数理解析研究所講究録
第1652巻 2009年 182-191

ブール多項式環における消去イデアルの計算について

永井 彰
AKIRA NAGAI
東京理科大学 理学研究科
TOKYO UNIVERSITY OF SCIENCE*

井上 秀太郎
SHUTARO INOUE
東京理科大学 理学研究科
TOKYO UNIVERSITY OF SCIENCE †

佐藤 洋祐
YOSUKE SATO
東京理科大学
TOKYO UNIVERSITY OF SCIENCE ‡

1 はじめに

グレブナー基底 (Gröbner basis) は代数方程式を解く強力なツールになっている. B.Buchberger は係数が体における多項式環にグレブナー基底を導入したが, 係数が体でない環におけるグレブナー基底についても多くの研究がある. その中の1つとして係数をブール環とする多項式環上のグレブナー基底 (Boolean Gröbner basis) が Sakai, K と Sato, Y によってブール方程式を解くために導入され, 非常に優れた特性をもっている. 以下では簡単のために, $\bar{X} = X_1, \ldots, X_n, \bar{A} = A_1, \ldots, A_m$ と表すことにする.

ブール多項式環 $B(\bar{X}, \bar{A})$ 上における消去イデアル (elimination ideal) とは, 与えられたイデアル $I \subset B(\bar{X}, \bar{A})$ に対して, $I \cap B(\bar{A})$ で定義される $B(\bar{A})$ のイデアルである. 消去イデアルを計算するには, 大きく分けて2つの方法がある. 1つは, (純) 辞書式順序 $X_1 > \ldots > X_n > A_1 > \ldots > A_m$ やブロック順序 $\bar{X} >> \bar{A}$ のもとでブーリアン・グレブナー基底を計算する素朴な方法であり, もう1つは, $\bar{A}$ をパラメータとして包括的ブーリアン・グレブナー基底を計算し, そこから消去イデアルを構成する方法である. 包括的ブーリアン・グレブナー基底を計算する方法としては, 変数 $\bar{X}, \bar{A}$ に対してブロック順序 $\bar{X} >> \bar{A}$ のもとでブーリアン・グレブナー基底を計算する方法と, 変数 $\bar{A}$ からなる係数ブール環 $B(\bar{A})$ をもつブール多項式環 $(B(\bar{A}))(\bar{X})$ 上でブーリアン・グレブナー基底を計算する方法がある. 一般的に, 後者は前者よりも理論的に優れているが, 計算効率が悪くメモリの消費も大きいため, 前者よりも効果は期待できない.

本研究では, 後者を求めるアルゴリズムの改良として, ブール多項式環 $B(\bar{A}, \bar{X})$ 上において与えられたイデアル $I = \langle f_1(\bar{A}, \bar{X}), \ldots, f_l(\bar{A}, \bar{X}) \rangle$ に対し, 変数 $\bar{A}$ に0, 1のビット列 $\bar{c}$ を宛がうことで, イデアル全体ではなく $\bar{X}$ のみからなるブール多項式環 $B(\bar{X})$ 上のイデアル $\langle f_1(\bar{c}, \bar{X}), \ldots, f_l(\bar{c}, \bar{X}) \rangle$ のブーリアン・グレブナー基底を計算し, そこから消去イデアル $I \cap B(\bar{A})$ を構成できる新しい方法を提唱した. また, 数式処理システム RISA/ASIR を用いてこのアルゴリズムを実装し, その有効性を示した.

*nagai@mi.kagu.tus.ac.jp
†inoue@mi.kagu.tus.ac.jp
‡ysato@mi.kagu.tus.ac.jp

2 ブール多項式環

定義 1
単位元 1 をもつ可換環 B が以下の性質を持つとき，これをブール環とよぶ.

$$\forall x \in B \quad x^2 = x$$

上の性質から次の性質もすぐに示される.

$$\forall x \in B \quad x + x = 0$$

証明 $x+x=(x+x)^2=x^2+x^2+x^2+x^2=x+x+x+x$ となり，$x+x=x+x+x+x$ の両辺から $x+x$ をひく. ∎

このように，ブール環上では $x=-x$ なので $-$ 記号を使う必要はないが，$-$ の意味を強調したいときには $-$ を用いることにする. また，ブール環の半順序を表すために記号 $\succeq$ を用いる. 例えば，ブール環 B の要素 a,b に対して，$a \succeq b$ は $ab=b$ を意味する。ブール環の例を以下に挙げる.

例 1
$B=\mathbb{GF}_2$ とすると，B はブール環となる.

例 2
$B=\mathbb{GF}_2 \times \mathbb{GF}_2$ とすると，B はブール環となる.

一般的に B の k 個の直積 B^k はブール環になる.

例 3
B をブール環，k を自然数とする. 直積 B^k は B の要素を取り出して k 個からなる組を元とした集合である. B^k の要素 p にたいして，$p_i \in B$ を p の i 番目 $(i=1,\ldots,k)$ の要素を表すのに用いることにする. $p,q \in B^k$ にたいして，和と積の演算 $p+q, p\cdot q$ を $(p+q)_i = p_i+q_i, p_i\cdot q_i (i=1,\ldots,k)$ で定義することによって，B^k はブール環になる.

例 4
集合の族は以下の演算でブール環になる.
$x,y \in B$ とし，$+$ と $\cdot$ を次のように定義する.
$x+y=(\bar{x}\cap y)\cup(x\cap\bar{y})$, $x\cdot y = x\cap y, 1+x=\bar{x}$. ここで,$\bar{x}$ は x の補集合を表す.

定義 2
ブール環 B の 0 でない要素 e が以下の性質を満たすとき，e はアトミックであるとよぶ. (アトミックな要素は $\succeq$ に関して，0 でない最小の要素である.)

$$c=e \text{ の場合を除き}, ce=c \text{ となる } 0 \text{ でない要素 } c \text{ が存在しない.}$$

補題 3
B を有限ブール環とし，B が少なくとも 1 つのアトミックな要素を持っているとする. このとき，B のすべてのアトミックな要素 $e_1,\ldots,e_k$ に対して，$e_ie_j=0 (i\neq j)$ と $e_1+e_2+\ldots+e_k=1$ が成り立つ.

証明 $e_ie_j=0$ は自明. 最後の等式を示す. $e_1+\ldots+e_k\neq 1$ とする. つまり，$e_1+\ldots+e_k+1\neq 0$ とする. 今 c を $e_1+\ldots+e_k+1 \succeq c$ を満たす B の最小要素（アトミックな要素）とすると，$c(e_1+\ldots+e_k+1)=c$. これは，$c(e_1+\ldots+e_k)=0$ を意味する. c が最小要素（アトミックな要素）であるので，ある e_i に対して $c=e_i$ となり，$e_i(e_1+\ldots+e_k)=0$ より $e_i=0$ が導かれ e_i の定義に矛盾する. ∎

定義 4
Bをブール環とする．イデアル$\langle X_1^2-X_1,\ldots,X_n^2-X_n\rangle$による剰余環$B[X_1,\ldots,X_n]/\langle X_1^2-X_1,\ldots,X_n^2-X_n\rangle$はブール環になる．この剰余環をブール多項式環 *(boolean polynomial ring)* とよび，$B(X_1,\ldots,X_n)$と表記する．また，ブール多項式環の要素をブール多項式とよぶ．

ブール多項式環は，一般の体とは異なる性質をもつ．ブール多項式環における任意のイデアルは主イデアル (*principal ideal*) になる．つまり，$\langle f_1,f_2\ldots,f_n\rangle=\langle f_1\cup f_2\cup\ldots\cup f_n\rangle$となる．$\supseteq$は明らかである．$\subseteq$については，$f_i=f_i\cdot(f_1\cup f_2\cup\ldots\cup f_n)$である．このように，ブール多項式環におけるすべてのイデアルは1つの多項式で生成されるイデアルと一致する．

例 5
$\langle X,Y\rangle=\langle XY+X+Y\rangle=\langle X\cup Y\rangle$

$B(X_1,\ldots,X_n)$のブール多項式は，各変数X_iをベキ等にした$B[X_1,\ldots,X_n]$の多項式によって一意的に表現される．$X_1,\ldots,X_n$と$Y_1,\ldots,Y_m$をそれぞれ$\bar{X},\bar{Y}$と表すことにする．また，単項を表す記号としてギリシャ文字α,β,γ等を，ブール環Bの要素を表す記号としてa,b,c等を，あるnに対してBのn組の要素を$\bar{a}$で表す。例えば，$\bar{a}=(a_1,\ldots,a_n),\bar{b}=(b_1,\ldots,b_m)$とし，$(\bar{a},\bar{b})$は$n+m$組の要素からなる$(a_1,\ldots,a_n,b_1,\ldots,b_m)$となる．変数$\bar{X}$と$\bar{Y}$からなるブール多項式に対して，$f(\bar{a},\bar{Y})$は$\bar{X}$に$\bar{a}$を代入した$B(\bar{Y})$上のブール多項式を意味する．

3 ブーリアン・グレブナー基底

ブーリアン・グレブナー基底は係数ブール環上の多項式環におけるグレブナー基底から計算可能である．このセクションでは前半は$B[\bar{X}]$上のグレブナー基底について説明し，後半部分で，$B(\bar{X})$上のグレブナー基底（ブーリアン・グレブナー基底）を説明する．また，$B[X_1,\ldots,X_n](B[\bar{X}])$の多項式に対して，最大の単項を$LT(f)$，その係数を$LC(f)$，最大の単項式すなわち$LC(f)LT(f)$を$LM(f)$，$f-LM(f)$を$Rd(f)$で表す．さらに$LT(F)$と$LM(F)$を集合$\{LT(f)\mid f\in F\}$と$\{LM(f)\mid f\in F\}$（$F$は$B[\bar{X}]$の部分集合），$T(\bar{X})$を変数$\bar{X}$からなる単項を表すために用いる．

定義 5
多項式環$B[\bar{X}]$のイデアルIに対して，Iの有限部分集合Gが$\langle LM(I)\rangle=\langle LM(G)\rangle$を満たすとき，$G$を$I$のグレブナー基底とよぶ．

定義 6
$f\in B[\bar{X}]$に対して，$a=LC(f),t=LT(f),h=Rd(f)$とする．fによるモノミアル・リダクション$\rightarrow_f$を以下で定義する．

$$bts+p\rightarrow_f(1-a)bts+absh+p.$$

注：*(bts+p)-((1-a)bts+absh+p)=bs(af)* である．

sは$T(\bar{X})$の単項，bは$ab\neq 0$を満たすBの要素，pは$B[\bar{X}]$の任意の多項式の場合，集合$F\subseteq B[\bar{X}]$にたいして，$g\rightarrow_F g'\Leftrightarrow$ある$f\in F$にたいして$g\rightarrow_f g'$

定理 7
Fが有限で，$\rightarrow_F$がネーター的であるとき，各$i=1,2....$にたいして，$g_i\rightarrow_F g_{i+1}$をみたす多項式の無限列$g_1,g_2,\ldots$は存在しない．

定理 8
I を多項式環 $B[\bar{X}]$ のイデアルとする. I の有限部分集合 G が I のグレブナー基底であることと, $\forall h \in I \xrightarrow{*}_G 0$ は同値である.

定義 9
グレブナー基底 G にたいし, G の任意の要素 f が自分以外の G の要素によるモノミアルリダクションによって書き換えられないとき, G を既約グレブナー基底とよぶ.

例 6
$B = \mathbb{GF}_2 \times \mathbb{GF}_2$ とする. 多項式環 $B[X]$ で, $\{(1,0)X, (0,1)X\}$ と $\{(1,1)X\}$ は同じイデアルの既約グレブナー基底である.

グレブナー基底を一意に求めるために, もう一つ定義を導入する.

定義 10
既約グレブナー基底 G がさらに以下の性質をもつとき G を正規グレブナー基底とよぶ.
・G の二つの要素で、最大単項が一致するものはない.

定理 11
正規グレブナー基底はユニークに定まる. すなわち, $\langle G \rangle = \langle G' \rangle$ なる正規グレブナー基底 G と G' は一致しなければならない.

上の例において, $\{(1,1)X\}$ は正規グレブナー基底であるが, もう一方は正規グレブナー基底ではない.

定義 12
多項式 f が, $LC(f)f = f$ をみたすとき, f はブール閉であるという. $lc(f)f$ を f のブール閉包とよび, $bc(f)$ で表す. (注意 任意の多項式のブール閉包はブール閉である.)

定理 13
G をイデアル I のグレブナー基底とする. このとき, $\{bc(g) \mid g \in G\} \setminus \{0\}$ もまた I のグレブナー基底となる.

体上の多項式環と同様に S 多項式を定義する.

定義 14
$a = LC(f), b = LC(g), tr = LT(f), sr = LT(g)$ とし, $GCD(t,s) = 1$ をみたす単項 t, s, r にたいして, 多項式 f, g を $f = atr + f'$ $g = bsr + g'$ とする. つまり, t と s は共通の変数をもっていない. 多項式 $bsf + atg = bsf' + atg'$ は f と g の S 多項式 ($S - polynomial$) とよび, $S(f,g)$ で表す.

体上の多項式環と同様に次の定理はグレブナー基底の計算に非常に重要である.

定理 15
G をブール閉である多項式の有限集合とする. このとき G がブーリアン・グレブナー基底であることは, 任意の多項式 f, $g \in G$ にたいして $S(f, g) \xrightarrow{*}_G 0$ が成り立つことと一致する.

与えられた有限集合 F にたいして, ブール閉包と S 多項式を計算することで, $\langle F \rangle$ のグレブナー基底を計算することができる. また, グレブナー基底から正規グレブナー基底を求めることは容易である.

アルゴリズム 1

BC

input:$B[\bar{X}]$ の有限部分集合 F

output:$\langle F' \rangle = \langle F \rangle$ をみたすブール閉な多項式の集合 F'

$F' \leftarrow \emptyset$

while $F \neq \emptyset$ *do*

  select f *from* F

  $F \leftarrow F \setminus \{f\}$

  while $f \neq 0$ *do*

    $F' \leftarrow F' \cup \{bc(f)\}$

    $f \leftarrow f - bc(f)$

  end

end

アルゴリズム 2

BGbasis

input:$B[\bar{X}]$ の有限部分集合 F と，$T(\bar{X})$ の項順序 $>$

*output:*項順序 $>$における $\langle F \rangle$ のグレブナー基底 G

$G \leftarrow BC(F)$

$B \leftarrow \{\{g_i, g_j\} \mid g_i, g_j \in G \; with g_i \neq g_j\}$

while $B \neq \emptyset$ *do*

  select $\{g_i, g_j\}$ *from* B

  $B \leftarrow B \setminus \{\{g_i, g_j\}\}$

  $S(g_i, g_j) \xrightarrow{*}_G h$

  if $h \neq 0$ *then*

    $B \leftarrow B \cup \{\{g, h\} \mid \forall g \in G\}$

    $G \leftarrow G \cup BC(\{h\})$

end

ここからはブール多項式環におけるグレブナー基底（ブーリアン・グレブナー基底）の説明に入る．読者は $B[\bar{X}]$ と $B(\bar{X})$ で混乱しないように注意されたし．ブール環の要素はすべてベキ等なので，ブール多項式環においても上のアルゴリズムは機能する．ブール多項式環においてもグレブナー基底を定義できる．各 l_i が 0 か 1 であるならば，項 $X_1^{l_1} \ldots X_n^{l_n}$ はブール単項 (*boolean power product*) という．変数 $\bar{X}$ からなるすべてのブール単項の集合を $BT(\bar{X})$ で表す．$B(\bar{X})$ 上のブール多項式 $f(\bar{X})$ は以下のようにユニークに表現できる．B の要素 $b_1, \ldots, b_k$ と異なるブール単項 $t_1, \ldots, t_k$ を用いて，$f(\bar{X}) = b_1 t_1 + \ldots + b_k t_k$ と一意表現できる．$b_1 t_1 + \ldots + b_k t_k$ を $f(\bar{X})$ の標準表現 (*canonical representation*) とよぶ．$BT(\bar{X})$ は $T(\bar{X})$ の部分集合なので，$T(\bar{X})$ 上の項順序 $\geq$ は，$BT(\bar{X})$ 上でも同様に定義できる．与えられた項順序 $\geq$ におけるブール多項式 $f = b_1 t_1 + \ldots + b_k t_k$ にたいして，$t_1, \ldots, t_k$ のなかの最大ブール単項 t_i を f の先頭ブール単項とよび，$BLT(f)$ で表し，$b_i t_i$ を f の先頭ブール単項式とよび，記号 $BLM(f)$ を用いる．b_i は f の先頭ブール係数とよび $BLC(f)$ で，$f - BLM(f)$ を $BRd(f)$ で表すことにする．また，ブール多項式の集合 F にたいして同じ表記 $BLT(F)$ と $BLM(F)$ を用いることにする．

定義 16
ブール多項式環 $B(\bar{X})$ のイデアル I にたいして，I の有限部分集合 G が $\langle BLM(I)\rangle = \langle BLM(G)\rangle$ を満たすとき，G を I のブーリアン・グレブナー基底とよぶ．

定理 17
I をブール多項式環 $B(\bar{X})$ のイデアルとする．I の有限部分集合 G が I のブーリアン・グレブナー基底であることと，$\forall h \in I \xrightarrow{*}_G 0$ は同値である．

ブール多項式環のブール閉包も同様に定義できる．

定義 18
(ブール閉) 多項式 f が，$BLC(f)f = f$ をみたすとき，f はブール閉 (*boolean closed*) であるという．$BLC(f)f$ を f のブール閉包 (*boolean closure*) とよび，$bc(f)$ で表す．である．

定理 19
G を I のブーリアン・グレブナー基底とする．このとき，$\{bc(g) \mid g \in G\} \setminus \{0\}$ もまた I のブーリアン・グレブナー基底となる．

定義 5.5 のように，ある項順序においてユニークに定まる正規ブーリアン・グレブナー基底を定義できる．ブーリアン・グレブナー基底の計算はいたってシンプルである．ブール多項式の有限集合 $F \subseteq B(\bar{X})$ が与えられたとする．$B[\bar{X}]$ においてイデアル $\langle F \cup \{X_1^2 - X_1, \ldots, X_n^2 - X_n\}\rangle$ のグレブナー基底 G を計算する．$G \setminus \{X_1^2 - X_1, \ldots, X_n^2 - X_n\}$ が $B(\bar{X})$ における $\langle F\rangle$ のブーリアン・グレブナー基底である．また，G が正規グレブナー基底であるとき，$G \setminus \{X_1^2 - X_1, \ldots, X_n^2 - X_n\}$ もまた正規ブーリアン・グレブナー基底である．

B をブール環，k を自然数とすると，直積 B^k はブール環になる．B^k の要素 p にたいして，$p_i \in B$ を p の i 番目 $(i = 1, \ldots, k)$ の要素を表すのに用いることにする．$B^k[\bar{X}]$ 上の多項式 $f(\bar{X})$ にたいして，$f_i (i = 1, \ldots, k)$ を f の係数 p を p_i に置き換えることにより得られる $B[\bar{X}]$ 上の多項式とし，$B^k(\bar{X})$ 上の多項式にたいしても $f(\bar{X})$ を同様に定義する．

定理 20
多項式環 $B^k[\bar{X}]$ において，G をブール閉な多項式の有限集合とする．このとき，G が I の (既約) グレブナー基底であることと，$i = 1, \ldots, k$ にたいして $G_i = \{g_i \mid g \in G\} \setminus \{0\}$ が $I_i = \{f_i \mid f \in I\} (\subseteq B[\bar{X}])$ の (既約) グレブナーであることは同値である．

系 21
ブール多項式環 $B^k(\bar{X})$ において，G をブール閉なブール多項式の有限集合とする．このとき，G が I の (既約) グレブナー基底であることと，$i = 1, \ldots, k$ にたいして $G_i = \{g_i \mid g \in G\} \setminus \{0\}$ が $I_i = \{f_i \mid f \in I\} (\subseteq B(\bar{X}))$ の (既約) グレブナーであることは同値である．

4 包括的ブーリアン・グレブナー基底

このセクションでは，包括的ブーリアン・グレブナー基底を計算する素朴な方法を紹介する．以下では簡単のために，$\bar{X} = X_1, \ldots, X_n, \bar{A} = A_1, \ldots, A_m$ と表すことにする．また，$T(\bar{X})$ 上に項順序が与えられているものとする．

定義 22
$F=\{f_1(\bar{A},\bar{X}),\ldots,f_l(\bar{A},\bar{X})\}$ がブール多項式環 $B(\bar{A},\bar{X})$ の有限部分集合であるとする．$B(\bar{A},\bar{X})$ の有限部分集合 $G=\{g_1(\bar{A},\bar{X}),\ldots,g_k(\bar{A},\bar{X})\}$ が F の包括的ブーリアン・グレブナー基底であるとは，B の拡大ブール環 B' の任意の要素 $\bar{a}$ にたいして，$G(\bar{a})=\{g_1(\bar{a},\bar{X}),\ldots,g_k(\bar{a},\bar{X})\}\backslash\{0\}$ が $\langle F(\bar{a})\rangle=\langle f_1(\bar{a},\bar{X}),\ldots,f_l(\bar{a},\bar{X})\rangle\subseteq B'(\bar{X})$ のブーリアン・グレブナー基底になっていることをいう．ここで，B' は B を部分環とするブール環と $\bar{a}=(a_1,\ldots,a_m)\in B'^m$ である．また，任意の $\bar{a}=(a_1,\ldots,a_m)\in B'^m$ にたいして，$G(\bar{a})$ が正規ブーリアン・グレブナー基底であるとき G を正規包括的ブーリアン・グレブナー基底とよぶ．

定理 23
$F=\{f_1(\bar{A},\bar{X}),\ldots,f_l(\bar{A},\bar{X})\}$ がブール多項式環 $B(\bar{A},\bar{X})$ の有限部分集合であるとする．$B(\bar{A},\bar{X})$ をブール環 $B(\bar{A})$ を係数にもつ多項式環 $(B(\bar{A}))(\bar{X})$ とみなし，$G=\{g_1(\bar{A},\bar{X}),\ldots,g_k(\bar{A},\bar{X})\}$ が $(B(\bar{A}))(\bar{X})$ におけるイデアル $\langle F\rangle$ の（正規）ブーリアン・グレブナー基底になっているとする．このとき，G は F の（正規）包括的ブーリアン・グレブナー基底になる．

5 消去イデアルを求める新しいアルゴリズム

$B(\bar{X})$ 上のブール多項式 $f_1(\bar{X}),f_2(\bar{X}),\ldots,f_l(\bar{X})$ を生成元とするイデアル $I=\langle f_1(\bar{X}),f_2(\bar{X}),\ldots,f_l(\bar{X})\rangle$ の正規ブーリアン・グレブナー基底を計算することによって以下の連立方程式を解くことができる．

$$\begin{cases} f_1(X_1,X_2,\ldots,X_n)=0 \\ \qquad\vdots \qquad\qquad\qquad \cdots \quad (1) \\ f_l(X_1,X_2,\ldots,X_n)=0 \end{cases}$$

他にも正規ブーリアン・グレブナー基底を計算することで多くのことを解決できる．例としてはイデアル所属問題があり，与えられたブール多項式 $h(\bar{X})$ とイデアル I にたいして $h(\bar{X})\in I$ であるか否かを判定できる．

今の場合では，$\langle f_1(\bar{X}),f_2(\bar{X}),\ldots,f_l(\bar{X})\rangle$ と $\langle f_1(\bar{X}),f_2(\bar{X}),\ldots,f_l(\bar{X}),h(\bar{X})\rangle$ の正規ブーリアン・グレブナー基底をそれぞれ計算して両者を比較し一致するかをみればよい．もしくは $h(\bar{X})$ の正規形 (*normal form*) を求めればよく，I の正規ブーリアン・グレブナー G を計算して $h(\bar{X})\xrightarrow{*}_G 0$ であるか否かをみればよい．また $h(\bar{X})$ が (1) のすべての解で 0 になるかどうかも今の方法で確かめることができる．他の問題についても正規ブーリアン・グレブナーを計算することさえできれば，その問題を解くができる．しかし残念ながら，変数が多い場合グレブナー基底の計算は困難である．今，(1) の 3 変数 X_1,X_2,X_3 だけの解を知りたいとする．このとき，消去イデアル $\langle f_1(\bar{X}),f_2(\bar{X}),\ldots,f_l(\bar{X})\rangle\cap B(X_1,X_2,X_3)$ のブーリアン・グレブナー基底が必要であり，イデアル I 全体のブーリアン・グレブナー基底は必ずしも必要ではない．また，3 変数 X_1,X_2,X_3 からなる多項式 $h(X_1,X_2,X_3)$ が (1) の解で 0 になるかの判定に必要なものも，イデアル I 全体のブーリアン・グレブナー基底ではなく，上の消去イデアルのブーリアン・グレブナー基底が必要である．消去イデアルを求める一般的な方法は（純）辞書式順序 $X_n>\ldots>X_4>X_3>X_2>X_1$ やブロック順序 $X_n,\ldots,X_4>>X_3,X_2,X_1$ のもとでイデアル全体のブーリアン・グレブナー基底を計算することである．

このセクションでは，イデアル全体のブーリアン・グレブナー基底を計算せずに，消去イデアルのブーリアン・グレブナー基底を計算するアルゴリズムを説明する．

補題 24
I を変数 $\bar{A}$ と $\bar{X}$ からなるブール多項式環 $B(\bar{A},\bar{X})$ のイデアルとし G を $T(\bar{X})$ のある項順序のもと，$(B(\bar{A})(\bar{X}))$ における I の正規ブーリアン・グレブナー基底とする．このとき，$G\cap B(\bar{A})$ は空集合か $B(\bar{A})$ のブール多項式 1 つからなる集合 $\{h(\bar{A})\}$ である．後者の場合，消去イデアル $I\cap B(\bar{A})$ は $\langle h(\bar{A})\rangle$ と一致し，そうでない場合は消去イデアルは $\{0\}$ となる．

補題 25

ブール多項式環 $B(A_1,\ldots,A_m)$ は直積 B^{2^m} と同型である. $B(A_1,\ldots,A_m)$ から B^{2^m} への同型写像 ϕ は $i=1,\ldots,2^m$ と $i-1$ の 2 進数表現 $c_1^i\ldots c_m^i$ を用いて次のように与えられる.

$$\phi(f(A_1,\ldots,A_m))_i = f(c_1^i,\ldots,c_m^i) = a_i$$

ϕ の逆写像 ϕ^{-1} は

$$\phi^{-1}((a_1,a_2,\ldots,a_{2^m})) = \sum_{i=1}^{2^m} a_i(A_1+c_1^i+1)(A_2+c_2^i+1)\cdots(A_m+c_m^i+1)$$

となる. ($c_k^i=0$ のとき $c_k^i+1=1$ となり, $c_k^i=1$ のとき $c_k^i+1=0$ となる)

この補題と系 5.13 によって新しいアルゴリズムを記述できる.

アルゴリズム 3

ElimBGB

input: $B(\bar{A},\bar{X})$ の有限部分集合 F, パラメーター $\bar{A}$, $T(\bar{A})$ の項順序 $>$

output: 項順序 $>$ における消去イデアル $\langle F\rangle \cap B(\bar{A})$ のグレブナー基底 G

$F' \leftarrow \{\phi(f) \mid f \in F\}$

$i \leftarrow 1$

while $i \leq 2^m$ *do*

　項順序 $>$ における $F_i' = \{f_i \in B(\bar{A}) \mid f \in F'\}$ の正規ブーリアン・グレブナー基底

　G_i を計算

　if $G_i \cap B \neq \emptyset$ *then* $b_i \leftarrow G_i \cap B$ の要素

　else $b_i \leftarrow 0$

　$i \leftarrow i+1$

end

$G \leftarrow \langle \phi^{-1}((b_1,b_2,\ldots,b_{2^m})) \rangle$ のブーリアン・グレブナー基底

アルゴリズム中の ϕ は補題 7.2 で定義された同型写像の拡張として得られた $(B(A_1,\ldots,A_m))(\bar{X})$ から $B^{2^m}(\bar{X})$ への同型写像である.

例 7

$F = \{f_1(\bar{X}), f_2(\bar{X}), \ldots, f_{18}(\bar{X})\}$

$f_1(\bar{X}) = X_1X_3X_{18} + \{d,p\}X_4X_{18}X_{20} + X_{11}X_{13} + \{a,d\}X_6X_{10} + X_5X_{18} + X_4,$

$f_2(\bar{X}) = X_2X_5 + X_4X_5 + \{k,q\}X_6X_8 + X_1X_{26}X_{27} + \{c,k\}X_4X_8 + X_{10} + X_6X_{10},$

$f_3(\bar{X}) = X_1X_2X_4 + X_3X_5X_{10} + \{d,i\}X_{11} + X_1 + X_5 + X_{12}X_{24}X_{28},$

$f_4(\bar{X}) = X_2X_4 + \{e,g\}X_3X_4 + X_1X_{12} + X_{12}X_{15} + X_5X_{10}X_{12} + X_3X_{11},$

$f_5(\bar{X}) = X_1X_3 + X_1X_5 + \{j,l\}X_2X_5X_{16} + X_{11}X_{12} + X_{11}X_{23} + X_{16} + 1,$

$f_6(\bar{X}) = X_6X_{17} + X_5X_9X_{30} + \{a,c\}X_8X_{10} + X_1X_{12} + X_{25}X_{29},$

$f_7(\bar{X}) = X_1X_{11} + X_{12} + X_2X_8 + X_3X_{11}X_{12} + X_{11}X_{12} + X_4X_6 + \{b,e\},$

$f_8(\bar{X}) = X_2 + X_4X_7 + \{c,f\}X_{12}X_{17}X_{21} + X_2X_3X_{12} + X_6X_7 + X_{12} + X_4X_{25} + X_1X_{11},$

$f_9(\bar{X}) = X_3 + X_3X_4 + \{k,m\}X_1X_3 + X_5X_6 + \{h,i\}X_7X_{24},$

$f_{10}(\bar{X}) = X_1 + \{g,i\}X_4X_5X_{11} + \{m,r\}X_1X_9X_{11} + X_2X_6 + X_{11} + 1,$

$f_{11}(\bar{X}) = X_3X_{20} + X_5 + X_5X_7 + X_{11} + \{l,o,s\}X_{13}X_{30} + X_{11}X_{18}X_{23},$

$f_{12}(\bar{X}) = X_3X_{14} + \{f,n,t\}X_1X_2 + X_2 + X_{11} + X_{11}X_{15} + X_{19}X_{22}$,
$f_{13}(\bar{X}) = X_2X_7 + \{f,j\}X_{11} + X_2X_3 + X_{11}X_{12} + X_9X_{13} + X_{13}$,
$f_{14}(\bar{X}) = X_3X_7 + X_8 + \{d,o\}X_8X_{13} + \{c,t\}X_2X_{23} + X_3X_{20}X_{22} + 1$,
$f_{15}(\bar{X}) = X_4X_9 + X_7X_{20} + \{b,l\}X_8X_{19} + X_{20}$,
$f_{16}(\bar{X}) = \{a,e,n\}X_7X_9 + X_3X_5 + X_6X_{22} + \{e,r\}X_{18}X_{29} + X_{19}X_{21}$,
$f_{17}(\bar{X}) = X_3 + X_{14} + X_{17}X_{18} + X_3X_4X_{19}$,
$f_{18}(\bar{X}) = X_7 + X_7X_{21} + X_{23}X_{24}\}$

$B(X_1,X_2,X_3)$ から B^8への同型写像 ϕ は $\phi(f(X_1,X_2,X_3) = (f(0,0,0), f(0,0,1), f(0,1,0), f(0,1,1), f(1,0,0), f(1,0,1), f(1,1,0), f(1,1,1))$ となる．今の場合 F_i' は以下のとおり．

$$F_1' = \{f_1(0,0,0,X_4,\ldots,X_{30}),\ldots,f_{18}(0,0,0,X_4,\ldots,X_{30})\}$$
$$F_2' = \{f_1(0,0,1,X_4,\ldots,X_{30}),\ldots,f_{18}(0,0,1,X_4,\ldots,X_{30})\}$$
$$\vdots$$
$$F_8' = \{f_1(1,1,1,X_4,\ldots,X_{30}),\ldots,f_{18}(1,1,1,X_4,\ldots,X_{30})\}$$

F_i' の正規ブーリアン・グレブナー基底を計算すると，
$b_1 = 0, b_2 = \{i\}, b_3 = \{k,q\}, b_4 = 0, b_5 = 0, b_6 = 0, b_7 = 0, b_8 = 0$
$\phi^{-1}((0,\{i\},\{k,q\},0,0,0,0)) = \{i\}(X_1+1)(X_2+1)X_3 + \{k,q\}(X_1+1)X_2(X_3+1)$

求めたかった正規ブーリアン・グレブナー基底は，
$G = \{\{i,k,q\}X_1X_2X_3 + \{i,k,q\}X_2X_3 + \{i\}X_1X_3 + \{i\}X_3 + \{k,q\}X_1X_2 + \{k,q\}X_2\}$

実装は，数式処理システム RISA/ASIR を用いた．計算時間については 1.6GHZ Intel Core Duo CPU と 2560MB の SDRAM の PC を用いて 160 秒であった．X_1,X_2,X_3 をパラメータとする包括的ブーリアン・グレブナー基底の計算に 2 時間費やしても計算は終わらなかった．また，辞書式順序などでブーリアン・グレブナー基底を計算してもこれも 2 時間では計算が止まらなかった．

この消去イデアルを求める新しいアルゴリズムは $T(\bar{X})$ に適切な項順序を与えることで，他の消去イデアルを計算できる．たとえば，b_i の代わりに $G_i \cap B(X_4,X_5)$ と (純) 辞書式順序 $X_n > \ldots > X_6 > X_5 > X_4$ を用いて，消去イデアル $\langle F\rangle \cap B(X_1,\ldots,X_5)$ を計算することが可能である．このときのブーリアン・グレブナー基底は $G = \{\{s,b,i,k,c,e,f,t,m,l\}X_3X_4X_5 + \{i\}X_4X_5 + \{s,b,k,c,e,f,t,m,l\}X_3X_5$
$+ \{s,b,i,k,c,e,f,t,m,l\}X_3X_4 + \{i\}X_4 + \{s,b,i,k,c,e,f,t,m,l\},$
$\{o\}X_5X_4 + \{o\}X_3X_5 + \{o\}X_4 + \{o\}X_3,$
$(1 + \{s,b,i,k,c,h,e,f,t,m,l\})X_3X_4 + (1 + \{s,b,i,k,c,h,e,f,t,m,l\})X_3\}$
となる．

6 結論

ElimBG が計算しているものは，$\bar{A}$をパラメータとする $\langle F\rangle$ の包括的ブーリアン・グレブナー基底である．実際パラメータの値は 0,1 だけでなく，B のすべての要素が考えられる．前のセクションを例に用いると，各パラメータ X_1,X_2,X_3の値は $\{a,b,c,\ldots,s,t\}$ の部分集合とそれらの補集合の可能性がある．つまり，$(2^{21})^3 = 2^{63}$もの代入がありえるが，このアルゴリズムでは 0,1 の代入を 8 通り調べるだけでよい．また，このアルゴリズムは 2^m個のブーリアン・グレブナー基底を計算する必要があるので，m がある程度小

さいときに有効であることがわかる．今後の課題としては，分散計算を実装することでより効率的に消去イデアルを求めることがあげられる．

参 考 文 献

[1] Buchberger,B.(1965).Ein Algorithms zum Auffinden der Basiselemente des Restklassenrings bach einem nulldimensionalen Polynomial.Doctoral Dissertation Math. Inst.University of Innsbruck, Austria.

[2] Kapur,D.(1995).An Approach for Solving Systems of Parametric Polynomial Equations. in Principles and Practices of Constraint Programming.(eds. Saraswat and Van Hentenryck),MIT Press, 217-244.

[3] Menju, S., Sakai, K., Sato,Y. and Aiba,A.(1993).A Study on Boolean Constraint Solvers. Constraint Logic Programming Selected Research The MIT Press, pp253-267.

[4] Montes, A.(2002) A new algorithm for discussing Gröbner bases with parameters. J.Symb. Comp. 33/2, 183-208.

[5] Manubens, M. and Montes,A. (2006).Improving DISPGB algorithm using the discriminant ideal. J.Symb. Comp. 41, 1245-1263.

[6] Rudeanu, S. Boolean functions and equations. North-Holland Publishing Co., Amsterdam-London;American Elsevier Publishing Co., Inc., New York, 1974.

[7] Sakai,K. and Sato, Y.(1988).Boolean Gröbner bases. ICOT Technical Momorandum 488.

[8] Sakai,K. and Sato, Y. and Menju, S. (1991). Boolean Gröbner bases(revised). ICOT Technical Report 613.

[9] Sato,Y.(1996).Set Constraint Solvers(Prolog Virsion). http://www.icot.or.jp/ARCHIVE/Museum/FUNDING/funding-96-E.html

[10] Sato,Y.(1998).Set Constraint Solvers(KLIC Virsion). http://www.icot.or.jp/ARCHIVE/Museum/FUNDING/funding-98-E.html

[11] Sato,Y.(1998).A new type of canonical Groebner bases in polynomial rings over Von Neumann regular rings. Proceedings of ISSAC 1998,ACM Press,317-32

[12] Sato,Y. and Inoue,S.On the Construction of Comprehensive Boolean Gröbner Bases. Proceedings of the Seventh Asian Symposium on Computer Mathematics(ASCM 2005),pp 145-148,2005.

[13] Suzuki, A and Sato, Y.(2003). An Alternative approach to Comprehensive Gröbner Bases . J. Symb. Comp. 36/3-4, 649-667.

[14] Suzuki, A and Sato, Y.(2006). A Simple Algorithm to Compute Comprehensive Gröbner Bases Using Gröbner Bases. International Symposium on Symbolic and Algebraic Computation (ISSAC 2006),Proceedings, 326-331.

[15] Weispfenning,V.(1989).Gröbner Bases in polynomial ideals over commmutative regular rings. In Davenport Ed,editer,EUROCAL'87,336-347.Springer LNCS 378

[16] Weispfenning,V.(1992). Comorehensive Gröbner Bases,J.Symbolic Computation(1992) 14,1-29