Boolean Buchberger Algorithm とその並列化 (1) - 基礎理論*

佐藤 洋祐, 毛受 哲, 佐藤 健, 岩山 登†
(財) 新世代コンピュータ技術開発機構‡

1 はじめに

ブール環上の多項式によって表現されたブール方程式は解としてその Boolean Gröbner base を一種の完備化手続きである Boolean Buchberger Algorithm によって求め解くことができる. われわれはこの方法による真偽値ブール代数に対するソルバーを並列論理型言語 KL1 により実装し評価をおこなった. 本稿では一般のブール代数に対する Boolean Gröbner base と Boolean Buchberger Algorithm について概説を与える.

2 Boolean Gröbner base

ブール代数 $(\mathrm{B}, \vee, \wedge, \neg, 0, 1)$ に対し
$x + y =_{def} (x \wedge \neg y) \vee (\neg x \wedge y), x \cdot y =_{def} x \wedge y$
と定義すると, $(\mathrm{B}, +, \cdot, 0, 1)$ は単位元 1 を持つ可換環になる. この環は次の 2 つの性質を持つ.

1. 任意の B の元 x について $x \cdot x = x$ である.
2. 任意の B の元 x について $x + x = 0$ である.

逆に単位元 1 を持つ可換環がこの 2 つの性質を持てば
$x \vee y =_{def} x + y + x \cdot y, x \wedge y =_{def} x \cdot y, \neg x =_{def} 1 + x$
によって $\vee, \wedge, \neg$ を定義することでブール代数になる. 従って上の 2 性質を持つ単位元をもつ可換環はブール代数と同一視できる. このような環をブール環と呼ぶ. ブール環 B 上の元を係数に持ち各変数の次数が 1 以下の多項式をブール多項式と呼ぶ. 各変数 X に対し $X \cdot X = X$ と置くことによってブール多項式全体もまたブール環になるが, これをブール多項式環と呼ぶ. ブール多項式の単項、すなわち含まれる変数がすべて異なる単項をブール単項と呼び, $\alpha, \beta, \gamma, \ldots$ で表す. 単項上の順序 $\geq$ が以下の性質を持つときアドミシブルな順序と呼ばれる.

1. 変数の集合として $\alpha \supseteq \beta$ なら $\alpha \geq \beta$ である.
2. $\alpha \geq \beta$ ならどんな単項 γ に対しても $\alpha\gamma \geq \beta\gamma$ である.

単項上のアドミシブルな全順序は辞書式順序に基づくもの全次数に基づくものなど色々考えられるが以下においてはそのような順序 $\geq$ を一つ固定し多項式の最大単項というときはいつもこの順序によるものとする. 最大単項として α を持つブール多項式を $a\alpha \oplus \phi$ のように表す. このブール多項式による書き換え $\Rightarrow_{a\alpha\oplus\phi}$ を次のように定義する. ブール多項式 $\varphi = \psi + ba\beta$ に対し $ab \neq 0$ なら $\varphi \Rightarrow_{a\alpha\oplus\phi} \varphi'$ である. ここで φ' は $\psi + b(1+a)\alpha\beta + ab\beta\phi$ で与えられるブール多項式である. この書き換えが妥当なものであることは以下のように説明される. まず $ba\beta = b(1+a)\alpha\beta + ba a\beta$ に注意する. 次に $a\alpha \oplus \phi = 0$ から $a\alpha = \phi$ がいえる. この両辺に $ab\beta$ をかけて $ba\alpha\beta = ba\beta\phi$ が得られる. したがって $a\alpha \oplus \phi = 0$ のもとで $ba\beta = b(1+a)\alpha\beta + ab\beta\phi$ である.

ブール多項式の集合 R に対し $\phi \Rightarrow_\varphi \psi$ なる R の元 φ が存在するとき $\phi \Rightarrow_R \psi$ と記す. また $\Rightarrow_R$ の反射推移閉包を $\stackrel{*}{\Rightarrow}_R$ で表す. つまり $\phi \stackrel{*}{\Rightarrow}_R \psi$ は 0 回以上有限回で ϕ を ψ に書き換えられることを表す.

ブール代数が真偽値ブール代数の場合, すなわち $\mathrm{B} = \{0, 1\}$ のとき, 係数として現れるのは 1 のみなので, 書き換え $\Rightarrow_{a\oplus\phi}$ は a に ϕ を代入することにほかならないことに注意されたい.

定理 2.1 どんなブール多項式の有限集合 R に対しても $\Rightarrow_R$ は停止性をもつ. つまり $\phi_0 \Rightarrow_R \phi_1 \Rightarrow_R \phi_2 \Rightarrow_R \cdots$ と無限に続く書き換えは存在しない.

定義 2.2 I をブール多項式環の有限生成イデアルとする. 有限個のブール多項式 G が以下の性質を満たすとき G は I の Boolean Gröbner base と呼ばれる.

1. $G \subseteq I$
2. $f \equiv g \pmod{I}$ (すなわち $f + g \in I$) ならばあるブール多項式 h が存在して $f \stackrel{*}{\Rightarrow}_G h, g \stackrel{*}{\Rightarrow}_G h$ が成り立つ.
3. G の元は相互に書き換えられることがない. つまりどんな $g \in G$ も g 以外の G の元 g' による書き換え $\Rightarrow_{g'}$ によって書き換えることはできない.
4. G の元の最大単項は各々異なる.

文献によっては Gröbner base の定義に条件 3 を含めないことも多い. しかし次の性質 2.3 の 3 をいうために必要なので本稿では条件 3 を要求する.
また通常の Gröbner base の場合条件 4 は条件 3 からの論理的帰結であるが, Boolean Gröbner base の場合性質

*Boolean Buchberger Algorithm and its Parallelization(1) - Basic Theory
†Yosuke Sato, Ken Satoh, Satoshi Menju, Noboru Iwayama
‡Institute for New Generation Computer Technology

3をいうためには条件4も必要になる.

性質 2.3 上で定義した Boolean Gröbner base は次の性質を持つ.

1. I の Boolean Gröbner base G が生成するイデアルは I である.
2. I によって与えられる制約すなわち連立方程式 $\{f = 0 \mid f \in I\}$ が解を持たないことと I の Boolean Gröbner base が B の元すなわち定数だけからなるブール多項式を含むことが同値になる.
3. I の Boolean Gröbner base G は一意に定まる. 従って G を I によって与えられる制約の標準形とみなすことができる.

3 Boolean Buchberger Algorithm

Boolean Gröbner base を求める Boolean Buchberger Algorithm を述べるのに必要な定義をいくつか与える. ブール多項式 $a\alpha \oplus \phi$ に対し, $a\phi + \phi$ をその係数自己要対 (coefficient self-critical pair) と呼び $csc(a\alpha \oplus \phi)$ で表す. また α の中の任意の変数 X に対し, $X\phi + \phi$ をその変数自己要対 (variable self-critical pair) と呼ぶ. ブール多項式 $a\alpha\gamma \oplus \phi, b\beta\gamma \oplus \psi$ に対し, $b\beta\phi + a\alpha\psi$ をその要対 (critical pair) と呼ぶ. ただしここで $ab \neq 0, \gamma \neq 1$, α と β は共通の変数を含まないものとする. 例えば $aXYZ \oplus bYW$ の係数自己要対は $(ab + b)YW$. 変数自己要対は $bXYW + bYW$ と $bYZW + bYW$ である. またブール多項式 $aXYZ \oplus bZ$ と $cXZW \oplus Y$ の要対は $aY + bcZW$ である. ただしここで $ac \neq 0$ とする. ブール多項式の有限集合 R とブール多項式 ϕ に対し, R の元と ϕ でつくられる要対と ϕ の変数自己要対のすべての集合を $CP(\phi, R)$ で表す.

ブール多項式の有限集合 R に対し R に含まれるブール多項式で最大単項が等しいものを足しあわせたブール多項式全体からなる集合を $Glue(R)$ で表す.
すなわち $\{a_1\alpha \oplus \phi_1, \ldots, a_n\alpha \oplus \phi_n\}$ を R の中の最大単項が α のブール多項式の集合とすると, $Glue(R)$ は $a_1\alpha \oplus \phi_1, \ldots, a_n\alpha \oplus \phi_n$ 全ての代わりに $(a_1 + \ldots + a_n)\alpha \oplus (\phi_1 + \ldots + \phi_n)$ を含む. 例えば
$R = \{aXY \oplus X, bXY \oplus Y, bXZ \oplus X, XZ \oplus Z\}$
とするとき,
$Glue(R) = \{(a+b)XY \oplus (X+Y), (b+1)XZ \oplus (X+Z)\}$
である.

ブール多項式の集合 R とブール多項式 ϕ に対し $\phi \downarrow_R$ は $\Rightarrow_R$ による ϕ の既約形の一つを表す.

定理 3.1 与えられたブール多項式の有限集合 E_0 に対し, それから生成されるイデアルの Boolean Gröbner base を求めるアルゴリズムは以下のように与えられる.

input $E \longleftarrow E_0, R \longleftarrow \emptyset$
while $E \neq \emptyset$
  choose $\phi \in E$ and $\phi' \longleftarrow \phi \downarrow_R$ ……(イ)
  if $\phi' \neq 0$ then $E \longleftarrow (E - \{\phi\}) \cup \{csc(\phi')\}$
    for every $a\alpha \oplus \psi \in R$
      if $a\alpha \Rightarrow_{\phi'} \varphi$
      then
      $E \longleftarrow E \cup \{\varphi + \psi\}, R \longleftarrow R - \{a\alpha \oplus \psi\}$
      else
      $R \longleftarrow (R - \{a\alpha \oplus \psi\}) \cup \{a\alpha \oplus (\psi \downarrow_{R \cup \{\phi'\}})\}$
      end-if
    end-for
    $E \longleftarrow E \cup CP(\phi', R), R \longleftarrow R \cup \{\phi'\}$
  else $E \longleftarrow (E - \{\phi\})$
  end-if
end-while
output $Glue(R)$ ……(ロ)

(ロ)で出力される $Glue(R)$ が求める Boolean Gröbner base である. (イ)における E の元の選択は公平でなければいけない. すなわち E のどの元もどこかで選ばれねばならない.

ブール代数が真偽値ブール代数の場合, 係数自己要対はすべて0なので考えなくてもよい. また (ロ) で出力される $Glue(R)$ は R に等しくなる.

4 謝辞

本論文に対して貴重な御意見を頂いた ICOT の研究員に感謝します.

参考文献

[1] B.Buchberger, Gröbner Bases: an Algorithmic method in Polynomial Ideal Theory, Technical Report, CAMP-LINZ, 1983.

[2] 岩山 登, 佐藤 健, 毛受 哲, 佐藤 洋祐, Boolean Buchberger Algorithm とその並列化 (2) – 動作解析, 情報処理学会第 43 回全国大会論文集, 7N-4.

[3] 佐藤 健, 毛受 哲, 岩山 登, 佐藤 洋祐, Boolean Buchberger Algorithm とその並列化 (3) – 並列アルゴリズム, 情報処理学会第 43 回全国大会論文集, 7N-5.

[4] 毛受 哲, 岩山 登, 佐藤 健, 佐藤 洋祐, Boolean Buchberger Algorithm とその並列化 (4) – 実現と評価, 情報処理学会第 43 回全国大会論文集, 7N-6.