

ブーリアン・グレブナー基底を用いたグラフ 3 彩色について

On the boolean Gröbner bases approach to the graph three-coloring problem

東京理科大学大学院理学研究科応用数学専攻 三觜奈々^{*1}

NANA MITSUHASHI

GRADUATE SCHOOL OF SCIENCE, TOKYO UNIVERSITY OF SCIENCE

東京理科大学理学部第一部応用数学科 鍋島克輔^{*2}

KATSUSUKE NABESHIMA

DEPARTMENT OF APPLIED MATHEMATICS, TOKYO UNIVERSITY OF SCIENCE

Abstract

A new algorithm for solving the graph three-coloring problem is introduced using Boolean Gröbner bases in the context of symbolic computation. It is shown that this algorithm is significantly more effective than Bayer's algorithm, which solves the problem using Gröbner bases. The results of computational experiments comparing the two algorithms are also reported.

1 はじめに

グレブナー基底を用いたグラフ 3 彩色問題の解法は, Bayer の方法として [1, 3] で紹介されている. しかしながら, グレブナー基底計算が用いているので, グラフの頂点数をすこし増やただけで計算結果が現実的な時間では返ってこないという状態になる. グレブナー基底を使用している時点で, 通常のグラフ 3 彩色問題を解くプログラムと比べると遅いのは致し方ないが, 代数的な構造に着目し離散的な問題を解いているので, 代数構造を調べることに關しては意味がある.

本稿ではグラフ 3 彩色問題をブーリアン・グレブナー基底を用いて解く方法を紹介する. ブーリアン・グレブナー基底 [6, 19, 18] とは, ブール多項式環上でのグレブナー基底のことであり, 集合制約問題を連立方程式と見なして解くことができる. 3 彩色問題は, 集合制約問題として扱うことができるため, ブーリアン・グレブナー基底を用いることにより解くことができる. 先行研究として第 2 著者により同様のテーマで研究が [12] により行われているが, 本稿はより改良されたものとなっている.

ブーリアン・グレブナー基底を用いた応用として数独の研究がある [2, 4, 5, 7, 9, 10, 11]. 数独はある意味, 81 頂点のグラフの問題と解釈することができると共に集合制約問題である. 本稿では, 数独の研究で得た手法をグラフの彩色問題の新たな解法として取り入れた. それにより, Bayer の方法より効率のよい解法を得ることができた. また得られた手法は, グラフ n 彩色問題に自然に拡張できることもわかった.

得られた解法は, Bayer の方法と共に計算機代数システム Risa/Asir[15] に実装し, 計算速度比較が行われたので, そのデータも本稿では与える.

^{*1} 〒 162-8601 東京都新宿区神楽坂 1-3 E-mail: 1423529@ed.tus.ac.jp

^{*2} 〒 162-8601 東京都新宿区神楽坂 1-3 E-mail: nabeshima@rs.tus.ac.jp

2 ブーリアン・グレブナー基底

ここでは、本稿で用いられるブーリアン・グレブナー基底について短く復習する．詳細については論文 [19] で述べられている．

定義 1

すべ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．

$\mathbb{Z}/2\mathbb{Z}$ はブール環である．また， m を自然数としたとき， $(\mathbb{Z}/2\mathbb{Z})^m$ もブール環となる．一般にべき集合はブール環と同型であると見なせる．

定義 2

$\langle \mathbf{B}, \wedge, \vee, \neg \rangle$ が次を満たすときブール代数という． $x, y, z \in \mathbf{B}$ とする．

1. $x \vee x = x \wedge x = x$
2. $x \vee y = y \vee x, x \wedge y = y \wedge x$
3. $(x \vee y) \vee z = x \vee (y \vee z), (x \wedge y) \wedge z = x \wedge (y \wedge z)$
4. $(x \vee y) \wedge x = x, (x \wedge y) \vee x = x$
5. $(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z), (x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$
6. $x \vee \neg x = 1, x \wedge \neg x = 0$

$a, b \in \mathbf{B}$ で， $a \wedge b = a \cdot b, a \vee b = a + b + a \cdot b, \neg a = 1 + a$ とすると $\langle \mathbf{B}, \wedge, \vee, \neg \rangle$ はブール代数となる．逆に， $a + b = (\neg a \vee b) \vee (a \wedge \neg b), a \cdot b = a \wedge b$ とすると， $\langle \mathbf{B}, +, \cdot \rangle$ はブール環となる．

集合を代数的に計算するとき，ブール代数がよく使われる．

定義 3

ブール環 $\mathbf{B}$ を係数にもつ多項式環 $\mathbf{B}[x_1, \dots, x_n]$ のイデアル $\langle x_1^2 - x_1, \dots, x_n^2 - x_n \rangle$ による剰余環をブール多項式環とよび， $\mathbf{B}(x_1, \dots, x_n)$ で表す．

集合制約問題を連立方程式を見なしブール代数で解くことができる理由の一つが次である．

定理 4

$\mathbf{B}(x_1, \dots, x_n)$ はブール環である．

項順序を固定する．多項式 $f \in \mathbf{B}[x_1, \dots, x_n]$ (or $\mathbf{B}(x_1, \dots, x_n)$) の先頭項を $\text{lt}(f)$ ，先頭係数を $\text{lc}(f)$ ，先頭単項式を $\text{lm}(f)$ と表す．このとき， $\text{lm}(f) = \text{lc}(f) \text{lt}(f)$ である．また，集合 $F \subset \mathbf{B}[x_1, \dots, x_n]$ (or $\mathbf{B}(x_1, \dots, x_n)$) に対して $\text{lm}(F) = \{\text{lm}(f) | f \in F\}$ とする．

定義 5

項順序を固定する．ブール多項式環 $\mathbf{B}(x_1, \dots, x_n)$ のイデアル I に対して， I の有限部分集合 G が $\langle \text{lm}(I) \rangle = \langle \text{lm}(G) \rangle$ を満たすとき， G を I のブーリアン・グレブナー基底という．

ブーリアン・グレブナー基底を計算するためのアルゴリズムは存在し実装も存在する [6, 13]．

$\mathbf{B}(x_1, \dots, x_n)$ はブール環なので $\wedge, \vee, \neg$ を集合の演算とすれば，集合の問題を $\mathbf{B}(x_1, \dots, x_n)$ 上で解くことができる．つまり， A, B を集合とするととき， $A \cup B = A + B + A \cdot B, A \cap B = A \cdot B, \neg A = 1 + A$ と定義すればよい．

3 Bayer の方法

グラフの 3 彩色問題とは、与えられたグラフを隣り合う頂点が同じ色にならないよう、3 色で塗り分けられるかどうか判定する問題である。この問題の解法として、 $\mathbb{C}[x_1, \dots, x_n]$ 上のグレブナー基底を用いる方法として Bayer の方法が知られている [1, 3]。ここでは Bayer の方法を復習する。

3.1 グラフのモデル化

G をグラフとし、 G の各頂点を $x_1, \dots, x_n$ とおく。 ω を 1 の原始 3 乗根とする。このとき、 $\omega, \omega^2, 1$ を 3 つの色とし、各頂点 x_i に $\omega, \omega^2, 1$ のうち 1 つを割り当てることを考える。このことは方程式 $x_i^3 - 1 = 0$ で表せる。また、頂点 x_i, x_j が隣接しているとき、2 つの頂点は異なる色で塗られる必要がある。従って x_i, x_j は $\omega, \omega^2, 1$ のうち異なる色を割り当てられることになり、このとき次が成り立つ。

補題 6

グラフ G の頂点 $x_i (1 \leq i \leq n)$ が $x_i^3 - 1 = 0$ を満たすとき、

$$x_i \neq x_j \iff x_i^2 + x_i x_j + x_j^2 = 0$$

が成り立つ。

3 色問題に対して、次のイデアルを定義する。

定義 7

グラフ G とその頂点 $x_1, \dots, x_n$ に対し

$$I := \langle x_i^3 - 1, x_i^2 + x_i x_j + x_j^2 \mid 1 \leq i \leq n, x_i, x_j \text{ は隣接} \rangle$$

とする。このとき、 I を G の 3 彩色イデアルという。

3.2 3 彩色判定方法

3 彩色イデアルに対して次の定理が成り立つ。

定理 8

I をグラフ G の 3 彩色イデアルとしたとき、グラフ G が

$$3 \text{ 彩色可能} \iff \mathbf{V}_{\mathbb{C}}(I) \neq \emptyset.$$

したがって、ヒルベルトの零点定理より、3 彩色イデアルの簡約グレブナー基底を計算することにより、グラフの 3 彩色問題は解くことが可能であることがわかる。次が、Bayer により紹介された方法である [1, 3]。

Bayer の方法

Step 1: グラフを 3 彩色イデアル I にモデル化する。

Step 2: I の簡約グレブナー基底 G を計算する。

Step 3: もし $G = \{1\}$ であれば G は 3 彩色不可能である。

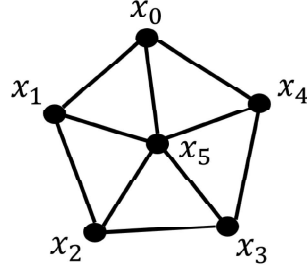
もし $G \neq \{1\}$ であれば G は 3 彩色可能である。

Bayer の方法を用いた例を次に与える.

例 1

図 1 の 6 頂点のグラフを考える. このグラフの 3 彩色イデアル I は次である.

図 1: 6 頂点のグラフ



$$I = \langle x_0^3 - 1, x_1^3 - 1, x_2^3 - 1, x_3^3 - 1, x_4^3 - 1, x_5^3 - 1, x_0^2 + x_0x_1 + x_1^2, x_0^2 + x_0x_4 + x_4^2, x_0^2 + x_0x_5 + x_5^2, x_1^2 + x_1x_2 + x_2^2, x_1^2 + x_1x_5 + x_5^2, x_2^2 + x_2x_3 + x_3^2, x_2^2 + x_2x_5 + x_5^2, x_3^2 + x_3x_4 + x_4^2, x_3^2 + x_3x_5 + x_5^2, x_4^2 + x_4x_5 + x_5^2 \rangle$$

I の簡約グレブナー基底を計算すると $\{1\}$ となるので, このグラフは 3 彩色不可能である.

4 ブーリアン・グレブナー基底を用いた 3 彩色問題の解法

ブーリアン・グレブナー基底による 3 彩色問題の解法を紹介する. ブーリアン・グレブナー基底を用いた数独の解法が [4, 5, 7, 2, 9, 10, 11] により紹介されている. この数独の解法を一般化することにより 3 彩色問題の解法を得る.

4.1 モデル化

s_1, s_2, s_3 をグラフ G の各頂点 $x_1, \dots, x_n$ に割り当てる 3 つの色とする. また集合 $\{s_1, s_2, s_3\}$ の冪集合を $\mathcal{P}(\{s_1, s_2, s_3\})$ と表す. このとき, $\mathcal{P}(\{s_1, s_2, s_3\})$ はブール環である.

頂点 x_i, x_j が隣接しているとき, x_i, x_j は s_1, s_2, s_3 のうち異なる色を割り当てられる. これは集合で表すと $x_i \cap x_j = \emptyset$ であり, $\mathcal{P}(\{s_1, s_2, s_3\})(x_1, \dots, x_n)$ 上のブール方程式に変換すると $x_i \cdot x_j = 0$ となる. ただし, 0 とは空集合のことである.

G が三角形を部分グラフとして含むとき, 三角形の頂点 x_i, x_j, x_k はそれぞれ異なる色を割り当てられる必要がある. このことは $x_i \cup x_j \cup x_k = \{s_1, s_2, s_3\}$ と表せるので $\mathcal{P}(\{s_1, s_2, s_3\})(x_1, \dots, x_n)$ 上のブール方程式に変換すると $x_i + x_j + x_k = 1$ となる. ただし, 1 とは全体集合 $\{s_1, s_2, s_3\}$ のことである.

このとき次が成り立つ.

定理 9

G をグラフとする. このときイデアル

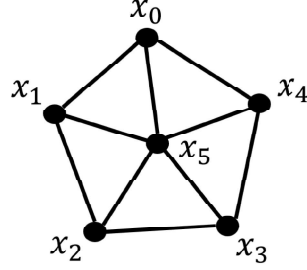
$$I := \langle x_i \cdot x_j, x_i + x_j + x_k + 1 \mid x_i, x_j \text{ は } G \text{ 内で隣接}, x_i, x_j, x_k \text{ は } G \text{ 内で三角形} \rangle$$

に対して, I のブーリアン・グレブナー基底に定数が含まれているならば, G は彩色不可能である.

しかし定理の逆、すなわち「 I のブーリアン・グレブナー基底に定数が含まれなければ 3 彩色可能」は成り立たない。以下が反例である。

例 2

例 1 と同じ次の 6 頂点のグラフを考える。



このグラフに対して、上記で定義したイデアルを考えると

$$I = \langle x_0 \cdot x_1, x_0 \cdot x_4, x_0 \cdot x_5, x_1 \cdot x_2, x_1 \cdot x_5, x_2 \cdot x_3, x_2 \cdot x_5, x_3 \cdot x_4, x_3 \cdot x_5, x_4 \cdot x_5, x_0 + x_1 + x_5 + 1, x_0 + x_4 + x_5 + 1, x_1 + x_2 + x_5 + 1, x_2 + x_3 + x_5 + 1, x_3 + x_4 + x_5 + 1 \rangle$$

であり、 I のブーリアン・グレブナー基底を計算すると $\{x_0, x_1, x_2, x_3, x_4, x_5 + 1\}$ となる。これは定数ではないが、このグラフは 3 彩色可能でないため定理の逆は成り立たない。

この計算結果は、 $x_0 = x_1 = x_2 = x_3 = x_4 = \emptyset$, $x_5 = \{s_1, s_2, s_3\}$ という解を意味している。

例 2 のようにシングルトンでない解もブール多項式から得ることができるが、我々はシングルトンの解のみが必要である。このようなことを避けるため次のようにする。

彩色をする際にあらかじめ 1 つの三角形に色を割り当てることにする。例えば、頂点 x_1, x_2, x_3 が三角形になっていたら、 $x_1 = \{s_1\}$, $x_2 = \{s_2\}$, $x_3 = \{s_3\}$ とする。これをブール方程式に変換すると、それぞれ $x_1 + s_1 = 0$, $x_2 + s_2 = 0$, $x_3 + s_3 = 0$ となる。

以上の定式化を用いて、ブール多項式環上の 3 彩色イデアルを次のように定義する。

定義 10

グラフ G から任意に三角形を 1 つ選び、その頂点を y_1, y_2, y_3 とする。このとき、グラフの各頂点 $x_1, \dots, x_n$ と、色 s_1, s_2, s_3 に対し

$$I := \langle y_1 + s_1, y_2 + s_2, y_3 + s_3, x_i \cdot x_j, x_i + x_j + x_k + 1 \mid x_i, x_j \text{ は隣接}, x_i, x_j, x_k \text{ は三角形} \rangle$$

と定義し、 I を G のブール多項式環上の 3 彩色イデアルという。

注意: グラフが三角形を 1 つも含まない場合は、任意に辺 $e(= x_i x_j)$ を 1 つ選び、その端点 x_i, x_j に $x_i = \{s_1\}$, $x_j = \{s_2\}$ というように色をあらかじめ割り当てておく。このようにしても、後に述べるアルゴリズムで 3 彩色可能性を判定することができる。

4.2 3 彩色判定方法

ここではグラフの 3 彩色判定法について述べる。ここで鍵となるのは、次の形をした多項式である。

定義 11

変数 x_i の 1 変数ブール多項式 f ($\neq 0$) を次のように分類する。

1. $f = x_i + s_k$ と書けるとき, f を解多項式という.
2. f が次のいずれかの形で書けるとき, f を半解多項式という. ただし, $s_k \neq s_l$ である.

$$f = (s_k + s_l) \cdot x_i, \quad f = (s_k + s_l) \cdot x_i + s_k$$
3. $f = s_k \cdot x_i$ と書けるとき, f を分岐多項式という.
4. f が上記のいずれの形でも書けないとき, f を矛盾多項式という.

解多項式は, 頂点に塗る色を表す. 例えば, 計算したブーリアン・グレブナー基底に式 $x_1 + s_2$ が含まれていたなら, $x_1 + s_2 = 0$ ということなので, 頂点 x_1 の色は s_2 となる.

半解多項式は, $\mathcal{P}(\{s_1, s_2, s_3\})$ 内に複数の解をもつ式である. 例えば, $(s_1 + s_2) \cdot x_1 = 0$ は, 解として $x_1 = \emptyset$ と $x_1 = \{s_3\}$ が考えられる. しかし前者の式は頂点 x_1 に色 s_1, s_2, s_3 のうちの 1 色を割り当てていることにならないため, 彩色の解ではない. このように, $\mathcal{P}(\{s_1, s_2, s_3\})$ 内に複数の解をもつが, その解のうち彩色の解になるものが 1 つのみである式を半解多項式という. 彩色であることを考えると半解多項式の解は 1 通りであるから, 半解多項式は解多項式に書き換えてよい.

分岐多項式は, 彩色の解を複数もつ式のことである. 例えば, $s_1 \cdot x_1$ は, $s_1 \cdot x_1 = 0$ ということなので彩色の解として $x_1 = \{s_2\}$ と $x_1 = \{s_3\}$ が考えられる.

矛盾多項式は, $\mathcal{P}(s_1, s_2, s_3)$ 内に解をもっているが, 彩色の解を 1 つももたない式のことである. 計算されたブーリアン・グレブナー基底に矛盾多項式が含まれていたなら, 多項式の変数には割り当てる色がないということなので, 彩色不可能と判定してよい.

次がブーリアン・グレブナー基底を用いた 3 彩色判定法である.

ブーリアン・グレブナー基底を用いた 3 彩色判定

Input: グラフ G の隣接行列 M

Output: グラフ G の 3 彩色可能性

Step 1: グラフ G をブール多項式環上の 3 彩色イデアル I にモデル化する.

Step 2: I のブーリアン・グレブナー基底 G を計算する.

Step 3: (i) G に矛盾多項式が含まれていれば, G は 3 彩色不可能.

(ここまでに分岐が発生していないか, 分岐がすべて終わってれば計算終了)

(ii) G にある半解多項式をすべて解多項式に書き換える.

Step 4: G の要素がすべて解多項式なら, G は 3 彩色可能. (計算終了)

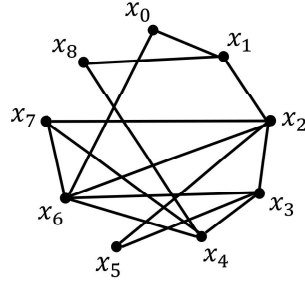
Step 5: (i) G から分岐多項式 $f(x_i)$ をとり, 解の候補のリスト $L = \{s_i | f(s_i) = 0\}$ を求める. このとき例えば $L = \{s_1, s_2\}$ なら, まず $x_i = s_1$ と仮定して (すなわち分岐多項式 $f(x_i)$ を解多項式 $x_i + s_1$ に書き換えて) Step 2 に戻る. 彩色不可能と判定されたら, 次は $x_i = s_2$ と仮定して Step 2 に戻る.

(ii) G から 2 変数多項式 g をとり, 解の候補のリスト $L = \{(s_i, s_j) | g(s_i, s_j) = 0\}$ を求める. (i) と同様, L の各元を仮定して (g を対応する解多項式に書き換えて) Step 2 に戻る.

このアルゴリズムは実際, グラフの彩色をしており 1 通りでも彩色ができれば彩色可能を返す.

例 3

次のグラフの 3 彩色判定をブーリアン・グレブナー基底を用いて行う.



このグラフのブール多項式環上の 3 彩色イデアルは

$$I = \langle s_1 + x_2, s_2 + x_3, s_3 + x_5, x_4 + x_7 + x_6 + 1, x_2 + x_7 + x_6 + 1, x_3 + x_2 + x_6 + 1, x_6 \cdot x_7, x_8 \cdot x_4, x_7 \cdot x_4, x_6 \cdot x_4, x_6 \cdot x_3, x_3 \cdot x_5, x_7 \cdot x_2, x_6 \cdot x_2, x_2 \cdot x_5, x_2 \cdot x_3, x_8 \cdot x_1, x_1 \cdot x_2, x_6 \cdot x_0, x_0 \cdot x_1 \rangle$$

であり I のブーリアン・グレブナー基底を計算すると

$$\{x_0 \cdot x_1 \cdot s_2, x_0 \cdot s_1 + x_0 \cdot s_2 + x_0, x_8 \cdot x_1 \cdot s_1 + x_8 \cdot x_1, x_1 \cdot s_1, s_1 + x_2, s_2 + x_3, s_1 + x_4, s_3 + x_5, s_1 + s_2 + x_6 + 1, s_2 + x_7, x_8 \cdot s_1\}$$

となる．このブーリアン・グレブナー基底に含まれる $x_8 \cdot s_1$ は分岐多項式であり， $x_8 \cdot s_1 = 0$ のシングルトン解は， $x_8 = \{s_2\}$ と $x_8 = \{s_3\}$ である． $x_8 = \{s_3\}$ と仮定，すなわち $x_8 \cdot s_1$ を $x_8 + s_3$ に書き換えてブーリアン・グレブナー基底をもう一度計算すると，

$$\{s_3 + x_8, s_2 + x_7, s_3 + x_6, s_3 + x_5, s_1 + x_4, s_2 + x_3, s_1 + x_2, s_2 + x_1, s_1 + x_0\}$$

となり，要素がすべて解多項式となったためこのグラフは 3 彩色可能である．

5 ブーリアン・グレブナー基底による 4 彩色問題の解法

4 彩色問題とは，与えられたグラフが，隣接する頂点が同色にならないよう 4 色で塗り分けられるかどうかを判定する問題である．前節で述べた 3 彩色問題の判定方法と同様の手法で，4 彩色問題を解くことができる．

5.1 モデル化

s_1, s_2, s_3, s_4 をグラフ G の各頂点 $x_1, \dots, x_n$ に割り当てる 4 つの色とし，集合 $\{s_1, s_2, s_3, s_4\}$ の冪集合を $\mathcal{P}(\{s_1, s_2, s_3, s_4\})$ と表す．このとき， $\mathcal{P}(\{s_1, s_2, s_3, s_4\})$ はブール環である．頂点 x_i, x_j が隣接しているとき， x_i, x_j は s_1, s_2, s_3, s_4 のうち異なる色を割り当てられる．これは集合で表すと $x_i \cap x_j = \emptyset$ であり， $\mathcal{P}(\{s_1, s_2, s_3, s_4\})(x_1, \dots, x_n)$ 上のブール方程式に変換すると $x_i \cdot x_j = 0$ となる．

G が 4 頂点の完全グラフ K_4 を部分グラフとして含むとき， K_4 の頂点 x_i, x_j, x_k, x_l はそれぞれ異なる色を割り当てられる必要がある．このことは $x_i \cup x_j \cup x_k \cup x_l = \{s_1, s_2, s_3, s_4\}$ と表せるので $\mathcal{P}(\{s_1, s_2, s_3, s_4\})(x_1, \dots, x_n)$ 上のブール方程式に変換すると $x_i + x_j + x_k + x_l = 1$ となる．

彩色をする際にあらかじめ 1 つの K_4 に色を割り当てることにする．例えば，頂点 x_1, x_2, x_3, x_4 が K_4 になっていたら， $x_1 = \{s_1\}$, $x_2 = \{s_2\}$, $x_3 = \{s_3\}$, $x_4 = \{s_4\}$ という式を立てる．ブール方程式に変換すると，それぞれ $x_1 + s_1 = 0$, $x_2 + s_2 = 0$, $x_3 + s_3 = 0$, $x_4 + s_4 = 0$ となる．

以上の定式化を用いて，ブール多項式環上の 4 彩色イデアルを次のように定義する．

定義 12

グラフ G から任意に K_4 を 1 つ選び, その頂点を y_1, y_2, y_3, y_4 とする. このとき, グラフの各頂点 $x_1, \dots, x_n$ と, 色 s_1, s_2, s_3, s_4 に対し

$$I = \langle y_1 + s_1, y_2 + s_2, y_3 + s_3, y_4 + s_4, x_i \cdot x_j, x_i + x_j + x_k + x_l + 1 \mid x_i, x_j \text{ は隣接}, x_i, x_j, x_k, x_l \text{ は } K_4 \rangle$$

と定義し, I を G のブール多項式環上の 4 彩色イデアルという.

5.2 4 彩色判定方法

1 変数多項式の分類は, 4 彩色の場合は次の形になる.

定義 13

変数 x_i の 1 変数ブール多項式 $f (\neq 0)$ を次のように分類する.

1. $f = x_i + s_k$ と書けるとき, f を解多項式という.
2. f が次のいずれかの形で書けるとき, f を半解多項式という.

$$f = (s_k + s_l + s_m) \cdot x_i, \quad f = (s_k + s_l + s_m) \cdot x_i + s_k, \quad f = (s_k + s_l) \cdot x_i + s_k$$

3. f が次のいずれかの形で書けるとき, f を分岐多項式という.

$$f = s_k \cdot x_i, \quad f = (s_k + s_l) \cdot x_i$$

4. f が上記のいずれの形でも書けないとき, f を矛盾多項式という.

これらを用いて, 以下のアルゴリズムで 4 彩色可能性を判定する.

ブーリアン・グレブナー基底を用いた 4 彩色判定

Input: グラフ G の隣接行列 M

Output: グラフ G の 4 彩色可能性

Step 1: グラフ G をブール多項式環上の 4 彩色イデアル I にモデル化する.

Step 2: I のブーリアン・グレブナー基底 G を計算する.

Step 3: (i) G に矛盾多項式が含まれていれば, G は 4 彩色不可能.

(ここまでに分岐が発生していないか, 分岐がすべて終わっていれば計算終了)

(ii) G にある半解多項式をすべて解多項式に書き換える.

Step 4: G の要素がすべて解多項式なら, G は 4 彩色可能. (計算終了)

Step 5: (i) G から分岐多項式 $f(x_i)$ をとり, x_i の解の候補を求める.

各解の候補をそれぞれ仮定しての Step 2 を実行する.

(ii) G から 2 変数多項式 $f(x_i, x_j)$ をとり, x_i, x_j の解の候補の組を求める.

(i) と同様, 各解の候補をそれぞれ仮定して Step 2 を実行する.

6 n 彩色の場合

一般の n 彩色についても、3 彩色と同様の方法で判定できる。

6.1 $\mathbb{C}[x_1, \dots, x_n]$ 上のグレブナー基底を用いた方法

グラフ G の各頂点を $x_1, \dots, x_k$ とおく。 α を 1 の n 乗根とし、 $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ を頂点に割り当てる n 個の色とすると、各 x_i に対して $x_i^n - 1 = 0$ が成り立つ。また x_i, x_j が隣接しているとき、次が成り立つ。

補題 14

グラフ G の頂点 x_i ($1 \leq i \leq k$ が $x_i^n - 1 = 0$ を満たすとき、

$$x_i \neq x_j \iff \sum_{l=0}^{n-1} x_i^{n-l-1} x_j^l = 0.$$

従って、グラフの n 彩色イデアルを次のように定義する。

定義 15

グラフ G とその頂点 $x = 1, \dots, x_k$ に対し

$$I := \left\langle x_i^2 - 1, \sum_{i=0}^{n-1} x_i^{n-l-1} x_j^l \mid 1 \leq i \leq k, x_i, x_j \text{ は隣接} \right\rangle$$

と定義でし、 I を G の n 彩色イデアルという。

n 彩色の時も、3 彩色同様に定理 8 が成り立つ。すなわち、 n 彩色イデアルの k 簡約グレブナー基底が $\{1\}$ ならば、 n 彩色不可能であり、 $\{1\}$ でなければ n 彩色可能である。

$\mathbb{C}[x_1, \dots, x_n]$ 上のグレブナー基底を用いた n 彩色判定法

Step 1: グラフを n 彩色イデアル I にモデル化する。

Step 2: I の簡約グレブナー基底 G を計算する。

Step 3: もし $G = \{1\}$ であれば G は n 彩色不可能である。

もし $G \neq \{1\}$ であれば G は n 彩色可能である。

6.2 ブーリアン・グレブナー基底を用いた方法

グラフの頂点を $x_1, \dots, x_k$ とおき、 $s_1, \dots, s_n$ を頂点に割り当てる n 個の色とする。頂点 x_i, x_j が隣接しているとき、 x_i, x_j は $s_1, \dots, s_n$ のうち異なる色を割り当てられる必要があり、このことは $\mathcal{P}(\{s_1, \dots, s_n\})(x_1, \dots, x_k)$ 上のブール方程式で $x_i \cdot x_j = 0$ と表せる。また、 G が K_n (n 頂点の完全グラフ) を部分グラフとして含むとき、 K_n の頂点 $y_1, \dots, y_n$ はそれぞれ異なる色を割り当てられる必要がある。このことは $\mathcal{P}(\{s_1, \dots, s_n\})(x_1, \dots, x_k)$ 上のブール方程式で $y_1 + \dots + y_n = 1$ と表せる。さらに、彩色をする際にあらかじめ 1 つの K_n に色を割り当てておくことを考える。例えば頂点 $y_1, \dots, y_n$ が K_n になっていたら $y_1 = \{s_1\}, \dots, y_n = \{s_n\}$ という式を立てる。

以上の定式化を用いて、ブール多項式環上の n 彩色イデアルを次のように定義する。

定義 16

グラフ G から任意に K_n を 1 つ選び, その頂点を $y_1, \dots, y_n$ とする. このとき, グラフの各頂点 $x_1, \dots, x_k$ と, 色 $s_1, \dots, s_n$ に対して

$$I := \langle y_1 + s_1, \dots, y_n + s_n, x_i \cdot x_j, x_{n1} + \dots + x_{nn} + 1 \mid x_i, x_j \text{ は隣接}, x_{n1}, \dots, x_{nn} \text{ は } K_n \rangle$$

と定義し, I を G のブール多項式環上の n 彩色イデアルという.

1 変数多項式を次のように分類する.

定義 17

変数 x_i の 0 でない 1 変数ブール多項式 f を次のように分類する.

1. $f = x_i + s_k$ と書けるとき, f を解多項式という.

2. f が次の形で書けるとき, f を半解多項式という.

$$(a) T = \{T' \subset \{s_1, \dots, s_n\} \mid |T'| = n - 1\}, M \in T \text{ に対して, } (\sum_{s_k \in M} s_k) \cdot x_i.$$

$$(b) T = \{T' \subset \{s_1, \dots, s_n\} \mid |T'| \leq n - 1\}, M \in T \text{ に対して, } (\sum_{s_k \in M} s_k) \cdot x_i + s_k.$$

3. f が次の形で書けるとき, f を分岐多項式という.

$$T = \{T' \subset \{s_1, \dots, s_n\} \mid |T'| < n - 1\}, M \in T \text{ に対して, } (\sum_{s_k \in M} s_k) \cdot x_i.$$

4. f が上記のいずれの形でも書けないとき, f を矛盾多項式という.

次がブーリアン・グレブナー基底を用いたグラフ n 彩色の判定法である.

ブーリアン・グレブナー基底を用いた n 彩色判定

Input: グラフ G の隣接行列 M

Output: グラフ G の n 彩色可能性

Step 1: グラフ G をブール多項式環上の n 彩色イデアル I にモデル化する.

Step 2: I のブーリアン・グレブナー基底 G を計算する.

Step 3: (i) G に矛盾多項式が含まれていれば, G は n 彩色不可能.

(ここまでに分岐が発生していないか, 分岐がすべて終わっていれば計算終了)

(ii) G にある半解多項式をすべて解多項式に書き換える.

Step 4: G の要素がすべて解多項式なら, G は n 彩色可能. (計算終了)

Step 5: (i) G から分岐多項式 $f(x_i)$ をとり, x_i の解の候補を求める. 各解の候補をそれぞれ仮定して Step 2 を実行する.

(ii) G から 2 変数多項式 $f(x_i, x_j)$ をとり, x_i, x_j の解の候補の組を求める. (i) と同様, 各解の候補をそれぞれ仮定してを仮定して Step 2 を実行する.

7 比較

本稿で紹介した『グレブナー基底を用いる Bayer の方法』(方法 1) と、『ブーリアン・グレブナー基底を用いた方法』(方法 2) は計算機代数システム Risa/Asir 上 [15] に実装した. 本節では, 3 彩色と 4 彩色の場合の計算時間を比較した. 使用した計算機は, OS: Windows 11, CPU: Interl(R), COre(TM) i9-10980XE@ 3.00GHz, メモリー 256GB であり, 数値は CPU 秒を表し, $> 3h$ は 3 時間経過しても出力が返ってこないことを意味する.

表 1 は与えられたグラフの 3 彩色可能性判定の計算時間を比較した. 測定に使用したグラフはすべて K_4 を部分グラフとして含まない連結グラフである.

表 1 方法 1 と方法 2 による計算時間の比較 (3 彩色)

頂点数	3 彩色可能性	方法 1	方法 2
10	不可	0	0
20	可	0.01562	0
30	不可	0.09375	0
40	可	0.5938	0.1094
50	不可	4039.6	0.1875
60	可	3.609	0.3125
70	不可	4.531	0.4844
80	可	14.88	1.75
90	不可	24.88	0.8594
100	可	84.09	2.203
110	不可	61.75	1.516
120	可	171.1	5.844
130	不可	159.7	4.234
140	可	455.7	31.69
150	不可	410.9	6.203

表 2 は与えられたグラフの 4 彩色可能性判定の計算時間を比較した. 測定に使用したグラフはすべて K_5 を部分グラフとして含まない連結グラフである.

表 1, 表 2 ではすべての頂点数において, ブーリアン・グレブナー基底を用いた方法の方が, $\mathbb{C}[x_1, \dots, x_n]$ 上のグレブナー基底を用いた Bayer の方法よりも圧倒的に速い. これは, ブーリアン・グレブナー基底の計算の速さが影響している. ブーリアン・グレブナー基底計算は, 係数膨張が起こらず各変数の次数も最大 1 ということが影響している.

表 2 方法 1 と方法 2 による計算時間の比較 (4 彩色)

頂点数	4 彩色可能性	方法 1	方法 2
10	不可	0.0625	0
20	可	>3h	0.1719
30	不可	10638.4	0.1562
40	可	>3h	0.8594
50	不可	>3h	4.375
60	可	>3h	8.172
70	不可	>3h	40.16
80	可	>3h	36.02
90	不可	>3h	127.9
100	可	>3h	109.2
110	不可	>3h	391.3
120	可	>3h	495.5
130	不可	>3h	777.5
140	可	>3h	1987
150	不可	>3h	3377

8 まとめと今後の研究

ブーリアン・グレブナー基底を用いてグラフの 3 彩色問題を解く方法を構成した．また，その方法を一般化することにより，4 彩色，任意の n 彩色についても問題を解けることがわかった．

グラフ 3 彩色問題の応用として生体認証セキュリティがある [16, 17]．これは，グラフの 3 彩色の難しさを利用したもので，3 彩色の難しいグラフを利用している．3 彩色の難しいグラフの構成は論文 [8] や [17] で議論しているが、『難しい (very hard)』ということについては，3 彩色を解くプログラムの実行時間で判断している．ブーリアン・グレブナー基底を用いた数独の難易度判定の研究 [5, 7, 9, 10, 11, 18] があり，同様の方法で，グラフの 3 彩色の『難しさ』に対する定義付けをすることが可能であると思われる．これは，ブーリアン・グレブナー基底を用いているからこそ可能となることであり，3 彩色の『難しさ』の数学的な定義が今後の研究課題である．

参 考 文 献

- [1] W. Adams and P. Loustau: An Introduction to Gröbner Bases, AMS, 1994
- [2] K. Arai, H. Watanabe On the Inoue invariants of the puzzles of Sudoku type. Communications of JSSAC, Vol.2 1–14, 2016
- [3] D. Bayer: The division algorithm and the Hilbert scheme, Ph.D. Thesis, Harvard University, 1982

- [4] 井上秀太郎, 佐藤洋祐, 鈴木晃, 鍋島克輔: ブーリアングレブナ基底を使った数独の解法, 数理解析研究所講究録, 第 1666 巻, pp.1–5, 2009
- [5] 井上秀太郎, 佐藤洋祐: グレブナ基底を使った数独の難易度判定と問題作成, 数理解析研究所講究録, 第 1785 巻, pp.51–56, 2012
- [6] S. Inoue: Efficient singleton set constraint solving by Boolean Gröbner bases, Communicaion of JSSAC, Vol.1, pp.27–38, 2012
- [7] S. Inoue and Y. Sato: A mathematical hierarchy of sudoku puzzles and its computation by Boolean Gröbner bases. Proc. 12th International Conference, AISC2014, Lecture Notes in Artificial Intelligence, Springer (LNAI 8884) pp.88–98, 2014
- [8] M. Kazunori and S. Nishihara: Constructive generation of very hard 3 – colorbilty instances. Discrete Applied Mathematics, Vol. 156, No.2, 218–229, 2008
- [9] T. Nakano, Y. Maruyama and S. Ohki On the mathematical evaluation of difficulty level of Sudoku puzzles by Boolena Gröbner bases. Far East Journal of Applied Mathematics, Vol. 106, 43–70, 2020
- [10] T. Nakano, M. Shindou, N. Mikoshiba and T. Yoshihara: The SMYI invariant and the MDSL conjecture in the CII algorithm for solving Sudoku puzzles. Far East Journal of Applied Mathematics, Vol. 114, 25–48, 2022
- [11] 中野哲夫, 進藤未来, 吉原元: Boolean Gröbner 基底を用いた数独パズルの数学的難易度指標の相関について. 数理解析研究所講究録, 第 2255 巻, pp.1–13, 2023
- [12] 鍋島克輔, 杉原彩: ブーリアン・グレブナー基底を用いたグラフ 3 彩色問題へのアプローチについて. 数理解析研究所講究録, 第 1906 号, pp.116–121.2014
- [13] A. Nagai and Y. Sato: An efficient implementation of Boolean Gröbner bases of a power set algebra. Proc. the 20th Asian Technology Conference in Mathematics(ATCM 2015), pp. 326–335, 2015
- [14] A. Nagai and Y. Sato: Parallel and distributed Boolean Gröbner bases computation in SageMath. Proc. the 21st Asian Technology Conference in Mathematics (ATCM 2016), pp. 269–278, 2016
- [15] M. Noro and T. Takeshima: Risa/Asir - A computer algebra system. *Proc. ISSAC 1992*, pp. 387–396, ACM, 1992. <http://www.math.kobe-u.ac.jp/Asir/asir.html>
- [16] 小田雅洋, 菊池浩明, 尾形わかは, 西垣正勝: G3C-ZKIP を用いた非対称性生体認証. コンピュータセキュリティシンポジウム 2008 論文集, pp. 695–700, 2008
- [17] 小田雅洋, 渡邊幸聖, 山本匠, 尾形わかは, 菊池浩明, 西垣正勝: グラフ 3 彩色問題を用いた非対称生体認証方式に対する検討. 社団法人映像情報メディア学会技術報告, VoL33, No. 54, pp. 53–56, 2009
- [18] Y. Sato, A. Nagai and S. Inoue: On the computation of elimination ideals of Boolean polynomial rings. Lecture Notes in Artificial Intelligence, Springer 5081, 334–348, 2008
- [19] Y. Sato, S. Inoue, A. Suzuki, K. Nabeshima and K. Sakai: Boolean Gröobner bases, Journal of symbolic Computation, Vol.46, No.5, pp.622–632, 2011