# ZKIPを実現するために組合せ問題を基本機能に分解する枠組み

岩崎 豪† 上嶋 章宏††
† 大阪電気通信大学大学院 †† 大阪電気通信大学大学院

## 1 はじめに

ランダム性と計算の関係は，最近2，30年の間に明らかにされた科学的発見の中でも最も魅力的なものの1つである．特に，確率的証明における多くの興味深い結果の1つとして，ゼロ知識証明（ZKIPと略記する）が挙げられ，誤り確率を導入することで誤りのない証明系よりもさらに強力かつ有用な証明系である．ゼロ知識証明は，知識が正しいという事実以外は何も検証者に伝えずに正しさを確信させるという性質を持ち，この性質を利用し，公開鍵暗号，ユーザ認証などに対しゼロ知識証明が用いられている [1].

ゼロ知識証明に関する結果の1つとして，クラスNPに属す全ての問題に対してゼロ知識証明を達成するプロトコルの設計が可能であり，3-彩色問題においてゼロ知識証明を実現する具体的なプロトコルも提示している [2].

一般に，全ての組合せ問題は，いくつかの基本的な性質を組み合わせて定められる条件群を満足する解を要請する問題と言え，その基本性質ごとに，3-彩色問題上で利用可能なグラフ構造を予め設計しておき，それらを適時組み合わせることで，個別的な還元方法の設計に要する手間を軽減できる可能性があると言える．

本稿では，基本性質・機能を表現するグラフ構造をベースに，組合せ問題を基本機能の組み合わせと捉え，それらに対し3-彩色問題への還元を容易に行うための枠組みの設計を試みる．

## 2 準備

本稿では，いくつかの集合の組で表現される入力に対し，要件を満たす部分集合あるいは部分集合族等の検出を目的とする組合せ問題を対象とする．例えば，入力グラフから様々な条件を満たす（1つ以上の）部分グラフを導出する問題などがそれに当たる．

組合せ問題の入力に集合 $S = \{s_1, s_2, \cdots, s_n\}$ が含まれ，ある条件を満たす $S$ の部分集合族 $\mathcal{S} = \{S_1, S_2, \cdots, S_p\}$ を導出することを考える．集合族 $\mathcal{S}$ が満たすべき条件は問題によって様々であるが，いずれも素朴な性質・機能の組み合わせによって表現される．入力される乗法標準形の論理式を真とする変数への真理値割り当てが存在するかを問うSATを一例として考える．本問題の解の条件は，(1) 各変数に真理値が割り当てられていること，(2) 各節に真を取るリテラルが少なくとも1つ存在すること，(3) 全ての節が (2) の条件を満足することの3つの性質を満たすことに相当する．他の様々な問題に関しても同様のことが言え，基本的な性質という観点では共通する項目が多く存在する．

そこで本研究では，3-彩色問題への具体的な還元方法の設計を容易にする目的で，以下に挙げる基本的な性質に注目し，それらの基本性質を3-彩色問題上で再現する仕組みを考える．

集合 $S$ の部分集合 $S_1, S_2, \cdots, S_p$ に対し，各集合 $S_i$ の要素数が，入力として与えられた数値 $k$ と等しいかを問われる状況は，様々な問題で現れる．サイズ $k$ のクリークが存在するかを問うクリーク問題などはその一例である．その際，各集合 $S_i$ の要素数を計算し，その結果が $k$ と等しいか否かを判定できる機能を3-彩色問題上で実現する必要がある．本稿では，このような機能を数え上げと呼ぶ．

また，部分集合族 $\mathcal{S}$ が集合 $S$ の分割であることが解の必要条件である場合も多い．例えば，$n$ 個の整数からなる集合 $S$ を2分割し，各集合内の数値の合計を等しくする分割問題では，$|\mathcal{S}| = 2$ の分割であることを確認する必要がある．以降，このような機能を分割と呼ぶ．

グラフ $(V, E)$ における頂点集合 $V$ 上での2頂点間の関係を示す辺集合 $E$ のように，集合 $S$ の要素間でのある関係を入力とする問題形式は一般的である．そのため，上記の数え上げ機能や分割機能などの集合 $S$ 上での性質を判定する機能だけでなく，各部分集合 $S_i$ 内の要素間に問題の要請上必要な関係が成立するかを判断する機能（以降，関係付けと呼ぶ）を考慮する必要がある．

次節では上記の基本機能について3-彩色問題上での実現方法を略説し，これらの機能を組み合わせて3-彩色問題への還元を実現できる問題の一例を4節で示す．

## 3 基本的性質の3-彩色問題における表現

グラフ $G = (V, E)$ の3-彩色 $f$ を $f : V \to \{0, 1, 2\}$ と定義する．以下では，2節で示した各機能を実現す

---

A Framework for Decomposing Combinatorial Problems into Basic Features to Realize ZKIP

† Go Iwasaki · Graduate School of Engineering, Osaka Electro-Communication University
†† Akihiro Uejima · Graduate School of Engineering, Osaka Electro-Communication University

るグラフ構造に対し，各グラフの 3-彩色 $f$ がどのように制限されるかを略説し，必要な機能を有するグラフであることを示す．以下の議論において，彩色 $f$ での色 1 は変数への真割り当てあるいは数値としての 1 など肯定的な意味を表現し，色 0 は逆に偽割り当てあるいは数値 0 などを表現するよう構成される（詳細は省略）．

まず，部分集合 $S_i \subseteq S$ をグラフ上で表現する必要がある．$|S| = n$ より，各 $S_i$ に対し $n$ 頂点 $v_1^i, v_2^i, \cdots, v_n^i$ を用意し，任意の $j \in \{1, 2, \cdots, n\}$ に対し $s_j \in S_i$ ならば $f(v_j^i) = 1$，$s_j \notin S_i$ ならば $f(v_j^i) = 0$ と彩色されるような $n$ 頂点からなるグラフにより部分集合 $S_i$ を表現する．

以下に，2 節で記述した数え上げにおける仕組み，グラフ構造を説明する．

部分集合 $S_i$ を表現する上記グラフの彩色 $f$ を基に，数え上げのグラフを彩色することによって 2 進数の計算を行う．

2 進数の計算を行うにあたり数値を格納する領域が必要となる．$|S| = n$ より，$|S_i|$ は高々 $n$ であり，$|S_i|$ は，$O(\log n)$ ビットの 2 進数で表現可能である．また，0 または 1 を毎回 $n$ 回加算するので，数え上げを表現するには，$O(n)$ 個の領域を確保する必要がある．確保した領域に 2 進数である 0 と 1 のビット列を表現し，最下位ビットの加算を行うと 1 ビット目の結果と桁上がりの有無が分かり，半加算器の機能を果たす．上記の操作を $O(\log n)$ 個の領域全てに対して行うことで，2 進数の加算を行うことができる．

半加算器の機能を果たすグラフ構造を図 1 に示す．

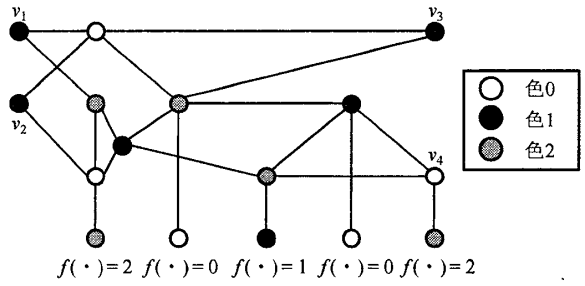


図 1: 半加算器を表現するグラフ構造

$v_1$, $v_2$ を入力とし，$v_3$ を桁上がり，$v_4$ を同桁の加算結果として出力とする．図 1 のグラフにおいて，下部 5 点は図のように彩色を固定でき，$f(v_1), f(v_2) \in \{0, 1\}$ と仮定できる（詳細は省略）．

2 入力に対応する 2 頂点 $v_1$, $v_2$ に対する彩色 $f$ の場合分けを以下に示す．$f(v_1)$, $f(v_2) = 0$ のとき，$f(v_3)$, $f(v_4) = 0$ となる．同様に，$(f(v_1), f(v_2)) \in \{(0, 1), (1, 0)\}$ のとき，$f(v_3) = 0$, $f(v_4) = 1$ となる．さらに，$f(v_1)$, $f(v_2) = 1$ のとき，$f(v_3) = 1$, $f(v_4) = 0$ となる．

数え上げを行うグラフ構造に対する構成時間は，$O(\log n) \times O(n)$ の領域が存在するため，$O(n \log n)$ で構成可能である．

また，半加算器の機能をもつグラフは，XOR ゲートを表現しており，AND，OR，NOT ゲートを表現するグラフも半加算器のグラフと同様に構成できる．例えば，集合 $S$ を部分集合 $S_i$, $S_j$ に分割し，2 つの部分集合が互いに素の関係であるかを問う場合，構成されたグラフのそれぞれの頂点について，XOR ゲートの役割を果たす 3-彩色問題のグラフを構成すれば，$S_i$, $S_j$ が互いに素であるかどうかを確認でき，分割を表現することができる．

## 4 3-彩色問題で表現できる組合せ問題

本節では，組合せ問題と見なすことができる Spiral Galaxy Puzzles（以下，SGP と呼ぶ）について以下に記述する．

SGP とは，四角格子状に配置された盤面と盤面上に配置された円集合を入力とし，円を中心とした点対称図形で盤面を過不足なく区切れるかを問う問題である．本問題の解の条件は，(1) 円を中心に区切った図形は点対称であること，(2) 点対称図形は隣接するマスと連結していること，(3) 盤面に存在する各マスが複数の点対称図形に含まれないこと，この 3 つの条件を満足することである．(1)，(2) は関係付け，(3) は分割と捉えることができ，それぞれに対応するグラフを構成することにより 3-彩色問題で表現できる．

## 5 まとめ

本研究では，既存の 3-彩色問題のゼロ知識証明プロトコルを用いるために組合せ問題を基本機能に分解し，3-彩色問題への多項式時間還元できる枠組みの構成を行った．これにより，組合せ問題を 3-彩色問題へ還元することでゼロ知識証明を行うことができる．

今後の課題として，論理ゲートを組み合わせることによる基本機能の追加が挙げられる．

## 参考文献

[1] O. Goldreich (著), 岡本 龍明, 藤崎 英一郎 (訳), **現代暗号・確率的証明・擬似乱数**, シュプリンガー・フェアラーク東京, 2001.

[2] O. Goldreich, S. Micali, A. Wigderson, "Proofs that Yield Nothing But Their Validity or All Languages in NP Zero-Knowledge Proof Systems," J. of ACM, Vol. 38, No. 1, pp. 691-729, 1991.