数理解析研究所講究録
1514巻 2006年 125-131

包括的ブーリアングレブナ基底の構成について

井上　秀太郎
SHUTARO INOUE
東京理科大学大学院理学研究科数学専攻
DEPARTMENT OF MATHEMATICS,GRADUATE SCHOOL OF SCIENCE,TOKYO UNIVERSITY OF SCIENCE*

佐藤　洋祐
YOSUKE SATO
東京理科大学理学部数理情報科学科
DEPARTMENT OF MATHEMATICAL INFORMATION SCIENCE,TOKYO UNIVERSITY OF SCIENCE†

Abstract

変数 $\bar{X}$ と $\bar{A}$ をもつブール多項式環におけるブロックオーダー $\bar{X} \gg \bar{A}$ のもとでのブーリアングレブナ基底が、実は主変数を $\bar{X}$、パラメータ変数を $\bar{A}$ とする包括的ブーリアングレブナ基底になることを示す．これにより、剰余環を利用して包括的ブーリアングレブナ基底を求める従来の方法よりもはるかに高速でメモリー消費量も少ない計算方法が得られる．

1　はじめに

包括的グレブナ基底とは簡単に述べるとパラメータを含むグレブナ基底のことである．一般的にそれらの計算は通常のグレブナ基底と比べより多くの時間とメモリを消費するという問題を抱えている．本研究ではブール多項式環上の包括的グレブナ基底に関してこれらの問題を解決する新しい計算方法について発表する．

ブール多項式環上の計算に対して次の定理が知られている．

定理

I をブール多項式環 $B(\bar{A},\bar{X})$ のイデアルとし，$G=\{g_1(\bar{A},\bar{X}),\ldots,g_m(\bar{A},\bar{X})\}$ を $B(\bar{A})$ を係数ブール環とするブール多項式環 A における I の分層ブーリアングレブナ基底とする．このとき，B の任意の要素 $\bar{a}$ にたいして，$\{g'_1(\bar{a},\bar{X}),\ldots,g'_{m'}(\bar{a},\bar{X})\}$ はブール多項式環 $B(\bar{X})$ において $I(\bar{a})=\{f(\bar{a},\bar{X}) \mid f(\bar{A},\bar{X})\in I\}$ の分層ブーリアングレブナ基底となる．

この定理を使用した計算方法は完全な包括的ブーリアングレブナ基底を計算できるが計算時間は通常のブーリアングレブナ基底よりも効率が悪く、メモリの消費も大きい．これらの問題の主な原因はパラメータの消去イデアルを考慮していないことである．本研究では次の定理に基づく消去イデアルを利用した新しい計算方法を提案し、数式処理システム Risa/Asir を用いて実装した．

*j1104605@ed.kagu.tus.ac.jp
†ysato@rs.kagu.tus.ac.jp

定理
I をブール多項式環 $B(\bar{A},\bar{X})$ のイデアルとし, $G=\{g_1(\bar{A},\bar{X}),\ldots,g_m(\bar{A},\bar{X}),\ h_1(\bar{A}),\ldots,h_l(\bar{A})\}$ を単項式順序 $\bar{X}>>\bar{A}$ としたときの I のブーリアングレブナ基底とする. このとき $G\setminus\{h_1(\bar{A}),\ldots,h_l(\bar{A})\}$ はブール多項式環 $(B(\bar{A})/\langle h_1(\bar{A}),\ldots,h_l(\bar{A})\rangle)(\bar{X})$ 上の I のブーリアングレブナ基底になる.
また $G'=\{g'_1(\bar{A},\bar{X}),\ldots,g'_{m'}(\bar{A},\bar{X})\}$ を $(B(\bar{A})/\langle h_1(\bar{A}),\ldots,h_l(\bar{A})\rangle)(\bar{X})$ 上の I の分層ブーリアングレブナ基底とする. このとき, $h_1(\bar{a})=0,\ldots,h_l(\bar{a})=0$ を満たす B の任意の要素 $\bar{a}$ にたいして, $\{g'_1(\bar{a},\bar{X}),\ldots,g'_{m'}(\bar{a},\bar{X})\}$ は $I(\bar{a})=\{f(\bar{a},\bar{X})\mid f(\bar{A},\bar{X})\in I\}$ の分層ブーリアングレブナ基底となる.

計算実験を行った結果、今までの方法と比較して圧倒的に高速であり、メモリ消費量も格段に抑えることが確認された. これにより集合ブール環における限量子消去法アルゴリズム等の実装の見通しがたった.

本論文では2節にブーリアングレブナ基底、3節に包括的グレブナ基底について述べる. 4節では包括的ブーリアングレブナ基底のアルゴリズムと問題点を示し、5節で新しい包括的ブーリアングレブナ基底のアルゴリズムを提案する.

2 ブーリアングレブナ基底

ブーリアングレブナ基底を次のように定義する.

定義 1 全ての要素が冪等であるような、単位元をもつ可換環 B をブール環とよぶ. ブール環 B を係数とする多項式環 $B[X_1,\ldots,X_n]$ のイデアル $\langle X_1^2-X_1,\ldots,X_n^2-X_n\rangle$ による剰余環をブール多項式環とよび、$B(X_1,\ldots,X_n)$ で表す. ブール多項式環におけるグレブナ基底をブーリアングレブナ基底とよぶ.

ブール多項式についての単項式簡約は次のように定義する.

定義 2 ブール多項式 $f=a\alpha+h$ による単項式簡約 $\rightarrow_f$ を

$$ba\beta\rightarrow_f b(1+a)\alpha\beta+ba\beta h$$

と定義する.(ただし $ab\neq 0$ とする.)

体を係数とする多項式環と違う点は、項として簡約できたとしても係数によっては簡約できないことである. 例えば $\{1\}*X*Y$ を $\{2\}*Y+\{1,2\}$ で簡約を試みても $\{1\}(1+\{2\})*X*Y+\{1\}*\{2\}*\{1,2\}*X=\{1\}*X*Y$ となり元の式と変わらない. また簡約が成功したしても必ず次数が下がるとは限らない. 例えば $\{1,2\}*X*Y$ を $\{2\}*Y+\{1,2\}$ で簡約すると $\{1\}*X*Y+\{2\}*X$ となる. 先頭項は共に $X*Y$ となっている. しかし簡約前と簡約後の先頭項が同じ場合でも係数は必ず小さくなる. よって簡約が無限に行われることはない. この現象は係数のブール環が整域ではないために生じる. また多項式 $\{1\}*X+\{2\}$ にたいして定数 $\{2\}$ を掛ける。すると多項式は $\{2\}$ となり先頭項が変化する. このためにブール多項式環では同値関係 $\overset{*}{\leftrightarrow}_F$ とイデアル $\langle F\rangle$ による同値関係は一般に一致しない. これらを解決するために次の用語を導入する.

定義 3 ブール多項式 f が $lc(f)f=f$ を満たすとき 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.

以上の定義により与えられた多項式に対して先頭項の係数が0になり、先頭項が変化することはなくなる. ブール閉を用いることによってブーリアングレブナ基底の定義に必要な次に定理が成り立つことが示せる.

定理 1 F をブール閉であるブール多項式の集合とする. 同値関係 $\overset{*}{\leftrightarrow}_F$ はイデアル $\langle F\rangle$ による同値関係と一致する. つまり任意のブール多項式 f,g に対して $f \overset{*}{\leftrightarrow}_F g \Leftrightarrow f-g \in \langle F\rangle$ が成り立つ.

以上より先ほどの単項式簡約を用いてブーリアングレブナ基底を定義することができる.

定義 4 多項式の有限集合 G が以下の 2 つの性質を満たすとき、G はブーリアングレブナ基底であるとよぶ.
- 任意のブール多項式 f,g に対して $f \overset{*}{\leftrightarrow}_G g \Leftrightarrow f-g \in \langle G\rangle$ が成り立つ.
- $\rightarrow_G$ がチャーチ・ロッサー性をもつ. つまり任意のブール多項式 f,g,h に対して

$$f \overset{*}{\leftrightarrow}_G g \Leftrightarrow \exists h\ f \overset{*}{\rightarrow}_G h, g \overset{*}{\rightarrow}_G h$$

が成り立つ.

定理 2 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基底であることは任意の多項式 $f,g \in G$ にたいして $SP(f,g) \overset{*}{\rightarrow}_G 0$ が成り立つことと一致する.

上記の定理はブーリアングレブナ基底の計算も係数が体のときと同じようにできることを示している. 注意しなければならないことは計算途中に現われたブール多項式をブール閉としなければならないことである. また簡約ブーリアングレブナ基底は一意に定まらない. しかし次にような性質を持つ.

定理 3 G を簡約ブーリアングレブナ基底とする. このとき G の任意の要素はブール閉である.

ブーリアングレブナ基底の一意性を得るために次の定義を行う.

定義 5 G を簡約ブーリアングレブナ基底とする. 任意の異なる多項式 $f,g \in G$ にたいして $LT(f) \neq LT(g)$ が成り立つとき G は分層ブーリアングレブナ基底であるとよぶ.

例として 2 つのイデアル $\langle\{1,2\} * X\rangle$ と $\langle\{1\} * X, \{2\} * X\rangle$ を考える. これらは同じイデアルの簡約ブーリアングレブナ基底となっている. しかし前者は分層ブーリアングレブナ基底となるが、後者はならない. このような条件を加えることによりブーリアングレブナ基底の一意性が得られる.

定理 4 G,H は $\langle G\rangle = \langle H\rangle$ を満たす分層ブーリアングレブナ基底であるとする. このとき $G = H$ が成り立つ.

ブール多項式に関しては以下の 2 つの定理が成り立つ.

定理 5 *(零点定理)*
I をブール多項式環 $B(\bar{X})$ のイデアルとする. このとき

$$V(I) = \emptyset \Leftrightarrow \exists a \in B \quad a \in I \qquad \textit{(弱形の零点定理)}$$

が成り立つ. また I が有限生成であると仮定する. このとき

$$f(\bar{X}) \in I \Leftrightarrow \forall \bar{a} \in V(I)\ f(\bar{a}) = 0 \qquad \textit{(強形の零点定理)}$$

が成り立つ.

定理 6 *(拡張定理)*
I をブール多項式環 $B(\bar{A},\bar{X})$ のイデアルとする. このとき任意の $\bar{a} \in V(I \cap B(\bar{X}))$ にたいして $(\bar{a},\bar{b}) \in V(I)$ となる $\bar{b}$ が存在する.

3 包括的グレブナ基底

包括的グレブナ基底を次のように定義する.

定義 6 I を係数が環 R である多項式環 $R[\bar{A},\bar{X}]$ のイデアルとする. このとき有限集合 $G \subseteq I$ が包括的グレブナ基底であるとは、R の拡大環 R' の任意の要素 $\bar{a}$ にたいして、$G(\bar{a}) = \{g(\bar{a},\bar{X})|g \in G\}$ が $I(\bar{a}) = \{f(\bar{a},\bar{X})|f \in I\}$ のグレブナ基底となることと定義する.

ブール多項式環のイデアルにおける包括的グレブナ基底を包括的ブーリアングレブナ基底と呼ぶ. 実際に係数を体とする多項式環の包括的グレブナ基底の例として $G = \{AX+Y, Y+1\}$ を与える. 変数順序 $X > Y > A$ の辞書式順序とすると G はグレブナ基底となっている. ここで変数 A をパラメータとして考える. $A \neq 0$ のときは $G = \{X+Y, Y+1\}$ となりグレブナ基底となるが、$A = 0$ のときは $G = \{Y, Y+1\}$ となりグレブナ基底にならない. そこでパラメータの値によらず常にグレブナ基底になる性質を持つパラメータ付きのグレブナ基底を求めることをお考える. 簡単な発想として 2 つの方法が考えられる.

1. 有理関数体 $Q(A)$ を係数体とする多項式環においてグレブナ基底を計算する.
2. 変数順序を $X > Y > A$ とする辞書式順序においてグレブナ基底を計算する.

しかしどちらの方法でも期待する結果を得る事はできない. 1 つ目の方法は分母にパラメーターがある場合に代入すらできない状況が考えられる. それは先ほどの例で上げた G の 1 つ目の多項式 $AX+Y$ を見れば明らかである. $X + \frac{1}{A}Y$ に対して A に 0 は代入できない. 2 つ目に関しても G が変数順序 $X > Y > A$ の辞書式順序のグレブナ基底であることから反例となっていることが分かる. このようにに包括的グレブナ基底を構成することは容易ではない.

それでは係数をブール環としたとき、つまり包括的ブーリアングレブナ基底の計算についてはどうだろうか. そこで先ほどの 2 つの方法を適用することを考えてみると、2 つ目の方法は関しては次のような例をある.

例 1 以下のブール多項式の集合を与える.

$$\begin{cases} (X*Y+X+Y) = \{1,2\}*(X*Y+X+Y) \\ \{1\}*X = \{1\} \\ A*Y = A \\ X*Y = 0 \end{cases}$$

ここで A は $\{a\}$ を置き換えたパラメーターであり、a は要素を表している. 単項式順序を $X \gg A$ としてブーリアングレブナ基底を計算すると次のようになる.

$$\begin{cases} X*Y \\ Y*A+\{2\}*A \\ (1+\{2\})*Y \\ X*A \\ (1+\{2\})*X+\{1\} \\ (1+\{2\})*A \end{cases}$$

これらに A に $\{2\}$ を代入すると、

$$\begin{cases} X*Y \\ Y*\{2\}+\{2\} \\ (1+\{2\})*Y \\ X*\{2\} \\ (1+\{2\})*X+\{1\} \end{cases}$$

となる. これらはブーリアングレブナ基底ではない.

上の例は順序に関してパラメーターを変数よりも下げてブーリアングレブナ基底を計算するだけでは包括的ブーリアングレブナ基底とはならないことを示している. しかし1つ目の方法つまりパラメーターを係数とみなしてブーリアングレブナ基底を計算する手法がうまくいくことが [6, ?] において示されている.

4 包括的ブーリアングレブナ基底のアルゴリズム

前節より包括的ブーリアングレブナ基底のアルゴリズムを述べる.

定理 7 I をブール多項式環 $B(\bar{A},\bar{X})$ のイデアルとし, $G=\{g_1(\bar{A},\bar{X}),\ldots,g_m(\bar{A},\bar{X})\}$ を $B(\bar{A})$ を係数ブール環とするブール多項式環 A における I の分層ブーリアングレブナ基底とする. このとき, B の任意の要素 $\bar{a}$ にたいして, $\{g\prime_1(\bar{a},\bar{X}),\ldots,g\prime_{m\prime}(\bar{a},\bar{X})\}$ はブール多項式環 $B(\bar{X})$ において $I(\bar{a})=\{f(\bar{a},\bar{X})\mid f(\bar{A},\bar{X})\in I\}$ の分層ブーリアングレブナ基底となる.

先ほど例に対してこのアルゴリズムを使うと次のようになる.

例 2
同じ例題を与える.

$$\begin{cases}(X*Y+X+Y)=\{1,2\}*(X*Y+X+Y)\\ \{1\}*X=\{1\}\\ A*Y=A\\ X*Y=0\end{cases}$$

係数を $B(A)$ とする多項式環として分層ブーリアングレブナ基底を計算すると

$$\begin{cases}(\{2\}*A+\{2\})*X*Y\\ (A+\{2\}+1)*Y+\{2\}*A\\ (A+\{2\}+1)*X+\{1\}*A+\{1\}\\ (\{2\}+1)*A\end{cases}$$

となる. これらに A に $\{2\}$ を代入すると

$$\begin{cases}X+\{1\}\\ Y+\{2\}\end{cases}$$

となり、A に $\{1\}$ を代入すると

$$\begin{cases}\{2\}*X*Y\\ (\{1,2\}+1)*X\\ (\{1,2\}+1)*Y\\ \{1\}\end{cases}$$

となる. 両方ともに分層ブーリアングレブナ基底となっている.

このアルゴリズムによって包括的ブーリアングレブナ基底を計算することができる. しかしパラメーターで構成されるブール多項式環を係数とするために次のような問題があった.

- 一般的に通常のブーリアングレブナ基底よりも計算時間を消費する.

- 多くのメモリを必要とする.

特にパラメータが多くなると時間とメモリの消費が非常に増えてしまい実用的ではなかった. 主な原因はパラメーターによる消去イデアルを考慮していないことによる無駄な計算である. この問題を解決するためにグレブナ基底のスタビリティーの理論を導入する.

5 包括的ブーリアングレブナ基底の新しいアルゴリズム

パラメータで構成される消去イデアルは順序を $\bar{X} >> \bar{A}$ としたときのブーリアングレブナ基底を計算することで求めることができる. スタビリティーの理論 [4, ?, 1] より多項式環 $\mathrm{B}(\bar{X}, \bar{A})$ のグレブナ基底はブール多項式環 $(\mathrm{B}(\bar{A})/I \cap \mathrm{B}(\bar{A}))(\bar{X})$ のグレブナ基底となっていることが分かる. また [5] の理論を適用することによって分層包括的ブーリアングレブナ基底も構成することができる.

定理 8 I をブール多項式環 $B(\bar{A}, \bar{X})$ のイデアルとし, $G = \{g_1(\bar{A}, \bar{X}), \ldots, g_m(\bar{A}, \bar{X}), h_1(\bar{A}), \ldots, h_l(\bar{A})\}$ を単項式順序 $\bar{X} >> \bar{A}$ としたときの I のブーリアングレブナ基底とする. このとき $G \setminus \{h_1(\bar{A}), \ldots, h_l(\bar{A})\}$ はブール多項式環 $(B(\bar{A})/\langle h_1(\bar{A}), \ldots, h_l(\bar{A})\rangle)(\bar{X})$ 上の I のブーリアングレブナ基底になる.
また $G' = \{g'_1(\bar{A}, \bar{X}), \ldots, g'_{m'}(\bar{A}, \bar{X})\}$ を $(B(\bar{A})/\langle h_1(\bar{A}), \ldots, h_l(\bar{A})\rangle)(\bar{X})$ 上の I の分層ブーリアングレブナ基底とする. このとき, $h_1(\bar{a}) = 0, \ldots, h_l(\bar{a}) = 0$ を満たす B の任意の要素 $\bar{a}$ にたいして, $\{g'_1(\bar{a}, \bar{X}), \ldots, g'_{m'}(\bar{a}, \bar{X})\}$ は $I(\bar{a}) = \{f(\bar{a}, \bar{X}) \mid f(\bar{A}, \bar{X}) \in I\}$ の分層ブーリアングレブナ基底となる.

再び同じ例を与えて、新しいアルゴリズムでブーリアングレブナ基底を計算して結果を比較する.

例 3
同じ例題を与える.

$$\begin{cases} (X * Y + X + Y) = \{1,2\} * (X * Y + X + Y) \\ \{1\} * X = \{1\} \\ A * Y = A \\ X * Y = 0 \end{cases}$$

これらの多項式に対して、新しいアルゴリズムでブーリアングレブナ基底を計算すると

$$\begin{cases} (\{2\} * A + \{2\}) * X * Y \\ (\{2\} * A + \{2\} + 1) * X + \{1\} \\ (\{2\} * A + \{2\} + 1) * X + \{2\} * A \\ (\{2\} + 1) * A \end{cases}$$

となる.A に $\{2\}$ を代入すると

$$\begin{cases} X + \{1\} \\ Y + \{2\} \end{cases}$$

となり、A に $\{1\}$ を代入すると

$$\begin{cases} \{2\} * X * Y \\ (\{2\} + 1) * X + \{1\} \\ (\{2\} + 1) * Y \\ \{1\} \end{cases}$$

となる.{2} を代入した場合は分層ブーリアングレブナ基底となるが、{1} を代入した場合は簡約された形になっていない.

上の例のように新しいアルゴリズムで計算されるブーリアングレブナ基底は正確には包括的ブーリアングレブナ基底ではない. 分層ブーリアングレブナ基底となることが保証されているのは $h_1(\bar{a})=0,\ldots,h_l(\bar{a})=0$ を満たす要素 a を代入したときだけである. これだけをを見ると新しいアルゴリズムは不完全である印象を持つかもしれない. しかし $h_1(\bar{a})=0,\ldots,h_l(\bar{a})=0$ を満たさない要素を代入した場合、イデアルのアフィン多様体は空集合となる. また新しいアルゴリズムではパラメータが増加しても変数として扱うために時間とメモリの消費量の増加を抑えられる. このことから応用する上で実用的なアルゴリズムであると考える.

6 おわりに

本論文で提唱した、包括的ブーリアングレブナ基底の新しいアルゴリズムは付録のデータが示すように、従来のアルゴリズムと比較して圧倒的に効率的であるが、このアルゴリズムにはさらに効率化の可能性がある。パラメーター部分の消去イデアルがあらかじめ判っている場合は、この消去イデアルによる剰余環を係数環とするブール多項式環を係数環とする多項式環で、アルゴリズムを展開する方がメモリー消費量を低くおさえられる。ただし、消去イデアルはブーリアングレブナ基底を計算するまでは判らないので、この方法を直接利用することは不可能である。しかしながら、ブーリアングレブナ基底の計算の途中でパラメーターのみからなる多項式が得られるたびにそれをインクリメンタルに消去イデアルに付けたし、その剰余環で作業を行うことが可能である。これはパラメーターのみの多項式をつけ加えて拡大したイデアルによる剰余環によるブール環の準同型にたいして、それまでのアルゴリズムがそのまま保存されるためである。この方法でアルゴリズムをさらに効率化することが可能になる。

今回の新しいアルゴリズムによって、集合ブール環上の限量子消去法の実装が現実に可能になったと考えられる。集合ブール環上において限量子消去法が可能であり、そのアルゴリズムとして包括的ブーリアングレブナ基底を用いるのが有効であることが筆者らの最近の研究で明らかになっている。従来のアルゴリズムでは現実的に不可能であった、集合ブール環上の限量子消去法の実装もこれからの課題である。

参 考 文 献

[1] Becker,T.(1994).On Groöbner Bases under Specialization.Applicable Algebra in Engineering,Communication and Computing.5,1-8

[2] Becker,T and V.Weispfenning,V.Groöbner Bases.Springer-Verlag,NewYork-Berlin-Heidelberg,1993.

[3] Gianni,P.(1989).Properties of Groöbner Bases under Specialization. EUROCAL'87,J.H.Davenport Ed.,Springer LNCS 378,293-297

[4] Kalkbrener,M.(1997).On the Stability of Groöbner Bases Under Specializations. J.Symb.Comp.24/1,51-58.

[5] Sato,Y. Suzuki,A and Nabeshima,K.(2003).ACGB on varieties.In Proceeding of CASC2003,313-318

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

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