Title	ブーリアングレブナ基底の時間割作成問題への応用 (数式処理 : その研究と目指すもの)
Author(s)	井上, 秀太郎
Citation	数理解析研究所講究録 (2013), 1843: 51-55
Issue Date	2013-07
URL	http://hdl.handle.net/2433/195011
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
第 1843 巻 2013 年 51-55

ブーリアングレブナ基底の時間割作成問題への応用

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、我々の数独解法アルゴリズムを時間割作成問題に適用し, 有効性を検証した.

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
$G =\mathrm{GB}(F \cup \{X_1^2 - X_1,\ldots,X_n^2 - X_n\})(X_1^2 - X_1,\ldots,X_n^2 - X_n \in \mathbf{B}[\bar{X}])$
$G = G\backslash\{X_1^2 - X_1,\ldots,X_n^2 - X_n\}$
end
return G

4 ブーリアングレブナ基底を使った数独の解法

時間割作成問題の前に数独解法アルゴリズムについて説明する．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．我々は集合制約問題への有効性を示すために、ブーリアングレブナ基底を使ったこの数独パズルの解法について研究を行ってきた．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 $\mathbf{GF}_2$ 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．

5 時間割作成問題への応用

本研究では、学校の時間割作成を想定し、教科と担当教員、その教科を受講する学生のデータが与えられているとき、1 時限から 6 時限まで 5 日間を対象に制約条件を満たす時間割の作成を行う．さらに以下の制約条件を加える．

- 担当教員と学生が同じ時間帯で重複しない．
- 教員の都合の悪い時間帯に配置しない．
- 全ての教科がどこかの時間帯に配置される．
- 特定の教師や学生の負担ができる限り偏らないように配慮する．

これらの制約条件を多項式で表し、ブーリアングレブナ基底を使用する．はじめに、時間帯に表す変数を $t_1, t_2, \ldots, t_{30}$ とし、この変数を使用して $S = \{t_1, t_2, \ldots, t_{30}\}$ とおく．時間帯変数を係数とする理由は全ての教科はどこかの時間帯に配置されるが、空きの時間帯が存在することはあるからであり、集合の要素数が 1 であるという条件の下での集合制約問題に帰着させるためである．教員数を n、学生のグループ数を m とする．教科を表す変数を $s_{k,g}$ とする．ただし、$k = 1, \ldots, n$ とし、$g = 1, \ldots, m$ とする．教員と学生を同じ時間帯に配置しないために添え字のどちらかが同じである変数同士の積は空集合とする．例えば、$s_{1,2}s_{1,3} = 0$ や $s_{2,2}s_{1,2} = 0$ が成り立つ．上記の方程式の左辺を係数が $\mathcal{P}(S)$ の多項式としてブーリアングレブナ基底の計算を繰り返す．基本的な解法は数独解法アルゴリズムと同様であるが、具体的な計算には改良を施した．

集合 $S = \{t_1, t_2, \dots, t_m\}$ とブール多項式の集合の係数部分を比較し, S を係数部分に現れている集合 S_1 と現れていない集合 S_2 で分ける. almost solution polynomial がブーリアングレブナ基底に存在する場合は係数ブール環を $\mathcal{P}(S_1)$ として計算を続ける. almost solution polynomial が存在しない場合, ブーリアングレブナ基底に associated solution polynomial $v_i + \{t_j\}$ を加えて再度ブーリアングレブナ基底の計算を行う. このとき, $s_j \in S_1$ のときも係数ブール環を $\mathcal{P}(S_1)$ として計算を続ける. $t_j \in S_2$ ならば, S_1 を $S_1 + \{t_j\}$, S_2 を $S_2 - \{t_j\}$ に変えて, 係数ブール環を $\mathcal{P}(S_1)$ として計算を続ける. さらに, $v_i + \{t_j\}$ と S_2 を保存することで, 全く同じ計算を避けることができる. このように係数ブール環を少しずつ拡大させることで, 重複計算を事前に止められる. almost solution polynomial が見つからない場合には、特に大規模な重複計算が発生する。このような場合だけでも上記の対処を行うことで大幅に計算量を抑えることができる。

6 さいごに

莫大な計算量を抑えるためにはアルゴリズムの改良だけでは限界がある. 最近の研究で almost solution polynomial が他にも存在する可能性を発見している. これを発見できれば、ブーリアングレブナ基底の計算回数を減少し、分岐の数も減らすことができる.

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.