数理解析研究所講究録
第 786 巻 1992 年 110-113

ブール多項式環上のグレブナー基底

佐藤 洋祐
(財) 新世代コンピュータ技術開発機構

1 概説

Buchberger によって考案されたグレブナー基底は可環体上の多項式環のイデアルに関する計算において多大の効力を発揮する. 筆者らはこれを変形しブール環上の多項式環によって表現されたブール方程式を解く方法を考案した. 本稿はこれについて解説する.

2 ブーリアン・グレブナー基底

ブール代数 $\langle \mathbf{B}, \vee, \wedge, \neg, 0, 1 \rangle$ に対し

$$x + y =_{\mathrm{def}} (x \wedge \neg y) \vee (\neg x \wedge y),\ x \cdot y =_{\mathrm{def}} x \wedge y$$

と定義すると, $\langle \mathbf{B}, +, \cdot, 0, 1 \rangle$ は単位元 1 を持つ可換環になる. この環は次の 2 つの性質を持つ.

1. 任意の $\mathbf{B}$ の元 x について $x \cdot x = x$ である.

2. 任意の $\mathbf{B}$ の元 x について $x + x = 0$ である.

逆に単位元 1 を持つ可換環がこの 2 つの性質を持てば

$$x \vee y =_{\mathrm{def}} x + y + x \cdot y,\ x \wedge y =_{\mathrm{def}} x \cdot y,\ \neg x =_{\mathrm{def}} 1 + x$$

によって $\vee, \wedge, \neg$ を定義することでブール代数になる.
従って上の 2 性質を持つ単位元をもつ可換環はブール代数と同一視できる. このような環を**ブール環**と呼ぶ. ブール環 $\mathbf{B}$ 上の元を係数に持ち各変数の次数が 1 以下の多項式を**ブール多項式**と呼ぶ. 各変数 X に対し $X \cdot X = X$ と置くことによってブール多項式全体もまたブール環になるが, これを**ブール多項式環**と呼ぶ. ブール多項式の単項、すなわち含まれる変数がすべて異なる単項を**ブール単項**と呼び, $\alpha, \beta, \gamma, \ldots$ で表す. 単項上の順序 $\geq$ が以下の性質を持つとき**アドミシブル**な順序と呼ばれる.

1. 変数の集合として $\alpha \supseteq \beta$ なら $\alpha \geq \beta$ である.

2. $\alpha \geq \beta$ ならどんな単項 γ に対しても $\alpha\gamma \geq \beta\gamma$ である.

単項上のアドミシブルな全順序は辞書式順序に基づくもの全次数に基づくものなど色々考えられるが以下においてはそのような順序 $\geq$ を一つ固定し多項式の最大単項というときはいつもこの順序によるものとする. 最大単項として α を持つブール多項式を $a\alpha \oplus \phi$ のように表す. このブール多項式による書き換え $\Rightarrow_{a\alpha\oplus\phi}$ を次のように定義する. ブール多項式 $\varphi = \psi + b\alpha\beta$ に対し $ab \neq 0$ なら $\varphi \Rightarrow_{a\alpha\oplus\phi} \varphi'$. ここで φ' は $\psi + b(1 + a)\alpha\beta + ab\beta\phi$ で与えられるブール多項式である. この書き換えが妥当なものであることは以下のように説明される. まず $b\alpha\beta = b(1 + a)\alpha\beta + ba\alpha\beta$ に注意する. 次に $a\alpha \oplus \phi = 0$ から $a\alpha = \phi$ がいえる. この両辺に $ab\beta$ をかけて $ba\alpha\beta = ba\beta\phi$ が得られる. したがって $a\alpha \oplus \phi = 0$ のもとで $b\alpha\beta = b(1 + a)\alpha\beta + ab\beta\phi$ がいえる.

ブール多項式の集合 R に対し $\phi \Rightarrow_\varphi \psi$ なる R の元 φ が存在するとき $\phi \Rightarrow_R \psi$ と記す. また $\Rightarrow_R$ の反射推移閉包を $\stackrel{*}{\Rightarrow}_R$ で表す. つまり $\phi \stackrel{*}{\Rightarrow}_R \psi$ は 0 回以上有限回で ϕ を ψ に書き換えられることを表す.

定理 2.1　どんなブール多項式の有限集合 R に対しても $\Rightarrow_R$ は停止性をもつ. つまり $\phi_0 \Rightarrow_R \phi_1 \Rightarrow_R \phi_2 \Rightarrow_R \cdots$ と無限に続く書き換えは存在しない.

定義 2.2　I をブール多項式環の有限生成イデアルとする. 有限個のブール多項式 G が以下の性質を満たすとき G は I のブーリアン・グレブナー基底と呼ばれる.

1. $G \subseteq I$
2. $f \equiv g \pmod I$ (すなわち $f+g \in I$) ならばあるブール多項式 h が存在して $f \Rightarrow_G h$, $g \Rightarrow_G h$ が成り立つ.
3. G の元は相互に書き換えられることがない. つまりどんな $g \in G$ も g 以外の G の元 g' による書き換え $\Rightarrow_{g'}$ によって書き換えることはできない.
4. G の元の最大単項は各々異なる.

文献によっては Gröbner base の定義に条件 3 を含めないことも多い. しかし次の性質 2.3 の 3 をいうために必要なので本稿では条件 3 を要求する.
また通常の Gröbner base の場合条件 4 は条件 3 からの論理的帰結であるが, ブーリアン・グレブナー基底の場合性質 3 をいうためには条件 4 も必要になる.

性質 2.3　上で定義した ブーリアン・グレブナー基底 は次の性質を持つ.

1. I の ブーリアン・グレブナー基底 G が生成するイデアルは I である.
2. I によって与えられる制約すなわち連立方程式
   $\{f = 0 \mid f \in I\}$ が解を持たないことと I の
   ブーリアン・グレブナー基底 が B の元すなわち定数だけからなるブール多項式を含むことが同値になる.
3. I の ブーリアン・グレブナー基底 G は一意に定まる. 従って G を I によって与えられる制約の標準形とみなすことができる.

ブーリアン・グレブナー基底 を求める Algorithm を述べるのに必要な定義をいくつか与える. ブール多項式 $a\alpha \oplus \phi$ に対し, $a\phi + \phi$ をその**係数自己要対** (coefficient self-critical pair) と呼び $csc(a\alpha \oplus \phi)$ で表す. また α の中の任意の変数 X に対し, $X\phi + \phi$ をその**変数自己要対** (variable self-critical pair) と呼ぶ. ブール多項式 $a\alpha\gamma \oplus \phi, b\beta\gamma \oplus \psi$ に対し, $b\beta\phi + a\alpha\psi$ をその**要対** (critical pair) と呼ぶ. ただしここで $ab \neq 0, \gamma \neq 1$, α と β は共通の変数を含まないものとする. 例えば $aXYZ \oplus bYW$ の係数自己要対は $(ab+b)YW$, 変数自己要対は
$bXYW + bYW$ と $bYZW + bYW$ である. またブール多項式 $aXYZ \oplus bZ$ と $cXZW \oplus Y$ の要対は $aY + bcZW$ である. ただしここで $ac \neq 0$ とする. ブール多項式の有限集合 R とブール多項式 ϕ に対し, R の元と ϕ でつくられる要対と ϕ の変数自己要対のすべての集合を $CP(\phi, R)$ で表す.

ブール多項式の有限集合 R に対し R に含まれるブール多項式で最大単項が等しいものを足しあわせたブール多項式全体からなる集合を $Glue(R)$ で表す.
すなわち $\{a_1\alpha \oplus \phi_1, \ldots, a_n\alpha \oplus \phi_n\}$ を R の中の最大単項が α のブール多項式の集合とすると, $Glue(R)$ は, $a_1\alpha \oplus \phi_1, \ldots, a_n\alpha \oplus \phi_n$ 全ての代わりに $(a_1 + \ldots + a_n)\alpha \oplus (\phi_1 + \ldots + \phi_n)$ を含む. 例えば
$R = \{aXY \oplus X, bXY \oplus Y, bXZ \oplus X, XZ \oplus Z\}$
とするとき,
$Glue(R) = \{(a+b)XY \oplus (X+Y), (b+1)XZ \oplus (X+Z)\}$

である.

ブール多項式の集合 R とブール多項式 ϕ に対し $\phi\downarrow_R$ は $\Rightarrow_R$ による ϕ の既約形の一つを表す.

Algorithm3.1 与えられたブール多項式の有限集合 E_0 に対し, それから生成されるイデアルの ブーリアン・グレブナー基底 を求めるアルゴリズムは以下のように与えられる.

input $E \leftarrow E_0, R \leftarrow \emptyset$
while $E \neq \emptyset$
  choose $\phi \in E$ and $\phi' \leftarrow \phi\downarrow_R$ ……(イ)
 if $\phi' \neq 0$ **then** $E \leftarrow (E - \{\phi\}) \cup \{csc(\phi')\}$
   for every $a\alpha \oplus \psi \in R$
    if $a\alpha \Rightarrow_{\phi'} \varphi$
    then
    $E \leftarrow E \cup \{\varphi + \psi\}, R \leftarrow R - \{a\alpha \oplus \psi\}$
    else
    $R \leftarrow (R - \{a\alpha \oplus \psi\}) \cup \{a\alpha \oplus (\psi\downarrow_{R\cup\{\phi'\}})\}$
    end-if
   end-for
   $E \leftarrow E \cup CP(\phi', R), R \leftarrow R \cup \{\phi'\}$
  else $E \leftarrow (E - \{\phi\})$
  end-if
end-while
output $Glue(R)$ ……(ロ)

(ロ)で出力される $Glue(R)$ が求める ブーリアン・グレブナー基底 である. (イ)における E の元の選択は公平でなければいけない. すなわち E のどの元もどこかで選ばれねばならない.

3 重要性質

最後に延長可能定理と汎用性定理について述べる. これらは通常のグレブナー基底にはないブーリアン・グレブナー基底特有の重要性質である.

定理 3.1 延長可能定理
ブール多項式の有限集合 E に含まれる変数 $\bar{X} = X_1, X_2, \ldots, X_k$, $\bar{Y} = Y_1, Y_2, \ldots, Y_l$ にたいしどの X_i についても $X_i \geq Y_1 Y_2 \cdots Y_l$ となるアドミシブル順序 $\geq$ をとる.
この順序の下での ブーリアン・グレブナー基底 は一般に

$$\{f_1(\bar{X}, \bar{Y}), \ldots, f_m(\bar{X}, \bar{Y}), g_1(\bar{Y}), \ldots, g_n(\bar{Y})\}$$

の形をとるが, $\{g_1(\bar{Y}) = 0, \ldots, g_n(\bar{Y}) = 0\}$ が解 $\bar{Y} = \bar{a}$ をもつとき, これを $\{f = 0 | f \in E\}$ の解に延長することができる. すなわち $\{f_1(\bar{X}, \bar{a}), \ldots, f_m(\bar{X}, \bar{a})\}$ が解をもつ.

変数 $\bar{Z} = Z_1, \ldots, Z_m$ からなるブール多項式環を $\mathbf{B}(\bar{Z})$ と記すことにする. ブール多項式環 $\mathbf{B}(\bar{X}, \bar{Y})$ は変数 $\bar{Y}$ からなるブール環 $\mathbf{B}(\bar{X})$ 上のブール多項式環 $(\mathbf{B}(\bar{X}))(\bar{Y})$ とみなすことができる.

定理 3.2 汎用性定理
$G = \{g_1\alpha_1 \oplus t_1, \ldots, g_k\alpha_k \oplus t_k\}$ をブール多項式環 $(\mathbf{B}(\bar{X}))(\bar{Y})$ における有限生成イデアル I のブーリアン・グレブナー基底とする。このとき変数 $\bar{X}$ への $\mathbf{B}$ の元の代入 θ に対して $G\theta = \{(g_i\theta)\alpha_i \oplus (t_i\theta) | g_i\theta \neq 0\}$ と

おくとき$G\theta$はまたブール多項式環$\mathbf{B}(\bar{Y})$のイデアル$I\theta$のブーリアン・グレブナー基底になる。このときさらに任意のブール多項式$f \in \mathbf{B}(\bar{X},\bar{Y})$に対して$(f\theta)\downarrow_{G\theta} = (f\downarrow_G)\theta$が成り立つ.

参考文献

[1] B.Buchberger, Gröbner Bases: an Algorithmic
method in Polynomial Ideal Theory, Technical Report, CAMP-LINZ, 1983.

[2] K.Sakai,Y.Sato,S.Menju, Boolean Gröbner bases(revised)
ICOT Technical Report, 1990.

[3] Y.Sato, K.Sakai, Zero-point theorem for Boolean polynomial ring
ICOT Technical Report, 1990.