平成16年度　大学院博士(前期)課程入学者選抜学力試験

# 専 門 科 目
# （情報科学）

［90分］

**注 意 事 項**

1. 試験開始の合図があるまで，この問題冊子を開かないでください.
2. 出題分野およびページは，下表のとおりです.

| 出 題 分 野 | ペ ー ジ | 問題数 | 選択方法 |
|---|---|---|---|
| 電 子 工 学 基 礎 | 1 | 1問 | 左の５分野から２分野を選択し，選択した各分野について１問を解答してください. |
| 情 報 工 学 基 礎 | 2 | 1問 | |
| ハ ー ド ウェア | 3 〜 4 | 2問 | |
| ソ フ ト ウェア | 5 〜 8 | 2問 | |
| 情 報 シ ス テ ム | 9 〜 12 | 2問 | |

3. 解答用紙は3枚に分かれているので，すべての解答用紙の所定欄に選択した分野名，問題番号（IまたはII），受験番号と氏名をはっきりと記入してください.
4. 問題に問いなどがある場合は，解答欄内に問いの番号（**問1**など）を記入してから解答を始めてください.
5. 計算または下書きに用いる用紙が3枚，下書きに用いる原稿用紙が1枚，解答用紙と一緒にあります.
6. 試験中に問題冊子の印刷不明瞭，ページの落丁・乱丁および解答用紙の汚れ等に気がついた場合は，静かに手を上げて監督員に知らせてください.
7. 試験終了後，問題冊子および下書き用紙は持ち帰ってください.
8. 設問ごとに配点が記されています.

# 電子工学基礎

**I** 図 1 の回路においてインダクタンス $L$ [H]，キャパシタンス $C$ [F]，抵抗 $R$[Ω] が直列に交流電源と接続されている．電源は正弦波で，電圧ベクトル $E$，実効値 $E_e$ [V]，角周波数 $\omega$ [rad/s] とする．回路は定常状態と仮定して以下の問いに答えよ．（配点 50 点）

**問 1**　電源側から見た回路のインピーダンスを求めよ．

**問 2**　$L$ と $C$ の間に

$$\omega L = \frac{1}{\omega C}$$

なる関係が成り立つ場合，抵抗 $R$ の両端に生じる電圧を求めよ．

**問 3**　電源の角周波数 $\omega$ を変えたときの回路に流れる電流 (実効値) の最大値を $I_0$ とし，その時の角周波数を $\omega_0$ とする．回路に流れる電流 (実効値) が $I_0$ の $1/\sqrt{2}$ となる角周波数 $\omega$ を $R$, $L$, $C$ と $\omega_0$ によって表せ．

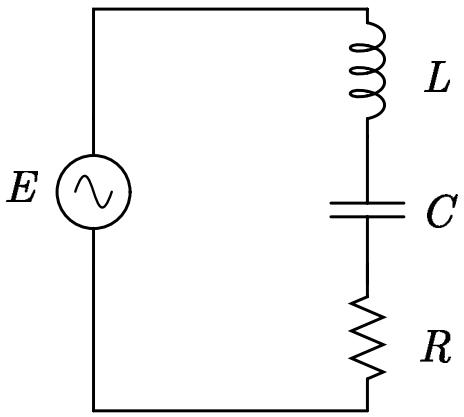



図 1: $LCR$ 回路

**電子工学基礎の問題は，このページで終りである．**

# 情報工学基礎

**I** 次の「関係」についての文章を読み，以下の問いに答えよ．（配点 50 点）

集合 $A$, $B$ の直積 $A \times B$ の部分集合 $R$，すなわち

$$R \subseteq A \times B$$

は $A$ から $B$ への（2 項）関係と呼ばれる．特に $A = B$ の場合，$A$ 上の関係と呼ばれる．$(a, b) \in R$ のとき，要素 $a$ と $b$ は $R$ の関係にあるといい，$aRb$ と書く．

関係 $R \subset A \times A$ が同値関係であるとは，

**反射的**　任意の $a \in A$ について $aRa$ が成り立つ

**対称的**　$aRb$ ならば $bRa$ が成り立つ

**推移的**　$aRb$ かつ $bRc$ ならば $aRc$ が成り立つ

という三つの性質を満たすことである．

$R$ を集合 $A$ 上の同値関係とするとき，$A$ の要素 $a$ と $R$ の関係にある $A$ の要素全体の集合，すなわち，$\{b \in A; aRb\}$ を $a$ の同値類といい，$[a]$ と書く．

**問 1**　以下の関係が同値関係かどうか理由を示して答えよ．

**問 1.1**　集合 $A$ の二つの要素 $a$, $b$ の間の等号関係

**問 1.2**　実数間の大小関係

**問 2**　$a$, $b$, $c$ を $A$ の任意の要素とし，$[a]$ を関係 $R$ の同値類とするとき，次の命題を証明せよ．

**問 2.1**　$a \in [a]$

**問 2.2**　$aRb$ と $[a] = [b]$ は同値である

**問 2.3**　$b, c \in [a]$ ならば $bRc$ である

**問 3**　整数の集合 $Z$ に対して 5 で割った余りが同じという関係を $R$ とする．$R$ が同値関係であることを示し，同値類をすべて挙げよ．

**情報工学基礎の問題は，このページで終りである．**

# ハードウェア

**I** 冗長入力 $\phi$ (don't care 項) が存在する論理関数 $Z(A, B, C, D)$ を

$$Z = \overline{A}B\overline{C}\overline{D} + AB\overline{C}\overline{D} + A\overline{B}C\overline{D} + \overline{A}B\overline{C}D$$

で与えたとき，以下の問いに答えよ．ただし，冗長入力 $\phi$ は

$$\phi : \overline{A}\overline{B}\overline{C}\overline{D},\ \overline{A}\overline{B}C\overline{D},\ AB\overline{C}D,\ \overline{A}BCD$$

とする．（配点 50 点）

**問 1**　冗長入力 $\phi$ を含め，関数 $Z$ をカルノー図で表現せよ．

**問 2**　関数 $Z$ を簡単化して示せ．

**問 3**　簡単化した関数 $Z$ を NAND ゲートで構成せよ．

**II** マイクロプロセッサ P は，命令長が 14 ビット固定長の命令セットと内部に 8 ビット幅のレジスタ W を持つ．表 1 は，このマイクロプロセッサ P がもついくつかの機械語命令のニーモニック表記，対応する機械語，およびその動作を示したものである． なお，表 1 のニーモニック中の N は数値である．また，機械語表記中の n は，数値 N を 8 ビットまたは 11 ビットの 2 進数として表記したものとする．例えば，レジスタ W に数値 5（16 進数表記）を代入する命令のニーモニック表記と機械語（2 進数表記および 16 進数表記）は，次のようになる．

| 命令 | 機械語 (2 進数表記) | 機械語 (16 進数表記) |
|---|---|---|
| `MOVLW 5` | `11 0000 0000 0101` | `3005` |

このマイクロプロセッサ P に関して，以下の問いに答えよ．ただし，設問中に現れる数値は，特に指定のない場合は 16 進数表記である．また，解答でも数値は 16 進数表記で表し，16 進数であることを示す「0x」や「H'」などの記号を付与する必要はない．（配点 50 点）

**問 1**　以下の命令に対応する機械語（2 進数表記および 16 進数表記）を示せ．

**問 1.1**　`MOVLW 0`

**問 1.2**　`ADDLW 5`

**問 1.3**　`GOTO 100`

**問 2**　マイクロプロセッサ P のプログラムメモリに，表 2 のような機械語のプログラムを格納し，0 番地から実行を開始した．実行開始から 10 命令（10 進数）を実行するまでの間の各命令実行段階において，　実行命令数（実行開始からの通し番号），
　命令実行を開始する時点でのプログラムカウンタ（PC）の値，　そこでフェッチした命令（機械語およびニーモニック表記），　その命令の実行が完了した時点でのレジスタ W の値を，各段階で順を追って表 3 の形式で示せ．

表 1:

| ニーモニック | 機械語（2 進数表記） | 命令の動作 |
|---|---|---|
| MOVLW N | 11 0000 nnnn nnnn | レジスタ W に数値 N を代入 |
| ADDLW N | 11 1110 nnnn nnnn | レジスタ W の内容に数値 N を加算し，結果をレジスタ W に代入 |
| GOTO N | 10 1nnn nnnn nnnn | N 番地へ無条件分岐 |

表 2:

| アドレス | 内容 |
|---|---|
| 0 | 3000 |
| 1 | 3e01 |
| 2 | 3e03 |
| 3 | 2802 |

表 3:

| 実行命令数 | PC の値 | フェッチした命令 | | レジスタ W の値 |
|---|---|---|---|---|
| | | (機械語) | (ニーモニック) | |
| 1 | | | | |
| 2<br>⋮<br>10 | | | | |

**ハードウェアの問題は，このページで終りである．**

# ソフトウェア

**I** 以下の要件を満たす音楽会のチケット予約システムの開発を考える．

- 利用者は，日時，会場，演奏者を指定して該当する公演の有無を調べることができる．
- 利用者は，開演される公演に対する会場の空席状況を知ることができる．
- 利用者は，空席のある会場のチケットを予約することができる．
- 会場には自由席はなく，チケットの予約は座席の予約も兼ねているものと仮定する．
- システムは，利用者の入力する情報の誤りを検出し訂正する機能は持たない．
- システムは，新規予約の受付のみを扱い，予約の照会や取り消しは扱わない．
- システムは，利用者の認証，発券や決済等の処理は扱わない．

表 1 に示すアクターと図 1 に示すユースケース図を用いて，システムを UML により設計した．このとき，システムの状態遷移図は図 2 となった．このシステムについて，以下の問いに答えよ．（配点 50 点）

**問 1**　図 1 の空欄 **(A)** ～ **(F)** に当てはまるのに最も適した語句を答えよ．

**問 2**　利用者が公演の有無の確認からチケット予約までを滞りなく行った場合について，シーケンス図を描きはじめたところ，図 3 のようになった．図 3 の未完成なシーケンス図を完成させよ．ただし，解答用紙には完成したシーケンス図を示すこと．

表 1: アクター一覧

| アクター | 役割り |
|---|---|
| 利用者 | システムの利用者 |
| 公演情報データベース | 公演の日時，会場，演奏者の情報を管理する |
| 空席情報データベース | 公演会場の空席情報を管理する |

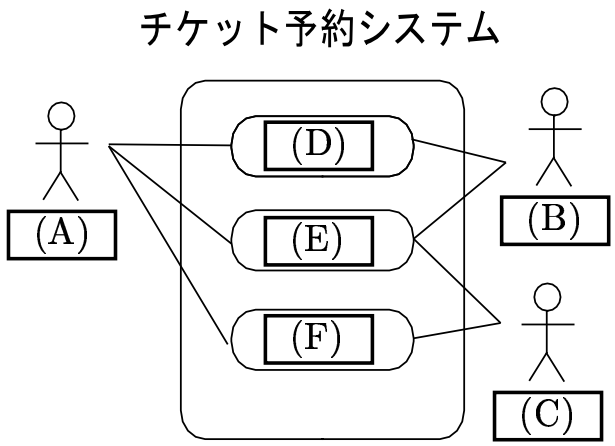



図 1: チケット予約システムのユースケース図

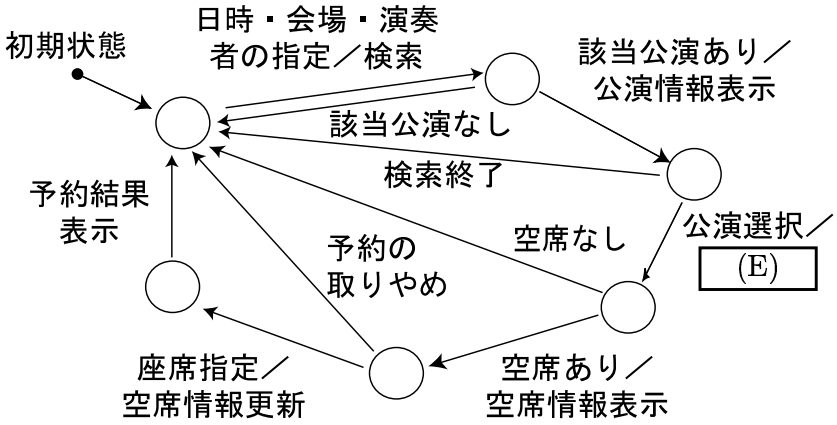



図 2: チケット予約システムの状態遷移図

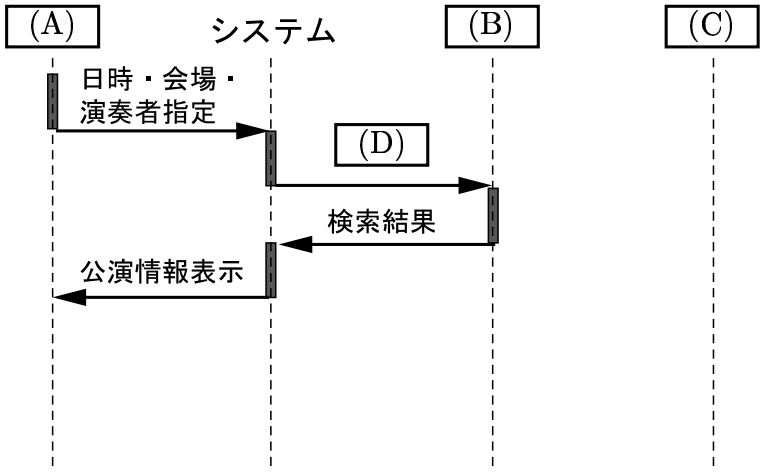



図 3: チケット予約システムのシーケンス図の一部

## II 以下の問いに答えよ．（配点 50 点）

**問 1** 完全性，最適性，計算量の性質に注目して，縦型（深さ優先）探索，横型（幅優先）探索それぞれの特徴を計 200 字以内で述べよ．

**問 2** 図 4 に示す木を左のノードから右のノードに向かって縦型（深さ優先）探索，横型（幅優先）探索，繰り返し縦型探索（反復深化法）で探索する．なお解ノードは J，N，R とし，いずれかの解が見つかったらその時点で探索は終了するものとする．

**問 2.1** それぞれの探索によって選ばれる解ノードを挙げよ．

**問 2.2** それぞれの探索によって解ノードを見つけるまでに調べるノードを順番に挙げよ．

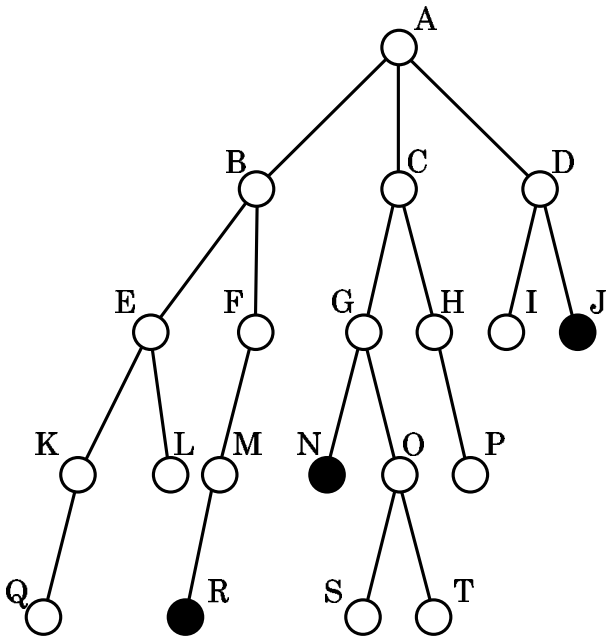



図 4: 木

**問 3**　ヒューリスティックスとは何かを 40 字以内で説明せよ.

**問 4**　最良優先探索とは何かを 300 字以内で説明せよ.

**ソフトウェアの問題は，このページで終りである．**

# 情報システム

**I** 表 1 のリレーション R0（「社員」）は第 2 正規形であるが，第 3 正規形ではない．ただし,「部門長」は「所属部門」に対して，決まっているものとする．また，R0 はテーブル（実表）である．このとき，以下の問いに答えよ．（配点 50 点）

表 1: リレーション R0

| 社員番号 | 社員名 | 年齢 | 所属部門 | 部門長 |
|---|---|---|---|---|
| 11 | A | 50 | B01 | 11 |
| 12 | B | 40 | B02 | 21 |
| 21 | C | 30 | B02 | 21 |
| 22 | D | 22 | B02 | 21 |
| 23 | E | 55 | B01 | 11 |
| 24 | F | 45 | B01 | 11 |

**問 1**　R0 を第 3 正規形に正規化し，リレーション R1，R2 を求め，求めた R1，R2 をテーブル（実表）で示せ．

**問 2**　問 1 で正規化を行なうときに，着目すべき従属性は，つぎに示す候補のうちどれか答えよ．

**着目すべき従属性の候補**

完全関数従属性，多値従属性，推移的関数従属性

**問 3**　問 2 の着目すべき従属性は，どの属性に対するものであるか．X→Y の形式で答えよ．ただし，X→Y は Y が X に関数従属することを示す．

**問 4**　次の SQL 文は，問 1 で求めたリレーション R1，R2 をテーブル（実表）ではなく，それぞれビュー（導出表）V1 と V2 として求めるものである．SQL 文中の空欄 (1) ～ (10) に最も適切な語句を入れて，SQL 文を完成させよ．ただし，記号「;」は SQL 文の区切りを表す．また，解答用紙には空欄の番号と語句との対応が明確になるように記せ．

```
CREATE VIEW (1) AS SELECT (2) , (3) , (4) , (5) FROM (6) ;

CREATE VIEW (7) AS SELECT DISTINCT (8) (9) FROM (10) ;
```

**問 5**　次の SQL 文は，V1 と V2 から，自然結合によりビュー V3 を生成し，V3 を用いて，部門長よりも年長の「社員名」,「所属部門」を求めるものである．SQL 文中の空欄 (11) ～ (21) に最も適切な語句を入れて，SQL 文を完成させよ．ただし，記号「;」は SQL 文の区切りを表す．また，解答用紙には空欄の番号と語句との対応が明確になるように記せ．

```
CREATE VIEW (11) AS SELECT * FROM (12) , (13)
    WHERE (14)  NATURAL JOIN (15) ;

SELECT (16) , (17)  FROM (18) , (19) ,WHERE (20) AND (21) ;
```

**II** 認証機能と秘密性を保証した電子メールのセキュリティにおいては，共通鍵暗号や公開鍵暗号が使用される．下記の処理手順 (a)~(j) は，送信者によるメッセージの暗号化から受信者によるメッセージの復号化までに行われる一連の処理ステップを示している．このとき，以下の問いに答えよ．（配点 50 点）

**処理手順**

（a） メッセージに署名を付加する

（b） セッション鍵を受信者の [ **(1)** ] を使って RSA で暗号化し，メッセージに追加する

（c） セッション鍵を使ってメッセージを復号化する

（d） ハッシュを [ **(2)** ] の非公開鍵（秘密鍵）を使って RSA で暗号化することにより，メッセージに対する署名を生成する

（e） 送信者はメッセージを作成する

（f） 受信者は自分の [ **(3)** ] を使い，RSA で復号化してセッション鍵を取り出す

（g） ハッシュ（署名）を送信者の公開鍵を使って [ **(4)** ] で復号化する

（h） ハッシュ関数 [ **(5)** ] を使ってメッセージからハッシュを作成する

（i） メッセージに対するハッシュを新しく生成し，この計算されたハッシュ値を復号化されたハッシュ（署名）と比較する（もしこの 2 つが一致すれば，署名は有効であると認められ，メッセージは本物だと確認される）

（j） メッセージと署名の組を，送信者によって生成された一度だけ有効な [ **(6)** ] を使って、 [ **(7)** ] で暗号化する

**問 1** (a)~(j) の処理手順を送信者のメッセージの暗号化から受信者によるメッセージの復号化までの手順を示すものに並び替えよ．ただし，(a)→(b)→ · · · のように順序がわかるように示せ．

**問 2** (a)~(j) の処理手順中の空欄 [ **(1)** ] ～ [ **(7)** ] に，最も適切な語句を下記の語群から選び，処理手順を完成させよ．ただし，解答用紙には空欄の番号と選択した語句との対応関係が明確になるように記せ．また，同一の語句を複数回用いてはいけない．

**候補となる語群:**

RSA，SHA-1，セッション鍵，公開鍵 ，非公開鍵（秘密鍵），3DES，送信者

**問 3**　(a)∼(j) の処理手順の中で，認証機能がどのように保証されるかを 100 字以内で説明せよ．ただし，説明では RSA 及び SHA-1 について言及すること。

**問 4**　(a)∼(j) の処理手順においては暗号の鍵交換問題をどのように解決しているかを 50 字以内で説明せよ．

**情報システムの問題は，このページで終りである．**

# 解 答 冊 子

専 門 科 目

（情報科学）

| 氏 名 | | 受験番号 | |
|---|---|---|---|

# 博士 (前期) 専門科目 (情報科学) 解答用紙 (1)

| 分 野 名 |
|---|
| |
| 問 題 番 号 |
| |
| 点 |

博士 (前期) 専門科目
情報科学 (1)

(枠内に解答を書くこと)

| 氏 名 | | 受験番号 | |
|---|---|---|---|

# 博士 (前期) 専門科目 (情報科学) 解答用紙 (2)

| 分 野 名 |
|---|
| |
| 問 題 番 号 |
| |
| 点 |

博士 (前期) 専門科目
情報科学 (2)

(枠内に解答を書くこと)

| 氏 名 | | 受験番号 | |
|---|---|---|---|

# 博士 (前期) 専門科目 (情報科学) 解答用紙 (3)

| 分 野 名 |
|---|
| |
| 問 題 番 号 |
| |
| 点 |

博士 (前期) 専門科目
情報科学 (3)

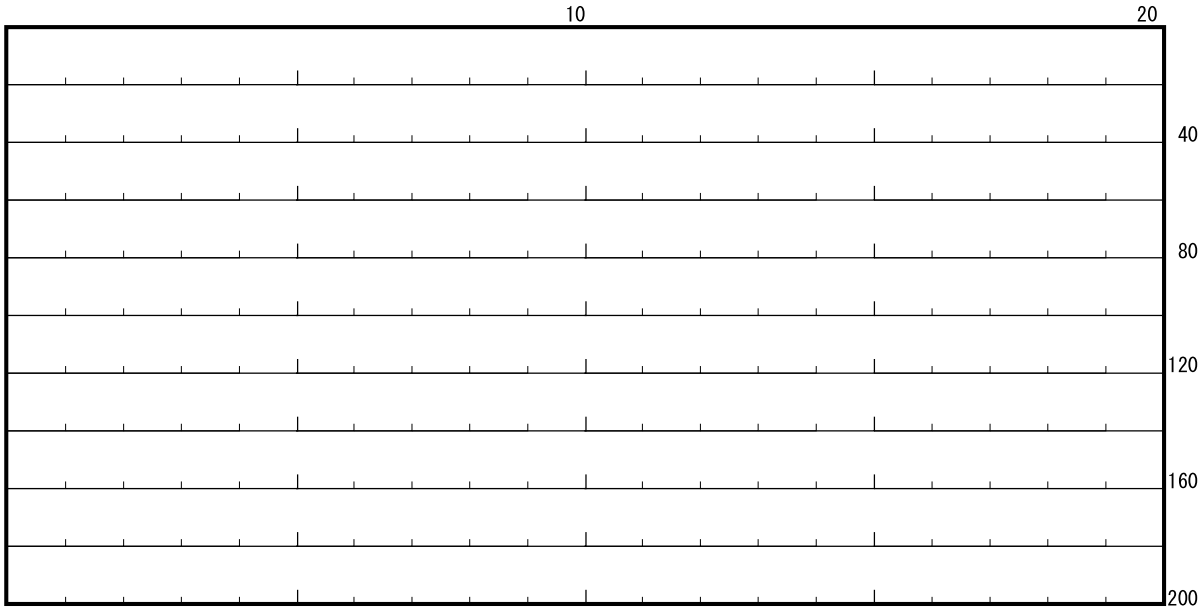
(枠内に解答を書くこと)

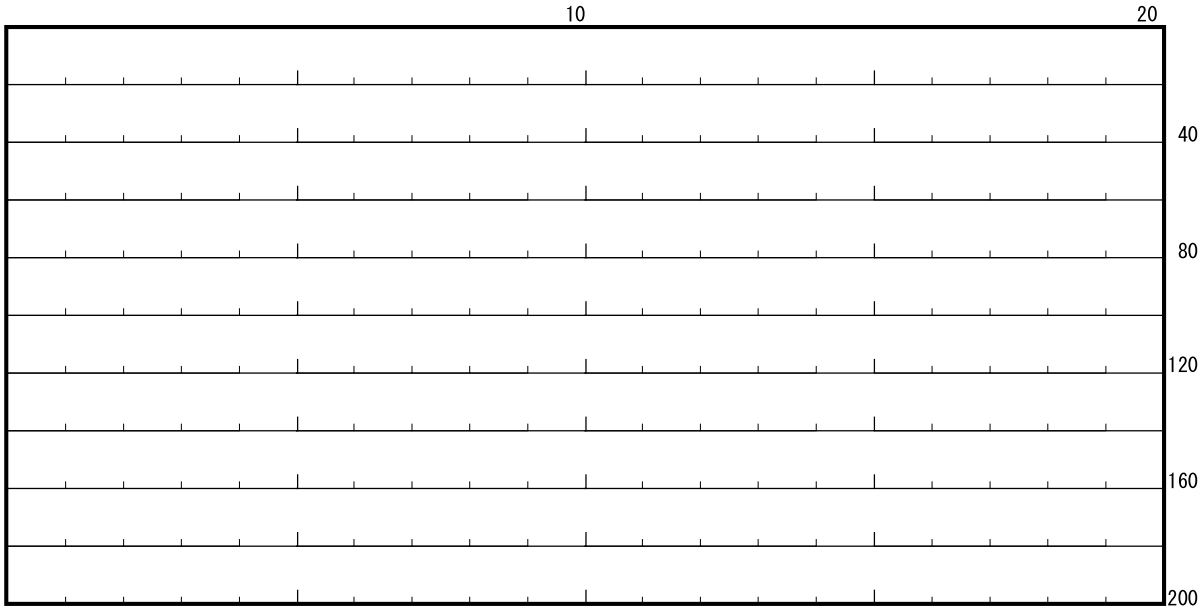
[計 算 用 紙/下 書 き 用 紙]

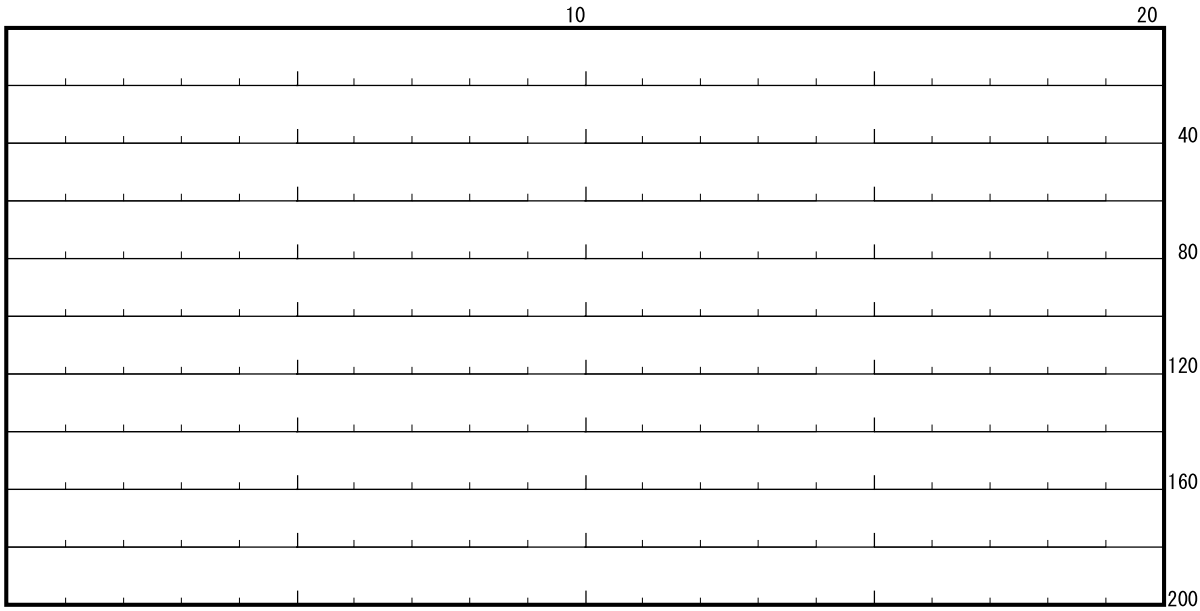
[計 算 用 紙/下 書 き 用 紙]

[計 算 用 紙/下 書 き 用 紙]

# ［下　書　き　用　紙］




（20字×10行×3）