数理解析研究所講究録
1120巻 1999年 51-57

鳩の巣原理に対する木状導出原理の証明サイズの上下限の改良

Improved Upper and Lower Bounds of the Size of Tree-Like Resolution for the Pigeonhole Principle

宮崎 修一　　岩間 一雄
Shuichi MIYAZAKI　Kazuo IWAMA

京都大学大学院情報学研究科
〒606-8501 京都市左京区吉田本町
{shuichi,iwama}@kuis.kyoto-u.ac.jp

摘要: 鳩の巣原理に対する木状導出原理の証明サイズの上下限の改良を行なう．上限は従来の$O(n^3n!)$を$O(n^2n!)$に，下限は従来の2^nを$(\frac{n}{4\log^2 n})^n$に改良する．本結果により，鳩の巣原理に対する木状導出原理の証明サイズが一般の導出原理の証明サイズの多項式では抑えられないことが導かれる．下限の証明には，バックトラック法と木状導出原理の関係を利用するという，これまでにない新たな手法を用いた．

キーワード: 導出原理，木状導出原理，鳩の巣原理

1 はじめに

証明系とは，和積形論理式の充足不能性を証明するための非決定性の手続きであり，多項式時間で計算可能な規則を適用していくことにより充足不能性を証明する．従って，全ての充足不能論理式に対して多項式時間で動作する証明系が存在すればNP=coNPとなる[5]．しかし，NP≠coNPであることが強く予想されているため，証明系に対する証明サイズの指数下限を証明するという研究は盛んに行なわれてきた．それでもなお，Fregeシステム[3]のように，未だ指数下限が示されていない証明系は数多く存在する．

導出原理は最も基本的な証明系であり，1985年にHakenにより初めて証明サイズの指数下限が示された．Hakenは鳩の巣原理を書き下した論理式を用いて指数下限を証明したのであるが，彼の証明は難しい手法を使っており，理解が困難であった．そのため，その後も多くの研究者達が，より簡単な証明を求めて研究を進めている[1, 4, 8]．

木状導出原理は，証明が一般の有向非循環グラフでなく，木に制限された導出原理である．証明サイズの観点からは，木状導出原理の方が一般の導出原理よりも指数的に弱いというのが直観的な常識である．しかし，それにも関わらず，そのことが証明されたのはごく最近である[2]．Bonetらは，一般の導出原理では多項式サイズで証明できるが，木状導出原理ではあるϵに対して$2^{\Omega(n^\epsilon)}$ステップかかってしまう論理式の例を示した[2]．

本論文では，上述と同様の分離を鳩の巣原理に対して行なう．鳩の巣原理に対する一般の導出原理の証明サイズの上限と木状導出原理の証明サイズの下限は，これまで$O(n^32^n)$および2^nであったため[4]，上記の分離を行なうことはできなかった．本論文では下限を$(\frac{n}{4\log^2 n})^n$に改良する．これにより，鳩の巣原理に対する木状導出原理の証明サイズが，一般の導出原理の最短証明サイズの多項式では抑えられないことが分かる．また，上限に対してもわずかながら改良を行なった．

本論文では，下限の証明に，バックトラック法と木状導出原理の等価性を利用している．この等価性は一般には認識されていたが，その有効性はこれまで認められていなかった．本論文では，バックトラック法を使って木状導出原理の証明サイズの解析を行なうことにより，これまでより大きな下限を出すことができた．

本稿の構成は以下の通りである．2節では，導出原理，バックトラック法，および，鳩の巣原理に対する基本的な定義を行なう．また，上述した導出原理とバックトラック法の関係についても述べる．3

節では鳩の巣原理に対する木状導出原理の証明サイズの下限 $(\frac{n}{4\log^2 n})^n$ を示す．4節では鳩の巣原理に対する一般の導出原理の証明サイズの上限 $O(n^2 2^n)$ を示し，これを用いて木状導出原理の証明サイズの上限 $O(n^2 n!)$ を示す．これら上下限に対する議論は，一般化された鳩の巣原理（$n+1$ 対 n に限らず，m 対 n $(m > n)$ の場合）に対しても成り立つことに注意されたい．最後に，5節で今後の研究課題について述べる．

2 導出原理および鳩の巣原理

論理変数 x またはその否定 $\bar{x}$ をリテラルと言い，リテラルの和を項と言う．項の積を和積形（CNF）論理式と呼ぶ．CNF 論理式 f の変数にどのように 0 または 1 を割り当てても $f = 1$ とできないとき，f は充足不能であると言う．

鳩の巣原理とは n 要素の集合と $n+1$ 要素の集合の間に全単射がないということを述べている．($n+1$ 羽の鳩が n 個の巣に入るとき，必ず 2 羽以上入る巣が存在するという形で表される．) PHP_n^{n+1} は鳩の巣原理を和積形論理式の形で書き下したものである．PHP_n^{n+1} は $n(n+1)$ 個の変数 $x_{i,j}$ $(1 \le i \le n+1, 1 \le j \le n)$ から成り，$x_{i,j} = 1$ のとき，鳩 i が巣 j に入ると考える．PHP_n^{n+1} は以下の 2 種類の項から出来ている．(i) $(x_{i,1} + x_{i,2} + \cdots + x_{i,n})$ $(1 \le i \le n+1)$，(ii) $(\overline{x_{i,k}} + \overline{x_{j,k}})$ $(1 \le k \le n,\ 1 \le i < j \le n+1)$．従って全部で $(n+1) + \frac{1}{2}(n^2(n+1))$ 項存在する．(i) は，各鳩が必ずどこかの巣に入ることを，(ii) は，各巣には高々 1 羽の鳩しか入らないことを表した項である．(i)，(ii) の条件を満たす変数割り当ては存在しないため，PHP_n^{n+1} は充足不能である．

導出原理とは充足不能論理式に対する証明系である．導出原理は導出規則と呼ばれるただ一つの規則からなっている．導出規則は 2 つの項 $(A+x)$ および $(B+\bar{x})$ から新たな項 $(A+B)$ を導出する規則である．ただし A および B はリテラルの和を表す．$(A+x)$ および $(B+\bar{x})$ から $(A+B)$ が導出されるとき，この導出により変数 x が削除されたという．

導出原理による充足不能論理式 f の証明とは項の列 $C_1, C_2, \cdots, C_t$ のことである．ここで，各 C_i は f 中の項であるか，2 つの項 C_j と C_k $(j,k < i)$ から導出された項である．また，C_t は空の項 $(\emptyset)$ である．証明中に現れた項の数を証明のサイズと言う．

導出原理による証明は有向非循環グラフにより表すこともできる（例えば [9] 参照）．この有向非循環グラフが木であるとき，証明は木状であるといい，この木を証明木という．以下に，証明木の形式的な定義を行なう．充足不能論理式 f に対する導出原理の証明木とは根付き二分木のことである．証明木の各頂点 v には項が対応しており，これを $Cl(v)$ と書く．$Cl(v)$ は以下の条件を満たしている．v が葉のとき，$Cl(v)$ は f 中の項であり，葉でない場合は 2 つの項 $Cl(v_1)$ と $Cl(v_2)$ から導出された項である．ただし，v_1 と v_2 は v の子である．さらに，v が根のとき，$Cl(v)$ は空の項 $(\emptyset)$ である．証明木の頂点数を証明木のサイズと言う．

バックトラック法 [7] とは，CNF 論理式の充足可能性問題 (SAT) に対する解法アルゴリズムの一つである．CNF 論理式 f，f 中の変数 x，および $a \in \{0,1\}$ に対して，x に a を代入することにより f を簡単化した結果を $f_{x=a}$ で表す．バックトラック法では，適当な変数 x に対して $f_{x=0}$ と $f_{x=1}$ を計算するという手続きを再帰的に行なうアルゴリズムである．いずれかの時点で論理式が 1 に簡単化されれば f は充足可能であり，全ての葉において 0 となれば f は充足不能である．

バックトラック法による探索の様子は，バックトラック木を用いて表すことができる．充足不能論理式 f に対するバックトラック木とは，根付き二分木であり，以下の 3 つの条件を満たすものを言う．(i) 頂点 v から二つの子への枝 e_1 と e_2 には同じ変数 x に対する変数代入のラベル $(x = 0)$ と $(x = 1)$ が付いている．(ii) 任意の葉 v と任意の変数 x に対して，x は根から v までの枝に高々 1 回しか現れない．(iii) 各頂点 v に対して，根から v までの枝に現れる変数代入からなる部分割り当てを $As(v)$ で表す．このとき，各頂点 v に対して v が葉であるとき，及びそのときに限り，f は $As(v)$ で 0 になる．バックトラック木の頂点数をバックトラック木のサイズと言う．

補題 1. f を充足不能な CNF 論理式とする．もし，f に対するサイズ k の木状導出原理の証明木が存在すれば，f に対するサイズ k 以下のバックトラック木が存在する．

証明. f に対する任意の証明木を R とする．木状導出原理の場合，最小の証明木は，根から葉までのどのパスにおいても同じ変数が高々 1 度しか現れないことが知られている [9]．したがって，一般性を

失うことなく R はそのような性質を持っていると仮定する．

上述の R からバックトラック木 B を作る．B は R と同型であり，この同型性により R の頂点 v_i に対応する B の頂点を u_i とする．ここで，B の各枝に以下のようにラベルを割り当てていく．v_i を R の頂点とし，v_{i_1} と v_{i_2} を v_i の子とする．さらに，$Cl(v_i) = (A + B)$，$Cl(v_{i_1}) = (A + x)$，$Cl(v_{i_2}) = (B + \overline{x})$ であるとする．このとき，枝 (u_i, u_{i_1}) および (u_i, u_{i_2}) に，それぞれラベル $(x = 0)$ および $(x = 1)$ を割り当てる．このようにしてできた木 B が f に対するバックトラック木であることを以下で示す．

B がバックトラック木の条件 (i) および (ii) を満たすことは容易に分かる．従って，以下では条件 (iii) が成り立つことを示すわけであるが，このために，B の各葉 u に対して，$As(u)$ により f が 0 になることを言う．もし，B の葉以外の頂点で f が 0 になる場合には，その頂点以下を切り捨てて，その頂点を葉にすることによりサイズを大きくせずに条件 (iii) を満たす木に変更できるため，上述のことを示せば十分である．そのために，「各 i に対して，バックトラック木 B の割り当て $As(u_i)$ が証明木 R の項 $Cl(v_i)$ を 0 にする．」という命題が成り立つことを示す．この命題が示されれば，R の葉に対応する項は f 中の項であることから，B の各葉 u に対して，$As(u)$ により f が 0 になることが言える．上記の命題を帰納法により示す．根に対して命題が成り立つことは明らかである．次に頂点 v_i に対して成り立つと仮定する．すなわち，項 $Cl(v_i)$ が割り当て $As(u_i)$ で 0 になる，と仮定する．このとき，v_i の子でも成り立つことを示す．v_i の子を v_{i_1}，v_{i_2} とし，$Cl(v_i) = (A + B)$，$Cl(v_{i_1}) = (A + x)$，$Cl(v_{i_2}) = (B + \overline{x})$ とする．このとき，B へのラベルの付け方から，枝 (v_i, v_{i_1}) にはラベル $(x = 0)$ が付けられているはずである．従って，$As(u_{i_1}) = As(u_i) \cup \{(x = 0)\}$ である．仮定より，$As(u_i)$ が項 $(A+B)$ を 0 にするので，$As(u_{i_1})$ は項 $(A + x)$ を 0 にする．同様の議論により，$As(u_{i_2})$ が $Cl(v_{i_2})$ を 0 にすることも示される．従って上記命題は示され，B が f に対するバックトラック木であり，B の頂点数は R の頂点数以下であることが示された．□

上記の補題より，木状導出原理の証明サイズの下限を与えるには，バックトラック木のサイズの下限を与えれば良いことが分かる．

3 証明サイズの下限について

本節では，PHP_n^{n+1} に対する木状導出原理の証明サイズの下限を与える．

定理 1. PHP_n^{n+1} に対する木状導出原理の証明木のサイズは少なくとも $(\frac{n}{4\log^2 n})^n$ である．

証明. ここでは，簡単のため，$(\frac{n}{4})^{\frac{n}{4}}$ 下限を示す．定理で述べられている $(\frac{n}{4\log^2 n})^n$ への拡張は本証明の後に述べる．簡単のため n を 4 の倍数とする．補題 1 より，PHP_n^{n+1} に対するバックトラック木のサイズが少なくとも $(\frac{n}{4})^{\frac{n}{4}}$ であることを言えば良い．B を PHP_n^{n+1} に対する任意のバックトラック木とする．前述のように，B の頂点 v は部分割り当て $As(v)$ に対応している．ここで，その部分割り当てを $(n + 1) \times n$ の行列で表すことにする．図 1 は，PHP_4^5 に対する部分割り当ての例を示している．列 i，行 j のセルは変数 $x_{i,j}$ に対応しており，そのセルに 0(1) が書き込まれている状態を，変数 $x_{i,j}$ に値 0(1) が割り当てられている状態と考える．例えば図 1(b) は，$x_{1,4} = x_{2,2} = x_{4,4} = x_{5,3} = 0$，$x_{3,3} = x_{4,1} = 1$ という割り当てを表している．従って，バックトラック木 B の頂点 v が葉であるための条件は，以下の (i) または (ii) が成り立つことである．(i) $As(v)$ のある列が全て 0 である．(ii) $As(v)$ のある行に 1 が 2 つ入っている．

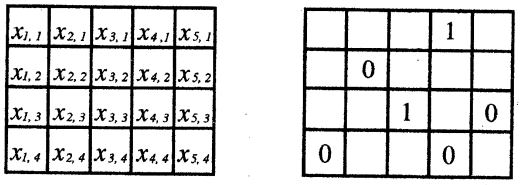

図 1: PHP_4^5 に対する部分割り当ての行列表現

ここで幾つかの表記法を定義する．部分割り当て A 中の 0 で，同じ行にも同じ列にも 1 がないものを**悪質な 0** と言い，それ以外の 0 を**良質な 0** と言う．また，$\#BZ(A)$ で A 中の悪質な 0 の数を表す．部分割り当て A で，変数 $x_{i,j}$ がまだ割り当てられておらず（すなわち，A の行列表現の (i, j) 成分が空白で），A の i 列目にも j 行目にも 1 が入っていないとき $x_{i,j}$ は**生きている**変数であると言う．例えば，図 1(b) の部分割り当てを A_0 とした場合，

$\#BZ(A_0) = 2$ ($x_{1,4}$ と $x_{2,2}$ に割り当てられた0) であり，$x_{2,4}$ は A_0 において生きている変数である．

v を B の頂点とし，v_0 と v_1 を v の子とする．また，枝 (v, v_0) と (v, v_1) に付けられているラベルをそれぞれ $(x = 0)$, $(x = 1)$ とする．このとき，頂点 v で値の代入に選ばれた変数を $Var(v)$ で表す．すなわち $Var(v) = x$ である．頂点 v に対し，$Var(v)$ に0が割り当てられた方の子（上の例では v_0）を $F(v)$，$Var(v)$ に1が割り当てられた方の子（上の例では v_1）を $T(v)$ と書く．

ここでは，バックトラック木 B の頂点数の下限を求めることが目的である．このために，B から別の木 S を作る．S の作り方を説明する前に，まず，S の持つ性質を示しておく．S の頂点集合は B の頂点集合の部分集合である．従って S の頂点数の下限はそのまま B の頂点数の下限になる．S の葉以外の頂点はちょうど1つの子，またはちょうど $\frac{n}{4}$ 個の子を持つ．また，S の高さは $\frac{n}{2}$ である．より正確には，根から各葉までのパスの長さはちょうど $\frac{n}{2}$ である．

S は以下のように作る．まず，S の根は B の根である．S の各頂点 v に対して S の子の集合 $CH(v)$ を以下のように選ぶ．$CH(v)$ は最初空であり，木 B を v から下に辿ることにより，$CH(v)$ に頂点を1つずつ加えていく．そのために，B の頂点を $T(v)$, $T(F(v)), T(F(F(v)))(= T(F^2(v))), \cdots, T(F^l(v)), \cdots$ という順に辿っていく．そして，$Var(F^l(v))$ $(l \geq 0)$ が $As(F^l(v))$ に対して生きている変数であるときに $T(F^l(v))$ を $CH(v)$ に加える．図2は S を作る際に B をどのように辿るかの例を示したものである．例えばこの例では，$Var(F^2(v))$ は $F^2(v)$ の生きている変数ではないので $CH(v)$ に $T(F^2(v))$ は選ばれていない．このようにして頂点を選んでいき，$|CH(v)|$ が $\frac{n}{4}$ になったところで子を選ぶのをやめる．この場合，v は $\frac{n}{4}$ 個の子を持つことになる．

しかし，$|CH(v)|$ が $\frac{n}{4}$ に達していない場合でも $CH(v)$ に頂点を加えるのをやめる条件がある．いずれかの列の悪質な0の数が $\frac{n}{2}$ に達した場合には $CH(v)$ に頂点を加える操作をやめてしまう．このことを正確に記述するために，B の頂点 $F^l(v)$ を考えてみる．$As(F^l(v))$ の各列の悪質な0の数は高々 $\frac{n}{2} - 1$ であり，$Var(F^l(v))$ は $x_{i,j}$ であるとする．また，$As(F^l(v))$ の i 列目はちょうど $\frac{n}{2} - 1$ 個

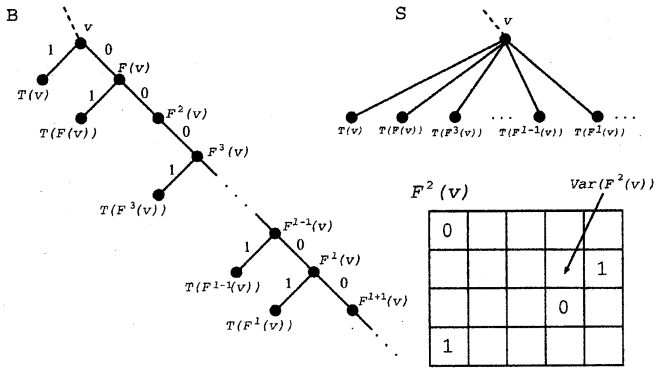

図 2: B から作られた S の一部分

の悪質な0を含んでおり，$As(F^l(v))$ の j 行目には1はないものとする．（図3に $n = 12$ の場合の例を示す．i 列目に8個の0があり，そのうち5個の0が悪質な0である．） この場合，$As(F^{l+1}(v))$ は i 列目に $\frac{n}{2}$ 個の悪質な0を含むことになり，これ以上 B を辿って $CH(v)$ に頂点を加えることはしない．つまり，$T(F^l(v))$ が最後に $CH(v)$ に選ばれた頂点となる．この場合，$|CH(v)| \leq \frac{n}{4}$ である．もし，$|CH(v)| < \frac{n}{4}$ であった場合は，最後に選ばれた $T(F^l(v))$ が S 中で v の子となる．従って，この場合は v はただ1つの子を持つ．

S の作り方から分かるように，S 中の深さ i の頂点に対応する割り当てには1がちょうど i 個あることに注意されたい．以上の操作を，根から全ての葉までの距離が $\frac{n}{2}$ になるまで続ける．

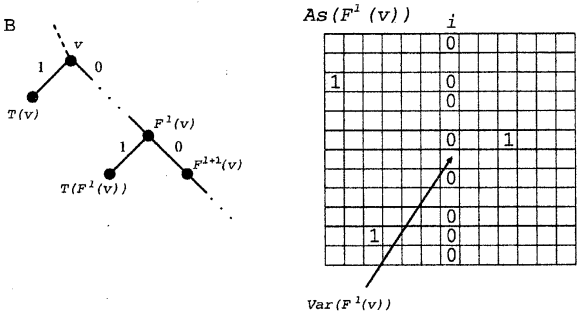

図 3: 頂点を $CH(v)$ に加えるのをやめる条件

まず，任意のバックトラック木 B から上記のように S を構成可能であることを示す．これには，S を構成するために B の頂点を辿っている間に，B の葉に到達しないことを示せば良い．ここで，u が

B の葉であるということは，$As(u)$ が PHP_n^{n+1} を 0 にするということであり，従って，$As(u)$ には 1 が 2 つある行が存在するか，全て 0 で埋まっている列が存在するかのどちらかである．前者のような割り当ては，B を辿る際にスキップしているので起こらない．以下では後者の場合が起こり得ないことを示す．S の構成法により，ある列の悪質な 0 の数が $\frac{n}{2}$ に達すると，B のその先は見ない．従って，我々の見ている範囲では悪質な 0 の数はどの列も高々 $\frac{n}{2}-1$ である．一方，S 中で深さ i にある頂点 v に対し $As(v)$ 中の 1 の数は i 個であり，S は深さ $\frac{n}{2}$ までしかないので，良質な（すなわち，同じ行に 1 を持った）0 の数はどの列においても高々 $\frac{n}{2}$ 個である．よって，どの列も 0 の数は高々 $n-1$ 個であり，葉に到達することはあり得ない．

補題 2. v を B 中の頂点とし，ある l に対して $v' = F^l(v)$ とする (図 4)．$T(v')$ が $CH(v)$ に加えられるなら，$\#BZ(As(F(v'))) = \#BZ(As(v'))+1$ であり，$T(v')$ が $CH(v)$ に加えられないなら，$\#BZ(As(F(v'))) = \#BZ(As(v'))$ である．

証明. $T(v')$ が $CH(v)$ に加えられるなら，$Var(v')$ は $As(v')$ に対して生きている変数であるため，$F(v')$ では $Var(v')$ の同じ行にも同じ列にも 1 がない．従って $Var(v')$ に代入された 0 は $As(F(v'))$ の悪質な 0 になり，$\#BZ(As(F(v'))) = \#BZ(As(v'))+1$ となる．逆の場合，すなわち $T(v')$ が $CH(v)$ に加えられない場合も同様にして示すことができる．□

以上の議論により，以下の特徴を持つ木 S を作ることが可能であることが分かった．S の任意の葉から根までの距離はちょうど $\frac{n}{2}$ ある．また，S の葉以外の頂点は子を 1 つ持つか，$\frac{n}{4}$ 個持つかのいずれかである．ここで，頂点 v が子を 1 つだけ持つとき，v とその子を結ぶ枝を**単純枝**と呼ぶことにする．

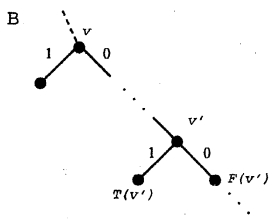

図 4: 補題 2 の例

補題 3. S 中の任意のパス $P = u_0u_1u_2\cdots u_{\frac{n}{2}}$ を考える．ただし，u_0 は根であり $u_{\frac{n}{2}}$ は葉である．もし，(u_{k-1},u_k) $(1 \le k \le \frac{n}{2})$ が単純枝でないなら，$\#BZ(As(u_k)) \le \#BZ(As(u_{k-1}))+\frac{n}{4}-1$ である．

証明. パス P 中の頂点 u_{k-1} と u_k を考える．v をバックトラック木 B 中の頂点で，u_{k-1} に対応している頂点とする．すると，B 中の $T(F^l(v))$ が S 中の u_k に対応するような l が存在する．補題 2 より，$\#BZ(As(F^l(v))) - \#BZ(As(v))$ は $T(v)$, $T(F(v)),T(F^2(v)),\cdots,T(F^{l-1}(v))$ の中で $CH(v)$ に加えられた頂点数に一致する．以上の理由から，$\#BZ(As(F^l(v)))-\#BZ(As(v)) \le \frac{n}{4}-1$ となる．また，$As(T(F^l(v)))$ は $As(F^l(v))$ のどこかのセルに 1 を 1 個加えたものなので $\#BZ(As(T(F^l(v))))$ $\le \#BZ(As(F^l(v)))$ となり，$\#BZ(As(T(F^l(v))))$ $\le$ $\#BZ(As(v))$ $+$ $\frac{n}{4}$ $-$ 1 である．すなわち，$\#BZ(As(u_k)) \le \#BZ(As(u_{k-1}))+\frac{n}{4}-1$ となる．□

補題 4. S 中の任意のパス $P = u_0u_1u_2\cdots u_{\frac{n}{2}}$ を考える．ただし，u_0 は根であり $u_{\frac{n}{2}}$ は葉である．もし，(u_{k-1},u_k) $(1 \le k \le \frac{n}{2})$ が単純枝であるなら，$\#BZ(As(u_k)) \le \#BZ(As(u_{k-1}))-\frac{n}{4}$ である．

証明. B 中の頂点 v と $T(F^l(v))$ をそれぞれ，S 中の u_{k-1} と u_k に対応する頂点とする．補題 3 と同様の議論により，$\#BZ(As(F^l(v)))-\#BZ(As(v))$ $\le \frac{n}{4}-1$ であることが分かる．$Var(F^l(v)) = x_{i,j}$ とする．(u_{k-1},u_k) が単純枝であるので，$As(F^l(v))$ の列 i には $\frac{n}{2}-1$ 個の悪質な 0 がある．ここで，$x_{i,j}$ に 1 を代入すると，少なくとも $\frac{n}{2}-1$ 個の悪質な 0 を良質に変えてしまうため，$\#BZ(As(T(F^l(v))))$ $\le \#BZ(As(F^l(v))) - (\frac{n}{2}-1)$ となる．よって，$\#BZ(As(T(F^l(v)))) \le \#BZ(As(v)) - \frac{n}{4}$，すなわち，$\#BZ(As(u_k)) \le \#BZ(As(u_{k-1})) - \frac{n}{4}$ である．□

補題 5. S 中の任意のパス $P = u_0u_1u_2\cdots u_{\frac{n}{2}}$ を考える．ただし，u_0 は根であり $u_{\frac{n}{2}}$ は葉である．このとき，P 中の単純枝の数は高々 $\frac{n}{4}$ である．

証明. P 中の単純枝の数が $\frac{n}{4}$ を超えると仮定する．パス P に沿って悪質な 0 の数を数える．根では当然 $\#BZ(As(u_0)) = 0$ である．根から下に行くに従って増加する悪質な 0 の数は，補題 3 より高々 $(\frac{n}{4}-1)(\frac{n}{4}-1) < \frac{n^2}{16}$ である．また，減少する悪質な 0 の数は，補題 4 より少なくとも $\frac{n}{4}(\frac{n}{4}+1) > \frac{n^2}{16}$ である．よって，葉では悪質な 0 の数が負となり矛

盾である．従って，P 中の単純枝の数は高々 $\frac{n}{4}$ である．□

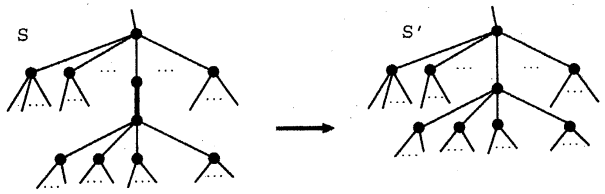

図 5: S の単純枝の除去

最後に，図 5 のように単純枝を全て取り去って新しい木 S' を作る．S' の各頂点はちょうど $\frac{n}{4}$ 個の子を持つ．また，補題 5 より，任意の葉から根までのパスの長さは少なくとも $\frac{n}{4}$ である．従って S' は，少なくとも $(\frac{n}{4})^{\frac{n}{4}}$ 個の頂点を持つ．□

注意. 上述の証明において，木 S を構成する際，各頂点の子の個数，各列に入り得る悪質な 0 の数，木 S の高さをそれぞれ，$\frac{n}{4}$，$\frac{n}{2}$，$\frac{n}{2}$ に制限した．それらを，それぞれ $\delta^2 n$，δn，$(1-\delta)n$ と置き，$\delta = \frac{1}{\log n}$ とすることにより，$(\delta^2 n)^{(1-\delta)^2 n} \geq (\frac{n}{4\log^2 n})^n$ という下限を得ることができる．

4 証明サイズの上限について

PHP_n^{n+1} に対する一般の導出原理の証明サイズは $O(n^3 2^n)$ であることが知られている [4]．本節では，文献 [4] の手法に工夫を加えることにより，上限の改良を行なう．また，ここで得られた上限から，木状導出原理の証明サイズの上限も導く．

定理 2. PHP_n^{n+1} に対する導出原理の証明でサイズ $O(n^2 2^n)$ のものが存在する．

証明. Q と R をそれぞれ集合 $\{1,2,\cdots,n+1\}$ と $\{1,2,\cdots,n\}$ の部分集合とする．このとき，$P_{Q,R}$ は $i \in Q$ かつ $j \in R$ である全てのリテラル $x_{i,j}$ の和を表すこととする．また，$[i,j]$ で集合 $\{i,i+1,\cdots,j-1,j\}$ を表すことにする．

はじめに，（導出原理による）証明の全体像を示し，後に細かな点について述べる．証明の第 0 レベルは 1 つの項 $P_{\{1\},[1,n]}$ から成る．第 1 レベルは n 個の項 $P_{[1,2],R^{(n-1)}}$ から成る．ただし，$R^{(n-1)}$ は $[1,n]$ の部分集合であり，そのサイズは $n-1$ である．よって，$R^{(n-1)}$ の取り方により $P_{[1,2],R^{(n-1)}}$ は n 個あるわけである．第 2 レベルは ${}_nC_{n-2}$ 個の項 $P_{[1,3],R^{(n-2)}}$ から成る．ただし，$R^{(n-2)}$ は $[1,n]$ の部分集合で，サイズは $n-2$ である．一般に第 i レベルは ${}_nC_{n-i}$ 個の項 $P_{[1,i+1],R^{(n-i)}}$ から成っている．ただし，$R^{(n-i)}$ は $[1,n]$ の部分集合でサイズは $n-i$ である．第 $(n-1)$ レベルには ${}_nC_1 = n$ 個の項 $P_{[1,n],\{1\}}, P_{[1,n],\{2\}}, \cdots, P_{[1,n],\{n\}}$ が存在する．最後に第 n レベルでは空の項 $(\emptyset)$ がただ 1 個存在する．これまでに現れた項を，ここでは**主項**と呼ぶことにする．主項は全部で $\Sigma_{i=0}^{i=n}({}_nC_i) = 2^n$ 個あることに注意されたい．図 6 は $n=4$ の場合の主項を表している．列 i，行 j に「+」があることは，項の中にリテラル $x_{i,j}$ が存在することを示している．

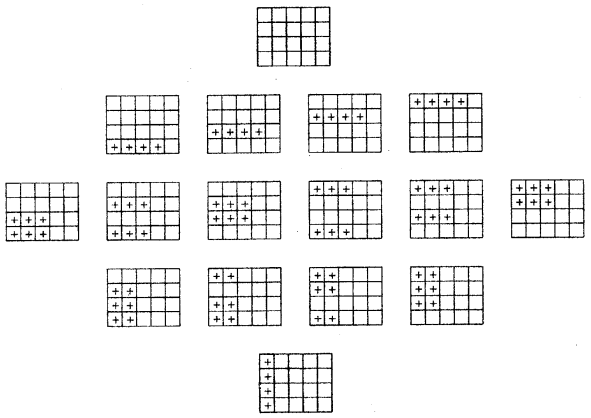

図 6: 証明に現れる主項

次に証明の細かな点について触れる．第 i レベルの各項は第 $(i-1)$ レベルにある項のうちの i 個の項と PHP_n^{n+1} 中に元々存在する項から以下のように作られる．第 i レベルの項 $P_{[1,i+1],\{j_1,j_2,\cdots,j_{n-i}\}}$ を作るために，第 $(i-1)$ レベルの i 項 $P_{[1,i],\{j_1,j_2,\cdots,j_{n-i},k\}}$ $(k \notin \{j_1,j_2,\cdots,j_{n-i}\})$ を使用する．まず，各 k に対して項 $P_{[1,i],\{j_1,j_2,\cdots,j_{n-i}\}} \cup \overline{x_{i+1,k}}$ を生成する．このためには，第 $(i-1)$ レベルの項 $P_{[1,i],\{j_1,j_2,\cdots,j_{n-i},k\}}$ と PHP_n^{n+1} 中の i 個の項 $(\overline{x_{1,k}}+\overline{x_{i+1,k}})(\overline{x_{2,k}}+\overline{x_{i+1,k}})\cdots(\overline{x_{i,k}}+\overline{x_{i+1,k}})$ を使用すれば良い．次に，今得られた i 個の項 $P_{[1,i],\{j_1,j_2,\cdots,j_{n-i}\}} \cup \overline{x_{i+1,k}}$ と PHP_n^{n+1} 中の項 $P_{\{i+1\},[1,n]}$ から，目的となる第 i レベルの項 $P_{[1,i+1],\{j_1,j_2,\cdots,j_{n-i}\}}$ を作る．第 2 レベルの $P_{[1,3],\{1,4\}}$ を第 1 レベルの 2 つの項 $P_{[1,2],\{1,2,4\}}$，$P_{[1,2],\{1,3,4\}}$ から作る様子を図 7 に示す．列 i，行 j にある「$-$」記号は，その項にリテラル $\overline{x_{i,j}}$ が存在することを示している．

上記の証明で，1 つの主項は $O(n^2)$ ステップで生成される．主項は全部で 2^n 個あるので，証明サイズは $O(n^2 2^n)$ である．□

系 1. PHP_n^{n+1} に対する木状導出原理の証明で

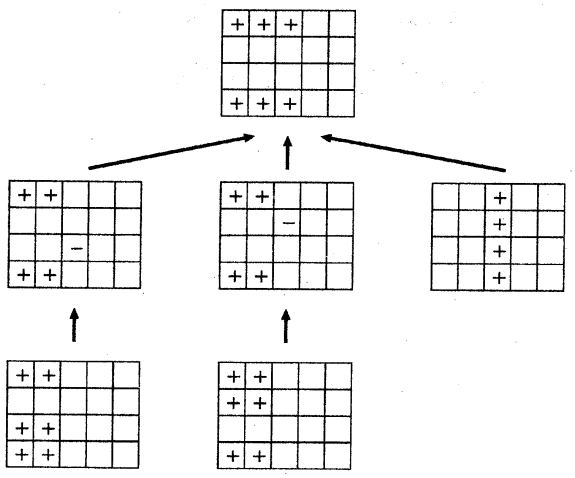

図 7: 主項の作り方

サイズ $O(n^2 n!)$ のものが存在する.

証明. 定理 2 の証明中で作った導出原理による証明を木状に展開する. 主項のみを考えると, 第 n レベルに 1 項, 第 $n-1$ レベルに n 項, 第 $(n-2)$ レベルに $n(n-1)$ 項存在することになる. 一般に, 第 i レベルには $n(n-1)\cdots(i+1)$ 個の主項が存在することになる. 従って, 主項の数は $1+\Sigma_{i=0}^{i=n-1} n(n-1)\cdots(i+1) \leq 2n!$ となる. 1 つの主項は $O(n^2)$ ステップで作ることができるため, この証明木のサイズは $O(n^2 n!)$ である. □

5 おわりに

定理 1 および定理 2 から, PHP_n^{n+1} に対する木状導出原理の証明サイズは, 一般の導出原理の証明サイズの多項式では収まらないことが分かる. 今後の課題は, 文献 [2] の改良として, 木状導出原理と一般の導出原理の証明サイズが 2^{cn} の比で異なる例を見つけることである. 別の研究テーマとしては, PHP_n^{n+1} に対する木状導出原理の証明サイズの上下限をさらに近付けることがあげられる. 本稿で得られた上限 $O(n^2 n!)$ と下限 $(\frac{n}{4\log^2 n})^n$ は, 共に $n^{(1-o(1))n}$ と同じ比率で増加するという点において, ある程度厳密である. 今後の重要な研究課題は $\Omega(n!)$ の下限を得ることである.

参考文献

[1] P. Beame and T. Pitassi, "Simplified and improved resolution lower bounds," *Proc. FOCS'96*, pp. 274–282, 1996.

[2] M. L. Bonet, J. L. Esteban, N. Galesi and J. Johannsen, "Exponential separations between restricted resolution and cutting planes proof systems," *Proc. FOCS'98*, pp. 638–647, 1998.

[3] S. Buss, "Polynomial size proofs of the propositional pigeonhole principle," *Journal of Symbolic Logic*, 52, pp. 916–927, 1987.

[4] S. Buss and T. Pitassi, "Resolution and the weak pigeonhole principle," *Proc. CSL'97*, LNCS 1414, pp.149–156, 1997.

[5] S. A. Cook and R. A. Reckhow, "The relative efficiency of propositional proof systems," *J. Symbolic Logic*, 44(1), pp. 36–50, 1979.

[6] A. Haken, "The intractability of resolution," *Theoretical Computer Science*, 39, pp. 297–308, 1985.

[7] P. Purdom, "A survey of average time analysis of satisfiability algorithms," *Journal of Information Processing*, 13(4), pp.449–455, 1990.

[8] A. A. Razborov, A. Wigderson and A. Yao, "Read-Once Branching programs, rectangular proofs of the pigeonhole principle and the transversal calculus," *Proc. STOC'97*, pp. 739–748, 1997.

[9] A. Urquhart, "The complexity of propositional proofs," *The Bulletin of Symbolic Logic*, Vol. 1, No. 4, pp. 425-467, 1995.