

2020 年度
修士論文

k -極大独立集合検証問題の
分散計算複雑性

Distributed Complexity of k -Maximal
Independent Set Verification

名古屋工業大学 大学院工学研究科 博士前期課程

情報工学専攻

片山・金研究室所属

2019 年度入学

学生番号：31414050 氏名：佐藤 僚祐

目次

第1章	はじめに	1
1.1	研究背景	1
1.2	本研究の目的と結果	2
1.3	関連研究	3
1.4	本研究の成果	3
1.5	論文の構成	4
第2章	諸定義	5
2.1	CONGEST モデル	5
2.2	2 者間通信複雑性	5
2.3	k -極大独立集合	7
2.4	k -極大独立集合検証問題	7
第3章	1-MIS 検証問題の $O(1)$ ラウンドアルゴリズム	8
第4章	k-MIS 検証問題の下界	10
4.1	2-MIS 検証問題の下界	10
4.2	3-MIS 検証問題の下界	13
4.3	k -MIS 検証問題の下界	16
第5章	まとめと今後の課題	21
5.1	まとめ	21
5.2	今後の課題	21

第1章

はじめに

1.1 研究背景

(句点と読点は全角の、と. にする) 分散グラフアルゴリズムとは、計算機を頂点、辺を通信リンクとみなしてネットワークをモデル化したグラフ上において、そのネットワーク自身を入力としてグラフに対して定義される諸問題を解く枠組みである。分散アルゴリズムにおける代表的なモデルのひとつとして CONGEST モデルが存在する。CONGEST モデルにおいて、各ノードは同期ラウンドに従って実行され、メッセージ交換によって協調動作を行う。各ノードは各ラウンドで (i) b ビットのメッセージを隣接ノードに送信 (ii) 隣接ノードからメッセージを受信 (iii) 内部計算の 3 つの動作をする。特に CONGEST モデルでは $b = O(\log n)$ が仮定される。CONGEST モデルにおいて、ある 1 つのノードにグラフ全体のトポロジの情報を集め、そのノード上で逐次アルゴリズムを実行するという素朴なアプローチから、任意の問題に対して自明に $O(n^2)$ ラウンドの上界を得ることができる。CONGEST モデルにおける下界の証明では、下界が $\Omega(n^2)$ ラウンドにどれだけ近づけることができるかに興味がある。

本研究ではグラフ上の最適化問題の一つである、最大独立点集合に注目する。CONGEST モデルにおいて、ネットワーク上の最大独立集合あるいはその近似解を発見する数多くの分散グラフアルゴリズムが研究されている。大きなサイズの独立集合は経済学、計算生物学、符号理論、実験計画法など様々な分野への応用に用いられる [1] が、そもそも最大独立集合問題は NP 完全であり、頂点数 n に対して n の多項式時間で解くことは、その近似を含めて絶望的であるとされている。分散グラフアルゴリズムの文脈からは、各ノードのローカル計算において指数時間の計算を許した場合における計算ラウンド数の複雑性に関して近年議論が進んでおり、最大独立集合の発見あるいはその近似解の発見に対して上界、下界の両面から、いくつかの結果が知られている。((ここ、具体的にどのような上下界が得られているか説明を入れる))。例えば、CONGEST モデルにおいて最大

重み付き独立集合の $(1 + \epsilon) \cdot \Delta$ -近似 (Δ は頂点の最大次数) を高確率で $(poly(\log \log n)/\epsilon)$ ラウンドで発見するアルゴリズム [1] や、最大独立集合を発見するアルゴリズムに対する $\Omega\left(\frac{n^2}{(\log n)^2}\right)$ ラウンドの下界 [2], 最大独立集合の $(\frac{3}{4} + \epsilon)$ -近似を発見するアルゴリズムに対する $\Omega\left(\frac{n^2}{(\log n)^3}\right)$ ラウンドの下界 [3] などが知られている. 逐次アルゴリズムにおける計算困難性から, 指数時間を要する内部計算を許容して分散グラフアルゴリズムの複雑性の議論を行うことの妥当性にはやや疑問が残る.

1.2 本研究の目的と結果

そこで今回, 我々は最大独立集合の局所最適解である k -極大独立集合 (k -Maximal Independent Set, k -MIS) について考える. (k -MIS はそれほど一般的な概念ではないので, [ここにラフな説明ほしい](#)) 独立集合のうち, k 個の頂点をその集合から取り除いて独立集合を維持したまま $k+1$ 個以上の頂点を追加することができないとき, その独立集合を k -MIS という. 与えられたグラフ $G = (V, E)$ に対する k -MIS の発見は, 自然な局所探索により実現することが可能である. すなわち, I を現在構成されている独立点集合とすると, 任意のサイズ k 以下の部分集合 $I' \subseteq I$ およびサイズ $k+1$ の部分集合 $U \subseteq V \setminus I$ について, $(I \setminus I') \cup U$ が独立点集合となるかどうかを確認し, そのような I', U が存在すれば I を更新することを繰り返すことで, 最終的に k -MIS を得ることができる. $k = O(1)$ の場合この処理は n の多項式時間内で収まるのが容易にわかる. 一方で, この更新処理, すなわち, 与えられた独立点集合 I が既に k -MIS を構成しているかどうか検証する問題が CONGEST モデル上で効率的に解けるかどうかは明らかではない. そこで, 本研究では k -MIS の検証問題 (verification) に着目し, その複雑性について議論を行う. 具体的には, 本研究は以下に挙げる結果を示す ([下に結果を itemize の箇条書きでまとめる](#)).

- CONGEST モデルにおいて, 1-MIS 検証問題は $O(1)$ ラウンドで解くことができる.
- CONGEST モデルにおいて, 2-MIS 検証問題には $\tilde{\Omega}(\sqrt{n})$ ラウンドの下界が存在する.
- CONGEST モデルにおいて, 3-MIS 検証問題には $\tilde{\Omega}(n)$ ラウンドの下界が存在する.
- CONGEST モデルにおいて, 任意の $l \geq 1$ に対して $k = 4l + 5$ としたときに k -MIS 検証問題には $\Omega\left(n^{2-\frac{1}{l+1}}/l\right)$ ラウンドの下界が存在する.

1.3 関連研究

CONGEST モデルにおける最大独立集合問題の通信複雑性としては、最大重み付き独立集合の $(1 + \epsilon) \cdot \Delta$ -近似 (Δ は頂点の最大次数) を高確率で見つけるアルゴリズムに対する $(poly(\log \log n)/\epsilon)$ ラウンドの上界 [1] や、最大独立集合を見つけるアルゴリズムに対する $\Omega\left(\frac{n^2}{(\log n)^2}\right)$ ラウンドの下界 [2], 最大独立集合の $(\frac{1}{2} + \epsilon)$ -近似を見つけるアルゴリズムに対する $\Omega\left(\frac{n}{(\log n)^3}\right)$ ラウンドの下界, $(\frac{3}{4} + \epsilon)$ -近似を見つけるアルゴリズムに対する $\Omega\left(\frac{n^2}{(\log n)^3}\right)$ ラウンドの下界 [3] が知られている。

極大独立集合 (0-MIS) 問題の複雑性に関して、CONGEST モデルにおいては $O(\log n)$ ラウンドの乱択アルゴリズム [4] や $poly(\log n)$ ラウンドの決定性アルゴリズム [5] が知られている。LOCAL モデルにおいては $O(\log \Delta) + poly(\log \log n)$ ラウンドの乱択アルゴリズムや $poly(\log n)$ ラウンドの決定性アルゴリズム [5], 乱択アルゴリズムに対する $\Omega\left(\frac{\log \log n}{\log \log \log n}\right)$ の下界や決定性アルゴリズムに対する $\Omega\left(\frac{\log n}{\log \log n}\right)$ の下界 [6] が知られている。

また集中型アルゴリズムについて、 $P = NP$ が成り立たない限り、任意の $\epsilon > 0$ に対して最大独立集合の $n^{\frac{1}{2}-\epsilon}$ 近似を発見するアルゴリズムは存在しないことが知られている [7]。

本研究の下界に関する結果は 2 者間通信の枠組みにおける交叉判定問題からの帰着に基づいているが、交叉判定問題からの帰着によって下界を示すという証明方法は多くの問題に対して用いられている。一部の例として最小カット発見問題と最小全域木問題に対する $\Omega(D + \sqrt{n})$ の下界 (D はグラフの直径) [8] や部分グラフ H_k 検出問題に対する $\Omega\left(\frac{n^{2-1/k}}{bk}\right)$ の下界 [9], 近似最大クリーク K_l 検出問題に対する $\Omega\left(\frac{n}{(l+\sqrt{n})b}\right)$ の下界 [10] などが挙げられる。

(集中型アルゴリズムの近似不可能性の結果も、具体的な近似率限界を挙げて説明する。また、CONGEST 上の極大独立点集合の結果 (すなわち 0-MIS の結果) も挙げる。s)

1.4 本研究の成果

今回、我々は k -MIS 検証問題に対するいくつかの複雑性を示した。その結果を表 1.1 にまとめた。最初に、1-MIS 検証問題が $O(1)$ ラウンドで解けることを証明した。次に、2-MIS 検証問題に対する $\tilde{\Omega}(\sqrt{n})$ ラウンドの下界と 3-MIS 検証問題に対する $\tilde{\Omega}(n)$ ラウンドの下界を証明した。最後に、任意の $l \geq 1$ に対して $k = 4l + 5$ としたときに k -MIS 検証問題に対する $\Omega\left(n^{2-\frac{1}{l+1}}/l\right)$ ラウンドの下界を証明した。特に、下界の証明のアイデアは 2 者間通信の枠組みにおける交叉判定問題からの帰着に基づいている。

表 1.1: 本研究が示した k -MIS 検証問題のラウンド複雑性

k	1	2	3	$4l + 5$
上界 or 下界	上界	下界	下界	下界
結果	$O(1)$	$\tilde{\Omega}(\sqrt{n})$	$\tilde{\Omega}(n)$	$\Omega\left(n^{2-\frac{1}{l+1}}/l\right)$

1.5 論文の構成

本論文は全 5 章で構成される。第 2 章ではグラフの構造と用語の定義をしている。第 3 章では 1-MIS 検証問題に対する $O(1)$ ラウンドアルゴリズムについて述べている。第 4 章では k -MIS 検証問題 ($k = 2, 3, 4l + 5 (l \geq 1)$) に対する下界について述べている。第 5 章ではまとめについて述べている。

第2章

諸定義

2.1 CONGEST モデル

本研究で考える CONGEST モデルは、単純無向連結グラフ $G = (V, E)$ により表現される。ここで V はノードの集合で $|V| = n$ とし、 E は通信リンクの集合である。CONGEST モデルでは計算機はラウンドに従って同期して動作するものとする。1 ラウンド内で、隣接頂点へのメッセージ送信、隣接頂点からのメッセージ受信、内部計算を行う。各辺は単位ラウンドあたり $b = O(\log n)$ ビットを双方向に伝送可能であり、各ノードは同一ラウンドに異なる接続辺に異なるメッセージを送信可能である。また、各ノードには $O(\log n)$ ビットの自然数値による ID が付与されており、自身の隣接ノードすべての ID を既知であるとする。各ノードはグラフのトポロジに関する事前知識を持たないものとする。

2.2 2 者間通信複雑性

2 者間通信複雑性の枠組みでは、アリスとボブの二人のプレイヤーがそれぞれ k ビットの $0/1$ のデータ列で構成されるプライベートな入力 x および y を持っているとする。プレイヤーの目標は、結合関数 $f(x, y)$ を計算することであり、複雑性の尺度として $f(x, y)$ を計算するためにアリスとボブが通信によって交換する必要のあるビット数が用いられる。

この枠組みにおける重要な問題として、交叉判定問題 (set-disjointness) がある。この問題では、アリスとボブはそれぞれ $x \in \{0, 1\}^k$ と $y \in \{0, 1\}^k$ を入力として持ち、目的は $DISJ_k(x, y) := \bigvee_{i=1}^k x_i \wedge y_i$ を計算することである。 k ビットの交叉判定問題を解くために、アリスとボブは通信によって $\Omega(k)$ ビット交換する必要があることが知られており [11]、この事実を用いて最小カット発見問題や最小全域木問題 [8]、部分グラフ検出問題や [9]、近似最大クリーク検出問題 [10] といったさまざまな問題に対する下界の証明がされている。

CONGEST モデルにおいて、入力グラフ上に特性 P があるかどうかの判定に対する下限

の証明を2者間交叉判定問題から帰着するアプローチは以下のとおりである．最初にアリスとボブは特殊なグラフ $G = (V, E)$ の構築と G を G_A と G_B に分割するカット辺 C の決定を行う．次に，アリスとボブは入力文字列に基づいてそれぞれ G_A に辺 E_A と頂点 V_A ， G_B に辺 E_B と頂点 V_B を追加する．このとき， $DISJ_k(x, y) = 1$ のときのみ，何らかの特性 P (例えば, P : 「グラフに与えられた MIS が 2-MIS でない」) を持つように辺や頂点を追加する．また，カット辺 C は入力文字列に依存しないようにする．グラフ G に辺や頂点を追加したグラフを $G^{x,y} = (V', E')$ とすると $V' = V \cup (V_A \cup V_B)$, $E' = E \cup (E_A \cup E_B)$ 表すことができる．グラフ $G^{x,y}$ の構造の概要を図 2.1 に示す．

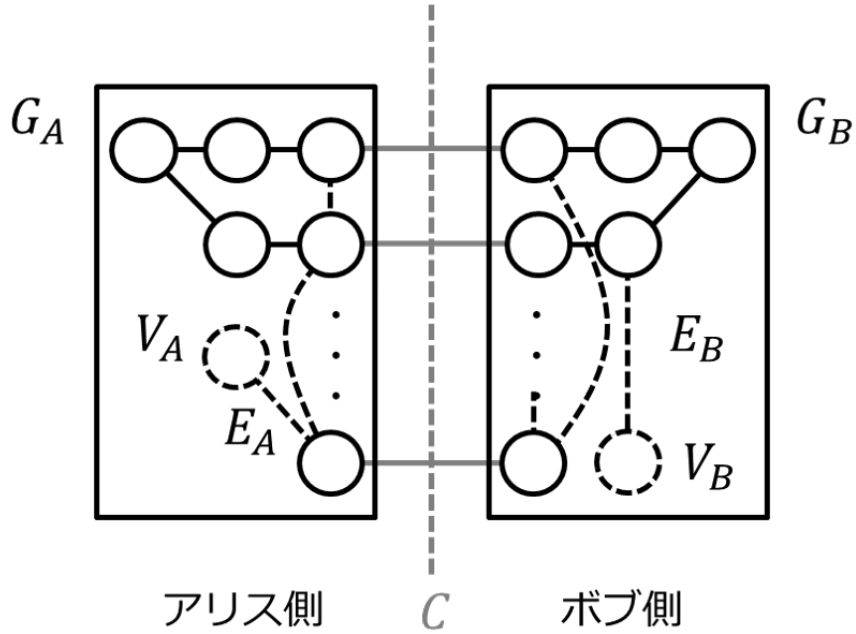


図 2.1: $G^{x,y} = (V', E')$

アリスとボブは，入力グラフ上に特性 P があるかを判定する分散アルゴリズムをシミュレートできる．アリスは G_A に含まれる頂点を，ボブは G_B に含まれる頂点をシミュレートする．2者間通信複雑性モデルでのシミュレートは，次のように実行される． G_A 中の辺で送信されるメッセージ，あるいは G_B 中の辺で送信されるメッセージは，アリスとボブがそれぞれお互いと通信せずにシミュレートできる．カット辺 C を通じて送信されるメッセージに対しては，お互い情報を交換する必要がある．CONGEST モデルにおいてグラフ上に特性 P があるかどうかを r ラウンドで判定するアルゴリズム A が存在したとすると，アリスとボブは特性 P の判定のために $O(r \cdot |C| \cdot \log n)$ ビット通信したことになる．これは，各ラウンドで，アルゴリズムが各辺で $O(\log n)$ ビットの通信を行っているから

である．このグラフにおいてアルゴリズム \mathcal{A} を実行すると同時に 2 者間交叉判定問題も解けていることになる．例えばアルゴリズムを実行した結果, 入力グラフに特性 P があると判定されれば $DISJ_k(x, y) = 1$ であることがわかるからである．交叉判定問題の通信複雑性よりアリスとボブは少なくとも $\Omega(k)$ ビットは通信しているはずである．したがって, $CONGEST$ モデルにおいて特性 P があるかどうかを判定する任意のアルゴリズムに対して $r = \Omega(k/|C| \cdot \log n)$ ラウンドの下界を得ることができる．カット辺の大きさが小さくなるほど下界が強くなる．

2.3 k -極大独立集合

定義 2.1. 頂点集合 I に対して, 以下を満たす頂点集合 $I' \subseteq I$ と $S \subseteq V \setminus I$ のペアが存在しないとき, I を k -極大独立集合と呼ぶ．

1. $|I'| \leq k$
2. $|S| \geq |I'| + 1$
3. $(I \setminus I') \cup S$ は独立集合

つまり, ある独立集合 I に対して, サイズ k の I の部分集合 I' を取り除いてサイズ $k+1$ 以上の V の部分集合 S を I に追加したものが新たな独立集合になり得ないとき, I を k -極大独立集合と定義する．

2.4 k -極大独立集合検証問題

定義 2.2. 入力としてグラフ G と独立集合 I が与えられる．各ノードはアルゴリズム \mathcal{A} に従って $\{0, 1\}$ のいずれかを返し以下の条件を満たす時, アルゴリズム \mathcal{A} は k -MIS 検証問題を解くアルゴリズムであると言う．

1. $\forall v \in V$ に対して, v が 0 を返すとき I は k -MIS である．
2. $\exists v \in V$ に対して, v が 1 を返すとき I は k -MIS ではない．

第3章

1-MIS 検証問題の $O(1)$ ラウンドアルゴリズム

この章では、1-MIS 検証問題を $O(1)$ ラウンドで解くアルゴリズムについて述べる。CONGEST モデルにおいて、入力としてグラフ G と独立集合 I が与えられたとき、1-MIS 検証問題を解くために次のようなアルゴリズム A を実行する。

1. 各頂点 $v \in I$ は、自分の ID である $v.id$ を隣接頂点全員に送信する。
2. 各頂点 $u \notin I$ のうち、2 種類以上の ID をもらった頂点はアルゴリズムから離脱する。
3. 離脱しなかった頂点 $u \notin I$ のうち、1 種類だけの ID ($v.id$ とする) を受信した頂点は離脱していない全隣接頂点へ $v.id$ を送信する。頂点 $u \notin I$ は、自身が持つ $v.id$ と違う $v.id$ が書かれたメッセージは無視し、自身が持つ $v.id$ と同じ $v.id$ が書かれたメッセージの数を記憶し、それを a とする。
4. 各頂点 $v \in I$ は、自身と同じ $v.id$ を返信してきた頂点の集合 ($v.X$ とする) のサイズを数え、そのサイズ $|v.X|$ を $v.X$ 中の頂点に送信し、0 を返す。
5. メッセージを受け取った $v.X$ 中の頂点は、送られたサイズ $|v.X|-1$ と a を比較する。比較した $v.X$ 中の頂点全てで $|v.X|-1 = a$ であればその $v.X$ 中の頂点は 0 を返し、一つでも等しくなければその $v.X$ 中の頂点は 1 を返す。

アルゴリズム A の各ステップは明らかに $O(1)$ ラウンドで CONGEST モデルで実装できる。アルゴリズム A について、以下の補題が成り立つ。

補題 3.1. アルゴリズム A は 1-MIS 検証問題を解くことができる。

証明. アルゴリズム A は与えられた入力に対して誤った答えを返すとする。このとき以下の 2 つのうち、どちらかが成り立つ。

1. 与えられた独立集合が 1-MIS であり, アルゴリズム \mathcal{A} が 1-MIS でないと返す.
2. 与えられた独立集合が 1-MIS でなく, アルゴリズム \mathcal{A} が 1-MIS であると返す.

アルゴリズム \mathcal{A} の 5 番目のステップで $|v.X|-1$ と a を比較して, $v.X$ 中の頂点全てでその値が等しいとき, $v.X$ の頂点はクリークを形成している. $v \in I$ は他の $v.X$ 頂点と隣接しており, かつ $|v.X|-1 \geq a$ であるが, 等号が成立するのは $v.X$ 内の全ての頂点 $u \notin I$ が他の $u' \notin I$ と隣接している場合のみだからである.

1. の場合, アルゴリズム \mathcal{A} が 1-MIS でないと返したということは, ある $v.X$ についてその中の頂点 $u \notin I$ が 1 を返したということである. この場合, この $v.X$ はクリークを形成していない. 従って, $v.X$ の中に少なくともサイズ 2 の独立集合が存在しているはずである. v とそれらを入れ替えることで独立集合を維持しつつサイズを大きくすることができるため与えられた独立集合は 1-MIS ではないが, これは仮定に矛盾する.

2. の場合, アルゴリズム \mathcal{A} が 1-MIS であると返したということは, 全ての $v.X$ についてその中の頂点 $u \notin I$ が 0 を返したということである. この場合, 全ての $v.X$ がクリークを形成している. 従って, $v.X$ の中には独立集合に追加できる可能性のある頂点は存在しない. また, 2 番目のステップで離脱した頂点も独立集合点に含まれている 1 頂点を取り除いただけ追加できる可能性はない. よって, 独立集合を維持しつつサイズを大きくするために追加できる頂点は存在しないため与えられた独立集合は 1-MIS であるが, これは仮定に矛盾する.

以上より, アルゴリズム \mathcal{A} は与えられた入力に対して正しい答えを返すことができるため, 1-MIS 検証問題を解くことができる.

第4章

k -MIS 検証問題の下界

この章では、 k -MIS 検証問題の下界についての議論を行う。4.1 節では、2-MIS 検証問題の下界についての定理とその証明を述べる。4.2 節では、3-MIS 検証問題の下界についての定理とその証明を述べる。4.3 節では、 k -MIS 検証問題 ($k = 4l + 5, l \geq 1$) の下界についての定理とその証明を述べる。

4.1 2-MIS 検証問題の下界

この節では 2-MIS 検証問題の下界についての議論を行う。具体的には、次の定理を証明する。

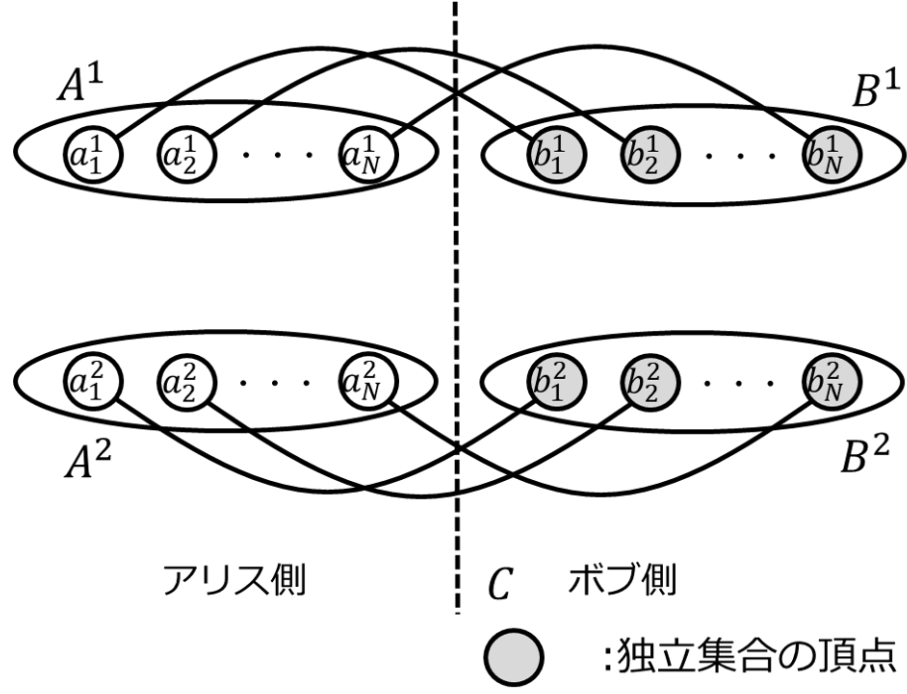
定理 4.1. CONGEST モデルにおいて、2-MIS 検証問題を解く全てのアルゴリズムは $\tilde{\Omega}(\sqrt{n})$ の通信ラウンド数を必要とする。

証明. まず初めにアリスとボブが構築するグラフ $G = (V, E)$ を図 4.1 に示す。

図中の頂点のうち灰色のものは独立集合に含まれる頂点とする。図中の辺を定式化すると以下ようになる。

- $\forall i((a_i^1, b_i^1), (a_i^2, b_i^2)) \in E$

このグラフが「 G 中に与えられている独立集合が、 $DISJ_{N \times N}(x, y) = 1$ のときのみ 2-MIS でない」という特性 P_2 を持つように、 G_A に構造 H_A 、 G_B に構造 H_B を追加する。(なお、 $DISJ_{N \times N}(x, y) := \bigvee_{i=1}^N \bigvee_{j=1}^N x_{i,j} \wedge y_{i,j}$ で定義される。) H_A と H_B の中身は以下のとおりである。

図 4.1: $G = (V, E)$

- $H_A: (a_i^1, a_j^2) \in E_A \Leftrightarrow x_{i,j} = 0$
- $H_B: W(y)$ 頂点のクリーク $K_{W(y)}(W(y))$ は 0/1 のデータ列 y 中に含まれる 1 の個数
を表す.) $K_{W(y)}$ 中の頂点 $c_{i,j} \in V_B$ は $y_{i,j} = 1$ であるような (i, j) でインデックスづ
けされるものとする.

このとき, $(c_{i,j}, b_i^1) \in E_B$ かつ $(c_{i,j}, b_j^2) \in E_B$

$G = (V, E)$ に辺と頂点を追加したグラフ $G^{x,y} = (V', E')$ を図 4.2 に示す.

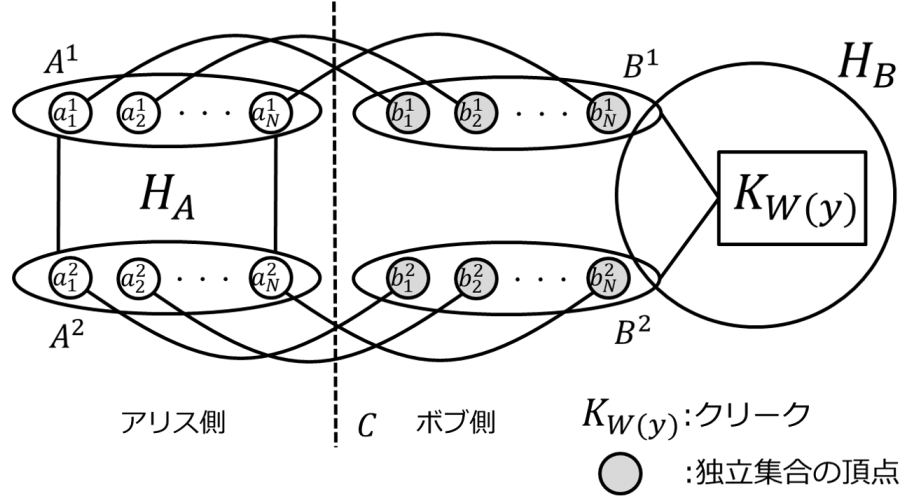
このグラフ $G^{x,y} = (V', E')$ が上記の特性 P_2 を満たしていることを示すために, 次の 2
点を確認する.

(i) $DISJ_{N \times N}(x, y) = 1$ のとき, グラフに与えられている独立集合が 2-MIS でない:

$x_{i,j} = y_{i,j} = 1$ とすると, b_i^1 と b_j^2 の 2 点を取り除いて $a_i^1, a_j^2, c_{i,j}$ の 3 点を追加できるこ
とから確認できる.

(ii) $DISJ_{N \times N}(x, y) = 0$ のとき, グラフに与えられている独立集合が 2-MIS である:

グラフに与えられている独立集合が 2-MIS でないと仮定する. このとき, ある 2 点を取り
除くことで独立集合に追加できる 3 点が存在する. 2 点の取り除き方は (1) b_i^1 と $b_j^1 (i \neq j)$,
(2) b_i^2 と $b_j^2 (i \neq j)$, (3) b_i^1 と b_j^2 が考えられる. (1) では a_i^1 と a_j^1 の 2 点しか追加できる可能

図 4.2: $G^{x,y} = (V', E')$

性がなく, (2) では a_i^2 と a_j^2 の 2 点しか追加できる可能性がない. (3) において, b_i^1 を取り除いて a_i^1 を追加し, b_j^2 を取り除いて a_j^2 を追加し, さらに $c_{i,j}$ を追加することを考える. a_i^1 と a_j^2 が両方とも追加できるのは $x_{i,j} = 1$ のときのみであり, $c_{i,j}$ が追加できる ($c_{i,j}$ が存在する) のは $y_{i,j} = 1$ のときのみであるが, これは $DISJ_{N \times N}(x, y) = 0$ に矛盾する. したがってグラフに与えられている独立集合から 2 点取り除いて 3 点追加することはできないため, この独立集合は 2-MIS である.

今回, $N \times N$ ビットの交叉判定インスタンスをグラフに埋め込んでおり, カット辺のサイズ $|C| = 2N$ であることがわかる. CONGEST モデルにおいてグラフ上に与えられた独立集合が 2-MIS であるかどうかを r ラウンドで判定するアルゴリズム \mathcal{A} が存在したとすると, アリスとボブは $O(r \cdot |C| \cdot \log n)$ ビット通信したことになる. このグラフにおいてアルゴリズム \mathcal{A} を実行すると同時に 2 者間交叉判定問題も解けていることになるので, 交叉判定問題の通信複雑性よりアリスとボブは少なくとも $\Omega(N \times N)$ ビットは通信しているはずである. よって, $r = \Omega(N/2 \log n) = \tilde{\Omega}(N)$ ラウンドの下界を得ることができる. 図 4.2 からわかる通り, A^1, A^2, B^1, B^2 はそれぞれ N 頂点で構成されており, $K_{W(y)}$ の頂点数は $O(N^2)$ であるため, グラフ全体の頂点数 n は $n = O(N + N^2)$ である. したがって $N = \Omega(\sqrt{n})$ になるため, $\tilde{\Omega}(\sqrt{n})$ ラウンドの下界を得ることができる.

4.2 3-MIS 検証問題の下界

この節では 3-MIS 検証問題の下界についての議論を行う．具体的には，次の定理を証明する．

定理 4.2. CONGEST モデルにおいて，3-MIS 検証問題を解く全てのアルゴリズムは $\tilde{\Omega}(n)$ の通信ラウンド数を必要とする．

証明. まず初めにアリスとボブが構築するグラフ $G = (V, E)$ を図 4.3 に示す．

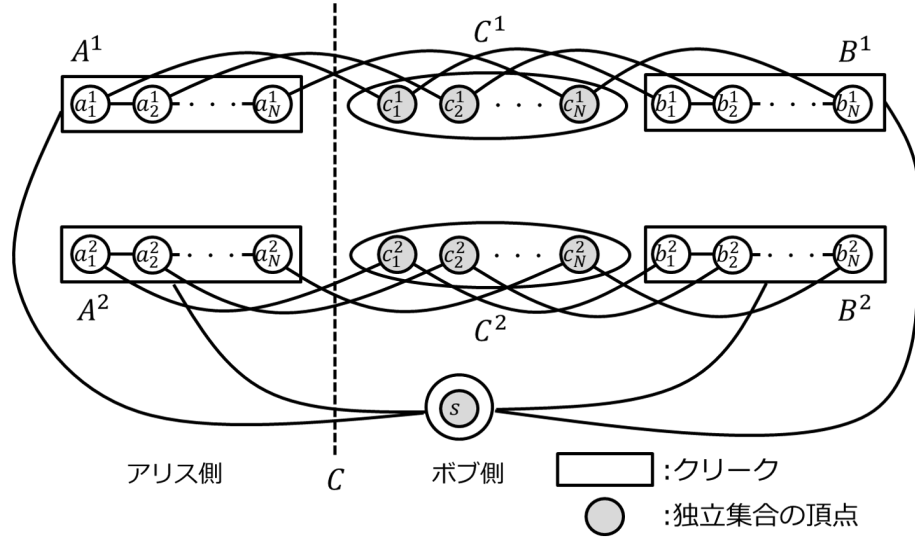


図 4.3: $G = (V, E)$

図中の頂点のうち灰色のものは独立集合に含まれる頂点とする．また，四角で囲まれている部分はクリークを表す．図中の辺を定式化すると以下ようになる．

- A^1, A^2, B^1, B^2 は N 頂点のクリーク K_N
- $\forall i((a_i^1, c_i^1), (a_i^2, c_i^2), (b_i^1, c_i^1), (b_i^2, c_i^2)) \in E$
- $\forall i((a_i^1, s), (a_i^2, s), (b_i^1, s), (b_i^2, s)) \in E$

このグラフが「 G 中に与えられている独立集合が， $DISJ_{N \times N}(x, y) = 1$ のときのみ 3-MIS でない」という特性 P_3 を持つように， G_A に構造 H_A ， G_B に構造 H_B を追加する． H_A と H_B の中身は以下のとおりである．

- $H_A: (a_i^1, a_j^2) \in E_A \Leftrightarrow x_{i,j} = 0$
- $H_B: (b_i^1, b_j^2) \in E_B \Leftrightarrow y_{i,j} = 0$

$G = (V, E)$ に辺を追加したグラフ $G^{x,y} = (V, E')$ を図 4.4 に示す.

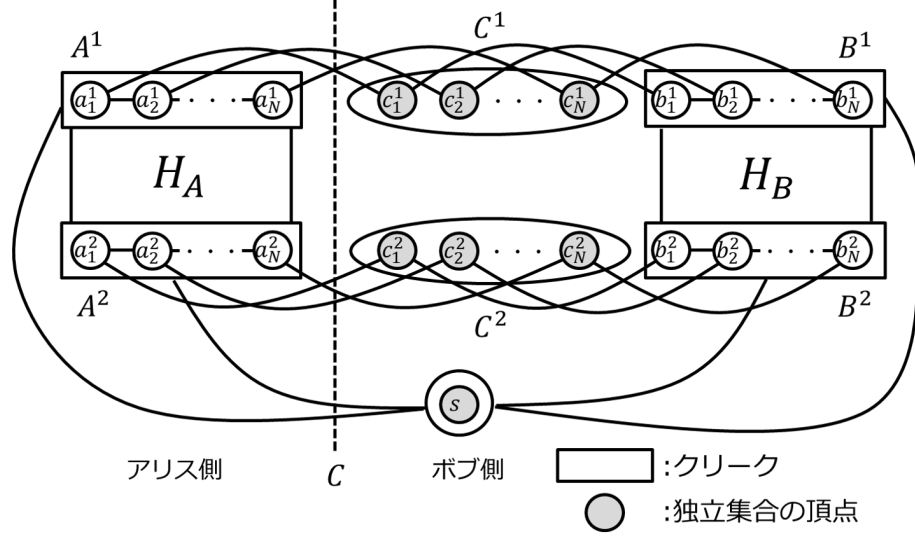


図 4.4: $G^{x,y} = (V, E')$

このグラフ $G^{x,y} = (V, E')$ が上記の特性 P_3 を満たしていることを示すために、次の2点を確認する.

(i) $DISJ_{N \times N}(x, y) = 1$ のとき、グラフに与えられている独立集合が 3-MIS でない:

$x_{i,j} = y_{i,j} = 1$ とすると、 s と c_i^1 と c_j^2 の3点を取り除いて $a_i^1, b_i^1, a_j^2, c_j^2$ の4点を追加できることから確認できる。

(ii) $DISJ_{N \times N}(x, y) = 0$ のとき、グラフに与えられている独立集合が 3-MIS である:

グラフに与えられている独立集合が 3-MIS でないと仮定する. このとき、ある3点を取り除くことで独立集合に追加できる4点が存在するが、 A^1, A^2, B^1, B^2 がそれぞれクリークであるため、4点を追加するためにはそれぞれから1点を選ぶ必要がある. c_i^1 を取り除いて a_i^1 と b_i^1 を追加し、 c_j^2 を取り除いて a_j^2 と b_j^2 を独立集合に追加したとする. a_i^1 と a_j^2 が両方とも追加できるのは $x_{i,j} = 1$ のときのみであり、 b_i^1 と b_j^2 が両方とも追加できるのは $y_{i,j} = 1$ のときのみであるが、これは $DISJ_{N \times N}(x, y) = 0$ に矛盾する. したがってグラフに与えられている独立集合から3点取り除いて4点追加することはできないため、この独立集合は 3-MIS である.

今回, $N \times N$ ビットの交叉判定インスタンスをグラフに埋め込んでおり, カット辺のサイズ $|C| = 4N$ であることがわかる. CONGEST モデルにおいてグラフ上に与えられた独立集合が 3-MIS であるかどうかを r ラウンドで判定するアルゴリズム \mathcal{A} が存在したとすると, アリスとボブは $O(r \cdot |C| \cdot \log n)$ ビット通信したことになる. このグラフにおいてアルゴリズム \mathcal{A} を実行すると同時に 2 者間交叉判定問題も解けていることになるので, 交叉判定問題の通信複雑性よりアリスとボブは少なくとも $\Omega(N \times N)$ ビットは通信しているはずである, よって, $r = \Omega(N/4 \log n) = \tilde{\Omega}(N)$ ラウンドの下界を得ることができる. 図 4.4 からわかる通り, $A^1, A^2, B^1, B^2, C^1, C^2$ はそれぞれ N 頂点で構成されているため, グラフ全体の頂点数 n は $n = O(N)$ である. したがって $N = \Omega(n)$ になるため, $\tilde{\Omega}(n)$ ラウンドの下界を得ることができる..

4.3 k -MIS 検証問題の下界

このセクションでは k -MIS 検証問題の下界についての議論を行う．具体的には、次の定理を証明する．

定理 4.3. CONGEST モデルにおいて、任意の $l \geq 1$ に対して $k = 4l + 5$ としたとき k -MIS 検証問題を解く全てのアルゴリズムは $\Omega\left(n^{2-\frac{1}{l+1}}/l\right)$ の通信ラウンド数を必要とする．

証明. 以下をを定義する．

定義 4.1. 証明の簡略化のために N の $l+1$ 乗根は整数であると仮定する．このとき $M = \sqrt[l+1]{N}$ とする．また、自然数 i, j, h が与えられたとき、 $\alpha_{i,h}(j)$ を j を i 進数で表したときの h 桁目の値と定義する．

まず初めにアリスとボブが構築するグラフ $G = (V, E)$ を図 4.5 に示す．

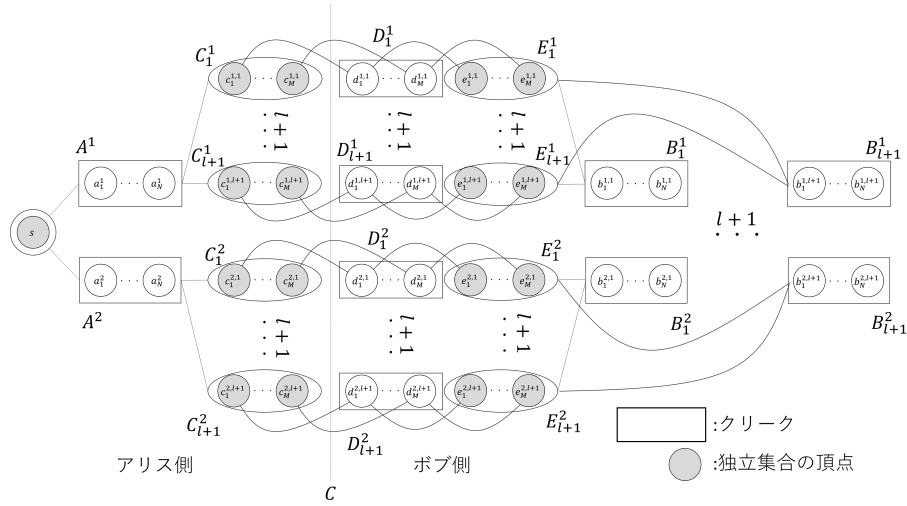


図 4.5: $G = (V, E)$

図中の頂点のうち灰色のものは独立集合に含まれる頂点とする．また、四角で囲まれている部分はクリークを表す．図中の辺を定式化すると以下ようになる．

- $A^1 = \{a_1^1, \dots, a_N^1\}$ と $A^2 = \{a_1^2, \dots, a_N^2\}$ は N 頂点のクリーク
- 任意の $1 \leq i \leq l+1$ に対して $B_i^1 = \{b_1^{1,i}, \dots, b_N^{1,i}\}$ と $B_i^2 = \{b_1^{2,i}, \dots, b_N^{2,i}\}$ は N 頂点のクリーク

- 任意の $1 \leq i \leq l+1$ に対して $D_i^1 = \{d_1^{1,i}, \dots, d_M^{1,i}\}$ と $D_i^2 = \{d_1^{2,i}, \dots, d_M^{2,i}\}$ は M 頂点のクリーク
- $\forall i((a_i^1, s), (a_i^2, s)) \in E$
- 任意の $1 \leq i \leq N$ と $1 \leq j \leq l+1$ に対して $(a_i^1, c_{\alpha_{M,j}(i-1)+1}^{1,j})$ と $(a_i^2, c_{\alpha_{M,j}(i-1)+1}^{2,j})$ が E に含まれる
- 任意の $1 \leq i \leq N$, $1 \leq j \leq l+1$ と $1 \leq h \leq l+1$ に対して $(b_i^{1,h}, e_{\alpha_{M,j}(i-1)+1}^{1,j})$ と $(b_i^{2,h}, e_{\alpha_{M,j}(i-1)+1}^{2,j})$ が E に含まれる
- 任意の $1 \leq i \leq M$ と $1 \leq j \leq l+1$ に対して $(c_i^{1,j}, d_i^{1,j})$ と $(e_i^{1,j}, d_i^{1,j})$ が E に含まれる
- 任意の $1 \leq i \leq M$ と $1 \leq j \leq l+1$ に対して $(c_i^{2,j}, d_i^{2,j})$ と $(e_i^{2,j}, d_i^{2,j})$ が E に含まれる

このグラフが「 G 中に与えられている独立集合が, $DISJ_{N \times N}(x, y) = 1$ のときのみ k -MIS でない」という特性 (P_k) を持つように, G_A に構造 H_A , G_B に構造 H_B を追加する. H_A と H_B の中身は以下のとおりである.

- $H_A : E_A = \{(a_i^1, a_j^2) \mid x_{i,j} = 0, 1 \leq i \leq N, 1 \leq j \leq N\}$
- $H_B : E_B = \{(a_i^{1,h}, a_j^{2,h}) \mid x_{i,j} = 0, 1 \leq i \leq N, 1 \leq j \leq N, 1 \leq h \leq l+1\}$

$G = (V, E)$ に辺を追加したグラフ $G^{x,y} = (V, E')$ を図 4.6 に示す.

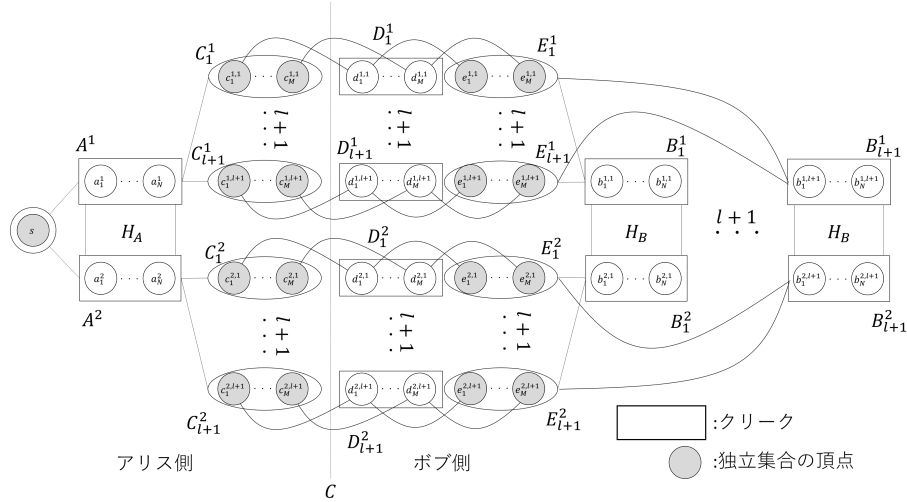


図 4.6: $G^{x,y} = (V, E')$

このグラフ $G^{x,y} = (V, E')$ が上記の特性 (P_k) を満たしていることを示すために、次の2点を確認する.

(i) $DISJ_{N \times N}(x, y) = 1$ のとき、グラフに与えられている独立集合が k -MIS でない:

$x_{i,j} = y_{i,j} = 1$ であると仮定する. このとき,

$$I' = \{s\} \cup \bigcup_{1 \leq h \leq l+1} c_{\alpha_{M,h}(i-1)+1}^{1,h} \cup \bigcup_{1 \leq h \leq l+1} c_{\alpha_{M,h}(j-1)+1}^{2,h} \cup \bigcup_{1 \leq h \leq l+1} e_{\alpha_{M,h}(i-1)+1}^{1,h} \cup \bigcup_{1 \leq h \leq l+1} e_{\alpha_{M,h}(j-1)+1}^{2,h}$$

$$S = \{a_i^1 \cup a_j^2\} \cup \bigcup_{1 \leq h \leq l+1} b_j^{1,h} \cup \bigcup_{1 \leq h \leq l+1} b_j^{2,h} \cup \bigcup_{1 \leq h \leq l+1} d_{\alpha_{M,h}(i-1)+1}^{1,h} \cup \bigcup_{1 \leq h \leq l+1} d_{\alpha_{M,h}(j-1)+1}^{2,h}$$

とすると $I \setminus I' \cup S$ は独立集合になる. ここで $|I'| = 4l + 5$ で $|S| = 4l + 6$ であることから, $k = 4l + 5$ に対して I は k -MIS でないことが確認できる.

(ii) $DISJ_{N \times N}(x, y) = 0$ のとき、グラフに与えられている独立集合が k -MIS である:

グラフに与えられている独立集合が k -MIS でないと仮定する. このとき, $I' \subseteq I$ をサイズ k 以下の独立集合, $S \subseteq V \setminus I$ を $(I \setminus I') \cup S$ が独立集合になるサイズ $|I'| + 1$ 以上の頂点集合とする. また, $(A^1 \cup A^2) \cap S$ を満たすノードの数を $num(A)$, $\bigcup_{1 \leq i \leq l+1} (B_i^1 \cup B_i^2) \cap S$ を満たすノードの数を $num(B)$, $(\bigcup_{1 \leq i \leq l+1} C_i^1 \cup \bigcup_{1 \leq i \leq l+1} C_i^2) \cap S$ を満たすノードの数を $num(C)$, $(\bigcup_{1 \leq i \leq l+1} D_i^1 \cup \bigcup_{1 \leq i \leq l+1} D_i^2) \cap S$ を満たすノードの数を $num(D)$, $(\bigcup_{1 \leq i \leq l+1} E_i^1 \cup \bigcup_{1 \leq i \leq l+1} E_i^2) \cap S$ を満たすノードの数を $num(E)$ とする. 任意の $1 \leq i \leq M$ と $1 \leq j \leq l + 1$ に対して $d_i^{1,j}$ を独立集合に追加するには $c_i^{1,j}$ と $e_i^{1,j}$ を独立集合から取り除く必要がある. また, 任意の $1 \leq i \leq M$ と $1 \leq j \leq l + 1$ に対して $d_i^{2,j}$ を独立集合に追加するには $c_i^{2,j}$ と $e_i^{2,j}$ を独立集合から取り除く必要がある. 従って, $num(D)$ の値は $num(C)$ によって上から抑えられる. また, $num(D)$ の値は $num(E)$ によっても上から抑えられる. 任意の $1 \leq i \leq N$ と $1 \leq j \leq l + 1$ に対して, $b_i^{1,j}$ を独立集合に追加するには, $\bigcup_{1 \leq h \leq l+1} e_{\alpha_{M,h}(i-1)+1}^{1,h}$ を独立集合から取り除く必要がある. 従って, 任意の $1 \leq i \leq l + 1$ に対して B_i^1 に含まれる頂点を独立集合に追加するには $\bigcup_{1 \leq j \leq l+1} E_j^1$ に含まれる頂点を少なくとも $l + 1$ 個独立集合から取り除く必要がある. 同様に任意の $1 \leq i \leq N$ と $1 \leq j \leq l + 1$ に対して, $b_i^{2,j}$ を独立集合に追加するには, $\bigcup_{1 \leq h \leq l+1} e_{\alpha_{M,h}(i-1)+1}^{2,h}$ を独立集合から取り除く必要がある. 従って, 任意の $1 \leq i \leq l + 1$ に対して B_i^2 に含まれる頂点を独立集合に追加するには $\bigcup_{1 \leq j \leq l+1} E_j^2$ に含まれる頂点を少なくとも $l + 1$ 個独立集合から取り除く必要がある. 任意の $1 \leq i \leq 2$ と $1 \leq j \leq l + 1$ に対して, B_j^i はクリークであるので, B_j^i に含まれる頂点は高々1つしか独立集合に加えることができない. 従って $\bigcup_{1 \leq i \leq l+1} B_i^1$ から独立

集合に加えられる頂点の数は高々 $l+1$ 個であり, $\bigcup_{1 \leq i \leq l+1} B_i^2$ から独立集合に加えられる頂点の数は高々 $l+1$ 個であるので, $\text{num}(B)$ の値は $\text{num}(E)$ の値によって上から抑えられる. 従って $|S| \geq |I'|+1$ を満たすには $(\text{num}(A) \geq 1)$ である必要があるが, A^1 と A^2 はそれぞれクリークあるため $\text{num}(A) = 1$ もしくは $\text{num}(A) = 2$ である.

はじめに $\text{num}(A) = 1$ の場合を考える. このとき, $A^1 \cup A^2$ に含まれる頂点を独立集合に追加するには頂点 s を独立集合から取り除かなければならない. 従って $|I'| = 1 + \text{num}(C) + \text{num}(E)$ と $|S| = 1 + \text{num}(D) + \text{num}(B)$ が成り立ち, $\text{num}(C) \geq \text{num}(B), \text{num}(D) \geq \text{num}(E)$ より $|I'| \geq |S|$ が成り立つがこれは I' と S の選択に矛盾する.

次に $\text{num}(A) = 2$ の場合について考える. $\text{num}(A) = 1$ の場合と同様に $A^1 \cup A^2$ に含まれる頂点を独立集合に追加するには頂点 s を独立集合から取り除かなければならない. 従って, $|I'| = 1 + \text{num}(C) + \text{num}(E)$ と $|S| = 2 + \text{num}(D) + \text{num}(B)$ が成り立つ. ここで $|S| \geq |I'|+1$ を満たすのは $\text{num}(C) = \text{num}(D)$ かつ $\text{num}(B) = \text{num}(E)$ のときのみである. また, 任意の $1 \leq i \leq N$ に対して a_i^1 を独立集合に追加するには頂点集合 $\bigcup_{1 \leq j \leq l+1} c_{\alpha_{M,j}(i-1)+1}^{1,j}$ を独立集合から取り除く必要がある. 同様に任意の $1 \leq i \leq N$ に対して a_i^2 を独立集合に追加するには頂点集合 $\bigcup_{1 \leq j \leq l+1} c_{\alpha_{M,j}(i-1)+1}^{2,j}$ を独立集合から取り除く必要がある. 従って, $\text{num}(C) \geq 2(l+1)$ が成り立つ. また, $\text{num}(E) \geq \text{num}(D) = \text{num}(C) \geq 2(l+1)$ が成り立つ. ここで, $|I'| \leq k = 4l+5$ であることから, $\text{num}(C) = \text{num}(E) = 2(l+1)$ となる. $S \cap (A^1 \cup A^2)$ に含まれるノードを a_i^1 と a_j^2 とする. a_i^1 と a_j^2 を独立集合に加えるために取り除かれる頂点は $\{s\} \cup \bigcup_{1 \leq h \leq l+1} c_{\alpha_{M,h}(i-1)+1}^{1,h} \cup \bigcup_{1 \leq h \leq l+1} c_{\alpha_{M,h}(j-1)+1}^{2,h}$ である. このとき, 任意の $\bigcup_{1 \leq i \leq l+1} (D_i^1 \cup D_i^2)$ に含まれる頂点で独立集合に含まれる可能性があるのは, $\bigcup_{1 \leq h \leq l+1} d_{\alpha_{M,h}(i-1)+1}^{1,h} \cup \bigcup_{1 \leq h \leq l+1} d_{\alpha_{M,h}(i-1)+1}^{2,h}$ のみである. これらの頂点を独立集合に追加するには $\bigcup_{1 \leq h \leq l+1} e_{\alpha_{M,h}(i-1)+1}^{1,h} \cup \bigcup_{1 \leq h \leq l+1} e_{\alpha_{M,h}(i-1)+1}^{2,h}$ を独立集合から取り除かなければならない. このとき, B_1^1 と B_1^2 で新しく独立集合に加えられる可能性があるのは $b_i^{1,1}$ と $b_j^{2,1}$ だけである. $b_i^{1,1}$ と $b_j^{2,1}$ の両方を独立集合に加えられるのは $b_i^{1,1}$ と $b_j^{2,1}$ の間に辺が存在しないときでありこれは $y_{i,j} = 1$ を意味する. また, a_i^1 と a_j^2 が独立集合に含まれることから, a_i^1 と a_j^2 の間に辺が存在しない. これは $x_{i,j} = 1$ を意味するが $\text{DISJ}_{N \times N}(x, y) = 0$ に矛盾する.

今回, $N \times N$ ビットの交叉判定インスタンスをグラフに埋め込んでおり, カット辺のサイズ $|C| = 2(l+1) \cdot M = 2(l+1) \cdot N^{1/(l+1)}$ であることがわかる. CONGEST モデルにおいてグラフ上に与えられた独立集合が k -MIS であるかどうかを r ラウンドで判定するアルゴリズム \mathcal{A} が存在したとすると, アリスとボブは $O(r \cdot |C| \cdot \log n)$ ビット通信したことになる.

このグラフにおいてアルゴリズム \mathcal{A} を実行すると同時に 2 者間交叉判定問題も解けていることになるので、交叉判定問題の通信複雑性よりアリスとボブは少なくとも $\Omega(N \times N)$ ビットは通信しているはずである。よって、 $r = \Omega\left(N^{2-\frac{1}{l+1}}/2(l+1)\log n\right) = \tilde{\Omega}\left(N^{2-\frac{1}{l+1}}/l\right)$ ラウンドの下界を得ることができる。任意の $1 \leq i \leq 2$ と $1 \leq j \leq l+1$ に対して頂点集合 A^i, B_j^i はそれぞれ N 頂点で、 C_j^i, D_j^i, E_j^i の頂点集合はそれぞれ $M = N^{1/(l+1)}$ 頂点で構成されているため、グラフ全体の頂点数 n は $n = O(N)$ である。したがって $N = \Omega(n)$ になるため、 $\tilde{\Omega}\left(n^{2-\frac{1}{l+1}}/l\right)$ ラウンドの下界を得ることができる。

第5章

まとめと今後の課題

5.1 まとめ

本研究では極大独立集合検証問題に対するいくつかの複雑性を示した．具体的には，1-MIS 検証問題に対する $O(1)$ ラウンドの上界，2-MIS 検証問題に対する $\tilde{\Omega}(\sqrt{n})$ ラウンドの下界，3-MIS 検証問題に対する $\tilde{\Omega}(n)$ ラウンドの下界， k -MIS 検証問題 ($k = 4l + 5, l \geq 1$) に対する $\tilde{\Omega}\left(n^{2-\frac{1}{l+1}}/l\right)$ ラウンドの下界を証明した．

5.2 今後の課題

4.3 節で一般の k に対する k -MIS 検証問題の下界を証明したが， $k = 4, \dots, 8$ については現在 3-MIS 検証問題と同じ下界しか得られていない．この下界をよりタイトにできるかが今後の課題である．

謝辞

本研究の機会を与え、数々の御指導を賜りました泉泰介准教授に深く感謝致します。また、本研究を進めるにあたり多くの助言を頂き、様々な御協力を頂きました泉研究室の学生みなさんに深く感謝致します。

参考文献

- [1] Ken-ichi Kawarabayashi, Seri Khoury, Aaron Schild, and Gregory Schwartzman. Improved distributed approximation to maximum independent set. *arXiv preprint arXiv:1906.11524*, 2019.
- [2] Keren Censor-Hillel, Seri Khoury, and Ami Paz. Quadratic and near-quadratic lower bounds for the congest model. *arXiv preprint arXiv:1705.05646*, 2017.
- [3] Yuval Efron, Ofer Grossman, and Seri Khoury. Beyond alice and bob: Improved inapproximability for maximum independent set in congest. *arXiv preprint arXiv:2003.07427*, 2020.
- [4] Michael Luby. A simple parallel algorithm for the maximal independent set problem. *SIAM journal on computing*, 15(4):1036–1053, 1986.
- [5] Václav Rozhoň and Mohsen Ghaffari. Polylogarithmic-time deterministic network decomposition and distributed derandomization. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 350–363, 2020.
- [6] Alkida Balliu, Sebastian Brandt, Juho Hirvonen, Dennis Olivetti, Mikaël Rabie, and Jukka Suomela. Lower bounds for maximal matchings and maximal independent sets. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 481–497. IEEE, 2019.
- [7] Johan Håstad. Clique is hard to approximate within $1 - \epsilon$. *Acta Mathematica*, 182(1):105–142, 1999.
- [8] Atish Das Sarma, Stephan Holzer, Liah Kor, Amos Korman, Danupon Nanongkai, Gopal Pandurangan, David Peleg, and Roger Wattenhofer. Distributed verifica-

- tion and hardness of distributed approximation. *SIAM Journal on Computing*, 41(5):1235–1265, 2012.
- [9] Orr Fischer, Tzlil Gonen, Fabian Kuhn, and Rotem Oshman. Possibilities and impossibilities for distributed subgraph detection. In *Proceedings of the 30th on Symposium on Parallelism in Algorithms and Architectures*, pages 153–162, 2018.
- [10] Artur Czumaj and Christian Konrad. Detecting cliques in congest networks. *Distributed Computing*, 33(6):533–543, 2020.
- [11] Bala Kalyanasundaram and Georg Schintger. The probabilistic communication complexity of set intersection. *SIAM Journal on Discrete Mathematics*, 5(4):545–557, 1992.