数理解析研究所講究録
第1907巻 2014年 110-115

ブーリアングレブナ基底を使用した集合制約解法の改良

井上　秀太郎
SHUTARO INOUE
東京理科大学理学部
DEPARTMENT OF MATHEMATICAL INFORMATION SCIENCE,TOKYO UNIVERSITY OF SCIENCE*

1　はじめに

すべての要素が冪等であるような単位元1をもつ可換環$\mathbf{B}$をブール環と呼ぶ. さらに多項式環$\mathbf{B}[X_1,\ldots,X_n]$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呼び、$\mathbf{B}(X_1,\ldots,X_n)$と表す. ブーリアングレブナ基底とはこのブール多項式環上のグレブナ基底のことである. 我々はブーリアングレブナ基底を使用した数独パズルの解法についての研究を行ってきた. 本稿では, これまでの方法を改良について説明する.

2　ブール多項式環

ブール環とブール多項式環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$\mathbf{B}$をブール環とよぶ.

定義 2 ブール環$\mathbf{B}$を係数とする多項式環$\mathbf{B}[X_1,\ldots,X_n]$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、$\mathbf{B}(X_1,\ldots,X_n)$で表す.

ブール多項式に関しては拡張定理と零点定理が成り立つ.

定理 1 (拡張定理) Iをブール多項式環$\mathbf{B}(\bar{A},\bar{X})$のイデアルとする. このとき任意の$\bar{a}\in V(I\cap\mathbf{B}(\bar{X}))$にたいして$(\bar{a},\bar{b})\in V(I)$となる$\bar{b}$が存在する.

定理 2 (零点定理) Iをブール多項式環$\mathbf{B}(\bar{X})$のイデアルとする. このとき

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

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

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

が成り立つ.

*sinoue@rs.kagu.tus.ac.jp

3 ブーリアングレブナ基底

まず始めに係数ブール環上の多項式環でのグレブナ基底について説明する. 以降は次の記号を使用する. ある順序に対してブール多項式 f の最大の単項式を $LM(f)$ で表し,$LM(f)$ の係数と項をそれぞれ $LC(f)$ と $LT(f)$ で表す. また $f - LM(f)$ を $Rd(f)$ で表す.

定義 3 ブール多項式環 $\mathbf{B}[\bar{X}]$ のイデアル I に対して,I の有限部分集合 G が I のグレブナ基底であるとは $\langle LM(I)\rangle = \langle LM(G)\rangle$ を満たすことである.

定義 4 ブール多項式 $f = a\alpha + h \in \mathbf{B}[\bar{X}]$ による単項式簡約 $\rightarrow_f$ を

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

と定義する.
(ただし $a = LC(f), b \in \mathbf{B}, ab \neq 0$ とし,$\alpha = LT(f), \beta \in T(\bar{X}), h = Rd(f)$ とする.)

係数ブール環上のグレブナ基底の計算には次の定義が必要になる.

定義 5 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.

一般の係数体のときと違い, 簡約グレブナ基底は一意性をもたない. よって新しい条件を加える.

定義 6 G を既約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 *stratified* であるとよぶ.

定理 3 G, H を $\langle G\rangle = \langle H\rangle$ を満たす *stratified* なグレブナ基底であるとする. このとき $G = H$ が成り立つ.

係数ブール環上のグレブナ基底は上記の単項式簡約を利用したブッフバーガーアルゴリズムで計算できる.

Algoritm BC
Input: F a finite subset of $\mathbf{B}[\bar{X}]$
Output: F' a set of boolean closed polynomials such that $\langle F\rangle = \langle F'\rangle$
begin
$F' = \emptyset$
while $F \neq \emptyset$ do
  select f from F
  $F = F \backslash \{f\}$
  $F' = F' \cup \{bc(f)\}$
  $F = F \cup \{f - bc(f)\}$
end
return F'

Algoritm GB
Input: F a finite subset of $\mathbf{B}[\bar{X}]$
Output: G a Gröbner basis of $\langle F\rangle$ w.r.t >
bigin
$G = BC(F)$
while
  $G' = G$

for each pair $\{p,q\}(p,q \in G', p \neq q)$ do
h = a normal form of $S(p,q)$ modulo G' i.e. $S(p,q) \xrightarrow{*}_G h$
if $h \neq 0$ then $G = G \cup \{h\}$
$G = G'$ do
end

ブーリアングレブナ基底に関しても今までの定義や定理と同じような議論ができる. またアルゴリズムも非常にシンプルである.

定義 7 ブール多項式環 $\mathbf{B}(\bar{X})$ のイデアル I に対して,I の有限部分集合 G が I のブーリアングレブナ基底であるとは $\langle LM(I)\rangle = \langle LM(G)\rangle$ を満たすことである.

Algoritm BGB
Input: F a finite subset of $\mathbf{B}(X_1,\ldots,X_n)$
Output: G a boolean Gröbner basis of $\langle F\rangle$ w.r.t >
begin
G =GB$(F \cup \{X_1^2 - X_1,\ldots,X_n^2 - X_n\})(X_1^2 - X_1,\ldots,X_n^2 - X_n \in \mathbf{B}[\bar{X}])$
$G = G\backslash\{X_1^2 - X_1,\ldots,X_n^2 - X_n\}$
end
return G

4 集合制約問題への応用

集合制約問題に対してブーリアングレブナ基底は次のように使用される. 以下の集合制約問題に対してブール方程式系は次のようになる.

$$\begin{cases} X \cup Y \subseteq \{1,2\} \\ 1 \in X \\ 2 \in Y \\ X \cap Y = \emptyset \end{cases} \iff \begin{cases} (1+\{1,2\})(XY+X+Y) = 0 \\ \{1\}X + \{1\} = 0 \\ \{2\}Y + \{2\} = 0 \\ XY = 0 \end{cases}$$

イデアル $\langle(1+\{1,2\})(XY+X+Y), \{1\}X+\{1\}, \{2\}Y+\{2\}, XY\rangle$ に対してブーリアングレブナ基底を計算すると $\{X+\{1\}, Y+\{2\}\}$ が得られる. これは $X = \{1\}, Y = \{2\}$ を意味する. 上記のように集合制約問題をブール方程式系に表現できれば, ブーリアングレブナ基底を計算することで解くことができる. しかし集合の要素数に関する条件はブール多項式で表現できないためにブーリアングレブナ基底だけで解くことができない. 以下の記述する数独は集合の要素数に関する条件を含む集合制約問題である.

5 ブーリアングレブナ基底を使った数独の解法

数独とは 9×9 ブロックの枠内に 1 から 9 までの数字を"縦, 横, 区分けされた 3×3 ブロックに同じ数字は入れられない"というルールに従って埋めていくペンシルパズルの 1 つである. 数独は集合の要素数が 1 であるという条件を含む集合制約問題であり, ブーリアングレブナ基底を利用して解くことができる. 我々の方法は始めに 81 個のブロックに対して変数を割り当てる.

$x_{1,1}$	$x_{1,2}$	$x_{1,3}$	$x_{1,4}$	$x_{1,5}$	$x_{1,6}$	$x_{1,7}$	$x_{1,8}$	$x_{1,9}$
$x_{2,1}$	$x_{2,2}$	$x_{2,3}$	$x_{2,4}$	$x_{2,5}$	$x_{2,6}$	$x_{2,7}$	$x_{2,8}$	$x_{2,9}$
$x_{3,1}$	$x_{3,2}$	$x_{3,3}$	$x_{3,4}$	$x_{3,5}$	$x_{3,6}$	$x_{3,7}$	$x_{3,8}$	$x_{3,9}$
$x_{4,1}$	$x_{4,2}$	$x_{4,3}$	$x_{4,4}$	$x_{4,5}$	$x_{4,6}$	$x_{4,7}$	$x_{4,8}$	$x_{4,9}$
$x_{5,1}$	$x_{5,2}$	$x_{5,3}$	$x_{5,4}$	$x_{5,5}$	$x_{5,6}$	$x_{5,7}$	$x_{5,8}$	$x_{5,9}$
$x_{6,1}$	$x_{6,2}$	$x_{6,3}$	$x_{6,4}$	$x_{6,5}$	$x_{6,6}$	$x_{6,7}$	$x_{6,8}$	$x_{6,9}$
$x_{7,1}$	$x_{7,2}$	$x_{7,3}$	$x_{7,4}$	$x_{7,5}$	$x_{7,6}$	$x_{7,7}$	$x_{7,8}$	$x_{7,9}$
$x_{8,1}$	$x_{8,2}$	$x_{8,3}$	$x_{8,4}$	$x_{8,5}$	$x_{8,6}$	$x_{8,7}$	$x_{8,8}$	$x_{8,9}$
$x_{9,1}$	$x_{9,2}$	$x_{9,3}$	$x_{9,4}$	$x_{9,5}$	$x_{9,6}$	$x_{9,7}$	$x_{9,8}$	$x_{9,9}$

さらに1から9までの数字は集合の要素とする. つまり $S=\{1,2,3,4,5,6,7,8,9\}$ としたとき, 係数ブール環は $\mathbf{B}=\mathcal{P}(S)$ となる. これらの変数を用いて、数独のルールを約1000個のブール多項式で表すことができる. さらに我々はalmost solution polynomialという特殊な形のブール多項式に注目した.

定義 8 $S=\{s_1,s_2,\ldots,s_k\}$ とする. $\mathcal{P}(S)$ から $(\mathbb{GF}_2)^k$ への同型写像 ϕ を次のように与える.

$$\phi(\{s_1\})=(1,0,\ldots,0),\phi(\{s_2\})=(0,1,\ldots,0),\ldots,\phi(\{s_k\})=(0,0,\ldots,1)$$

$\mathcal{P}(S)$ から $\mathbb{GF}_2$ への同型写像 ϕ_j を次のように与える.
任意の $T\subseteq S$ に対して,

$$\phi_j(T)=\begin{cases}1 & s_j\in T\\ 0 & s_j\notin T\end{cases}$$

定義 9 変数 X_i と集合の要素 s_j に対して、次の条件のどちらかを満たすブール多項式 f,g を X_i の s_j に関する *almost solution polynomial* とよぶ.

(i) $\phi_j(f(\bar{X}))=X_i+1$

(ii) j 以外の全ての $t\in S$ に対して $\phi_t(g(\bar{X}))=X_i$

X_i の s_j に関する *almost solution polynomial* に対して $X_i+\{s_j\}$ を *associated solution polynomial* とよぶ.

almost solution polynomialは数独の解を探す重要な手がかりとなる. 我々はalmost solution polynomialが任意の項順序のブーリアングレブナ基底を計算すれば得られることを示した.

定理 4 $I\subseteq\mathbf{B}(\bar{x})$ を定数項を含まないイデアルとし,G を任意の単項式順序での I の簡約ブーリアングレブナ基底とする. 任意の *almost solution polynomialf* に対して, $f\in I$ ならば $f\in G$ となる.

ブーリアングレブナ基底を計算し, almost solution polynomial を associated solution polynomial に置き換えることで数独の空きマスに数字を埋めていくことができる. しかし常に almost solution polynomial が見つかるとは限らない. この場合は適当な associated solution polynomial を付け加えてブーリアングレブナ基底の計算を続ける必要がある. 我々の方法は与えられた数独パズルに解がない場合や複数の解がある場合にも対応している.

6 最小多項式

最小多項式を次のように定義する.

定義 10 I をブール多項式環 $\mathbf{B}(\bar{X})$ のイデアルとする. それぞれの変数 X_i に対して、*1* 変数ブール多項式 $f(X_i)$ が $I \cap \mathbf{B}(X_i) = \langle f(X_i) \rangle$ を満たすとき $f(X_i)$ を I に関する X_i の最小多項式と呼ぶ.

$\mathbb{GF}_2$ 上での最小多項式の計算は容易である.

補題 1 $I \subseteq \mathbb{GF}_2(\bar{X})$ をイデアルとし,G を任意の単項式順序での I の簡約ブーリアングレブナ基底とする. I が最小多項式 $f(X_i)$ を含むならば G は $g = cX_i + d_1t_1 + \cdots + d_lt_l + e$ を含む.

ブーリアングレブナ基底の中から almost solution polynomials を見つけ出すことで, ブール多項式環上での最小多項式に対して次の定理が得られる.

定理 5 $I \subseteq \mathbf{B}(\bar{X})$ をイデアルとし,G を任意の単項式順序での I の *stratified* ブーリアングレブナ基底とする. $I \cap \mathbf{B}(X_i) = \langle aX_i + b \rangle$ ならば G は $g = cX_i + d_1t_1 + \cdots + d_lt_l + e$ を含む. ただし $LT(g) = X_i$、$c(1 + d_1 \vee \cdots \vee d_l) = a$、$e(1 + d_1 \vee \cdots \vee d_l) = b$ とする.

7 集合制約の解法の改良

これまで associated solution polynomial を見つけるために 1 変数の多項式に注目してきた. 今回の改良では 2 変数に注目する. 2 つの変数 X_{i_1},X_{i_2} に対し. $X_{i_1} + X_{i_2}$ の最小多項式に関する次の定理が得られる.

定理 6 I をブール多項式環 $\mathbf{B}(\bar{X})$ のイデアルとする. I に関する $X_{i_1} + X_{i_2}$ の最小多項式が $(\{s_{j_1}\} + \{s_{j_2}\})(X_{i_1} + X_{i_2}) + \{s_{j_1}\} + \{s_{j_2}\}$ となるとき, $(\{s_{j_1}\} + \{s_{j_2}\} + 1)(X_{i_1} + X_{i_2})$ は *associated solution polynomial* となる.

定理 7 I をブール多項式環 $\mathbf{B}(\bar{X})$ のイデアルとする. I に関する $X_{i_1} + X_{i_2}$ の最小多項式が $(\{s_{j_1}\} + \{s_{j_2}\} + 1)(X_{i_1} + X_{i_2})$ かつ $X_{i_1}X_{i_2} \in I$ となるとき, $(\{s_{j_1}\} + \{s_{j_2}\})(X_{i_1} + X_{i_2})$ は *associated solution polynomial* となる.

この定理は $X_{i_1} + X_{i_2}$ の最小多項式を計算すれば associated solution polynomial を探せることを示している. 例えば, イデアルの中に $(\{1\} + \{2\})(X_1 + X_2) + \{1\} + \{2\}$ が含まれているとき, 集合の要素数が 1 であるという条件の下では $(\{1\} + \{2\} + 1)(X_1 + X_2)$ が associated solution polynomial となる. ただし、いくつかの注意点がある. 1 つ目に, 最小多項式の確認にはブーリアングレブナ基底の計算が必要になる. どんな順序でも良いのでブーリアングレブナ基底を計算すれば発見できる almost solution polynomials のような性質はない. 2 つ目は, 1 変数の最小多項式ならばブーリアングレブナ基底の計算は合計で 1 回となるが, 2 変数の場合は変数組合わせの個数分, ブーリアングレブナ基底の計算が必要となる. よって今回の方法は非常に計算負担が増えることが想像できる. 実際, 次の計算実験では計算時間の大幅な増加が確認できた.

8 計算実験

数独 300 問に対し, これまでの方法と新しい方法で計算実験を行った. puzzle1,2,3 はそれぞれ 100 問, 難易度は puzzle1 が易しく, puzzle3 は難しい問題となっている. ただし, この難易度はあくまで人間が解いたときに感じる難しさを基準にしている. 最小多項式を使用した新しい方法は空きマスに数字を埋める確率が高いので, これまでグレブナー基底の計算のみで解けなかった問題のいくつかは解けるようになっている. しかし, 計算時間の増加が非常に大きく, 非効率的な方法であることが分かる.

puzzle	Old method	New method
1	80	88
2	62	70
3	50	55

グレブナー基底の計算のみで解けた問題数

puzzle	Old method	New method
1	80.3	1523
2	94.7	2823
3	98.7	3123

1問解くのに必要な計算時間の平均（単位：秒）

参　献

[1] Inoue, S.(2009). On the Computation of Comprehensive Boolean Gröbner Bases. Proceedings of the 11th International Workshop on Computer Algebra in Scientific Computing(CASC 2009), LNCS 5743, pp 130-141, Springer-Verlag Berlin Heidelberg.

[2] Sakai, K. and Sato, Y. (1988). Boolean Gröbner bases. ICOT Technical Momorandum 488. http://www.icot.or.jp/ARCHIVE/Museum/TRTM/tm-list-E.html

[3] Sakai, K., Sato, Y. and Menju, S. (1991). Boolean Gröbner bases(revised). ICOT Technical Report 613.
http://www.icot.or.jp/ARCHIVE/Museum/TRTM/tr-list-E.html

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

[5] Sato, Y. et al.(1998). Set Constrains Solvers(Klic version).
http://www.jipdec.jp/icot/ARCHIVE/Museum/FUNDING/funding-98-E.html

[6] Sato, Y., Nagai, A. and Inoue, I.(2008). On the Computation of Elimination Ideals of Boolean Polynomial Rings, LNAI 5081, pp 338-348, Springer-Verlag Berlin Heidelberg.

[7] Weispfenning, V. (1989). Gröbner bases in polynomial ideals over commutative regular rings. In Davenport Ed., editor, *EUROCAL'87*, pp 336-347. Springer LNCS 378, 1989.