情報領域演習第二 L 演習 (クラス 3) レポート

学籍番号: 1810678
名前: 山田朔也

2019 年 5 月 11 日

1　問 1

1.1　(a)

回路素子の情報の保存の方法が、電圧の High か Low の二通りで表すのが電圧の検出をする上で一番簡単であるから。

1.2　(b)

上記にもあるが、回路は High と Low の二通りの情報を保存しておくことができる。そのため、そのうちの High の情報しか使用しない 1 進法は同一の回路であっても、2 進法に比べて半分の情報しか保存しておくことができずに、回路の肥大化を招くことが理由である。

1.3　(c)

一部の数学的問題 (素因数分解など) の解を得るのに、2 進数であれば時間がかかるが、1 進数であればエラトステネスの篩で十分計算できる。そういった人為的に計算を簡易化する上で計算機構に 1 進数を用いる利点があるだろう。

2　問 2

2 で割っていくという操作はつまり、(本来は入らないが)2 進数の 1 桁目に変換したい数値を入れ、それを 2 で割ることで桁上げをしているということに他ならない。そのため、2 で割り切れたものは桁上りをするが、2 で割り切れなかったものは桁上げされず、その桁に残り続ける。そのため、変換対象の数 N を 2 で割っていき、最後にあまりを逆順に並べればいいのである。

3　問 3

3.1　(a)

表 1　$x \oplus y$ の真理値表

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

3.2　(b)

$x \oplus x$ で入力される組は $0 \oplus 0$ と $1 \oplus 1$ しかなく、これらはどちらも 0 と等しいため、$x \oplus x = 0$ は成立する。

3.3　(c)

表 1 から、$y = 0$ のとき $x \oplus 0 = x$ は成立し、$y = 1$ のとき $x \oplus = \overline{x}$ も成立する。

3.4　(d)

$x \oplus (y \oplus z)$ と $(x \oplus y) \oplus z$ を真理値表にまとめると

表 2　$x \oplus (y \oplus z)$ と $(x \oplus y) \oplus z$ の真理値表

x	y	z	$y \oplus z$	$x \oplus y$	$x \oplus (y \oplus z)$	$(x \oplus y) \oplus z$
0	0	0	0	0	0	0
0	0	1	1	0	1	1
0	1	0	1	1	1	1
0	1	1	0	1	0	0
1	0	0	0	1	1	1
1	0	1	1	1	0	0
1	1	0	1	0	0	0
1	1	1	0	0	1	1

表 2 のようになるため、この表から $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ は成立する。

3.5　(e)

鍵 k をランダムに作成することによって、その結果作成される暗号文 $t \oplus k$ も完全にランダムなものとなる。そのため、外部の攻撃者からは頻度分析などを利用しても内容文を知り得ることはできないと考えられる。

4　問 4

4.1　(a)

$x \uparrow y$ の式に $y = x$ を代入すると

$$\begin{aligned} x \uparrow x &= \overline{(x \cdot x)} \\ &= \overline{x} \end{aligned} \tag{1}$$

となるため $\overline{x} = x \uparrow x$ は成立する。

4.2　(b)

$$\begin{aligned} x \cdot y &= \overline{\overline{x \cdot y}} \\ &= \overline{x \uparrow y} \\ &= (x \uparrow y) \uparrow (x \uparrow y) \end{aligned} \tag{2}$$

よって $x \cdot y$ は $(x \uparrow y) \uparrow (x \uparrow y)$ と表される。

4.3　(c)

$$\begin{aligned} x + y &= \overline{\overline{x + y}} \\ &= \overline{\overline{x} \cdot \overline{y}} \\ &= \overline{(x \uparrow x) \cdot (y \uparrow y)} \\ &= (x \uparrow x) \uparrow (y \uparrow y) \end{aligned} \tag{3}$$

よって $x + y$ は $(x \uparrow x) \uparrow (y \uparrow y)$ と表される。