

解答用紙の選択科目名に「情報」と記入し、選択科目マーク欄の「情報」をマークしてから解答してください。情報の解答は解答用紙の解答欄 (1)～(84) にマークしてください。

情報 I

以下、法制度に関しては、日本のものについて考えるものとする。

「個人情報の保護に関する法律」（個人情報保護法）に関する次の文章を読み、設問に回答しなさい。

個人情報取扱 者は、顔識別機能付きカメラシステムにより特定の個人を識別することができるカメラ画像やそこから得られた データを取り扱う場合、個人情報を取り扱うことになるため、利用目的をできる限り特定し、当該利用目的の範囲内でカメラ画像や データ等を利用しなければなりません。

具体的には、どのような個人情報の取扱いが行われているかを本人が利用目的から合理的に予測・想定できる程度に利用目的を特定しなければならない①ため、従来型防犯カメラの場合と異なり、犯罪防止目的であることだけでなく、顔識別機能を用いていることも明らかにして、利用目的を特定しなければなりません。

顔識別機能付きカメラシステムを利用する場合は、設置されたカメラの外観等から犯罪防止目的で顔識別機能が用いられていることを認識することが困難であるため、【②】に当たらず、個人情報の利用目的を本人に通知し、又は しなければなりません。（中略）また、本人から理解を得るためできる限り分かりやすく情報提供を行うため、顔識別機能付きカメラシステムの運用 、同システムで取り扱われる個人情報の利用目的、問い合わせ先、さらに詳細な情報を掲載した Web サイトの 又は QR コード等を店舗や駅・空港等の入口や、カメラの設置場所等に掲示することが望ましいと考えられます。

（出典：個人情報保護委員会『「個人情報の保護に関する法律についてのガイドライン」に関する Q&A」（A1-14）を一部改変）

（ア）空欄 ～ に入るもっとも適した語を選択肢から選び、その番号を解答欄にマークしなさい。

【 ～ の選択肢】

- (1) URL (2) 公表 (3) 氏名 (4) 合意 (5) 客体
(6) 消費 (7) コンソール (8) 事業 (9) 主体 (0) 顔特徴

(イ) 下線部①について、個人情報保護法が定められている背景の説明として適切でないものを選択肢から選び、その番号を解答欄 にマークしなさい。

- (1) デジタル社会の進展に伴い個人情報の利用が著しく拡大していること。
- (2) 個人情報の適正かつ効果的な活用が、新たな産業の創出や、活力ある経済社会と豊かな国民生活の実現に資するものであること。
- (3) 本人による事前の同意なく第三者が個人情報を取得することは許されないこと。
- (4) 個人の権利利益を保護する必要があること。
- (5) 個人情報の有用性に配慮すべきであること。

(ウ) 空欄②にあてはまるものを選択肢から選び、その番号を解答欄 にマークしなさい。なお、各選択肢で「法」は個人情報保護法を指すものとする。

- (1) 「本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合」(法第 21 条第 4 項第 1 号)
- (2) 「当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合」(法第 21 条第 4 項第 2 号)
- (3) 「国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合」(法第 21 条第 4 項第 3 号)
- (4) 「取得の状況からみて利用目的が明らかであると認められる場合」(法第 21 条第 4 項第 4 号)
- (5) 「人の生命、身体又は財産の保護のために緊急に必要がある場合」(法第 21 条第 2 項但書)

情報Ⅱ

以下の設問において、 $A \cdot B$ は、 A と B の論理積 (AND) を表し、 $A+B$ は、 A と B の論理和 (OR) を表し、 \overline{A} は、 A の否定 (NOT) を表す。

(ア) 次の例のように、ある論理式を等価な別の論理式で表すこともできる。

$$\overline{A \cdot B} = \overline{A} + \overline{B}$$

この例にならって、次のそれぞれの式が正しくなるように、空欄 $\boxed{(8)} \sim \boxed{(17)}$ に入るもっとも適したものを選択肢の中から選び、解答欄にマークしなさい。

$$(\overline{A} + C) \cdot (B + \overline{C} + \overline{D}) = \overline{A} \cdot \boxed{(8)} + \boxed{(9)} \cdot \boxed{(10)} + \boxed{(11)} \cdot \boxed{(12)}$$

(選択肢の番号が $\boxed{(9)} < \boxed{(11)}$ 、 $\boxed{(9)} < \boxed{(10)}$ 、 $\boxed{(11)} < \boxed{(12)}$ となるように選ぶこと。)

$$\overline{A} \cdot B + \overline{B} \cdot \overline{C} \cdot D + C \cdot D = (B + D) \cdot (\boxed{(13)} + \boxed{(14)}) \cdot (\boxed{(15)} + \boxed{(16)} + \boxed{(17)})$$

(選択肢の番号が $\boxed{(13)} < \boxed{(14)}$ 、 $\boxed{(15)} < \boxed{(16)} < \boxed{(17)}$ となるように選ぶこと。)

【 $\boxed{(8)} \sim \boxed{(17)}$ の選択肢】

(1) A (2) \overline{A} (3) B (4) \overline{B}

(5) C (6) \overline{C} (7) D (8) \overline{D}

(イ) 2進法で表現された数の各桁を、その値が 0 であるか 1 であるかに応じて、真偽値の 0(偽) と 1(真) をとる命題変数だとして扱うことにする。この場合に、2進法による数の表現と各桁を命題変数だとして作られた論理式の関係について述べた次の文章の空欄 $\boxed{(18)} \sim \boxed{(25)}$ に入るもっとも適したものを選択肢の中から選び、解答欄にマークしなさい。

4 桁の 2 進法表現 $A_3A_2A_1A_0$ で表される数 X を考える。4 桁の 2 進法表現が表している 0 および正の整数は 10 進法表現で 0 から 15 になり、 X もその範囲の値を表す。 X が 15_{10} を表す場合、 $A_3 \cdot A_2 \cdot A_1 \cdot A_0$ という論理式の値は 1(真) になる。

X の値に応じて次の表の条件を満たすような論理式は、以下のようになる。

$$\boxed{(18)} \cdot \boxed{(19)} + \boxed{(20)} \cdot \boxed{(21)}$$

(選択肢の番号が $\boxed{(18)} < \boxed{(19)}$ 、 $\boxed{(18)} < \boxed{(20)}$ 、 $\boxed{(20)} < \boxed{(21)}$ となるように選ぶこと。)

X の値 (10 進数)	論理式の真偽値
1,3,5,7,8,10,12	真
2,4,6,9,11	偽

これとは真偽を逆にした、次の表の条件を満たすような論理式は、次のようになる。

$$\boxed{(22)} \cdot \boxed{(23)} + \boxed{(24)} \cdot \boxed{(25)}$$

(選択肢の番号が $\boxed{(22)} < \boxed{(23)}$ 、 $\boxed{(22)} < \boxed{(24)}$ 、 $\boxed{(24)} < \boxed{(25)}$ となるように選ぶこと。)

X の値 (10 進数)	論理式の真偽値
1,3,5,7,8,10,12	偽
2,4,6,9,11	真

【 $\boxed{(18)} \sim \boxed{(25)}$ の選択肢】

- (1) A_0 (2) $\overline{A_0}$ (3) A_1 (4) $\overline{A_1}$
 (5) A_2 (6) $\overline{A_2}$ (7) A_3 (8) $\overline{A_3}$

(ウ) 前問と同様に、2 進法による数の表現と各桁を命題変数だとして作られた論理式の関係について述べた次の文章の空欄 $\boxed{(26)} \sim \boxed{(33)}$ に入るもっとも適したものを選択肢の中から選び、解答欄にマークしなさい。

A_1A_0 および B_1B_0 で表される 2 ビットの 2 進法表現で表される数と、これら 2 数の積を表す 4 ビットの 2 進法表現の数 $C_3C_2C_1C_0$ を考える。 A_1, B_1, C_3 が上位ビットである。このとき、 C_3 および C_2 を表す論理式はそれぞれ以下になる。

$$C_3 = \boxed{(26)} \cdot \boxed{(27)} \cdot \boxed{(28)} \cdot \boxed{(29)}$$

(選択肢の番号が $\boxed{(26)} < \boxed{(27)} < \boxed{(28)} < \boxed{(29)}$ となるように選ぶこと。)

$$C_2 = \boxed{(30)} \cdot \boxed{(31)} \cdot \boxed{(32)} + \boxed{(30)} \cdot \boxed{(31)} \cdot \boxed{(33)}$$

(選択肢の番号が $\boxed{(30)} < \boxed{(31)}$ 、 $\boxed{(32)} < \boxed{(33)}$ となるように選ぶこと。)

【(26) ～ (33) の選択肢】

- (1) A_0 (2) $\overline{A_0}$ (3) A_1 (4) $\overline{A_1}$
 (5) B_0 (6) $\overline{B_0}$ (7) B_1 (8) $\overline{B_1}$

情報Ⅲ

空欄

(34)

 ～

(44)	(45)	(46)
------	------	------

 に入るもっとも適した数字を解答欄にマークしなさい。

ある正の整数 x を別の正の整数 n で割った余りを $x \bmod n$ と表現する。 $2^x \bmod n$ を考えると、 n が 3, 5, 11 などの特定の素数の場合に x を 1 から $n-1$ まで順に増やしたとき、その計算結果として、1 から $n-1$ までのすべての整数が重複することなく出現することがわかっている。また $n = 7, 17, 23, 31$ の場合は $3^x \bmod n$ に対して同様の法則性があることがわかっている。

例えば $n = 5$ の場合、 $y = 2^x \bmod 5$ の計算結果は、 $x = 1$ のとき $y = \boxed{(34)}$ 、 $x = 2$ のとき $y = \boxed{(35)}$ 、 $x = 3$ のとき $y = \boxed{(36)}$ 、 $x = 4$ のとき $y = \boxed{(37)}$ となる

この仕組みを利用してアリスとボブの二人が第三者に知られることなく秘密の数字を共有する方法について考える。アリスは誰にも教えない秘密の数字として A 、ボブは秘密の数字 B を用意するものとする。

上に示した性質を持つ x と n の組み合わせとなる具体的な数として g と p を使用することについてアリスとボブは合意しており、この情報は外部に知られる可能性があるものとする。

この前提においてアリスは $g^A \bmod p$ を計算してボブに送る。この情報は第三者に見られる可能性がある。同様にボブは $g^B \bmod p$ を計算してアリスに送る。

この時 $(g^A \bmod p)^B \bmod p = (g^B \bmod p)^A \bmod p = g^{AB} \bmod p$ が成り立つことがわかっている。この性質を利用することによってアリスとボブは秘密の数字 $g^{AB} \bmod p$ を第三者に知られることなく共有することができる。

今、アリスとボブが $g = 2, p = 19$ を使用することに合意した上でアリスは $A = 13$ 、ボブは $B = 15$ を秘密の数字として選んだとする。

これまで説明した方法でアリスとボブが第三者に知られることなく秘密の数字を共有したい場合は、次のようになる。

- アリスがボブに対して送信する数字は

(38)	(39)	(40)
------	------	------
- ボブがアリスに対して送信する数字は

(41)	(42)	(43)
------	------	------
- 両者が共有する秘密の数字は

(44)	(45)	(46)
------	------	------

情報Ⅳ

次の文章の空欄 (58) (59) (60)、(61) (62) (63) の各欄にあてはまる数字を解答欄にマークしなさい。また、(47) ～ (57) にはもっとも適したものを選択肢から選び、解答欄にマークしなさい。ただし、 $A + B$ は A と B の論理和 (OR) を表し、 $A \cdot B$ は A と B の論理積 (AND) を表す。また、 \bar{A} は A の否定 (NOT) を表す。

算術論理演算装置 (Arithmetic Logic Unit、以下 ALU と表記) は、コンピュータを構成する基本的な装置のひとつである。図 1 に示す ALU は 8 種類の演算、論理積 (AND)、論理和 (OR)、加算 (ADD)、減算 (SUB)、左論理シフト (SLL)、右論理シフト (SRL)、左算術シフト (SLA)、右算術シフト (SRA) を実行可能である。

ALU への入力は、2 組の 8 ビットのデータ $a[7..0]$ 、 $b[7..0]$ および 3 ビットの制御信号 $c[2..0]$ であり、出力は 8 ビットのデータ $z[7..0]$ である。ここで、 $c[2..0]$ は 3 個の信号 c_2 、 c_1 、 c_0 をまとめて表記したものである。同様に $a[7..0]$ は 8 個の信号をまとめて表記しており、算術演算 (ADD、SUB、SLA、SRA) を行うときは、信号 (0 または 1) を並べたビット列 $a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0$ を 2 の補数表現による整数と考える。 $b[7..0]$ 、 $z[7..0]$ についても同じである。

8 種類の演算のうち、どの演算の結果が出力されるかは、 $c[2..0]$ により決定される。 $c[2..0]$ と実行される演算の対応を図 1 右の動作表に示す。

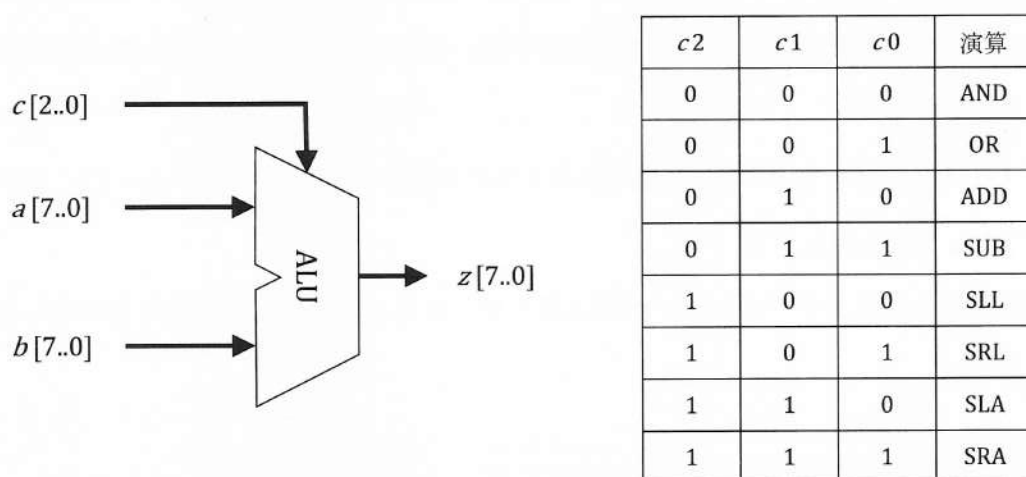


図 1

(ア) ALU 内部の重要モジュールのひとつがシフタ回路である。シフタは入力されたビット列を左あ

るいは右に指定されたビット数分だけシフト（移動）させる回路であり、空いたビットの処理の違いにより、論理シフトと算術シフトに分類される。論理シフトの場合は、ビットを移動させた結果、空いたビットには0が挿入され、ビット列からあふれたビットは捨てられる。

算術シフトは、2の補数表現において符号を表す最上位ビットを固定とし、残りのビットを左もしくは右に指定されたビット数分シフトさせる。左算術シフトでは空いたビットに0が、右算術シフトでは空いたビットに最上位と同じ値が挿入される。いずれもビット列からあふれたビットは捨てられる。このとき、左にあふれたビットの値が最上位ビットと違う場合はオーバーフローと呼び、計算結果がそのビット列で表現できる範囲を超えていることを意味する。

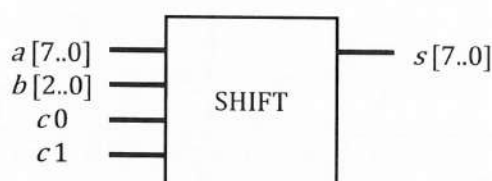


図 2

図 2 のようなシフタ回路を構成しよう。この回路は、 $b[7..0]$ の下位 3 ビット $b[2..0]$ をシフトするビット数とし、入力 $a[7..0]$ に対してシフト演算を実行し、 $s[7..0]$ を出力する。ALU への制御信号のうち、 $c2$ は 1 とする。 $c0$ が 0 の場合は (47)、1 の場合は (48) の指定になり、 $c1$ が 0 の場合は (49)、1 の場合は (50) の指定となる。ここで、 $b[2..0]$ ビットの左算術シフトは、オーバーフローが起こらない場合、 $a[7..0]$ と $2^{(b[2..0])}$ の (51) を行う演算に相当し、 $b[2..0]$ ビットの右算術シフトは、 $a[7..0]$ と $2^{(b[2..0])}$ の (52) を行う演算に相当する。ただし、選択肢 (8) は整数の除算（商の整数部分を求める）とする。

【(47) ～ (52) の選択肢】

- (1) 論理シフト (2) 算術シフト (3) 右シフト (4) 左シフト
- (5) 加算 (6) 減算 (7) 乗算 (8) 除算

(イ) 図 3 に示す回路はマルチプレクサ（データセレクタ）と呼ばれ、2つの入力 X と Y から 1つを選択して Z に出力する機能を持つ。出力は制御信号 C によって決定され、その挙動は図中右の動作表のようになる。

図 4 は、マルチプレクサを用いて、図 2 のシフタ回路の右論理シフトおよび右算術シフトの部分を実現した回路図である。図 4 の中の ア は (53)、イ は (54)、ウ は (55)、エ は (56) である。

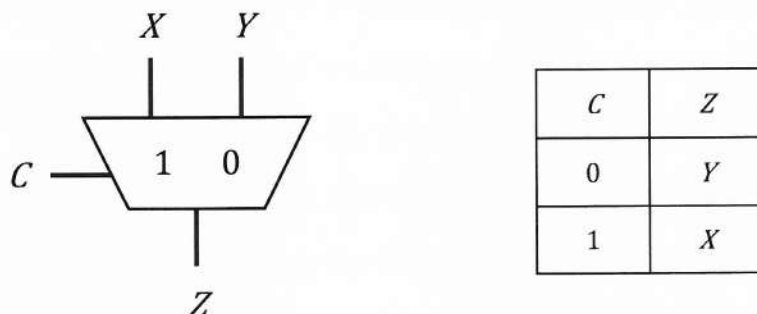


図 3

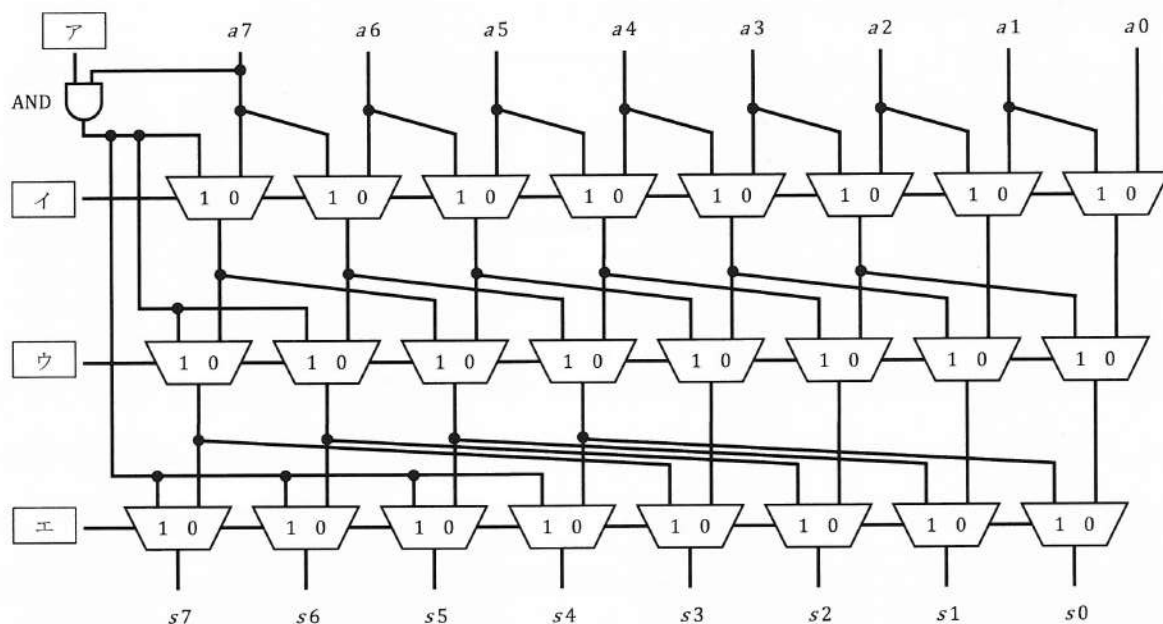


図 4

入力が n ビットであるとき、図 4 のように右論理シフト、右算術シフトを実現する回路に必要なマルチプレクサの数は $\boxed{(57)}$ となる。ただし、 n は 2 のべき乗に限り、シフトするビット数は、0 から $n-1$ の範囲とする。 $n=16$ の場合は $\boxed{(58)}\boxed{(59)}\boxed{(60)}$ 個、 $n=64$ の場合は $\boxed{(61)}\boxed{(62)}\boxed{(63)}$ 個である。

【 $\boxed{(53)} \sim \boxed{(56)}$ の選択肢】

- (1) c_0 (2) c_1 (3) b_0 (4) b_1 (5) b_2

【 $\boxed{(57)}$ の選択肢】

- (1) n (2) $\log_2(n)$ (3) $n \log_2(n)$ (4) $2n \log_2(n)$

情報V

セル・オートマトンとは、複数個のセルから構成され、あるセルの時刻 $t+1$ における状態が、時刻 t における近傍のセルの状態によって決まるようなシステムである。ただし、 t は 1 以上の整数であるとする。ここでは次のようなセル・オートマトンを考える。

- 5 個のセル C_1, \dots, C_5 が環状に並んでいる。 C_1 の右隣は C_2 、 C_2 の右隣は C_3 、 \dots と順に並んでおり、 C_5 の右隣は C_1 であるとする。逆に、 C_5 の左隣は C_4 、 C_4 の左隣は C_3 、 \dots となり、 C_1 の左隣は C_5 である。
- 各セルの状態は 0, 1 の 2 種類である。
- あるセルの次の状態を決める近傍は、そのセル自身と左右両隣のセルである。次の表は、セルの状態の変化を決める規則 f を表している。 x, y, z は、時刻 t における左隣、そのセル自身、右隣の 3 個のセルの状態であり、 $f(x, y, z)$ は時刻 $t+1$ におけるそのセルの状態である。

x, y, z	0,0,0	0,0,1	0,1,0	0,1,1	1,0,0	1,0,1	1,1,0	1,1,1
$f(x, y, z)$	0	1	1	1	1	0	0	0

(ア) 次の文章の空欄

(64)	(65)	(66)	(67)	(68)
------	------	------	------	------

 ～

(69)	(70)	(71)	(72)
------	------	------	------

 に入るもっとも適切な数字を解答欄にマークしなさい。

セル・オートマトン全体の状態を、5 個のセルの状態を書き並べて表す。例えば、 C_1, \dots, C_5 の状態がそれぞれ 0, 1, 1, 0, 0 であることを 01100 と書く。

- 時刻 1 における状態が 11000 ならば、時刻 2 における状態は

(64)	(65)	(66)	(67)	(68)
------	------	------	------	------

 となる。
- 時刻 1 における状態が 0

(69)	(70)	(71)	(72)
------	------	------	------

 ならば、時刻 2 における状態は 01001 となる。

(イ) 次の文章の空欄

(73)	(74)
------	------

 ～

(75)	(76)
------	------

 に当てはまるものを下の選択肢から選び、その番号を解答欄にマークしなさい。ただし、 $a \bmod b$ は a を b で割った余りを表す。

上の状態変化の表において、注目しているセルを C_n とし、 C_1, \dots, C_5 の時刻 t における状態をそれぞれ c_1, \dots, c_5 として、 C_n の時刻 $t+1$ の状態を c_1, \dots, c_5 を使って表したい。まず y は、 C_n の時刻 t

における状態であるから $y = c_n$ である。次に、 C_n の左隣のセルは、 $l(n) = \boxed{(73)} \boxed{(74)}$ とおけば $C_{l(n)}$ であるから、 $x = c_{l(n)}$ となる。同様に $r(n) = \boxed{(75)} \boxed{(76)}$ とおけば、 $z = c_{r(n)}$ である。したがって、 C_n の時刻 $t + 1$ における状態は $f(c_{l(n)}, c_n, c_{r(n)})$ と表すことができる。

【 $\boxed{(73)} \boxed{(74)} \sim \boxed{(75)} \boxed{(76)}$ の選択肢】

- (11) $n \bmod 5$ (12) $(n + 1) \bmod 5$ (13) $(n + 2) \bmod 5$
 (14) $(n + 3) \bmod 5$ (15) $(n + 4) \bmod 5$ (16) $(n \bmod 5) + 1$
 (17) $((n + 1) \bmod 5) + 1$ (18) $((n + 2) \bmod 5) + 1$ (19) $((n + 3) \bmod 5) + 1$
 (20) $((n + 4) \bmod 5) + 1$ (21) $(n \bmod 5) - 1$ (22) $((n + 1) \bmod 5) - 1$
 (23) $((n + 2) \bmod 5) - 1$ (24) $((n + 3) \bmod 5) - 1$ (25) $((n + 4) \bmod 5) - 1$

(ウ) 次の文章の空欄 $\boxed{(77)} \boxed{(78)} \boxed{(79)} \boxed{(80)} \boxed{(81)}$ に入るもっとも適切な数字を解答欄にマークしなさい。

C_1, \dots, C_5 の時刻 1 における状態を入力とし、時刻 2, 3, 4, ... における状態を順に出力するアルゴリズムを次のように書いた。

変数 c_1, \dots, c_5 の値を与えられた状態、関数 f, l, r は上で定義したものとする。

処理 A を繰り返す。

処理 A の始め

変数 n の値を最初は 1 とし、1 ずつ増やしながら 5 になるまで処理 B を繰り返す。

処理 B の始め

c_n の値を $f(c_{l(n)}, c_n, c_{r(n)})$ とする。

処理 B の終わり

c_1, \dots, c_5 の値を出力する。

処理 A の終わり

しかし、このアルゴリズムは正しくない。例えば、時刻 1 における状態が 00100 ならば、時刻 2 における状態は 01110 になるが、このアルゴリズムは $\boxed{(77)} \boxed{(78)} \boxed{(79)} \boxed{(80)} \boxed{(81)}$ と出力する。

(エ) 次の文章の空欄 $\boxed{(82)} \sim \boxed{(84)}$ に当てはまるものを下の選択肢から選び、その番号を解答欄にマークしなさい。

上のアルゴリズムを正しく書き直すと次のようになる。ただし、 d_1, \dots, d_5 は変数である。

変数 c_1, \dots, c_5 を与えられた状態、関数 f, l, r は上で定義したものとする。

処理 A を繰り返す。

処理 A の始め

変数 n の値を最初は 1 とし、1 ずつ増やしながら 5 になるまで処理 B を繰り返す。

処理 B の始め

$\boxed{(82)}$ の値を $\boxed{(83)}$ とする。

処理 B の終わり

n の値を最初は 1 とし、1 ずつ増やしながら 5 になるまで処理 C を繰り返す。

処理 C の始め

c_n の値を $\boxed{(84)}$ とする。

処理 C の終わり

c_1, \dots, c_5 の値を出力する。

処理 A の終わり

【 $\boxed{(82)}$ ～ $\boxed{(84)}$ の選択肢】

(1) 1 (2) n (3) c_n (4) $c_{l(n)}$ (5) $c_{r(n)}$ (6) d_n (7) $f(c_{l(n)}, c_n, c_{r(n)})$