ブーリアン・グレブナー基底の Syzygy 基底による特徴付け

佐藤洋祐[†] 毛受哲[††] 相場亮[†††]

ブール多項式環すなわちブール環上の多項式環におけるグレブナー基底を構成するため，文献 6) では多項式によるリダクションをブール環固有の性質を用いて定義し，これに基づいて定義されたグレブナー基底(ブーリアン・グレブナー基底) を求めるアルゴリズムを与えた．このアルゴリズムでは通常のグレブナー基底を求めるときに必要なS多項式の計算の他に，自己C多項式と呼ばれる独自の多項式の計算が必要である．本稿ではブーリアン・グレブナー基底が syzygy 基底を用いて特徴付けられることを示す．これにより自己C多項式の果たす役割が明らかになるとともに，ブーリアン・グレブナー基底の計算における不要なS多項式の除去の方法が与えられる．

Characterization of Boolean Gröbner Bases by Syzygy Bases

YOSUKE SATO,[†] SATOSHI MENJU[††] and AKIRA AIBA[†††]

A special polynomial reduction is induced in Ref. 6) using the own properties of Boolean ring. It enables us to define and construct Gröbner bases in Boolean polynomial ring (Boolean Gröbner bases). The algorithm presented there requires calculation of so-called self-critical-polynomials in addition to standard s-polynomials. In this paper, we show that Boolean Gröbner bases are characterized in terms of syzygy bases. It enables us to show that self-critical-polynomials are s-polynomials of special kinds. We also give a criterion to detect redundant s-polynomials in the algorithm of construction of Boolean Gröbner bases.

1. はじめに

Buchberger によって導入されたグレブナー基底[1]は多項式環のイデアルに関する多くの問題において多大な効力を発揮する．しかしながら，係数環が体でないとき，多項式によるリダクションが簡単に定義できないため，グレブナー基底を単純に定義することはできない．体ではない係数環におけるグレブナー基底についていろいろな研究がなされているが，特に係数環が単位元をもつ可換環であるとき，弱グレブナー基底と呼ばれるものがグレブナー基底の一般化として重要である．係数環がネーター環でいくつかの計算可能性に関する条件を満たすとき，syzygy 基底の計算によって弱グレブナー基底を計算することが可能である．しかしながらこの syzygy 基底の計算のアルゴリズムは非常に遅い．係数環がさらに単項イデアル整域である場合，文献 4) では体上の多項式環における Taylor レブグ基底弱を基底に類似の簡単な syzygy 使ってナー基底を計算するアルゴリズムが与えられ，さらに文献 3) と同様な方法で不要なS多項式を除去する方法が与えられている．

文献 6) でわれわれは，係数環がブール環という特殊な多項式環（ブール多項式環）においてブール環固有の性質を使って多項式によるリダクションを定義し，これを用いて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）を定義した．また通常のS多項式のほかに自己C多項式なるものを導入し，これらを計算することによってブーリアン・グレブナー基底が Buchberger のアルゴリズムと同様な方法で与えられることを示した．本稿ではブーリアン・グレブナー基底が実は弱グレブナー基底であり，したがって syzygy 基底を用いて特徴付けられることを示す．これにより，自己C多項式が実はS多項式の一種であることが明らかになるとともに，ブーリアン・グレブナー基底の計算における不要なS多項式の除去方法が与えられる．

以下では，まず2章でブーリアン・グレブナー基底について概説を与え，文献 4) から本稿で引用する結果を述べる．3章でブーリアン・グレブナー基底の syzygy 基底による特徴付けとそれから導かれる主要

† 立命館大学理工学部情報工学科
Department of Computer Science and System Engineering, Ritsumeikan University
†† 日本電気(株)C&Cシステム研究所システム基礎研究部
NEC C&C System Laboratory
††† (財)新世代コンピュータ技術開発機構
Institute for New Generation Computer Technology

結果を述べ，最後に4章でブーリアン・グレブナー基底を求めるアルゴリズムにおいて不要なS多項式の除去方法がどのくらい有効か調べたわれわれの実験結果を与える．

2. 準　　備

2.1 ブーリアン・グレブナー基底

単位元1を持つ可換環$\mathbf{B}$は，すべての元がベキ等元になるとき，すなわち

$\forall a\in\mathbf{B}\quad a^2=a.$

をみたすとき，**ブール環**と呼ばれ，次の性質を持つ．

$\forall a\in\mathbf{B}\quad a+a=0.$

以下では，与えられたブール環$\mathbf{B}$を係数環とする多項式環 $\mathbf{B}[X_1, X_2, \cdots, X_n]$ を考える．$\mathbf{B}$ の要素を表す文字として $a, b, c, \cdots$ を，$X_1, X_2, \cdots, X_n$ からなる項を表す文字として $\alpha, \beta, \gamma, \cdots$ を使う．

項上の全順序$>$が以下の性質を持つとき**アドミシブル**であるという．

1. $\alpha>\beta$ ならば任意の項γにたいして $\alpha\gamma>\beta\gamma$.
2. 1と異なる任意の項αにたいして $\alpha>1$.

以下では$>$をアドミシブルな全順序とする．多項式fの順序最大の項（最大項）を $lpp(f)$ で，その係数を $lc(f)(\in\mathbf{B})$ で，さらに f からその最大単項すなわち $lc(f)lpp(f)$ を取り除いた残りの部分を $res(f)$ でそれぞれ表す．

多項式 f にたいし，$lc(f)=a$, $lpp(f)=\alpha$, $res(f)=h$ であるとき，f を記号 $a\alpha\triangleright h$ で表すものとする．多項式 $a\alpha\triangleright h$ は $ah=h$ が成り立つとき**ルール**と呼ばれる．

ルール $f=a\alpha\triangleright h$ による多項式上の **リダクション** $\rightarrow_f$ を以下のように定義する．

$b\alpha\gamma+g \rightarrow_f (1+a)b\alpha\gamma+b\gamma h+g.$

ただし，ここで多項式 $b\alpha\gamma+g$ は $a\neq b0$ をみたすものに限定する．（注意．ブール環では $-$（マイナス）は扱わないが，仮に$-$を用いれば $a+a=0$ より $(1+a)=(1-a)$ となるが，この形にすると上式の意味は明白であろう．）

F をルールの集合とする．F によるリダクション $\rightarrow_F$ を F に含まれるあるルールによるリダクションすなわち $h\rightarrow_F h'\Leftrightarrow\exists f\in F h\rightarrow_f h'$ で定義する．$\rightarrow_F$ の推移反射閉包を $\overset{*}{\rightarrow}_F$ で表す．F が有限集合のとき $\rightarrow_F$ は停止性を持つ．すなわち無限に続く多項式のリダクション $f_0\rightarrow_F f_1\rightarrow_F f_2\cdots$ は存在しない．（無限集合の場合には $\rightarrow_F$ は一般に停止性は持たない．）多項式 f と g が $f\overset{*}{\rightarrow}_F g$ かつ g は F の任意の要素でリダクションできないとき，g は f の$\rightarrow_F$による**既約形**であるという．$\rightarrow_F$ による f の既約形は一般には一つ以上存在するが $f\downarrow_F$ でそのうちの一つを表す．

注意．リダクションをルールによってのみ定義したのは次の性質を保証するためである．$\rightarrow_F$ の対称推移反射閉包（$\overset{*}{\leftrightarrow}_F$ で表す）による同値関係は，F で生成されるイデアルによる同値関係と一致する．すなわち，F で生成されるイデアルを I とおくと，任意の多項式 g, g' に対し $g\overset{*}{\leftrightarrow}_F g'\Leftrightarrow g+g'\in I$ が成り立つ．

一般の多項式によってもリダクションは同様に定義できるが，その場合この性質は成り立たない．例えば，$F=\{aX+1\}(a\neq1)$ とおくと，$a+1=(a+1)(aX+1)$ なので $a+1$ と0は F で生成されるイデアルに関して同値になるが，$a+1\overset{*}{\leftrightarrow}_F 0$ は成り立たない．

I を $\mathbf{B}[X_1, X_2, \cdots, X_n]$ のイデアルとする．ルールの有限集合 G が以下の性質をみたすとき，G は I の**ブーリアン・グレブナー基底**と呼ばれる．

1. I は G で生成されるイデアルである．
2. $g+g'\in I\Leftrightarrow$ ある多項式 h が存在して $g\overset{*}{\rightarrow}_G h$ かつ $g'\overset{*}{\rightarrow}_G h$ が成り立つ．
   （特に $g\in I\Leftrightarrow g\overset{*}{\rightarrow}_G 0$.）

ルール f と g にたいし以下で定義される多項式を f と g の **S多項式**と呼び $\mathrm{sp}(f, g)$ と表す．

$$\mathrm{sp}(f,g)=lc(g)\frac{lpp(g)}{\mathrm{GCD}(lpp(f),lpp(g))}f+lc(f)\frac{lpp(f)}{\mathrm{GCD}(lpp(f),lpp(g))}g$$

ここで $\mathrm{GCD}(lpp(f), lpp(g))$ は項 $lpp(f)$ と $lpp(g)$ の最大公約項を表す．

多項式 h にたいし以下で定義される多項式をその**自己C多項式**と呼び $\mathrm{scp}(h)$ で表す．

$\mathrm{scp}(h)=(1+lc(h))h.$

ブーリアン・グレブナー基底は次のように特徴付けられる．

定理 2.1.1 ルールの有限集合 G は，$\mathrm{GCD}(lpp(f), lpp(g))\neq1$ なる任意のルール $f, g\in G$ にたいして $\mathrm{sp}(f, g)\overset{*}{\rightarrow}_G 0$ が成り立つとき，かつそのときに限りブーリアン・グレブナー基底になる．

与えられた多項式の有限式の有限集合 F にたいし，F で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 $E\leftarrow F$, $R\leftarrow\emptyset$

while $E\neq\emptyset$

choose $h \in E$
if $h \downarrow_R = 0$
then
$E \leftarrow E - \{h\}$
else let $f = h \downarrow_R$ and
$E \leftarrow (E - \{h\}) \cup \{\mathrm{scp}(f)\} \cup$
$\{\mathrm{sp}(lc(f)f, g) \mid g \subset R$
$, \mathrm{GCD}(lpp(f), lpp(g)) \neq 1\}$
$R \leftarrow R \cup \{lc(f)f\}$
end-if
end-while
output R

R が求めるブーリアン・グレブナー基底である.

2.2 弱グレブナー基底

この節では，本稿で引用する文献 4) の結果について述べる.

I を $\mathbf{B}[X_1, \cdots, X_n]$ のイデアルとする.（本節の結果はブール環だけでなく，一般の単位元を持つ可換環 $\mathbf{B}$ にたいして成り立つ.）

I の有限部分集合 G はその最大単項の集合，すなわち $\{lc(g)lpp(g) \mid g \in G\}$，と I の最大単項の集合，すなわち $\{lc(g)lpp(g) \mid g \in I\}$，が同じイデアルを生成するとき I の**弱グレブナー基底**と呼ばれる.

m 個の単項の列 $M = (a_1\alpha_1, a_2\alpha_2, \cdots, a_m\alpha_m)$ に対し $\sum_{i=1}^{m} a_i\alpha_i h_i = 0$ となるような m 個の多項式の列 $(h_1, h_2, \cdots, h_m)$ を M の **syzygy** と呼ぶ.（通常は第一 syzygy と呼ばれている.）特に，すべての h_i が単項で，そのうち 0 でないもの $h_{i_1}, \cdots, h_{i_k}$ に対して，$lpp(h_{i_1})\alpha_{i_1} = \cdots = lpp(h_{i_k})\alpha_{i_k}$ が成り立つとき，**homogeneous** な **syzygy** と呼ぶ. M の syzygy の全体は明らかにモデュールを形成するが，これを S_M で表す.

与えられた多項式 $f, f_1, \cdots, f_l$ に対し，ある多項式 $g_1, \cdots, g_l$ を用いて

$$f = \sum_{i=1}^{l} g_i f_i \quad (lpp(f) = \max_{i=1}^{l} lpp(g_i)lpp(f_i))$$

のように表されるとき，これを f の $f_1, \cdots, f_l$ による**弱グレブナー表現**と呼ぶ.

定理 2.2.1 I を多項式の集合 $G = \{g_1, \cdots, g_m\}$ で生成されるイデアル，M を G のすべての要素の最大単項を添字の順に並べたもの，L を S_M の homogeneous な基底（すなわち L は S_M の基底であり，かつ L の元はすべて homogeneous）とする.

このとき次の二つは同値である.

（C1） G は I の弱グレブナー基底である.

（C2） L の任意の元 $(h_1, \cdots, h_m)$ にたいし $\sum_{i=1}^{m} h_i g_i$ は G による弱グレブナー表現が可能である.

3. 主要結果

3.1 ブーリアン・グレブナー基底の特徴付け

本節ではブーリアン・グレブナー基底が syzygy 基底によって特徴付けられることを示す.

まず，ルールの有限集合がブーリアン・グレブナー基底であることはそれが弱グレブナー基底であることに同値であることを示す.

定理 3.1.1 G をルールの有限集合，I をそれから生成されるイデアルとする. このとき G が I のブーリアン・グレブナー基底になるのは G が I の弱グレブナー基底になることに同値である.

証明： $G = \{a_1\alpha_1 \triangleright f_1, \cdots, a_m\alpha_m \triangleright f_m\}$ をイデアル I のブーリアン・グレブナー基底とするとき，G が I の弱グレブナー基底になることを示す. すなわち，$a\alpha \triangleright f$ を I に含まれる任意の多項式とするとき，$a\alpha$ が $a_1\alpha_1$, $\cdots$, $a_m\alpha_m$ の線形和として与えられることを示す.

ブーリアン・グレブナー基底の定義により $a\alpha \triangleright f \xrightarrow{*}_G 0$. したがって，$a\alpha$ はあるルール $a_i\alpha_i \triangleright f_i$ によってリダクション可能でなければならない. すなわち $\alpha = \alpha_i\gamma$ となる項 γ が存在し $a_i a \neq 0$ が成り立つ. ここでもし $(1 + a_i)a = 0$, すなわち $a = aa_i$ なら $a\alpha = a\gamma a_i\alpha_i$ となるから，$a\alpha$ は $a_1\alpha_1, \cdots, a_m\alpha_m$ の線形和として表される. もし $(1 + a_i)a \neq 0$ なら $a\alpha = a\gamma a_i\alpha_i + (1 + a_i)a\alpha$ となるが，$a\alpha \triangleright f \xrightarrow{*}_{a_i\alpha_i \triangleright f_i} (1 + a_i)a\alpha \triangleright (a\gamma f_i + f) \in I$ なので，$(1 + a_i)a\alpha$ はあるルール $a_j\alpha_j \triangleright f_j$ によってリダクション可能でなければならない. 上と同様のことを繰り返していくと，$a\alpha \triangleright f \xrightarrow{*}_G 0$ なので，ある段階で $(1 + a_k)\cdots(1 + a_j)(1 + a_i)a = 0$ となり，$a\alpha$ が $a_i\alpha_i, a_j\alpha_j, \cdots, a_k\alpha_k$ の線形和として与えられる.

逆を証明するために，$G = \{a_1\alpha_1 \triangleright f_1, \cdots, a_m\alpha_m \triangleright f_m\}$ がブーリアン・グレブナー基底ではないと仮定しよう. I を G で生成されるイデアルとする. 仮定より，G で既約な 0 ではない多項式 $f \in I$ が存在する.

もし $\alpha_i | lpp(f)$ なら $lc(f)a_i = 0$ であることに注意する. さて，もし f の最大単項が G の元の最大単項の線形和で表せる，すなわちある多項式 $h_1, h_2, \cdots, h_m$ にたいして $lc(f)lpp(f) = \sum_{i=1}^{m} h_i a_i \alpha_i$ が成り立つとしよう. このとき，ある i にたいして $\alpha_i | lpp(f)$ でなければならず，したがって上で注意したことから $lc(f)a_i$

$=0$ となる．式の両辺に $lc(f)$ を掛けると，左辺はそのままで右辺から $a_i\alpha_i$ が取り除かれる．この操作を何回か繰り返すと $lc(f)lpp(f)=0$ が得られるが，これは明らかに矛盾である． □

補題 3.1.2 F をルールの有限集合とする．多項式 g にたいして $g \xrightarrow{*}_F 0$ が成り立てば，g は F による弱グレブナー表現として表される．

証明： g がルール $a\alpha \triangleright f$ によって g' にリダクションされるとする．仮定より g は α で割り切れる項を含むから，$g=b\alpha\gamma+h$ と表され，したがって $g'=(1+a)b\alpha\gamma+b\gamma f+h$ と表されるので，$g=(a\alpha \triangleright f)b\gamma+g'$ が成り立つ．

ここで，もし $lpp(g)=\alpha\gamma$ なら $lpp(g)\geq lpp(g')$ であり，したがって $lpp(g)=lpp(a\alpha \triangleright f)lpp(b\gamma)$，そうでなければ $lpp(g)>\alpha\gamma$ となり，したがって $lpp(g)=lpp(g')$ が成り立つ．

さて $g \xrightarrow{*}_F 0$ より $g \to_{f_1} g_1 \to_{f_2} g_2 \cdots \to_{f_k} 0$ なるルール $f_1, \cdots, f_k \subset F$ がある．それぞれのステップで上の操作を繰り返すと，最後に g は $f_1, \cdots, f_k$ によって弱グレブナー表現として表される． □

定理 3.1.3 $G=\{g_1, \cdots, g_m\}$ をルールの有限集合，M を G のすべての要素の最大単項を添字の順に並べたもの，L を S_M の homogeneous な基底とする．このとき，L のあらゆる元 $(h_1, \cdots, h_m)$ にたいして $\sum_{i=1}^{m} h_i g_i \xrightarrow{*}_G 0$ が成り立つとき，かつそのときに限り G はブーリアン・グレブナー基底になる．

証明： G がブーリアン・グレブナー基底ならば $\sum_{i=1}^{m} h_i g_i$ は G で生成されるイデアルに含まれるので定義より $\sum_{i=1}^{m} h_i g_i \xrightarrow{*}_G 0$.

逆に L のあらゆる元 $(h_1, \cdots, h_m)$ にたいして $\sum_{i=1}^{m} h_i g_i \xrightarrow{*}_G 0$ が成り立つとしよう．補題 3.1.2. により $\sum_{i=1}^{m} h_i g_i$ は G による弱グレブナー表現として表される．したがって定理 2.2.1. により G は弱グレブナー基底になり，定理 3.1.1. によりブーリアン・グレブナー基底になることがいえる． □

3.2 不要なS多項式の除去

m (>2) 個の単項の列 $(a_1\alpha_1, \cdots, a_m\alpha_m)$ を M とおく．$1\leq i<j<k\leq m$ なる自然数 i, j, k にたいし

$$\alpha_{ij}=\mathrm{LCM}(\alpha_i, \alpha_j),\quad \alpha_{jk}=\mathrm{LCM}(\alpha_i, \alpha_j, \alpha_k),$$

とおく．ここで LCM は最小公倍項を表す．さらに

$$C_{ij}=\frac{a_j\alpha_{ij}}{\alpha_i}\vec{e}_i+\frac{a_i\alpha_{ij}}{\alpha_j}\vec{e}_j,\quad C_i=(1+a_i)\vec{e}_i,$$

とおく．ここで $\vec{e}_i$ は i 番目の成分が1で残りの成分は0であるような m 個の列を表す．

定理 3.2.1 $L=\{C_{ij}|1\leq i<j\leq m\}\cup\{C_i|1\leq i\leq m\}$ とおくと，L は S_M の homogeneous な基底になる．

証明： C_{ij} と C_i が homogeneous な M の syzygy であるのは明らか．

さて，M の homogeneous な syzygy の全体は S_M の基底をなすので，M のどんな homogeneous な syzygy も L の要素の線形和として表されることを示せばよい．$(b_1\beta_1, \cdots, b_m\beta_m)$ を M の homogeneous な syzygy とする．

すなわち $b_1a_1+\cdots+b_ma_m=0$ かつ $\beta_1\alpha_1=\cdots=\beta_m\alpha_m$ (これを γ とおく) であるとする．$b_i\beta_i\vec{e}_i=b_ia_i\beta_i\vec{e}_i+b_i(1+a_i)\beta_i\vec{e}_i=b_ia_i\beta_i\vec{e}_i+b_i\beta_iC_i$ と表されることに注意すると，

$$\begin{aligned}
&(b_1\beta_1, \cdots, b_m\beta_m)\\
&=(b_1a_1\beta_1, \cdots, b_ma_m\beta_m)+\sum_{i=1}^{m} b_i\beta_iC_i\\
&=((b_1a_1+\cdots+b_ma_m)\beta_1, b_2a_2\beta_2, \cdots, b_ma_m\beta_m)\\
&\quad+b_2a_2\beta_1\vec{e}_1+\cdots+b_ma_m\beta_1\vec{e}_1+\sum_{i=1}^{m} b_i\beta_iC_i\\
&=(0, b_2a_2\beta_2, \cdots, b_ma_m\beta_m)+b_2a_2\beta_1\vec{e}_1+\cdots\\
&\quad+b_ma_m\beta_1\vec{e}_1+\sum_{i=1}^{m} b_i\beta_iC_i\\
&=(0, b_2a_2\beta_2+b_2a_1\beta_2, \cdots, b_ma_m\beta_m+b_ma_1\beta_m)\\
&\quad+\sum_{i=2}^{m}(b_ia_i\beta_1\vec{e}_1+b_ia_1\beta_i\vec{e}_i)+\sum_{i=1}^{m} b_i\beta_iC_i\\
&=(0, b_2(a_2+a_1)\beta_2, \cdots, b_m(a_m+a_1)\beta_m)\\
&\quad+\sum_{i=2}^{m} b_i(a_i(\gamma/\alpha_1)\vec{e}_1+a_1(\gamma/\alpha_i)\vec{e}_i)+\sum_{i=1}^{m} b_i\beta_iC_i\\
&=(0, b_2(a_2+a_1)\beta_2, \cdots, b_m(a_m+a_1)\beta_m)\\
&\quad+\sum_{i=2}^{m} b_i(\gamma/\alpha_{1i})C_{1i}+\sum_{i=1}^{m} b_i\beta_iC_i
\end{aligned}$$

となる．したがって $(0, b_2(a_2+a_1)\beta_2, \cdots, b_m(a_m+a_1)\beta_m)$ はまた M の homogeneous な syzygy になる．この操作を繰り返し行うと，最後に $(b_1\beta_1, \cdots, b_m\beta_m)$ は L の要素の線形和として表される． □

多項式の集合 F (適当に並べられているとする) にたいするS多項式は，通常は F の単項の列の syzygy 全体から成るモデュールの基底の元と F の内積として定義される．例えば係数環が体のとき，Buchberger によって与えられたS多項式はモデュールの基底として Taylor 基底を用いたもので，これの特殊なケース

にあたる．m 個の多項式の列 $(a_1\alpha_1 \triangleright h_1, \cdots, a_m\alpha_m \triangleright h_m)$ を F とおく．このとき，$a_i\alpha_i \triangleright h_i$ の自己C多項式は，上の記号を使うと $F\cdot C_i$ と表され，通常のS多項式の一種であることがわかる．

補題 3.2.2 $\alpha_k | \alpha_{ij}$ かつ $a_k a_i a_j = a_i a_j$ ならば，C_{ij} は C_{ik}, C_{jk}, C_i, C_j の線形和として表される．

証明：次式において左辺を定義にしたがって計算することにより，その成立が容易に示される．

$$a_k\frac{\alpha_{ijk}}{\alpha_{ij}}C_{ij}+a_j\frac{\alpha_{ijk}}{\alpha_{ik}}C_{ik}+a_i\frac{\alpha_{ijk}}{\alpha_{jk}}C_{jk}=0$$

$\alpha_k | \alpha_{ij}$ ゆえ $\alpha_{ijk}=\alpha_{ij}$ となるので，上式より a_kC_{ij} は C_{ik} と C_{jk} の線形和で表される．

一方，$a_ia_j+a_ka_ia_j=0$ より $(1+a_k)a_j=a_j+a_ka_j=a_j+a_ka_j+a_ia_j+a_ka_ia_j=(1+a_k)a_j(1+a_i)$ が得られる．

同様に，$(1+a_k)a_i=(1+a_k)a_i(1+a_j)$ が成り立つ．したがって

$$\begin{aligned}(1+a_k)C_{ij}&=(1+a_k)a_j(\alpha_{ij}/\alpha_i)\vec{e}_i\\&\quad+(1+a_k)a_i(\alpha_{ij}/\alpha_j)\vec{e}_j\\&=(1+a_k)a_j(1+a_i)(\alpha_{ij}/\alpha_i)\vec{e}_i\\&\quad+(1+a_k)a_i(1+a_j)(\alpha_{ij}/\alpha_j)\vec{e}_j\\&=(1+a_k)a_j(\alpha_{ij}/\alpha_i)C_i\\&\quad+(1+a_k)a_i(\alpha_{ij}/\alpha_j)C_j.\end{aligned}$$

以上を合わせると C_{ij} が C_{ik}, C_{jk}, C_i, C_j の線形和として表されることが分かる．□

この補題は次のように一般化される．

系 3.2.3 $1\leq k\leq l$ なるあらゆる k にたいし $\alpha_{nk} | \alpha_{ij}$ であり，さらに $(a_{n_1}\vee a_{n_2}\cdots\vee a_{n_l})a_ia_j=a_ia_j$ が成り立つとき，C_{ij} は $C_{in_1}C_{in_2}, \cdots, C_{jn_1}, C_{jn_1}, C_{jn_2}, \cdots, C_{jn_l}, C_i, C_j$ の線形和として表される．

（ここで記号∨はブール代数の和を表す．すなわち $a\vee b=a+b+ab$.）

証明：補題と同様にして，$a_{n_1}C_{ij}, \cdots, a_{n_l}C_{ij}$ と $(1+(a_{n_1}\vee a_{n_2}\vee\cdots\vee a_{n_l}))C_{ij}$ が $C_{in_1}, C_{in_2}, \cdots, C_{in_l}, C_{jn_1}, C_{jn_2}, \cdots, C_{jn_l}, C_i, C_j$ の線形和として表されることが示される．さて，ブール代数の性質より $a_{n_1}\vee a_{n_2}\vee\cdots\vee a_{n_l}=b_1a_{n_1}+b_2a_{n_2}+\cdots+b_la_{n_l}$ なる $\mathbf{B}$ の元 $b_1, b_2, \cdots, b_l$ が存在する．これを使うと $C_{ij}=(1+(a_{n_1}\vee a_{n_2}\vee\cdots\vee a_{n_l}))C_{ij}+b_1a_{n_1}C_{ij}+\cdots+b_la_{n_l}C_{ij}$ となり，上と合わせて C_{ij} が $C_{in_1}, C_{in_2}, \cdots, C_{in_l}, C_{jn_1}, C_{jn_2}, \cdots, C_{jn_l}, C_i, C_j$ の線形和として表されることが示される．□

この系により，不要なS多項式の計算を除去することによって，ブーリアン・グレブナー基底を求めるアルゴリズムを，次のように改良できる．

F を多項式の有限集合とする．

input $E\leftarrow F$, $R\leftarrow\emptyset$
　while $E\neq\emptyset$
　　choose $h\in E$
　　if $h\downarrow_R=0$
　　then
　　$E\leftarrow E-\{h\}$
　　else let $f=h\downarrow_R$ **and**
　　$E\leftarrow(E-\{h\})\cup\{\mathrm{scp}(f)\}\cup$
　　$\{\mathrm{cp}(lc(f)f, g) | g\in R, (\neg\mathrm{Red}(f, g, R)\}$
　　$R\leftarrow R\cup\{lc(f)f\}$
　　end-if
　end-while
output R

R は F で生成されるイデアルのブーリアン・グレブナー基底になる．

$\mathrm{Red}(f, g, R)$ は不要なS多項式の計算を除去するためのもので，以下のいずれかの場合に限って真となる．

場合 1) $\mathrm{GCD}(lpp(f), lpp(g))=1$；

場合 2) R の中に $lc(f)f$ と g のどちらとも異なるルール $h_1, \cdots h_l$ があって，それぞれにたいして $lpp(h_i) | \mathrm{LCM}(lpp(f), lpp(g))$ が成り立ち，かつ $(lc(h_1)\vee\cdots\vee lc(h_l))lc(f)lc(g)=lc(f)lc(g)$ となる．

4. 実験結果

定数記号の可算集合 {a 1, a 2, a 3, …} の有限部分集合と有限部分集合の補集合の全体はブール環を形成する．われわれは集合制約の解消系のため，このブール環上の多項式環のブーリアン・グレブナー基底を求めるアルゴリズムをインプリメントした[5]．

これを使って前章で述べた，不要なS多項式の計算を除去する方法が，どのくらい有効か調べるための実験を行った．次表はその実験結果の一部である．#1-#5 は，それぞれ多項式の集合のブーリアン・グレブナー基底を，不要なS多項式の計算を除去する方法を組み込んだものと組み込まないもの，両方のアルゴリズムによって計算した例である．表の上から，与えられた多項式全体の中に現れる，係数としての集合に含まれる定数記号の数，すなわちその中に現れる a 1, a 2, a 3, … の総数，次に，多項式の変数の総数を表し，続いて，不要なS多項式の計算を除去する方法を組み込んだアルゴリズムによって，ブーリアン・グレブナー基底を求めた際生成されたS多項式の数，除去さ

れたS多項式の数，生成された自己C多項式の数，計算に要した時間，最後に，不要なS多項式の計算を除去する方法を組み込まないアルゴリズムによる計算時間，を表す．系3.2.3の第2の条件は係数に関するものであり，含まれる定数記号の数が増えると係数が複雑になり，これを満たさない場合が多くなるかもしれず，実際に生成されるS多項式の数にたいする，余分なS多項式の数の割合は減少するかもしれない．しかしながら，#1-#4 の結果ではあまりかわらない．したがって，余分なS多項式除去の算法が有効で，実際，計算時間も短縮されていることが分かる．また，#5のように変数の数が増えると計算時間も増えるが，余分なS多項式の数の割合も増加し，したがって計算時間も著しく減少する傾向が一般にあることが，その他の実験によって得られた．

	#1	#2	#3	#4	#5
elements	4	9	14	23	7
variables	13	12	13	13	17
created sp's	1058	1234	886	1021	6027
removed sp's	1272	1921	1165	1400	18532
created scp's	163	195	181	207	460
time(sec)	55	57	45	62	1718
(removing redundant sp's)					
time(sec)	107	129	98	131	10423
(not removing redundant sp's)					

5. おわりに

本論文は文献 6) で導入されたブーリアン・グレブナー基底が syzygy 基底によって特徴付けられることを示した．これにより，ブーリアン・グレブナー基底を求めるときに必要な自己C多項式が特別なものではなく，実はS多項式の一種であることが明らかになった．またブーリアン・グレブナー基底を求めるアルゴリズムにおいて，余分なS多項式の計算が除去できることを示し，実際にインプリメントを行いその有効性について実験した．その結果，係数が複雑になっても余分なS多項式の割合は減少せず，変数の数が増えると著しく増加する傾向が得られ，この方法の有効性が実証された．

参考文献

1) Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal, PhD thesis, Universität Innsbruck (1965).
2) Buchberger, B.: A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Bases, *EUROSAM 79*, *Springer Lec. Notes Comp. Sci.*, Vol. 72, pp. 3-21 (1979).
3) Gebauer, R. and Möller, H. M.: On an Installation of Buchberger's Algorithm, *J. Symbol. Comput.*, Vol. 6, pp. 275-286 (1988).
4) Möller, H. M.: On the Construction of Gröbner Bases Using Syzygies, *J. Symbol. Comput.*, Vol. 6, pp. 345-359 (1988).
5) Sato, Y., Sakai, K. and Menju, S.: Solving Constraints over Sets by Boolean Gröbner Bases, *Proceeding of The Logic Programming Conference '91*, pp. 73-79 (1991).
6) Sakai, K., Sato, Y. and Menju, S.: Boolean Gröbner Bases, ICOT Technical Report (1992).

(平成4年9月30日受付)
(平成5年4月 8 日採録)

佐藤 洋祐（正会員）

1956 年生．1979 年名古屋大学理学部数学科卒業．1983年神戸大学大学院理学研究科数学専攻修士課程修了．1986年ニューヨーク州立大学バッファロー校大学院博士課程修了．Ph. D.（集合論）．1987年三菱電機(株)入社後(財)新世代コンピュータ技術開発機構へ出向．1993年より立命館大学理工学部情報工学科助教授．制約論理プログラミング，計算機代数，TRS 等に興味を持つ．日本数学会会員．

毛受 哲（正会員）

1962 年生．1985 年東京工業大学理学部情報科学科卒業．1987年同大学大学院理工学研究科情報科学専攻修士課程修了．同年日本電気(株)入社．同年7月より(財)新世代コンピュータ技術開発機構へ出向し，制約論理プログラミングのための制約評価アルゴリズムの研究に従事．1993年4月より日本電気(株) C&C システム研究所システム基礎研究部に所属．人工知能学会，ソフトウェア科学会各会員．

相場 亮（正会員）

1986 年慶應義塾大学大学院工学研究科数理工学専攻博士課程修了．工学博士．同年，日本電気(株)に入社．C&C システム研究所コンピュータシステム研究部に勤務．1987年より(財)新世代コンピュータ技術開発機構に出向．第1研究室研究員，同主任研究員，第4研究室室長代理を経て現在第2研究部部長代理．制約論理プログラミング言語の研究に従事．日本ソフトウェア科学会，人工知能学会各会員．