整理番号
15

2022年度4月入学（2021年度10月入学含む）東京農工大学工学府博士前期課程

問題用紙　専門科目

情報工学専攻

16枚のうち1

受験番号	MC−

【注意】 1 ～ 11 のうち、4問を選び解答せよ。解答用紙は対応する問題番号のものを用い、選択しなかったすべての問題の解答用紙全体に、大きく×を付すこと。裏面を用いる場合は表面の最下行に、その旨を明記すること。解答の指示を守らないときには、本科目の採点を行わない場合がある。

1

RSA 暗号は、二つの素数 p と q の積 $N = pq$ を素因数分解することが困難であることを利用した公開鍵暗号である。$ed \equiv 1 \ (mod\ (p-1)(q-1))$ を満たす自然数の組 (e, d) に対して、公開鍵を (N, e)、秘密鍵を d とし、メッセージ $M \in \{0, \ldots, N-1\}$ を暗号化した暗号文は $C = M^e \ (mod\ N)$、暗号文の復号は $M = C^d \ (mod\ N)$ で与えられる。また、復号した暗号文が元のメッセージと一致することは、任意の素数 p と自然数 $a \in \{1, \ldots, p-1\}$ に対して $a^{p-1} \equiv 1 \ (mod\ p)$ が成り立つこと(フェルマーの小定理)を利用して保証される。RSA 暗号に関して以下の問いに答えよ。

〔1〕二つの素数 $p = 7$ と $q = 13$ を用いた RSA 暗号において、公開鍵が $(N, e) = (91,5)$ であるとき、秘密鍵 d を求めよ。答えのみでよい。

〔2〕公開鍵が $(N, e) = (391,3)$ である RSA 暗号に関して、暗号文 $C_1 = 2$ に対応するメッセージが $M_1 = 246$ であることが分かっているとき、暗号文 $C_2 = 16$ に対応するメッセージ $M_2 \in \{0, \ldots, 390\}$ を求めよ。答えのみでよい。

〔3〕RSA 暗号の鍵を作るための素数の候補として $p = 77059$ を考える。p が「素数である」か「素数ではない」か判定し、理由とともに答えよ。ただし、必要があれば $2^{77050} \equiv 18127 \ (mod\ 77059)$ であることを用いてもよい。

整理番号
15

2022年度4月入学（2021年度10月入学含む）東京農工大学工学府博士前期課程

問　題　用　紙　　専門科目

情報工学専攻

16枚のうち2

受験番号	MC－

2

都市Aから都市Bまで、荷物1、荷物2、…、荷物nを何台かのトラックで輸送する。ここで、荷物i ($i = 1,2,\ldots,n$)の重さは正の定数w_iで与えられており、トラックは番号1、番号2、…、番号nまでのn台が使用可能である。1個の荷物を複数台のトラックに分割して積むことはできないが、1台のトラックには複数個の荷物を積むことができ、1台のトラックに積める荷物の重さの合計は正の定数Wまでである。なお、各トラックは1回しか使うことはできない（同じトラックが2回以上都市Aから都市Bに行くことはできない）。

いま、なるべく少ない台数のトラックを用いて全ての荷物を運びたいとする。どの荷物をどのトラックに積み、どのトラックを使用すれば良いかという問題を、0-1整数計画問題（0-1整数最適化問題）として定式化することを考える。

変数x_{ij}を「荷物i ($i = 1,2,\ldots,n$)をトラックj ($j = 1,2,\ldots,n$)に積むときに1、積まないときに0をとる0-1変数」、変数y_jを「トラックj ($j = 1,2,\ldots,n$)を使用するときに1、使用しないときに0をとる0-1変数」と定義したとする。そうすると、解きたい問題は以下の0-1整数計画問題に定式化できる。

$$\text{minimize} \quad \sum_{j=1}^{n} y_j$$

$$\text{subject to} \quad \sum_{\boxed{ア}=1}^{n} x_{ij} = 1 \quad \left(\boxed{イ} = 1,2,\ldots,n\right),$$

$$\sum_{i=1}^{n} w_i x_{ij} \leq W \cdot y_j \quad (j = 1,2,\ldots,n),$$

$$x_{ij} \in \{0,1\} \quad (i = 1,2,\ldots,n,\ j = 1,2,\ldots,n),$$

$$y_j \in \{0,1\} \quad (j = 1,2,\ldots,n).$$

上記の定式化について、以下の問いに答えよ。ただし、解答に際しては上記で定義された以外の変数を新たに導入することはできない。また、制約式を追加せよという問いにおいては、定義された変数に関して線形な等式制約系または線形な不等式制約系を書くこと。

〔1〕正しい定式化となるように、空欄 ア と イ に入る適切な文字を示せ。

〔2〕定式化に「荷物2と荷物4は同じトラックに積む」という制約式を追加せよ。

〔3〕定式化に「使われるトラックの番号は使われないトラックの番号より小さい」という制約式を追加せよ。

〔4〕定式化に「トラック3に荷物を積むならばトラック5に荷物を7個以上積む」という制約式を追加せよ。

整理番号
15

2022年度4月入学（2021年度10月入学含む）東京農工大学工学府博士前期課程

問　題　用　紙　　専門科目

情報工学
専攻

16枚のうち3

受験番号	MC−

3

頂点集合 V、枝集合 E からなる無向グラフ $G=(V, E)$ に対して、以下の問いに答えよ。ただし、G は、並行枝や自己閉路をもたないものとする。また、$|V|$ は頂点数、$|E|$ は枝数を表すものとする。

〔1〕G が木であるとき、$|V|$ と $|E|$ の間に成り立つ等式を示せ。ただし、答えのみでよい。

〔2〕G が森であるとき、$|V|$ と $|E|$ の間に不等式 $|V|>|E|$ が成り立つことを証明せよ。

〔3〕V の部分集合 F に対して、F に属する全頂点を G から開放除去すると、残りのグラフに閉路が存在しなくなるとき、F をフィードバック頂点集合という。G が次数 d (≥ 2)の正則グラフであると仮定する。このとき、F、V、E に関して以下の不等式が成り立つことを証明せよ。

$$|F|>(|E|-|V|)/(d-1)$$

ただし、無向グラフのある頂点の次数とは、その頂点に接続する枝の本数である。また、無向グラフの全頂点の次数が等しく d であるとき、そのグラフを次数 d の正則グラフという。さらに、無向グラフの頂点を開放除去するとは、そのグラフからその頂点とその頂点に接続するすべての枝を除去することを意味する。

整理番号
15

2022年度4月入学（2021年度10月入学含む）東京農工大学工学府博士前期課程

問　題　用　紙　　専門科目

情報工学専攻

16枚のうち4

受験番号	MC－

4

図4－1に示すネットワークにおいて端末Aが端末Fおよび端末Gと通信する場合を考える。そのとき、以下の問いに答えよ。但し、各端末やルータの経路情報は適切に設定されているものとする。また、ルータCはNAT（Network Address Translation）機能を持ち、インタフェースC1側にはプライベートアドレス、インタフェースC2側にはグローバルアドレスが割り振られているものとする。

〔1〕 端末Aが端末Fおよび端末G宛にフレームを送出するとき、次の各フレームに含まれる送信元MACアドレス（SrcMAC）、宛先MACアドレス（DstMAC）、送信元IPアドレス（SrcIP）、宛先IPアドレス（DstIP）をそれぞれ示せ。なお、MACアドレスやIPアドレスを示す際、端末の場合には端末名（たとえばA）、ネットワーク機器の場合にはインタフェース名（たとえばC1、D2）で示すこと。

（1） 端末Aが端末Fに向けて送信するフレーム
（2） 端末Aが端末Gに向けて送信するフレーム
（3） 端末Fが受信するフレーム
（4） 端末Gが受信するフレーム

〔2〕 端末Aが端末F宛にICMP（Internet Control Message Protocol）エコー要求パケットを、IPヘッダ中のTTL（Time To Live）フィールドの値を変えながら送信した。TTLが次の各値のとき、端末Aが受信するICMPパケットの送信元IPアドレスとICMPメッセージのタイプ番号を示せ。なお、ICMPメッセージのタイプ番号とその名称は解答用紙に記載されている。

（1） TTL＝1
（2） TTL＝2
（3） TTL＝3

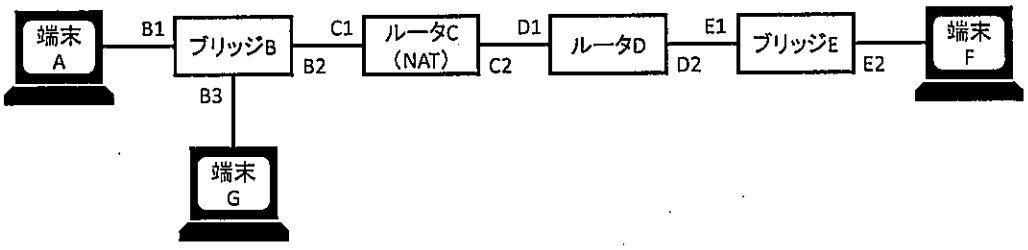


図4－1 対象となるネットワーク構成

整理番号
１５

2022年度４月入学（2021年度10月入学含む）東京農工大学工学府博士前期課程

問　題　用　紙　　専門科目

情報工学専攻

16枚のうち５

受験番号	MC－

5

以下の問いに答えよ。

〔1〕データベースに関する以下の問いに答えよ。

（ア）複数の処理をひとつの処理としてまとめたものを何と呼ぶか答えよ。

（イ）ACID 特性が示す 4 つの性質の名称を答えよ。

（ウ）デッドロックが生じる危険性はあるものの、Conflict serializable なスケジュールを実現するロック確保手法の名称を答えよ。

〔2〕以下の 3 つの関係データベース TableR, TableS, TableT（図 5） を SQL で操作することを考える。アルファベットが属性名、数値が値である。（ア）～（ウ）の SQL クエリを実行したときに返ってくる関係表を答えよ。

A	B	C
1	2	3
6	7	8
9	7	8

TableR

B	C	D
2	3	4
2	3	5
7	8	10

TableS

D	E
2	3
4	3
10	8

TableT

図 5 : TableR, TableS, TableT

（ア）SELECT A FROM TableR WHERE B > 5

（イ）SELECT B, E FROM TableS, TableT WHERE TableS.D < TableT.D

（ウ）(TableR NATURAL JOIN TableS) NATURAL JOIN TableT

整理番号
１５

2022年度4月入学（2021年度10月入学含む）東京農工大学工学府博士前期課程

問　題　用　紙　　専門科目

情報工学
専攻

16枚のうち6

受験番号	MC－

6

以下の問いに答えよ。

Linux などの汎用 OS が実行されるプロセッサは、通常、プロセッサモードを有する。名称はプロセッサによって異なるが、たとえば、MIPS プロセッサでは、カーネルモード、ユーザモードと呼ばれるプロセッサモードを有する。

〔1〕カーネルモード、ユーザモードはそれぞれどのような機能を有し、どのようなプログラムが実行されるかを示せ。カーネルモード、ユーザモードごとに解答せよ。

〔2〕なぜ、このようなプロセッサモードを導入したか理由を簡潔に論ぜよ。

〔3〕どのような操作でこの二つのモードの遷移が起こるかをそれぞれのモード遷移ごとに示せ。

整理番号
15

2022年度4月入学（2021年度10月入学含む）東京農工大学工学府博士前期課程

問　題　用　紙　　専門科目

情報工学専攻

16枚のうち7

受験番号	MC－

7

画像処理に関する以下の問い〔1〕、〔2〕に答えよ。なお、処理を施す前のグレースケール画像を図7－1に示す。結果画像については、画素値が非負となる画像では0を黒、画素値が正負の値をとる画像では0をグレーとして表示している。

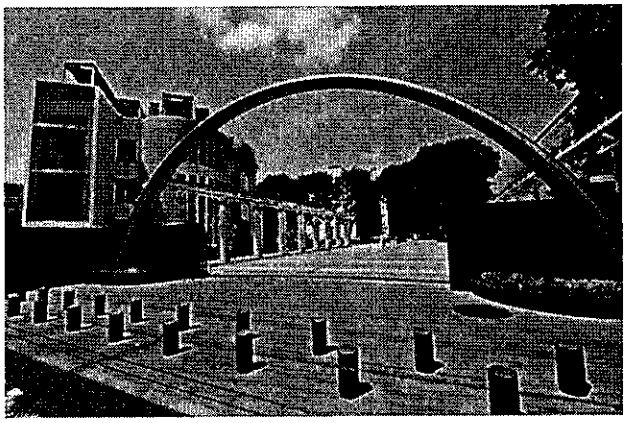


図7－1

整理番号
15

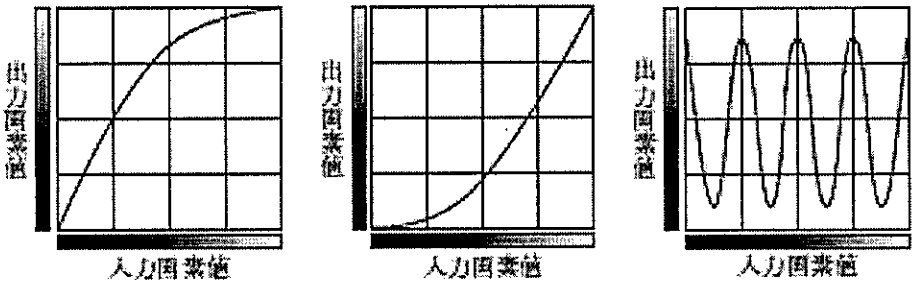
2022年度4月入学（2021年度10月入学含む）東京農工大学工学府博士前期課程

問　題　用　紙　　専門科目　　専攻

16枚のうち8

受験番号	MC−

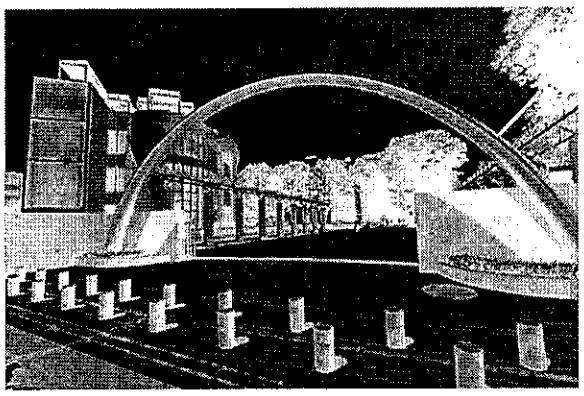
〔1〕 トーンカーブ（階調変換関数）とは、入力画像の画素値と出力画像の画素値を対応付ける関数である。トーンカーブにより濃淡変換を行うことを考える。図7−2（1）〜（3）に示したトーンカーブを図7−1の画像に施した結果の画像として適切なものを解答群〔1〕から選択せよ。



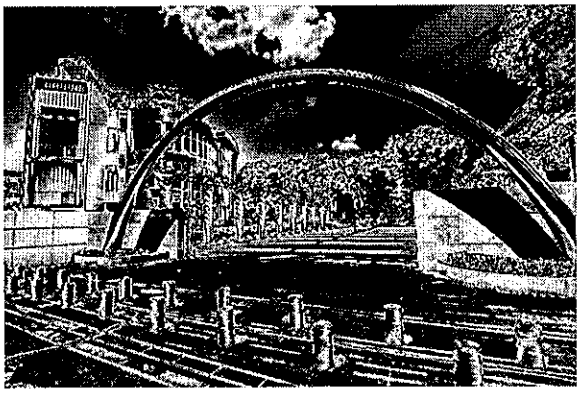
（1）　（2）　（3）

図7−2

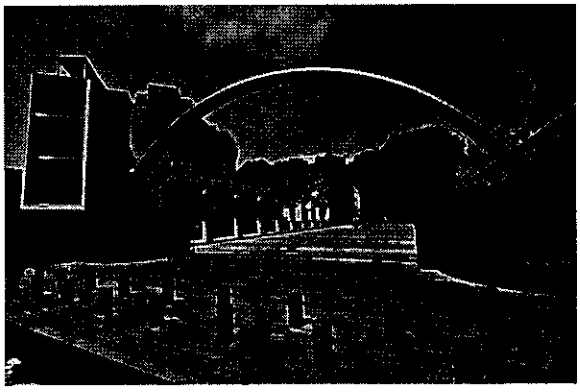
解答群〔1〕：



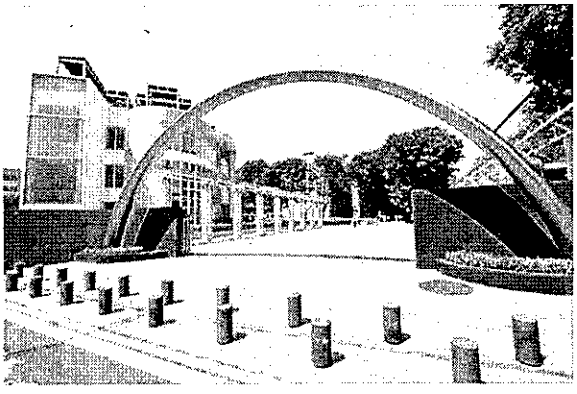
（あ）



（い）



（う）



（え）

〔2〕 画像の空間フィルタリングについて考える。
(A) 図7−3（1）〜（3）に示したフィルタを図7−1の画像に施した結果の画像として適切なものを解答群〔2〕から選択せよ。

0	1	0
1	−4	1
0	1	0

（1）

0	0	0
−1	1	0
0	0	0

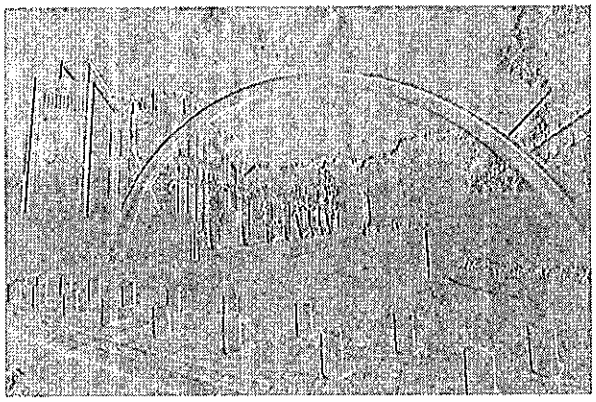
（2）

0	0	0
0	1	0
0	−1	0

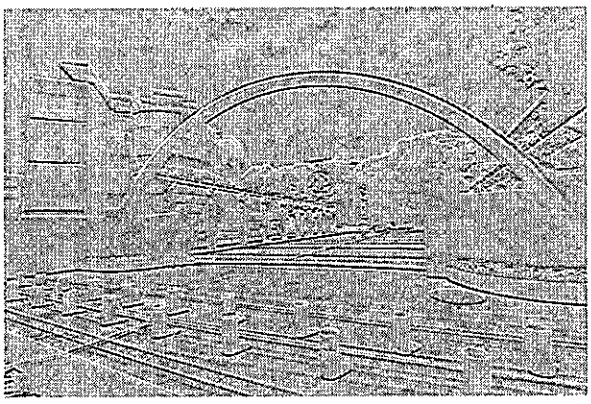
（3）

図7−3

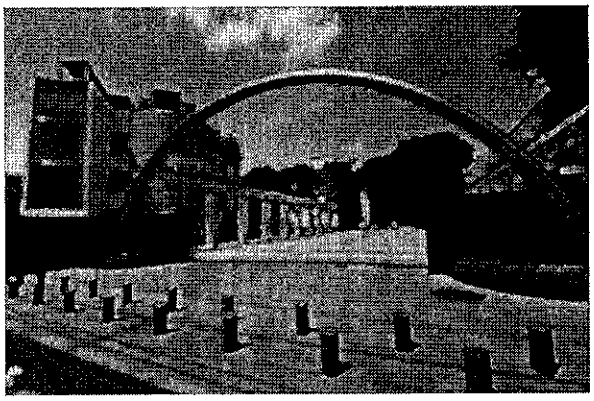
解答群〔2〕：



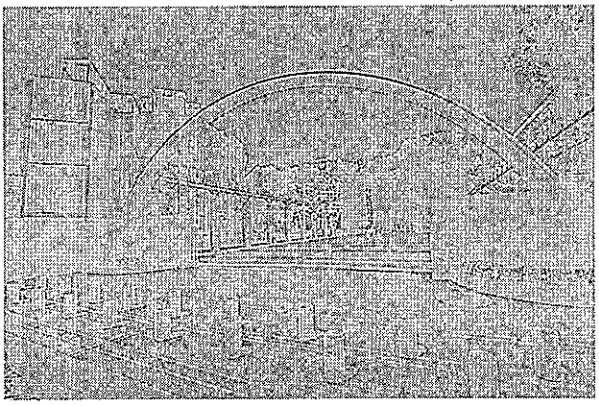
（あ）



（い）



（う）



（え）

（B）図7−4に示すフィルタについて、空欄に入る適切な語句を答えよ。

このフィルタは［（1）］フィルタと呼ばれる。原画像から［（2）］フィルタの出力を引くことで、画素値の変化を強調する。kの値が大きくなるほど［（1）］の度合いが［（3）］。

$-\frac{k}{9}$	$-\frac{k}{9}$	$-\frac{k}{9}$
$-\frac{k}{9}$	$1+\frac{8}{9}k$	$-\frac{k}{9}$
$-\frac{k}{9}$	$-\frac{k}{9}$	$-\frac{k}{9}$

図7−4

（C）図7−5に示す画像は、図7−1の画像に胡麻塩状のノイズを付加した画像である（右側に一部を拡大して表示している）。この画像に何らかの処理を行って、できるだけ図7−1に近い画像を得るための処理について考える。ガウシアンフィルタのような平滑化フィルタを施すとエッジ部分もぼやけてしまうが、これを避けるために用いられるフィルタの例を一つ挙げ、そのフィルタの処理について50字程度で説明せよ。

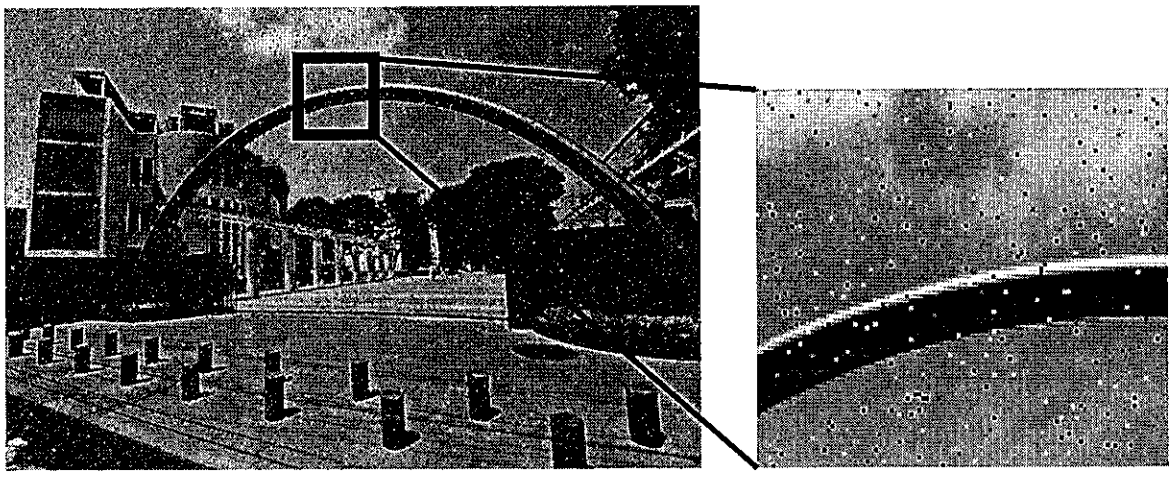


図7−5

整理番号	2022年度4月入学（2021年度10月入学含む）東京農工大学工学府博士前期課程	情報工学専攻
15	問　題　用　紙　専門科目	

16枚のうち11	受験番号	MC−

8

コンピュータグラフィックスにおける「シェーディング」に関する以下の文章を読み、問い〔1〕～〔5〕に答えよ。

コンピュータグラフィックスにおいて、光沢のある面の陰影付けを簡易に行う手法として、フォンのシェーディングモデルがよく知られている。フォンのモデルにおいては、物体表面における反射光は、拡散反射光、鏡面反射光、[(1)] の3つからなると考える。図8－1に示すように、反射面 S 上の点 P において、面の法線ベクトルを N、視線方向ベクトルを V、光源方向ベクトルを L、正反射方向ベクトルを R とおく。これらのベクトル N, V, L, R はいずれも単位ベクトルとする。このとき、点Pにおける視線方向への反射光のうち、拡散反射光を I_d 、鏡面反射光を I_s とおくと、

$I_d = k_d I_i($ [(A)] $)$ ， $I_s = k_s I_i($ [(B)] $)^n$

と表される。ここで、I_i は入射光の強さ、k_d は拡散反射係数、k_s は鏡面反射係数である。また、n は鏡面反射で生じる [(2)] の特性を制御するパラメータであり、n を大きくするほど小さく鋭い [(2)] が現れる。

〔1〕文章中の空欄 (1)、(2) に入る適切な語句を答えよ。

〔2〕文章中の空欄 (A)、(B) に入る適切な数式を示せ。ただし、変数としてベクトル N, V, L, R だけを用いること。

〔3〕3つのベクトル N, L, R の間の関係式を求めよ。答えだけでよい。

〔4〕xyz 空間において、面 S が3点 $P_1(1, 0, 0)$， $P_2(0, 1, 0)$， $P_3(0, 0, 2)$ を通る平面であるとき、法線ベクトル N を求めよ。答えだけでなく答えに至る過程も示すこと。

〔5〕前問〔4〕の平面 S を、z 軸正方向からの平行光源で照らしたとき、正反射方向ベクトル R を求めよ。答えだけでなく答えに至る過程も示すこと。

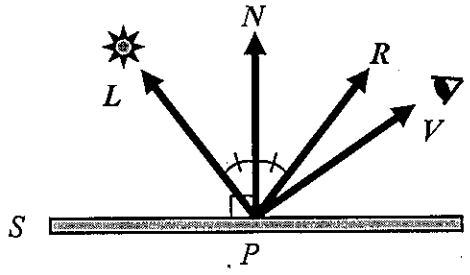


図8－1　フォンのシェーディングモデル

整理番号	2022年度4月入学（2021年度10月入学含む）東京農工大学工学府博士前期課程	情報工学専攻
15	問　題　用　紙　　専門科目	

16枚のうち12	受験番号	MC－

9

2次元ユークリッド空間上の5つの標本点

$$x_1 = \begin{pmatrix}0\\0\end{pmatrix}, x_2 = \begin{pmatrix}2\\2\end{pmatrix}, x_3 = \begin{pmatrix}1\\-1\end{pmatrix}, x_4 = \begin{pmatrix}-2\\-2\end{pmatrix}, x_5 = \begin{pmatrix}-1\\1\end{pmatrix},$$

を原点を通る直線Sに正射影することを考える。ただし、直線Sの方向ベクトルは

$$u = \begin{pmatrix}u_1\\u_2\end{pmatrix}$$

で与えられ、そのノルムは$||u|| = \sqrt{u^\top u} = 1$であるとする（図9－1を参照）。このとき、以下の問いに答えよ。なお、〔1〕から〔3〕は答えのみでよいが、〔4〕は導出過程も示しなさい。

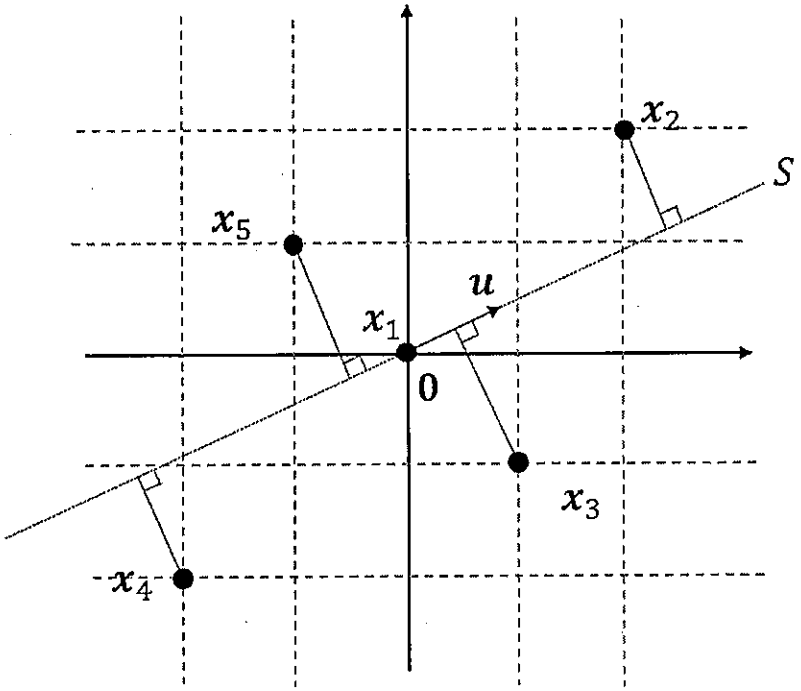


図9－1　5つの標本点と方向ベクトルがuの直線S

〔1〕原点から各標本点までの長さの2乗$||x_i||^2$ $(i = 1,2,3,4,5)$を求めなさい。

〔2〕各標本点をSへ正射影した点から原点までの長さを$c_i(i = 1,2,3,4,5)$とする。c_i^2をu_1, u_2を用いて表しなさい。

〔3〕各標本点からSへの垂線の長さを$d_i(i = 1,2,3,4,5)$とする。d_i^2をu_1, u_2を用いて表しなさい。

〔4〕$\sum_{i=1}^{5} d_i^2$を最小にするuを求めなさい。

整理番号
15

2022年度4月入学（2021年度10月入学含む）東京農工大学工学府博士前期課程

問題用紙　専門科目

情報工学専攻

16枚のうち13

受験番号	MC－

10

以下に3つの前提と1つの結論を示す。

結論　$\exists x(C(x) \wedge \neg D(x))$
前提1　$\forall x(E(x) \rightarrow A(x) \vee B(x) \vee C(x))$
前提2　$\forall x(A(x) \vee B(x) \rightarrow D(x))$
前提3　$\exists x(E(x) \wedge \neg D(x))$

上記の論理式において $A(x)$は「xは神奈川県である」、$B(x)$は「xは千葉県である」、$C(x)$は「xは埼玉県である」、$D(x)$は「xは海に面している」、$E(x)$は「xは南関東地域である」を表現する。また、xは県を表す変数である。以下の問いに答えよ

〔1〕結論および前提1、2、3を自然言語文で示せ。ただし、答えのみでよい。

〔2〕結論の否定および前提1、2、3のスコーレム標準形を示せ。ただし、答えのみでよい。解答において、$\exists x$ がその量化子のスコープ内にあると考え $\forall x$ に置き換える際に導入するスコーレム関数fを用いてもよい。

〔3〕導出グラフを用いて、前提1、2、3が満たされるときに結論が満たされることを示せ。

整理番号
15

2022年度4月入学（2021年度10月入学含む）東京農工大学工学府博士前期課程

問　題　用　紙　　専門科目

情報工学専攻

16枚のうち14

受験番号	MC－

11　図11－1は32ビットマルチサイクルMIPSプロセッサの一部の命令を実現した内部ブロック図である。

図中にある 符号拡張 は、16ビットデータの符号を維持したまま32ビット幅に拡張するモジュールである。 4 は定数4を示し、 <<2 は左に2ビットシフトする。

図11－2は、制御ユニット（Control Unit）の状態遷移図であり、以下の動作を行う。

・E1 はレジスタ間算術論理演算命令の命令実行ステージであり、命令フォーマットは最上位ビット（MSB）から[*Op* コード(6)＋第一ソースレジスタ *Rs*(5)＋第二ソースレジスタ *Rt*(5)＋ディスティネーションレジスタ *Rd*(5)＋シフト量(5)＋ファンクションコード(6)]が並ぶ。ただし()内の数値はビット幅を示す。レジスタ間算術論理演算命令では、*Op* コードはすべて0であり、演算の種類はファンクションコードで区別する。本問題ではシフト量は考慮せず、すべて0として扱う。例として、add命令の場合、【add *Rd*, *Rs*, *Rt*: *Rd*←*Rs*+*Rt*】という動作を行う。

・E2 はメモリアクセス命令の命令実行ステージであり、命令フォーマットは[*Op* コード(6)＋ソースレジスタ *Rs*(5)＋ターゲットレジスタ *Rt*(5)＋アドレスフィールド *Address*(16)]となる。[X]をメモリ番地 X のメモリデータを示すものとすると、ロードワード（lw）命令の場合、*Op* コードは $100011_{(2)}$ で【lw *Rt*, *Address*(*Rs*): *Rt*←[*Rs*+*Address*]】と動作し、M1でメモリからデータを読み出し、W2でそのデータをレジスタに書き込む。ストアワード（sw）命令の場合、*Op* コードは $101011_{(2)}$ で【sw *Rt*, *Address*(*Rs*):[*Rs*+*Address*]←*Rt*）】と動作し、M2でレジスタの値をメモリに書き込む。

・E3 は条件分岐命令の命令実行ステージであり、命令フォーマットはメモリアクセス命令と同じものである。beq 命令の場合、*Op* コードは $000100_{(2)}$ で【beq *Rs*, *Rt*, L1: *Rs*=*Rt* であればラベル L1 にある命令に分岐】と動作する。ここでラベル L1 は、beq 命令の次の命令から *Address* 命令先の命令に付与される。すなわち、beq 命令から5つ先の命令に分岐する場合は $0004_{(16)}$ が、beq 命令の3つ前の命令に分岐する場合は $FFFC_{(16)}$ が、それぞれ *Address* フィールドに入る。

本問題における設計では、命令フェッチステージ（F）において、命令をメモリから読み出した直後にPCの更新（PC←PC+4）を行い、次命令のフェッチに備える。また、条件分岐命令における分岐先アドレス計算は命令デコードステージ（D）において行い、条件が成立すればPCに分岐先アドレスを命令実行ステージにおいて書き込み、不成立であればPC+4のままとなる。

ALU Controller は ALU の動作を決定するモジュールであり、*Op* コードに従って出力される2ビットの ALUOp の値により、加算や減算を行わせたり、ファンクションコード（func）の内容に応じて ALU の動作を決定する ALUControl 信号を出力する。条件分岐命令（beq）では、BEQ 信号には1が出力され、ALU の演算結果が0のとき、zero_flag には1が出力される。

整理番号
１５

2021年度４月入学（2020年度10月入学含む）東京農工大学工学府博士前期課程

問　題　用　紙　　専門科目

情報工学専攻

16枚のうち15

受験番号	MC－

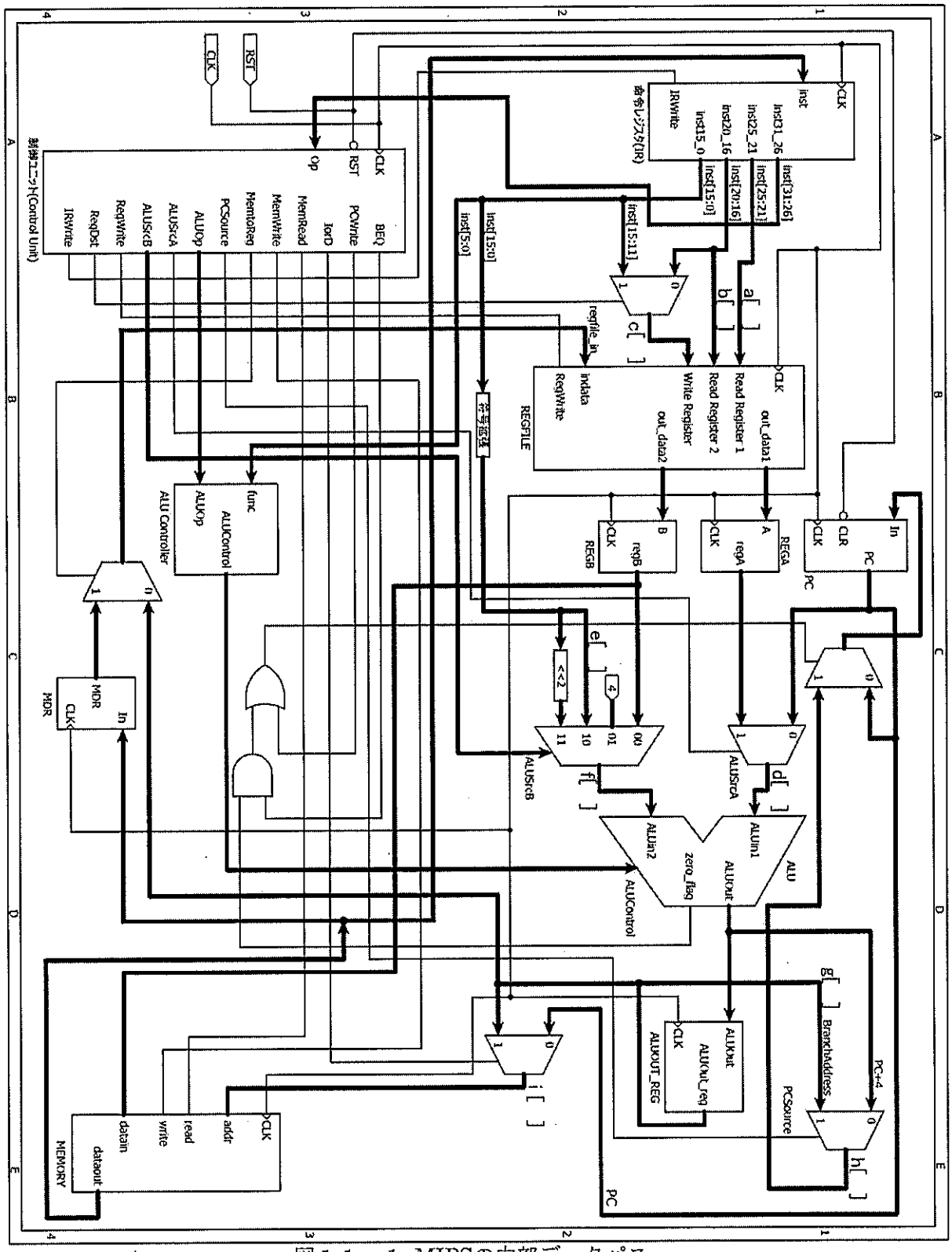


図１１－１　MIPSの内部データパス

整理番号
１５

2021年度４月入学（2020年度10月入学含む）東京農工大学工学府博士前期課程

問　題　用　紙　　専門科目

情報工学専攻

16枚のうち16

受験番号	MC－

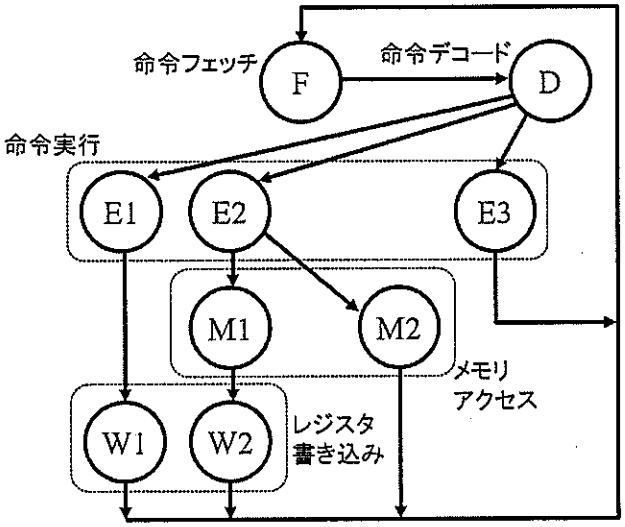


図１１―２　制御ユニット（Control Unit）の状態遷移図

以下の命令を実行したとき、指定したステージにおけるa ～ i のバスの値をビット幅が判るように、6ビット以下は2進数で、それ以外は16進数で示せ。ここで、前に0x がついている定数は16進数を表すものとし、命令フェッチ時のプログラムカウンタは、すべて0xD7000000であるとする。

〔1〕 add $13, $21, $16（命令実行ステージ以降）($21＝0xFFFFFFF7, $16＝0x00000003)

a[　　]　b[　　]　c[　　]　d[　　]　f[　　]

〔2〕 lw $7, 0x300($17)（命令実行ステージ）($17=0x00000014)

a[　　]　c[　　]　d[　　]　e[　　]　i[　　]

〔3〕 beq $19, $23, L3（beq命令から11命令先の命令）（命令デコードステージ、$19と$23は異なる値を持つ）

a[　　]　b[　　]　f[　　]　g[　　]　h[　　]

〔4〕 sw $19, 0x24($9)（命令実行ステージ）

($9=0x0000008, $19= 0x00000036)

a[　　]　b[　　]　d[　　]　e[　　]　i[　　]