使われる．この利点を複数述べよ．なお1の補数表現とは，n 桁の2進整数 X に対して $2^n - X - 1$ である．
   (iii) 10進数表現での $-13-10$ を2の補数表現を用いて計算せよ．過程も示すこと．ただし，数は6ビットで表されているものとする．
   (iv) 数が5ビットで表されている時，問い(iii)の計算を行うとオーバーフローが生じて誤った答が得られる．これをビット列での計算過程を用いて示せ．
   (v) 問い(iii)(iv)の結果を踏まえ，2進整数 A，B の加算 $S = A + B$ においてオーバーフローを検出する条件を考える．その条件を，被加数 A，加数 B，和 S の符号桁をそれぞれ a，b，s として，これらを用いた論理式で示せ．

専門用語の英訳

2 進整数	binary integer number
比較器	comparator
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

固定小数点表示	fixed-point number representation
最上位桁	most significant bit
符号桁	sign bit
最下位桁	least significant bit
2 の補数	two's complement
1 の補数	one's complement
オーバーフロー	overflow
被加数	augend
加数	addend
和	sum

【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. ハッシュ法は，与えられたデータ (要素の集合) 内に，質問した要素（探索キー）が含まれているかどうかを答える探索問題に対する代表的な手法の一つである．配列を用いたハッシュ法に関するプログラム A について，以下の問い (i)〜(iv) に答えよ．なお，プログラム A は C 言語で書かれている．またプログラム A の下に，実行後のコンソール出力を示す．

プログラム A

```
#define N 13
#define M 17

// ハッシュ関数
int hash(int x) {
    return x%M;
}

// データ（要素の集合）を配列に蓄える手続き
void store(int *htb, int *data, int n) {
    for ( int i=0; i<n; i++ ) {
        int j = hash(data[i]);
        while( htb[j]!=[ 1 ] )
            j = (j+1)%M;
        htb[j] = data[i];
    }
}

// 与えられた要素を探索する手続き
int search(int *htb, int x) {
    int j = hash(x);
    while( htb[j]!=[ 2 ] & htb[j]!= x)
        j = (j+1)%M;
    if ( htb[j]==[ 3 ] )
        return j;
    else
        return -1;
}

// 与えられた要素を配列から削除する手続き
void delete(int *htb, int x) {
    [        (a)        ]
}

int main(void) {
    int x, htb[M];
    for ( int i=0; i<M; i++ )
        htb[i] = 0;

    int data[N] = {2,3,6,7,8,11,14,15,17,18,19,20,22};
    store(htb,data,N);
    x = search(htb,20);
    printf("'20' is found at %d\n", x);

    delete(htb,19);
    x = search(htb,20);
    printf("'20' is found at %d\n", x);

    return 0;
}
```

(B)

[プログラム A 実行後の出力]
```
'20' is found at 5
'20' is found at 5
```

(i) プログラム A 内の (B) の部分が正しく動くように空欄 1 ～ 3 を埋めよ.

(ii) プログラム A を実行後の配列 htb 内の要素を順に示せ.

(iii) ハッシュ法の性能 (比較回数) について,「データ数」(プログラム A 中では N) と「ハッシュ表のサイズ」(プログラム A 中では M) という単語を用いて簡潔に述べよ.

(iv) ハッシュ法において配列から要素を削除する際には, 単にその要素が格納されているデータを配列から削除する (該当箇所を 0 で初期化する) のみでは, その後に探索を実行する際に正しく動作しなくなる問題が生じる. その理由について簡潔に述べるとともに, この点に注意して, プログラムが正しく動作するように空欄 (a) を埋めて関数 delete を完成させよ. なお, 空欄 (a) は数行にわたって記述してよい. また, データ中の要素としては正の整数のみが処理されることを想定してよい.

2. 各々が等しい長さ n (≥ 1) の配列である M (≥ 2) 個のブロック A_i ($i = 1, \ldots, M$), および区間 $[0, 1]$ に分布しかつ最小値 0, 最大値 1 を含む $N = Mn$ 個の数値からなる集合 S が与えられている. これらの数値をあらかじめ昇順にソートして M 等分割し, $i = 1, \ldots, M$ の順番に A_i に格納する. すなわち, A_i の j 番目の要素を $A_i[j]$ ($j = 1, \ldots, n$) と表すと, 各 A_i ($i = 1, \ldots, M$) について $A_i[j] \leq A_i[j+1]$ ($1 \leq j \leq n-1$), 各 A_i ($i = 1, \ldots, M-1$) について $A_i[n] \leq A_{i+1}[1]$, かつ $A_1[1] = 0$, $A_M[n] = 1$ である. 別に 区間 $[0, 1]$ 内に存在する 1 個の数値 x が与えられた時, これらのブロックを用いて以下の手順で x が S に属するか否かを調べる.

(1) $i = 1$ から M に向かって昇順に $A_i[n]$ と x を比較し, 最初に $A_i[n] \geq x$ となる i を求める.

(2) A_i の内部を探索し, x が含まれるか否かを調べる.

手順 (2) においては, 以下の 2 種類の何れかの探索手法を用いる.

- 逐次探索法 : $j = 1$ から n に向かって昇順に $A_i[j]$ と x を比較し, 最初に $A_i[j] \geq x$ となる j について, $x = A_i[j]$ であれば x は S に属し, そうでなければ x は S に属さないと判定し終了する.
- m-ブロック探索法 : A_i をさらに各々が等しい長さ h (≥ 1) の配列である m (≥ 2) 個のブロック B_k ($k = 1, \ldots, m; n = mh$) に m 等分割し, $k = 1$ から m に向かって昇順に $B_k[h]$ と x を比較し, 最初に $B_k[h] \geq x$ となる k を求め, B_k の内部を逐次探索法で調べ, x が S に属するか否かを判定し終了する.

なお, 常に N は n で割り切れ, n は h で割り切れるものとする. また, n や h は本来は整数であるが、解析の都合上, 連続な値を取る実数と見なしてよい. 上記の探索アルゴリズムについて以下の問いに答えよ.

(i) 手順 (2) において逐次探索法を用いる場合, 手順 (1) と手順 (2) を合わせた最悪の比較回数を N と n を用いて理由と共に答えよ.

(ii) N が一定である場合, (i) の最悪の比較回数を最小化する n を N を用いて表す式を導出せよ.

(iii) 手順 (2) において最悪の比較回数が最小となる h を用いる m-ブロック探索法を用いる場合, 手順 (1) と手順 (2) を合わせた最悪の比較回数を N と n を用いて理由と共に答えよ.

(iv) N が一定である場合, (iii) の最悪の比較回数を最小化する n を N を用いて表す式を導出せよ.

専門用語の英訳

ハッシュ表	hash table
ハッシュ関数	hash function
探索キー	search key
探索問題	search problem
配列	array
区間	interval
昇順	ascending order
ソート	sort
配列	array
ブロック	block
比較	comparison
逐次探索法	sequential search method
m-ブロック探索法	m-block search method

【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．以下の拡張ユークリッドアルゴリズム A について問い(i)-(iv)に答えよ．
アルゴリズム A（入力：二つの整数a, b（ただし$a > b \geq 0$））
[ステップ 1] $z_0 = a, z_1 = b, x_0 = 1, x_1 = 0, y_0 = 0, y_1 = 1, i = 1$ と代入する．
[ステップ 2] もし$z_i = 0$ ならば $d = z_{i-1}, x = x_{i-1}, y = y_{i-1}$ を出力して停止する．
[ステップ 3] もし$z_i \neq 0$ ならば z_{i-1} を z_i で割った商を q_i，余りを z_{i+1} として，$x_{i+1} = x_{i-1} - q_i x_i$, $y_{i+1} = y_{i-1} - q_i y_i$ かつ $i = i + 1$ と代入してステップ 2 へ戻る．

(i) A に $a = 5$, $b = 3$ を入力したとき，A が停止するまでに計算される数列 $(z_0, z_1, \ldots)$ を求めよ．
(ii) $i = k$ で A が停止したとき，任意の $j \in \{0, \ldots, k-1\}$ で $ax_j + by_j = z_j$ であることを示せ．
(iii) $i = k$ で A が停止したとき，任意の $j \in \{1, \ldots, k-1\}$ で $GCD(z_j, z_{j+1}) = GCD(z_{j-1}, z_j)$ であることを示し，$d = GCD(a, b)$ が成立することを示せ．ただし異なる二つの整数 m, n に対して $GCD(m, n)$ は m と n の最大公約数を表す．また整数 $n \geq 0$ に対して $GCD(n, 0) = n$ とする．
(iv) p を素数，n を $1 \leq n \leq p-1$ となる整数とする．このとき A を用いて p を法とする n の乗法に関する逆元を求める方法を与えよ．ただし p を法とする n の乗法に関する逆元とは $nm \equiv 1 \pmod{p}$ を満たす整数 m $(1 \leq m \leq p-1)$ である．

2．n ビット入力 k ビット出力のハッシュ関数 h: $\{0,1\}^n \to \{0,1\}^k$ （ただし$n > k$）について問い(i)-(iii)に答えよ．
(i) $2^k + 1$ 個の異なる入力について h を計算すれば必ず衝突が発見できる，つまり $h(x) = h(x')$ となる入力の組 (x, x') が発見できることを示せ．
(ii) 各入力 $x \in \{0,1\}^n$ に対するハッシュ関数の出力値 $h(x)$ が $\{0,1\}^k$ 上で一様かつ他の入力に対する出力値とは独立にランダムに決まるとする．ある $y \in \{0,1\}^k$ が与えられたとき，y で衝突が発生する，つまり $h(x) = h(x') = y$ となる異なる入力 $x, x' \in \{0,1\}^n$ が存在する確率を求めよ．
(iii) 各入力 $x \in \{0,1\}^n$ に対するハッシュ関数の出力値 $h(x)$ が $\{0,1\}^k$ 上で一様かつ他の入力に対する出力値とは独立にランダムに決まるとする．ある異なる t 個の入力の集合 T が与えられたとき，衝突を発生させる入力の組が集合 T の中に存在する，すなわち $h(x) = h(x')$ となる異なる $x, x' \in T$ が存在する確率を求めよ．

専門用語の英訳	
拡張ユークリッドアルゴリズム	extended Euclidean algorithm
最大公約数	greatest common divisor
法	modulo
逆元	inverse
ハッシュ関数	hash function
衝突	collision