アルゴリズム 82−2
(2002. 1. 24)

充足可能性保存変換に基づいた命題論理証明システムの提案

永田 拓也
明治大学大学院 理工学研究科
nagata@cs.meiji.ac.jp

概要: 充足可能性保存変換に基づいた命題論理証明システムを提案し、その証明システムで鳩の巣原理とk-クリークトートロジーが多項式サイズの証明を持つことを示す。またその証明システムを使った証明アルゴリズムも提案しベンチマークの結果を示す。

A propositional proof system based on satisfiability-preserving transformations

Takuya Nagata
School of Sience and Technology, Meiji University
nagata@cs.meiji.ac.jp

abstract
We propose a propositional proof system based on satisfiability-preserving transformations which has polynomial size proof of the pigeonhole principle and the k-clique tautorogy.We also present an algorithm for SAT that uses the proof system and show benchmark results.

1 はじめに

フレーゲシステムを代表とする多くの命題論理証明システムにおいて、証明の1ステップでは、これまでに証明された論理式によって含意される新たな論理式を導く。したがって、この1ステップを論理式の集合に対する変換とみたときこの変換は充足可能性を保存する等価変換である。これは、反証システムの代表であるレゾリューションでも同様である。しかしながら、反証システムにおいては論理式の充足不能を示すことが目的である。その1ステップは等価変換である必要は無く充足可能性を保存する変換であれば十分である。本稿ではこの考えに基づいた反証システム (キューブカッティングと呼ぶ) を提案し、レゾリューションでは多項式ステップで証明できない問題である鳩の巣原理とカッティングプレーンでは係数に多項式の上限があるときに多項式ステップで証明出来ない問題であるk-クリークトートロジーが多項式ステップで証明できることを示す。またこの証明システムを使った証明アルゴリズムを提案し、ベンチマークの結果を示す。

2 定義

命題変数または命題変数の否定をリテラルと呼ぶ。リテラルの和をクローズと呼ぶ。クローズはリテラルの集合として表現される。クローズの積でできたブール式をCNFと呼ぶ。CNFはクローズの集合として表現される。変数集合の部分集合に対する割り当てを部分割り当てと呼ぶ。部分割り当てをCNFに代入した結果は各クローズにその割り当てを代入し、整理したCNFである。変数 x に 0 を割り当てることを $\neg x$ と表現し、1を割り当てることを x と表現すると部分割り当てはリテラルの集合として表現される。これはクローズの表現と一致する。関数 F に部分割り当て α を代入した関数を $F(\alpha)$ と書く。リテラルの集合からリテラルの集合への関数 rev を次のように定義する。

$$rev(c) = \{\neg x | x \in c\}$$

リテラルの集合から変数の集合への関数 var を次のように定義する。

$$var(c) = \{x | x \in c \lor \neg x \in c\}$$

3 証明システムとその強さ

F, F' を証明システムとする。F の任意の証明を F' の証明に多項式時間でマッピングできるとき F' は F を p-シミュレートすると言う。代表的な証明システムには次のようなものがある。レゾリューションは鳩の巣原理の多項式サイズの証明を持たないことが知られている証明システムである [1]。カッティングプレーンは整数計画法に基づく証明システムである。カッティングプレーンは鳩の巣原理理の多項式サイズの証明を持つが、係数に多項式の上限があるとき k-クリークトートロジーの多項式サイズの証明は持たないことが知られている [2] [3]。カッティングプレーンはレゾリューションを p-シミュレートする。フレーゲシステムは現在多項式の証明サイズを持たない問題が知られていない証明システムである。フレーゲシステムはカッティングプレーンを p-シミュレートする。TF substitution フレーゲシステムはフレーゲシステムを拡張した証明システムである [4]。TF substitution フレーゲシステムはフレーゲシステムを p-シミュレートする。TF substitution フレーゲシステムはキューブカッティングを p-シミュレートすると予想される。

4 キューブカッティング

今回提案する反証システムがこのキューブカッティングである。キューブカッティングは次のルールからなる反証システムである。以下のルールを繰り返し適用し、エンプティクローズ (リテラルが 1 つもないクローズ) が導き出せたらその式は充足不能である。

- レゾリューション

  レゾリューションは 2 つのクローズ

  $a(\ni x), b(\ni \neg x)$ からクローズ $(a \cup b) \setminus \{x, \neg x\}$ を作るルールである。

- 含意クローズの削除

  2 つのクローズ a, b の間に $a \Rightarrow b$ の関係があるなら b を削除するルールである。

- キューブのカット

  関数 F と部分割り当て α のペア (F, α) をキューブと呼ぶ。キューブのカットは 2 つのキューブ $(F, \alpha), (F, \beta)(\alpha \neq \beta)$ の間に $(F, \alpha) \leq_{syn} (F, \beta)$ の関係が成り立つとき F に $rev(\alpha)$ を足すルールである。ここでキューブの二項関係 $\leq_{syn}$ は以下のように定義される。

  CNF G のどのクローズ c に対しても CNF F のクローズで c を含意するもの (c の部分集合であるもの) が存在するとき F は G を構文的に含意すると言う。F に対する 2 つの部分割当て α,$\beta(var(\alpha) = var(\beta))$ に対して $F(\alpha)$ が $F(\beta)$ を構文的に含意するとき $(F, \alpha) \leq_{syn} (F, \beta)$ であると定義する。

  キューブカットのルールは次のように正当化される。$F(\alpha)$ が $F(\beta)$ を構文的に含意するならば $F(\alpha)$ が $F(\beta)$ を含意する、すなわち前者の充足割り当てが全て後者の充足割り当てになることは明らかである。このとき、F の充足割り当て $\gamma \supseteq \alpha$ があれば $(\gamma \setminus \alpha) \cup \beta$ も F の充足割り当てである。F の充足割り当てで $F \cup \{rev(\alpha)\}$ の充足割り当てで無いものは α の拡張に限るから、$F(\alpha)$ が $F(\beta)$ を含意するという条件のもとで F の充足可能性と $F \cup \{rev(\alpha)\}$ の充足可能性は一致する。

  なお構文的含意よりも弱い含意関係をカットの条件として使うことは考えられるが理論的な含意そのものを用いることはその判定が co-NP 完全なので不適当である。

5 キューブカッティングによる証明

5.1 鳩の巣原理

鳩の巣原理は $n+1$ 羽の鳩が n 個の巣に入るとき、必ず 2 羽以上鳩が入っている巣があるという命題である。レゾリューションは多項式サイズの鳩の巣原理の証明を持たないことが証明されている。この命題を表す式は次のようになる。

式には次の変数が使われる。

$(1 \leq i \leq n+1, 1 \leq j \leq n)$

$p_{ij} = 1 \Leftrightarrow$ 鳩 i は巣 j に入っている。

鳩の巣原理の否定は次のクローズからなる式である。

1. 全ての鳩はいずれかの巣に入る。

   $$(1 \leq i \leq n+1) \quad \bigvee_{j=1}^{n} p_{ij}$$

2. 1 つの巣に鳩は 2 羽入らない。

   $$(1 \leq i \neq i' \leq n+1, 1 \leq j \leq n) \quad \neg p_{ij} \vee \neg p_{i'j}$$

キューブカティングによる証明は次のようになる。F を鳩の巣原理のクローズセットとする。以下得たク

ローズはすべて F に足し、F は随時変化するものとする。

1. 鳩 1 が巣 1 に入らずに他の鳩が巣 1 に入るキューブをカットする。

   $(2 \leq i \leq n+1, 2 \leq j \leq n)$
   $(F, \neg p_{11} p_{1j} p_{i1} \neg p_{ij}) \leq_{syn} (F, p_{11} \neg p_{1j} \neg p_{i1} p_{ij})$

   よりクローズ $(p_{11} \vee \neg p_{1j} \vee \neg p_{i1} \vee p_{ij})$ を得る。

   これと、デフォルト の クローズ $(\neg p_{11} \vee \neg p_{i1})$ $(\neg p_{1j} \vee \neg p_{ij})$ をレゾリューションすることでクローズ $(\neg p_{1j} \vee \neg p_{i1})$ を得る。

   これらを全て加えて、含意クローズを削除したクローズセットは次のようになる。

   (a) 全ての鳩はいずれかの巣に入る。
   $(1 \leq i \leq n+1) \quad \bigvee_{j=1}^{n} p_{ij}$
   (b) 1 つの巣に鳩は 2 羽入らない。
   $(1 \leq i \neq i' \leq n+1, 1 \leq j \leq n) \quad \neg p_{ij} \vee \neg p_{i'j}$
   (c) 鳩 1 が巣 1 以外の巣に入るなら鳩 1 以外の鳩は巣 1 に入れない。
   $(2 \leq i \leq n+1, 2 \leq j \leq n) \quad \neg p_{1j} \vee \neg p_{i1}$

   ここでキューブカットの条件 (構文的含意) が成り立つ理由を説明する。デフォルトのクローズである $\bigvee_{j=1}^{n} p_{ij}$ を鳩 i の要求と名前を付ける。またデフォルトのクローズセット $(1 \leq i \neq i' \leq n+1) \neg p_{ij} \vee \neg p_{i'j}$ を巣 j の要求と名前を付ける。部分割り当て $\neg p_{11} p_{1j} p_{i1} \neg p_{ij}$ を α_{ij} と置き、$p_{11} \neg p_{1j} \neg p_{i1} p_{ij}$ を β_{ij} と置く。これらはともに (入り方は違うが) 鳩 1,i が巣 1,j に入るという意味の部分割り当てである。$F(\beta_{ij})$ において、鳩 1 の要求と鳩 i の要求のクローズは満たされて消滅する。それ以外の鳩 i' の要求のクローズは代入の影響を受けず、$F(\alpha_{ij})$ のなかでも同様であるので構文的に含意される条件を満たす。巣 1 の要求は各 $i' \neq 1$ に対してクローズ $\neg p_{i'1}$ となるがこのうち $\neg p_{i1}$ は満たされて消滅する。残りのクローズ $\neg pi'1$, $i' \neq 1, i$ はすべて $F(\alpha_{ij})$ のクローズでもある。巣 j の要求についても同様である。最後にこれまでに加えられたクローズ $\neg p_{1j'} \neg p_{i'1}, i' \neq 1, j' \neq 1, (i', j') < (i, j)$ について確認する。$i = i'$ または $j = j'$ のときは β_{ij} の代入によってこのクローズは満たされて消滅する。それ以外のときはこのクローズは α_{ij} と β_{ij} のどちらの代入によっても影響を受けない。以上より $F(\alpha_{ij})$ は $F(\beta_{ij})$ を構文的に含意する。

2. 鳩 1 が巣 1 に入らないキューブをカットする。
   $(2 \leq j \leq n+1)$
   $(F, \neg p_{11} p_{1j}) \leq_{syn} (F, p_{11} \neg p_{1j})$
   よりクローズ $(p_{11} \vee \neg p_{1j})$ を得る。

   これらのクローズと デフォルトのクローズ $(\bigvee_{j=1}^{n} p_{1j})$ をレゾリューションすることでクローズ (p_{11}) を得る。これとデフォルトクローズ $(2 \leq i \leq n+1)(\neg p_{11} \vee \neg p_{i1})$ をレゾリューションしてクローズ $(\neg p_{i1})$ を得る。これとデフォルトクローズ $\bigvee_{j=1}^{n} p_{ij}$ をレゾリューションして $\bigvee_{j=2}^{n} p_{ij}$ を得る。

   これらを全て加え、含意クローズの削除をしたクローズセットは次のようになる。

   (a) 鳩 1 は巣 1 に入る。
   p_{11}
   $(2 \leq i \leq n+1) \quad \neg p_{i1}$
   (b) 全ての鳩はいずれかの巣に入る。
   $(2 \leq i \leq n+1) \quad \bigvee_{j=2}^{n} p_{ij}$
   (c) 1 つの巣に鳩は 2 羽入らない。
   $(1 \leq i \neq i' \leq n+1, 2 \leq j \leq n) \quad \neg p_{ij} \vee \neg p_{i'j}$

   キューブカットの条件 (構文的含意) が成り立つ理由を説明する。割り当て $\neg p_{11} p_{1j}$ を α_j と置き、$p_{11} \neg p_{1j}$ を β_j と置く。$F(\beta_j)$ において鳩 1 の要求は満たされて消滅する。鳩 $i (\neq 1)$ の要求は α_j, β_j の代入で影響を受けない。よって構文的含意の条件を満たす。巣 1 の要求は β_j の代入によって $\neg p_{i1} (2 \leq i \leq n+1)$ になる。F に α_j を代入すると「鳩 1 が巣 1 以外の巣に入るなら鳩 1 以外の鳩は巣 1 に入れない。」のクローズが $\neg p_{i1} (2 \leq i \leq n+1)$ になる。よって構文的含意の条件を満たす。巣 j の要求は β_j を代入すると $\neg p_{ij} \vee \neg p_{i'j} (2 \leq i \neq i' \leq n+1)$ になる。一方 α_j を代入すると巣 j の要求は $\neg p_{ij} (2 \leq i \leq n+1)$ になる。これは構文的含意の条件を満たす。巣 $j' (\neq 1, j)$ は α_j, β_j の代入によって影響を受けない。よって構文的含意の条件を満たす。「鳩 1 が巣 1 以外の巣に入るなら鳩 1 以外の鳩は巣 1 に入れない。」のクローズは β_j の代入によって $\neg p_{1j'} \vee \neg p_{i1} \quad (2 \leq i \leq n+1, 2 \leq j' \neq j \leq n)$

になる。一方 α を代入すると「鳩 1 が巣 1 以外の巣に入るなら鳩 1 以外の鳩は巣 1 に入れない。」のクローズは $\neg p_{i1}(2 \leq i \leq n+1)$ になる。これは構文的含意の条件を満たす。これまでに加えられたクローズ $p_{11} \vee \neg p_{1j'}(2 \leq j' < j)$ は β_j の代入で満たされて消滅する。以上より $F(\alpha_j)$ は $F(\beta_j)$ を構文的に含意する。

3. 鳩 1 が巣 1 以外の巣に入るキューブをカットする。

   $(2 \leq j \leq n)$

   $(F, p_{1j}) \leq_{syn} (F, \neg p_{1j})$

   よりクローズ $(\neg p_{1j})$ を得る。

   構文的含意が成り立つ理由を説明する。p_{1j} を α_j と置き、$\neg p_{1j}$ を β_j と置く。鳩 1 の要求はすでに p_{11} になっているので代入の影響を受けない。巣 j の要求は β_j の代入によって $\neg p_{ij} \vee \neg p_{i'j}(2 \leq i \neq i' \leq n+1)$ になる。一方 α_j を代入すると巣 j の要求は $\neg p_{ij}(2 \leq i \leq n+1)$ になる。これは構文的含意の条件を満たす。その他のクローズはすべて α_j, β_j の代入の影響を受けないクローズである。以上より $F(\alpha_j)$ は $F(\beta_j)$ を構文的に含意する。

   これらを全て加え、含意クローズの削除をしたクローズセットは次のようになる。

   (a) 鳩 1 は巣 1 に入る。

   p_{11}

   $(2 \leq j \leq n) \quad \neg p_{1j}$

   $(2 \leq i \leq n+1) \quad \neg p_{i1}$

   (b) 全ての鳩はいずれかの巣に入る。

   $(2 \leq i \leq n+1) \quad \bigvee_{j=2}^{n} p_{ij}$

   (c) 1 つの巣に鳩は 2 羽入らない。

   $(2 \leq i \neq i' \leq n+1, 2 \leq j \leq n) \quad \neg p_{ij} \vee \neg p_{i'j}$

以上より鳩 1 が巣 1 に入ることが決定し、残りのクローズは鳩 2, 鳩 3,,, 鳩 n+1 と巣 2, 巣 3,,, 巣 n による鳩の巣原理を表す。つまりサイズ n の鳩の巣原理をサイズ n-1 の鳩の巣原理に帰着することが出来た。

5.2 k-クリークトートロジー

k-クリークトートロジーは完全 k-1 部グラフが部分グラフとして k-クリークを持たないという命題である。カッティングプレーンは係数の大きさに多項式の上限があるとき多項式サイズの k-クリークトートロジーの証明を持たないことが証明されている。k-クリークトートロジーは次のような式で表される。

式には次の命題変数が使われる。

$(1 \leq i \leq k, 1 \leq j \leq n)$

$q_{ij} = 1 \Leftrightarrow$ クリークの頂点 i は頂点 j である。

$(1 \leq i \leq k-1, 1 \leq j \leq n)$

$c_{ij} = 1 \Leftrightarrow$ 色 i で頂点 j は塗られている。

k-クリークトートロジーの否定は次のクローズからなる式である。

1. クリークの頂点はグラフの頂点に 1 対 1 に割り当てられる。

   $(1 \leq i \leq k) \quad \bigvee_{j=1}^{n} q_{ij}$

   $(1 \leq i \leq k, 1 \leq j \neq j' \leq n) \quad \neg q_{ij} \vee \neg q_{ij'}$

   $(1 \leq i \neq i' \leq k, 1 \leq j \leq n) \quad \neg q_{ij} \vee \neg q_{i'j}$

2. グラフの頂点は丁度 1 色で塗られる。

   $(1 \leq j \leq n) \quad \bigvee_{l=1}^{k-1} c_{lj}$

   $(1 \leq l \neq l' \leq k-1, 1 \leq j \leq n) \quad \neg c_{lj} \vee \neg c_{l'j}$

3. クリークの頂点のペアは同色で塗られない。

   $(1 \leq i \neq i' \leq k, 1 \leq j \neq j' \leq n, 1 \leq l \leq k-1)$

   $\neg q_{ij} \vee \neg q_{i'j'} \vee \neg c_{lj} \vee \neg c_{lj'}$

キューブカティングによる証明は次のようになる。F を k-クリークトートロジーのクローズセットとする。以下得たクローズはすべて F に足し、F は随時変化するものとする。

1. 頂点 1 と同色の頂点がクリークの頂点になるようなキューブをカットする。

   $(1 \leq i \leq k, 2 \leq j \leq n, 1 \leq l \leq k-1)$

   $(F, \neg q_{i1} q_{ij} c_{l1} c_{lj}) \leq_{syn} (F, q_{i1} \neg q_{ij} c_{l1} c_{lj})$

   より $(q_{i1} \vee \neg q_{ij} \vee \neg c_{l1} \vee \neg c_{lj})$ を得る。これと $(\neg q_{i1} \vee \neg q_{ij})$ をレゾリューションして $(\neg q_{ij} \vee \neg c_{l1} \vee \neg c_{lj})$ を得る。

   これらを全て加え、含意クローズの削除をしたクローズセットは次のようになる。

   (a) クリークの頂点はグラフの頂点に 1 対 1 に割り当てられる。

   $(1 \leq i \leq k) \quad \bigvee_{j=1}^{n} q_{ij}$

$(1 \le i \le k, 1 \le j \ne j' \le n)$ $\neg q_{ij} \vee \neg q_{ij'}$
$(1 \le i \ne i' \le k, 1 \le j \le n)$ $\neg q_{ij} \vee \neg q_{i'j}$

(b) グラフの頂点は丁度1色で塗られる。

$(1 \le j \le n)$ $\bigvee_{l=1}^{k-1} c_{lj}$
$(1 \le l \ne l' \le k-1, 1 \le j \le n)$ $\neg c_{lj} \vee \neg c_{l'j}$

(c) グラフの頂点1と同色で塗られたグラフの頂点はクリークの頂点にならない。

$(1 \le i \le k, 2 \le j \le n, 1 \le l \le k-1)$
$\neg q_{ij} \vee \neg c_{l1} \vee \neg c_{lj}$

(d) クリークの頂点のペアは同色で塗られない。

$(1 \le i \ne i' \le k, 2 \le j \ne j' \le n,$
$1 \le l \le k-1)$
$\neg q_{ij} \vee \neg q_{i'j'} \vee \neg c_{lj} \vee \neg c_{lj'}$

2. グラフの頂点1がクリークの頂点1にならずに他のグラフの頂点がクリークの頂点1になるようなキューブをカットする。

$(2 \le i \le k, 2 \le j \le n)$
$(F, \neg q_{11} q_{1j} q_{i1} \neg q_{ij}) \le_{syn} (F, q_{11} \neg q_{1j} \neg q_{i1} q_{ij})$
よりクローズ $(q_{11} \vee \neg q_{1j} \vee \neg q_{i1} \vee q_{ij})$ を得る。これと $(\neg q_{11} \vee \neg q_{1j}), (\neg q_{i1} \vee \neg q_{ij})$ をレゾリューションして $(\neg q_{1j} \vee \neg q_{i1})$ を得る。

これらを全て加え、含意クローズの削除をしたクローズセットは次のようになる。

(a) クリークの頂点はグラフの頂点に1対1に割り当てられる。

$(1 \le i \le k)$ $\bigvee_{j=1}^{n} q_{ij}$
$(1 \le i \le k, 1 \le j \ne j' \le n)$ $\neg q_{ij} \vee \neg q_{ij'}$
$(1 \le i \ne i' \le k, 1 \le j \le n)$ $\neg q_{ij} \vee \neg q_{i'j}$

(b) グラフの頂点は丁度1色で塗られる。

$(1 \le j \le n)$ $\bigvee_{l=1}^{k-1} c_{lj}$
$(1 \le l \ne l' \le k-1, 1 \le j \le n)$ $\neg c_{lj} \vee \neg c_{l'j}$

(c) グラフの頂点1と同色で塗られたグラフの頂点はクリークの頂点にならない。

$(1 \le i \le k, 2 \le j \le n, 1 \le l \le k-1)$
$\neg q_{ij} \vee \neg c_{l1} \vee \neg c_{lj}$

(d) クリークの頂点のペアは同色で塗られない。

$(1 \le i \ne i' \le k, 2 \le j \ne j' \le n,$
$1 \le l \le k-1)$
$\neg q_{ij} \vee \neg q_{i'j'} \vee \neg c_{lj} \vee \neg c_{lj'}$

(e) グラフの頂点1がクリークの頂点1以外のクリークの頂点になるなら他の頂点はクリークの頂点1になれない。

$(2 \le i \le k, 2 \le j \le n)$ $(\neg q_{1j} \vee \neg q_{i1})$

3. クリークの頂点1がグラフの頂点1にならないキューブをカットする。

$(2 \le j \le n)$
$(F, \neg q_{11} q_{1j}) \le_{syn} (F, q_{11} \neg q_{1j})$
より $(q_{11} \vee \neg q_{1j})$ を得る。

これと $\bigvee_{j=1}^{n} q_{1j}$ をレゾリューションして (q_{11}) を得る。これと $(2 \le j \le n, 2 \le i \le k)$ $(\neg q_{11} \vee \neg q_{1j})$, $(\neg q_{11} \vee \neg q_{i1})$ をレゾリューションして $(\neg q_{1j}), (\neg q_{i1})$ を得る。これらのクローズと $\bigvee_{j=1}^{n} q_{ij}$ をレゾリューションして $\bigvee_{j=2}^{n} q_{ij}$ を得る。

これらを全て加え、含意クローズの削除をしたクローズセットは次のようになる。

(a) クリークの頂点1はグラフの頂点1である。

q_{11}
$(2 \le i \le k)$ $\neg q_{i1}$
$(2 \le j \le n)$ $\neg q_{1j}$

(b) クリークの頂点はグラフの頂点に1対1に割り当てられる。

$(2 \le i \le k)$ $\bigvee_{j=2}^{n} q_{ij}$
$(2 \le i \le k, 2 \le j \ne j' \le n)$ $\neg q_{ij} \vee \neg q_{ij'}$
$(2 \le i \ne i' \le k, 2 \le j \le n)$ $\neg q_{ij} \vee \neg q_{i'j}$

(c) グラフの頂点は丁度1色で塗られる。

$(1 \le j \le n)$ $\bigvee_{l=1}^{k-1} c_{lj}$
$(1 \le l \ne l' \le k-1, 1 \le j \le n)$ $\neg c_{lj} \vee \neg c_{l'j}$

(d) グラフの頂点1と同色で塗られたグラフの頂点はクリークの頂点にならない。

$(2 \le i \le k, 2 \le j \le n, 1 \le l \le k-1)$
$\neg q_{ij} \vee \neg c_{l1} \vee \neg c_{lj}$

(e) クリークの頂点のペアは同色で塗られない。

$(2 \le i \ne i' \le k, 2 \le j \ne j' \le n,$
$1 \le l \le k-1)$
$\neg q_{ij} \vee \neg q_{i'j'} \vee \neg c_{lj} \vee \neg c_{lj'}$

4. グラフの頂点 1 が色 1 で塗られずに他のクリークの頂点が色 1 で塗られるようなキューブをカットする。

$(2 \le i \le k, 2 \le j \le n, 2 \le l \le k-1)$

$(F, q_{ij} \neg c_{11} c_{1j} c_{l1} \neg c_{lj}) \le_{syn} (F, q_{ij} c_{11} \neg c_{1j} \neg c_{l1} c_{lj})$

より $(F, \neg q_{ij} \vee c_{11} \vee \neg c_{1j} \vee \neg c_{l1} \vee c_{lj})$ を得る。これと $(\neg c_{11} \vee \neg_c l1), (\neg c_{1j} \vee \neg c_{lj})$ をレゾリューションして $(\neg q_{ij} \vee \neg c_{1j} \vee \neg c_{l1})$ を得る。

これらを全て加え、含意クローズの削除をしたクローズセットは次のようになる。

(a) クリークの頂点 1 はグラフの頂点 1 である。

q_{11}

$(2 \le i \le k) \quad \neg q_{i1}$

$(2 \le j \le n) \quad \neg q_{1j}$

(b) クリークの頂点はグラフの頂点に 1 対 1 に割り当てられる。

$(2 \le i \le k) \quad \bigvee_{j=2}^{n} q_{ij}$

$(2 \le i \le k, 2 \le j \ne j' \le n) \quad \neg q_{ij} \vee \neg q_{ij'}$

$(2 \le i \ne i' \le k, 2 \le j \le n) \quad \neg q_{ij} \vee \neg q_{i'j}$

(c) グラフの頂点は丁度 1 色で塗られる。

$(1 \le j \le n) \quad \bigvee_{l=1}^{k-1} c_{lj}$

$(1 \le l \ne l' \le k-1, 1 \le j \le n) \quad \neg c_{lj} \vee \neg c_{l'j}$

(d) グラフの頂点 1 と同色で塗られたグラフの頂点はクリークの頂点にならない。

$(2 \le i \le k, 2 \le j \le n, 1 \le l \le k-1)$

$\neg q_{ij} \vee \neg c_{l1} \vee \neg c_{lj}$

(e) クリークの頂点のペアは同色で塗られない。

$(2 \le i \ne i' \le k, 2 \le j \ne j' \le n,$

$1 \le l \le k-1)$

$\neg q_{ij} \vee \neg q_{i'j'} \vee \neg c_{lj} \vee \neg c_{lj'}$

(f) グラフの頂点 1 が色 1 で塗られないならグラフの頂点 1 以外のクリークの頂点は色 1 で塗れない。

$(2 \le i \le k, 2 \le j \le n, 2 \le l \le k-1)$

$(\neg q_{ij} \vee \neg c_{1j} \vee \neg c_{l1})$

5. グラフの頂点 1 が色 1 で塗られないキューブをカットする。

$(2 \le l \le k-1)$

$(F, \neg c_{11} c_{l1}) \le_{syn} (F, c_{11} \neg c_{l1})$

より $(c_{11} \vee \neg c_{l1})$ を得る。これらのクローズと $(\neg c_{11} \vee \neg c_{l1})$ をレゾリューションして $(\neg c_{l1})$ を得る。

これらのクローズと $\bigvee_{l=1}^{k-1} c_{l1}$ をレゾリューションして (c_{11}) を得る。これと $(\neg c_{11} \vee \neg c_{1j} \vee \neg q_{ij})$ をレゾリューションして $(\neg c_{1j} \vee \neg q_{ij})$ を得る。

これらを全て加え、含意クローズの削除をしたクローズセットは次のようになる。

(a) クリークの頂点 1 はグラフの頂点 1 である。

q_{11}

$(2 \le i \le k) \quad \neg q_{i1}$

$(2 \le j \le n) \quad \neg q_{1j}$

(b) グラフの頂点 1 は色 1 で塗られる。

c_{11}

$(2 \le l \le k-1) \quad \neg c_{l1}$

(c) クリークの頂点はグラフの頂点に 1 対 1 に割り当てられる。

$(2 \le i \le k) \quad \bigvee_{j=2}^{n} q_{ij}$

$(2 \le i \le k, 2 \le j \ne j' \le n) \quad \neg q_{ij} \vee \neg q_{ij'}$

$(2 \le i \ne i' \le k, 2 \le j \le n) \quad \neg q_{ij} \vee \neg q_{i'j}$

(d) グラフの頂点は丁度 1 色で塗られる。

$(2 \le j \le n) \quad \bigvee_{l=1}^{k-1} c_{lj}$

$(1 \le l \ne l' \le k-1, 2 \le j \le n) \quad \neg c_{lj} \vee \neg c_{l'j}$

(e) 色 1 で塗られたグラフの頂点はクリークの頂点にならない。

$(2 \le i \le k, 2 \le j \le n)$

$\neg q_{ij} \vee \neg c_{1j}$

(f) クリークの頂点のペアは同色で塗られない。

$(2 \le i \ne i' \le k, 2 \le j \ne j' \le n,$

$(2 \le l \le k-1)$

$\neg q_{ij} \vee \neg q_{i'j'} \vee \neg c_{lj} \vee \neg c_{lj'}$

6. グラフの頂点 1 でないグラフの頂点が色 1 で塗られるキューブをカットする。

$(2 \le j \le n)$

$(F, c_{1j} \neg c_{2j}) \le_{syn} (F, \neg c_{1j} c_{2j})$

より $(\neg c_{1j} \vee c_{2j})$ を得る。

これと $(\neg c_{1j} \vee \neg c_{2j})$ をレゾリューションして $(\neg c_{1j})$ を得る。これと $\bigvee_{l=1}^{k-1} c_{lj}$ をレゾリューションして $\bigvee_{l=2}^{k-1} c_{lj}$ を得る。

これらを全て加え、含意クローズの削除をしたクローズセットは次のようになる。

(a) クリークの頂点 1 はグラフの頂点 1 である。

q_{11}

$(2 \le i \le k) \quad \neg q_{i1}$

$(2 \le j \le n) \quad \neg q_{1j}$

(b) グラフの頂点 1 は色 1 で塗られる。

c_{11}

$(2 \le l \le k-1) \quad \neg c_{l1}$

(c) グラフの頂点 1 以外のグラフの頂点は色 1 で塗られない。

$(2 \le j \le n) \quad \neg c_{1j}$

(d) クリークの頂点はグラフの頂点に 1 対 1 に割り当てられる。

$(2 \le i \le k) \quad \bigvee_{j=2}^{n} q_{ij}$

$(2 \le i \le k, 2 \le j \ne j' \le n) \quad \neg q_{ij} \vee \neg q_{ij'}$

$(2 \le i \ne i' \le k, 2 \le j \le n) \quad \neg q_{ij} \vee \neg q_{i'j}$

(e) グラフの頂点は丁度 1 色で塗られる。

$(2 \le j \le n) \quad \bigvee_{l=1}^{k-1} c_{lj}$

$(2 \le l \ne l' \le k-1, 2 \le j \le n) \quad \neg c_{lj} \vee \neg c_{l'j}$

(f) クリークの頂点のペアは同色で塗られない。

$(2 \le i \ne i' \le k, 2 \le j \ne j' \le n,$

$2 \le l \le k-1)$

$\neg q_{ij} \vee \neg q_{i'j'} \vee \neg c_{lj} \vee \neg c_{lj'}$

以上よりグラフの頂点数 n, クリークのサイズ k の式がグラフの頂点数 n-1、クリークのサイズ k-1 の式に帰着できた。

6 キューブカッティングを用いたアルゴリズム

キューブカッティングの有用な戦略を提案する。いま (F, α) をカットしたいとする。これをターゲットキューブと呼ぶ。比較対象となるキューブを (F, β) とする。

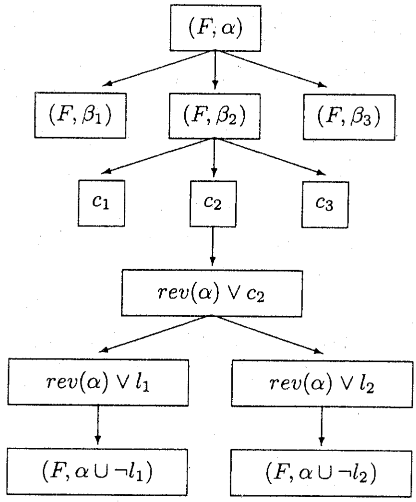

図 1: キューブカッティングの探索木

$F(\alpha)$ が $F(\beta)$ を構文的に含意するならカットできる。そうでない場合は $F(\alpha)$ が構文的に含意しないクローズが $F(\beta)$ にある。もしこれらのクローズが全て $F(\alpha)$ にあれば $F(\alpha)$ は $F(\beta)$ を構文的に含意する。構文的に含意しないクローズの 1 つを c と置く。$F(\alpha)$ が c を持つためには F にクローズ $rev(\alpha) \vee c$ があれば良い。$rev(\alpha) \vee c$ を得るためには $(F, \alpha \vee rev(c))$ がカットできれば良い。よって次のターゲットキューブとして $(F, \alpha \vee rev(c))$ を選ぶ。キューブは比較対象となるキューブを部分割り当ての長さの指数倍持つので部分割り当てが長くなりすぎるのは良くない。もし c のサイズが大きすぎる場合は $rev(\alpha)$ を含み $rev(\alpha) \vee c$ を含意するようなクローズでその替わりとする。例えば c に含まれるリテラルを $l_1, l_2, , l_n$ として $rev(\alpha) \vee l_1, rev(\alpha) \vee l_2, , , rev(\alpha) \vee l_n$ のどれかが得られれば (F, α) と (F, β) を比較するときに c の問題は解決する。よって $(F, \alpha \cup \neg l_1), (F, \alpha \cup \neg l_2), , , (F, \alpha \cup \neg l_n)$ を次のターゲットキューブとして選ぶ。これは図 1 のようなツリーになる。

このツリーをどう探索するのが良いかは今後の課題であるが今回は幅優先探索で行った。また初期のターゲットキューブには長さ 1 の部分割り当てを持つキューブを使った。

7 ベンチマーク結果

キューブカッティングを使った反証アルゴリズムを実装し、鳩の巣原理、k-クリークトートロジー、2nd DIMACS implementation Challenge, Satisfiability のベンチマーク例題に対して実行した。計算機は CPU AMD Athlon XP 1900+(1.6Ghz) memory 1.5GB を使用した。表中の深さとは図 1 の木を探索したときの深さの最大値である。ただし深さはターゲットキューブから次のターゲットキューブまでを 1 単位とする。holex.cnf は巣の数が x の鳩の巣原理である。clique-x-y.cnf はクリークのサイズが x グラフの頂点数が y のクリークトートロジーである。

8 終りに

本稿では充足可能性保存変換に基づいた証明システムを提案し、鳩の巣原理、k-クリークトートロジーが多項式サイズで証明できることを示した。またこの証明システムを使った証明アルゴリズムを提案しベンチマークの結果を示した。

参考文献

[1] J.Krajiček , P.Pudlák,and A.Wood. Exponential Lower Bounds to the size of Bounded Depth Frege Proofs of the Pigeonhole Principle. In Random Structures and Algorithms. vol. 7 pp. 1539 (1995).

[2] Maria Bonet, Toniann Pitassi, and Ran Raz. Lower bound proofs for cutting plane proofs with small coefficients.The Journal of Symbolic Logic. 62 (1997) 708 - 728.

[3] P. Pudl'ak. Lower bounds for resolution and cutting plane proofs and monotone computations. Journal of Symbolic Logic, 62:981–998, 1997.

[4] S.Buss. Some remarks on lengths of propositional proofs. Archive for Mathematical Logic, 34 (1995), pp. 377–394.

問題	変数	実行時間 (s)	深さ
hole5.cnf	30	0	4
hole6.cnf	42	1	4
hole7.cnf	56	1	4
hole8.cnf	72	2	4
hole9.cnf	90	3	4
hole10.cnf	110	6	4
hole11.cnf	132	11	4
hole12.cnf	156	18	4
hole13.cnf	182	32	4
hole14.cnf	210	53	4
hole15.cnf	240	90	4
hole16.cnf	272	155	4
hole17.cnf	306	227	4
hole18.cnf	342	356	4
hole19.cnf	380	547	4
hole20.cnf	420	830	4
clique-4-6.cnf	42	153	5
clique-4-7.cnf	49	451	5
clique-4-8.cnf	56	1143	5
clique-4-9.cnf	63	2654	5
clique-4-10.cnf	70	5474	5
clique-5-6.cnf	54	429	5
clique-5-7.cnf	63	1323	5
clique-5-8.cnf	72	3863	5
clique-5-9.cnf	81	10475	5
clique-5-10.cnf	90	21898	5
clique-6-7.cnf	77	5821	5
clique-6-8.cnf	88	16542	5
clique-6-9.cnf	99	44077	5
ssa7552-038.cnf	1501	1995	3
ssa7552-158.cnf	1363	57	2
ssa7552-159.cnf	1363	126	2
ssa7552-160.cnf	1391	186	2
ii8a1.cnf	66	30	5
hanoi4.cnf	718	1878	3

表 1: ベンチマーク結果