数学ノート 0001　リード-マラー標準形

近藤友祐 (@elecello_)

初稿：2020 年 6 月 21 日　　更新：2020 年 8 月 27 日
この文書の場所：　https://elecello.com/works.html

命題論理において, **和積標準形 (conjunctive normal form, CNF)** や**積和標準形 (disjunctive normal form, DNF)**—すなわち，任意の命題論理式は $\bigwedge_i \bigvee_j l_{ij}$ や $\bigvee_i \bigwedge_j l_{ij}$ の形に順序などを除き一意的に同値変形できること（ここに各 l_{ij} は命題変数かその否定である）—は有名である[*1].

CNF や DNF と比べるとあまり知られていないであろう標準形として，**リード-マラー標準形 (Reed–Muller normal form)** というものがある．これは命題論理式を，和が排他的論理和，積が論理積であるような “多項式” の形— たとえば “$1 \oplus x_0 \oplus x_1x_2 \oplus x_0x_2x_3$” のような形—に一意的に同値変形したものである（ただし “$\wedge$” は省略した）．排他的論理和や論理積は 2 つの元からなる有限体 $GF(2)$ での加法と乗法に対応するので，線型代数との関係を持ったり，符号理論などの工学方面にも重要だったりするんだろうなと思う．知らんけど．このような代数的側面に注目され，Reed–Muller 標準形は **algebraic normal form (ANF)** との異名をもつ．また **ring sum normal form (RSNF, RNF)**, **Zhegalkin normal form (ZNF)**, **XOR normal form (XNF)** とも呼ばれるらしい．いい加減にしてくれ．

約束：以後，n は正整数を表すものとする[*2]．公理的集合論の慣例に倣って，$n = \{0, 1, 2, \dots, n-1\}$ であるとする．また，$\mathbb{B} := 2 = \{0, 1\}$ と定め，直積 $\mathbb{B}^n$ から $\mathbb{B}$ への関数を n-変数ブール関数と呼ぶ．n-変数ブール関数全体の集合 ${}^{(\mathbb{B}^n)}\mathbb{B}$ を $\mathsf{BooleanFunc}(n)$ と書く．$\mathbb{B}^n$ の元 $\langle b_0, b_1, \dots, b_{n-1}\rangle$ を $\vec{b}$ と略記する．有限集合 S に対し，$|S|$ で S の濃度を表す.

定義 1. n を正整数とする.

1. 各 $I \subseteq n$ について，n-変数ブール関数 $x^I \colon \mathbb{B}^n \to \mathbb{B}$ を次のように定める：

$$x^I(\vec{b}) = 1 \qquad :\Longleftrightarrow \qquad \forall i \in I\,[b_i = 1]. \tag{1}$$

2. 各 $\mathcal{F} \subseteq \mathcal{P}(n)$ について，n-変数ブール関数 $\bigoplus_{I\in\mathcal{F}} x^I \colon \mathbb{B}^n \to \mathbb{B}$ を次のように定める：

$$\left(\bigoplus_{I\in\mathcal{F}} x^I\right)(\vec{b}) = 1 \qquad :\Longleftrightarrow \qquad \left|\left\{ I \in \mathcal{F} \;\middle|\; x^I(\vec{b}) = 1 \right\}\right| \text{ が奇数.} \tag{2}$$

x^I とは “単項式” $\prod_{i\in I} x_i$ が表すブール関数のことである．例として, $n = 334$, $\mathcal{F} = \{\{\}, \{0\}, \{1, 2\}, \{0, 2, 3\}\} \subseteq \mathcal{P}(n)$ に対して，$\bigoplus_{I\in\mathcal{F}} x^I$ というのは “$1 \oplus x_0 \oplus x_1x_2 \oplus x_0x_2x_3$” が表す 334-変数ブール関数のことである.

[*1] どっちがどっちだか紛らわしくてなかなか覚えられない.
[*2] 本稿では $n = 0$ の場合を除外した．もっとも以下の議論に包摂されているとは思うのだが.

定理 2. (リード-マラー標準形，Algebraic Normal Form)　任意の n-変数ブール関数について，そのリード-マラー標準形が存在する．つまり，

$$(\forall n \geqslant 1)(\forall f \in \mathsf{BooleanFunc}(n))(\exists! \mathcal{F} \subseteq \mathcal{P}(n))[f = \bigoplus_{I \in \mathcal{F}} x^I]. \tag{3}$$

証明. n を正整数とする．写像 $\varphi\colon \mathcal{P}(\mathcal{P}(n)) \to \mathsf{BooleanFunc}(n)$ を

$$\varphi\colon \qquad \mathcal{P}(\mathcal{P}(n)) \ni \quad \mathcal{F} \ \mapsto \bigoplus_{I \in \mathcal{F}} x^I \quad \in \mathsf{BooleanFunc}(n) \tag{4}$$

とおくことで定める．以下の Claims 1, 2 で，この φ が全単射であることを示していく．

Claim 1.　φ は単射である（いわば，“異なる多項式は異なるブール関数を表す”）．
$\vdash$ 単射性を示すために，$\mathcal{F}, \mathcal{G} \in \mathcal{P}(\mathcal{P}(n))$ について $\mathcal{F} \neq \mathcal{G}$ が成り立っていると仮定する [want: $\varphi(\mathcal{F}) \neq \varphi(\mathcal{G})$]．いま，$\mathcal{F} \neq \mathcal{G}$ なので，集合族 $\mathcal{D} := (\mathcal{F} \setminus \mathcal{G}) \cup (\mathcal{G} \setminus \mathcal{F})$ [非交和] は空でない．そこで，$\mathcal{D}$ の元のうち濃度が最小のものを 1 つ固定し，それを I^* とおく．対称性により，一般性を失わず，$I^* \in \mathcal{F} \setminus \mathcal{G}$ としてよい．この I^* を用い，$\mathbb{B}^n$ の元 $\vec{b}^*$ を，各 $i < n$ に対し

$$b_i^* = 1 \ :\Longleftrightarrow \ i \in I^* \tag{5}$$

とすることで定める．この定義より，明らかに

$$\forall I \subseteq n \ \left[x^I(\vec{b}^*) = 1 \iff I \subseteq I^*\right] \tag{6}$$

が成り立つ[*3]．

今ほしい $\varphi(\mathcal{F}) \neq \varphi(\mathcal{G})$ を示すためには，$\varphi(\mathcal{F})(\vec{b}^*) \neq \varphi(\mathcal{G})(\vec{b}^*)$，つまり $\left(\bigoplus_{I \in \mathcal{F}} x^I\right)(\vec{b}^*) \neq \left(\bigoplus_{I \in \mathcal{G}} x^I\right)(\vec{b}^*)$ を示せばよい．そのためには集合

$$\mathcal{F}' := \left\{ I \in \mathcal{F} \;\middle|\; x^I(\vec{b}^*) = 1 \right\}, \qquad \mathcal{G}' := \left\{ I \in \mathcal{G} \;\middle|\; x^I(\vec{b}^*) = 1 \right\} \tag{7}$$

の濃度の偶奇が異なることを示せばよい．**以下これを示す．**

まず，式 (6) より

$$\mathcal{F}' := \{ I \in \mathcal{F} \mid I \subseteq I^* \}, \qquad \mathcal{G}' := \{ I \in \mathcal{G} \mid I \subseteq I^* \} \tag{8}$$

である．

$$\mathcal{H} := \{ I \in \mathcal{F} \cap \mathcal{G} \mid I \subseteq I^* \} \tag{9}$$

と定めることで，$\mathcal{F}', \mathcal{G}'$ は

$$\mathcal{F}' := \{ I \in \mathcal{F} \setminus \mathcal{G} \mid I \subseteq I^* \} \cup \mathcal{H} \quad \text{[非交和]}, \qquad \mathcal{G}' := \{ I \in \mathcal{G} \setminus \mathcal{F} \mid I \subseteq I^* \} \cup \mathcal{H} \quad \text{[非交和]} \tag{10}$$

と分割できる．

[*3] (∵) 任意の $I \subseteq n$ に対し，$x^I(\vec{b}^*) = 1 \iff \forall i \in I\,[b_i^* = 1] \iff \forall i \in I\,[i \in I^*] \iff I \subseteq I^*$.

Subclaim 1-1. $\{I \in \mathcal{F} \setminus \mathcal{G} \mid I \subseteq I^*\} = \{I^*\}$.

$\vdash\vdash$ "$\supseteq$": I^* は，その定め方より $\mathcal{F} \setminus \mathcal{G}$ の元である．また $I^* \subseteq I^*$ は自明． "$\subseteq$": $I \in \mathcal{F} \setminus \mathcal{G}$ で $I \subseteq I^*$ をみたす I を勝手にとる．$|I| \leqslant |I^*|$ である．$\mathcal{F} \setminus \mathcal{G} \subseteq \mathcal{D}$ なので $I \in \mathcal{D}$ であり，I^* は，その定め方より $\mathcal{D}$ の要素のうち濃度が最小のものであった．したがって $|I| \geqslant |I^*|$ である．合わせて $|I| = |I^*|$ である．$I \subseteq I^*$ で I, I^* は有限だったので $I = I^*$ である． $\dashv\dashv$(Subclaim 1-1.)

Subclaim 1-2. $\{I \in \mathcal{G} \setminus \mathcal{F} \mid I \subseteq I^*\} = \varnothing$.

$\vdash\vdash$ $I \in \mathcal{G} \setminus \mathcal{F}$ かつ $I \subseteq I^*$ であるような集合 I が存在したとして矛盾を導く．まず $|I| \leqslant |I^*|$ である．次に $\mathcal{G} \setminus \mathcal{F} \subseteq \mathcal{D}$ なので $I \in \mathcal{D}$ であり，I^* は，その定め方より $\mathcal{D}$ の要素のうち濃度が最小のものであった．したがって $|I| \geqslant |I^*|$ である．合わせて $|I| = |I^*|$ である．$I \subseteq I^*$ で I, I^* は有限だったので $I = I^*$ である．よって $\mathcal{G} \setminus \mathcal{F} \ni I = I^* \in \mathcal{F} \setminus \mathcal{G}$ となるが，$\mathcal{G} \setminus \mathcal{F}$ と $\mathcal{F} \setminus \mathcal{G}$ は交わらないので，これは矛盾である． $\dashv\dashv$(Subclaim 1-2.)

Subclaims 1-1, 1-2 より

$$\mathcal{F}' = \{I^*\} \cup \mathcal{H} \text{ [非交和]}, \qquad \mathcal{G}' = \varnothing \cup \mathcal{H} = \mathcal{H} \tag{11}$$

がわかった．よって $\mathcal{F}'$ と $\mathcal{G}'$ の濃度の偶奇は異なる．**これが示すべきことであった．** $\dashv$(Claim 1.)

Claim 2. φ は全射である（いわば，"どんなブール関数に対しても，それを表す多項式が存在する"）．

$\vdash$ 一般に，濃度が等しい**有限**集合の間に単射があれば，それは全射でもある．さて，$|\mathrm{dom}(\varphi)| = |\mathcal{P}(\mathcal{P}(n))| = 2^{2^n}$ であり，$|\mathrm{cod}(\varphi)| = |\mathsf{BooleanFunc}(n)| = \left|{}^{(\mathbb{B}^n)}\mathbb{B}\right| = 2^{2^n}$ であるから $|\mathrm{dom}(\varphi)| = |\mathrm{cod}(\varphi)|$ である．Claim 1 より φ は単射なので，上に述べたことより φ は全射である． $\dashv$(Claim 2.)

定理の証明に戻る．$f \in \mathsf{BooleanFunc}(n)$ を任意にとる．$f = \bigoplus_{I \in \mathcal{F}} x^I$ であるような $\mathcal{F}$ が唯一存在することを示せばよい．

存在： $\mathcal{F} := \varphi^{-1}(f)$ と定めよ (Claims 1, 2 により φ には逆写像が存在することに注意せよ)．すると $f = \varphi(\varphi^{-1}(f)) = \varphi(\mathcal{F}) = \bigoplus_{I \in \mathcal{F}} x^I$ である．

唯一性： $\mathcal{G} \in \mathcal{P}(\mathcal{P}(n))$ が $f = \bigoplus_{I \in \mathcal{G}} x^I$ を満たしているとする．すると $\varphi(\mathcal{G}) = \bigoplus_{I \in \mathcal{G}} x^I = f = \bigoplus_{I \in \mathcal{F}} x^I = \varphi(\mathcal{F})$ となる．φ は単射だったので $\mathcal{G} = \mathcal{F}$ である．

以上で定理 2 が示された． □

注意 3. 定理 2 の証明における $\varphi^{-1}\colon \mathsf{BooleanFunc}(n) \to \mathcal{P}(\mathcal{P}(n))$ は，いわば真理値表を受け取ってそのリード-マラー標準形を返す関数である．ところが，定理 2 の証明では，Claim 2 を見ればわかる通り，$\varphi^{-1}(f)$ を具体的にどのように計算するかについては全く分析していない．つまり，真理値表からリード-マラー標準形を作る具体的なアルゴリズムを与えたわけではない．そのようなアルゴリズムを模索するのはまた別の話であり，おそらく計算複雑性とかいろいろな話が関連してくるのだと思う．

参考文献

[1] Wikipedia contributors, 'Algebraic normal form', *Wikipedia, The Free Encyclopedia*, 4 May 2020, 21:00 UTC, `https://en.wikipedia.org/w/index.php?title=Algebraic_normal_form&oldid=954893840` [accessed 21 June 2020].