情報－Ⅱ

学習指導要領（2）- 知・技 - ア
学習指導要領（3）- 知・技 - ア
学習指導要領（3）- 思・判・表 - ア
学習内容（2）- ア メディアとコミュニケーション
学習内容（3）- ア コンピュータの仕組みと処理

(ア) 文字と2進数(2進法で表された数)の対応付け(符号化)について述べた次の文章の空欄に入るもっとも適切な数字をマークしなさい。

A、B、C、D、Eの5つの文字を2進数に変換して、通信や保存に使うことを考える。たとえば、次のような方式で変換する。

A → 00、B → 01、C → 10、D → 110、E → 111

この方式を用いると、ADCは、0011010という7ビットに変換され、この7ビットから元のADCを一意に復元できる。この場合、元の文字列中の各文字の出現割合によって、変換後の2進数の元の文字1文字あたりの期待されるビット数は変化する。たとえば、A、B、C、D、Eの出現割合が、それぞれ等しかった場合は、出現割合を確率とみてビット数の期待値を計算すれば、ビット数の期待値は2.4ビットになる。

A、B、C、D、Eの出現確率が、それぞれ、

$$0.45, 0.25, 0.16, 0.09, 0.05 \tag{1}$$

だった場合、変換後の1文字あたりのビット数の期待値は、(9).(10)(11)ビットになる。

A、B、C、D、Eの出現確率が、上と異なり、それぞれ、

$$0.05, 0.09, 0.16, 0.25, 0.45 \tag{2}$$

だった場合、変換後の1文字あたりのビット数の期待値は、(12).(13)(14)ビットになり、効率が悪くなる。つまり、ある出現確率が与えられた場合、出現確率の高い文字に短い符号を割り当て、低い文字に長い符号を割り当てたほうが、期待されるビット数が小さくなることがわかる。

また、この出現確率(1)に対して、変換後の1文字あたりのビット数を、(9).(10)(11)ビットよりも小さくすることが可能で、もっとも効率のよい2進数への割り当てを用いた場合、(15).(16)(17)ビットになる。

このような符号を作るためのひとつの考え方は、0で始まるすべての符号と1で始まるすべての符号の出現確率をできるだけ同じにすることであり、さらに、00、01、10、11で始まる符号の出現確率をできるだけ同じにすることであり、より長い符号についても同様の考え方で符号を構成することである。

たとえば、

$$0.25, 0.25, 0.25, 0.125, 0.125$$

という出現確率があった場合、0.125 を二つ組み合わせると、0.25 となって、他の 3 つと等しくなる。そこで、次のような符号を考える。

$$00, 01, 10, 110, 111$$

こうすると、00、01、10、11 で始まる符号の出現確率が同じになり、この 5 つの文字の符号の変換後のビット数の期待値は、2.25 ビットになる。このような割り当てに当てはまらない割り当て方、たとえば、

$$0, 100, 101, 110, 111$$

のように符号を割り当てたとすると、期待値は、2.5 ビットになって 2.25 ビットより大きくなってしまう。この場合、0 で始まる符号の出現確率は、0.25 であるが、1 で始まる符号の出現確率は 0.75 であり、大きく違っているからである。

このような考え方は、文字の種類が増えても同様に適用できる。たとえば、A、B、C、D、E、F、G の 7 つの文字を変換する場合、元の文字列中の各文字の出現確率が次のように与えられたとすると、もっとも効率よい 2 進数への割り当てを用いた場合、変換後の 1 文字あたりのビット数の期待値は、(18). (19)(20) となる。

$$0.33, 0.20, 0.16, 0.11, 0.08, 0.07, 0.05$$

学習指導要領（3）- 知・技 - ア
学習指導要領（3）- 知・技 - イ
学習内容（3）- ア コンピュータの仕組みと処理
学習内容（3）- イ アルゴリズムとプログラム

(イ) 次の文章は、ある暗号方式の原理に関して説明したものである。空欄に入るもっとも適した数字をマークしなさい。

整数から別の整数へ変換する暗号方式を考える。ここで説明する暗号方式では、次のようにして、元の整数 a から、暗号化された整数 b を計算する。ただし、$x \pmod{y}$ は x を y で割った余りを表し、$z \equiv x \pmod{y}$ は x を y で割った余りと z を y で割った余りが等しいことを表している。

(1) 2 つの素数 p, q を選ぶ。

(2) 2 つの素数の積、$n = pq$ を求める。

(3) $(p-1)$ と $(q-1)$ の最小公倍数 L を求める。

(4) L と互いに素な、e $(3 \leqq e \leqq L-1)$ を選ぶ。

(5) $ed \equiv 1 \pmod{L}$ となる d を求める

(6) $a^e \pmod{n}$ を求めて b とする

b から a を得るには次のようにする。

(1) $b^d \pmod{n}$ を求める

したがって、暗号化するには、n, e の組がわかってればよく、復号するには、n, d の組がわかっていればよい。

実際には非常に大きな素数を用いるが、ここでは小さな値、$p = 13$ および $q = 17$ を用いて具体例を示す。まず、$n = 221$ が得られ、$L = 48$ が得られる。$e = 5$ とすると、積 ed を L で割ったときの余りが 1 になる d は (21)(22) である。$e = 11$ の場合は、$d =$ (23)(24) となる。ここでは、$e = 5$ を用いて暗号化する。$a =$ (25)(26)(27) とすると、a の e 乗 (つまり 5 乗) を n で割った余りが b であり、$b = 15$ が得られる。復号するには、b の d 乗を n で割った余りを求めればよく、計算すると、(25)(26)(27) が得られて、a の値になることがわかる。

$a^e \pmod{n}$ の計算は、桁数が多くなり、計算量が多くなるようにみえる。しかしながら、指数部を 2 進数で表現し、下位ビットに相当する部分の余りから順番に計算していく高速に計算できるアルゴリズムが知られており、a^e をそのまま計算する必要はない。