問題 1

図 1 のように透磁率 μ_0 の媒質中の xy 平面上に，一辺が $2a$ の正方形の巻数 N の十分細いコイル A がある．このコイルの中心は xyz 空間の原点 O にある．また $b > a > 0$ なる $x = -b$，$z = 0$ に y 方向に無限に長い細い直線導体 B があり，y の正から負の向きに一定の電流 I_B が流れている．ただし，これらの導体の透磁率も μ_0 とせよ．

(1) 図 1 の xy 平面上の点 P $(x, y, 0)$（ただし $x \neq -b$）を考える．I_B により点 P に生ずる磁束密度 $\boldsymbol{B}(x)$ を求めよ．

(2) コイル A に図 1 のように一定の電流 I_A が流れている．このときコイル A 上の線素ベクトル $\mathrm{d}\boldsymbol{s}$ に働く磁気力 $\mathrm{d}\boldsymbol{F}$ を示せ．ただし，$\mathrm{d}\boldsymbol{s}$ の向きはコイルの電流と同じ向きとする．

(3) 問(2)の結果に基づきコイル A に働く力の大きさと向きを求めよ．

(4) 電流 I_B により発生しコイル A に鎖交する磁束を求めよ．

(5) コイル A と直線導体 B の相互インダクタンスを求めよ．

(6) 問(5)を利用して，コイル A と直線導体 B の間に働く力の大きさと向きを仮想変位の原理に基づき求めよ．

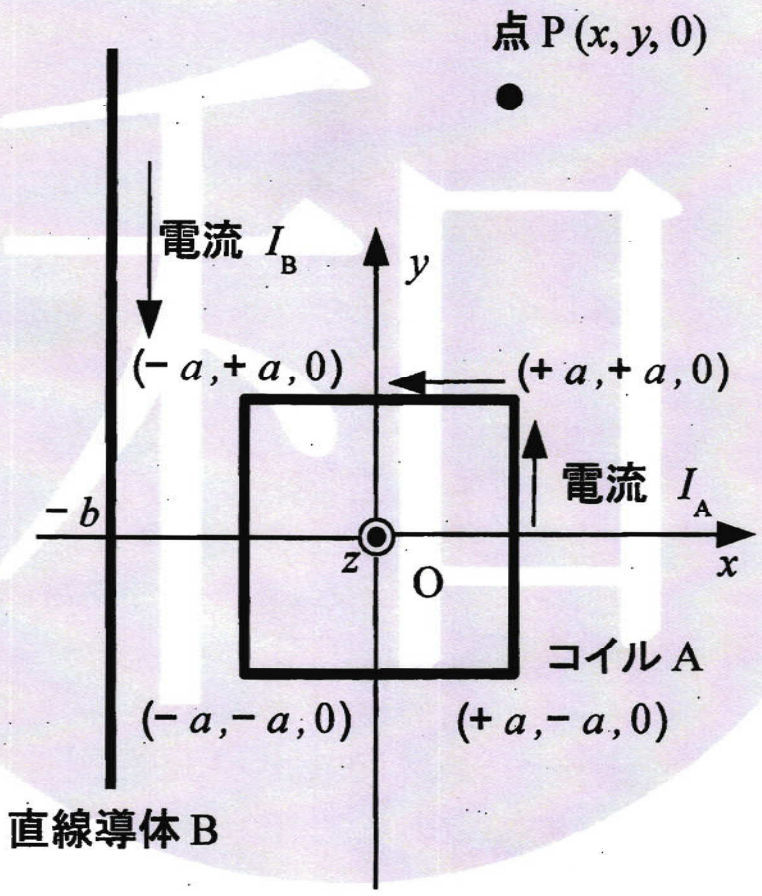


図 1

Problem 1

As shown in Fig. 1, there is a sufficiently thin square coil A of side length $2a$ and of winding number N in a medium with magnetic permeability μ_0 on the xy-plain. Its center is at the origin O of the xyz-space. There is a fine line conductor B which is infinitely long in the y-direction at $x=-b$ and $z=0$, where $b>a>0$. A constant current I_B flows in the y-direction from positive to negative in conductor B. Let us assume that the magnetic permeability of these conductors is also μ_0.

(1) Find the magnetic flux density $\boldsymbol{B}(x)$ produced by I_B at a point P $(x, y, 0)$, where $x \neq -b$, on the xy-plain in Fig. 1.

(2) A constant current I_A flows in coil A as shown in Fig. 1. Find the magnetic force $d\boldsymbol{F}$ acting on a line element vector $d\boldsymbol{s}$ in coil A. The direction of $d\boldsymbol{s}$ is identical to that of the coil current.

(3) Find the magnitude and the direction of the force acting on coil A based on the result of Question (2).

(4) Find the magnetic flux produced by current I_B and linked to coil A.

(5) Find the mutual inductance between coil A and line conductor B.

(6) Find the magnitude and the direction of the force between coil A and line conductor B based on the virtual displacement principle using the result of Question (5).

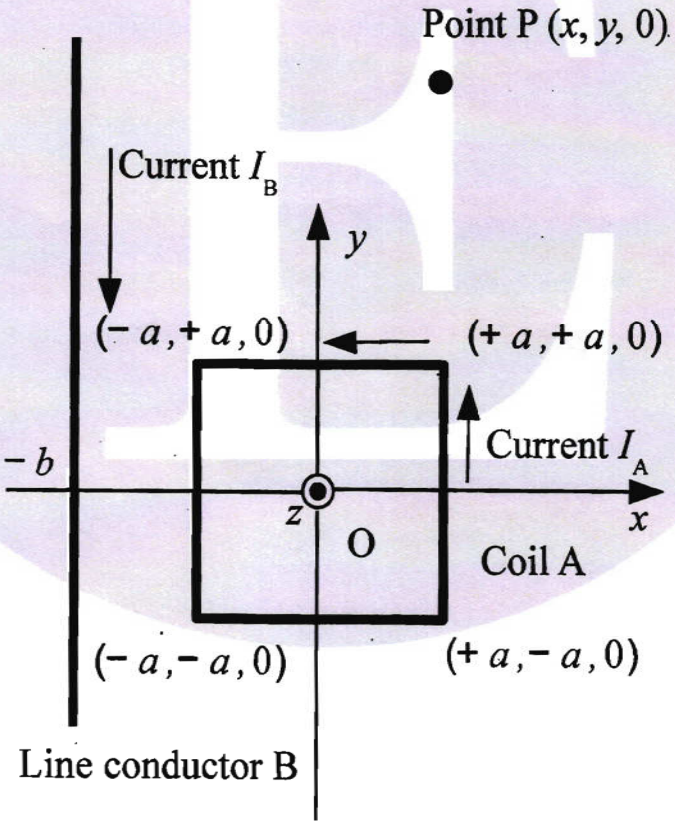


Fig. 1

問題 2

以下の問に答えよ．記号は凡例に従う．演算増幅器に関して，増幅率と入力インピーダンスは無限大，出力インピーダンスはゼロ，出力は飽和しないとする．時刻 $t=0$ においてキャパシタの電荷はゼロ，インダクタの電流はゼロとする．必要であれば時間領域の関数 $f(t)$ に関する以下のラプラス変換の公式を用いてもよい．$u(t)$ は単位ステップ入力である．

$$f(t) \Leftrightarrow F(s) = \int_0^\infty f(t) e^{-st} dt$$

$$u(t) \Leftrightarrow \frac{1}{s}$$

$$e^{-at} u(t) \Leftrightarrow \frac{1}{s+a}$$

$$te^{-at} u(t) \Leftrightarrow \frac{1}{(s+a)^2}$$

$$e^{-at} \sin bt \cdot u(t) \Leftrightarrow \frac{b}{(s+a)^2 + b^2}$$

(1) 図１に示す回路の電流 I を求めよ．

(2) 図２に示す回路について以下の問(2-1) (2-2)に答えよ．図２で $V_0 = 1\,\mathrm{V}$，$R_1 = 4\,\Omega$，$L_1 = 1\,\mathrm{H}$ である．

(2-1) $C_1 = 0.25\,\mathrm{F}$ の時，$t > 0$ での電流 $i(t)$ を求め，$i(t)$ の波形の概形を図示せよ．

(2-2) $C_1 = 0.2\,\mathrm{F}$ の時，$t > 0$ での電流 $i(t)$ を求め，$i(t)$ の波形の概形を図示せよ．

(3) 演算増幅器を用いた回路について以下の問(3-1) (3-2) (3-3)に答えよ．

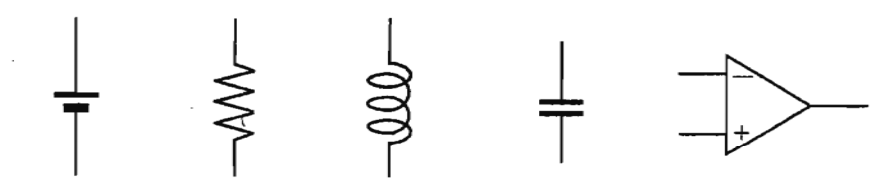
(3-1) 図３に示す回路について，出力電圧 V_{OUT} を入力電圧 V_{IN1}，V_{IN2} を用いて表せ．

(3-2) 図４に示す回路の入力に図５に示す信号を与えた場合，出力電圧波形を図示せよ．ただし，$R_5 = 200\,\mathrm{k}\Omega$，$C_2 = 1\,\mu\mathrm{F}$ とする．

(3-3) 演算増幅器を用いて微分方程式の解を時間変化する電圧波形でシミュレーションする回路を考える．図３と図４に示す回路構成を利用して，式(i)に示す微分方程式の解 $x(t)$ を出力する回路図を図示せよ．ただし，時刻を t (s)，電圧を x (V)，回路の入力電圧を a (V)とし，$x(0) = 0\,\mathrm{V}$ とする．

$$\frac{dx}{dt} - 2x = a \qquad \text{(i)}$$

凡例



直流電圧源　抵抗　インダクタ　キャパシタ　演算増幅器

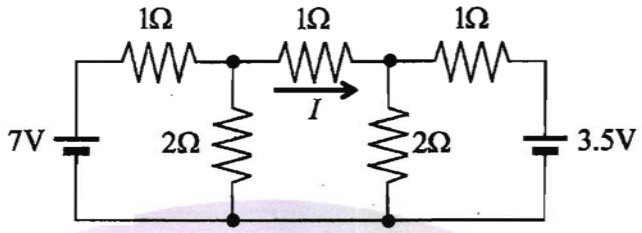


図 1

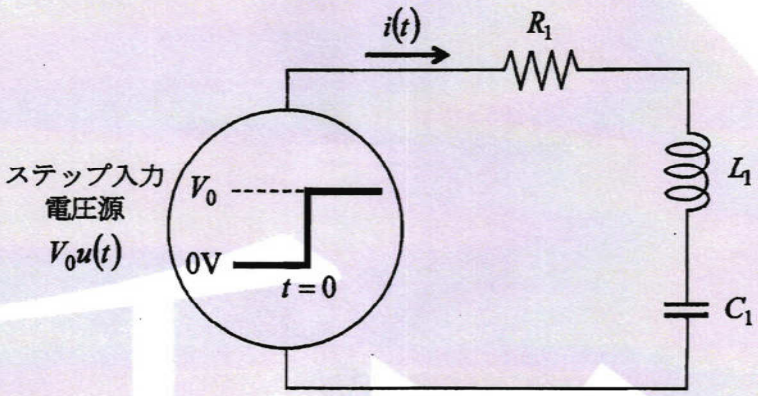


図 2

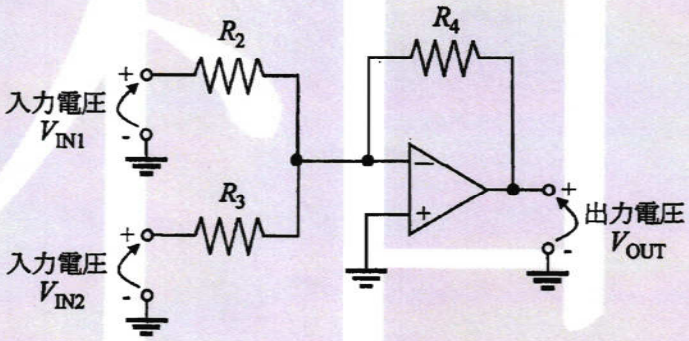


図 3

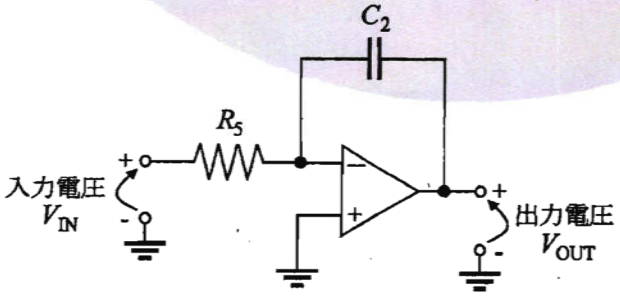


図 4

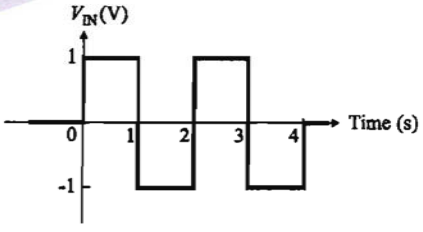


図 5

Problem 2

Answer the following questions. Symbols in the figures can be found in the legend. Assume that the operational amplifier has an infinite gain, an infinite input impedance, and a zero output impedance. Assume that the output of the operational amplifier is never saturated. Assume that, at the time of $t=0$, no charges are stored in the capacitor and no current flows through the inductor. If necessary, use the following formulae of the Laplace transform regarding a time domain function $f(t)$. $u(t)$ is a unit step input.

$$f(t) \Leftrightarrow F(s) = \int_0^\infty f(t)e^{-st}dt$$

$$u(t) \Leftrightarrow \frac{1}{s}$$

$$e^{-at}u(t) \Leftrightarrow \frac{1}{s+a}$$

$$te^{-at}u(t) \Leftrightarrow \frac{1}{(s+a)^2}$$

$$e^{-at}\sin bt \cdot u(t) \Leftrightarrow \frac{b}{(s+a)^2+b^2}$$

(1) Determine the current I in the circuit shown in Fig. 1.

(2) Answer the following questions (2-1) and (2-2) on the circuit shown in Fig. 2, where $V_0 = 1\,\mathrm{V}$, $R_1 = 4\,\Omega$ and $L_1 = 1\,\mathrm{H}$.

(2-1) When $C_1 = 0.25\,\mathrm{F}$, find the current $i(t)$ for $t>0$ and sketch the waveform of $i(t)$.

(2-2) When $C_1 = 0.2\,\mathrm{F}$, find the current $i(t)$ for $t>0$ and sketch the waveform of $i(t)$.

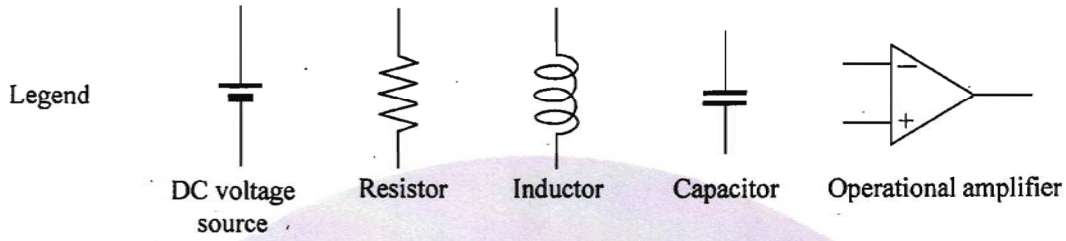
(3) Answer the following questions (3-1), (3-2) and (3-3) on circuits using operational amplifiers.

(3-1) On the circuit shown in Fig. 3, express the output voltage V_{OUT} with the input voltages V_{IN1} and V_{IN2}.

(3-2) The signal shown in Fig. 5 is applied to the input of the circuit shown in Fig. 4, where $R_5 = 200\,\mathrm{k}\Omega$ and $C_2 = 1\,\mu\mathrm{F}$. Draw the waveform of the output voltage.

(3-3) Consider a circuit using operational amplifiers to simulate the solution of a differential equation as a voltage waveform in the time-domain. Draw the circuit whose output voltage simulates the solution $x(t)$ of the differential equation shown in Eq. (i) using the circuit configurations shown in Figs. 3 and 4. Here, the time is t (s), the voltage is x (V), the input voltage of the circuit is set to a (V), and $x(0) = 0$ V.

$$\frac{dx}{dt} - 2x = a \qquad \text{(i)}$$



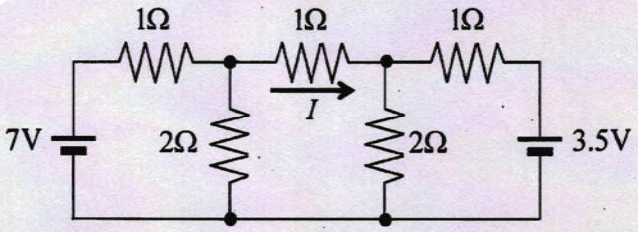


Fig. 1

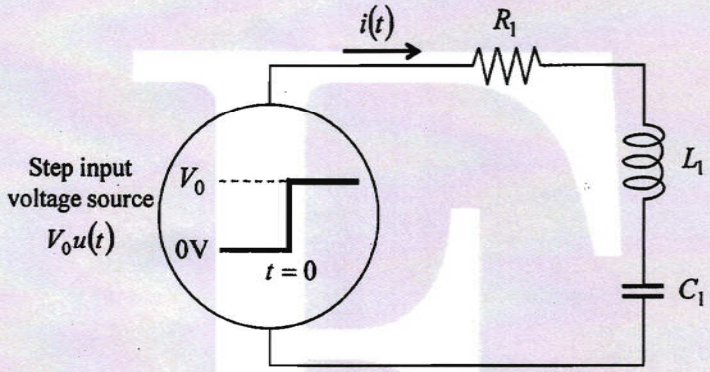


Fig. 2

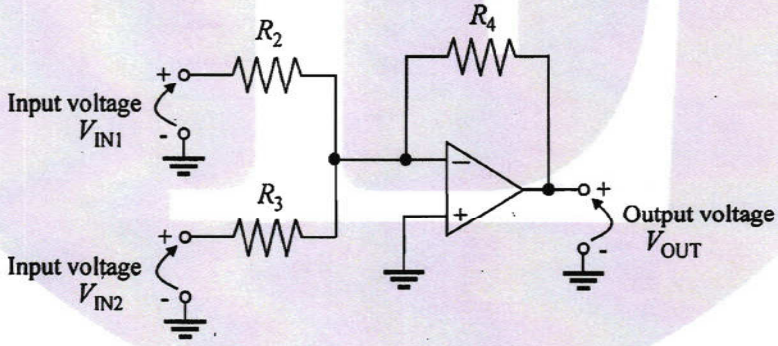


Fig. 3

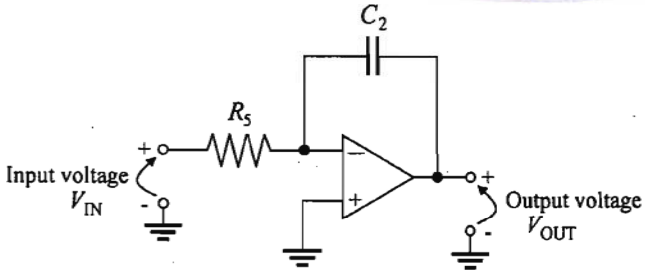


Fig. 4

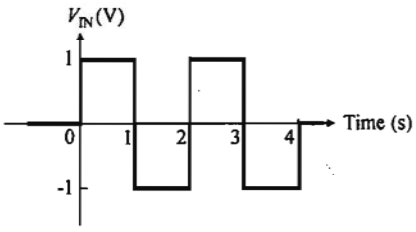


Fig. 5

問題３

天気の情報を符号化することを考える．以下，情報符号化と誤り訂正符号に関する各問に答えよ．ただし，符号語は 0 と 1 で表される２元符号とする．平均符号語長は小数点以下２桁まで求めよ．

(1) いま天気を表す記号が表１に示す符号で表されるものとする．各天気になる確率が等しく 1/5 である場合の平均符号語長を求めよ．また各記号に対する符号語長が表 1 の符号と同一である語頭符号の例を１つ挙げよ．語頭符号とは各符号語が他の符号語の接頭部になっていない符号である．

表１

記号	晴	曇	雨	雪	霧
符号	100	110	10	00	01

(2) 表１に示す各天気となる確率をそれぞれ p(晴)=1/3，p(曇)=1/4，p(雨)=1/6，p(雪)=1/8，p(霧)=1/8 とした場合に，それぞれの確率からハフマン符号を１つ求めよ．また求めた符号の平均符号語長を求めよ．

(3) 表２に示す符号 B は，伝送路において雑音によって発生した誤りを検出するために符号 A から生成したものである．この誤り検出はどのような仕組みか説明せよ．またこの仕組みでは誤りを訂正できないことを説明せよ．

表２

記号	晴	曇	雨	雪	霧
符号 A	000	001	011	010	100
符号 B	0000	0011	0110	0101	1001

(4) ハミング符号化によって誤り訂正が可能な符号を生成する．いまハミング符号のパリティ検査行列 H が式(i)で与えられるものとして生成行列を求めよ．またこの生成行列を用いて表２の符号 A から生成した符号を示し，１つの誤りが生じた場合の例を１つ挙げて検出，訂正の仕組みを説明せよ．

$$H=\begin{bmatrix}0&1&0&1&1&0\\0&1&1&0&0&1\\1&0&1&0&1&0\end{bmatrix} \qquad \text{(i)}$$

(5) 問(4)で生成した符号の誤り訂正能力について説明せよ．またハミング符号化を拡張することで誤り率をさらに改善させる符号化の手法を簡単に説明せよ．

Problem 3

Consider coding weather information. Answer the following questions about the information coding and the error correcting code. Suppose that a codeword is represented by a sequence of binary digits, 0 and 1. Answer the average code length to two decimal places.

(1) Suppose that the symbols of the weather types are represented by the code shown in Table 1. Calculate the average code length when the probabilities of the weather types are all 1/5. Also, give an example of a prefix code that has the same codeword length for each symbol as the code shown in Table 1. Here, a prefix code is a code in which there is no codeword that coincides with a prefix of any other codewords.

Table 1

Symbol	Sunny	Cloudy	Rain	Snow	Fog
Code	100	110	10	00	01

(2) Give a Huffman code when the probabilities of the weather types shown in Table 1 are p(Sunny)=1/3, p(Cloudy)=1/4, p(Rain)=1/6, p(Snow)=1/8 and p(Fog)=1/8. Also, calculate the average code length of the Huffman code.

(3) The code B shown in Table 2 is generated from the code A in order to detect errors caused by noise in a channel. Explain the mechanism of this error detection method. Also, explain why this method cannot correct errors.

Table 2

Symbol	Sunny	Cloudy	Rain	Snow	Fog
Code A	000	001	011	010	100
Code B	0000	0011	0110	0101	1001

(4) Suppose that the code for error correction is generated by Hamming coding. Give the generator matrix when the parity check matrix H of the Hamming code is given in Eq. (i). Also, show the code generated from the code A in Table 2 by using the generator matrix. In addition, explain the mechanism of the error detection and correction methods by giving an example of a situation when an error occurs.

$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \quad \text{(i)}$$

(5) Explain the error correcting capability of the code generated in Question (4). Also, briefly explain a method that extends Hamming coding to further improve the error rate.

問題 4

以下のハッシュ表に関する C プログラムについて問に答えよ．なお，以下で M は素数，hash(char *)は文字列に対して整数を返すハッシュ関数，h2(char *)は文字列に対して 0 より大きくかつ M 未満の整数を返す関数とする．また，プログラム中の strcmp は引数として文字列を 2 つ取る関数であり，2 つの引数が等しければ 0 を，そうでなければ 0 以外の値を返す．さらに算術演算のオーバーフローは考えないことにする．

```
enum mark_t {h_free, h_used};
struct {
   enum mark_t mark;
   char *data;
} htable[M];
int n_used;

void init ()
{
   for (int i=0; i < M; i++) htable[i].mark = h_free;
   n_used = 0;
}
int insert(char *d)
{
   int h = hash(d) % M, hh = h2(d);
   if (n_used >= M) return -1;
   while (htable[h].mark == h_used) {
      if (!strcmp(d, htable[h].data)) return -1;
      h = (h + hh) % M;
   }
   htable[h].data = d; htable[h].mark = h_used;
   n_used++; return h;
}
```

(1) 「insert が正しく動作する」とは，それまでに insert(s)が実行されていない文字列 s に対し，かつそのような s に限り，insert(s)によって htable 内のある場所が割り当てられ，関係する情報が格納されることを言う．最初に init を実行したとする．n_used $< M$ のときに insert は常に正しく動作する．その理由を「正しく動作する」の定義に即して示せ．

(2) 最初に init を実行し，その後 insert が何回か実行されたとせよ．与えられた文字列 d に対し，それが htable 内にあるかどうかを検索する search を次のように設計する．

```
int search(char *d)
{
  int h = hash(d) % M, hh = h2(d);
  while (htable[h].mark == h_used) {
    if (!strcmp(d, htable[h].data)) return h;
    h = (h + hh) % M;
  }
  return -1;
}
```

文字列 s に対し，search(s) は，s が htable 内に格納されていればその場所の添字を，いなければ–1 を返す．insert を参照しつつその理由を説明せよ．

(3) h2(d) = 1 （返り値として常に 1 を返す）とするとき，htable 内の添字 m にある要素を削除する関数を以下のように設計する．

```
void delete(int m)
{
  htable[m].mark = h_free;
  n_used = n_used-1;
}
```

(a) この実行により，以後の search や insert が正しく動作しない可能性があることを示せ．

(b) htable[m] に，可能ならば他所から要素を移すことで，delete を完成させたい．添字 i が以下の条件を満たすとき，htable[i] の要素は htable[m] に移してはいけないことを示せ．

- $m<i$ のとき，ある j ($m+1 \leqq j \leqq i$) に対して htable[j].mark = h_free が成り立つか，または $m <$ hash(htable[i].data) mod $M \leqq i$ が成り立つ．
- $i<m$ のとき，ある j ($m+1 \leqq j \leqq M-1$ または $0 \leqq j \leqq i$) に対して htable[j].mark = h_free が成り立つか，または hash(htable[i].data) mod $M \leqq i$ か $m <$ hash(htable[i].data) mod M が成り立つ．

(c) 正しく動作する delete を書け．プログラミング言語の種類は問わない．

Problem 4

Answer the questions on the C program below for hash tables. Suppose that M is a prime number, that `hash(char *)` is a hash function of strings that returns an integer, and that `h2(char *)` is a function of strings that returns an integer larger than 0 and less than M. In the program, `strcmp` is a function taking two strings as arguments. It returns 0 if the arguments are the same, and returns a value other than 0 if not. We do not consider any overflow in arithmetic operations.

```
enum mark_t {h_free, h_used};
struct {
   enum mark_t mark;
   char *data;
} htable[M];
int n_used;

void init ()
{
   for (int i=0; i < M; i++) htable[i].mark = h_free;
   n_used = 0;
}
int insert(char *d)
{
   int h = hash(d) % M, hh = h2(d);
   if (n_used >= M) return -1;
   while (htable[h].mark == h_used) {
      if (!strcmp(d, htable[h].data)) return -1;
      h = (h + hh) % M;
   }
   htable[h].data = d; htable[h].mark = h_used;
   n_used++; return h;
}
```

(1) We mean by "`insert` correctly works" that for a string s for which `insert(`s`)` has not been executed before, and for such s only, by execution of `insert(`s`)`, a location is assigned within `htable`, and related information is stored there. Suppose that `init` is executed first. When `n_used` < M, `insert` always works correctly. Show its reason, based on the definition of "correctly work."

(2) Suppose that `init` is executed first, and then `insert` is executed several times. We design `search` that searches `htable` for a given string *d*.

```
int search(char *d)
{
  int h = hash(d) % M, hh = h2(d);
  while (htable[h].mark == h_used) {
    if (!strcmp(d, htable[h].data)) return h;
    h = (h + hh) % M;
  }
  return -1;
}
```

For a string *s*, `search(s)` returns the index of *s* in `htable` if it is stored there, and −1 otherwise. Show its reason by referring to `insert`.

(3) Assuming h2 (*d*) = 1 (always returns 1), we design a function that deletes the item stored at the index *m* in `htable`.

```
void delete(int m)
{
  htable[m].mark = h_free;
  n_used = n_used-1;
}
```

(a) Show that, by executing this function, subsequent executions of `search` or `insert` may not work correctly.

(b) We consider completing `delete` by, if available, moving an item to `htable[`*m*`]` from somewhere. Show that when index *i* satisfies the condition below, we must not move the item in `htable[`*i*`]` to `htable[`*m*`]`.

- When $m<i$, there is some j ($m+1 \leqq j \leqq i$) such that `htable[`*j*`].mark = h_free`, or $m <$ `hash(htable[`*i*`].data)` mod $M \leqq i$.
- When $i<m$, there is some j ($m+1 \leqq j \leqq M-1$ or $0 \leqq j \leqq i$) such that `htable[`*j*`].mark = h_free`, or either `hash(htable[`*i*`].data)` mod $M \leqq i$ or $m <$ `hash(htable[`*i*`].data)` mod M.

(c) Write a correct `delete`. You can use any programming language.

問題A

入力変数 $x_1, x_2, \ldots, x_n$ において，x_1 を最も下位のビット，x_n を最も上位のビットとする．図1に示す入出力を持つ組合せ回路 LeastFlip(n) を作りたい．LeastFlip(n)は値が 1 である最も下位のビット x_i を検出し，0 に反転したものを出力変数 y_i に出力する．また，その他の出力値は対応する入力値と同じ値を持つ．たとえば n が 4 の場合，LeastFlip(4) は，x_1=0, x_2=1, x_3=1, x_4=1 という入力値に対しては，y_1=0, y_2=0, y_3=1, y_4=1 を出力する．なお，入力値が全て 0 の場合は出力も全て 0 とする．以下の問に答えよ．回路を設計する場合は，できるだけ簡潔な回路とすること．また，AND ゲート，OR ゲート，インバータの記号は図2に示すものを使用すること．

(1) n=2 の場合について，LeastFlip(2)の入力 x_1, x_2，出力 y_1, y_2 に対する真理値表を示せ．

(2) n=3 の場合について，LeastFlip(3)の出力のうち，y_1, y_2 を実現する回路を，LeastFlip(2)を用いて設計せよ．

(3) 問(2)の回路に出力 y_3 を実現する回路を追加して，LeastFlip(3)を完成せよ．

(4) 入力変数 $x_1, x_2, \ldots, x_n$ が，x_1 を最下位ビット，x_n を最上位ビットとする n 桁の2進数を表現していると考える．出力変数 $y_1, y_2, \ldots, y_n$ も同様に n 桁の2進数を表現しているとする．$x_1, x_2, \ldots, x_n$ で表現される入力値から 1 引いた値を $y_1, y_2, \ldots, y_n$ として出力する，図3に示す組合せ回路 Decrement(n)を設計したい．なお，入力値が 0 である場合には，出力値も 0 とする．n=3 の場合について，Decrement(3)の入力 x_1, x_2, x_3，出力 y_1, y_2, y_3 に対する真理値表を示せ．

(5) Decrement(3)と AND ゲートのみを使って，LeastFlip(3) を設計せよ．

(6) LeastFlip(n)は Decrement(n)と AND ゲートのみを使って作成できる理由を説明せよ．

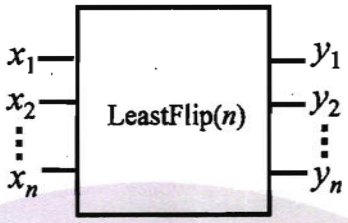
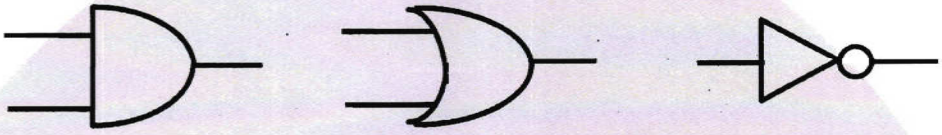


図 1



ANDゲート　ORゲート　インバータ

図 2

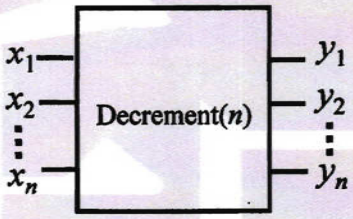


図 3

Problem A

Given a set of input variables $x_1, x_2, \ldots, x_n$, we assume that x_1 is the lowest bit and x_n is the highest bit. We would like to design a circuit, called LeastFlip(n), whose inputs and outputs are shown in Fig. 1. LeastFlip(n) identifies the lowest input variable x_i whose value is 1 and assigns 0 to y_i. All of the other outputs have the same values as their corresponding inputs. For example, when n=4, LeastFlip(4) generates the output values y_1=0, y_2=0, y_3=1, y_4=1 for the input values x_1=0, x_2=1, x_3=1, x_4=1. If all the input values are 0, the output values to be generated are all 0.

Answer the following questions. When designing a circuit, it must be simplified as much as possible. Use the notations for AND gates, OR gates and inverter gates shown in Fig. 2.

(1) When n=2, show the truth table for LeastFlip(2) with inputs x_1, x_2, and outputs y_1, y_2.

(2) When n=3, design a circuit for the outputs y_1, y_2 of LeastFlip(3) by utilizing LeastFlip(2).

(3) By adding a circuit for the output y_3 to the circuit of Question (2), complete LeastFlip(3).

(4) Input variables $x_1, x_2, \ldots, x_n$ are supposed to represent an n-digit binary number where x_1 is the least significant bit and x_n is the most significant bit. Output variables $y_1, y_2, \ldots, y_n$ also represent an n-digit binary number in the same way. We would like to design a combinational circuit, called Decrement(n) as shown in Fig. 3, which receives an input number represented with x_1, $x_2, \ldots, x_n$ and generates an output number represented with $y_1, y_2, \ldots, y_n$, in such a way that the output number equals to the input number minus 1. If the input number is 0, the output number should also be 0. When n=3, show the truth table for Decrement(3) with inputs x_1, x_2, x_3 and outputs y_1, y_2, y_3.

(5) Design a circuit for LeastFlip(3) by using only Decrement(3) and AND gates.

(6) Explain the reason why LeastFlip(n) can be designed with only Decrement(n) and AND gates.

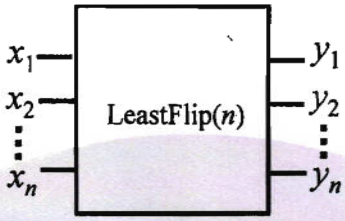


Fig. 1

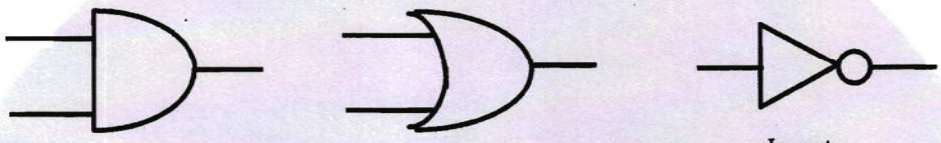


Fig. 2

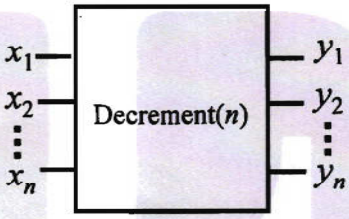


Fig. 3

問題 B

ネットワークを介してメッセージ交換を行う際には，ネットワーク上での盗聴や改ざんを防ぐために，送信者がメッセージ（平文）を暗号化鍵（K_e）で暗号化や署名をして通信を行い，受信者が復号鍵（K_d）を用いて暗号文の復号や署名を検証する暗号化技法が良く用いられる．

K_e と K_d に異なる鍵を用いる公開鍵暗号方式には，以下の特徴がある．

送信者 A が，受信者 B の公開鍵 K_p^B を用いて暗号化した暗号文は，受信者 B が持つ私有鍵 K_s^B のみで復号できるため，ネットワーク上での盗聴を防ぐことができる．

一方，送信者 A が，送信者 A の私有鍵 K_s^A を用いた署名は，受信者 B が送信者 A の公開鍵 K_p^A を用いて検証することで，内容が改ざんされていないことが確認できる．

以下の問に答えよ．

(1) 公開鍵暗号方式の一つである RSA アルゴリズムを用いて “aa” から “ge” までの 161 種の英字列で構成されるメッセージを第三者が暗号化鍵 K_e=(53,161)で暗号化した暗号文を復号した元のメッセージを推定したい．以下の問に推定の過程とともに示せ．

ここで，RSA アルゴリズムでは，平文 M ($0 \le M < n$ を満たす整数) から暗号文 C を暗号化鍵 $K_e=(e,n)$ で生成するには $C=M^e \bmod n$ を用い，暗号文 C から平文 M を復号鍵 K_d=(d,n) で生成するには $M=C^d \bmod n$ が用いられる．n は，2 つの素数 p, q を用いて $n=p \cdot q$ として表され，d および e は，$L=(p-1)\cdot(q-1)$ として，$d \cdot e \bmod L=1$ を満たす組合せから選ばれる．さらに，メッセージ及び暗号文は “aa”=0,…, “az”=25, “ba”=26,…, “ge”=160 と符号化して表現されていると考えよ．

(a) 暗号鍵 K_e に対応した復号鍵 K_d を推定せよ．

(b) 問(a)で推定した復号鍵 K_d を用いることで，暗号文 “ca, af, ad” を復号した元のメッセージを推定せよ．

(2) 次に，問(1) で述べた RSA アルゴリズムを用いてメッセージを暗号化することを考える．復号鍵を持たない第三者が元のメッセージを推定することが極端に難しくなるようにするためには，どうすれば良いか簡潔に答えよ．

(3) 送信者 A から受信者 B に対して，メッセージの内容が改ざんされていないことが確認でき，第三者には盗聴されない暗号文として送信するためには，送信者 A および受信者 B は，公開鍵暗号方式を用いたどの様な手法を用いれば良いか，その方式について述べよ．

(4) 第三者 X が，X の公開鍵 K_p^X を受信者 B の公開鍵と偽って送信者 A に伝えた場合，送信者 A が受信者 B 宛に生成した暗号文には，どのような危険性があるか述べよ．また，このような危険性を回避するためのアイデアについて述べよ．

Problem B

When we exchange messages through a network, cryptographic technologies are often used to encrypt or sign plain text messages using an encryption key (K_e) at the sender side and decrypt the ciphertext messages or verify the signature using a decryption key (K_d) at the receiver side to avoid eavesdropping and falsification.

The public key cryptography using two different keys for K_e and K_d has the following characteristics.

When sender A encrypts a plain text message with the public key of receiver B, K_p^B, the ciphertext message can be decrypted only with the private key of receiver B, K_s^B. It means that the original plain text message cannot be eavesdropped.

On the other hand, when sender A signs a plain text message with the private key of sender A , K_s^A, the signature can be verified with the public key of sender A, K_p^A, by receiver B. It means that the original plain text message is not falsified.

Answer the following questions.

(1) The RSA algorithm is a typical public key cryptographic technology. When a third-party encrypts 161 types of alphabetical messages from "aa" to "ge" using RSA with encryption key K_e=(53, 161), we would like to infer the original plain text messages from ciphertext messages. Answer the following questions with break process.
Here, in RSA, a plain text message M (M is an integer such that $0 \le M < n$) is encrypted to the ciphertext message C using encryption key $K_e = (e,n)$ as $C = M^e \bmod n$. A ciphertext message C is decrypted to the plain text message M using decryption key $K_d = (d,n)$ as $M = C^d \bmod n$. Here, n is computed using two prime numbers p and q as $n = p \cdot q$. Furthermore, d and e are selected so that $d \cdot e \bmod L = 1$, where $L = (p-1) \cdot (q-1)$. Assume that plain text messages and ciphertext messages are encoded as "aa"=0,..., "az"=25, "ba"=26,..., "ge"=160.
   (a) Infer the decryption key K_d corresponding to encryption key K_e.
   (b) Using decryption key K_d in Question (a), infer the original plain text messages of ciphertext messages "ca, af, ad".

(2) Suppose that we are the sender and convert messages using the RSA algorithm described in Question (1). We would like to make it extremely difficult for those who do not have the decryption key to infer the original plain text messages. Describe such a method briefly.

(3) Consider sending messages from sender A to receiver B in such a way that the messages sent from sender A cannot be eavesdropped on the network and receiver B can verify that the messages are not falsified. Describe what kind of methods should be applied at sender A and receiver B in order to implement this feature using a public key cryptographic technique.

(4) Describe what kinds of risks exist when sender A generates the ciphertext messages to receiver B, if a third-party X falsely gives the public key of X (K_p^X) as the public key of B to sender A. Also answer some ideas to avoid those risks.

問題C

金属を高温にすると，金属表面から電子が飛び出すことがある．このことについて，以下の問に答えよ．ただし，電荷素量，金属内自由電子の質量をそれぞれq，mとする．

(1) この現象は何と呼ばれているか．

(2) 金属内部の自由電子のフェルミ準位と金属外部の真空準位の差をWと表すとき，Wを何と呼ぶか．

(3) 金属表面に垂直外向きの座標をxとし，表面に平行な平面を$y-z$平面とする．金属内自由電子が金属表面から外部へ放出されるために，その電子のx方向の速度成分v_xが満たすべき条件式を示せ．ただし，フェルミ準位以上のエネルギーを持つ電子が金属内を自由に運動しており，フェルミ準位を差し引いた残りのエネルギーがその電子の並進運動エネルギーに対応していると考えよ．

(4) v_xをもつ自由電子が単位体積あたり$n(v_x)$個あると仮定すると，これらの電子が表面から流れ出ることにより生じる単位面積あたりの電流i_xはどのようにあらわされるか．

(5) この金属内自由電子の速度分布関数を$f(v_x,v_y,v_z)$とする時，表面から流れ出る全電流の面密度i_s（即ち全ての速度成分に対するi_xの和）を表す式を求めよ．ここでv_y，v_zは速度のy方向およびz方向成分であり，この金属の単位体積あたりの自由電子数はnとする．

(6) (5)で金属内自由電子がマクスウェル・ボルツマンの速度分布則

$$f(v_x,v_y,v_z)=\left(\frac{m}{2\pi kT}\right)^{\frac{3}{2}}\exp\left[-\frac{m(v_x^2+v_y^2+v_z^2)}{2kT}\right]$$

に従うと仮定して，i_sを求めよ．ただしk，T，πはそれぞれボルツマン定数，絶対温度，円周率である．

(7) 問(1)の現象を利用した素子や装置を一つ例示せよ．

(8) 高温にしなくても，金属表面に光を照射すると，やはり電子が飛び出すことがある．この現象は何と呼ばれているか．

(9) 低温で自由電子の熱運動が無視できる場合，電子を飛び出させるために光の周波数νが満たすべき条件式を示せ．必要ならプランク定数hを用いよ．

Problem C

When a metal is heated up to a high temperature, electrons are often emitted from the metal surface. Answer the following questions regarding this phenomenon. Here, let q and m be the elementary charge and the mass of free electrons in the metal, respectively.

(1) What is this phenomenon called?

(2) When the difference between the Fermi level of free electrons in the metal and the vacuum level outside the metal is denoted as W, what is W called?

(3) Suppose an outward-going coordinate normal to the metal surface is x, and a plane parallel to the surface is $y-z$ plane. Show the condition that the x-component of the electron velocity, v_x, should satisfy in order for free electrons inside the metal to go out from the metal surface. Here you can assume that electrons having their energies larger than the Fermi level are moving freely in the metal, and that the energy difference from the Fermi level corresponds to the kinetic energy of their translational motion.

(4) Assume the number of free electrons per unit volume having v_x is $n(v_x)$. Express current per unit area, i_x, when those electrons are flowing out of the surface.

(5) If the free electrons inside the metal follow a velocity distribution function $f(v_x, v_y, v_z)$, obtain a formula expressing the total current per unit area i_s flowing out of the surface, namely, the summation of i_x over all velocity components. Here, v_y and v_z are velocities in y and z directions, and the number of free electrons per unit volume in the metal is n.

(6) In (5), by assuming the free electrons in the metal follow the Maxwell-Boltzmann's velocity distribution law

$$f(v_x, v_y, v_z) = \left(\frac{m}{2\pi kT}\right)^{\frac{3}{2}} \exp\left[-\frac{m(v_x^2 + v_y^2 + v_z^2)}{2kT}\right],$$

obtain i_s. Here, k, T, and π are the Boltzmann's constant, the absolute temperature, and the circular constant, respectively.

(7) Name one device or instrument utilizing the phenomenon in Question (1).

(8) Even without heating, when the metal surface is illuminated by light, electrons can be emitted. What is this phenomenon called?

(9) When the thermal motion of free electrons is negligible because of low temperature, show the condition that the optical frequency ν should satisfy for making electrons jump out. Use the Planck's constant h as necessary.

問題D

図１(a)のように，金属ゲート，絶縁膜（厚さ d，誘電率ε）とｐ型半導体（アクセプタ密度 N_A）からなる MIS（Metal-Insulator-Semiconductor）構造において，直流バイアス電圧 V および微小交流電圧の周波数 f がそれぞれ可変である容量計を用いて容量測定（C-V 測定）を行うことを考える．ここでの容量 C は，単位面積あたりの値とする．また，金属ゲートと半導体の間のバイアス電圧がゼロのときは図１(b)に示すようなフラットバンド状態となっているとする．ここで，E_F はフェルミ準位である．図２は，異なる２種類の交流周波数において得られた C-V 曲線（Ⅰおよび Ⅱ）である．このとき，以下の問に答えよ．なお，絶縁膜は十分厚いとし，また，界面準位の影響は無視できるものとする．

(1) 図２の横軸の符号の組み合わせとして正しいものを A と B から選べ．なお，ここでのバイアス電圧 V は，半導体側を接地したものとして定義する．
(2) 図２の P，Q，R の各電圧領域におけるバンド図の概略を図１(b)にならって描け．その際，図中の注記は省略してよいが，フェルミ準位の位置は破線で示すこと．
(3) 図２の Q の領域では直流バイアス電圧の変化によって大きな容量変化が生じているが，その理由を説明せよ．
(4) 図２における C_0 を与える式を求めよ．
(5) 低周波数および高周波数での C-V 測定により，図２に示すような２本の異なる C-V 曲線が得られている．高周波数での C-V 曲線に対応するものを Ⅰ，Ⅱ から選べ．また，そのような周波数依存性が現れる理由を述べよ．
(6) アクセプタ密度 N_A を増加させると図２の C_1 の値はどのように変化するかを説明せよ．
(7) 絶縁膜の誘電率εだけを高めると図２のⅡの C-V 曲線はどのように変化するか，概略図を用いて説明せよ．また，この MIS 構造を電界効果トランジスタ（FET）のチャネル部分に用いた場合，このように絶縁膜の誘電率を高めることによってどのような効果が FET にもたらされるかを述べよ．

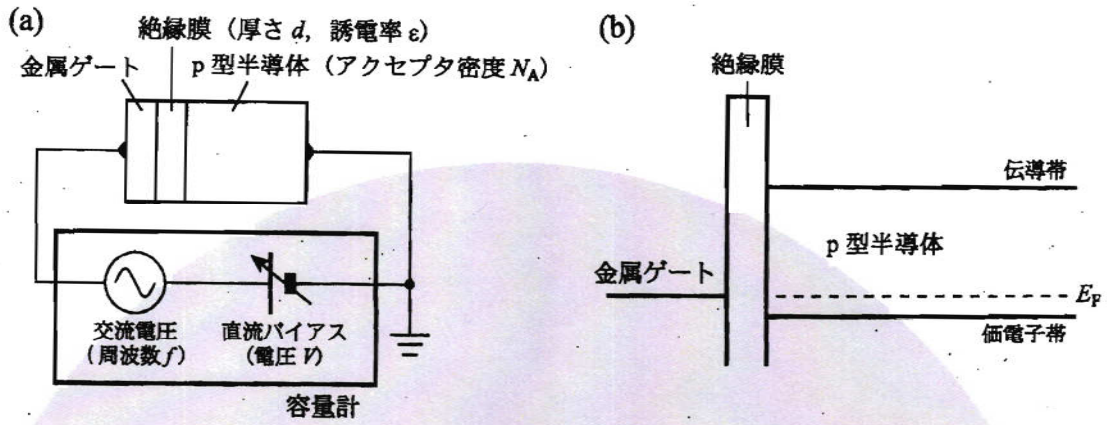


図 1

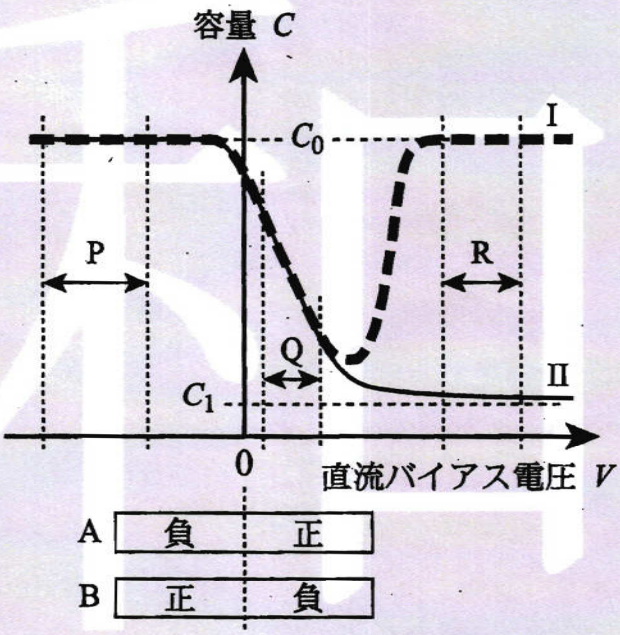


図 2

Problem D

Consider performing capacitance-voltage (C-V) measurements by a capacitance meter with a variable DC bias voltage V and a small AC voltage with a variable frequency f on a MIS (Metal-Insulator-Semiconductor) structure consisting of a metal gate, an insulator (thickness: d, dielectric constant: ε), and a p-type semiconductor (acceptor density: N_A), as shown in Fig. 1(a). Here, capacitance C is determined on a unit area. Assume that a null bias voltage between the metal gate and semiconductor gives the flat band condition as shown in Fig. 1(b), where E_F is the Fermi level. Figure 2 shows the C-V curves (I and II) acquired at two different frequencies. Answer the following questions. Note that the insulator is sufficiently thick and that any influences of interface states can be neglected.

(1) Choose A or B for the correct pair of bias signs for the horizontal axis in Fig. 2. Here, the bias voltage V is defined with respect to the grounded semiconductor.

(2) Schematically draw the respective band diagrams at the bias conditions P, Q and R in Fig. 2, similarly to Fig. 1(b). You may omit the notes in the figure, but you should indicate the Fermi level position by the dashed line.

(3) In the Q region in Fig. 2, a large capacitance change occurs according to the DC bias sweep. Explain its reason.

(4) Give an expression of C_0 in Fig. 2.

(5) The C-V measurements at low and high frequencies provide two different C-V curves shown in Fig. 2. Choose I or II for the C-V curve acquired at the high frequency, and explain the reason why such frequency dependence appears.

(6) Explain how the value of C_1 in Fig. 2 changes when the acceptor density N_A is increased.

(7) Explain how the C-V curve II in Fig. 2 changes when only the dielectric constant ε of the insulator is increased, by using a schematic drawing. When, in addition, this MIS structure is applied to the channel region in a field-effect transistor (FET), describe what influence is brought to the FET by such an increase of the dielectric constant of the insulator.

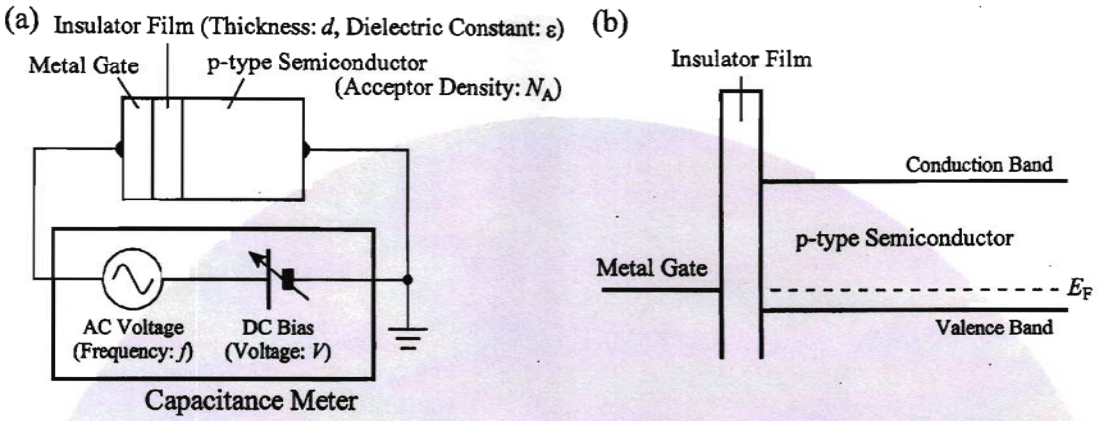


Fig. 1

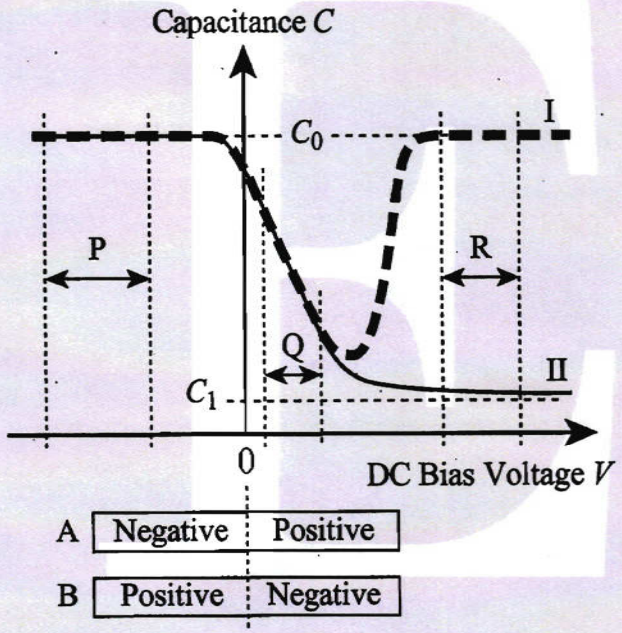


Fig. 2

問題E

フィードバック制御系について以下の問に答えよ．

(1) 図１のフィードバック制御系において，制御器の伝達関数を$G_c(s)=K$ $(K>0)$，制御対象の伝達関数を$G_p(s)=\dfrac{1}{s(Ts+1)}$ とする．ただし $R(s)$は基準入力，$C(s)$は制御量であり，時間信号$r(t)$，$c(t)$をそれぞれラプラス変換したものである．なお，T は正の定数とする．制御系全体の伝達関数を求めよ．

(2) 一般に二次系の伝達関数は$G(s)=\dfrac{\omega_n^2}{s^2+2\zeta\omega_n s+\omega_n^2}$として表せる．このとき，$\omega_n$を固有角周波数，$\zeta$を減衰率という．問(1)の制御系において$T=0.1$の時，減衰率$\zeta=0.5$となる$K$の値を求めよ．また，入力$r(t)=1+t$ $(t\geq 0)$に対する定常偏差εを求めよ．

(3) 問(1)の制御系において，系の単位ステップ応答が臨界制動となるKの値（$=K_c$）を求めよ．また，Kの値がK_cより大きい場合と小さい場合の両方について系の単位ステップ応答がどうなるかを論ぜよ．

(4) 問(1)の制御系に対して，内側にフィードバックループを加えたものを図２に示す．$H(s)=K_d s$ （$K_d>0$）として，図２の系全体の伝達関数を求めよ．また，K_dの値によって系の安定性がどのようになるかを説明せよ．

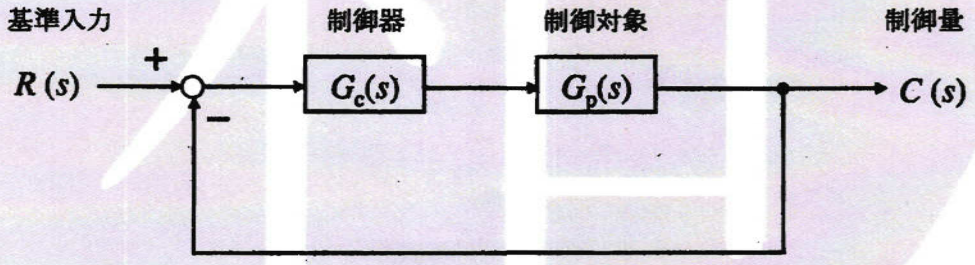


図１

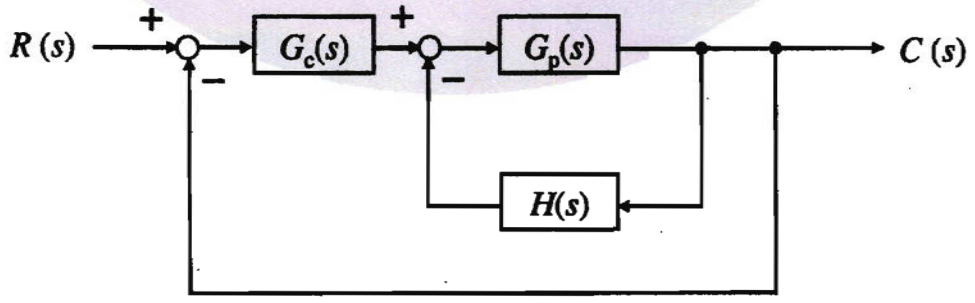


図２

Problem E

Answer the following questions on a feedback control system.

(1) In the feedback control system shown in Fig.1, the transfer function of Controller is given by $G_c(s)=K\ (K>0)$, and the transfer function of Plant is given by $G_p(s)=\dfrac{1}{s(Ts+1)}$. Here $R(s)$ and $C(s)$ denote the reference input and the controlled variable, respectively, which are expressed by the Laplace transformation of time signals $r(t)$ and $c(t)$. T is a positive constant. Find the transfer function of the whole control system.

(2) In general, the transfer function of a second-order control system is expressed by $G(s)=\dfrac{\omega_n^2}{s^2+2\zeta\omega_n s+\omega_n^2}$, where ω_n and ζ denote the natural angular frequency and the damping ratio, respectively. When $T=0.1$ in the control system given in Question (1), find K that makes the damping ratio $\zeta=0.5$. Then find the steady state error ε for the input $r(t)=1+t\ (t\geq 0)$.

(3) In the control system given in Question (1), find $K\ (=K_c)$ that makes the system show the critical damping in response to the unit step input. Then describe how the system responds to the unit step input in the case that K is larger than K_c and also in the case that K is smaller than K_c.

(4) Figure 2 shows the control system where an inner feedback loop is added to the system given in Question (1). When $H(s)=K_d s\ (K_d>0)$, find the transfer function of the whole system shown in Fig.2. Then describe how the stability of this system depends on K_d.

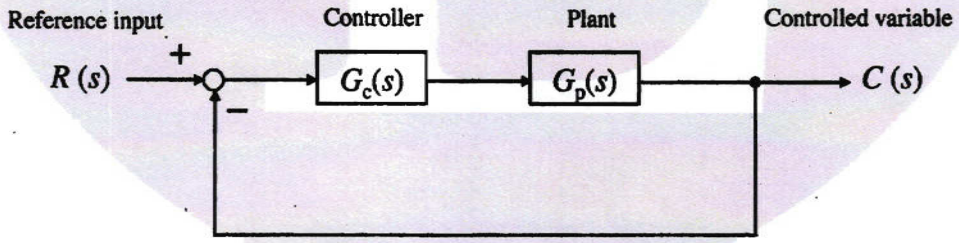


Fig.1

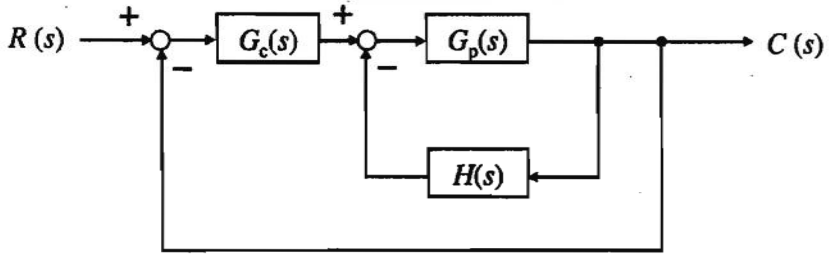


Fig.2

問題 F

図 1 のように，半径 a の導体 A，半径 b の接地された導体 B からなる同軸円筒ケーブルがある（$a<b$）．このケーブルの導体 AB 間の絶縁を，固体絶縁材料あるいは窒素ガスでとる場合について考えてみよう．

最初に，導体 A と導体 B の間に誘電率 ε，絶縁破壊電界 E_b の固体絶縁材料を詰めて絶縁をとった．このとき，以下の問に答えよ．

(1) 導体 A に電圧 V を印加すると，導体 A に単位長さあたり電荷密度 q の電荷が発生した．このとき，中心軸から距離 r（$a \le r \le b$）における電界の大きさを q を用いて表せ．

(2) 問(1)で求めた電界の大きさを，V を用いて表せ．

(3) 導体 B の半径 b を固定値として，導体 A の半径 a は自由に設定できるとする．このとき，導体 AB 間の絶縁破壊電圧が最大になるような半径 a の値を求めよ．

次に，導体 AB 間の固体絶縁材料を窒素ガスに置き換えて，窒素ガスで絶縁をとった．窒素ガスの絶縁破壊について，以下の問に答えよ．

(4) 窒素ガス中の放電において，電子の平均速度を v_e，電子と窒素分子の密度をそれぞれ n_e，n_g，電子と窒素分子の衝突断面積を σ とする．このとき，次の文章の下線部(i)～(iii)の関係式を完成させよ．ただし，窒素分子の平均速度は v_e より十分小さいと仮定する．

「電子の平均自由行程 λ_e と，電子の窒素分子に対する衝突周波数 f_e の間には，$\lambda_e =$ (i)＿＿＿＿ の関係が成立する．また，f_e と n_g の間には $f_e =$ (ii)＿＿＿＿ の関係がある．よって，λ_e と n_g の関係は $\lambda_e =$ (iii)＿＿＿＿ で表される．」

(5) 窒素ガスの圧力を大気圧から大幅に増加させると，導体 AB 間の絶縁破壊電圧は増加した．また，圧力を大気圧から大幅に減少させた場合も，絶縁破壊電圧は増加した．それぞれの理由を説明せよ．

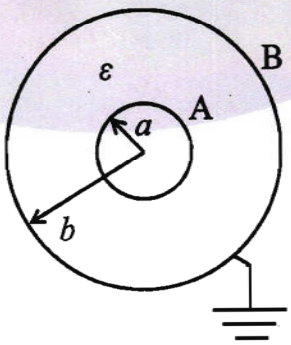


図 1

Problem F

Figure 1 shows a coaxial cylindrical cable composed of conductor A of radius a and grounded conductor B of radius b ($a < b$). Let us consider insulation between conductors A and B of the cable using a solid dielectric material or nitrogen gas.

First, the space between conductors A and B is filled with a solid dielectric material of permittivity ε and breakdown field strength E_b for the insulation. Answer the following questions.

(1) When a voltage V is applied to conductor A, a charge with a charge density q per unit length is induced on conductor A. Express the electric field strength at a distance r ($a \leq r \leq b$) from the center axis of the cable in terms of q.

(2) Express the electric field strength in Question (1) in terms of V.

(3) Let us assume that the radius b of conductor B is a fixed value and the radius a of conductor A is variable. Find the radius a that maximizes the breakdown voltage between conductors A and B.

Next, the solid dielectric material between conductors A and B is replaced with a nitrogen gas as an insulator. Answer the following questions on breakdown phenomena in the nitrogen gas.

(4) In the nitrogen-gas discharge, let v_e be the average electron velocity, n_e and n_g be the densities of electrons and nitrogen molecules, respectively, and σ be the collision cross-section between electrons and nitrogen molecules. Assume that the average velocity of nitrogen molecules is sufficiently lower than v_e. Complete the equations in (i) to (iii) in the following description.

> "The relation between the mean free path of electrons, λ_e, and the collision frequency of electrons with nitrogen molecules, f_e, is expressed as λ_e = (i)_____. The relation between f_e and n_g is expressed as f_e = (ii)_____. Therefore, the relation between λ_e and n_g is expressed as λ_e = (iii)_____."

(5) When the pressure of the nitrogen gas is significantly increased from the atmospheric pressure, the breakdown voltage between conductors A and B increases. Also when the pressure is significantly decreased from the atmospheric pressure, the breakdown voltage increases. Describe the reasons for both cases.

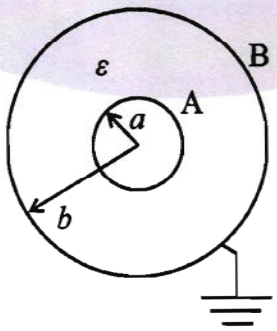


Fig. 1