アルゴリズム 58－1
（1997．9．19）

# 情報エントロピーに基づく関数の複雑度解析

中川 晃成

龍谷大学 理工学部 電子情報学科

情報エントロピーを用いて関数の複雑度を評価する方法を確立した。ここで定義した複雑度は「情報複雑度 information complexity」と名付ける。まず、定義を与えた後、この定義が自然であることを示すためのいくつかの簡単な性質を述べる。ここで、Shannonの「相互情報量」の拡張が必要であった。次に、論理関数に対し情報複雑度による評価を適用し、等重率の仮定の下でいくつかの有用な結果の得られることを示す。特に、論理関数の変換群に対して、情報複雑度を用いた不変量の完全系が導入出来ることが予想される。およそすべての情報の変換を伴った操作は「関数」と見なすことが出来る。このような関数に情報エントロピーという明確な意味を持つ量に基礎をおいて複雑度が導入出来たことは、情報処理一般を定量的に評価するための理論的基盤が与えられたことを意味する。

# Complexity Analysis by Information Entropy

Nakagawa Akinari

Ryukoku University, Faculty of Science and Technology

A new method is established that measures the complexity of functions, based upon the information entropy. Thereby, the complexity measure introduced in this paper is termed 'information complexity.' After giving its definition, some simple properties are presented, which properties are considered to represent the 'rationality' of the definition. In it, the mutual information, introduced first by Shannon, is developed so as to treat more than three probability variables. By means of the information complexity, the complexity analysis of Boolean functions is performed, yielding, under the assumption of 'equi-probability,' several valuable results. In particular, it is conjectured that a complete set of invariants under the transformation of Boolean functions can be defined in terms of the information complexity. The manipulation in general that accompanies transformation of information can be regarded as a 'function'; the complexity, defined here to these functions using the information entropy with having definite meaning, supplies the firm theoretical basis to evaluate the process of information manipulation quantitatively.

## 1. はじめに

およそすべての情報の変換を伴った操作は「関数」と見なすことが出来る。即ち、与えられた情報から何らかの情報を取り出す操作は関数と考えて良い。本論文では、Shannonの情報エントロピーに基づき、この様な関数に複雑度を定義することを試みる。これはShannon [1] の導入した「相互情報量」の一つの応用となっている。そこで、ここで導入する複雑度を「情報複雑度 information complexity」と名付ける。以下の定義において、関数は必ずしも「一価」である必要はなく「多価」関数、即ち、確率的関数でも良い。

関数、特に論理関数の複雑度については、計算複雑度、或いは計算論的学習理論の観点から近年活発な研究が行なわれている [2, 3, and references therein]。本論文で与える情報複雑度は、これらとは全く異なる立場から定義したものである。それにもかかわらず、以下に定義する情報複雑度が計算複雑度に対してもその尺度となり得る可能性を示唆すると思われる結果が既に存在する ([4]; **3.2**)。このことは情報複雑度が情報処理一般に対する新しい観点からの寄与をもたらす可能性をも示唆する。

## 2. 定義と性質

情報複雑度の定義にはShannonの相互情報量 [1] を用いるので、相互情報量のときと同じ設定が必要となる。即ち、関数 $y = f(x)$ の独立変数 $x$ と従属変数 $y$ はともに確率分布すると仮定する(以下では $y$ は陽に用いず、$f$ をもってこれに替える)。従って、関数 $f(x)$ は確率変数 $x$ から確率変数 $f$ への確率分布の変換を与えることになる。しかし、逆に、ここで扱う関数は普通の意味の(数学的な意味での一価)関数に限らず、$f(x)$ の値が $x$ の値によって一意に決まらない多価関数(確率的関数)であっても良い。また簡単のため、本論文では離散分布の場合のみを扱う(連続な分布の場合への拡張はもちろん直ちに可能である)。

以下に定義する情報複雑度は、一変数関数ではなく多変数関数の場合や、同じ独立変数を持ついくつかの関数を同時に考える場合に、特別の様相を呈し、それだけにより興味深い結果を示す。

### 2.1 $C_x(f)$

関数 $f(x)$ の情報複雑度 $C_x(f)$ を、

$$C_x(f) = I(F;X) \qquad \text{(定義 1–1)}$$

と定義しようというのが本論文の発想である。これは、$x$ が $f$ に関して持つ情報量(又はその逆)である。

では多変数関数の場合はどう定義すれば良いだろうか。例えば、二変数関数 $f(x,y)$ に対して、変数 $x$ についての $f$ の情報複雑度 $C_x(f)$ を $I(F;X)$ により与えるのは適切ではない。これは、「条件付き相互情報量」を用いて、

$$C_x(f) = I(F;X|Y) \qquad \text{(定義 1–2)}$$

と定義されるべきである。$I(F;X)$ では $f$ の $y$ に関する依存性が $x$ に関する依存性を打ち消してしまうからである(例えば、次節の $f = x \text{ XOR } y$)。ここで、$f$ を何変数の関数と見なすかにより $C_x(f)$ の定義式が異なってくることに注意せよ(定義 1–1 と 1–2)。しかし、この様に定義することで、逆に、何変数の関数と見なしても $C_x(f)$ は同じ値をとる様になる。

$C_x(f)$ は次の不等式を満たす。

$$0 \le C_x(f) \le H(X) \qquad \text{(性質 1)}$$

$C_x(f)$ の正値性は相互情報量としての定義より直ちに出る。右側の不等式は、例えば二変数関数についてなら、$H(X) - C_x(f) = H(X|FY) + I(X;Y) \ge 0$ と変形出来ることより得られる。特に、$f(x,y)$ が $x,y$ の一価関数、即ち、$H(F|XY) = 0$ であるときには、それぞれが等号となるための条件は、

$$C_x(f) = 0 \;\Leftrightarrow\; H(F|Y) = 0$$

$$C_x(f) = H(X) \;\Leftrightarrow\; H(X|FY) = H(F|XY) = I(X;Y) = 0$$

である。これは、前者は $f$ が $y$ のみの(一価)関数であるとき、後者は $x$ と $y$ が互いに独立で、かつ $y$ を与えたとき $f$ と $x$ が一対一対応であるとき、それぞれ成り立つことを意味する。これらの条件は各々の場合に適合した明確な意味を持っており、このことが $C_x(f)$ の定義の正当性を別の面から保証していると考えることも出来る。

### 2.2 $C_{x;y}(f)$

二変数関数 $f(x,y)$ には $C_x(f)$, $C_y(f)$ の他に $C_{xy}(f) = I(F;XY)$ が定義される。そこで、新たな複雑度 $C_{x;y}(f)$ を、

$$C_{x;y}(f) = [C_x(f) + C_y(f)] - C_{xy}(f) \qquad \text{(定義 2)}$$

により定義する。明らかに $C_{x;y}(f)$ は $x$ と $y$ について対称である。

$C_{x;y}(f)$ は次の不等式を満たす。

$$C_{x;y}(f) \le C_x(f) \qquad \text{(性質 2–1)}$$

この不等式は、$C_x(f)-C_{x;y}(f)=C_{xy}(f)-C_y(f)=I(F;X)\geq 0$ より得られる。一方、$C_{x;y}(f)$ の正値性は、$C_x(f)$ などとは異なり、必ずしも成り立たない。しかし、$C_{x;y}(f)=I(X;Y|F)-I(X;Y)$ と書けるから、

$$\text{If } I(X;Y)=0\text{ , then } 0\leq C_{x;y}(f)\text{ .} \qquad \text{(性質 2–2)}$$

が成り立つ。ここで、$I(X;Y)=0$ は $x$ と $y$ が互いに独立であることを意味する。それぞれが等号となるための条件は、

$$\text{Under } I(X;Y)=0\text{ , } C_{x;y}(f)=0 \Leftrightarrow I(X;Y|F)=0$$

$$C_{x;y}(f)=C_x(f) \Leftrightarrow I(F;X)=0$$

である。

二変数関数については、独立変数ごとの複雑度は $C_x(f)$, $C_y(f)$ によって評価するのが当然であろうが、二つの変数を同時に考えたときの複雑度は $C_{xy}(f)$ よりむしろ $C_{x;y}(f)$ で評価するのが適当である。二変数関数 $f(x,y)$ について、「複雑度」の名は、$C_{xy}(f)$ より $C_{x;y}(f)$ にこそふさわしい。

**2.3** $C_x(f;g)$

前節で行なったことの類似が同じ独立変数を持つ二つの関数についても行なえる。即ち、二つの関数 $f(x,y),g(x,y)$ については $C_x(f)$, $C_x(g)$ の他に $C_x(fg)=I(FG;X|Y)$ を用いて、

$$C_x(f;g)=[C_x(f)+C_x(g)]-C_x(fg) \qquad \text{(定義 3)}$$

を定義する。$C_x(f;g)$ は今度は $f$ と $g$ について対称である。

$C_x(f;g)$ は次の不等式を満たす。

$$C_x(f;g)\leq C_x(f) \qquad \text{(性質 3–1)}$$

この不等式は、$C_x(f)-C_x(f;g)=C_x(fg)-C_x(g)=I(F;X|GY)\geq 0$ より得られる。一方、$C_x(f;g)$ の正値性は、再び、必ずしも成り立たない。しかし、$C_x(f;g)=I(F;G|Y)-I(F;G|XY)$ と書けるから、

$$\text{If } I(F;G|XY)=0\text{ , then } 0\leq C_x(f;g)\text{ .} \qquad \text{(性質 3–2)}$$

が成り立つ。ここで、$I(F;G|XY)=0$ は、$x$, $y$ を与えたとき $f$ と $g$ が互いに独立であることを表す($C_x(f;g)$ の正値性の成り立つためのこの条件は $C_{x;y}(f)$ のそれとは異なることに注意せよ)。それぞれが等号となるための条件は、

$$\text{Under } I(F;G|XY)=0\text{ , } C_x(f;g)=0 \Leftrightarrow I(F;G|Y)=0$$

$$C_x(f;g)=C_x(f) \Leftrightarrow I(F;X|GY)=0$$

である。

**2.4** $C_{x;y}(f;g)$

二つの関数 $f$, $g$ が二変数 $x$, $y$ の関数であるときには、**2.2** と **2.3** の考え方を同時に適応して、

$$\begin{aligned} C_{x;y}(f;g)&=[C_{x;y}(f)+C_{x;y}(g)]-C_{x;y}(fg)\\ &=[C_x(f;g)+C_y(f;g)]-C_{xy}(f;g)\end{aligned} \qquad \text{(定義 4)}$$

が定義出来る。この定義が可能でありまた自然であるのは、再右辺の等号が成り立つことによる。$C_{x;y}(f;g)$ は $x$ と $y$、$f$ と $g$ についてそれぞれ対称である。

$C_{x;y}(f;g)$ の正値性については、$I(X;Y)=0$, $I(F;G|XY)=0$ の条件の下では成り立つと思われる(反例は今のところ見い出していない)。しかし、その証明を与えることは出来なかった。また、$C_{x;y}(f;g)$ と、$C_{x;y}(f)$ 或いは $C_x(f;g)$ との大小関係については、**2.2** や **2.3** の場合と異なり、$C_{x;y}(f;g)$ の方が大きくなることも小さくなることもある。

**2.5** いくつかの多変数関数

ここまで行なったことは、当然、三変数以上の関数、或いは共通の独立変数を持つ三つ以上の関数についても適用出来る様に拡張可能である。しかも、その正値性が同様の条件の下で成立する。ここ

では例として、四つの四変数関数の場合にのみ定義を具体的に書き下すと、

$$C_{x;y;z;w}(f) = [C_x(f) + C_y(f) + C_z(f) + C_w(f)] - C_{xyzw}(f) \qquad \text{(定義 2)'}$$

$$C_x(f;g;k;l) = [C_x(f) + C_x(g) + C_x(k) + C_x(l)] - C_x(fgkl) \qquad \text{(定義 3)'}$$

となる。ここで、

$$\begin{aligned} C_{x;y;z;w}(f) &= [C_x(f) + C_y(f) - C_{xy}(f)] + [C_{xy}(f) + C_z(f) - C_{xyz}(f)] \\ &\quad + [C_{xyz}(f) + C_w(f) - C_{xyzw}(f)] \\ &= C_{x;y}(f) + C_{xy;z}(f) + C_{xyz;w}(f) \end{aligned}$$

$$\begin{aligned} C_x(f;g;k;l) &= [C_x(f) + C_x(g) - C_x(fg)] + [C_x(fg) + C_x(k) - C_x(fgk)] \\ &\quad + [C_x(fgk) + C_x(l) - C_x(fgkl)] \\ &= C_x(f;g) + C_x(fg;k) + C_x(fgk;l) \end{aligned}$$

などと変形出来ること(鎖則)は注目して良い。$C_{x;y;z;w}(f;g;k;l)$ なども同様に定義出来る。

正値性については、**B** で新たに定義されている(条件付き)相互情報量の拡張 $I_1$, $I_2$ が必要となる。これらを用いると、

$$C_{x;y;z;w}(f) = I_1(X;Y;Z;W|F) - I_1(X;Y;Z;W)$$

$$C_x(f;g;k;l) = I_2(F;G;K;L|YZW) - I_2(F;G;K;L|XYZW)$$

と書けるから、

$$\text{If } I_1(X;Y;Z;W) = 0 \text{ , then } 0 \le C_{x;y;z;w}(f) \text{ .} \qquad \text{(性質 2–2)'}$$

$$\text{If } I_2(F;G;K;L|XYZW) \text{ , then } 0 \le C_x(f;g;k;l) \text{ .} \qquad \text{(性質 3–2)'}$$

が成り立つことがわかる。

## 3. 論理関数

ここでは例として、情報複雑度により論理関数の複雑度を評価してみよう。前節で述べた様に、論理関数に情報複雑度を定義するためには、その独立変数に何らかの確率分布を導入しなければならない。もちろん、対象とする問題に応じてそれにふさわしい確率分布を導入することが可能である。ここでは、各独立変数はTRUE とFALSE の値を等確率で取るものと仮定する(等重率の仮定)。この仮定の下では、以下に示す様に種々の有用な(もちろん他の場合もそれに応じた)結果が得られる。

### 3.1 $C_{x_i}(f)$

まず、簡単な例を挙げる。前節で与えた定義通りに計算すると、$f$ = TRUE については $C_x(f) = 0$、$f = x$ については $C_x(f) = 1$ となる。$C_x(f)$ は $x$ が $f$ に関して持つ情報量であったことを思い出せば、この結果は良く理解出来る。但し、後者の情報複雑度が 1 であるのは等重率の仮定に由来することに注意せよ。即ち、$0 \le p \le 1$ として確率 $p$ と $1-p$ を持つ二値確率分布のエントロピー $h(p)$

$$h(p) = -p\log p - (1-p)\log(1-p) \qquad (0 \le p \le 1)$$

を用いて、$h(1/2) = 1$ であることが使われている。

では、$f = xy$(積は AND を表す)についてはどうか。直接定義式より計算しても良いが、$y$ = TRUE のとき $f = x$、$y$ = FALSE のとき $f$ = FALSE になることに着目すれば、上の結果から $C_x(f) = (1+0)/2 = 1/2$ であることが推定出来る。この計算方法は、$f$ が $x$, $y$ の一意関数、即ち、$H(F|XY) = 0$ であるとの条件の下では、$C_x(f) = I(F;X|Y) = H(F|Y)$ となることより、正当化される。このことは、一般化すると、$n$ 変数論理関数 $f(x_1, x_2, \ldots, x_n)$ の $C_{x_i}(f)$ が、

$$C_{x_i}(f) = \frac{1}{2^{n-1}} \left[ \begin{array}{c} \textit{the number of assignments of } (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \\ \textit{which makes } f(x_i = \text{FALSE}) \neq f(x_i = \text{TRUE}) \end{array} \right]$$

により、求められることを示している。XOR $\oplus$ による展開 $f = p \oplus (x_i q)$ を用いると、右辺の括弧の中は、さらに *'the number of assignments of* $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ *which makes* $q$ = TRUE'

と書き換えることが出来る。従って、この系として、直ちに、

$0 \le C_{x_i}(f) \le 1$ ; specifically, $C_{x_i}(f) = k/2^{n-1} \quad (k = 0, 1, 2, \ldots, 2^{n-1})$

The number of $n$-variable Boolean functions $f$'s that satisfy $C_{x_i}(f) = k/2^{n-1}$ is given by $2^{2^{n-1}} \times \binom{2^{n-1}}{k}$.

For any $i$'s, $C_{x_i}(f) = 0 \Leftrightarrow f =$ FALSE or TRUE

For any $i$'s, $C_{x_i}(f) = 1 \Leftrightarrow f = x_1 \oplus x_2 \oplus \cdots \oplus x_n$ or its total negation

が得られる。上の第二式は、固定された大きな $n$ について、$C_{x_i}(f)$ の値の分布は、平均 1/2、分散 $1/2^{n+1}$ の Gauss 分布で近似されることを示している。よって、$C_{x_i}(f)$ が 1/2 に近い値を取る $f$ の割合は $n$ とともに指数的に増えてゆく。

### 3.2 Fourier 係数による表現

等重率の仮定の下では、$C_{x_i}(f)$ の値は **C** に与えた Fourier 係数による簡単な表現を持つ。即ち、$n$ 変数論理関数 $f(x_1, x_2, \ldots, x_n)$ について、その Fourier 係数 $f_\xi$ ($\xi \in \{1, -1\}^n$) を用いて、

$$C_{x_i}(f) = \frac{1}{2^{n-1}} \sum_{x\,(x_i=1)} h\left(\frac{1}{2}\left[1 + \sum_{\xi\,(\xi_i=1)} f_\xi \chi_\xi(x)\right]\right) = 1 - \sum_{\xi\,(\xi_i=1)} |f_\xi|^2 = \sum_{\xi\,(\xi_i=-1)} |f_\xi|^2$$

と与えられる (Table 1)。ここで、$\sum_{\xi\,(\xi_i=\pm 1)}$ は $\xi \in \{1, -1\}^n$ のうち $\xi_i = \pm 1$ となるもののみについての和を表す。また、$\sum_{\emptyset} = 0$ と定める。証明には、**3.1** の $C_{x_i}(f)$ についての言葉による表現を Fourier 係数 $f_\xi$ を用いた数学的表現に直し、$\chi_\xi$ の直交性を用いれば良い ( $C_i(f)$ に限らず $C_{x_i x_j}(f)$, $C_{x_i x_j x_k}(f), \ldots$ についても $f_\xi$ により書き下すことが出来るが、$h(p)$ を通して表現したままになる)。さらに、$|\xi|$ を $\xi_i = -1$ を満たす $i$ の数とすれば、上式の $x_i$ についての和として、

$$\sum_{i=1}^{n} C_{x_i}(f) = \sum_{\xi \in \{1,-1\}^n} |\xi| |f_\xi|^2$$

を得る。これは、Linial et al. [4] の Lemma 11 に他ならない。彼らはこの右辺を論理関数 $f(x)$ の独立変数 $x$ についての average sensitivity と呼んだ。本論文では、これが左辺の「各変数ごとの情報複雑度の和」と等しいことを示したのである。即ち、average sensitivity の情報複雑度による新しい特徴付けが出来たことになる。但し、本論文では、単なる和 $\sum_{i=1}^{n} C_{x_i}(f)$ ではなく、**2.5** の

$$C_{x_1;x_2;\ldots;x_n}(f) = \sum_{i=1}^{n} C_{x_i}(f) - C_{x_1 x_2 \cdots x_n}(f) = \sum_{\xi \in \{1,-1\}^n} |\xi| |f_\xi|^2 - h\left(\frac{1 + f_{11\cdots 1}}{2}\right)$$

の方が論理関数の複雑度を評価するための本質的な量であると考える (**2.2**; compare Tables 1 and 3)。

[4] は average sensitivity が論理関数の計算複雑度の尺度となることを示しているから、このことは直ちに本論文の情報複雑度もまたその能力を持つことを意味する。このことはさらに、単に論理関数に対してだけではなく、計算論的学習理論一般についても、情報複雑度の観点からの貢献が可能であることを示唆している。

### 3.3 $C_{x_i;x_j}(f), C_{x_i;x_j;x_k}(f), \ldots$ 不変量の完全系

$n$ 変数論理関数の全体は各変数の否定 ($x_i \leftrightarrow \bar{x}_i$)、及び関数の全否定 ($f \leftrightarrow \bar{f}$) なる変換の下で同値類に分類される (変換群による類別) [5, 6]。各 $C_{x_i}(f)$ の値はこれらの変換の下では不変である (変換の不変量)。もちろん、さらに変数の互換 ($x_i \leftrightarrow x_j$) を許したときには対応する $C_{x_i}(f)$ の値が交換される。その結果、$n$ 次元空間内において、同じ $(C_{x_1}(f), C_{x_2}(f), \ldots, C_{x_n}(f))$ の値を取る論理関数の個数の分布は美しい対称性を成す (Table 2)。但し、その分布を陽に表す表現は今のところ得られていない (各 $C_{x_i}(f)$ のそれについては **3.1** で与えた)。

不変量の組で、その組による類別が変換群による類別と一致するものを、その変換群の「不変量の

完全系」と呼ぶ。$n$ 変数論理関数について定義される $2^n-1$ 個の情報複雑度の組

$$C_{x_1}(f), C_{x_2}(f), \ldots, C_{x_n}(f),\ C_{x_1;x_2}(f), \ldots, C_{x_{n-1};x_n},\ C_{x_1;x_2;x_3}(f),\ \ldots,\ C_{x_1;x_2;\ldots;x_n}(f)$$

は上に述べた論理関数の変換群に対して明らかに不変量となっている。しかも、それらは完全系を成すものと予想される (Table 3)。真理値表における TRUE と FALSE の比として計算される Fourier 係数に基づいて不変量の完全系が定義出来ることが知られている [5, 6]。上に与えた情報複雑度による不変量の組が完全系を成すことが証明出来れば、Fourier 係数によるそれとは全く異なる思想に基づいて不変量の完全系が得られたことになる。情報複雑度による不変量の完全系は、Fourier 係数によるそれに比べると、情報複雑度という明確な意味を持つものから成り立っている点で、より優れている。

## 4. おわりに

本論文では、情報複雑度 information complexity の定義とそれが示す簡単な性質について述べた。あわせて、論理関数の複雑度を情報複雑度により評価し、種々の有用な結果を得た。はじめに述べた様に、およそすべての情報の変換を伴った操作は「関数」と見なすことが出来る。このような関数に情報エントロピーという明確な意味を持つ量に基礎をおいて複雑度が導入出来たことは、情報処理一般を定量的に評価するための理論的基盤が与えられたことを意味する。特に、計算複雑度や計算論的学習理論に対する全く新しい観点からの貢献の可能性について指摘した。

### A. 記法 (エントロピーと相互情報量)

確率変数 $x$ が確率分布 $p(x)$ を持つとき、そのエントロピー $H(X)$ は、

$$H(X) = -\sum_x p(x)\log p(x)$$

で定義される。対数の底はどの様に定めても定数倍することにより相互に変換可能であるので、本論文では論理関数の複雑度に関して述べることもあり、底を 2 に固定する。エントロピーは確率変数ではなく確率分布に対して定義されるものであるが、両者を同一視して上述の記法を用いる。また、$H(X|Y) = H(XY) - H(Y)$ は $y$ の下での $x$ の条件付きエントロピーである。

二つの確率変数 $x$ と $y$ の「相互情報量 $I(X;Y)$」は、

$$I(X;Y) = [H(X)+H(Y)] - H(XY) = \sum_{x,y} p(x,y)\log\frac{p(x,y)}{p(x)p(y)}$$

で定義される。また、三つの確率変数 $x,y,z$ が与えられているとき、$z$ の下での $x$ と $y$ の「条件付き相互情報量 $I(X;Y|Z)$」は、

$$I(X;Y|Z) = [H(X|Z)+H(Y|Z)] - H(XY|Z) = \sum_{x,y,z} p(x,y,z)\log\frac{p(x,y,z)p(z)}{p(x,z)p(y,z)}$$

で定義される。

エントロピー $H(X), H(X|Y)$ や相互情報量 $I(X:Y), I(X:Y|Z)$ の正値性は本文において繰り返し使われる。

### B. 相互情報量の拡張

(条件付き) 相互情報量は二つの確率分布 (変数) 間に定義されていたが、これを三つ以上の確率変数の場合についても拡張することが出来る。しかもこの拡張は以下に示す様に二通りに可能である。ここでは、四つの変数の場合について具体的に書き下す。その他の場合についても容易に類推されるであろう。第一の方法の拡張を $I_1(X;Y;Z;W|F)$、第二のそれを $I_2(F;G;K;L|X)$ と書くと、

$$\begin{aligned} I_1(X;Y;Z;W|F) &= [H(XYZ|F)+H(YZW|F)+H(ZWX|F)+H(WXY|F)] \\ &\quad -3H(XYZW|F) \\ &= I(X;Y|ZWF) + I(XY;Z|WF) + I(XYZ;W|F) \end{aligned}$$

$$I_2(F;G;K;L|X) = [H(F|X) + H(G|X) + H(K|X) + H(L|X)] - H(FGKL|X)$$
$$= I(F;G|X) + I(FG;K|X) + I(FGK;L|X)$$

で定義される。どちらの場合も正値性が成り立つことは、その再右辺の表現(鎖則)より明らかである。$I_1(X;Y;Z;W) = 0$ は $x,y,z,w$ が互いに独立であること、$I_2(F;G;K;L|X) = 0$ は $x$ を与えたとき $f,g,k,l$ が互いに独立であることを表す。

**C. 論理関数の Fourier 変換**

Fourier 変換とはベクトル空間における正規直交基底の変換である。論理関数に Fourier 変換を定義する [6, 7] には、次の様なベクトル空間を導入すれば良い。まず、FALSE を 1、TRUE を $-1$ と同一視する。すると、関数 $f : \{1,-1\}^n \to \mathbf{R}$ は $n$ 変数状態関数を表す。その全体は、通常のスカラー倍とベクトル積により $2^n$ 次元のベクトル空間 $S$ を成す。$n$ 変数論理関数の全体はベクトル空間 $S$ の有限部分空間 ($2^{2^n}$ 個の元から成る) である。

ベクトル空間 $S$ に基底と内積を導入しよう。$\xi = (\xi_1, \xi_2, \ldots, \xi_n) \in \{1,-1\}^n$ に対し、$n$ 変数論理関数 $\chi_\xi(x)$ を、

$$\chi_\xi(x) = \prod_{i\,(\xi_i=-1)} x_i\,, \qquad \text{here } x = (x_1, x_2, \ldots, x_n) \in \{1,-1\}^n$$

により定義する。ここで、$\prod_{i\,(\xi_i=-1)}$ は $i = 1,2,\ldots,n$ のうち $\xi_i = -1$ となるもののみについての積を表す。また、$\prod_\emptyset = 1$ と定める。Boole 定数 $1,-1$ の間の積はXOR を表すから、実は $\chi_\xi(x)$ は parity function である。こうして定義した $\{\chi_\xi(x)\}$ の個数はベクトル空間 $S$ の次元と同じく $2^n$ であり、しかも互いに $\xi$ が異なるとき線形独立であるから、これらはベクトル空間 $S$ の基底となっている。さらに、このベクトル空間 $S$ に、

$$\langle f,g\rangle = \frac{1}{2^n} \sum_{x\in\{1,-1\}^n} f(x)g(x)\,.$$

なる内積を定義する。すると、これは基底 $\{\chi_\xi\}$ を正規直交基底とする内積になっている。即ち、$\langle \chi_\xi, \chi_\eta\rangle = \delta_{\xi\eta}$ を満たす。このことから、状態関数 $f(x)$ に対して Fourier 変換 $f_\xi = \langle f, \chi_\xi\rangle$ とその逆変換

$$f(x) = \sum_{\xi\in\{1,-1\}^n} f_\xi\, \chi_\xi(x)$$

が成り立つことがわかる。特に、$f(x)$ が論理関数であれば、Parseval の等式より $\|f\| \equiv \sqrt{\langle f,f\rangle} = 1$ と、各 $\xi \in \{1,-1\}^n$ について $-1 \le f_\xi \le 1$ が成り立つ (逆は真ならず)。Fourier 係数 $f_\xi$ は、本質的には関数 $f \oplus \chi_\xi$ の真理値表におけるTRUE とFALSE の比に等しく、そのため **3.3** で与えた論理関数の変換群の下で簡便なる変換の性質 (単なる符号の逆転) を示す。

**参考文献**


[1] C. E. Shannon, A mathematical theory of communication, *Bell System Tech. J.*, Vol. 27, pp. 379–423, pp. 623–656 (1948).

[2] J. van Leeuwen (ed.), *Handbook of Theoretical Computer Science*, Elsevier (1990).

[3] M. S. Paterson, *Boolean Function Complexity*, Cambridge Univ. P. (1992).

[4] N. Linial, Y. Mansour, and N. Nisan, Constant depth circuits, Fourier transform, and learnability, *J. ACM*, Vol. 40 (3), 607–620 (1993).

[5] S. W. Golomb, On the classification of Boolean functions, *IRE Trans. Circuit Theory*, Vol. 6, pp. 176–186 (1959).

[6] M. A. Harrison, *Introduction to Switching and Automata Theory*, McGraw-Hill (1965).

[7] J. Ninomiya, A study of the structures of Boolean functions and its application to the synthesis of switching circuits, *Mem. Fac. Engineering, Nagoya Univ.*, Vol. 13 (2), pp. 149–363 (1961).

**Table 1.** Information complexities and Fourier coefficients of some 3-variable Boolean functions.

| $f(x,y,z)^\dagger$ | $f_{1,1,1}$ | $f_{-1,1,1}$ | $f_{1,-1,1}$ | $f_{1,1,-1}$ | $f_{1,-1,-1}$ | $f_{-1,1,-1}$ | $f_{-1,-1,1}$ | $f_{-1,-1,-1}$ | $C_x$ | $C_y$ | $C_z$ | sum$^\ddagger$ | $C_{xyz}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FALSE | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $xyz$ | 3/4 | 1/4 | 1/4 | 1/4 | −1/4 | −1/4 | −1/4 | 1/4 | 1/4 | 1/4 | 1/4 | 3/4 | 0.544 |
| $yz$ | 1/2 | 0 | 1/2 | 1/2 | −1/2 | 0 | 0 | 0 | 0 | 1/2 | 1/2 | 1 | 0.811 |
| $x$ | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| $x(y+z)$ | 1/4 | 3/4 | 1/4 | 1/4 | 1/4 | −1/4 | −1/4 | −1/4 | 3/4 | 1/4 | 1/4 | 5/4 | 0.954 |
| $x(y\oplus z)$ | 1/2 | 1/2 | 0 | 0 | 1/2 | 0 | 0 | −1/2 | 1/2 | 1/2 | 1/2 | 3/2 | 0.811 |
| $xyz+\bar{x}\bar{y}\bar{z}$ | 1/2 | 0 | 0 | 0 | −1/2 | −1/2 | −1/2 | 0 | 1/2 | 1/2 | 1/2 | 3/2 | 0.811 |
| $yz+zx+xy$ | 0 | 1/2 | 1/2 | 1/2 | 0 | 0 | 0 | −1/2 | 1/2 | 1/2 | 1/2 | 3/2 | 1 |
| $xy+\bar{x}z$ | 0 | 0 | 1/2 | 1/2 | 0 | 1/2 | −1/2 | 0 | 1/2 | 1/2 | 1/2 | 3/2 | 1 |
| $xyz+\bar{y}\bar{z}$ | 1/4 | 1/4 | −1/4 | −1/4 | −3/4 | −1/4 | −1/4 | 1/4 | 1/4 | 3/4 | 3/4 | 7/4 | 0.954 |
| $xyz+\bar{x}(\bar{y}+\bar{z})$ | 0 | −1/2 | 0 | 0 | 0 | −1/2 | −1/2 | 1/2 | 1 | 1/2 | 1/2 | 2 | 1 |
| $y\oplus z$ | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 2 | 1 |
| $\bar{x}yz+x\bar{y}z+xy\bar{z}$ | 1/4 | 1/4 | 1/4 | 1/4 | 1/4 | 1/4 | 1/4 | −3/4 | 3/4 | 3/4 | 3/4 | 9/4 | 0.954 |
| $x\oplus y\oplus z$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 3 | 1 |

† In this column, product, sum (+), oplus ($\oplus$), and bar ($\bar{\ }$) denote AND, OR, XOR, and NOT, respectively. ‡ (sum) $= C_x(f) + C_y(f) + C_z(f)$

**Table 2.** Symmetry in the number of 3-variable Boolean functions in the $(C_x, C_y, C_z)$-space.

| number | $(C_x(f), C_y(f), C_z(f))$ |
|---|---|
| 2 | $(0,0,0)$, $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, $(0,1,1)$, $(1,0,1)$, $(1,1,0)$, $(1,1,1)$ |
| 8 | $(0,\frac{1}{2},\frac{1}{2})$, $(\frac{1}{2},0,\frac{1}{2})$, $(\frac{1}{2},\frac{1}{2},0)$, $(1,\frac{1}{2},\frac{1}{2})$, $(\frac{1}{2},1,\frac{1}{2})$, $(\frac{1}{2},\frac{1}{2},1)$ |
| 16 | $(\frac{1}{4},\frac{1}{4},\frac{1}{4})$, $(\frac{3}{4},\frac{1}{4},\frac{1}{4})$, $(\frac{1}{4},\frac{3}{4},\frac{1}{4})$, $(\frac{1}{4},\frac{1}{4},\frac{3}{4})$, $(\frac{1}{4},\frac{3}{4},\frac{3}{4})$, $(\frac{3}{4},\frac{1}{4},\frac{3}{4})$, $(\frac{3}{4},\frac{3}{4},\frac{1}{4})$, $(\frac{3}{4},\frac{3}{4},\frac{3}{4})$ |
| 64 | $(\frac{1}{2},\frac{1}{2},\frac{1}{2})$ |

**Table 3.** Complete set of invariants by information complexities.

| N$^\dagger$ | $f(x,y,z)$ | | $C_x$ | $C_y$ | $C_z$ | $C_{y;z}$ | $C_{z;x}$ | $C_{x;y}$ | $C_{x;y;z}$ |
|---|---|---|---|---|---|---|---|---|---|
| 2 (1·1·2) | FALSE | 00000000 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 (2·3·1) | $x$ | 10101010 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 24(4·3·2) | $yz$ | 11000000 | 0 | 0.5 | 0.5 | 0.189 | 0 | 0 | 0.189 |
| 16(8·1·2) | $xyz$ | 10000000 | 0.25 | 0.25 | 0.25 | 0.094 | 0.094 | 0.094 | 0.206 |
| 48(8·3·2) | $x(y+z)$ | 10101000 | 0.75 | 0.25 | 0.25 | 0.094 | 0.094 | 0.094 | 0.296 |
| 24(8·3·1) | $xy+\bar{x}z$ | 11011000 | 0.5 | 0.5 | 0.5 | 0 | 0.189 | 0.189 | 0.5 |
| 8 (8·1·1) | $yz+zx+xy$ | 11101000 | 0.5 | 0.5 | 0.5 | 0.189 | 0.189 | 0.189 | 0.5 |
| 8 (4·1·2) | $xyz+\bar{x}\bar{y}\bar{z}$ | 10000001 | 0.5 | 0.5 | 0.5 | 0.189 | 0.189 | 0.189 | 0.689 |
| 24(4·3·2) | $x(y\oplus z)$ | 00101000 | 0.5 | 0.5 | 0.5 | 0.5 | 0.189 | 0.189 | 0.689 |
| 48(8·3·2) | $xyz+\bar{y}\bar{z}$ | 10000011 | 0.25 | 0.75 | 0.75 | 0.594 | 0.094 | 0.094 | 0.796 |
| 24(8·3·1) | $xyz+\bar{x}(\bar{y}+\bar{z})$ | 10010101 | 1 | 0.5 | 0.5 | 0.189 | 0.5 | 0.5 | 1 |
| 6 (2·3·1) | $y\oplus z$ | 00111100 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |
| 16(8·1·2) | $\bar{x}yz+x\bar{y}z+xy\bar{z}$ | 01101000 | 0.75 | 0.75 | 0.75 | 0.594 | 0.594 | 0.594 | 1.296 |
| 2 (2·1·1) | $x\oplus y\oplus z$ | 10010110 | 1 | 1 | 1 | 1 | 1 | 1 | 2 |

† The number of Boolean functions belonging to respective equivalent classes.