ブール関数の複雑さに関する研究

博士学位論文

ブール関数の複雑さに関する研究

東北大学大学院情報科学研究科

情報基礎科学専攻

西関研究室

福原 秀明

2010 年 1 月 29 日

目 次

第1章　序論

1.1　本論文の背景

ソフトウェア開発を行う際に重要な情報の一つは，考慮下の問題を計算機で解くために，どの程度の時間がかかるか，また，どの程度のメモリが必要となるか，という情報である．理論計算機科学の分野では，上記のような時間的・空間的リソースの量を問題の複雑さと定義し，それを明らかにすることを目標としている．問題の複雑さを明らかにするために古くから取られているアプローチは，計算機で解くべき問題をブール関数として定式化し，計算機の理論的モデルであるチューリング機械を用いて議論を行う，というものである．本分野で長年注目を浴びてきたP vs. NP問題は，このチューリング機械を基に定義されている問題であり，計算機で現実的な時間内に解ける問題と解けない問題を区別する問題に深くかかわっている．ここで，Pとはチューリング機械が入力長の多項式時間で解を求められる問題の集合であり，NPとはチューリング機械が与えられた正しい解に対してその正当性を入力長の多項式時間で検証できる問題の集合である．

理論計算機科学の分野において，問題の複雑さを明らかにしようとする研究の立場は大きく分けて二つある。一つは問題を解くために必要となるリソースの十分な量、つまりリソースの量の上界を明らかにする立場である。もう一つは、問題を解くために最低限必要となるリソースの量、つまりリソースの量の下界を明らかにする立場である。上界と下界が一致すれば，考慮下の問題の複雑さを正確に求めたこととなるため，問題の複雑さ解明のために小さな上界の導出と大きな下界の導出が求められる．上界を明らかにする立場であるアルゴリズム理論と比べると，下界を明らかにする証明手法のほうが少ないのが実情である．本論文はこの下界を明らかにする立場に基づくものである。

下界を研究する意義としては，アルゴリズムを設計するにあたり，時間計算量を小さくするためにどこまで労力をかければよいか，ということに関する目標が得られることがある．また，ある問題の下界が非常に大きいことが既に判明して

いれば，正面からその問題に立ち向かうのではなく，近似アルゴリズムで解決するという方法を取ることもできるだろう．アルゴリズムが複数の手続きで構成されている場合には，計算時間のボトルネックとなっている手続きの時間計算量の上界と下界の差が大きければ，その手続きに対して改善を図れることによりアルゴリズム全体の時間計算量が劇的に改善される可能性がある．このように，下界を研究する意義はアルゴリズムの観点から非常に大きい．

本論文では，論理回路に制限を加えたブール式，量子回路の演算で定義される量子質問モデル，という二つの計算モデルについて扱う．論理回路はチューリング機械に並ぶ代表的な計算モデルであり，そのサイズがチューリング機械の計算時間と対応するという結果が知られている．よって，論理回路における研究の進展はチューリング機械における研究の進展に繋がる．ブール式は，各演算子を論理ゲートとみなせば，論理回路の各ゲートの出次数を 1 に制限した回路とみなせる．ブール式は論理回路との関係性や，命題論理を表現することから古くから研究の対象とされてきた．ブール式のサイズとは式に現れる変数の数のことであり，ブール関数 f のブール式複雑さとは f を表すブール式の中でサイズが最小であるブール式のサイズのことである．論理回路のサイズにおいては $2^n/n$，ブール式のサイズにおいては $2^n/\log(n)$ という下界を持つ関数が存在することが知られている一方で、明示的に定義された関数に対する下界の中で現在知られている最大のものは，論理回路は $5n - o(n)$[15]，ブール式は $n^{3-o(1)}$[11] である．これは，強力な下界導出手法が存在していないという事情による．明示的に定義された関数に対する超多項式の下界の導出は，論理回路の分野における重要な課題である．

論理回路は AND ゲート，OR ゲート，NOT ゲートなどの論理ゲートを用いて決定的計算を行う回路であるが，量子計算を行える量子論理ゲートを用いた回路として，量子回路がある．そして，量子回路を基に興味深い計算モデルである量子質問モデルが提案されている．質問モデルとは，問題に対する正しい出力を得るために，入力の情報はどの程度必要なのか，という点に着目して提案されたモデルであり，複雑さは入力へのアクセス回数で定義される．入力へのアクセスを質問と呼ぶ．決定的質問モデルでは，入力への一回の質問によってある 1 ビットを得ることができる．一方，量子質問モデルでは，入力への一回の質問によってある 1 量子ビットを得ることができる．どちらのモデルにおいてもその複雑さは，最悪な入力に対する質問回数を最小とするアルゴリズムの質問回数として定義される．このモデルが特に注目されるようになった契機は，Grover の探索アルゴリズム [10] の発表である．このアルゴリズムが解く探索問題とは，未知の n 個の要素

の中から目的物を探し出す問題である．決定的なアルゴリズムでは最悪では n 回の探索が必要であるが，量子計算が行えるアルゴリズムでは $O(\sqrt{n})$ 回の探索で高確率で目的物を見つけることができる．探索問題は入力 n ビット中で値が 1 のビットを探し出す問題と考えると，量子質問モデルにおいて OR 関数を計算する問題ととらえることができる．このように，探索問題は量子質問モデルで表現できる．量子計算の分野においては，決定的計算や確率的計算を行うモデルと量子計算を行うモデルとの間に，どの程度の計算力の差があるかを示すことが重要な課題となっている．量子質問モデルにおいても，その古典的モデルである決定的質問モデルとの間の計算力の差を明らかにすることが重要な課題である．確率 ϵ の誤りを許す量子質問複雑さ Q_ϵ と決定的質問複雑さ D に対して，多くの研究者たちが次の予想を掲げており，重要な未解決問題である．

2 乗ギャップ予想 [5] 任意のブール関数 f と $\epsilon \in [0, 1/2)$ に対して，

$$Q_\epsilon(f) = \Omega(\sqrt{D(f)}).$$

問題の複雑さに対する下界研究において，任意のブール関数 f に対し、その最適値が f に対する複雑さの下界を与えるような数理計画問題を導入する方法がある．f から最適値への写像を下界指標と呼ぶ．例えば，Khrapchenko の指標 [19] はブール式複雑さに対する下界指標であり，以下のような数理計画問題で定義される．

Khrapchenko の指標 [19] 任意のブール関数 $f : \{0,1\} \to \{0,1\}^n$ に対して，

$$\begin{aligned} \text{maximize} \quad & \frac{|C|^2}{|A||B|} \\ \text{subject to} \quad & A \subseteq f^{-1}(0) \\ & B \subseteq f^{-1}(1) \\ & C = \{(x,y) \in A \times B : d_H(x,y) = 1\}. \end{aligned}$$

ここで，$f^{-1}(0)$ は $f(x) = 0$ である全ての $x \in \{0,1\}^n$ からなる集合であり，$f^{-1}(1)$ は $f(y) = 1$ である全ての $y \in \{0,1\}^n$ からなる集合である．また，$x, y \in \{0,1\}^n$ に対する $d_H(x,y)$ は x と y のハミング距離である．

数理計画問題による下界導出の手法には，次の三つの利点がある．

1. 任意の関数に対し下界が導出できる．
2. 数値計算により下界が導出できる．
3. 下界導出のために，数理計画問題の定理を利用できる．

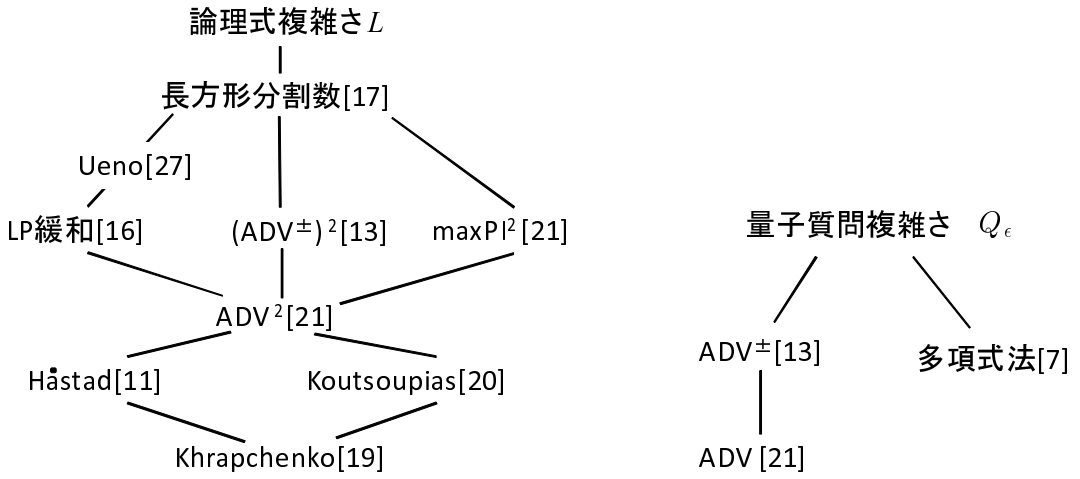

図 1.1: ブール式複雑さの下界を与える指標の関係図（左）と量子質問複雑さの下界を与える指標の関係図（右）.

項目 1 については，NP 完全問題や指数完全問題に対しても非自明な下界を導出できることが期待される．項目 2 については，計算機を用いて下界の値を数値的に求めることができるため，解析的な下界に関する洞察を得ることができるという利点がある．項目 3 については，下界を最大化問題として定式化し，その許容解を構成することによって下界を得るという手法を用いることが可能となる．

本論文では特に，量子敵対者限界 (ADV) と長方形分割数という下界指標を取り上げ，これらを用いて量子質問複雑さとブール式複雑さの下界の導出を試みる．ADV は 2003 年に Barnum ら [6] によって提案された量子質問複雑さに対する下界指標であり，その後の 2005 年に Laprante ら [21] によってその 2 乗の値がブール式複雑さに対する下界指標でもあることが示された．長方形分割数は 1990 年に Karchmer ら [17] によって提案されたブール式複雑さに対する下界指標である．量子敵対者限界は，量子質問複雑さとブール式複雑さの二つの下界を与える．長方形分割数は，ブール式複雑さに対して現在までに提案されている指標の中で最も大きな下界を示す可能性を持つ．これら二つの指標と，他のブール式複雑さの下界指標との関係を図 1.1 に示す．下界指標に特に名前がつけられていない場合には，著者名を記している．図 1.1 において，二つの下界指標の間の実線は，任意の関数に対して，上にある下界指標の値が下にある下界指標の値以上の値を与える下界指標であることを意味する．ブール式複雑さと量子質問複雑さ自身も下界指標であり，図 1.1 では共に最も上に位置する．図 1.1 内の maxPI[21] と $\mathrm{ADV}^{\pm}$[13] は共

に量子敵対者限界 ADV に部分的な変更を加えた指標である．各指標についてより詳しくは，文献 [19, 20, 11, 21, 13, 16, 17, 7] を参考にされたい．

下界指標を利用することで、最簡な式を求めることができる可能性がある．なぜなら，ブール式複雑さの下界指標の値とあるブール式 F のサイズが一致すれば F が最簡であることが分かるからである．ブール式については，大きな下界を求めること以外にも最簡な式，つまり，上界と下界が一致する式を求めることが，実際にブール式を用いて関数を表現する場合に重要である．指数的な論理式複雑さの下界を持つブール式が存在することが知られている一方で，特定の関数に対しては $n^{3-o(1)}$ という多項式の下界しか得られていない現状からも，最簡な式を求める困難さは明らかである．しかし，限定された関数のクラスに対しては，現状でも最簡な式を特定することができる可能性がある．最簡な式に関する研究は [2] や [26] などに見られる．

1.2　結果の概要と意義

本論文では，ソフトランクとシングルトン被覆数という下界指標を導入する．ソフトランクは量子敵対者限界に対する下界指標であり，よって，量子質問複雑さに対する下界指標である．一方，シングルトン被覆数は長方形分割数に対する下界指標であり，よって，ブール式複雑さに対する下界指標である．ソフトランクとシングルトン被覆数を用いて以下の三つの結果を示す．

一つ目は，ソフトランクを用いて示される量子質問複雑さに関する結果であり，パリティノード付き一回読み決定木で表される任意のブール関数に対し，2 乗ギャップ予想が成立する，というものである．ここで，一回読み決定木とは各変数が決定木の中に一回しか現れない決定木のことであり，パリティノードは通常の内部ノードではない，排他的論理和関数を計算する特殊なノードのことである．さらに，その結果を拡張し，基底関数が $\{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}, \mathrm{XOR}, \mathrm{MUX}\}$ である一回読みブール式によって表される任意の関数に対しても，2 乗ギャップ予想が成立することを示す．ここで，一回読みブール式とは各変数が式の中に一回しか現れないブール式のことである．また，XOR は 2 変数排他的論理和関数であり，MUX は 2 入力マルチプレクサ関数である．これらの結果は，前述の 2 乗ギャップ予想に対するさらなる証拠を示すものである．

二つ目は，長方形分割数を定義している数理計画問題の条件を緩和することに

より，計算量を著しく改善したシングルトン被覆数と呼ばれる下界指標が得られるというものである．シングルトン被覆数を用いて 8 入力マルチプレクサ関数に対するブール式複雑さの下界が得られ，その下界は Ueno の手法によって得られる下界よりも大きいことも示す．

三つ目は，量子敵対者限界を用いて示される最簡なブール式に関する結果である．合成関数に対する量子敵対者限界の性質を用いることにより，基底を $\mathfrak{B} = \{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}, \mathrm{XOR}, \mathrm{MUX}\}$ とした一回読みブール式のある部分クラスは，演算子を再帰的に最簡なブール式に置き換えるという操作により，標準基底 $\{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}\}$ 上の最簡なブール式が得られることを示す．さらに，基底を $\mathfrak{B}$ とする一回読み式に対して標準形を定義し，標準形が NPN 同値類の代表元とできることを示す．NPN 同値である関数は全て本質的に同じ構造を持つ式によって表現されるという事実から，標準形を用いることにより，本質的に構造が異なる最簡な式の集合を定義することが可能となる．

1.3　本論文の構成

本論文の残りは 2 章から 6 章の 5 つの章で構成される．

第 2 章　準備

第 2 章では，本論文を通して必要な基礎的な定義と，それに関連する既に知られている性質について述べる．具体的には，本研究の対象とする計算モデルである，ブール式，決定的質問モデル，量子質問モデルの定義を行う．量子質問モデルについては，その背景知識も紹介する．さらに，下界指標である量子敵対者限界と長方形分割数についての定義を行う．

第 3 章　一回読みブール関数に対する量子質問複雑さの下界

第 3 章では，ソフトランクを導入し，ソフトランクを用いてパリティノード付き一回読み決定木と $\{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}, \mathrm{XOR}, \mathrm{MUX}\}$ を基底関数とする一回読みブール式が表す関数に対し，2 乗ギャップ予想が成立することを示す．

第 4 章　シングルトン被覆によるブール式複雑さの下界

第 4 章では，シングルトン被覆数を導入し，シングルトン被覆数を用いて，8 入力マルチプレクサ関数に対して，Ueno の手法より大きな下界を与えることができ

ることを示す.

第 5 章　最簡なブール式のクラスとその NPN 代表元

第 5 章では，量子敵対者法を用いて，{AND, OR, NOT, XOR, MUX} を基底関数とする一回読みブール式のある部分クラスが，単純な基底変換により標準基底 {AND, OR, NOT} 上の最簡なブール式に変形できることを示す．さらに，最簡なブール式のうち本質的に構造が異なる式を標準形という概念を用いて示す.

第 6 章　まとめ

第 6 章では，本研究のまとめをする.

第2章　準備

2.1　はじめに

本章では，ブール式，決定的質問モデル，量子質問モデルの三つの計算モデルを紹介すると共に，各計算モデルにおける複雑さの尺度である，ブール式複雑さ，決定的質問複雑さ，量子質問複雑さの定義を与える．その後，ブール式複雑さの下界となる二つの指標，量子敵対者限界と長方形分割数の定義を与える．

2.2　ブール関数とブール式

0 と 1 の 2 つの値しかとらない変数を論理変数という．一般に，値 0 は偽，値 1 のは真の状態を表しているものと考える．関数

$$f : \{0,1\}^n \to \{0,1\}$$

を n 変数ブール関数という．変数の個数を省略しても混同の恐れがない場合には，単にブール関数ということもある．本論文において用いる基本的な五つのブール関数論理否定 NOT，論理積 AND，論理和 OR，排他的論理和 XOR，2 入力マルチプレクサ関数 MUX の真理値表を表 2.1，2.2，2.3 に示す．

n を任意の自然数とする．ある $i \in \{1,2,\ldots,n\}$ に対し，i 番目の変数への割り当てを出力する n 変数ブール関数をプロジェクション関数 $\mathrm{PROJ}_{i,n}$ と呼ぶ．変数の数を特に指定しない場合には，PROJ_i と記す．

あるブール関数 f に対して，f の否定関数を $\bar{f}$ と記す．すなわち，任意の入力 $\boldsymbol{x}$ に対して，$f(\boldsymbol{x}) = 0$ のとき $\bar{f}(\boldsymbol{x}) = 1$，$f(\boldsymbol{x}) = 1$ のとき $\bar{f}(\boldsymbol{x}) = 0$ となる．

ブール関数を式として表現する場合には，次に示すブール式が用いられる．

定義 2.1 ($\mathfrak{B}$ 式) 基底 $\mathfrak{B}$ をあるブール関数の集合とする．$\mathfrak{B}$ を基底とするブール式とは，以下のような式のことである．$\mathfrak{B}$ を基底とするブール式を $\mathfrak{B}$ 上のブール式や $\mathfrak{B}$ 式とも呼ぶことにする．

表 2.1: NOT 関数の真理値表

x	NOT(x)
0	1
1	0

表 2.2: AND 関数，OR 関数，XOR 関数の真理値表

x	y	AND(x,y)	OR(x,y)	XOR(x,y)
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

表 2.3: MUX 関数の真理値表

x	y	z	MUX(x,y,z)
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

1. 定数 0 と 1 は $\mathfrak{B}$ 式である．

2. 論理変数を $x_1, x_2, \ldots$ で表す．自然数 i に対して，x_i は $\mathfrak{B}$ 式であり，x_i の表す関数はプロジェクション関数 PROJ_i である．

3. $\mathfrak{B}$ に含まれる任意の k 変数ブール関数 f に対して，その関数名を OP_f とする．任意の k 個の $\mathfrak{B}$ 式 $F_1, F_2, \ldots, F_k$ に対し，$\mathrm{OP}_f(F_1, F_2, \ldots, F_k)$ は $\mathfrak{B}$ 式である．式 $\mathrm{OP}_f(F_1, F_2, \ldots, F_k)$ は，式 $F_1, F_2, \ldots, F_k$ が表すブール関数と f との合成によって得られる関数を表す．

例えば，$\mathcal{B} = \{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}, \mathrm{XOR}, \mathrm{MUX}\}$ とすると，次の式は $\mathcal{B}$ 式である．論理変数 $x_1, x_2, \ldots, x_6$ を定義域を $\{0, 1\}$ とする論理変数とする．

$$\mathrm{AND}(\mathrm{OR}(x_1, x_2), \mathrm{MUX}(\mathrm{XOR}(x_2, x_3), x_6, \mathrm{AND}(x_5, x_4))).$$

関数 NOT，AND，OR，XOR は，式において，それぞれ $\neg$，$\wedge$，$\vee$，$\oplus$ という演算記号を用いても表す．すなわち，二つの論理変数 x_1 と x_2 に対し，$\mathrm{NOT}(x_1)$ を $\neg x_1$，$\mathrm{AND}(x_1, x_2)$ を $x_1 \wedge x_2$，$\mathrm{OR}(x_1, x_2)$ を $x_1 \vee x_2$，$\mathrm{XOR}(x_1, x_2)$ を $x_1 \oplus x_2$ とも書く．これらの演算記号を用いると，関数 MUX は次の式で表される．x_1, x_2, x_3 を論理変数とする．

$$\mathrm{MUX}(x_1, x_2, x_3) = (\neg x_1 \wedge x_2) \vee (x_1 \wedge x_3).$$

演算子 $\wedge$ はしばしば省略される．例えば、$x_1 \wedge x_2$ を $x_1 x_2$ とも書く．また，変数に否定演算子 $\neg$ が付く場合、上線付きの変数として書く．例えば，$\neg x_1$ を $\bar{x}_1$ と書く．論理変数と否定演算子のついた論理変数は**リテラル**と呼ばれる．

基本演算 $\{\wedge, \vee, \neg\}$ において成立する基本公式を以下に示す．これらの等式を用いて，ブール関数を表現する式を任意に変形できるので，その解析が容易になる．

1. 定数に関する演算律

$$1 \vee x = 1,\ 1 \wedge x = x,$$

$$0 \vee x = x,\ 0 \wedge x = 0.$$

2. 巾等律

$$x \vee x = x,\ x \wedge x = x.$$

3. 交換律

$$x \vee y = y \vee x,\ x \wedge y = y \wedge x.$$

4. 結合律

$$(x \vee y) \vee z = x \vee (y \vee z),\ (x \wedge y) \wedge z = x \wedge (y \wedge z).$$

5. 分配律

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z),\ x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

6. 二重否定の法則

$$\neg(\neg x) = x.$$

7. 補元律

$$x \vee \neg x = 1,\ x \wedge \neg x = 0.$$

8. ド・モルガンの法則

$$\neg(x \vee y) = \neg x \wedge \neg y,\ \neg(x \wedge y) = \neg x \vee \neg y.$$

ブール式の複雑さは，$\{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}\}$ を基底とするブール式を用いて定義される．この基底を標準基底と呼ぶ.

定義 2.2 $\mathfrak{B}^* = \{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}\}$ とする．$\mathfrak{B}^*$ 式 F の**サイズ** $\mathrm{size}(F)$ とは，F に現れる論理変数の個数であり．ブール関数 f の**ブール式複雑さ** $L(f)$ とは，f を表す $\mathfrak{B}^*$ 式の中で，サイズが最小の $\mathfrak{B}^*$ 式のサイズのことである．ブール関数 f を表す $\mathfrak{B}^*$ 式 F のサイズが $L(f)$ に等しいとき，F を最簡な式という.

基底を明記せず単にブール式と書いた場合には，標準基底上のブール式を意味する．また，ブール式 F と F が表す関数 f をしばしば同一視する．例えば，$L(F)$ と表記した場合，それは $L(f)$ を意味する.

2.3　長方形分割数

本節では，ブール式複雑さの下界を与える指標である長方形分割数の定義を与える.

Karchmer と Wigderson[17] は任意のブール関数に対するブール式複雑さを，Karchmer-Wigderson game と呼ばれるコミュニケーションゲームを用いた特徴付けを行った．このゲームへの入力は，n 変数ブール関数 f である．このゲームは，二人のプレイヤー，アリスとボブによって行われる．まず，アリスには $f(x) = 1$ である，ある入力 $x = (x_1, \ldots, x_n)$ が与えられ，ボブには $f(y) = 0$ である，ある入力 $y = (y_1, \ldots, y_n)$ が与えられる．彼らの目標は，$x_i \neq y_i$ であるインデックス i を見つけることであり，そのために彼らは互いにメッセージを送りあうことができる．より具体的には，このコミュニケーションプロトコルは，次のような二分木で表現される．$X = \{x | f(x) = 0\}$，$Y = \{y | f(y) = 1\}$ とする．

- 各内部ノード v が $a_v : X \to \{0, 1\}$ か $b_v : Y \to \{0, 1\}$ のどちらかの関数でラベル付けられている．a_v のラベルが付けられたノード v ではアリスがメッセージを送ることを表し，b_v のラベルが付けられたノード v ではボブがメッセージを送ることを表す．

- 任意の (x, y) に対して，根から下ることで到達する葉には $x_i \neq y_i$ であるようなあるインデックス i でラベル付けられている．

葉の数を最小にするコミュニケーションプロトコルの葉の数を，プロトコル分割数 $C^P(f)$ と呼ぶ．

定理 2.1 ([17]) 任意のブール関数 f に対して，$L(f) = C^P(f)$

定義 2.3 (コミュニケーション行列) f のコミュニケーション行列 M_f を次のように定義する．M_f の行と列は $f^{-1}(0)$ の要素と $f^{-1}(y)$ の要素でそれぞれ番号づけられているとし，成分 $(x \in f^{-1}(0), y \in f^{-1}(1))$ を $M_f[x, y] = \{i | x_i \neq y_i\}$ とする．$X \subseteq f^{-1}(0)$，$Y \subseteq f^{-1}(1)$ に対し，直積 $X \times Y$ を M_f の長方形と呼ぶ．ある i $(i \in \{1, 2, \ldots, n\})$ が存在して，$X \times Y$ に含まれる任意の (x, y) に対して，$M_f[x, y] \ni i$ であるとき，$X \times Y$ を単色長方形と呼ぶ．M_f の長方形の集合 $R_1, R_2, \ldots, R_k$ が M_f を覆うとは，任意の $(x, y) \in f^{-1}(0) \times f^{-1}(1)$ に対し，ある i $(i \in \{1, 2, \ldots, k\}$ が存在して，$(x, y) \in R_i$ が成り立つことである．

定義 2.4 (長方形分割数) ブール関数 f に対して，そのコミュニケーション行列を M_f とする．M_f を覆うために必要な互いに素な単色長方形の集合の要素数の最小値を f の**長方形分割数**と呼び，$C^D(f)$ と記す．

ブール関数 f に対する任意のコミュニケーションプロトコルを考える．そのプロトコルにおける任意の葉 l に対し，R_l を葉 l に到達する $(x, y) \in f^{-1}(0) \times f^{-1}(1)$ の集合とすると，R_l は明らかに単色である．また，異なる葉 l, l' に対し，$R_l \cap R_{l'} = \emptyset$ なので，$\{R_l \mid l$ はプロトコルの葉 $\}$ は M_f を覆う互いに素な単色長方形の集合である．よって，任意のブール関数 f に対して $C^D(f) \leq C^P(f)$ となり，次の系が得られる．

系 2.2 任意のブール関数 f に対して，$L(f) \geq C^D(f)$ である．

2.4　決定的質問モデル

ブール関数 $f : \{0,1\}^n \to \{0,1\}$ を計算する決定的質問アルゴリズムとは，f の任意の入力割り当て $\boldsymbol{a} \in \{0,1\}^n$ に対し，$\boldsymbol{a}$ が入力として与えられると $f(\boldsymbol{a})$ を出力するものである．ただし，アルゴリズムは入力 $\boldsymbol{a}$ に直接アクセスできず，オラクルへのアクセスを通して間接的に $\boldsymbol{a}$ に関する情報を得る．オラクルは整数 $i \in \{1, 2, \ldots, n\}$ が入力として与えられると，割り当て $\boldsymbol{a}$ の i ビット目の値 a_i を返す．このようにアルゴリズムはオラクルに 1 回質問することによって割り当て $\boldsymbol{a}$ の特定の 1 ビットを得ることができる．f を計算する決定的質問アルゴリズム A に対し，A の決定的質問複雑さとは，全ての入力割り当て $\boldsymbol{a}$ の中でアルゴリズム A が $f(\boldsymbol{a})$ を出力するために要する質問回数の最大値である．

定義 2.5 任意のブール関数 f に対して，f の**決定的質問複雑さ**とは，f を計算する決定的質問アルゴリズムの中で，決定的質問複雑さが最小であるアルゴリズムの決定的質問複雑さであり，$D(f)$ と記す．

決定的質問アルゴリズムと以下で定義する決定木は，後に示すように等価である．

n をある自然数とする．本論文において，決定木とは根つき順序二分木のことであり，各内部ノードはある $i \in \{1, 2, \ldots, n\}$ に対する論理変数 x_i でラベル付けられており，各葉は 0 か 1 の値でラベル付けられている．図 2.1 に決定木の例を示す．決定木 T に現れる論理変数が $x_1, x_2, \ldots, x_n$ のとき，T は n 変数ブール関数を表す．$\mathbf{a} \in \{0,1\}^n$ に対する決定木の出力は次のようにして決まる．根から始まり，次の操作を繰り返す：現在対象としているノードが葉であるときは，操作を終了しその葉の値 (0 または 1）を出力する．そうではなくノードのラベルが x_i である場合には，$a_i = 0$ であるときには左の子へ，$a_i = 1$ であるときには右の子へ進む．

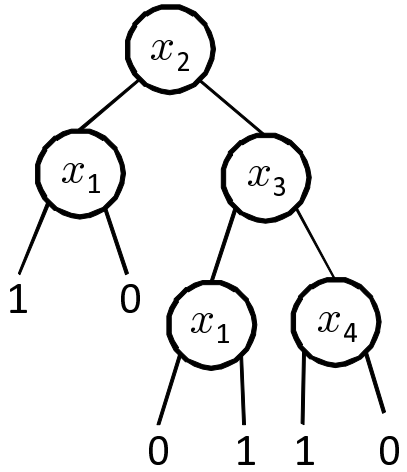

図 2.1: 決定木の例

ある決定木が n 変数ブール関数 f を計算するとは，任意の $\mathbf{a} \in \{0,1\}^n$ に対して，その決定木の出力が $f(\mathbf{a})$ となるときをいう．以下ではしばしば決定木 T とそれが計算する関数を同一視し，$\mathbf{a} \in \{0,1\}^n$ に対する T の出力を $T(\mathbf{a})$ と記す．

定義 2.6 任意の決定木 T に対して，T の深さとは，T の根から葉までのパスの中で最長のパスの長さである．ブール関数 f に対する**決定木の複雑さ**とは，f を計算する深さが最小の木の深さである．

決定木をアルゴリズムと見立てたとき，$\mathbf{a}$ の各桁 a_i $(i \in \{1,2,\ldots,n\})$ の値を参照することは $\mathbf{a}$ を有するオラクルに対して質問をすることとみなすことができる．よって，決定木と決定的質問アルゴリズムは等価である．決定木の深さは最悪な入力に対する質問回数に対応するため，決定木複雑さは決定的質問複雑さと等価である．よって，f に対する決定木複雑さも決定的質問複雑さと同じ記号を用いて $D(f)$ と記すこととする．

定義 2.7 ある決定木 T に対して，$\bar{T}$ を T の各葉のラベルの 0 と 1 を反転して得られる木とする．

明らかに，$\bar{T}$ の計算する関数は T の計算する関数の否定関数である．すなわち，任意の x に対して，$\bar{T}(x) = 1 - T(x)$ である．

2.5　量子質問モデル

本章では，まず準備として量子計算で用いられる演算について定義する．記法等については，文献 [18] と [24] に準ずる．次に，量子力学の公理系について紹介する．それを基に量子アルゴリズムが定義されることを示し，量子アルゴリズムの例として Deutsch のアルゴリズムと Grover のアルゴリズムを紹介する．最後に，Grover のアルゴリズムを契機として提案された量子質問モデルと，その複雑さである量子質問複雑さを定義し，量子質問複雑さの下界を導出する既存の手法である量子敵対者法について紹介する．

2.5.1　量子計算のための準備

量子計算では，ある n に対する n 個の複素数の組 $(z_1, z_2, \ldots, z_n)$ の全てを要素とするベクトル空間 $\mathbf{C}^n$ を考える．量子力学においては，慣用的な記号を用いて列ベクトルを

$$|\psi\rangle$$

のように表記する．ψ はベクトルに対するラベルである．ベクトルに対するラベルとして，ψ や φ などがしばしば用いられる．$|\cdot\rangle$ はそれが列ベクトルであることを示す記号である．列ベクトルをケットと呼ぶことがある．一方，列ベクトル $|\psi\rangle$ の各成分を複素共役の値にした後，転置を取ったベクトルを $\langle\psi|$ と表記する．つまり，$\langle\cdot|$ は行ベクトルを表記するための記号である．行ベクトルをブラと呼ぶことがある．$|\psi\rangle$ と $|\varphi\rangle$ の内積を $\langle\psi|\varphi\rangle$ と表記する．$|\psi\rangle$ と $|\varphi\rangle$ のテンソル積を $|\psi\rangle \otimes |\varphi\rangle$ と表記し，$|\psi\rangle|\varphi\rangle$，$|\psi, \varphi\rangle$，$|\psi\varphi\rangle$ などとしばしば略記する．行列に対するテンソル積も同じ記号を用いる．A を m 行 n 列の行列，B を p 行 q 列の行列とする．このとき，A と B のテンソル積 $A \otimes B$ は次式で表される．$A \otimes B$ は mp 行 nq 列の行列となる．

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \ldots & A_{1n}B \\ A_{21}B & A_{22}B & \ldots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \ldots & A_{mn}B \end{bmatrix}$$

この表現において $A_{11}B$ のような項は p 行 q 列の部分行列を示す．この部分行列の各成分は B の対応する成分に比例し，全ての比例定数は A_{11} である．例えば，べ

クトル $(1,2)$ と $(2,3)$ のテンソル積はベクトルであり，

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix} \otimes \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 1\times 2 \\ 1\times 3 \\ 2\times 2 \\ 2\times 3 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \\ 4 \\ 6 \end{bmatrix}.$$

行列に対しても同様であり，

$$\begin{bmatrix} 1 & 2i \\ 0 & i \end{bmatrix} \otimes \begin{bmatrix} 2 & 1 \\ 3 & i \end{bmatrix} = \begin{bmatrix} 1\times 2 & 1\times 1 & 2i\times 2 & 2i\times 1 \\ 1\times 3 & 1\times i & 2i\times 3 & 2i\times i \\ 0\times 2 & 0\times 1 & i\times 2 & i\times 1 \\ 0\times 3 & 0\times i & i\times 3 & i\times i \end{bmatrix} = \begin{bmatrix} 2 & 1 & 4i & 2i \\ 3 & i & 6i & -2 \\ 0 & 0 & 2i & i \\ 0 & 0 & 3i & i \end{bmatrix}$$

などのように計算する．行列 A と B に対する，通常の行列積は AB と表記する．行列 A にベクトル $|\psi\rangle$ を右から掛ける行列積は $A|\psi\rangle$ と表記する．行列 A の共役転置行列を A^* と表記する．

2.5.2　量子力学の枠組み

公理 1 任意の孤立した物理システムに関して，システムの状態空間と呼ぶ内積を伴う複素ベクトル空間（つまり Hilbert 空間）が存在する．システムは状態空間の単位ベクトルである状態ベクトルによって完全に記述できる．

最も簡単な量子力学システムは**量子ビット**（qubit）である．1 量子ビットは 2 次元状態空間を持つ．$|0\rangle$ と $|1\rangle$ がその状態空間の基底を形成する．ここで，

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix},\ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

とする．このとき状態空間における任意の状態ベクトルは次のように書ける．

$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix},$$

ここで a と b は複素数である．$|\psi\rangle$ が単位ベクトルであるという条件 $\langle\psi|\psi\rangle = 1$ は $|a|^2 + |b|^2 = 1$ と等価であり，条件 $\langle\psi|\psi\rangle = 1$ を状態ベクトルの**正規化条件**と呼ぶ．この条件は，後に測定に関する公理において見るように，測定が正しく行われるために必要な条件でもある．

n を任意の自然数とする．任意の $i \in \{1, 2, \ldots, n\}$ に対して，$\alpha_i \in \mathbf{C}$ とする．任意の線形結合 $\sum_i \alpha_i |\psi_i\rangle$ は，状態 $|\psi_i\rangle$ に対する**振幅** α_i を以て状態 $|\psi_i\rangle$ を重ね合わせたものである．したがって，例えば，

$$\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

は状態 $|0\rangle$ に対して振幅 $\sqrt{2}$，状態 $|1\rangle$ に対して振幅 $-1/\sqrt{2}$ で，状態 $|0\rangle$ と $|1\rangle$ を重ね合わせたものである．

k 個の量子ビットのテンソル積を k 量子ビットと呼ぶ．k 量子ビットは 2^k 次元状態空間を持つ．任意の k 量子ビットに対して，テンソル積の演算において最も左に表記される量子ビットから数えて i $(i \in \{1, 2, \ldots, k\})$ 番目の量子ビットを第 i 量子ビットと呼ぶ．

公理 2 閉じた量子システムの時間発展はユニタリ変換で記述される．つまり時刻 t_1 におけるシステムの状態 $|\psi\rangle$ は，時刻 t_2 におけるシステムの状態 $|\psi'\rangle$ と時刻 t_1 と t_2 だけに依存するユニタリ行列 U によって次式のように関係づけられる．

$$|\psi'\rangle = U|\psi\rangle.$$

量子計算においては，k 個の量子ビットに作用するユニタリ行列 U を k 量子ビット（ユニタリ）ゲートとも呼ぶ．

この公理により，状態ベクトルの内積が保存される．実際，1 量子ビットの例を見ると，時刻 t の状態ベクトルを $|\psi_t\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ とし，ユニタリ行列 U を作用することで得られる時刻 $t+1$ の状態ベクトルを $|\psi_{t+1}\rangle$ とすると，

$$\begin{aligned} \langle\psi_{t+1}|\psi_{t+1}\rangle &= \langle\psi_t|U^*U|\psi_t\rangle \\ &= \langle\psi_t|\psi_t\rangle \\ &= |\alpha_0|^2 + |\alpha_1|^2 \end{aligned}$$

となる．内積が保存されるため，先に述べた状態 $|\psi\rangle$ に対する正規化条件 $\langle\psi|\psi\rangle = 1$ は，計算の開始時刻で満たされていれば，計算が進んだどの時刻においても常に満たされる．よって次に述べる測定をどの時刻でも正しく行うことができる．

公理 3 k 個の物理システムを一つの複合システムとして扱うとき，複合物理システムの状態空間は部分システムの状態空間 $\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_k$ のテンソル積空間 $\mathcal{H}_1 \otimes$

$\mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_k$ である．$1 \leq i \leq k$ なる各 i について i 番目システムが状態 $|\psi_i\rangle$ にあるとき，この複合システムの状態は

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_k\rangle \tag{2.1}$$

である．

小節 2.5.1 で述べたように，(2.1) を記号 $\otimes$ を省略して $|\psi_1\rangle|\psi_2\rangle \ldots |\psi_k\rangle$ や $|\psi_1\psi_2 \ldots \psi_k\rangle$ のようにしばしば書く．

逆に，2 量子ビットの複合システムの状態が常に $|\psi_1\rangle \otimes |\psi_2\rangle$ という積の形で書けるとは限らないということは重要である．2 量子ビットを独立に準備した後，孤立のままであれば量子ビットはそれぞれ閉じたシステムを形成し，その状態を積の形で書くことができる．しかし，量子ビットが相互作用するとそのシステムは両方の量子ビットを含むので，積の形でその状態を記述することができない可能性がある．例えば，2 量子ビットの状態

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$$

は

$$|\psi\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle)(\beta_0|0\rangle + \beta_1|1\rangle)$$

という積の形で書くことができない．このような状態を量子ビットがもつれ合っている，あるいは，量子もつれと呼ぶ．量子もつれは量子計算と量子情報において重要な役割を果たし，量子テレポーテーションの根幹を成す．

公理 4 ある量子システム A の状態空間 $\mathcal{H}_A$ に対する与えられた正規直交基底 $B = \{|\varphi_i\rangle\}$ に対して，$\mathcal{H}_A$ 上の *Von Neumann* 測定を実行することができる．与えられた状態が

$$|\psi\rangle = \sum_i \alpha_i |\varphi_i\rangle$$

であるとき，*Von Neumann* 測定を実行すると，確率 $|\alpha_i|^2$ でラベル i を出力し，システムの状態は $|\varphi_i\rangle$ となる．さらに，二つの状態空間 $\mathcal{H}_A$ と $\mathcal{H}_B$ から成る複合状態空間 $\mathcal{H}_A \otimes \mathcal{H}_B$ の状態 $|\psi\rangle = \sum_{i,j} \alpha_{i,j}|\varphi_i\rangle|\gamma_j\rangle$ が与えられたとき，システム A に対して *Von Neumann* 測定を行うと，確率 $|\alpha_i|$ でラベル i が得られ，状態は $\sum_j |\varphi_i\rangle|\gamma_j\rangle$ となる．

ある複合システムの状態が次の状態にあるとき，二つの量子ビットをともに測定することを考える．

$$|\psi\rangle = \sqrt{\frac{1}{11}}|0\rangle|0\rangle + \sqrt{\frac{5}{11}}|0\rangle|1\rangle + \sqrt{\frac{2}{11}}|1\rangle|0\rangle + \sqrt{\frac{3}{11}}|1\rangle|1\rangle.$$

基底 $B = \{|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle\}$ に対して観測を行うと，確率 $1/11$ で 00，確率 $5/11$ で 01，確率 $2/11$ で 10，確率 $3/11$ で 11 を得る．このように，第 1 量子ビットにおいて 0 を観測する確率は $1/11 + 5/11 = 6/11$ である．第 1 量子ビットを観測することにより何が生じるかを見るためには $|\psi\rangle$ を次のように書き直すのが便利である．

$$|\psi\rangle = \sqrt{\frac{6}{11}}|0\rangle \left(\sqrt{\frac{1}{6}}|0\rangle + \sqrt{\frac{5}{6}}|1\rangle\right) + \sqrt{\frac{5}{11}}|1\rangle \left(\sqrt{\frac{2}{5}}|0\rangle + \sqrt{\frac{3}{5}}|1\rangle\right).$$

第 1 量子ビットにおいて 0 を観測する確率は $6/11$ であり，その観測後の第 2 量子ビットの状態は，

$$\sqrt{\frac{1}{6}}|0\rangle + \sqrt{\frac{5}{6}}|1\rangle$$

となる．

2.5.3　量子回路モデル

公理 2 において，量子計算はユニタリ行列を状態ベクトルに左から掛けることによって行われることを示したが，ユニタリ行列をゲートに対応させた量子回路モデルが量子アルゴリズムを示す場合に有用である．量子回路は論理回路の量子版と言える．確率的チューリングマシンの量子版である量子チューリングマシンと量子回路の関係として，回路の一様性を仮定すれば計算能力が等価であることが知られている．これは論理回路と決定性チューリングマシンの間の関係と同様の関係であり，非常に興味深いが，論旨から外れるためこれ以上の説明は省略する．詳しくは [30] を参照されたい．

量子回路モデルにおいては，信号線によって量子ビットが運ばれ，その量子ビットに量子ゲートが作用する．n 個の量子ビットに作用する量子ゲートは，n 本の入力のための信号線と n 本の出力のための信号線を持つ．量子回路は図 2.2 のような回路図でしばしば描かれる．信号線は水平な線で示され，量子ビットは信号線に沿って左から右に伝達される．量子ゲートは長方形で示される．図 2.2 の右端に示されている小さな三角形は，そこで計算基底における単一量子ビットの測定が行

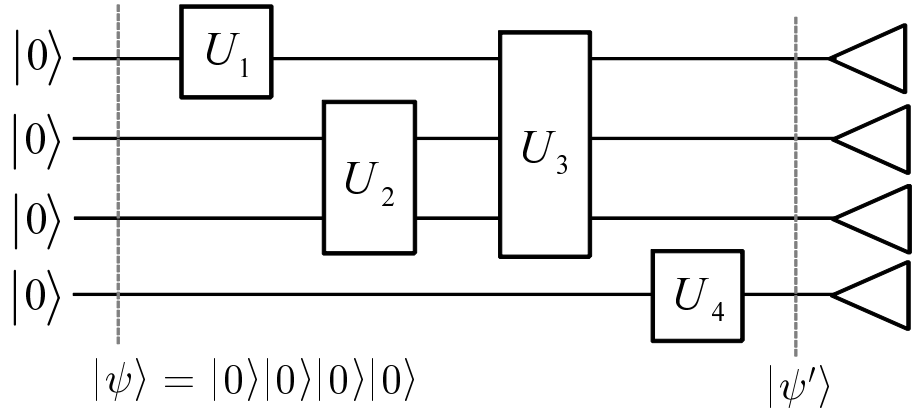

図 2.2: 量子回路の例．4 量子ビットの状態 $|0000\rangle$ が回路に左から入る．その 4 量子ビットに U_1, U_2, U_3, U_4 が順に適用され，回路の右側まで到達したときに状態 $|\psi'\rangle$ が測定される．

われることを意味する．図 2.2 の例を見ると，状態が $|\psi_i\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle$ である 4 量子ビットが左から入っている．これらの量子ビットは U_1, U_2, U_3, U_4 の四つのゲートが適用される．回路の出力として，4 量子ビットの状態 $|\psi_f\rangle$ を得る．

次に，今後の説明で用いるアダマールゲートと量子 NOT ゲートを示す．アダマールゲートは記号 H を用いて表す．1 量子ビットに対するアダマールゲートは，次のようなユニタリ行列である．

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

また，n 量子ビットに対するアダマールゲート H は，1 量子ビットに対するアダマールゲートの n 階のテンソル積であり，$H^{\otimes n}$ と書くこととする．量子 NOT ゲートは記号 X を用いて表す．1 量子ビットに対する量子 NOT ゲートは，次のようなユニタリ行列である．

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

2.5.4　Deutsch のアルゴリズム

Deutsch のアルゴリズムは以下のような問題を解く．未知の 1 変数ブール関数 $f : \{0, 1\} \to \{0, 1\}$ を計算する量子回路が与えられたと仮定する．この量子回路をブラックボックスまたはオラクルとして用いる．つまり，この回路を利用することで

入力 x に対する $f(x)$ の値を得ることができるが，回路の内部の動きについてはなにも情報を得ることができない．Deutsch のアルゴリズムが解く問題とは，$f(0) \oplus f(1)$ の値を決定することである．ここで $\oplus$ は排他的論理和である．$f(0) \oplus f(1) = 0$ であるならば $f(0) = f(1)$ である，つまり，f が定数であることがわかるが，$f(0)$ や $f(1)$ の個々の値はわからない．一方，$f(0) \oplus f(1) = 1$ であるならば $f(0) \neq f(1)$ である，つまり，f がバランスしていることがわかるが，$f(0)$ や $f(1)$ の個々の値はわからない．よって，$f(0) \oplus f(1)$ の値を決定する問題は，f が定数関数かバランスした関数かを決定する問題である．

Deutsch の問題
入力：未知の関数 $f : \{0, 1\} \to \{0, 1\}$ を計算するブラックボックス
問題：ブラックボックスを利用して $f(0) \oplus f(1)$ の値を決定せよ．

$f(0) \oplus f(1)$ の値を決定するために，古典的なアルゴリズムではオラクルに何回質問することが必要だろうか．明らかにこの答えは 2 回である．オラクルへの古典的質問を 1 回することで $f(0)$ の値を得たと仮定する．このとき，$f(1)$ の値に応じて，$f(0) \oplus f(1)$ は 0 にも 1 にもなりうる．つまり，$f(1)$ の値を得るためにオラクルに二回目の質問をすることなしに $f(0) \oplus f(1)$ の値を決定することはできない．Deutsch のアルゴリズムは f に対する量子オラクルに対し **1 回**の質問をするだけで $f(0) \oplus f(1)$ の値を決めることができる．

与えられたブラックボックスを表す量子回路は，次のようなユニタリー行列で表現できる．

$$U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle.$$

例えば，状態 $|0\rangle|0\rangle$ をブラックボックスに与えると，$|0\rangle|0 \oplus f(0)\rangle = |0\rangle|f(0)\rangle$ が得られる．その後，第 2 量子ビットを測定すれば $f(0)$ の値が得られる．これは $f(0)$ の値を得るための古典的質問と等価である．同様に，状態 $|1\rangle|0\rangle$ をブラックボックスに与えたあと測定を行えば $f(1)$ の値を得ることができる．Deutsch のアルゴリズムでは，上記のような状態を与えるのではなく，量子重ね合わせの状態をブラックボックスに与える．Deutsch のアルゴリズムの詳細を以下に示す．

図 2.3 に示す回路は Deutsch のアルゴリズムを実装した量子回路である．初期状態は

$$|\psi_0\rangle = |0\rangle|0\rangle$$

である．次に第 2 量子ビットに量子 NOT ゲートを適用し，

$$|\psi_1\rangle = |0\rangle|1\rangle$$

を得る．次に両方の量子ビットにアダマールゲートを適用し，

$$\begin{aligned} |\psi_2\rangle &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{\sqrt{2}}|0\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}|1\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

を得る．次に U_f ゲートを適用し，

$$\begin{aligned} |\psi_3\rangle &= \frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) + \frac{(-1)^{f(1)}}{\sqrt{2}}|1\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= (-1)^{f(0)}\left(\frac{|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

を得る．ここで，最後の等式は $(-1)^{f(0)}(-1)^{f(1)} = (-1)^{f(0)\oplus f(1)}$ であることを用いた．

もし f が定数関数，つまり $f(0) \oplus f(1) = 0$ であるならば，

$$|\psi_3\rangle = (-1)^{f(0)}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

であり，最後に第 1 量子ビットにアダマールゲートを適用することにより，

$$|\psi_4\rangle = (-1)^{f(0)}|0\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

を得る．第 1 量子ビットの基底状態 $|0\rangle$ の振幅の二乗は 1 である．よって，$|\psi_4\rangle$ の第 1 量子ビットを測定すれば，値 $0 = f(0) \oplus f(1)$ を得られる．

もし f がバランスした関数，つまり $f(0) \oplus f(1) = 1$ であるならば，

$$|\psi_3\rangle = (-1)^{f(0)}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

であり，最後に第 1 量子ビットにアダマールゲートを適用することにより，

$$|\psi_4\rangle = (-1)^{f(0)}|1\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

を得る．第 1 量子ビットの基底状態 $|1\rangle$ の振幅の二乗は 1 である．よって，$|\psi_4\rangle$ の第 1 量子ビットを測定すれば，値 $1 = f(0) \oplus f(1)$ を得られる．このように，Deutsch のアルゴリズムを実装した回路の最後で第 1 量子ビットを測定すれば $f(0) \oplus f(1)$ の値を得ることができる．

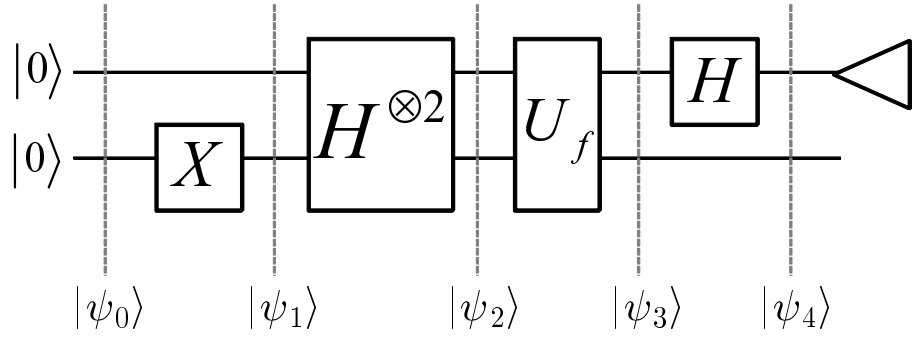

図 2.3: Deutch のアルゴリズムを実装した回路．2 量子ビットが入力として左から入る．その後，第 2 量子ビットに X が適用され，第 1，第 2 の両方の量子ビットに $H^{\otimes 2}$，U_f が適用され，第 1 量子ビットに H が適用される．最後に第 1 量子ビットが観測される．

2.5.5　Grover のアルゴリズム

本小節では，探索問題とそれを解く Grover のアルゴリズムを紹介する．

探索問題とは，解を知っているオラクルが与えられたとき，解を要素として含む可能性のある集合から解を探し出す問題である．ある要素が解であるかどうかを知るためには，解を知っているオラクルに質問をする以外に方法はない．この問題の定式化を行うと，以下のようになる．

探索問題

入力: 未知の関数 $f : \{0,1\}^n \to \{0,1\}$ を計算するブラックボックス．

問題: $f(x) = 1$ である入力 $x \in \{0,1\}^n$ を見つけよ．

探索問題は $f(x) = 1$ となるような入力 x を複数持つ f が与えられる可能性があるが，議論を簡単にするためにそのような入力は 1 つのみであるとする．$f(x) = 1$ となるような入力 x を複数持つ f の場合でも以下で行う議論と同様の議論が可能である．詳しくは [18, 10] を参考にされたい．

古典的アルゴリズムでは $O(2^n)$ より少ない質問回数で探索問題を解くアルゴリズムは知られていないが，Grover のアルゴリズムは $O(\sqrt{2^n})$ の質問回数で確率 $O(1)$ で探索問題の解を得ることができる．$f(x) = 1$ となるような x が存在しない f の場合については，Grover のアルゴリズムは必ず間違う，つまり，$f(x) = 0$ となるような x を出力するので，出力値 x の関数値 $f(x)$ を確認する質問をさらに 1 回することで，$f(x) = 1$ となるような x が存在しない f であることも高確率で示すこ

とができる．

前小節 2.5.4 と同様に，ブラックボックスを表す量子回路 U_f は以下のように表される．$x, b \in \{0, 1\}$ とする．よって，$|x\rangle$ と $|b\rangle$ は 1 量子ビットである．

$$U_f : |x\rangle|b\rangle \mapsto |x\rangle|b \oplus f(x)\rangle.$$

第 2 量子ビットを $(|0\rangle - |1\rangle)/\sqrt{2})$ とすると，

$$U_f|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = (-1)^{f(x)}|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

となる．第 2 量子ビットの値が $(|0\rangle - |1\rangle)/\sqrt{2})$ のまま変わっていないため，第 2 量子ビットを $(|0\rangle - |1\rangle)/\sqrt{2})$ に固定すれば，U_f の適用に関しては第 2 量子ビットを無視できる．Grover のアルゴリズムでは，U_f 以外の量子ゲートは第 2 量子ビットに作用させないため，以降では第 2 量子ビットを省略することとする．例えば，U_f に関しては，

$$U_f : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$$

と書く．

Grover のアルゴリズムの定義のために，いくつか定義を行う．$U_{0^\perp}$ を以下のように定義する．

$$U_{0^\perp} : \begin{cases} |x\rangle \mapsto -|x\rangle, \ x \neq 00\ldots0 \\ |00\ldots0\rangle \mapsto |00\ldots0\rangle \end{cases}.$$

この Grover の繰り返し G を以下のように定義する．

Grover の繰り返し G

1. 入力される n 量子ビットに対して U_f を適用する．
2. 手順 1 の後に出力される n 量子ビットに対して，n 量子ビットアダマールゲート $H^{\otimes n}$ を適用する．
3. 手順 2 の後に出力される n 量子ビットに対して，$U_{0^\perp}$ を適用する．
4. 手順 3 の後に出力される n 量子ビットに対して，n 量子ビットアダマールゲート $H^{\otimes n}$ を適用する．

よって G は $G = H^{\otimes n}U_{0^\perp}H^{\otimes n}U_f$ というユニタリ行列で表される．量子回路で書くと図 2.5.5 のようになる．第 2 量子ビットは $(|0\rangle - |1\rangle)/\sqrt{2}$ のままで終始変化しないため，図 2.5.5 内でも省略されている点に注意されたい．

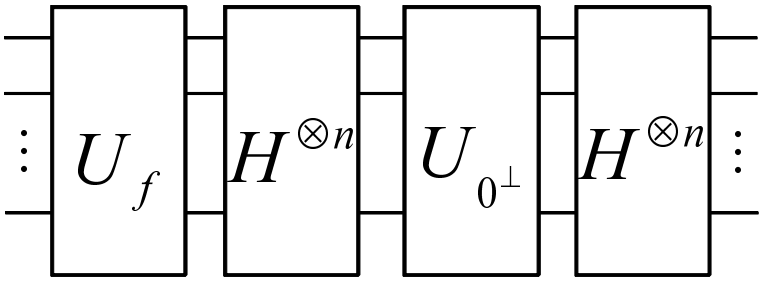

図 2.4: 入力される n 量子ビットに対して，Grover の繰り返し $G = H^{\otimes n} U_{0^\perp} H^{\otimes n} U_f$ を適用する回路.

Grover の繰り返し G を用いると，Grover のアルゴリズムが簡潔に書ける．$N = 2^n$ とする．

Grover のアルゴリズム

1.n 量子ビットの初期状態 $|00\ldots0\rangle$ から始める．

2.n 量子ビットのアダマールゲート $H^{\otimes n}$ を適用する．その結果，状態は

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

となる．

3.Grover の繰り返し G を $\lfloor \pi/(4\sqrt{N}) \rfloor$ 回繰り返す.

4. 測定する．

Grover のアルゴリズムを実装した回路は，図 2.5 のようになる．

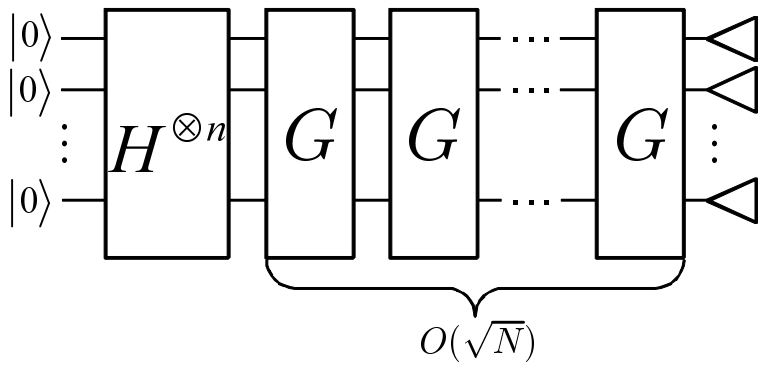

図 2.5: Grover のアルゴリズム

次に Grover のアルゴリズムの動作の説明を行う．初めに n 量子ビットのアダマー

ルゲートを通すことで，重ねあわせの状態 $(1/\sqrt{N})\sum_{x=0}^{N-1}|x\rangle$ を得る．この状態を次の二つの部分の和に分ける．一つ目の部分は $f(x)=0$ である x の和である．すなわち，探索問題の解ではない‘悪い’入力 x についての和である．悪い入力の集合を $X_{\rm bad}$ とする．二つ目の部分は $f(x)=1$ である x の和である．すなわち，探索問題の解である‘良い’入力 x についての和である．良い入力の集合を $X_{\rm good}$ とする．すでに述べたように，$f(x)=1$ であるような入力 x は一つしかないとしているので，$X_{\rm good}=\{w\}$ $(w\in\{0,1\}^n)$ である．二つの状態 $|\psi_{\rm good}\rangle$ と $|\psi_{\rm bad}\rangle$ を以下のように定義する．

$$\begin{aligned}|\psi_{\rm good}\rangle &= |w\rangle \\ |\psi_{\rm bad}\rangle &= \frac{1}{N-1}\sum_{x\in X_{\rm bad}}|x\rangle.\end{aligned}$$

$|w\rangle$ と $|\psi_{\rm bad}\rangle$ を用いて $(1/\sqrt{N})\sum_{x=0}^{N-1}|x\rangle$ を表すと，

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle=\frac{1}{\sqrt{N}}|w\rangle+\sqrt{\frac{N-1}{N}}|\psi_{\rm bad}\rangle$$

となる．よって，$|w\rangle$ の振幅を 1 に近づけてから測定を行えば正しい解が得られる．この振幅を増幅させる効果を与えるのが，Grover の繰り返し G である．

Grover の繰り返し G が $|w\rangle$ の振幅を増幅させることを示す．状態 $|\psi\rangle$ を

$$|\psi\rangle=H|00\ldots0\rangle$$

とする．$|\psi\rangle$ に $HU_{0^\perp}H$ を左から掛けると，

$$HU_{0^\perp}H|\psi\rangle=|\psi\rangle \tag{2.2}$$

となる．式 (2.2) は $H^2=I$ であることを用いれば容易に導かれる．$V_\psi^\perp$ を $|\psi\rangle$ に直交するベクトル空間とする．この空間は $x\neq00\ldots0$ 以外の x に対する $H|x\rangle$ によって張られる空間である．よって，$x\neq00\ldots0$ であるような x に対して，

$$HU_{0^\perp}HH|x\rangle=-H|x\rangle$$

となる．よって，$HU_{0^\perp}H$ を左から掛けるという演算は $V_\psi^\perp$ に含まれるベクトルの振幅を-1 倍する効果がある．したがって，$HU_{0^\perp}H$ を次のように書くこととする．

$$U_{\psi^\perp}=HU_{0^\perp}H.$$

よって，Grover の繰り返し G は

$$G = U_{\psi^\perp} U_f$$

と書ける．ここで，今後の議論に用いる 3 つの命題を示す．

命題 2.1 $|\psi\rangle = (1/\sqrt{N}) \sum_{x=0}^{N-1} |x\rangle$ とする．このとき，$HU_{0^\perp}H = 2|\psi\rangle\langle\psi| - I$ である．

証明: まず，$U_{0^\perp} = 2|00\ldots0\rangle\langle00\ldots0| - I$ であることを示す．状態に $U_{0^\perp}$ を掛けることにより，その状態の $|00\ldots0\rangle$ 以外の基底の振幅は-1 倍される．つまり，$U_{0^\perp}$ は以下のような行列である．

$$U_{0^\perp} = \begin{pmatrix} 1 & 0 & 0 & 0 & \ldots & 0 \\ 0 & -1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & -1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & -1 \end{pmatrix}$$

この行列は明らかに $2|00\ldots0\rangle\langle00\ldots0| - I$ と等価である．よって，

$$\begin{aligned} HU_{0^\perp}H &= H(2|00\ldots0\rangle\langle00\ldots0| - I)H \\ &= 2H|00\ldots0\rangle\langle00\ldots0|H - HH \\ &= 2|\psi\rangle\langle\psi| - I \end{aligned}$$

となる．ここで，$H^* = H$，$H^2 = I$ を用いている．

□

命題 2.2 $H|00\ldots0\rangle$ に直交する任意の n-q ビットの状態 $|\phi\rangle$ はその振幅の和が 0 である．

証明: $|\phi\rangle$ について，基底 $|00\ldots0\rangle, |00\ldots1\rangle, \ldots, |11\ldots1\rangle$ の振幅をそれぞれ $\alpha_0, \alpha_1, \ldots, \alpha_{2^n}$ とする．一方

$$H|00\ldots0\rangle = \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} |x\rangle$$

であるから，$H|00\ldots0\rangle$ の各基底の振幅は全て $1/\sqrt{N}$ である．$H|00\ldots0\rangle$ と $|\phi\rangle$ は直交するので，

$$\frac{1}{\sqrt{N}}\sum_{x=1}^{2^n}\alpha_x = 0.$$

よって，$\sum_{x=1}^{2^n}\alpha_x = 0$ となる．

□

命題 2.3 n 量子ビットの状態に対して $U_{\psi^\perp}$ を左から掛けることは，振幅について‘平均に対して反転を取る’演算である．より具体的には，ある重ね合わせ状態を

$$|\phi\rangle = \sum_{x=1}^{2^n}\alpha_x|x\rangle$$

とし，振幅の平均を

$$\mu = \frac{1}{N}\sum_{x=1}^{2^n}\alpha_x$$

とすると，

$$U_{\psi\perp}|\phi\rangle = \sum_{x=1}^{2^n}(2\mu-\alpha_x)|x\rangle$$

が成り立つ．

証明: 状態 $|\phi\rangle$ を $|\psi\rangle$ に平行な成分と $|\psi\rangle$ に直交する成分 $|\bar{\psi}\rangle$ とに分解する．すなわち，

$$|\phi\rangle = \alpha|\psi\rangle + \beta|\bar{\psi}\rangle$$

と表現する．このとき，命題 2.5.5 を用いると，振幅の和は $N\alpha$ となる．よって，α は μ を用いて以下のようにあらわすことができる．

$$\alpha = \frac{1}{\sqrt{N}}\mu.$$

命題 2.1 より，$U_{\psi^\perp}|\phi\rangle$ は

$$\begin{aligned}
U_{\psi^\perp}|\phi\rangle &= (2|\psi\rangle\langle\psi| - I)|\phi\rangle && (2.3)\\
&= 2\alpha|\psi\rangle\langle\psi|\psi\rangle + 2\beta|\psi\rangle\langle\psi|\bar{\psi}\rangle - |\phi\rangle && (2.4)\\
&= 2\alpha|\psi\rangle - |\phi\rangle && (2.5)\\
&= 2\frac{\mu}{\sqrt{N}}|\psi\rangle - |\phi\rangle && (2.6)\\
&= \sum_{x=1}^{2^n}(2\mu-\alpha_x)|x\rangle && (2.7)
\end{aligned}$$

となる．

□

$H|00\ldots0\rangle$ の各基底の振幅は全て実数であり，Grover の繰り返しを適用しても振幅はやはり実数のままである．よって，横軸は N 個の基底のラベルを表し，縦軸は振幅を表す，つまり，横軸より上にあれば正の振幅を表し，横軸より下にあれば負の振幅を表す，図 2.6 のようなグラフで表現することができる．

U_f の適用後，$|w\rangle$ の振幅は-1 倍される．よって，図 2.7 のように振幅の平均が少し下がる．

命題 2.2 においても示したように，$U_{\psi^\perp}$ を掛けることは平均に対して反転させることであるので，図 2.8 のように $|w\rangle$ の振幅の大きさは約 3 倍になる．また，他の基底の振幅は少し下がる．

もう一度の U_f の適用により，$|w\rangle$ の振幅は再び負になり，振幅の平均は少しさがる．振幅の平均の反転を取るごとに，$|w\rangle$ の振幅は大まかに言って $2/\sqrt{N}$ が足されることとなり，他の基底の振幅は少しずつ小さくなる．よって，大まかに言えば $\sqrt{N}/2$ 回 Grover の繰り返しを適用すれば，$|w\rangle$ の振幅は 1 に近づくこととなる．より詳細な解析は [18] を参照されたい．

2.6　量子質問モデル

前節で，Grover のアルゴリズムを用いれば，関数 $f : \{0,1\}^n \to \{0,1\}$ に対する探索問題について，ブラックボックスの呼び出し回数が $O(\sqrt{2^n})$ 回で，$f(x) = 1$ という解 x があるならば高確率でそれを出力することができ，解がない場合も解がないことを示す出力を高確率で行うことが可能であることを述べた．これは，Grover のアルゴリズムを用いれば $f(x) = 1$ であるような x があるかどうかを決定する決定問題を解くことができることを示している．この決定問題は次のような長さ n の論理変数 $X = (X_1, X_2, \ldots, X_n)$ の OR 関数 g を計算する問題と等価である．

$$g(X) = X_1 \vee X_2 \vee \cdots \vee X_n.$$

g を任意の関数へと拡張することで，次に述べる質問モデルが得られる．

量子質問とは，オラクルへの入力が量子重ね合わせ状態であり，返される値も量子重ね合わせ状態である．割り当て $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ に対するオラ

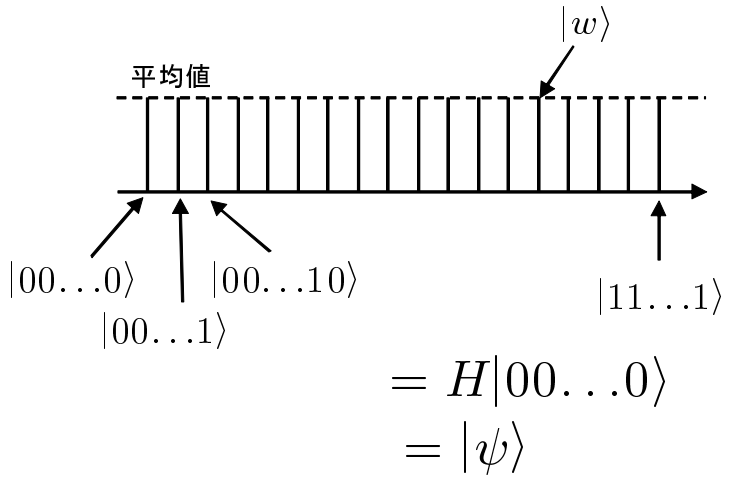

図 2.6: 探索問題への N 個の入力によってラベルづけられた横軸に対し，直行する線で実数の振幅を表している.

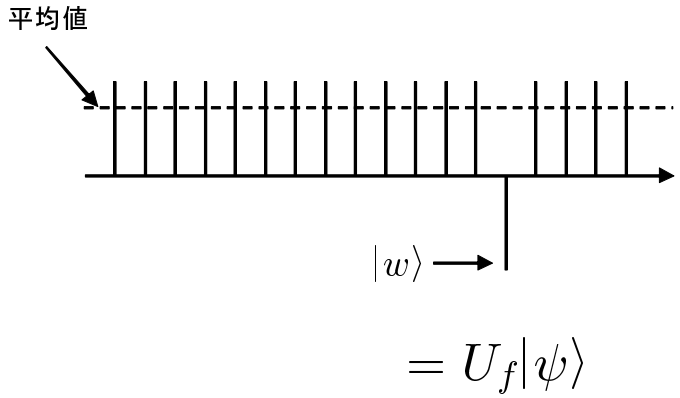

図 2.7: U_f を一回適用した後の状態.

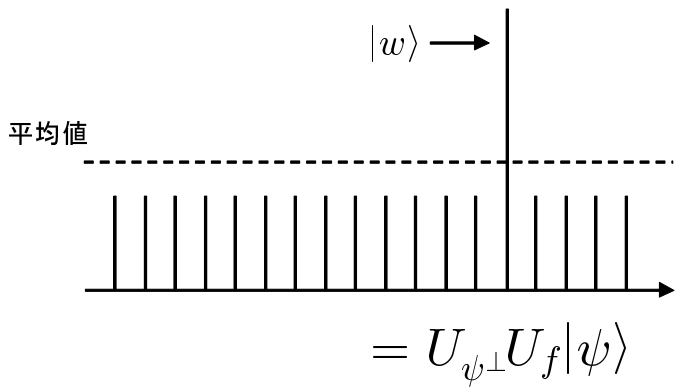

図 2.8: 平均値に対する反転を取った状態.

クルを表す量子ゲートは,

$$O_{\boldsymbol{x}} : |i\rangle|z\rangle \to (-1)^{x_i}|i\rangle|z\rangle. \tag{2.8}$$

で表される．ここで，$|i\rangle$ はオラクルへの入力のための量子ビットであり，$i \in \{0,1\}^{\lceil \log n \rceil}$ である．$|z\rangle$ は計算作業領域の量子ビットである．

量子質問モデルのアルゴリズムは，全ての量子ビットを 0 に初期化した状態 $|00\ldots0\rangle|00\ldots\rangle|0\rangle$ を初期状態として選ぶ．表記を簡単にするために，全ての量子ビットを 0 である状態を $|\mathbf{0}\rangle$ と書くこととする．その後，x には依存しないユニタリ行列の適用とブラックボックスへの質問 O_x を交互に行い，最後に観測を行って計算結果を得る．アルゴリズムが全部で T 回の質問を行うとすると，観測直前の状態は一般に x に依存しないユニタリ行列 $U_0, U_1, \ldots U_T$ を用いて状態ベクトルと行列の積で以下のように表される．

$$|\psi_x^T\rangle = U_T O_x U_{T-1} \ldots U_1 O_x U_0 |0\rangle.$$

のように表される．測定はこの状態の特定の 1 量子ビットに対して行い，得られた 1 ビット $a = \{0,1\}$ をアルゴリズムは出力する．ブール関数 f を誤り率 ϵ で計算する量子質問アルゴリズムとは，f の任意の入力割り当て $\boldsymbol{x} \in \{0,1\}^n$ に対して，アルゴリズムの出力を a としたとき，$a = f(\boldsymbol{x})$ となる確率が少なくとも $1-\epsilon$ であるものをいう．f を誤り率 ϵ で計算する量子アルゴリズム A に対し，A の量子質問複雑さとは，全ての入力割り当て $\boldsymbol{x} \in \{0,1\}^n$ の中でアルゴリズム A が少なくとも確率 $1-\epsilon$ で $f(\boldsymbol{x})$ を出力するために必要となる質問回数の最大値である．

定義 2.8 任意のブール関数 f に対して，f の ϵ **誤り量子質問複雑さ**とは，f を誤り率 ϵ で計算する量子質問アルゴリズムの中で，量子質問複雑さが最小のアルゴリズムの量子質問複雑さであり，$Q_\epsilon(f)$ と書く．特に ϵ を指定しない場合には，単に量子質問複雑さと呼ぶ.

k をある自然数とする．i を定義域が $\{0,1\}^{\lceil \log n \rceil}$ である変数とし，z を定義域が $\{0,1\}^k$ である変数とする．状態が $\sum_{i,z} \alpha_{i,z}|i\rangle|z\rangle$ である量子質問アルゴリズム A を考える．ある $j \in \{0,1\}^{\lfloor \log N \rfloor}$ に対して，$\sum_z \alpha_{j,z} = 1$ であるとき，$\sum_{i \neq j} \sum_z \alpha_{i,z} = 0$ であるので，A の状態は $|j\rangle \sum_z \alpha_{j,z}|z\rangle$ と書ける．ここでオラクルに質問すると，入力割り当て $\boldsymbol{x}$ の j ビット目 x_j に関する情報のみが必ず得られるので，古典的質問と等価である．このように，量子質問モデルは古典的質問をシミュレートできるため，任意のブール関数 f に対して，$D(f) \geq Q_\epsilon(f)$ が成り立つ.

2.7　量子敵対者限界

本節では．任意のブール関数 f に対し，f に依存して定まる数理計画問題の設計手法を与える．得られた数理計画問題の最適値は f の量子敵対者限界と呼ばれ，$Q_\epsilon(f)$ の下界を与える．量子敵対者限界は多項式法 [7] と並んで，量子質問複雑さの下界を導出するための主要な方法の一つである．

2.7.1　量子敵対者法とは

n 次元ベクトル v の表記の仕方として，各成分の値を明示したい場合には，$(v_1, v_2, \ldots, v_n)$ と書くこととする．以下では，特に指定のない場合，行列はある n に対する $2^n \times 2^n$ の正方行列とし，その行と列は n ビットの系列で番号づけられているとする．

$\boldsymbol{x}$ をあるビット列行列 A とビット列 $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$ に対して，A の $(\boldsymbol{x}, \boldsymbol{y})$ 成分を $A[\boldsymbol{x}, \boldsymbol{y}]$ と記す．また，A^* を A の共役転置行列とする．列ベクトル v に対して，v の l_2 ノルムを $|v|$ と記す．すなわち，$|v| = \sqrt{v^* v}$．正方行列 A に対して，A のスペクトルノルムを $\|A\|$ と記す．すなわち，

$$\begin{aligned} \|A\| &= \sqrt{(\text{maximum eigenvalue of } A^*A)} \\ &= \max_{v:|v|\neq 0, v\in\{0,1\}^n} \frac{|Av|}{|v|}. \end{aligned}$$

とする．任意の実対称行列 A に対して，そのスペクトルノルムは A の固有値の絶対値の中の最大値と等しい．行列 A と B のアダマール積を $A \circ B$ と記す．すなわち，任意の $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$ に対して，$(A \circ B)[\boldsymbol{x}, \boldsymbol{y}] = A[\boldsymbol{x}, \boldsymbol{y}]B[\boldsymbol{x}, \boldsymbol{y}]$ とする．各成分が 0 か 1 であるような行列をブール行列と呼ぶ．ブール行列 A に対して，A の否定行列を $\bar{A}$ と記す．すなわち，任意の $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$ に対して，$\bar{A}[\boldsymbol{x}, \boldsymbol{y}] = 1 - A[\boldsymbol{x}, \boldsymbol{y}]$ とする．行列を行と列のラベルを明示して表記する場合，以下のように各成分と対応する行と列のラベルを線で区切り併記する．

	00	01	10	11
00	0	2	1	0
01	2	0	0	1
10	1	0	0	2
11	0	1	2	0

行列 A を上の表で定義した場合，$A[00,01] = A[01,00] = A[10,11] = A[11,10] = 2$，$A[00,10] = A[01,11] = A[10,00] = A[11,01] = 1$ であり，A のその他の成分は 0 である．

ブール関数 $f : \{0,1\}^n \to \{0,1\}$ に対して，次の条件を満たす Γ を f の敵対者行列と呼ぶ．

1. Γ は対称行列である．
2. 各 $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$ に対して，$\Gamma[\boldsymbol{x}, \boldsymbol{y}] \geq 0$.
3. ある $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$ に対して，$\Gamma[\boldsymbol{x}, \boldsymbol{y}] > 0$.
4. $f(\boldsymbol{x}) = f(\boldsymbol{y})$ のとき，$\Gamma[\boldsymbol{x}, \boldsymbol{y}] = 0$.

ブール行列 D_i を，任意の $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$ に対し，$\boldsymbol{x}$ と $\boldsymbol{y}$ の第 i 成分が異なるとき，またそのときに限り $D_i[\boldsymbol{x}, \boldsymbol{y}] = 1$ であるような行列とする．

量子敵対者法は考慮下の関数 f によって指定される数理計画問題によって定式化され，その最適解が f の量子質問複雑さ $Q_\epsilon(f)$ の下界を与える [6]．その最適値 $\mathrm{ADV}(f)$ を f の**量子敵対者限界**と呼ぶ．

定義 2.9 $f : \{0,1\}^n \to \{0,1\}$ とする．Φ_f を f の敵対者行列全てからなる集合とする．f の量子敵対者限界を次のように定義する．

$$\mathrm{ADV}(f) = \max_{\Gamma \in \Phi_f} \min_{i \in \{1,2,\ldots,n\}} \frac{\|\Gamma\|}{\|\Gamma \circ D_i\|}.$$

定理 2.3 ([6]) 任意のブール関数 f と任意の $\epsilon \in [0, 1/2)$ に対して，

$$Q_\epsilon(f) \geq \frac{1 - 2\sqrt{\epsilon(1-\epsilon)}}{2} \mathrm{ADV}(f).$$

$\mathrm{ADV}(f)$ は量子質問複雑さ $Q_\epsilon(f)$ の下界を与えるだけではなく，その 2 乗値はブール式複雑さ $L(f)$ の下界をも与える．

定理 2.4 ([21]) 任意のブール関数 f に対して，

$$\mathrm{ADV}^2(f) \leq L(f).$$

定義 2.10 あるブール関数 f に対して，$\mathrm{ADV}^2(f) = L(f)$ であるとき，f を ADV タイトであるという．

ADV(f) を定義する数理計画問題には，次に示す双対表現が存在する．その双対表現によって定義される数理計画問題の最適値を MM(f) と記す．

定義 2.11 関数 $p : \{0,1\}^n \times \{1,2,\ldots,n\} \to \mathcal{R}$ が $\{1,2,\ldots,n\}$ 上の確率分布族であるとは，任意の $\boldsymbol{x} \in \{0,1\}^n$，任意の $i \in \{1,2,\ldots,n\}$ に対し，$p_{\boldsymbol{x}}(i) \geq 0$，かつ $\sum_i p_{\boldsymbol{x}}(i) = 1$ を満たすことである．$\{1,2,\ldots n\}$ の確率分布族の集合を P_n と表記する．ブール関数 $f : \{0,1\}^n \to \{0,1\}$ に対して，MM(f) を次のように定義する．

$$\mathrm{MM}(f) = \min_{p \in P_n} \max_{\substack{\boldsymbol{x} \in f^{-1}(0) \\ \boldsymbol{y} \in f^{-1}(1)}} \frac{1}{\sum_{i:x_i \neq y_i} \sqrt{p_{\boldsymbol{x}}(i) p_{\boldsymbol{y}}(i)}}.$$

ここで，$c \in \{0,1\}$ に対して，$f^{-1}(c) = \{x \in \{0,1\}^n \mid f(x) = c\}$ とする．

定理 2.5 任意のブール関数 f に対して，ADV(f) = MM(f) が成立する．

f をあるブール関数とする．ADV(f) は目的関数 $\min_{i \in \{1,2,\ldots,n\}}(\|\Gamma\|/\|\Gamma \circ D_i\|)$ を最大化する数理計画問題の最適値とみなせる．この数理計画問題を $\mathcal{A}$ と呼ぶことにする．$\mathcal{A}$ の任意の許容解 $\Gamma \in \Phi_f$ に対する目的関数の値は ADV(f) の下界を与える．一方，MM(f) は目的関数 $\max_{\boldsymbol{x} \in f^{-1}(0), \boldsymbol{y} \in f^{-1}(1)}(1/\sum_{i:x_i \neq y_i} \sqrt{p_{\boldsymbol{x}}(i) p_{\boldsymbol{y}}(i)})$ を最小化する数理計画問題の最適値とみなせる．この数理計画問題を $\mathcal{B}$ と呼ぶことにする．定理 2.5 より，$\mathcal{B}$ の任意の許容解 $p \in P_n$ に対する目的関数の値は ADV(f) の上界を与える．このように，数理計画問題の許容解を実際に与えることで ADV(f) の上界と下界を示すことができる．本論文の第 3 章ではこの手法を用いている．

2.7.2　定理 2.3 の証明

本小節では，量子敵対者法が量子質問複雑さの下界を与える理由について説明する．

ブール関数 $f : \{0,1\}^n \to \{0,1\}$ を誤り率 ϵ で計算する量子質問アルゴリズムを考える．入力割り当て $\boldsymbol{x} \in \{0,1\}^n$ とすると，各 $t \geq 0$ に対してブラックボックス $O_{\boldsymbol{x}}$ に t 回質問した後の量子アルゴリズムの状態は，

$$|\psi_{\boldsymbol{x}}^t\rangle = U_t O_{\boldsymbol{x}} \ldots U_1 O_{\boldsymbol{x}} U_0 |0\rangle \tag{2.9}$$

のように表される．ここで，$U_1, U_2, \ldots, U_t$ は $\boldsymbol{x}$ に依存しないユニタリ行列である．

量子質問アルゴリズムが関数 f を計算するために T 回の質問を必要とすることを示す一般的なアプローチは，$f(\boldsymbol{x}) = 1$ を満たす入力 $\boldsymbol{x}$ に対するブラックボック

ス $O_{\boldsymbol{x}}$ と $f(\boldsymbol{y}) = 1$ を満たす入力 $\boldsymbol{y}$ に対するブラックボックス $O_{\boldsymbol{y}}$ をそのアルゴリズムが高精度では区別できないことを示すことである．任意の量子質問アルゴリズム A に対して，ブラックボックス $O_{\boldsymbol{x}}$ が与えられた時に A が T 回質問した後の状態を $|\psi_{\boldsymbol{x}}^T\rangle$ とし，ブラックボックス $O_{\boldsymbol{y}}$ が与えられた時に A が T 回質問した後の状態を $|\psi_{\boldsymbol{y}}^T\rangle$ とする．$f(\boldsymbol{x})$ と $f(\boldsymbol{y})$ を高精度で計算する量子質問アルゴリズムは，状態 $|\psi_{\boldsymbol{x}}^T\rangle$ と状態 $|\psi_{\boldsymbol{y}}^T\rangle$ を高精度で区別できなければならない．この区別可能性を測る指標として，最も単純な指標は内積である．これは測定の公理 4 からも妥当なものと考えられる．つまり，二つの量子状態が確実に区別可能であることとその二つの量子状態の内積が直交していることは同値である．二つの量子状態が高確率で区別可能であることとその二つの量子状態の内積の絶対値が小さいことは同値である．

定理 2.6 n を任意の自然数とする．$\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$ とし，$\boldsymbol{x} \neq \boldsymbol{y}$ かつ $\boldsymbol{z} \in \{\boldsymbol{x}, \boldsymbol{y}\}$ とする．入力 $|\psi_{\boldsymbol{z}}\rangle$ が与えられたとき，$\boldsymbol{z} = \boldsymbol{x}$ であるか $\boldsymbol{z} = \boldsymbol{y}$ であるかを推測する任意の手続きは，高々確率 $1 - \epsilon = 1/2(1 + \sqrt{1 - \epsilon'^2})$ でしか正しく推測できない．ここで，$\epsilon' = |\langle\psi_{\boldsymbol{x}}|\psi_{\boldsymbol{y}}\rangle|$ である．この確率は最適な観測により達成される．

アルゴリズムの計算の進度を測るために $t \in \{0, 1, \ldots, T\}$ に対し，重み W^t を次のように定義する．

$$W^t = \sum_{\boldsymbol{x},\boldsymbol{y} \in \{0,1\}^n} \langle\psi_{\boldsymbol{x}}^t|\psi_{\boldsymbol{y}}^t\rangle \Gamma[\boldsymbol{x}, \boldsymbol{y}] \delta_{\boldsymbol{x}} \delta_{\boldsymbol{y}}. \tag{2.10}$$

ここで，Γ は任意に固定した f の敵対者行列，δ は Γ の最大固有値に対応する正規化された固有ベクトルとし，$\delta_{\boldsymbol{x}}$ は δ の $\boldsymbol{x}$ 番目の成分とする．

アルゴリズムはブラックボックスに質問をする前の状態 $|\psi_{\boldsymbol{x}}^0\rangle$ から計算を始めると，状態 $|\psi_{\boldsymbol{x}}^0\rangle$ は入力割り当てに依存しないので $|\psi_{\boldsymbol{x}}^0\rangle = |\psi_{\boldsymbol{y}}^0\rangle$ である．初期の重みは，

$$W^0 = \sum_{x,y \in \{0,1\}^n} \Gamma[x, y] \delta_x \delta_y = ||\Gamma|| \tag{2.11}$$

である．ここで，$||\Gamma||$ は Γ のスペクトルノルムを表す．入力割り当てが $\boldsymbol{x}$ であれば，T 回の質問の後の最終状態は $|\psi_{\boldsymbol{x}}^T\rangle$ であり，入力割り当てが $\boldsymbol{y}$ であれば，T 回の質問の後の最終状態は $|\psi_{\boldsymbol{y}}^T\rangle$ である．$f(\boldsymbol{x}) \neq f(\boldsymbol{y})$ であれば，定理 2.6 より，$|\langle\psi_{\boldsymbol{x}}^T|\psi_{\boldsymbol{y}}^T\rangle| \leq 2\sqrt{\epsilon(1-\epsilon)}$ でなければならない．ゆえに，$W^T \leq 2\sqrt{\epsilon(1-\epsilon)}W^0$ でなければならない．もし重みが一回の質問ごとに高々 Δ しか減少することができなければ，アルゴリズムはそのブラックボックスに対して $((1 - 2\sqrt{\epsilon(1-\epsilon)})W^0)/\Delta$

回の質問をする必要がある．Δ の上界は文献 [14] の定理 2 の証明にあるように，式 (2.9) を用いて導出でき，

$$\Delta \leq 2 \max_i ||\Gamma_i||$$

となる．これらのことから，定理 2.3 が成立することが分かる．

2.7.3　合成関数に対するコスト付き量子敵対者限界

Høyer らは $h = f \circ (g_1, g_2, \ldots, g_k)$ という形の合成関数に対する量子敵対者限界 $\mathrm{ADV}(h)$ を評価するために，量子敵対者限界を一般化したコスト付き量子敵対者限界という概念を与えている．

コスト付き量子敵対者限界の定義を示した後，Høyer らの結果について記す．

定義 2.12 $f : \{0,1\}^n \to \{0,1\}$ とし，Φ_f を f に対する敵対者行列の集合とする．各ベクトル $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{R}_+^n$ に対して，$\mathrm{ADV}_\alpha(f)$ を次のように定義する．

$$\mathrm{ADV}_\alpha(f) = \max_{\Gamma \in \Phi_f} \min_{i \in \{1,2,\ldots,n\}} \frac{\alpha_i \|\Gamma\|}{\|\Gamma \circ D_i\|}.$$

$\alpha = (1, 1, \ldots, 1)$ のとき，$\mathrm{ADV}_\alpha(f) = \mathrm{ADV}(f)$ であることに注意されたい．

定義 2.13 h を以下で与えられる n 変数ブール関数とする．k を任意の自然数とし，$n_1, n_2, \ldots, n_k$ を $n = n_1 + n_2 + \cdots + n_k$ を満たす任意の自然数とする．ある k 変数ブール関数 $f : \{0,1\}^k \to \{0,1\}$ と k 個のブール関数 $g_1 : \{0,1\}^{n_1} \to \{0,1\}$，…，$g_k : \{0,1\}^{n_k} \to \{0,1\}$ に対して，

$$h(x) = f(g_1(x^1), g_2(x^2), \ldots, g_k(x^k)).$$

ここで，x は k 個のビット列 $x^1 \in \{0,1\}^{n_1}$, $x^2 \in \{0,1\}^{n_2}$, …, $x^k \in \{0,1\}^{n_k}$ の連接とする．このとき，h を f と $g_1, g_2, \ldots, g_k$ との合成関数と呼び，$h = f \circ (g_1, g_2, \ldots, g_k)$ と書く．

定理 2.7 ([12]) k を任意の自然数する．任意の k 変数ブール関数 f と任意のブール関数 $g_1, g_2, \ldots, g_k$ に対し，$h = f \circ (g_1, g_2, \ldots, g_k)$ とする．このとき，

$$\mathrm{ADV}(h) = \mathrm{ADV}_\alpha(f).$$

ここで，$\alpha_i = \mathrm{ADV}(g_i)$ とし，$\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ とする．

定理 2.7 を用いる際には，各部分関数 g_i の入力が互いに素でなければならいという制限があることに注意されたい．

複雑な関数 h に対して量子敵対者限界を計算する問題を，より小さい関数に対する量子敵対者限界を計算するいくつかの部分問題に帰着できるという点で，定理 2.7 は有用である．実際，Høyer らは n 変数一回読み関数の敵対者限界が $\sqrt{n}$ であることがこの定理によりただちに導出できることを示している [12]．より具体的には，彼らはまず 2 変数 AND 関数と 2 変数 OR 関数に対して，以下の命題を示した．

命題 2.4 ([12]) 任意の $\alpha = (\alpha_1, \alpha_2) \in \mathcal{R}_+^2$ に対して，

$$\mathrm{ADV}_\alpha(\mathrm{AND}) = \mathrm{ADV}_\alpha(\mathrm{OR}) = \sqrt{\alpha_1^2 + \alpha_2^2}. \tag{2.12}$$

そしてその後に定理 2.7 を適用して一回読み関数に対する $\sqrt{n}$ の量子敵対者限界を導出している．

しかし，AND と OR 以外の多くの関数 f に対して $\mathrm{ADV}_\alpha(f)$ を α を用いた式で表すことは非常に困難である．本論文の第 3 章における我々の技術的な成果は，2 変数排他的論理和関数 XOR に対する $\mathrm{ADV}_\alpha(\mathrm{XOR})$ と 2 入力マルチプレクサ関数 MUX に対する $\mathrm{ADV}_\alpha(\mathrm{MUX})$ を α を用いた式で表現したことである．

以下に，量子敵対者限界を定義している数理計画問題のの双対表現を示す．双対表現は最小化問題となる．主表現は最大化問題で定義されているので，任意の許容解（最適解ではなくとも）が ADV_α の下界を与えることに注意されたい．同様に，双対表現に対する任意の許容解は上界を与える．ADV_α に対する精密な評価を行うために，我々は主表現と双対表現の両方の定式化を用いる．

定義 2.14 $p : \{0,1\}^n \times \{1,2,\ldots,n\} \to \mathcal{R}$ を，$p_x(i) \geq 0$ かつ各 $x \in \{0,1\}^n$ に対して $\sum_{i\in\{1,2,\ldots,n\}} p_x(i) = 1$ という意味での確率分布の集合とする．そのような p 全てからなる集合を P_n と記す．あるブール関数 $f : \{0,1\}^n \to \{0,1\}$ に対して，$\mathrm{MM}_\alpha(f)$ を次のように定義する．

$$\mathrm{MM}_\alpha(f) = \min_{p\in P_n} \max_{\substack{x\in f^{-1}(0)\\ y\in f^{-1}(1)}} \frac{1}{\sum_{i:x_i\neq y_i} \sqrt{p_x(i)p_y(i)}/\alpha_i}.$$

定理 2.8 ([12]) 任意の $f : \{0,1\}^n \to \{0,1\}$ と任意の $\alpha \in \mathcal{R}_+^n$ に対して，

$$\mathrm{ADV}_\alpha(f) = \mathrm{MM}_\alpha(f).$$

最後にコスト付き量子敵対者限界に関する基本的で有用な性質をいくつか示す．定義 2.12 から ADV_α は各 α_i に関して単調増加であることが容易にわかる．このことを命題として以下に示す．二つのベクトル $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ と $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$ に対して，任意の $i \in \{1, 2, \ldots, n\}$ に対し $\alpha_i \leq \beta_i$ であるとき，$\alpha \leq \beta$ と書くことにする．

命題 2.5 $f : \{0,1\}^n \to \{0,1\}$ とする．$\alpha \leq \beta$ であるような任意の二つのベクトル $\alpha, \beta \in \mathcal{R}_+^n$ に対して，

$$\mathrm{ADV}_\alpha(f) \leq \mathrm{ADV}_\beta(f).$$

さらに，コスト付き量子敵対者限界は以下のような 3 つの命題で示される有用な性質を持つ．

命題 2.6 $f : \{0,1\}^n \to \{0,1\}$ とし，$\alpha \in \mathcal{R}_+^n$ とする．このとき，任意の $c \in \mathcal{R}_+$ に対して，

$$\mathrm{ADV}_{c\alpha}(f) = c\mathrm{ADV}_\alpha(f).$$

命題 2.7 $f : \{0,1\}^n \to \{0,1\}$ とし，$\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{R}_+^n$ とする．$\{1, 2, \ldots, n\}$ 上のある置換 π に対して，関数 $f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$ を $\pi(f)$ と記す．また，ベクトル $(\alpha_{\pi(1)}, \alpha_{\pi(2)}, \ldots, \alpha_{\pi(n)})$ を $\pi(\alpha)$ と記す．$\{1, 2, \ldots, n\}$ 上の任意の置換 π に対して，

$$\mathrm{ADV}_{\pi(\alpha)}(\pi(f)) = \mathrm{ADV}_\alpha(f).$$

命題 2.8 $f : \{0,1\}^n \to \{0,1\}$ とし，$\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{R}_+^n$ とする．ビット $v \in \{0,1\}$ に対して，$v^0 = v$ とし，$v^1 = \bar{v}$ とする．f' をあるビット列 $b = (b_1, b_2, \ldots, b_n) \in \{0,1\}^n$ に対して $f'(x_1, x_2, \ldots, x_n) = f(x_1^{b_1}, x_2^{b_2}, \ldots, x_n^{b_n})$ とする．このとき任意の f' に対して，

$$\mathrm{ADV}_\alpha(f') = \mathrm{ADV}_\alpha(f).$$

命題 2.6 は定義から明らかであり，命題 2.7 と命題 2.8 は，次に述べる命題から容易に導かれる．

命題 2.9 n を任意の自然数とし，M を $2^n \times 2^n$ の正方行列 M とする．任意の $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$ に対し，M の行 $\boldsymbol{x}$ と行 $\boldsymbol{y}$ を入れ替え，列 $\boldsymbol{x}$ と列 $\boldsymbol{y}$ を入れ替えて得られる正方行列を M' とすると，

$$||M|| = ||M'||.$$

証明: M の固有値 a に対応する固有ベクトル $\boldsymbol{v}$ の $\boldsymbol{x}$ 番目の成分と $\boldsymbol{y}$ 番目の成分を入れ替えたベクトルを $\boldsymbol{v}'$ とする．$M'\boldsymbol{v}' = a\boldsymbol{v}'$ となることは明らかである．

□

第3章　一回読みブール関数に対する量子質問複雑さの下界

3.1　はじめに

量子計算理論における最も大きな課題は，量子計算が古典的な計算モデルである決定的計算や確率的計算に比べてどの程度優れているか，ということを明らかにすることである．いくつかの特定の問題に対しては，現在知られている古典的アルゴリズムよりも効率のよい量子アルゴリズムが知られている一方，量子計算が古典的計算よりもそれほど大きくは優れていないことを示す多くの結果が存在する [1]．特に，興味深い結果の多くは質問モデルにおいて示されている．

量子質問モデルにおける主要な結果の一つは，2.5.5 節で紹介した Grover の探索アルゴリズムである [10]．これは $O(\sqrt{n})$ 回の質問で n 変数 OR 関数を計算する量子アルゴリズムとみなせる．一方で，決定的質問アルゴリズムでは n 回の質問を必要とする．言い換えると，n 変数 OR 関数を OR_n と記すことにすると，任意の $\epsilon \in (0, 1/2)$ に対して $Q_\epsilon(\mathrm{OR}_n) = O(\sqrt{n})$ であるが，$D(\mathrm{OR}_n) = n$ である．このように，OR 関数は量子計算が決定的計算に対して二乗の速度向上をもたらす例である．

一方，Barnum と Saks [5] は n 変数の任意の一回読み関数 f に対して $Q_\epsilon(f) = \Omega(\sqrt{n})$ であることを示している．ここで，一回読み関数とは基底 $\{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}\}$ 上のブール式で各変数が一回しか現れないブール式で表現されるブール関数である．任意の自然数 n に対する OR_n は一回読み関数なので，Grover のアルゴリズムは OR_n に対する最適な量子質問アルゴリズムの一つであるということができる．この結果は，一回読み関数に関しては，量子アルゴリズムは古典的な決定性アルゴリズムに比べ二乗を超える速度向上を達成できないことを意味する．

任意のブール関数に対して，量子アルゴリズムが決定的アルゴリズムに比べ二乗を越える速度向上を達成できるか否かという問題は，量子質問複雑さにおける重要な未解決問題の一つである．第 1 章で述べたように，多くの研究者は否定的

な命題，すなわち以下の 2 乗ギャップ予想が成立すると予想している．

2 乗ギャップ予想 [5] 任意のブール関数 f と $\epsilon \in [0, 1/2)$ に対して，

$$Q_\epsilon(f) = \Omega(\sqrt{D(f)}).$$

2 乗ギャップ予想は定義域が $\{0,1\}^n$ の要素全てである全体関数に対するものであることに注意されたい．定義域が制限された部分関数については，量子質問複雑さと決定的質問複雑さとの間に非常に大きなギャップが存在することが知られている [25]．量子質問複雑さの下界を決定的質問複雑さを用いて表すという意味での，これまでに知られている最良の結果は，任意のブール関数 f と $\epsilon \in (0, 1/2)$ に対する $Q_\epsilon(f) = \Omega(D(f)^{1/6})$ という結果 [7] と，$\epsilon = 0$ に対する $Q_\epsilon(f) = \Omega(D(f)^{1/3})$ という結果 [23] である．一回読み関数に対する Barum と Saks の結果以外にもいくつかの結果が 2 乗ギャップ予想に対する証拠を与えている．例えば，パリティ関数や多数決関数を含む全ての対称関数に対して $Q_\epsilon(f) = \Omega(D(f))$ が成立することが知られている [7].

本章では 2 乗ギャップ予想に対するさらなる証拠を示す．まず，パリティノード付き一回読み決定木が計算する任意の関数に対して，2 乗ギャップ予想が成立することを示す．ここで，一回読み決定木とは各変数 x_i が決定木の中に高々1 回しか現れない決定木のことである．また，パリティノードは子を一つしか持たない特殊な内部頂点であり，パリティノードが根である決定木の計算する関数は，根につけられたラベルの変数と，根の子の部分木が計算する関数との排他的論理和である．任意の自然数 n に対して，n 変数論理積関数，n 変数論理和関数，n 変数パリティ関数は全てパリティノード付き一回読み決定木で計算できる．

さらに，その結果を拡張し，基底を $\mathcal{B} = \{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}, \mathrm{XOR}, \mathrm{MUX}\}$ に拡張した一回読み関数に対しても 2 乗ギャップ予想が成立することを示す．ここで，XOR は 2 変数排他的論理和関数であり，MUX は 2 入力マルチプレクサ関数である．XOR と MUX は標準基底 $\{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}\}$ 上の一回読みブール式では表現できないので，基底 $\mathcal{B}$ 上の一階読み関数のクラスは $\{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}\}$ 上の一回読み関数のクラスを真に含む．したがって，我々の結果は [5] における一回読み関数に対する結果を拡張した結果といえる．

本章では，2 乗ギャップ予想が成立することを示すために，まず，パリティノード付き一回読み決定木に対する，ブール関数の複雑さ指標であるソフトランクを導入する．ソフトランクは次に示すように決定木の平衡度を表す．深さが d である全ての決定木の中で，ソフトランクの値が最大となる決定木は最も平衡した決

定木である完全ニ分木で，そのソフトランクは d である．ソフトランクの値が最小となる決定木は最も平衡していない決定木である決定リストであり，そのソフトランクは $\sqrt{d}$ である．決定リストとは，根から最も遠い内部頂点の二つの子は共に葉であり，それ以外の内部頂点の片方の子は葉であり，もう片方の子は内部頂点であるような決定木である．ブール関数 f を計算する決定木の深さは f の決定的質問複雑さ $D(f)$ の上界であるので，ソフトランクが量子質問複雑さの下界を与えることを示すことで，$Q_\epsilon(f) = \Omega(D(f)^{1/2})$ が直ちに導かれる．

一回読み $\mathfrak{B}$ 式に対しては，決定木の深さとソフトランクの定義を一回読み $\mathfrak{B}$ 式に対するブール関数の複雑さ指標として拡張する．決定木の深さを拡張したブール関数の複雑さ指標を決定的深さ d と呼ぶことにすると，(1) 一回読み $\mathfrak{B}$ 式の決定的深さが決定的質問複雑さの上界を与えること，(2) 一回読み $\mathfrak{B}$ 式のソフトランクが量子質問複雑さの下界を与えること，(3) 任意の一回読み $\mathfrak{B}$ 式 F に対して，F の決定的深さの二乗根が F のソフトランクの下界を与えること，の三つを示すことにより，$Q_\epsilon(f) = \Omega(D(f)^{1/2})$ を導く．

ソフトランクが量子質問複雑さの下界を与えることを示すために，量子敵対者限界を用いる．量子敵対者限界は量子質問複雑さの下界を導出する際に用いられる最も成功した手法の一つであり [3, 4, 6, 22, 28]，与えられたブール関数によって定まる数理計画問題の最適値として定義される．定理 2.7 で示したように，$h = f \circ (g_1, g_2, \ldots, g_k)$ という合成関数に対しては，h に対する量子敵対者限界 $\mathrm{ADV}(h)$ は，$\alpha = (\mathrm{ADV}(g_1), \mathrm{ADV}(g_2), \ldots, \mathrm{ADV}(g_k))$ としたときのコスト付き量子敵対者限界 $\mathrm{ADV}_\alpha(f)$ と等しくなる．パリティノード付き一回読み決定木の表す関数は MUX と XOR を用いた合成関数として表現でき，一回読み $\mathfrak{B}$ 式の表す関数は $\mathfrak{B}$ に含まれる関数の合成関数として表現できるため，定理 2.7 を利用することで量子質問複雑さの下界を導出することができる．

3.2　パリティノード付き一回読み決定木

本節ではパリティノード付き一回読み決定木の定義を与える．

各変数 x_i が決定木の中に高々1 回しか現れないとき，その決定木を一回読み決定木と呼ぶ．一回読み決定木でパリティノードと呼ばれる特別な頂点を持つものをパリティノードつき一回読み決定木と呼ぶ．一回読み決定木をパリティノード付き一回読み決定木と呼ぶ．パリティノードとは通常の内部ノードと同様にある変数でラベル

付けられているが，ただ一つの子しか持たない．入力割り当て $\boldsymbol{a} = (a_1, a_2, \ldots, a_n) \in \{0,1\}^n$ に対する，パリティノード付き決定木 T の出力値 $T(a) \in \{0,1\}$ の評価は，通常の決定木と同様に根からある葉への道を辿ることによって行われる．現在のノードがパリティノードでない場合には通常の決定木と同様である．現在のノードが変数 x_i でラベルづけられたパリティノードである場合には，まず唯一の子に進み，v が根である部分木 T' に対して再帰的に出力値の評価を行い，$a_i \oplus T'(\boldsymbol{a})$ を出力する．言い換えると，$a_i = 0$ の場合は，部分木 T' の出力の評価を行うが，$x_i = 1$ の場合には部分木 T の表す関数の否定関数の出力の評価を行う．

このように，部分木 T' を子として持つパリティノードは，左の子の部分木を T' とし右の子の部分木を $\bar{T}'$ とする同じ変数ラベルの通常の内部ノードに，表す関数を変えることなく置き換えることができる．しかし，その結果得られる決定木は一回読み決定木であるとは限らない．図 3.1 に例を示す．

非冗長なパリティノード付き一回読み決定木のクラスを $\mathrm{DT}_\oplus$ と記す．ここで，非冗長な決定木とは次の二つの条件を満たす決定木のことである．

1. 子が葉であるようなパリティノードが存在しない．
2. 子が二つとも同じ値でラベルづけられた葉であるような通常の内部頂点が存在しない．

$\mathrm{DT}_\oplus$ に属する任意の決定木はパリティノードのない通常の決定木に前述の方法で深さを変えずに変形できることに注意されたい．したがって，$\mathrm{DT}_\oplus$ に属する決定木 T の深さも，T が表す関数 f に対する $D(f)$ の上界を与える．

3.2.1　パリティノード付一回読み決定木の合成関数による表現

$\mathrm{DT}_\oplus$ に属する決定木 T の表す関数は，XOR と MUX の二つの関数を用いた合成関数で再帰的に表現できる．T の根が x_i でラベルづけられた通常の内部ノードである場合には，その内部ノードの左の子の部分木を T_1，右の子の部分木を T_2 とすると，T は $\mathrm{MUX}(x_i, T_1, T_2)$ で表される．同様に，T の根が x_i でラベルづけられたパリティノードである場合には，その子の部分木を T_1 とすると，T は $\mathrm{XOR}(x_i, T_1)$ で表される．同様に，部分木 T_1 や T_2 も XOR と MUX を用いた合成関数で再帰的に表現できる．例えば，図 3.1 の左の木は次のように表現される．

$$\mathrm{MUX}(x_1, \mathrm{MUX}(x_2, 0, 1), \mathrm{XOR}(x_3, \mathrm{MUX}(x_4, \mathrm{MUX}(x_5, 1, 0), 0))).$$

$\mathrm{MUX}(x_2, 0, 1)$ は x_2 と，$\mathrm{MUX}(x_5, 1, 0)$ は $\bar{x}_5$ と等価であることに注意すると，この式は次のように簡単かできる．

$$\mathrm{MUX}(x_1, x_2, \mathrm{XOR}(x_3, \mathrm{MUX}(x_4, \bar{x}_5, 0))).$$

3.2.2　ソフトランク

ここでは，パリティノード付き決定木に対する複雑さ指標である，**ソフトランク**の定義を与える．ソフトランクは，決定木学習の分野で提案された複雑さ指標であるランク [9] と同様に，木の平衡度を表す．まずランクの定義を与える．

定義 3.1 (ランク [9]) パリティノード付き決定木 T に対して，T のランク $r(T)$ を以下のように再帰的に定義する．T が葉であるとき，$r(T) = 0$ である．T の根がパリティノードであるとき，そのパリティノードの子の部分木を T_1 とすると，$r(T) = r(T_1) + 1$ である．T の根が通常の内部ノードであるとき，その内部ノードの左の子と右の子をそれぞれ T_1, T_2 とすると，

$$r(T) = \begin{cases} \max\{r(T_1), r(T_2)\} & \text{if } r(T_1) \neq r(T_2), \\ r(T_1) + 1 & \text{if } r(T_1) = r(T_2). \end{cases}$$

よって，二つの木 T_1 と T_2 を通常の内部ノードで結合した木 $T = \mathrm{MUX}(x_i, T_1, T_2)$ のランクは，T_1 と T_2 のランクの差 $|r(T_1) - r(T_2)| = 0$ ではない限り，T_1 と T_2 のどちらのランクよりも大きくならない．一方，T のソフトランクは，T_1 と T_2 のソフトランクの差で決定されるある量で常に増加する．

定義 3.2 (ソフトランク) パリティノード付き決定木 T に対して，T のソフトランク $\tilde{r}(T)$ を以下のように再帰的に定義する．T が葉であるとき，$\tilde{r}(T) = 0$ である．T の根がパリティノードであるとき，そのパリティノードの子の部分木を T_1 とすると，$\tilde{r}(T) = \tilde{r}(T_1) + 1$ である．T の根が通常の内部ノードであるとき，その内部ノードの左の子と右の子をそれぞれ T_1, T_2 とすると，

$$\begin{aligned} \tilde{r}(T) &= \min\{\tilde{r}(T_1), \tilde{r}(T_2)\} + \sqrt{l^2 + 1} \\ &= \max\{\tilde{r}(T_1), \tilde{r}(T_2)\} - l + \sqrt{l^2 + 1}. \end{aligned}$$

ここで，$l = |\tilde{r}(T_1) - \tilde{r}(T_2)|$ とする．

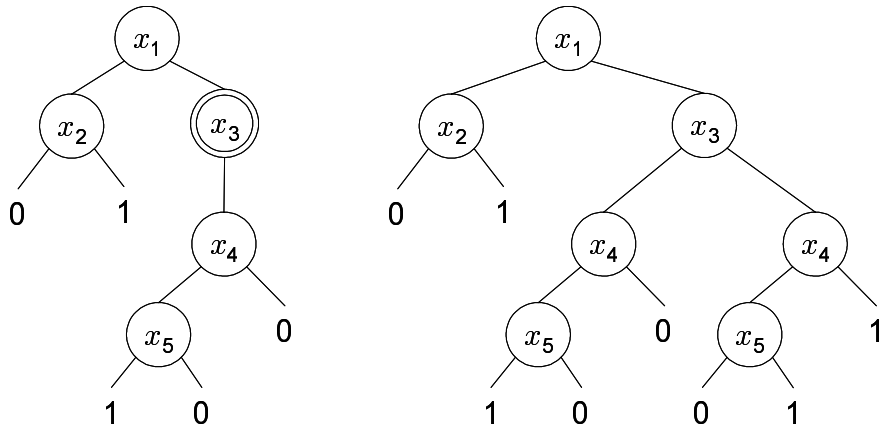

図 3.1: $\mathrm{DT}_{\oplus}$ に属する決定木（左）と左の木と等価な通常の決定木（右）．x_3 のラベルを持つ二重丸で示された頂点はパリティノードを表す.

ソフトランクが木の平衡度を表す指標であることは，次の観察によって理解できる．関数 σ を $\sigma(l) = -l + \sqrt{l^2+1}$ と定義すると，$T = \mathrm{MUX}(x_i, T_1, T_2)$ のとき，

$$\tilde{r}(T) = \max\{\tilde{r}(T_1), \tilde{r}(T_2)\} + \sigma(|\tilde{r}(T_1) - \tilde{r}(T_2)|) \tag{3.1}$$

と書ける．$\sigma(l)$ は l について単調減少なので，2 つの木 T_1 と T_2 のソフトランクの差 $|\tilde{r}(T_1) - \tilde{r}(T_2)|$ が小さい（すなわち T_1 と T_2 が平衡している）ほど T のソフトランク $\tilde{r}(T)$ は大きくなる．したがって，$\tilde{r}(T)$ を T の平衡度と考えると直感に合う定義になっている.

ランクは再帰式 (3.1) において関数 σ を

$$\delta(l) = \begin{cases} 1 & \text{if } l = 0 \\ 0 & \text{if } l > 0 \end{cases}$$

で定義される δ で置き換えることによって得られる．任意の $l \geq 0$ に対し，$\sigma(l) \geq \delta(l)$ であることから次の命題を直ちに導くことができる.

命題 3.1 任意のパリティノード付き決定木 T に対して，

$$\tilde{r}(T) \geq r(T).$$

ランクもソフトランクも，木の内部ノード数の線形時間で求めることができる．実際，図 3.1 の左の木 T のランクとソフトランクは容易に求められ，$r(T) = 2$，$\tilde{r}(T) = 1 + \sqrt{3}$ となる．図 3.1 の右の木についても同じ結果が得られることに注

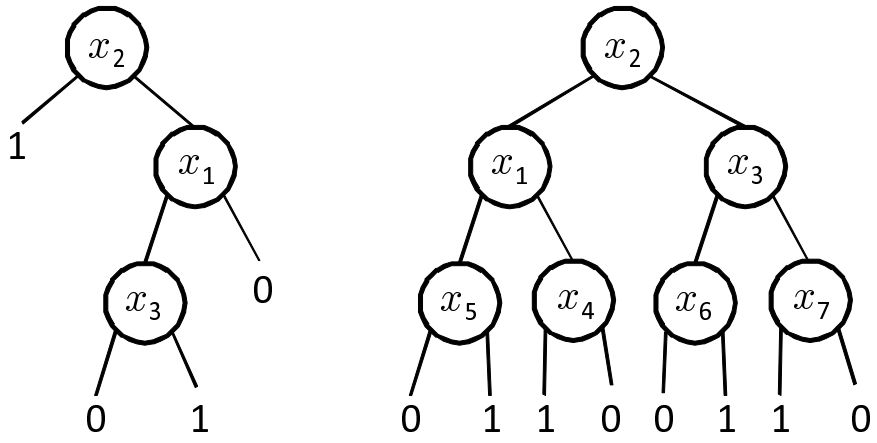

図 3.2: 決定リスト（左）と完全ニ分木（右）.

意されたい．一般的に，パリティノード付き決定木 T を T と同じ関数を表すパリティノードのない決定木 T' に変形したとき，$r(T) = r(T')$ かつ $\tilde{r}(T) = \tilde{r}(T')$ が成り立つ.

ここで，以降の命題で用いる，決定リストと完全ニ分木という特殊な構造を持つ決定木を定義する．決定リストとは，根から最も遠い内部頂点の子は二つとも葉であり，それ以外の任意の内部頂点の子は片方が葉でもう片方がある内部頂点である決定木である．完全二分木とは，全ての葉が同じ深さにある決定木である．決定リストと完全ニ分木の例を図 3.2 に示す.

次の命題では，ソフトランクの取りうる値の範囲を示す.

命題 3.2 深さが d である任意の決定木 T に対して,

$$\sqrt{d} \leq \tilde{r}(T) \leq d.$$

さらに，最初の等式が成り立つのは T が決定リストのときであり，二番目の等式が成り立つのは T が完全二分木のときである.

証明: 一般性を欠くことなく，パリティノードのない決定木を考えてよい．$\tilde{r}_{\max}(d)$ と $\tilde{r}_{\min}(d)$ をそれぞれ深さ d の決定木 T の中での $\tilde{r}(T)$ の最大値と最小値とする．$\tilde{r}_{\max}(0) = \tilde{r}_{\min}(0)$ であることと，$\tilde{r}_{\max}(d)$ と $\tilde{r}_{\min}(d)$ が d に対して単調増加であることは明らかである．T を深さが d である任意の木とする．T_1 と T_2 を T の根の子の部分木とする．T_1 の深さを $d-1$，T_2 の深さを $d' \leq d-1$ と仮定する.

まず，$\tilde{r}_{\max}(d) = d$ であることを示す．ソフトランクの定義と $\tilde{r}_{\max}$ の単調増加性より，$l = |\tilde{r}(T_1) - \tilde{r}(T_2)|$ とおくと，

$$\begin{aligned}\tilde{r}(T) &= \max\{\tilde{r}(T_1), \tilde{r}(T_2)\} - l + \sqrt{l^2+1} \\ &\leq \max\{\tilde{r}_{\max}(d-1), \tilde{r}_{\max}(d')\} - l + \sqrt{l^2+1} \\ &= \tilde{r}_{\max}(d-1) - l + \sqrt{l^2+1}.\end{aligned}$$

任意の $l \geq 0$ に対して $-l + \sqrt{l^2+1} \leq 1$ であるから，

$$\tilde{r}(T) \leq \tilde{r}_{\max}(d-1) + 1.$$

よって次の漸化式を得る．

$$\tilde{r}_{\max}(T) \leq \tilde{r}_{\max}(d-1) + 1.$$

ゆえに，

$$\tilde{r}_{\max}(d) \leq d.$$

一方，深さ d の完全二分木のソフトランクは d であるので，

$$\tilde{r}_{\max}(d) = d.$$

次に $\tilde{r}_{\min}(d) = \sqrt{d}$ を示す．ソフトランクの定義から，

$$\tilde{r}(T) = \begin{cases} \tilde{r}(T_1) + \sqrt{l^2+1} & \text{if } \tilde{r}(T_2) > \tilde{r}(T_1), \\ \tilde{r}(T_1) - l + \sqrt{l^2+1} & \text{if } \tilde{r}(T_2) \leq \tilde{r}(T_1). \end{cases}$$

よって，$\tilde{r}(T)$ は $\tilde{r}(T_2)$ について単調増加であることが分かる．

$$\tilde{r}(T) \geq \tilde{r}(T_1) - l + \sqrt{l^2+1}.$$

したがって，$\tilde{r}(T)$ は $\tilde{r}(T_2) = 0$ のとき最小となるので，

$$\tilde{r}(T) \geq \sqrt{\tilde{r}(T_1)^2 + 1} \geq \sqrt{\tilde{r}_{\min}(d-1)^2 + 1}.$$

よって次の漸化式を得る．

$$\tilde{r}_{\min}(d) \geq \sqrt{\tilde{r}_{\min}(d-1)^2 + 1}.$$

ゆえに，

$$\tilde{r}_{\min}(d) \geq \sqrt{d}.$$

一方で，深さが d である決定リストのソフトランクは $\sqrt{d}$ であるから，

$$\tilde{r}_{\min}(d) = \sqrt{d}.$$

□

3.3　パリティ関数に対するコスト付き量子敵対者限界

本節では，$\mathrm{ADV}_\alpha(\mathrm{XOR})$ を α の l_1 ノルムで正確に表現できることを示す．

定理 3.1 任意の $\alpha = (a, b) \in \mathrm{R}_+^2$ に対して，

$$\mathrm{ADV}_\alpha(\mathrm{XOR}) = a + b.$$

証明: まず，$\mathrm{ADV}_\alpha(\mathrm{XOR}) \leq a + b$ を示す．確率分布族 $p : \{0,1\}^2 \times \{1,2\} \to \mathcal{R}_+$ を以下のように定義する．任意の $x \in \{0,1\}^2$ に対して，

$$p_x(i) = \begin{cases} \frac{a}{a+b} & \text{if } i = 1, \\ \frac{b}{a+b} & \text{if } i = 2. \end{cases}$$

p が $\mathrm{MM}_\alpha(\mathrm{XOR})$ を定義している最適化問題の許容解であることは明らかである．XOR の値を 0 とする入力割り当てと 1 とする入力割り当ての全てのペア $(x, y) \in \{(00, 01), (00, 10), (11, 01), (11, 10)\}$ に対して，次の式が成り立つことは容易に確かめられる．

$$\frac{1}{\sum_{i:x_i \neq y_i} \sqrt{p_x(i)p_y(i)}/\alpha_i} = a + b.$$

したがって，定理 2.5 から $\mathrm{ADV}_\alpha(\mathrm{XOR}) = \mathrm{MM}_\alpha(\mathrm{XOR}) \leq a + b$ である．

次に $\mathrm{ADV}_\alpha(\mathrm{XOR}) \geq a + b$ を示す．XOR に対する敵対者行列 Γ を以下のように定義する．

	00	01	10	11
00	0	b	a	0
01	b	0	0	a
10	a	0	0	b
11	0	a	b	0

上記の Γ が $\mathrm{ADV}_\alpha(\mathrm{XOR})$ を定義している数理計画問題の許容解であることは容易に確かめられる．Γ の固有方程式は，次の式になる．

$$|\Gamma - xI| = (x + a - b)(x + a + b)(x - a + b)(x - a - b).$$

よって，$a + b$ は Γ の固有値の絶対値の最大値であり，$\|\Gamma\| = a + b$ を得る．同様に，$\Gamma \circ D_1$ に対する固有方程式と $\Gamma \circ D_2$ に対する固有方程式はそれぞれ以下のようになる．

$$\begin{aligned} |\Gamma \circ D_1 - xI| &= (x - a)^2(x + a)^2, \\ |\Gamma \circ D_2 - xI| &= (x - b)^2(x + b)^2. \end{aligned}$$

よって，$\|\Gamma \circ D_1\| = a$ と $\|\Gamma \circ D_2\| = b$ を得る．したがって，任意の $i \in \{1, 2\}$ に対して，

$$\frac{\alpha_i \|\Gamma\|}{\|\Gamma \circ D_i\|} = a + b$$

となる．以上より $\mathrm{ADV}_\alpha(\mathrm{XOR}) \geq a + b$ を得る．

□

3.4　マルチプレクサ関数に対するコスト付き量子敵対者限界の上界と下界

2 入力マルチプレクサ関数 MUX に対して，我々は $\mathrm{ADV}_\alpha(\mathrm{MUX})$ の正確な表現を導出することに成功してはいない．代わりに，$\mathrm{ADV}_\alpha(\mathrm{MUX})$ の上界と下界を与える．$\mathrm{MUX}(x_1, x_2, x_3) = \mathrm{MUX}(\bar{x}_1, x_3, x_2)$ であるので，命題 2.7 と 2.8 より，任意の $\alpha = (a, b, c) \in \mathrm{R}_+^3$ に対して，

$$\mathrm{ADV}_{(a,c,b)}(\mathrm{MUX}) = \mathrm{ADV}_{(a,b,c)}(\mathrm{MUX})$$

であることに注意されたい．よって，一般性を欠くことなくコストベクトル $\alpha = (a, b, c)$ について $b \leq c$ であると仮定してよい．

定理 3.2 $b \leq c$ であるような任意の $\alpha = (a, b, c) \in \mathrm{R}_+^3$ に対して，

$$\mathrm{ADV}_\alpha(\mathrm{MUX}) \geq b + \sqrt{(c-b)^2 + a^2}$$

が成り立つ．

証明: $b \leq c$ と仮定する．初めに，$a = 1$ のとき，$\alpha = (1, b, c)$ に対して，

$$\mathrm{ADV}_\alpha(\mathrm{MUX}) \geq b + \sqrt{(c-b)^2 + 1} \tag{3.2}$$

を示せば十分であることを示す．命題 2.6 より任意の $\alpha = (a, b, c) \in \mathrm{R}_+^3$ に対して，$\beta = (1, b/a, c/a)$ としたとき，$\mathrm{ADV}_\alpha(\mathrm{MUX}) = a\mathrm{ADV}_\beta(\mathrm{MUX})$ が成立する．よって，式 (3.2) が示せれば，題意を示したことになる．

	000	001	010	011	100	101	110	111
000	0	0	0	0	0	0	0	0
001	0	0	b	0	0	1	0	0
010	0	b	0	0	0	0	1	0
011	0	0	0	0	0	0	0	0
100	0	0	0	0	0	$\sqrt{c(c-b)}$	0	0
101	0	1	0	0	$\sqrt{c(c-b)}$	0	b	0
110	0	0	1	0	0	b	0	$\sqrt{c(c-b)}$
111	0	0	0	0	0	0	$\sqrt{c(c-b)}$	0

図 3.3: MUX に対する敵対者行列 Γ

以下の 4 つの条件を満たすような MUX に対する敵対者行列を構成することによって式 (3.2) を示す.

$$\|\Gamma\| \geq b + \sqrt{(c-b)^2+1} \tag{3.3}$$

$$\|\Gamma \circ D_1\| = 1, \tag{3.4}$$

$$\|\Gamma \circ D_2\| = b, \tag{3.5}$$

$$\|\Gamma \circ D_3\| = c. \tag{3.6}$$

ADV_α の定義から，式 (3.2) は式 (3.3)，式 (3.4)，式 (3.5)，式 (3.6) から得られる．図 3.3 にそのような Γ を与える．Γ が実際に MUX に対する敵対者行列であることは容易に確かめられる．

以下で (3.3)，(3.4)，(3.5)，(3.6) の各条件が成立することを検証する．

まず，(3.3) を検証する．行列 A を

$$A = \begin{bmatrix} b & 0 & 1 \\ 0 & 0 & \sqrt{c(c-b)} \\ 1 & \sqrt{c(c-b)} & b \end{bmatrix} \tag{3.7}$$

と定義する．λ を A の固有値とし対応する固有ベクトルを $v = (v_1, v_2, v_3)^T$ とする．すなわち，$Av = \lambda v$．$v' = (0, v_1, v_1, 0, v_2, v_3, v_3, v_2)^T$ と $v'' = (0, v_1, -v_1, 0, v_2, -v_3, v_3, -v_2)^T$ がそれぞれ λ と $-\lambda$ に対応する Γ の固有ベクトルであることは容易に確かめられる．すなわち，$\Gamma v' = \lambda v'$，$\Gamma v'' = -\lambda v''$．よって，$\Gamma$ の固有値の絶対値の最大値は A の固有値の絶対値の最大値に等しい．よって，λ_1，λ_2，λ_3 を

A の 3 つの固有値とすると，次の 6 つの値 λ_1，$-\lambda_1$，λ_2，$-\lambda_2$，λ_3，$-\lambda_3$ が Γ の固有値となる．Γ の残り 2 つの固有値は共に 0 であり，対応する固有ベクトルは $(1,0,0,0,0,0,0,0)^T$ と $(0,0,0,1,0,0,0,0)^T$ であることに注意されたい．すなわち，$\|\Gamma\| = \|A\|$ である．A の固有多項式は

$$\begin{aligned} p_A(x) &= |A - xI| \\ &= -x^3 + 2bx^2 + (c(c-b) - b^2 + 1)x - bc(c-b) \end{aligned}$$

であり，その根が A の固有値 $\lambda_1, \lambda_2, \lambda_3$ である．一般性を失わずに $\lambda_1 \geq \lambda_2 \geq \lambda_3$ と仮定する．

$$x_0 = b + \sqrt{(c-b)^2 + 1}$$

とおく．$c \geq b$ であるので，

$$p_A(x_0) = b(c-b)(\sqrt{(c-b)^2+1} - (c-b)) \geq 0.$$

$p_A(\lambda_1) = 0$，$p_A(+\infty) = -\infty$ であるので，$\lambda_1 \geq x_0$ でなければならない．したがって，$x_0 \geq ||\Gamma||$ となり，(3.3) が確かめられた．

次に (3.4) を示す．上記と同様の議論により，$\Gamma \circ D_1$ の固有値の絶対値の最大値は以下で定義する行列 B の固有値の絶対値の最大値に等しい．

$$B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

明らかに，$\|\Gamma \circ D_1\| = \|B\| = 1$ である．

次に (3.5) を示す．上記と同様の議論により，$\Gamma \circ D_2$ の固有値の絶対値の最大値は以下で定義する C の固有値の絶対値の最大値に等しい．

$$C = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}.$$

明らかに，$\|\Gamma \circ D_2\| = \|C\| = b$ である．

最後に (3.6) を示す．上記と同様の議論により，$\Gamma \circ D_3$ の固有値の絶対値の最大値は，以下で定義する D の固有値の絶対値の最大値に等しい．

$$D = \begin{bmatrix} b & 0 & 0 \\ 0 & 0 & \sqrt{c(c-b)} \\ 0 & \sqrt{c(c-b)} & b \end{bmatrix}.$$

明らかに，$\|\Gamma \circ D_3\| = \|D\| = c$ である．

□

以下の定理で我々が与える $\mathrm{ADV}_\alpha(\mathrm{MUX})$ の上界から，定理 3.2 の下界がほとんどタイトであることが分かる．

定理 3.3 $b \le c$ を満たす任意の $\alpha = (a, b, c) \in \mathrm{R}_+^3$ に対して，

$$\mathrm{ADV}_\alpha(\mathrm{MUX}) \le \frac{b + c + \sqrt{(c-b)^2 + 4a^2}}{2}$$

が成立する．

証明: 定理 3.2 の証明と同様に，$a = 1$ の場合，すなわち，$b \le c$ を満たす任意の $\alpha = (1, b, c) \in \mathrm{R}_+^3$ に対して

$$\mathrm{ADV}_\alpha(\mathrm{MUX}) \le \frac{b + c + \sqrt{(c-b)^2 + 4}}{2} \tag{3.8}$$

であることを示せば十分である．

(3.8) を示すために，量子敵対者法の双対表現を用いる．言い換えると，$\mathrm{MM}_\alpha(\mathrm{MUX})$ を定義している数理計画問題の許容解を構成し，それにより $\mathrm{ADV}_\alpha(\mathrm{MUX})$ の上界を導出する．

$A = \frac{b+c+\sqrt{(c-b)^2+4}}{2}$ と置く．確率分布族 $p : \{0,1\}^3 \times \{1,2,3\} \to \mathcal{R}_+$ を以下のように定義する．各 $x \in \{0,1\}^3$ に対して，

$$p_x(i) = \begin{array}{|c|ccc|}\hline x \backslash i & 1 & 2 & 3 \\ \hline 000, 001, 010, 011 & d & 1-d & 0 \\ 100, 111 & f & g & 1-f-g \\ 110, 101 & j & 0 & 1-j \\ \hline \end{array}$$

とする．ここで，

$$\begin{aligned} d &= 1 - \frac{b}{A}, \\ f &= \frac{b^2(A-b)}{A(bA - b^2 + 1)^2}, \\ g &= \frac{b}{A(bA - b^2 + 1)^2}, \\ j &= \frac{1}{A^2 - bA}. \end{aligned}$$

とする．p が $\mathrm{MM}_\alpha(\mathrm{MUX})$ の許容解であること，すなわち，各入力 x に対して p_x が確率分布であることは容易に確かめられる．MUX の出力値を 0 と 1 とする入力割り当ての任意のペア $(x,y) \in \mathrm{MUX}^{-1}(0) \times \mathrm{MUX}^{-1}(1)$ に対して，

$$\frac{1}{\sum_{i:x_i \neq y_i} \sqrt{p_x(i)p_y(i)}/\alpha_i} \leq A. \tag{3.9}$$

であることを示す必要がある．$\alpha = (1,b,c)$ であるので，$\alpha_1 = 1$，$\alpha_2 = b$，$\alpha_3 = c$ となることに注意されたい．16 個のペアからなる集合 $\mathrm{MUX}^{-1}(0) \times \mathrm{MUX}^{-1}(1)$ を 6 つのクラスに分け，それぞれのクラスに対して式 (3.9) が成立することを示す．

$(x,y) \in \{(000,010),(000,011),(001,010),(001,011)\}$, の場合，

$$\frac{1}{\sum_{i:x_i \neq y_i} \sqrt{p_x(i)p_y(i)}/\alpha_i} = \frac{b}{1-d} = A.$$

$(x,y) \in \{(000,101),(001,101),(110,010),(110,011)\}$ の場合，

$$\frac{1}{\sum_{i:x_i \neq y_i} \sqrt{p_x(i)p_y(i)}/\alpha_i} = \frac{1}{\sqrt{dj}} = A.$$

$(x,y) \in \{(000,111),(001,111),(100,010),(100,011)\}$ の場合，

$$\frac{1}{\sum_{i:x_i \neq y_i} \sqrt{p_x(i)p_y(i)}/\alpha_i} = \left(\sqrt{df} + \frac{\sqrt{(1-d)g}}{b}\right)^{-1} = A.$$

$(x,y) \in \{(100,101),(110,111)\}$ の場合，

$$\frac{1}{\sum_{i:x_i \neq y_i} \sqrt{p_x(i)p_y(i)}/\alpha_i} = \frac{c}{\sqrt{(1-f-g)(1-j)}} \leq A.$$

最後の不等式が成立する理由は次の式による．

$$\frac{A\sqrt{(1-f-g)(1-j)}}{c} = \frac{\sqrt{A-b-1}\sqrt{A-b+1}\sqrt{bA+1}}{\sqrt{c}\sqrt{c-b}\sqrt{bA-b^2+1}} \geq 1.$$

上記の不等式は次の式によって成立する．

$$(A-b-1)(A-b+1)(bA+1)-c(c-b)(bA-b^2+1) = \frac{1}{2}((c-b)\sqrt{(c-b)^2+4}-(c-b)^2) \geq 0.$$

$(x,y) = (100,111)$ の場合に対して式 (3.9) が成立することを示す．

$$w = \sqrt{c^2 - 2b^3c + 4},$$

$$z = b^2c^2 + (2b - b^3)c,$$

とする．このとき，

$$A\left(\frac{g}{b}+\frac{1-f-g}{c}\right)=\frac{b^2c^3+w(z+1)+(b^4+3)c+3b}{b^2c^3+wz+(b^4+3)c}\geq 1$$

したがって，

$$\frac{1}{\sum_{i:x_i\neq y_i}\sqrt{p_x(i)p_y(i)}/\alpha_i}=\left(\frac{g}{b}+\frac{1-f-g}{c}\right)^{-1}\leq A.$$

$(x,y)=(110,101)$ の場合，

$$\frac{1}{\sum_{i:x_i\neq y_i}\sqrt{p_x(i)p_y(i)}/\alpha_i}=\frac{c}{1-j}=A.$$

□

簡単な計算により，任意の α に対する $\mathrm{ADV}_\alpha(\mathrm{MUX})$ の下界と上界が小さな定数（高々1.2）の差を許して一致することが分かる．さらに，上界と下界は $b=c$ のときは完全に一致する．言い換えると，$b=c$ のとき $\mathrm{ADV}_{(a,b,c)}(\mathrm{MUX})$ の正確な表現を得たと言える．具体的には，$\mathrm{ADV}_{(a,b,b)}(\mathrm{MUX})=a+b$ である．

系 3.4 任意の $a,b\in\mathcal{R}$ に対して，

$$\mathrm{ADV}_{(a,b,b)}(\mathrm{MUX})=a+b$$

が成り立つ．

3.5　パリティノード付き一回読み決定木に対するソフトランクを用いた量子質問複雑さの下界

定理 3.1 と定理 3.2 を定理 2.7 と共に用いることで，$\mathrm{DT}_\oplus$ に属する決定木の量子質問複雑さの下界を導出することができる．この導出は，小節 3.2.1 において示したように，$\mathrm{DT}_\oplus$ が二つの関数 XOR と MUX を持ちいた合成関数として再帰的に定義される関数からなるという観察に基づく．

定理 3.5 $\mathrm{DT}_\oplus$ に属する任意の決定木 T に対して，

$$\mathrm{ADV}(T)\geq\tilde{r}(T)\geq r(T)$$

が成り立つ．

証明: 命題 3.1 より，$\tilde{r}(T) \geq r(T)$ である．T の深さに関する帰納法で $\mathrm{ADV}(T) \geq \tilde{r}(T)$ を示す.

（基底段階 1）T の深さが 0 であるとき，すなわち T が葉であるとき，明らかに $\mathrm{ADV}(T) = \tilde{r}(T) = 0$ である.

（基底段階 2）T の深さが 1 であるとき，T の根は通常の内部頂点であり，その子は値の異なるラベルが付けられた二つの葉である．明らかに $\tilde{r}(T) = 1$ である．さらに，T は $T(x) = x_i$ もくしくは $T(x) = \bar{x}_i$ という関数を計算する木である．このような関数に対する量子敵対者限界は，次の敵対者行列 Γ を用いれば容易に $\mathrm{ADV}(T) \geq \tilde{r}(T)$ を満たすことが示せる．

$$\Gamma = \begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

（帰納段階）T の深さ d が 2 以上であるとき，T の根がパリティノードである場合（場合 1）と通常の内部頂点である場合（場合 2）の二つの場合を考える必要がある.

まず，場合 1 について考える．このとき，T の根はある変数 x_i によってラベルづけられたパリティノードであり，深さが $d-1$ のただ一つの子の部分木 T_1 を持つ．明らかに，T は関数 $\mathrm{XOR}(x_i, T_1)$ を計算する．この関数に定理 2.7 を適用すると，

$$\mathrm{ADV}(T) = \mathrm{ADV}_{\alpha}(\mathrm{XOR})$$

を得る．ここで，$\alpha = (\mathrm{ADV}(x_i), \mathrm{ADV}(T_1)) = (1, \mathrm{ADV}(T_1))$ である．よって，定理 3.1 より，

$$\mathrm{ADV}(T) = 1 + \mathrm{ADV}(T_1) \tag{3.10}$$

を得る．帰納法の仮定より，

$$\mathrm{ADV}(T_1) \geq \tilde{r}(T_1) \tag{3.11}$$

であり，ソフトランクの定義から

$$\tilde{r}(T) = 1 + \tilde{r}(T_1) \tag{3.12}$$

を得る．式 (3.10)，式 (3.11)，式 (3.12) より

$$\mathrm{ADV}(T) \geq \tilde{r}(T)$$

を得る．

次に場合 2 について考える．このとき，T の根はある変数 x_i でラベルづけられた通常の内部頂点であり，深さが高々$d-1$ である二つの子の部分木を持つ．T の左の子の部分木を T_1 とし，右の子の部分木を T_2 とする．明らかに T が計算する関数は $\mathrm{MUX}(x_i, T_1, T_2)$ である．一般性を欠くことなく，$\mathrm{ADV}(T_1) \leq \mathrm{ADV}(T_2)$ を仮定できる．なぜなら，そうでなければ等価な関数 $\mathrm{MUX}(\bar{x}_i, T_2, T_1)$ について検証すればよいからである．

この関数に定理 2.7 を適用することで

$$\mathrm{ADV}(T) = \mathrm{ADV}_{\alpha}(\mathrm{MUX}) \tag{3.13}$$

を得る．ここで，$\alpha = (1, \mathrm{ADV}(T_1), \mathrm{ADV}(T_2))$ である．帰納法の仮定から，

$$\mathrm{ADV}(T_1) \geq \tilde{r}(T_1),\ \mathrm{ADV}(T_2) \geq \tilde{r}(T_2) \tag{3.14}$$

である．ここで，$\tilde{r}(T_1) \leq \tilde{r}(T_2)$ という場合と $\tilde{r}(T_2) \leq \tilde{r}(T_1)$ という二つの場合を考える．

まず，$\tilde{r}(T_1) \leq \tilde{r}(T_2)$ の場合について考える．$\beta = (1, \tilde{r}(T_1), \tilde{r}(T_2))$ とする．(3.14) より，$\alpha \geq \beta$ が成り立つ．よって，命題 2.5 より，

$$\mathrm{ADV}_{\alpha}(\mathrm{MUX}) \geq \mathrm{ADV}_{\beta}(\mathrm{MUX}) \tag{3.15}$$

であり，定理 3.2 より

$$\begin{aligned} \mathrm{ADV}_{\beta}(\mathrm{MUX}) &\geq \tilde{r}(T_1) + \sqrt{(\tilde{r}(T_2) - \tilde{r}(T_1))^2 + 1} \\ &= \tilde{r}(T) \end{aligned} \tag{3.16}$$

を得る．ここで最後の等式は，$\tilde{r}(T_1) \leq \tilde{r}(T_2)$ であることとソフトランクの定義から得られる．式 (3.13)，式 (3.15)，式 (3.16) より，

$$\mathrm{ADV}(T) \geq \tilde{r}(T)$$

を得る．

最後に $\tilde{r}(T_2) \leq \tilde{r}(T_1)$ の場合を考える．$\beta = (1, \tilde{r}(T_2), \tilde{r}(T_1))$ とする．$\mathrm{ADV}(T_1) \leq \mathrm{ADV}(T_2)$ という仮定と帰納法の仮定 (3.14) により，

$$\tilde{r}(T_2) \leq \tilde{r}(T_1) \leq \mathrm{ADV}(T_1)$$

と

$$\tilde{r}(T_1) \leq \mathrm{ADV}(T_1) \leq \mathrm{ADV}(T_2)$$

を得る．よって，$\beta \leq \alpha$ である．したがって，命題 2.5 と定理 3.2 により，

$$\begin{aligned} \mathrm{ADV}_\alpha(\mathrm{MUX}) &\geq \mathrm{ADV}_\beta(\mathrm{MUX}) \\ &\geq \tilde{r}(T_2) + \sqrt{(\tilde{r}(T_1) - \tilde{r}(T_2))^2 + 1} \\ &= \tilde{r}(T) \end{aligned} \tag{3.17}$$

を得る．式 (3.17) と式 (3.13) より，

$$\mathrm{ADV}(T) \geq \tilde{r}(T)$$

を得る．

□

上記の定理 3.5 を定理 2.3 と共に用いることで，$\mathrm{DT}_\oplus$ に属する任意の決定木 T に対し，T のソフトランクが T の量子質問複雑さの下界を与えることが分かる．さらに，そのことから $\mathrm{DT}_\oplus$ に属す決定木が計算する関数に対して，決定的質問複雑さと量子質問複雑さの差が高々2 乗しかないことを示すことができる．

定理 3.6 $\mathrm{DT}_\oplus$ に属する任意の決定木 T と任意の $\epsilon \in [0, 1/2)$ に対して，

$$Q_\epsilon(T) = \Omega(\tilde{r}(T))$$

と

$$Q_\epsilon(T) = \Omega(\sqrt{D(f)}))$$

が成り立つ．

証明: 定理 2.3 と定理 3.5 より，

$$Q_\epsilon(T) = \Omega(\tilde{r}(T))$$

は明らかである．T の深さを d とすると，$d \geq D(T)$．命題 3.2 より $\tilde{r}(T) \geq \sqrt{d}$ であることから

$$Q_\epsilon(T) = \Omega(\sqrt{D(T)})$$

を得る．

□

3.6　定理 3.5 の応用

本節では，$\mathrm{DT}_{\oplus}$ に属する決定木で表すことのできるいくつかの関数に対してソフトランクの下界を示すことにより，定理 3.5 の有用性を示す．

3.6.1　AND 関数と OR 関数

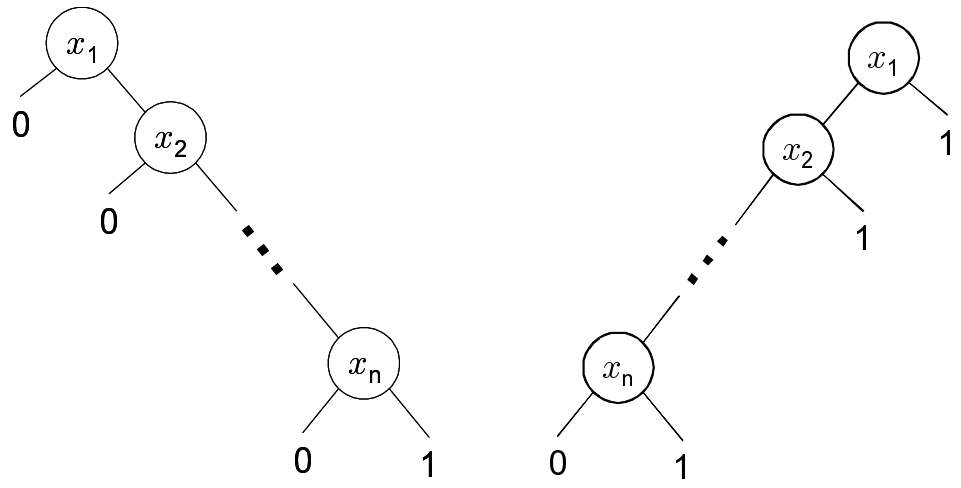

図 3.4: AND_n を計算する決定木（左）と OR_n を計算する木

n 変数 AND 関数 AND_n は

$$\mathrm{AND}_n = \mathrm{MUX}(x_n, 0, \mathrm{AND}_{n-1})$$

のように再帰的に表すことができる．したがって，AND_n は図 3.4 の左に示すように，深さ n の一回読み決定木で計算される．AND_n のソフトランクは，ソフトランクの定義から

$$\tilde{r}(\mathrm{AND}_n) = \sqrt{(\tilde{r}(\mathrm{AND}_n))^2 + 1}$$

という再帰式で表されるので，$\tilde{r}(\mathrm{AND}_n) = \sqrt{n}$ となる．よって，定理 3.5 より，

$$\mathrm{ADV}(\mathrm{AND}_n) \geq \sqrt{n}$$

となる．AND_n を表す決定木のランクは 1 であるので，AND_n に対しては，ランクを用いてはよい下界を導出することができないことに注意されたい．一方，n 変数 OR 関数 OR_n も

$$\mathrm{OR}_n = \mathrm{MUX}(x_n, \mathrm{OR}_{n-1}, 1)$$

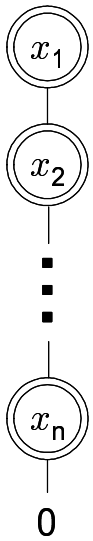

図 3.5: PARITY_n を計算するパリティノード付き決定木

のように再帰的に表すことができる．OR_n は図 3.4 の右に示すように深さ n の一回読み決定木で計算され，そのソフトランクの値は AND の場合と同様に $\sqrt{n}$ となる．よって，定理 3.5 より，

$$\mathrm{ADV}(\mathrm{OR}_n) \geq \sqrt{n}$$

となる．

3.6.2　PARITY 関数

n 変数パリティ関数 PARITY_n は

$$\mathrm{PARITY}_n = \mathrm{XOR}(x_n, \mathrm{PARITY}_{n-1})$$

のように XOR 関数を用いて再帰的に表すことができる．よって，この関数を図 3.5 のような深さが n のパリティノード付き一回読み決定木で表すことができる．明らかにこの木のソフトランクは n である．よって，定理 3.5 より，

$$\mathrm{ADV}(\mathrm{PARITY}_n) \geq n$$

を得る．

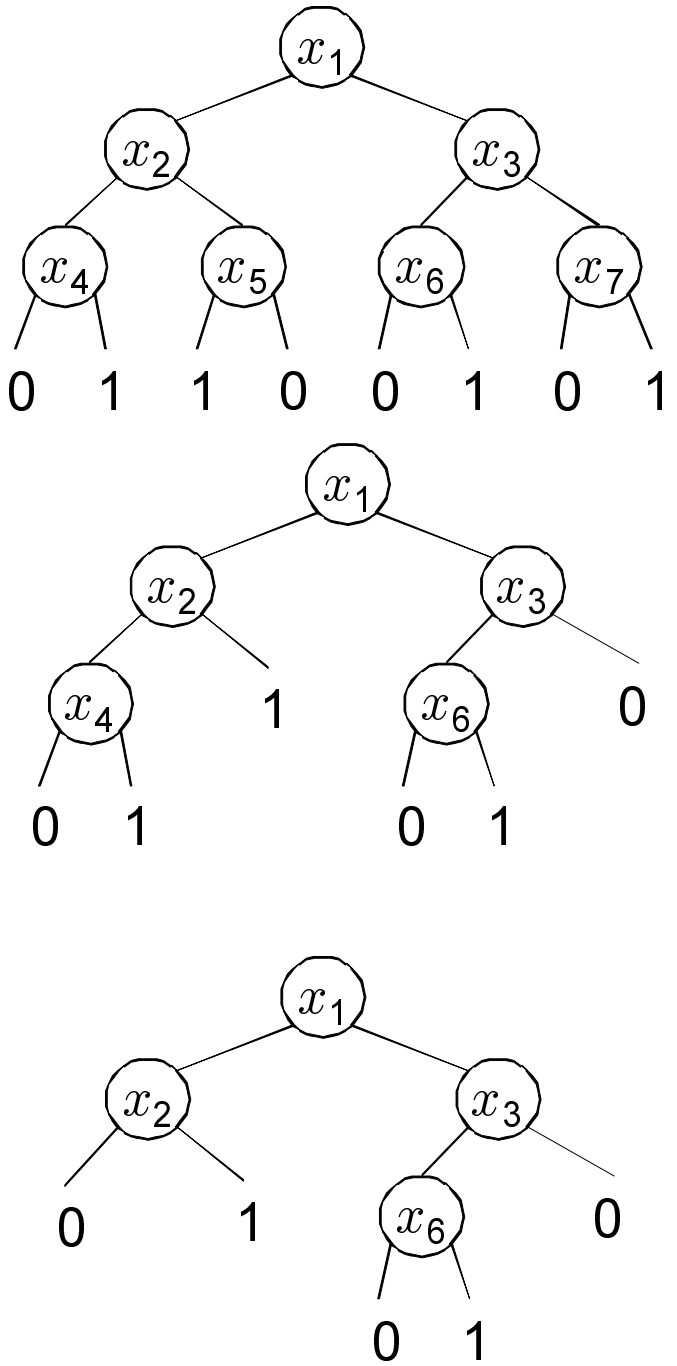

図 3.6: AVL 決定木の例

3.6.3　一回読み AVL 決定木

本小節では一回読み AVL 決定木で表される関数を考える．一回読み AVL 決定木は，探索のための効率のよいデータ構造の一つである AVL 木と同じ構造を持つ決定木であり，さらに，内部頂点に同じ変数が高々1 回しか現れないという一回読みの条件を付け加えた決定木である．AVL 木は，任意の内部頂点に対して，その左の子の部分木と右の子の部分木の深さの差が高々1 であるような決定木である．図 3.6 に AVL 決定木の例を示す．

定理 3.7 深さが d である任意の一回読み AVL 決定木 T に対して，

$$\mathrm{ADV}(T) \geq \left\lceil \frac{d}{2} \right\rceil$$

が成り立つ．

証明: $r_d = \min\{r(T) \mid T$ は深さが d の AVL 決定木 $\}$ とする．d に関する帰納法で

$$r_d = \left\lceil \frac{d}{2} \right\rceil \tag{3.18}$$

を証明する．式 (3.18) を定理 3.5 と共に用いることにより題意を示せる．

（基底段階）深さ $d = 0$ の AVL 決定木は葉のみの木である．したがって，$r_0 = 0$ が成り立つ．

（帰納段階）$d \leq k$ のとき 3.18 が成立すると仮定する．AVL 決定木の部分決定木も AVL 決定木であることとランクの定義から，r_d は d に対して単調増加である．よって，深さが $k+1$ でランクが r_{k+1} である AVL 決定木の根の子の二つの部分木は，それぞれランクが r_k である AVL 決定木とランクが r_{k-1} である AVL 決定木としてよい．このとき，k が偶数ならば，

$$\begin{aligned} r_k &= \left\lceil \frac{k}{2} \right\rceil = \frac{k}{2} \\ r_{k-1} &= \left\lceil \frac{k-1}{2} \right\rceil = \frac{k}{2} \end{aligned}$$

であるから，ランクの定義より，

$$r_{k+1} = \frac{k}{2} + 1 = \left\lceil \frac{k+1}{2} \right\rceil$$

となる．一方，k が奇数ならば，

$$\begin{aligned} r_k &= \left\lceil \frac{k}{2} \right\rceil = \frac{k+1}{2} \\ r_{k-1} &= \left\lceil \frac{k-1}{2} \right\rceil = \frac{k}{2} \end{aligned}$$

であるから，ランクの定義より，

$$r_{k+1} = \frac{k+1}{2} = \left\lceil \frac{k+1}{2} \right\rceil$$

となる．

□

3.7　基底関数を拡張した一回読みブール式に対する量子質問複雑さの下界

本節では基底 $\mathcal{B}$ を $\mathcal{B} = \{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}, \mathrm{XOR}, \mathrm{MUX}\}$ とした一回読みブール式の量子質問複雑さの下界を導出する．ここで，あるブール式が一回読みであるとは，各変数がその式の中で高々一回しか現れないのときを言う．一回読み $\mathfrak{B}$ 式全てからなるクラスを $\mathcal{F}$ とする．

基底が $\{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}\}$ である任意のブール式に対し，ド・モルガンの規則を使えば論理否定 $\neg$ が論理変数にしか付かない式に必ず変形できる．基底 $\mathcal{B}$ 上の式についても，次の二つの等式をド・モルガンの規則とともに再帰的に用いれば，同様に $\neg$ が論理変数にしか付かない式に変形できる．

$$\neg\mathrm{XOR}(F_1, F_2) = \mathrm{XOR}(\bar{F}_1, F_2) = \mathrm{XOR}(F_1, \bar{F}_2)$$

$$\neg\mathrm{MUX}(F_1, F_2, F_3) = \mathrm{MUX}(F_1, \bar{F}_2, \bar{F}_3)$$

よって，$\mathcal{B}$ 上のブール式についても一般性を欠くことなく $\neg$ は論理変数以外には付かないと仮定してよい．

$\mathfrak{B}$ 式 F の構文木とは，次のように再帰的に定義される木のことである．F が定数 $a \in \{0, 1\}$ であるときは，F の構文木はラベルが a である葉のみの木である．$F = \mathrm{OP}(F_1, F_2, \ldots, F_k)$ $(\mathrm{OP} \in \mathfrak{B})$ とする．このとき，F の構文木は OP を根のラベルとし，根の子の部分木が左から順に $T_1, T_2, \ldots, T_k$ である木である．ここで，$T_1, T_2, \ldots, T_k$ はそれぞれ $F_1, F_2, \ldots, F_k$ の構文木である．

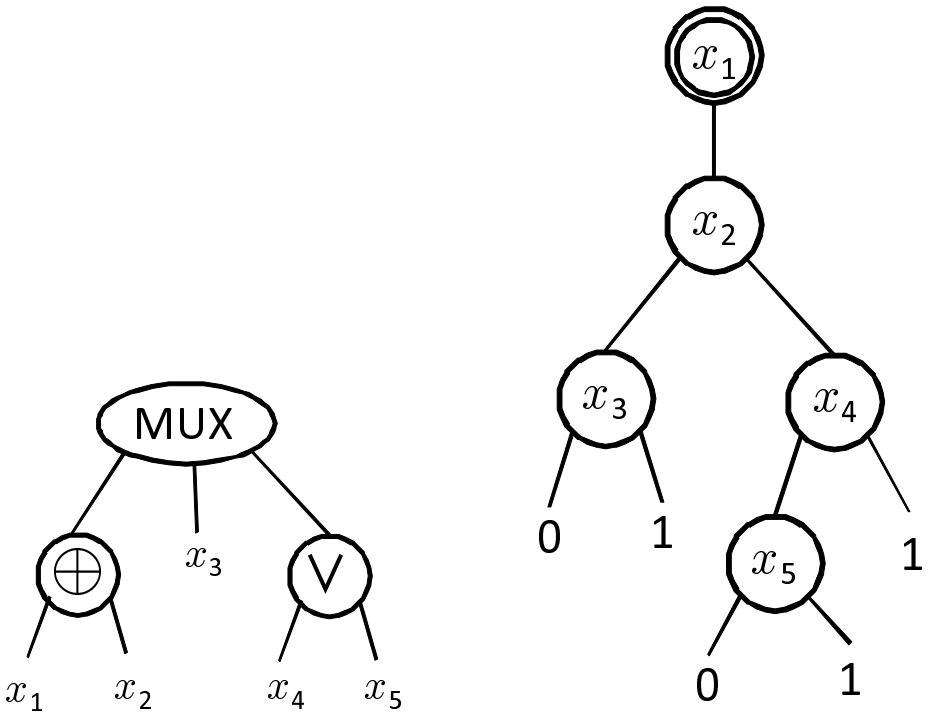

図 3.7: ブール式 $F = \mathrm{MUX}((x_1 \oplus x_2), x_3, x_4 \vee x_5)$ の構文木（左）と F と表す関数と同じ関数を計算するパリティノード付き決定木

定義 3.3 $\mathfrak{B}$ を任意のブール関数の集合とする．$\mathfrak{B}$ 式 F の構文木を T とする．このとき，F の構文木深さとは T の深さのことである．

ブール式 $F = \mathrm{MUX}((x_1 \oplus x_2), x_3, x_4 \vee x_5)$ に対する構文木と F と同じ関数を計算する決定木を例として図 3.7 に示す．構文木（左）の深さは 2 であるのに対し，決定木（右）の深さは 4 である．ブール式に対する構文木の深さとそのブール式の表す関数を計算する決定木の深さは，一般的に異なることに注意されたい．

本節で示す結果は節 3.5 のパリティノード付き一回読み決定木のクラス $\mathrm{DT}_\oplus$ に対する結果の拡張である．その理由は，$\mathrm{DT}_\oplus$ に含まれる任意の決定木が計算する関数は，基底を $\{\mathrm{XOR}, \mathrm{MUX}\}$ とする一回読みブール式で明らかに表されるからである．

節 3.5 においては，パリティノード付き一回読み決定木 T の量子質問複雑さの下界導出のために，二つの指標ソフトランク $\tilde{r}(T)$ と決定木の深さ $d(T)$ を用いた．本節では，これら二つの指標の定義域を $\mathrm{DT}_\oplus$ から $\mathcal{F}$ へと拡張し，節 3.5 と同様に，ソフトランクと決定木深さを用いることで一回読み $\mathfrak{B}$ 式の量子質問複雑さの下界

導出を行う．

定義 3.4 F を $\mathcal{F}$ に属する式とする．以下で定義される $\tilde{r}(F)$ を F のソフトランクと呼び，$d(F)$ を F の決定的深さと呼ぶ．

1. F が単一のリテラルであるとき，$\tilde{r}(F) = d(F) = 1$ とする．
2. ある二つの式 G_1 と G_2 に対して $F = G_1 \wedge G_2$ または $F = G_1 \vee G_2$ であるとき，

$$\begin{aligned} \tilde{r}(F) &= \sqrt{\tilde{r}(G_1)^2 + \tilde{r}(G_2)^2} \\ d(F) &= d(G_1) + d(G_2) \end{aligned}$$

とする．

3. ある二つの式 G_1 と G_2 に対して $F = \mathrm{XOR}(G_1, G_2)$ であるとき，

$$\begin{aligned} \tilde{r}(F) &= \tilde{r}(G_1) + \tilde{r}(G_2) \\ d(F) &= d(G_1) + d(G_2) \end{aligned}$$

とする．

4. ある三つの式 G_1 と G_2 と G_3 に対して $F = \mathrm{MUX}(G_1, G_2, G_3)$ であるとき，

$$\begin{aligned} \tilde{r}(F) &= \min\{\tilde{r}(G_2)\tilde{r}(G_3)\} + \sqrt{\tilde{r}(G_1)^2 + (\tilde{r}(G_2) - \tilde{r}(G_3)))^2} \\ d(F) &= d(G_1) + \max\{d(G_2), d(G_3)\} \end{aligned}$$

とする．

$F \in \mathrm{DT}_{\oplus}$ のとき，$\tilde{r}(F)$ の定義は定義 3.2 の決定木表現に基づく定義と一致する．$d(F)$ も決定木表現の深さと一致する．

このようにして拡張されたソフトランクは一回読み $\mathfrak{B}$ 式の表す関数の量子敵対者限界の下界を与える．

定理 3.8 $\mathcal{F}$ に含まれる任意の式 F に対して，

$$\mathrm{ADV}(F) \geq \tilde{r}(F).$$

証明: F の深さによる帰納法で $\mathrm{ADV}(F) \geq \tilde{r}(F)$ を証明する．

(基底段階) F の構文的深さが 0 であるとき，すなわち，F がリテラルのみであるとき，明らかに $\mathrm{ADV}(F) = \tilde{r}(F) = 1$ である．

(帰納段階) F の深さが 1 より大きい場合，次の 3 つの場合を考える．$F = G_1 \vee G_2$ または $F = G_1 \wedge G_2$ である場合（場合 1），$F = \mathrm{XOR}(G_1, G_2)$（場合 2），$F = \mathrm{MUX}(G_1, G_2, G_3)$ (場合 3).

まず場合 1，すなわち，$F = G_1 \vee G_2$ または $F = G_1 \wedge G_2$ の場合を考える．定理 2.7 と命題 2.4 より，

$$\mathrm{ADV}(F) = \sqrt{\mathrm{ADV}(G_1)^2 + \mathrm{ADV}(G_2)^2}. \tag{3.19}$$

を得る．帰納法の仮定から，

$$\mathrm{ADV}(G_1) \geq \tilde{r}(G_1), \ \ \mathrm{ADV}(G_2) \geq \tilde{r}(G_2) \tag{3.20}$$

を得る．r の定義から，

$$\tilde{r}(F) = \sqrt{\tilde{r}(G_1)^2 + \tilde{r}(G_2)^2}. \tag{3.21}$$

を得る．(3.19)，(3.20)，(3.21) より，

$$\mathrm{ADV}(F) \geq \tilde{r}(F),$$

を得る．

次に，場合 2，すなわち，$F = \mathrm{XOR}(G_1, G_2)$ のときを考える．定理 3.1 から，

$$\mathrm{ADV}(F) = \mathrm{ADV}(G_1) + \mathrm{ADV}(G_2). \tag{3.22}$$

を得る．帰納法の仮定から，

$$\mathrm{ADV}(G_1) \geq \tilde{r}(G_1), \ \ \mathrm{ADV}(G_2) \geq \tilde{r}(G_2) \tag{3.23}$$

を得る．r の定義から，

$$\tilde{r}(F) = \tilde{r}(G_1) + \tilde{r}(G_2). \tag{3.24}$$

を得る．(3.22)．(3.23)，(3.24) より，

$$\mathrm{ADV}(F) \geq \tilde{r}(F),$$

を得る．

最後に場合 3，すなわち，$F = \mathrm{MUX}(G_1, G_2, G_3)$ のときを考える．一般性を欠くことなく $\mathrm{ADV}(G_2) \leq \mathrm{ADV}(G_3)$ を仮定できる．なぜなら，もしそうでなければ代わりに等価な関数 $\mathrm{MUX}(\bar{G}_1, G_3, G_2)$ を検証すればよいからである．

定理 2.7 を適用することにより，$\alpha = (\mathrm{ADV}(G_1), \mathrm{ADV}(G_2), \mathrm{ADV}(G_3))$ とすると，

$$\mathrm{ADV}(F) = \mathrm{ADV}_\alpha(\mathrm{MUX}) \tag{3.25}$$

を得る．帰納法の仮定より，各 i $(1 \leq i \leq 3)$ に対して，

$$\mathrm{ADV}(G_i) \geq \tilde{r}(G_i). \tag{3.26}$$

ここで，$\tilde{r}(G_2) \leq \tilde{r}(G_3)$ の場合と $\tilde{r}(G_3) \leq \tilde{r}(G_2)$ の場合を考える．

$\tilde{r}(G_2) \leq \tilde{r}(G_3)$ の場合を考える．$\beta = (\tilde{r}(G_1), \tilde{r}(G_2), \tilde{r}(G_3))$ とする．(3.26) より，$\alpha \geq \beta$ を得る．したがって，命題 2.5 より，

$$\mathrm{ADV}_\alpha(\mathrm{MUX}) \geq \mathrm{ADV}_\beta(\mathrm{MUX}) \tag{3.27}$$

となる．定理 3.2 より，

$$\begin{aligned} \mathrm{ADV}_\beta(\mathrm{MUX}) &\geq \tilde{r}(G_2) + \sqrt{(\tilde{r}(G_3) - \tilde{r}(G_2))^2 + \tilde{r}(G_1)^2} \\ &= \tilde{r}(F), \end{aligned} \tag{3.28}$$

を得る．ここで，最後の等式はソフトランクの定義から導かれる．(3.25)，(3.27)，(3.28) より，

$$\mathrm{ADV}(F) \geq \tilde{r}(F),$$

を得る．

最後に $\tilde{r}(G_3) \leq \tilde{r}(G_2)$ の場合を考える．$\beta = (\tilde{r}(G_1), \tilde{r}(G_3), \tilde{r}(G_2))$ とする．$\mathrm{ADV}(G_2) \leq \mathrm{ADV}(G_3)$ という仮定と帰納法の仮定 (3.26) より，

$$\tilde{r}(G_3) \leq \tilde{r}(G_2) \leq \mathrm{ADV}(G_2) \leq \mathrm{ADV}(G_3).$$

を得る．ゆえに $\beta \leq \alpha$ を得る．したがって，命題 2.5 と定理 3.2 を適用することにより，

$$\begin{aligned} \mathrm{ADV}_\alpha(\mathrm{MUX}) &\geq \mathrm{ADV}_\beta(\mathrm{MUX}) \\ &\geq \tilde{r}(G_3) + \sqrt{(\tilde{r}(G_2) - \tilde{r}(G_3))^2 + \tilde{r}(G_1)^2} \\ &= \tilde{r}(F). \end{aligned}$$

を得る．上記の不等式と (3.25) より，

$$\mathrm{ADV}(F) \geq \tilde{r}(F)$$

を得る．

□

定理 2.3 と共に上記の定理 3.8 を用いると，直ちに以下の結果を得る．

系 3.9 任意の一回読み $\mathfrak{B}$ 式 F と任意の $\epsilon \in [0, 1/2)$ に対して，

$$Q_\epsilon(F) = \Omega(\tilde{r}(F)).$$

が成り立つ．

さらに，$\mathcal{F}$ に含まれる任意の式によって表される関数に対して，決定的質問複雑さと量子質問複雑さの差が高々2 乗しかないことを示す．これがチュ結果である．これを示すために，まず二つの補題を示す．

補題 3.10 任意の一回読み $\mathfrak{B}$ 式 F に対して，

$$d(F) \geq D(F)$$

が成り立つ．

証明: F に対する決定性質問アルゴリズムを次のように構成する．もし F が x_i または $\bar{x}_i$ という単一のリテラルであった場合には，入力割り当てにおける x_i の値を質問する．$F = x_i$ であるならばオラクルから得た値をそのまま出力し，$F = \bar{x}_i$ であるならばオラクルから得た値の否定を出力する．$\mathcal{F}$ に含まれるある 2 つの式 F_1 と F_2 に対して $F = F_1 \wedge F_2$ または $F = F_1 \vee F_2$ または $F = \mathrm{XOR}(F_1, F_2)$ である場合は，F_1 と F_2 の値を得るために F_1 と F_2 をそれぞれ再帰的に評価した後に F の値を計算して出力する．$\mathcal{F}$ に含まれるある 3 つの式 F_1 と F_2 と F_3 に対して $F = \mathrm{MUX}(F_1, F_2, F_3)$ である場合は，初めに F_1 を評価し，F_1 の値に応じて F_2 か F_3 を評価する．上記のアルゴリズムによってなされる質問回数が $d(F)$ で抑えられるのは明らかである．

□

補題 3.11 任意の一回読み $\mathfrak{B}$ 式 F に対して,

$$\sqrt{d(F)} \leq \tilde{r}(F). \tag{3.29}$$

が成り立つ.

証明: F の深さによる帰納法で (3.29) を示す.

(基底段階) F の構文的深さが 0 である場合，すなわち，F があるリテラルであるとき，明らかに $\tilde{r}(F) = d(F) = 1$ となる．よって (3.29) が成り立つ.

(帰納段階) 次の 3 つの場合を考える．$F = G_1 \vee G_2$ または $F = G_1 \wedge G_2$ の場合（場合 1）と $F = \mathrm{XOR}(G_1, G_2)$ の場合（場合 2）と $F = \mathrm{MUX}(G_1, G_2, G_3)$ の場合（場合 3）である.

まず $F = G_1 \wedge G_2$ または $F = G_1 \vee G_2$ の場合を考える．$\tilde{r}$ と d の定義から,

$$\tilde{r}(F) = \sqrt{\tilde{r}(G_1)^2 + \tilde{r}(G_2)^2}$$

と

$$d(F) = d(G_1) + d(G_2)$$

を得る．帰納法の仮定 $\tilde{r}(G_1) \geq \sqrt{d(G_1)}$ と $\tilde{r}(G_2) \geq \sqrt{d(G_2)}$ を上記の式と共に用いると，式 (3.29) を得る.

次に $F = \mathrm{XOR}(G_1, G_2)$ の場合を考える．$\tilde{r}$ と d の定義から,

$$\tilde{r}(F) = \tilde{r}(G_1) + \tilde{r}(G_2)$$

と

$$d(F) = d(G_1) + d(G_2).$$

を得る．帰納法の仮定から,

$$\begin{aligned} \tilde{r}(F) &= \tilde{r}(G_1) + \tilde{r}(G_2) \\ &\geq \sqrt{d(G_1)} + \sqrt{d(G_2)} \\ &\geq \sqrt{d(G_1) + d(G_2)} \\ &= \sqrt{d(F)}, \end{aligned}$$

を得る．よって，(3.29) が成立する.

最後に，$F = \mathrm{MUX}(G_1, G_2, G_3)$ の場合を考える．$\tilde{r}$ と d の定義から,

$$d(F) = d(G_1) + \max\{d(G_2), d(G_3)\} \tag{3.30}$$

と

$$\tilde{r}(F) = \begin{cases} \tilde{r}(G_2) + \sqrt{l^2 + \tilde{r}(G_1)^2} & \text{if } \tilde{r}(G_3) > \tilde{r}(G_2), \\ \tilde{r}(G_3) + \sqrt{l^2 + \tilde{r}(G_1)^2} & \text{if } \tilde{r}(G_3) \leq \tilde{r}(G_2), \end{cases}$$

を得る．ここで，$l = |\tilde{r}(G_2) - \tilde{r}(G_3)|$．$\tilde{r}(G_3) > \tilde{r}(G_2)$ の場合は，$\tilde{r}(F)$ は $\tilde{r}(G_2)$ について単調増加関数なので，$\tilde{r}(G_2) = 0$ のとき最小化される．$\tilde{r}(G_3) \leq \tilde{r}(G_2)$ の場合は，$\tilde{r}(F)$ は $\tilde{r}(G_3)$ について単調増加関数なので，$\tilde{r}(G_3) = 0$ のとき最小化される．よって，どちらの場合も次の式を得る．

$$\tilde{r}(F) \geq \sqrt{\max\{\tilde{r}(G_2), \tilde{r}(G_3)\}^2 + \tilde{r}(G_1)^2}.$$

帰納法の仮定と上記の不等式と式 (3.30) より，

$$\tilde{r}(F) \geq \sqrt{d(F)}.$$

□

系 3.9 と補題 3.10 と補題 3.11 の不等式を全て繋げると本節の主定理を得る．

定理 3.12 任意の一回読み $\mathfrak{B}$ 式 F に対して，

$$Q_\epsilon(F) = \Omega(\sqrt{D(F)})$$

が成り立つ．

3.8　まとめ

本節では，まずパリティノード付き一回読み決定木 T によって表されるブール関数を考え，その有界誤り量子質問複雑さの下界を決定木のソフトランク $\tilde{r}(T)$ が与えることを示した．ソフトランクは与えられた木の形の平衡度を測るものである．したがって，この下界はブール関数の量子質問複雑さが，それを表す決定木の平衡度に深く関係していることを示している．ソフトランクはいくつかの関数族に対しては容易に求めることが可能であり，本章では実際にソフトランクを入力変数の数 n の関数として解析的に評価することにより，n 変数 OR 関数の計算に $\Omega(\sqrt{n})$ 回の質問を要すること，n 変数パリティ関数の計算に $\Omega(n)$ 回の質問を要することを導いた．次に，この結果を拡張し，基底 $B = \{\text{AND}, \text{OR}, \text{NOT}, \text{XOR}, \text{MUX}\}$ 上の一回読みブール式 F によって表される任意の関数に対しても，F のソフトランク

$\tilde{r}(F)$ が量子質問複雑さの下界を与えることを示した．また，$\mathcal{F}$ に属する式によって表される関数に対して，決定的アルゴリズムと量子アルゴリズムの間の質問複雑さの差が高々2 乗しかないことも示した．この分野における重要な 2 乗ギャップ予想を裏付けるものである..

本章の技術的な貢献は，2 変数排他的論理和関 XOR と 2 入力マルチプレクサ関数 MUX に対するコスト付き量子敵対者限界の精密な限界を与えたことである．これらの限界を Høyer らの合成関数に対する定理 [13] と共に用いることでパリティノード付き一回読み決定木や一回読み $\mathfrak{B}$ 式の量子質問複雑さの下界を導出している．$\mathrm{ADV}_\alpha(\mathrm{XOR})$ と $\mathrm{ADV}_\alpha(\mathrm{MUX})$ の限界を導出するために，以下のような方法で明示的に敵対者行列を構成した．半正定値計画問題を解くパッケージを用いて，様々なコストベクトル α に対する，最適な敵対者行列 Γ^*_α を 12 桁程度の精度で数値的に計算した．得られた各敵対者行列を観察し，α の要素を用いて Γ^*_α を代数的に表現しようと試みた．幸運なことに，XOR に関しては正確な表現を得ることができ，それは定理 3.1 の証明で示しているように，

	00	01	10	11
00	0	b	a	0
01	b	0	0	a
10	a	0	0	b
11	0	a	b	0

である．しかしながら，図 3.3 で与えた敵対者行列は最適ではない．数値計算結果の観察に基づいて，著者は $\alpha = (1, b, c)$ に対する最適な敵対者行列が次の形をした行列であることを確信している．それは，

	001	010	100	101	110	111
001	0	$b - x^2/b$	0	$\sqrt{1-x^2}$	0	0
010	$b - x^2/b$	0	x	0	$\sqrt{1-x^2}$	0
100	0	x	0	$\sqrt{c(c-b)}$	0	0
101	$\sqrt{1-x^2}$	0	$\sqrt{c(c-b)}$	0	b	0
110	0	$\sqrt{1-x^2}$	0	b	0	$\sqrt{c(c-b)}$
111	0	0	0	0	$\sqrt{c(c-b)}$	0

という行列である．ただし，成分が全て 0 であるような行と列は除いており，x はこの行列のスペクトルノルムを最大にする実数である．しかしながら，我々は x の

値を b と c を用いて代数的に表現することに成功していない．本節では，後の議論を容易にし，かつ，よい近似を得るために，x の値を定数 0 と固定して，下界導出を行った．

Høyer ら [13] が導入した量子敵対者限界の改良版 $\mathrm{ADV}^{\pm}$ を用いることも可能であったことを注意しておく．$\mathrm{ADV}^{\pm}$ は ADV よりも常に大きな下界を与えることができる．しかし，より複雑な計算が必要となると予想される．

第4章　シングルトン被覆数による ブール式複雑さの下界

4.1　はじめに

ブール式複雑さの下界を得るための一つのアプローチとして，長方形分割数を求める手法がある．しかし，長方形分割数は整数計画問題で表現されるため，数値的に求めるのは困難であるだけでなく、漸近的な下界を解析的に求めることも難しい. そこで，これまでにその緩和問題が幾つか考えられてきた．近年 Ueno[27] により提案されたランク制約付き緩和問題は，多数決関数と多数決関数を用いたある合成関数に対して，既存の下界よりも大きな下界を導出している．本章では，新たな緩和問題を提案し，8 入力マルチプレクサ関数に対しては，既存の緩和問題による下界よりも大きな下界を与えることができることを示す.

4.2　長方形分割数の数理計画問題による表現

Karchmer ら [16] は長方形分割数を整数計画問題で定式化し，さらにそれを線形緩和した問題を与えた．それらを以下に示す.

命題 4.1 ブール関数 f に対して，f のコミュニケーション行列 M_f の単色長方形全体からなる集合を $\mathfrak{R}_f$ とする．f の長方形分割数 $C^D(f)$ は，次の整数計画問題 IP_f^1 の最適値に一致する．
IP_f^1 :

$$
\begin{array}{ll}
\text{minimize} & \sum_{R\in\mathfrak{R}_f} z_R \\
\text{subject to} & \sum_{R\in\{R'\in\mathfrak{R}_f \mid c\in R'\}} z_R = 1 \quad \text{for each } c \in f^{-1}(0)\times f^{-1}(1) \\
& z_R \in \{0,1\} \quad \text{for each } R \in \mathfrak{R}_f.
\end{array}
$$

上の整数計画問題 IP_f^1 の任意の許容解 z_R に対し，$R \in \mathfrak{R}' \Leftrightarrow z_R = 1$ により定義される集合 $\mathfrak{R}' \subseteq \mathfrak{R}_f$ は M_f を覆う互いに素な単色長方形の集合であり，逆に M_f を

覆う互いに素な単色長方形の任意の集合 $\mathfrak{R}'$ に対し $z_R = 1 \Leftrightarrow R \in \mathfrak{R}'$ で定義される z_R は整数計画問題 IP_f^1 の許容解となっている．このことより，上の命題が成り立つ．

整数計画問題 IP_f^1 の制約条件を緩和することにより，次の線形計画問題 $\mathcal{P}_f^1$ が得られる．

$\mathcal{P}_f^1$:

$$\begin{array}{ll} \text{minimize} & \sum_{R\in\mathfrak{R}_f} z_R \\ \text{subject to} & \sum_{R\in\{R'\in\mathfrak{R}_f \mid c\in R'\}} z_R = 1 \quad \text{for each } c \in f^{-1}(0)\times f^{-1}(1) \\ & z_R \geq 0 \quad \text{for each } R \in \mathfrak{R}_f. \end{array}$$

$\mathcal{P}_f^1$ の最適値を $\mathrm{LP}(f)$ と記す．以下に $\mathcal{P}_f^1$ の双対問題を示す．

$\mathcal{D}_f^1$:

$$\begin{array}{ll} \text{maximize} & \sum_{c\in f^{-1}(0)\times f^{-1}(1)} w_c \\ \text{subject to} & \sum_{c\in R} w_c \leq 1 \quad \text{for each } R \in \mathfrak{R}_f \\ & w_c \in \mathcal{R} \quad \text{for each } c \in f^{-1}(0)\times f^{-1}(1). \end{array}$$

命題 4.2 任意の関数 f に対して，$C^D(f) \geq \mathrm{IP}(f)$.

$\mathrm{LP}(f)$ は $C^D(f)$ の下界を与え，もとの整数計画問題より扱い易いが，以下のような上界が知られている．

定理 4.1 任意の n 変数ブール関数 f に対して，$\mathrm{IP}(f) \leq 4n^2$.

Ueno[27] は上の緩和問題 $\mathcal{P}_f^1$ に制約を追加することで，$\mathrm{LP}(f)$ より大きな下界を与える可能性がある線形計画問題 $\mathcal{P}_f^2$ を定義し，実際に多数決関数などに対し既存の下界よりも大きな下界を得ることに成功している．以下に $\mathcal{P}_f^2$ を示す．

グラフ $G_f = (V, E)$ を次のように定義する．

- $V = \mathfrak{R}_f$.
- $E = \{(R_1, R_2) \in V^2 \mid R_1 \cap R_2 = \emptyset\}$.

V の部分集合によって誘導される G_f の部分グラフからなる集合を $G \in \mathcal{G}_f$ とする．$G \in \mathcal{G}_f$ の最大独立点集合の要素数を $\alpha(G)$ とする．$G \in \mathcal{G}_f$ に対し，$V(G)$ で G の頂点集合を表すとする．$V(G) \subseteq \mathfrak{R}_f$ に注意されたい．任意のブール関数 f に対し，$\mathrm{Ueno}(f)$ を次の線形計画問題の最適値として定義する．

$\mathcal{P}_f^2$:

$$\begin{array}{ll} \text{minimize} & \sum_{R\in\mathfrak{R}} z_R \\ \text{subject to} & \sum_{R\in\{R'\in\mathfrak{R}_f | c\in R'\}} z_R = 1 \quad \text{for each } c \in f^{-1}(0)\times f^{-1}(1) \\ & \sum_{R\in V(G)} z_R \le \alpha(G) \quad \text{for each } G \in \mathcal{G}_f \\ & z_R \ge 0 \quad \text{for each } R \in \mathfrak{R}_f. \end{array}$$

$\mathcal{P}_f^2$ の双対問題は以下のようになる．
$\mathcal{D}_f^2$:

$$\begin{array}{ll} \text{maximize} & \sum_{c\in f^{-1}(0)\times f^{-1}(1)} w_c + \sum_{G\in\mathcal{G}_f} \alpha(G) z_G \\ \text{subject to} & \sum_{c\in R} w_c + \sum_{G\in\{G'\in\mathcal{G}_f | R\in V(G')\}} z_G \le 1 \quad \text{for each } R \in \mathfrak{R}_f \\ & z_G \le 1 \quad \text{for each } G \in \mathcal{G}_f \\ & w_c \in \mathcal{R} \quad \text{for each } c \in f^{-1}(0)\times f^{-1}(1). \end{array}$$

$\mathcal{P}_f^2$ は $\mathcal{P}_f^1$ に制約式を追加したものであることと，$\mathcal{P}_f^2$ は IP_f^1 と等価な以下の整数計画問題 IP_f^2 の線形計画緩和問題とみなせることから，次の命題 4.3 が得られる．
IP_f^2 :

$$\begin{array}{ll} \text{minimize} & \sum_{R\in\mathfrak{R}_f} z_R \\ \text{subject to} & \sum_{R\in\{R'\in\mathfrak{R}_f | c\in R'\}} z_R = 1 \quad \text{for each } c \in f^{-1}(0)\times f^{-1}(1) \\ & \sum_{R\in V(G)} z_R \le \alpha(G) \quad \text{for each } G \in \mathcal{G}_f \\ & z_R \in \{0,1\} \quad \text{for each } R \in \mathfrak{R}_f. \end{array}$$

命題 4.3 任意のブール関数 f に対して，$C^D(f) \ge \mathrm{Ueno}(f) \ge \mathrm{IP}(f)$.

4.3　シングルトン被覆数による緩和整数計画問題

本章では，長方形分割数を定義している整数計画問題 IP_f^1 に対する新たな緩和問題 IP_f^3 を与え，8 入力マルチプレクサ関数に対しては，Ueno よりも大きな下界を与えることを示す．まず，IP_f^3 の定義に必要な，シングルトンというセルと，セパレータという長方形集合を定義する．

定義 4.1 (シングルトン) ブール関数 f に対し，$(x,y) \in f^{-1}(0)\times f^{-1}(1)$ がシングルトンであるとは，$|M_f[x,y]| = 1$ であるときを言う．

定義 4.2 (セパレータ) コミュニケーション行列 M_f の長方形の集合 $\mathfrak{M}$ が M_f のセパレータであるとは，$\mathfrak{M}$ が次の三つの条件を満たすことである．

1. 任意の長方形 $M_1, M_2 \in \mathfrak{M}$ に対し，$M_1 \neq M_2$ ならば $M_1 \cap M_2 = \emptyset$.
2. 各 $M \in \mathfrak{M}$ は少なくとも一つのシングルトンを含む．
3. $M \in \mathfrak{M}$ が含むシングルトンの集合を S_M とする．このとき，

$$\mathrm{Color}(M) = \bigcup_{(x,y)\in S_M} M_f[x,y]$$

と定義すると，任意の $M_1, M_2 \in \mathfrak{M}$ に対し，$M_1 \neq M_2$ ならば，$\mathrm{Color}(M_1) \cap \mathrm{Color}(M_2) = \emptyset$.

M_f の任意の長方形 M に対して，次のような整数計画問題 IP^3_M を定義する．S_M を M に含まれる M_f の単色長方形の集合とし，$\mathfrak{R}_M$ を M に含まれる M_f の単色長方形の集合とする．すなわち，$S_M = \{(x,y) \mid |M_f[x,y]| = 1\}$，$\mathcal{R}_M = \{R \in \mathfrak{R}_f \mid R \subseteq M$ とする．

IP^3_M :

$$\begin{array}{ll} \text{minimize} & \sum_{r\in \mathrm{R}_i} z_r \\ \text{subject to} & \sum_{r\ni c} z_r = 1 \quad \text{for each } c \in S_i \\ & \sum_{r\ni c} z_r \leq 1 \quad \text{for each } c \in r_i, c \notin S_i \\ & z_r \in \{0,1\} \quad \text{for each } r \in \mathrm{R}_i. \end{array}$$

IP^3_M の最適値を台 M における f のシングルトン被覆数と呼び，$\mathrm{SC}(f,M)$ と記す．特に $M = M_f$ のとき，単にシングルトン被覆数と呼び $\mathrm{SC}(f)$ と記す．明らかに $C^D(f) \geq \mathrm{SC}(f)$ である．よって，$\mathrm{SC}(f)$ は $L(f)$ の下界を与える．任意の台 M に対し，$\mathrm{SC}(M,f) \leq \mathrm{SC}(f)$ である．

定理 4.2 任意のブール関数 f，M_f の任意のセパレータ $\mathfrak{M}$ に対して，$L(f) \geq C^D(f) \geq \sum_{M\in\mathfrak{M}} \mathrm{SC}(f,M)$ が成立する．

証明: f を任意のブール関数とする．f のコミュニケーション行列 M_f に対して，$\mathfrak{R}_f$ を単色長方形の集合とし，$\mathfrak{M}$ を任意のセパレータとする．$z'_R \in \{0,1\}$ $(R \in \mathfrak{R}_f)$ を IP^1_f の任意の許容解とする．$\mathfrak{M}$ に含まれる各長方形 M に対し，M の単色長方形の集合を $\mathfrak{R}_M$ と記すこととする．任意の $M \in \mathfrak{M}$ と任意の $R \in \mathfrak{R}_M$ に対し，

$$z_R = \begin{cases} \bigvee\limits_{\substack{R'\in\mathfrak{R}_f \\ R=R'\cap M}} z'_{R'} & R \text{ がシングルトンを含む場合} \\ 0 & R \text{ がシングルトンを含まない場合} \end{cases}$$

表 4.1: 2-MUX のコミュニケーション行列

	001	011	110	111
000	{1}	{1,2}	{2,3}	{1,2,3}
010	{1,2}	{1}	{3}	{1,3}
100	{1,3}	{1,2,3}	{2}	{1,2}
101	{3}	{2,3}	{1,2}	{2}

とおくと，z_R $(R \in \mathfrak{R}_M)$ は IP^3_M の許容解となる．また，$z_R = 1$ のとき，$z'_{R'} = 1$ $(R = R' \cap M)$ を満たす $R' \in \mathfrak{R}_f$ がただ一つ存在する．これは次に述べる理由による．M_f のある素な単色長方形 R_1, R_2 に対して，$z_{R_1} = z_{R_2} = 1$ であると仮定する．まず，$R_1, R_2 \in \mathfrak{R}_M$ の場合を考えると，$R_1 \neq R_2$ のとき，z_R の定義から明らかに z_{R_1} と z_{R_2} を 1 とする原因となった $R'_1 \in \mathfrak{R}_f$ と $R'_2 \in \mathfrak{R}_f$ は異なる．次に，$R_1 \in \mathfrak{R}_{M_1}$ $R_2 \in \mathfrak{R}_{M_2} (M_1 \neq M_2,\ M_1 \in \mathfrak{M},\ M_2 \in \mathfrak{M})$ の場合を考えると，セパレータの定義により，M_1 に含まれるシングルトンと M_2 に含まれるシングルトンを同時に覆う単色長方形は存在しないため，z_{R_1} と z_{R_2} を 1 とする原因となった $R'_1 \in \mathfrak{R}_f$ と $R'_2 \in \mathfrak{R}_f$ は異なる．よって，以下の式が成り立つ．

$$\sum_{M \in \mathfrak{M}} \sum_{R \in \mathfrak{R}_M} z_R \leq \sum_{R' \in \mathfrak{R}_f} z'_{R'}.$$

□

以降の小節では，マルチプレクサ関数に対するセパレータ $\mathfrak{M}$ を考える．ある自然数 k に対する k 入力マルチプレクサ関数 k-MUX とは以下のような $k + \log(k)$ 変数ブール関数である．ビット列 x に対して，$(x)_2$ を x を二進数として解釈した値とする．例えば，$(011)_2 = 3$ である．

$$k\text{-MUX}(x_1 x_2 \cdots x_{\log(k)} y_1 y_2 \cdots y_k) = \begin{cases} 1 & \text{if } y_{(x_1 \cdots x_j)_2 + 1} = 1 \\ 0 & \text{otherwise.} \end{cases}$$

4.3.1　2 入力マルチプレクサ関数に対するブール式複雑さ

2-MUX のコミュニケーション行列は表 4.1 のようになる．2-MUX においては，SC，LP，Ueno のどれを用いてもブール式複雑さのタイトな下界を得ることがで

きる．以下では，$\mathcal{N}_i'$ を用いて 2-MUX のブール式複雑さを導くとともに，2-MUX に対する $\mathcal{P}_1$ と $\mathcal{P}_2$ の最適解についても示す．

定理 4.3 $L(\text{2-MUX}) = 4$.

証明: サイズが 4 のブール式 $(\bar{x}_1 \wedge y_1) \vee (x_1 \wedge y_2)$ は 2-MUX を表すため，$L(\text{2-MUX}) \leq 4$.

$\mathfrak{M}$ を次の M_1, M_2, M_3 からなる長方形の集合とする．$M_1 = \{\{000\} \times \{001\}\}$，$M_2 = \{\{100\} \times \{110\}\}$，$M_3 = \{\{010, 101\} \times \{001, 110\}\}$ とする．M_1, M_2, M_3 が互いに素であり，$\text{Color}(M_1) = 1$，$\text{Color}(M_2) = 2$，$\text{Color}(M_3) = 3$ であるため，$\mathfrak{M}$ はセパレータである．明らかに $\text{SC}(f, M_1) = \text{SC}(f, M_2) = 1$ である．$\text{IP}^3_{M_3}$ については，二つのシングルトンを含む単色長方形が表 4.2 のように存在しないため，$\text{SC}(f, M_3) = 2$ となる．よって，定理 4.2 より，$L(\text{2-MUX}) \geq 4$.

表 4.2: 2-MUX に対する r_3 のコミュニケーション行列

	001	110
010	{1,2}	{3}
101	{3}	{1,2}

□

定理 4.4 $\text{LP}(\text{2-MUX}) = \text{Ueno}(\text{2-MUX}) = 4$

証明: $C = \{(000, 001), (100, 110), (010, 110), (101, 001)\}$ とする．w_c を次のように定義する．

$$w_c = \begin{cases} 1 & \text{if } c \in C \\ 0 & \text{otherwise} \end{cases}$$

この w_c が線形計画問題 $\mathcal{D}^1_{\text{2-MUX}}$ の許容解であり，目的関数の値を 4 にすることは容易に確かめられる．定理 4.3 より，これは最適解である．よって，$\text{LP}(\text{2-MUX}) = \text{Ueno}(\text{2-MUX}) = 4$.

□

表 4.3: M_5 で誘導された $M_{4\text{-MUX}}$ の部分コミュニケーション行列．色つきの長方形は $\mathrm{IP}^3_{M_5}$ に対する最適解の一つを表す．

	001001	010110	100110	111001
000110	{1,2,3,4}	{5}	{6}	{5,6}
011001	{5}	{1,2,3,4}	{5,6}	{6}
101001	{6}	{5,6}	{1,2,3,4}	{5}
110110	{5,6}	{6}	{5}	{1,2,3,4}

4.3.2　4 入力マルチプレクサ関数に対するブール式複雑さ

$M_1 = \{000000 \times 000001\}$，$M_2 = \{010000 \times 010010\}$，$M_3 = \{100000 \times 100100\}$，$M_4 = \{110000 \times 111000\}$，$M_5 = \{\{000110, 011001, 101001, 110110\} \times \{001001, 010110, 100110, 111001\}\}$ とおく．$M_1, M_2, \ldots, M_5$ が互いに素であることと，$\mathrm{Color}(M_1) = \{1\}$，$\mathrm{Color}(M_2) = \{2\}$，$\mathrm{Color}(M_3) = \{3\}$，$\mathrm{Color}(M_4) = \{4\}$，$\mathrm{Color}(M_5) = \{5, 6\}$ であることとは容易に確かめられる．よって，$\mathfrak{M} = \{M_1, M_2, \ldots, M_5\}$ は $M_{4\text{-MUX}}$ に対するセパレータである．

定理 4.5 $\mathfrak{M}$ を上で定義した 4-MUX のコミュニケーション行列 $M_{4\text{-MUX}}$ のセパレータとすると，

$$\mathrm{SC}(f, \mathfrak{M}) = \sum_{M \in \mathfrak{M}} \mathrm{SC}(f, M) = 10.$$

証明: 明らかに，任意の $i \in \{1, 2, 3, 4\}$ に対して，$\mathrm{SC}(\text{2-MUX}, M_i) = 1$ である．$\mathrm{SC}(\text{2-MUX}, M_5)$ については，計算機による数値計算によって，$\mathrm{SC}(\text{2-MUX}, M_5) = 6$ という結果を得ることができる．その最適解の一つを表 4.3 に示す．

□

この定理は $L(\text{4-MUX}) \geq 10$ を意味する．一方，サイズが 10 のブール式 $\bar{x}_1(\bar{x}_2 y_1 \vee x_2 y_2) \vee x_1(\bar{x}_2 y_3 \vee x_2 y_4)$ が 4-MUX を表すことから，$L(\text{4-MUX}) \leq 10$ を得る．次の定理は以上の結果をまとめたものである．

定理 4.6 $L(\text{4-MUX}) = 10.$

4-MUX に対しても，LP と Ueno はタイトな下界を与える．

定理 4.7 LP(4-MUX) = Ueno(4-MUX) = 10.

証明: LP(4-MUX) ≥ 10 を示せばよい．$C_1 = \{(000000, 000001), (010000, 010010), (100000, 100100), (110000, 111000), (000110, 010110), (000110, 100110), (011001, 001001), (011001, 111001), (101001, 001001), (101001, 111001), (110110, 010110), (110110, 100110)\}$, $C_2 = \{(000110, 111001), (011001, 100110), (101001, 010110), (110110, 001001)\}$ とする．$C_1 = M_1 \cup M_2 \cup M_3 \cup M_4 \cup S_{M_5}$ となっており，$C_2 \subseteq M_5$ であり，任意の $(x, y) \in C_2$ に対して，$M_{\text{4-MUX}}[x, y] = \{5, 6\}$ となっている．表 4.3 を参照されたい．w_c を次のように定義する．

$$w_c = \begin{cases} 1 & \text{if } c \in C_1 \\ -0.5 & \text{if } c \in C_2 \\ 0 & \text{otherwise} \end{cases}$$

考慮すべき単色長方形は，$M_1, M_2, M_3, M_4, S_{M_5}$ の各シングルトン 8 つと，$\{\{101001, 110110\} \times \{001001, 010110\}\}$，$\{\{000110, 011001\} \times \{100110, 111001\}\}$，$\{\{000110, 101001\} \times \{010110, 111001\}\}$，$\{\{011001, 110110\} \times \{001001, 100110\}\}$ の 4 つのみである．これらの各単色長方形 R において，$\sum_{c \in R} w_c = 1$ となることは容易に確かめられる．さらに，この w_c によって与えられる目的関数の値は 10 である．よって，LP(4-MUX) ≥ 10.

□

4.3.3　8 入力マルチプレクサ関数に対するブール式複雑さの下界

$P = 10010110$，$\bar{P} = 01101001$ とし，ビット列と P もしくは $\bar{P}$ を繋げて表記したものは，それらの連接を表すものとする．例えば，$001P = 00110010110$ である．

$M_1 = \{00000000000\} \times \{00000000001\}$, $M_2 = \{00100000000\} \times \{00100000010\}$, $M_3 = \{01000000000\} \times \{01000000100\}$, $M_4 = \{01100000000\} \times \{01100001000\}$, $M_5 = \{10000000000\} \times \{10000010000\}$, $M_6 = \{10100000000\} \times \{10100100000\}$, $M_7 = \{11000000000\} \times \{11001000000\}$, $M_8 = \{11100000000\} \times \{11110000000\}$, $M_9 = \{000P, 001\bar{P}, 010\bar{P}, 011P, 100\bar{P}, 101P, 110P, 111\bar{P}\} \times \{000\bar{P}, 001P, 010P, 011\bar{P}, 100P, 101\bar{P}, 110\bar{P}, 111P\}$ とおく．$M_1, M_2, \ldots, M_9$ が互いに素であること

と，$1 \leq i \leq 8$ に対して $\mathrm{Color}(M_i) = \{i\}$ であること，$\mathrm{Color}(M_9) = \{9, 10, 11\}$ であることは容易に確かめられる．よって，$\mathfrak{M} = \{M_1, M_2, \ldots, M_9\}$ はセパレータである．計算機で $\mathrm{IP}^3_{M_9}$ を解くことにより，以下の二つの定理を得た．

定理 4.8 $\mathfrak{M}$ を上で定義した $M_{8\text{-MUX}}$ のセパレータとすると，

$$\mathrm{SC}(8\text{-MUX}) = \sum_{M \in \mathfrak{M}} \mathrm{SC}(8\text{-MUX}, M) = 20.$$

$M_1, M_2, \ldots, M_8$ は全てシングルトンである．よって，$1 \leq i \leq 8$ に対して $\mathrm{SC}(8\text{-MUX}, M_i) = 1$ であることは明らかである．計算機を用いて $\mathrm{IP}^3_{M_9}$ を解いた結果，$\mathrm{SC}(8\text{-MUX}, M_9) = 12$ という結果を得たことから，上記の定理が得られた．表 4.4 に M_9 によって誘導される $M_{8\text{-MUX}}$ の部分コミュニケーション行列を示す．計算機によって求めた $\mathrm{IP}^3_{M_9}$ の最適解を以下に記す．M_9 に含まれる単色長方形の集合を $\mathfrak{R}_{M_9}$ とする．$R \in \mathfrak{R}_{M_9}$ に対し，

$$x_R = \begin{cases} 1 & R \in \mathfrak{R} \text{ のとき} \\ 0 & R \notin \mathfrak{R} \text{ のとき} \end{cases}$$

ここで，$\mathfrak{R} = \{\{000P, 011P\} \times \{100P, 111P\},\ \{001\bar{P}, 010\bar{P}\} \times \{101\bar{P}, 110\bar{P}\},\ \{100\bar{P}, 111\bar{P}\} \times \{000\bar{P}, 011\bar{P}\},\ \{101P, 110P\} \times \{001P, 010P\},\ \{000P, 001\bar{P}\} \times \{010P, 011\bar{P}\},\ \{100\bar{P}, 101P\} \times \{110\bar{P}, 111P\},\ \{010\bar{P}, 011P\} \times \{000\bar{P}, 001P\},\ \{110P, 111\bar{P}\} \times \{100P, 101\bar{P}\},\ \{000P, 100\bar{P}\} \times \{001P, 101\bar{P}\},\ \{010\bar{P}, 110P\} \times \{011\bar{P}, 111P\},\ \{001\bar{P}, 101P\} \times \{000\bar{P}, 100P\},\ \{011P, 111\bar{P}\} \times \{010P, 110\bar{P}\}\}$ である．

一方 LP や Ueno は 8-MUX に対して SC よりも真に小さい下界しか得られない．

定理 4.9 8-MUX に対するコミュニケーション行列を M とする．このとき，

$$\mathrm{Ueno}(8\text{-MUX}) \leq 18 + 2/3.$$

4.4　まとめと今後の課題

ブール式複雑さの下界を表す指標である長方形分割数は，整数計画問題 IP^1_f の最適値として表現される．本章では IP^1_f を緩和した整数計画問題 IP^3_f を与え，その最適値 $\mathrm{SC}(f)$ が長方形分割数の下界を与えることを示した．IP^3_f は次のような

緩和によって得られる数理計画問題であるすなわち，セパレータという概念を導入して問題を小さな部分問題へと分割すると共に，IP_f^1 においては”全てのセル”を被覆する単色長方形の集合であった許容解の範囲を，IP_f^3 においては”シングルトン”を被覆する単色長方形の集合に制限するという緩和である．このようにすることで，問題を幾つかの部分問題に分けて解くことができ，関数によっては長方形分割数を求める場合に比べて，非常に高速に解くことが可能である．

最適値がブール式複雑さの下界を与える三つの数理計画問題 (1)IP_f^3，(2)IP_f^1 に対する線形緩和問題 LP_f^1，(3)LP_f^1 に対して制限を加えた LP_f^2，を k-MUX 関数 ($k \in \{2, 4, 8\}$) に対して解いた結果，2-MUX と 4-MUX ではどの数理計画問題の最適値も自明な上界と一致する下界を与えるが，8-MUX ではどの数理計画問題の最適値も自明な上界とは一致せず，IP_f^3 の最適値が LP_f^1 と IP_f^2 の最適値よりも大きいことを示した．著者は一般の k-MUX の場合においても，上記の数理計画問題の中では IP_f^3 の最適値が最も大きな下界を与えるのではないかと予想している．

今後の課題としては，一般の k に対する $SC(k\text{-MUX})$ を k を用いた式で解析的に評価することと，SC がタイトな下界を与える他の関数を発見すること，が挙げられる．

表 4.4: M_9 で誘導された $M_{8\text{-MUX}}$ のコミュニケーション行列，ここで $\mathrm{B} = \{1,2,3,4,5,6,7,8\}$ とする．

	$000\bar{P}$	$001P$	$010P$	$011\bar{P}$	$100P$	$101\bar{P}$	$110\bar{P}$	$111P$
$000P$	B	$\{9\}$	$\{10\}$	$\{9,10\}\cup\mathrm{B}$	$\{11\}$	$\{9,11\}\cup\mathrm{B}$	$\{10,11\}\cup\mathrm{B}$	$\{9,10,11\}$
$001\bar{P}$	$\{9\}$	B	$\{9,10\}\cup\mathrm{B}$	$\{10\}$	$\{9,11\}\cup\mathrm{B}$	$\{11\}$	$\{9,10,11\}$	$\{10,11\}\cup\mathrm{B}$
$010\bar{P}$	$\{10\}$	$\{9,10\}\cup\mathrm{B}$	B	$\{9\}$	$\{10,11\}\cup\mathrm{B}$	$\{9,10,11\}$	$\{11\}$	$\{9,11\}\cup\mathrm{B}$
$011P$	$\{9,10\}\cup\mathrm{B}$	$\{10\}$	$\{9\}$	B	$\{9,10,11\}$	$\{10,11\}\cup\mathrm{B}$	$\{9,11\}\cup\mathrm{B}$	$\{11\}$
$100\bar{P}$	$\{11\}$	$\{9,11\}\cup\mathrm{B}$	$\{10,11\}\cup\mathrm{B}$	$\{9,10,11\}$	B	$\{9\}$	$\{10\}$	$\{9,10\}\cup\mathrm{B}$
$101P$	$\{9,11\}\cup\mathrm{B}$	$\{11\}$	$\{9,10,11\}$	$\{10,11\}\cup\mathrm{B}$	$\{9\}$	B	$\{9,10\}\cup\mathrm{B}$	$\{10\}$
$110P$	$\{10,11\}\cup\mathrm{B}$	$\{9,10,11\}$	$\{11\}$	$\{9,11\}\cup\mathrm{B}$	$\{10\}$	$\{9,10\}\cup\mathrm{B}$	B	$\{9\}$
$111\bar{P}$	$\{9,10,11\}$	$\{10,11\}\cup\mathrm{B}$	$\{9,11\}\cup\mathrm{B}$	$\{11\}$	$\{9,10\}\cup\mathrm{B}$	$\{10\}$	$\{9\}$	B

第5章　最簡なブール式のクラスとそのNPN代表元

5.1　はじめに

計算複雑さの理論における目標の一つは，様々なブール関数に対してブール式複雑さの精密な限界を与えることである．第 2 章で定義したとおり，ブール関数 f のブール式複雑さとは f を表す最小の標準基底 $\{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}\}$ 上のブール式のサイズである．そのような最小な式は f に対する最簡な式と呼ばれる．この目標に対する通常の，しかし意義の大きいアプローチは，特定の “難しい” 問題に対してできるだけ大きな下界を与えようというものである．例えば，NP に含まれるある関数に対してブール式複雑さの超多項式下界を示すことができれば，長年に渡る未解決問題である $\mathrm{NC}^1 \neq \mathrm{NP}$ を証明したことになる．しかしながら，ブール式複雑さに対する大きい下界を導出するための手法が整備されておらず，明示的に定義された特定のブール関数に対して現在知られている最大の下界は $\Omega(n^{3-o(1)})$ にすぎない．

本章で取る別のアプローチは，最簡な式のみからなるある大きなクラス C を明示的に構成する，一般的な手法を与えることである．そのようなクラス C を構成する意義は以下の 4 つである．

1. C に含まれるブール式 F のサイズが F の表す関数のブール式複雑さを正確に与える．

2. 応用分野において，最簡な式は記憶容量を節約するために役立つ．

3. 最簡な式が持つ構造や性質について洞察を得る可能性がある．

4. 回路計算量や決定木複雑さのような他の複雑さの指標とブール式複雑さとの間の関係についての研究材料が，C に含まれるブール式から得られる可能性がある．

上記の 3 番目と 4 番目の意義に対しては，C に含まれるブール式を生成し観察する必要があり，その際には計算機が用いることが考えられる．しかしながら，同じ NPN 同値類に属するブール式は本質的に同じ構造を持つので，それらを全て生成することは明らかに時間の浪費である．(ここで，二つのブール関数が NPN 同値であるとは，入力変数の入れ替え，入力変数の否定，出力の否定を適当に取ることにより，片方の関数からもう片方の関数へ変形できるときをいう.）実際，論理回路や決定木や BDD といった自然な表現モデルにおいては，同じ NPN 同値類に属するブール関数は本質的に同じ最簡な表現形を持ち，同じ複雑さを持つ．よって，NPN 同値類の代表元のみからなる部分クラス C を構成することは意義のある目標である．

本章では，ある基底上の一回読みブール式で表現される関数に着目する．一回読みブール式とは，各変数が高々一回しか現れないブール式のことである．本研究の出発点は n 変数パリティ関数 PARITY_n に対する最簡なブール式に関する Khrapchenko の結果である．Khrapchenko[19] は，ある整数 k に対して $n = 2^k$ が成り立つとき，PARITY_n に対する最簡なブール式を構成し，そのサイズがちょうど n^2 になることを示した．実際，$n = 2^k$ のとき PARITY_n は $\mathrm{PARITY}_n = \mathrm{XOR} \circ (\mathrm{PARITY}_{n/2}, \mathrm{PARITY}_{n/2})$ という再帰式で表される．複雑さが 4 の $\mathrm{XOR}(x_1, x_2)$ に対するサイズが 4 の最簡なブール式 $(\bar{x}_1 \wedge x_2) \vee (x_1 \wedge \bar{x}_2)$ を用いてこの再帰式を展開することにより，PARITY_n に対するサイズが $4^k = n^2$ の標準基底ブール式が得られる．ここで $\circ$ は定義 2.13 で定義したように，関数の合成を表す．一方，再帰式 $\mathrm{PARITY}_n = \mathrm{XOR} \circ (\mathrm{PARITY}_{n/2}, \mathrm{PARITY}_{n/2})$ をそのまま展開することにより，基底 {XOR} 上の一回読みブール式が得られる．よって，Khrapchenko の結果は基底 {XOR} 上の一回読みブール式 F に対し，F に現れる各基底演算をその最簡形ブール式で置き換えることにより，標準基底上の最簡なブール式が得られることを示している．一般に一回読みブール式に対するこの性質は次のように記述できる．$\mathfrak{B}$ を任意のブール関数の集合とする．一回読み $\mathfrak{B}$ 式 F が最簡化可能であるとは，F に現れる各演算子をその最簡な式で置き換えることにより，F を最簡な式に変換できるときをいう．さらに，基底 $\mathfrak{B}$ 上の一回読み $\mathfrak{B}$ 式のクラス C が最簡化可能であるとは，C に含まれる各 F が最簡化可能であるときを言うこととする．このとき，一回読み式のどのようなクラスが最簡化可能であろうか，という自然な問いが生じる．

ブール関数の集合 $\mathfrak{B}$ に対して，一回読み $\mathfrak{B}$ 式を $\mathrm{ROF}(\mathfrak{B})$ と記す．本論文では，$\mathrm{ADV}^2(f) = L(f)$ を満たすブール関数 f からなる任意の基底 $\mathfrak{B}$ を考え，$\mathrm{ROF}(\mathfrak{B})$ の

ある部分クラス $C_{\mathfrak{B}}$ が最簡化可能であることを示す．$\mathfrak{B}^* = \{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}, \mathrm{XOR}, \mathrm{MUX}\}$ はそのような基底の一つである．本章で定義するクラス $C_{\mathfrak{B}^*}$ は 2^k 変数パリティ関数を含むので，本章で示す結果は Khrapchenko の結果を拡張した結果である．

次に，ROF($\mathfrak{B}^*$) における NPN 同値類を考える．本章では，以下の二つの性質を持つ ROF($\mathfrak{B}^*$) に対する標準形ブール式を定義する．

1. ROF($\mathfrak{B}^*$) に属する任意のブール式 F は F と NPN 同値な標準形ブール式に効率良く変形できる．

2. 異なる標準形ブール式は NPN 同値ではない．

よって，標準形が ROF($\mathfrak{B}^*$) の NPN 同値類の代表元とできる．$C_{\mathfrak{B}^*}$ は ROF($\mathfrak{B}^*$) の部分集合であるので，上記の標準形ブール式を示せば，それは $C_{\mathfrak{B}^*}$ に対する標準形でもあることに注意されたい．

本章の構成は以下の通りである．まず，第 5.2 節では形式的複雑さ指標 M を定義し，M とブール式複雑さが一致する関数に対して，最簡な式を生成するアルゴリズムを示す．このアルゴリズムはブール関数に対する M の値を求める計算時間に依存する上に，本質的に同じ構造を持つ式，すなわち，NPN 同値である式を生成してしまう．第 5.3 節以降では，それとは異なり，ブール関数に対する複雑さ指標の計算時間に依存せず，最簡な式の NPN 同値類の代表元のみを高速に生成するアルゴリズムを示す．第 5.3 節では，量子敵対者限界を用いることで，ROF($\mathfrak{B}^*$) の部分クラスである最簡化可能なブール式のクラス $C_{\mathfrak{B}^*}$ を与える．第 5.4 節では，NPN 同値についての定義を与えると共に，NPN 同値に関する性質をいくつか述べる．第 5.5 節では，一回読み $\mathfrak{B}^*$ 式に対する標準形を定義し，任意の一回読み $\mathfrak{B}^*$ 式は標準形に変形できることと，異なる標準形の表す関数は NPN 同値ではないことを示す．よって，異なる標準形を全て生成できれば容易に最簡なブール式を得ることができる．第 5.6 節では，本章のまとめを行う．

5.2　ブール式の複雑さ指標を用いた最簡な式の生成アルゴリズム

本節では，任意の形式的複雑さ指標 M に対し，$L(f) = M(f)$ を満たす任意の関数 f を表す最簡な式全体からなるクラスを生成するアルゴリズムを示す．形式的

複雑さ指標は，以下のように定義される．

定義 5.1 $\mathcal{R}$ を実数全てからなる集合とする．M をブール関数から実数への関数とする．M が以下の三つの条件を全て満たすとき，M を形式的複雑さ指標と言う．

1. 任意の自然数 i に対して，$M(\mathrm{PROJ}_i) = 1$.
2. 任意のブール関数 f に対して，$M(f) = M(\bar{f})$.
3. 任意のブール関数 f, g に対して，$M(f \vee g) \leq M(f) + M(g)$.

ADV^2 や長方形分割数，LP は形式的複雑さ指標である．任意の形式的複雑さ指標は，ブール式複雑さの下界を与える．

定理 5.1 ([29]) 任意の形式的複雑さ指標 M と任意のブール関数 f に対して，

$$L(f) \geq M(f).$$

定義 5.2 形式的複雑さ指標 M とブール関数 f に対し，$M(f) = L(f)$ が成立するとき，関数 f は M タイトであるという．

定義 5.2 に従えば，$\mathrm{ADV}^2(f) = L(f)$ を満たす任意のブール関数 f を ADV^2 タイトと呼ぶべきであるが，簡便さのために，定義 2.10 で定義したように f を ADV タイトと呼ぶことに注意されたい．

本章では，ブール式 F と F が表すブール関数 f を同一視し，$L(F)$，$M(F)$，$\mathrm{ADV}(F)$ などと記すことがある．これらはそれぞれ $L(f)$，$M(f)$，$\mathrm{ADV}(f)$ を意味する．同様に，ブール式が M タイトであるとは，f が M タイトであることであり，その条件を $L(F) = L(M)$ と書くこともある．

F を $\{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}\}$ 上のブール式とする．一般性を欠くことなく，F には否定リテラルを除いて $\neg$ が現れないと仮定する．F に現れる全ての AND を OR に，OR を AND に，x_i を $\bar{x}_i$ に，$\bar{x}_i$ を x_i に置き変えることによって得られるブール式を $\bar{F}$ と記す．ド・モルガンの法則により，$\bar{F}$ の表す関数は F の表す関数の否定関数である．また，$F^0 = F$，$F^1 = \bar{F}$ とする．

任意の形式的複雑さ指標 M に対して，n 変数ブール式のクラス $G_{n,M}$ を次のように定義する．

定義 5.3 形式的複雑さ指標 M に対して，$G_{n,M}$ を次の手続きによって得られるブール式のクラスとする．

- $G_{n,M} = \{x_1, \bar{x}_1, \ldots, x_n, \bar{x}_n\}$
- $G_{n,M}$ に含まれる全ての式の対 (F_1, F_2)，および全ての $\epsilon_1, \epsilon_2 \in \{0, 1\}$ に対して，
  - $M(F_1^{\epsilon_1} \vee F_2^{\epsilon_2}) = M(F_1) + M(F_2)$ ならば，$G_{n,M}$ に $F_1^{\epsilon_1} \vee F_2^{\epsilon_2}$ を含める．
  - $M(F_1^{\epsilon_1} \wedge F_2^{\epsilon_2}) = M(F_1) + M(F_2)$ ならば，$G_{n,M}$ に $F_1^{\epsilon_1} \wedge F_2^{\epsilon_2}$ を含める．
- 上の操作を $G_{n,M}$ が大きくならなくなるまで繰り返す．

以下の定理に示すように，$G_{n,M}$ は M タイトで最簡な n 変数ブール式全体からなる集合となっている．

定理 5.2 B_n を n 変数ブール式全てからなる集合とする．このとき，

$$G_{n,m} = \{F \in B_n \mid M(F) = L(F) = \mathrm{size}(F)\}.$$

定義 5.3 で示した $G_{n,M}$ を生成するアルゴリズムの計算時間は，指標 M の計算量が支配的である．ADV や長方形分割数などの有用な形式的複雑さ指標は一般に計算量が大きく，$n \geq 6$ のとき上のアルゴリズムを用いて $G_{n,M}$ を生成することは事実上不可能である．

定理 5.2 の証明のために，以下の補題を示す．

補題 5.3 M を形式的複雑さ指標とし，h を M タイトなブール関数とする．h を表す最簡なブール式が $F \wedge G$ または $F \vee G$ であるとき，F と G も M タイトである．

証明: 式 F と G の表す関数をそれぞれ f と g とする．h が M タイトであることと，$F \wedge G$ または $F \vee G$ が h を表す最簡なブール式であることより，

$$M(h) = L(h) = L(f) + L(g). \tag{5.1}$$

定理 5.1 より，

$$M(f) \leq L(f),\ M(g) \leq L(g). \tag{5.2}$$

M が形式的複雑さ指標であることより，

$$M(h) \leq M(f) + M(g). \tag{5.3}$$

式 (5.1)，(5.2)，(5.3) より，

$$M(f) = L(f),\ M(g) = L(g).$$

□

定理 5.2 の証明:
まず，$G_{n,M}$ に含まれる任意のブール式 F が最簡であり M タイトであることを，F の構文的深さに関する帰納法で示す.
(基底段階)F の深さが 0 のとき，F は単一のリテラルのみからなるブール式である．これは明らかに最簡である．単一のリテラル x_i と $\bar{x}_i$ の表す関数はそれぞれ PROJ_i と $\overline{\mathrm{PROJ}_i}$ であり，形式的複雑さ指標の定義より M タイトである.
(帰納段階) F の構文的深さ d を $d \geq 1$ とし，$F = F_1 \vee F_2$ と仮定する．$F = F_1 \wedge F_2$ の場合も同様に証明できる．$G_{n,M}$ の定義より,

$$M(F_1 \vee F_2) = M(F_1) + M(F_2). \tag{5.4}$$

F_1 と F_2 は深さが $d-1$ 以下であるため，帰納法の仮定より,

$$\mathrm{L}(F_1) = M(F_1),\ \mathrm{L}(F_2) = M(F_2), \tag{5.5}$$

$$\mathrm{L}(F_1) = \mathrm{size}(F_1),\ \mathrm{L}(F_2) = \mathrm{size}(F_2). \tag{5.6}$$

L の定義，および，式 (5.4) と (5.5) より,

$$\begin{aligned} \mathrm{L}(F_1 \vee F_2) &\leq \mathrm{L}(F_1) + \mathrm{L}(F_2) \\ &= \mathrm{M}(F_1) + \mathrm{M}(F_2) \\ &= \mathrm{M}(F_1 \vee F_2). \end{aligned}$$

一方，定理 5.1 より $\mathrm{M}(f_1 \vee f_2) \leq \mathrm{L}(f_1 \vee f_2)$ であるので,

$$M(F_1 \vee F_2) = \mathrm{L}(F_1 \vee F_2) \tag{5.7}$$

および

$$L(F_1 \vee F_2) = L(F_1) + L(F_2) \tag{5.8}$$

が得られる．(5.5) より，F は M タイトである．さらに，式 (5.6) と (5.8) を用いると,

$$L(F_1 \vee F_2) = \mathrm{size}(F_1) + \mathrm{size}(F_2) = \mathrm{size}(F)$$

が得られる．よって，F は最簡である.

次に，任意の M タイトで最簡な n 変数ブール式 F が $G_{n,M}$ の中に存在することを F の構文的深さに関する帰納法で示す.

（基底段階）F の深さが 0 のとき，F は単一のリテラルのみからなるブール式である．定義 5.3 より $G_{n,M}$ は F を含む．

（帰納段階）F の構文的深さ d を $d \geq 1$ とし，$F = F_1 \vee F_2$ と仮定する．$F = F_1 \wedge F_2$ の場合も同様に証明できる．F が M タイトであるから，補題 5.3 より，F_1 と F_2 も M タイトである．帰納法の仮定より，F_1 と F_2 は $G_{n,M}$ に含まれる．よって，定義 5.3 により F は $G_{n,M}$ に含まれる．

□

5.3　最簡化可能な式

$\mathfrak{B}$ をブール関数の集合とする．一回読み $\mathfrak{B}$ 式全てからなる集合を $\mathrm{ROF}(\mathfrak{B})$ と表記することにする．一回読み $\mathfrak{B}$ 式 F に対して，F の展開式とは，F に現れる各演算子 h を h の最簡式で置き換えることによって得られる，標準基底 $\{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}\}$ 上のブール式とする．

定義 5.4 一回読み $\mathfrak{B}$ 式 F が最簡化可能であるとは，F の展開式が最簡であるときを言う．さらに，一回読み $\mathfrak{B}$ 式のクラス C が最簡化可能であるとは，C に含まれる各式が最簡化可能であるときを言う．

例えば $F = (x_1 \wedge x_2) \oplus (x_3 \vee x_4)$ は基底 $\mathfrak{B} = \{\mathrm{AND}, \mathrm{OR}, \mathrm{XOR}\}$ 上の一回読み $\mathfrak{B}$ 式であるが，その展開式

$$(\overline{x_1 \wedge x_2} \wedge (x_3 \vee x_4)) \vee ((x_1 \wedge x_2) \wedge \overline{x_3 \vee x_4})$$

が最簡であるので，F は最簡化可能である．

以上の定義を基に，本章で考える最簡化可能な式のクラスを与える．下記の補題は，定理 2.4，定理 2.7，定理 2.8 の三つを用いると直ちに得られる．

補題 5.4 $\mathfrak{B}$ を AND，OR，NOT を含むブール関数の集合とする．式 F を，ある k 変数基底関数 $h \in \mathfrak{B}$ と $\mathfrak{B}$ 式 $G_1, G_2, \ldots, G_k$ に対し，$h(G_1, G_2, \ldots, G_k)$ で表される一回読み $\mathfrak{B}$ 式とする．

このとき，以下が成り立つ．

1. h が AND または OR であるとき，つまり，$F = G_1 \wedge G_2$ または $F = G_1 \vee G_2$ であるとき，
$$\mathrm{AND}(F) = \sqrt{\mathrm{ADV}^2(G_1) + \mathrm{ADV}^2(G_2)}.$$

2. h が NOT であるとき，つまり，$F = \neg G_1$ であるとき，

$$\mathrm{ADV}(F) = \mathrm{ADV}(G_1).$$

3. $\mathrm{ADV}(G_1) = \cdots = \mathrm{ADV}(G_k)$ であるとき，

$$\mathrm{ADV}(F) = \mathrm{ADV}(h)\mathrm{ADV}(G_1).$$

上記の補題において，h および各 G_i が全て ADV タイトであり最簡化可能であれば，式 F も ADV タイトであり最簡化可能であることが容易にわかる．その理由は以下のようになる．a_i を h の最簡式における変数 x_i の出現回数とする．このとき，$\sum_{i=1}^{k} a_i = L(h)$ である．F の展開式のサイズは

$$\sum_{i=1}^{k} a_i L(G_i)$$

となる．よって，$L(G_1) = L(G_2) = \cdots = L(G_k)$ ならば F の展開式のサイズは $L(h)L(G_1)$ となるからである．

最簡化可能な式のクラスを以下のように再帰的に構成することができる．

定理 5.5 $\mathfrak{B}$ を ADV タイトな関数の集合とする．$C_{\mathfrak{B}}$ を以下のように再帰的に定義されるような一回読み $\mathfrak{B}$ 式の集合とする．

1. 任意の変数 x_i は $C_{\mathfrak{B}}$ に含まれる．

2. $C_{\mathfrak{B}}$ に含まれる $\mathfrak{B}$ 式 G_1 と G_2 に対して，G_1 と G_2 に現れる変数集合が素ならば，$G_1 \wedge G_2$，$G_1 \vee G_2$，$\neg G_1$ の三つの $\mathfrak{B}$ 式は全て $C_{\mathfrak{B}}$ に含まれる．

3. 入力変数の数が k である任意の基底関数 $h \in \mathfrak{B}$ と $\mathrm{ADV}(G_1) = \cdots = \mathrm{ADV}(G_k)$ を満たし，現れる変数集合が互いに素な k 個の $\mathfrak{B}$ 式 $G_1, G_2, \ldots, G_k \in C_{\mathfrak{B}}$ に対して，$h(G_1, G_2, \ldots, G_k)$ は $C_{\mathfrak{B}}$ に含まれる．

4. $C_{\mathfrak{B}}$ は上記の *1*，*2*，*3* で定義される式のみを含む．

このとき，クラス $C_{\mathfrak{B}}$ は最簡化可能である．

5.4　NPN 同値性

本節では NPN 同値性の定義を与え，いくつかの有用な性質について記す．

二つのブール関数が NPN 同値であるとは，片方の関数に対して入力の否定 (Input **N**egation) と入力の入れ替え (Input **P**ermutation) と出力の否定 (Output **N**egation) を適当に取ることでもう片方の関数を得ることができるときを言う．二つのブール関数が NP 同値であるとは，片方の関数に対して入力の否定 (Input **N**egation) と入力の入れ替え (Input **P**ermutation) を適当に取ることでもう片方の関数を得ることができるときを言う．より正確には，NPN 同値と NP 同値の定義は以下のようになる．

定義 5.5 論理変数 $x \in \{0,1\}$ に対して，$x^0 = x$，$x^1 = \bar{x}$ と定義する．n 変数ブール関数 f と g が NPN 同値であるとは，ある $\tau^I \in \{0,1\}^n$，$\tau^O \in \{0,1\}$ および $\{1,2,\ldots,n\}$ 上の置換 π が存在して，任意の $(x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ に対して以下の等式が成り立つことであり，$f \simeq_{\mathrm{NPN}} g$ と記す．

$$f(x_1, x_2, \ldots, x_n) = \left(g(x_{\pi(1)}^{\tau_1^I}, x_{\pi(2)}^{\tau_2^I} \ldots, x_{\pi(n)}^{\tau_n^I})\right)^{\tau^O}.$$

ここで，$\tau^I = (\tau_1^I, \tau_2^I, \ldots, \tau_n^I)$ である．さらに f と g が NP 同値であるとは，f と g が $\tau^O = 0$ のときに NPN 同値であるときをいい，$f \simeq_{\mathrm{NP}} g$ と記す．

定義 5.6 n 変数ブール関数に対する部分割り当てとは，$\{0,1,*\}$ の要素のことである．n 変数ブール関数 f と f に対する部分割り当て $\rho = (\rho_1, \rho_2, \ldots, \rho_n) \in \{0,1,*\}^n$ に対し，f の各入力変数 x_i（ただし $i \in \{j \mid \rho \neq *\}$）を定数 ρ_i に制限することによって得られるブール関数を f_ρ と記す．特に，ある変数 x_i のみを定数 $y \in \{0,1\}$ に制限した $n-1$ 変数関数を $f_{x_i=y}$ と記す．$f_{x_i=0}$ と $f_{x_i=1}$ が異なる関数であるとき，f は x_i に依存するという．

以下の 3 つの事実は，上記の定義 5.5 から容易に導ける．

事実 1 任意のブール関数 f と g に対して，f と g の依存する変数の数が異なるならば，f と g は NPN 同値ではない．

事実 2 二つのブール関数 f と g に対して，$|f^{-1}(0)| \neq |g^{-1}(0)|$ かつ $|f^{-1}(0)| \neq |g^{-1}(1)|$ であれば，f と g は NPN 同値ではない．また，$|f^{-1}(0)| \neq |g^{-1}(0)|$ であれば，f と g は NP 同値ではない．

事実 3 n をある自然数とし，$\rho \in \{0,1,*\}^n$ とする．n 変数ブール関数 f と g が NPN 同値であるならば，f_ρ と g_ρ は NPN 同値である．また，f と g が NP 同値であるならば，f_ρ と g_ρ は NP 同値である．

5.5　ADV タイトな関数を表す式の NPN 代表元

以下では基底関数を $\mathfrak{B}^* = \{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}, \mathrm{XOR}, \mathrm{MUX}\}$ に固定する．

NP 同値も NPN 同値も明らかに同値関係であるため，クラス $\mathrm{ROF}(\mathfrak{B}^*)$ は同値類に分割される．本節では $\mathrm{ROF}(\mathfrak{B}^*)$ に対する標準形を与え，標準形一回読み $\mathfrak{B}^*$ 式が $\mathrm{ROF}(\mathfrak{B}^*)$ の NPN 同値類の代表元となることを示す．

まずブール関数に対する自己双対の概念を拡張する．拡張された自己双対性は NP 同値類を分類するために用いられる．

定義 5.7 (自己双対) ブール関数 f が自己双対であるとは，$f \simeq_{\mathrm{NP}} \bar{f}$ であるときをいう．

ブール関数 f が自己双対であるとき，f の NPN 同値類は明らかに f の NP 同値類と等しい．この場合，f の NP 同値類に含まれる関数は全て自己双対であるので，このような f の NP 同値類を自己双対型に分類する．一方で，f が自己双対ではない場合は，f の NPN 同値類が f の NP 同値類と $\bar{f}$ の NP 同値類に分割される．この場合は，後で述べる方法でそれらの NP 同値類を P 型と N 型に分類する．したがって，$\mathrm{ROF}(\mathfrak{B}^*)$ の NP 同値類のうち自己双対型と P 型のみを集めてくることで，$\mathrm{ROF}(\mathfrak{B}^*)$ の NPN 同値類の代表元が得られる．上記の観察に基づき，$\mathrm{ROF}(\mathfrak{B}^*)$ に含まれる NP 同値類の代表元を与える標準形を考え，それらを自己双対型，P 型，N 型の三つの型に分類する．

次の小節では，骨格式の概念と $\mathrm{ROF}(\mathfrak{B}^*)$ の NP 代表元を表す標準骨格式を導入する．

5.5.1　骨格式

骨格式は一回読み式に含まれる自明な同値性を排除するように定義される．例えば，$(x_1 \vee x_2) \vee x_3$ と $(x_1 \vee x_2) \vee \bar{x}_3$ と $\bar{x}_1 \vee (\bar{x}_2 \vee x_3)$ は NP 同値であるが，我々はこれらを同一の骨格式 $\mathrm{OR}(\cdot,\cdot,\cdot)$ として扱う．より具体的には，骨格式表現において，

連続する OR を併合し引数が無限の単一の OR に置き換える（連続する AND や XOR も同様に併合する）．さらに，ド・モルガンの規則と $\neg(g_1 \oplus g_2) = ((\neg g_1) \oplus g_2)$ や $\neg\mathrm{MUX}(g_1, g_2, g_3) = \mathrm{MUX}(g_1, \neg g_2, \neg g_3)$ といった変換規則を再帰的に適用することにより，NOT が否定リテラルとしてしか現れない式が得られるので，骨格式表現においては NOT は除かれる．しかし，以下の議論を簡単にするために，NOT が $\mathrm{NOT}(\mathrm{XOR}(\cdot, \cdot, \ldots, \cdot))$ という形で現れることは許す．簡便さのために合成関数 $\mathrm{NOT} \circ \mathrm{XOR}$ を NXOR 記すことにする．

次の定義では，一回読み $\mathfrak{B}^*$ 式を内部頂点が $\{\mathrm{AND}, \mathrm{OR}, \mathrm{XOR}, \mathrm{NXOR}, \mathrm{MUX}\}$ のいずれかの関数に対応する関数名でラベルづけられた根付き順序木として再定義する．ここで，MUX を除く演算子の引数の数に制限はない．その後，葉のラベルがない $\mathfrak{B}^*$ 式として骨格式を定義する．

根付き順序木 T に対して，T の内部頂点の集合を nodes_T，T の葉の集合を leaves_T と記すこととする．

定義 5.8 一回読み $\mathfrak{B}^*$ 式 F とは，三つ組 $F = (T, \mathrm{OP}, \mathrm{lit})$ で以下の条件を満たすものとする．ここで，T は根付き順序木とし，nodes_T を T の全ての内部頂点からなる集合，leaves_T を T の全ての葉からなる集合とする．また，OP を内部頂点へラベルを割り当てる関数 $\mathrm{OP} : \mathrm{nodes}_T \to \{\mathrm{AND}, \mathrm{OR}, \mathrm{XOR}, \mathrm{NXOR}, \mathrm{MUX}\}$，lit を葉へラベルを割り当てる関数 $\mathrm{lit} : \mathrm{leaves}_T \to \{x_1, \bar{x}_1, x_2, \bar{x}_2, \ldots, x_n, \bar{x}_n\}$ とする．

1. n を leaves_T の要素数とする．任意の互いに異なる葉 $l_1, l_2 \in \mathrm{leaves}_T$ と任意の $1 \leq i \leq n$ に対して，$\{\mathrm{lit}(l_1), \mathrm{lit}(l_2)\} \not\subseteq \{x_i, \bar{x}_i\}$.

2. 各内部頂点 $v \in \mathrm{nodes}_T$ に対して，$\mathrm{OP}(v) \neq \mathrm{MUX}$ であるとき，v の子の数は 2 以上であり，$\mathrm{OP}(v) = \mathrm{MUX}$ であるとき，v の子の数は 3 である．

3. AND または OR がラベルづけられた各頂点において，その子のラベルが親と同じラベルではない．

4. XOR または NXOR がラベルづけられた各頂点にておいて，その子のラベルが XOR でも NXOR でもない．

条件 *2,3,4* を全て満たす対 (T, OP) を**骨格式**と呼ぶ．ある一回読み $\mathfrak{B}^*$ 式 $F = (T, \mathrm{OP}, \mathrm{lit})$ に対して，骨格式 (T, OP) を特に F' と記す．ある骨格式 $\mathbb{F} = (T, \mathrm{OP})$ に対して，$\mathbb{F}$ の葉に論理変数 $x_1, x_2, \ldots, x_n$ を左から右へラベル付けることで得られる一回読み $\mathfrak{B}^*$ 式を $\mathbb{F}(x_1, x_2, \ldots, x_n)$ と記す．ここで，n は $\mathbb{F}$ の葉の数である．

以下では，骨格式 $\mathbb{F}$ を式 $\mathbb{F}(x_1, x_2, \ldots, x_n)$ が表す関数としばしば同一視する．例えば，あるブール関数 f に対して，$\mathbb{F} \simeq_{\mathrm{NP}} f$ と書いた場合には，$\mathbb{F}(x_1, x_2, \ldots, x_n)$ の表す関数と f が NP 同値であることを意味する．

後の議論で用いる有用な命題を次に示す．

命題 5.1 $\mathbb{F} = (T, \mathrm{OP})$ を根 r が k 変数関数 h でラベル付けられている骨格式とする．$\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k$ を r の子の部分骨格式とする．関数 $f_1, f_2, \ldots, f_k$ を各 $1 \leq i \leq k$ に対して $\mathbb{F}_i \simeq_{\mathrm{NP}} f_i$ であるような関数とする．このとき，$\mathbb{F} \simeq_{\mathrm{NP}} h \circ (f_1, f_2, \ldots, f_k)$ が成り立つ．

証明: 各 $i \in \{1, 2, \ldots, k\}$ に対して，部分骨格式 $\mathbb{F}_i$ の葉の数を N_i とする．NP 同値の定義から，各 $i \in \{1, 2, \ldots, N_i\}$ に対して

$$\mathbb{F}_i(x_{i,\pi_i(1)}^{\tau_i^I(1)}, x_{i,\pi_i(2)}^{\tau_i^I(2)} \ldots, x_{i,\pi_i(N_i)}^{\tau_i^I(N_i)}) = f_i(x_{i,1}, x_{i,2}, \ldots, x_{i,N_i})$$

となるような π_i と τ_i^I が存在する．このとき，次の式は明らかに $h \circ (f_1, f_2, \ldots, f_k)$ を表す．

$$\mathbb{F}(x_{1,\pi_1(1)}^{\tau_1^I(1)}, x_{1,\pi_1(2)}^{\tau_1^I(2)}, \ldots, x_{1,\pi_1(N_1)}^{\tau_1^I(N_1)}, x_{2,\pi_2(1)}^{\tau_2^I(1)}, \ldots, x_{2,\pi_2(N_2)}^{\tau_2^I(N_2)}, \ldots, x_{k,\pi_x(1)}^{\tau_1^I(1)}, \ldots, x_{k,\pi_x(N_k)}^{\tau_1^I(N_k)}).$$

よって，$\mathbb{F} \simeq_{\mathrm{NP}} h \circ (f_1, f_2, \ldots, f_k)$ である．

□

5.5.2　標準骨格式

本小節では，標準骨格式の定義を与える．各標準骨格式は $\mathrm{ROF}(\mathfrak{B}^*)$ の NP 代表元に 1 対 1 に対応する．定義は少し複雑であるので，異なる骨格式が同じ NP 同値類に属する関数を表す可能性を排除するためのアイディアについて，初めに直観的な説明を与える．

まず初めに，$\mathrm{AND}(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3)$ と $\mathrm{AND}(\mathbb{G}_1, \mathbb{G}_3, \mathbb{G}_2)$ は一般的には異なる骨格式であるが，それらの表す関数は NP 同値である．この問題を解消するために，骨格式の集合上に辞書式順序を導入し，$\mathrm{OP}(u) \in \{\mathrm{AND}, \mathrm{OR}, \mathrm{XOR}, \mathrm{NXOR}\}$ である内部頂点 u に対して，u の子の部分骨格式が左から右へ降順に並んでいるような骨

格式のみを許すことにする．二つの骨格式 $\mathbb{F}$ と $\mathbb{G}$ に対して，$\mathbb{F}$ が $\mathbb{G}$ の順序より大きいとき，$\mathbb{F} > \mathbb{G}$ と書くこととする．

次に，$\mathrm{XOR}(\mathbb{G}_1, \mathbb{G}_2)$ と $\mathrm{XOR}(\bar{\mathbb{G}}_1, \bar{\mathbb{G}}_2)$ は一般的には異なる骨格式であるが，それらの表す関数は NP 同値である．ここで，$\bar{\mathbb{G}}_i$ $(1 \leq i \leq 2)$ は $\mathbb{G}_i$ の表す関数の否定関数と NP 同値な関数を表す骨格式である（否定骨格式の正式な定義は後に与える）．この問題を解消するために，$\mathrm{OP}(u) \in \{\mathrm{XOR}, \mathrm{NXOR}\}$ である任意の内部頂点 u に対して，u を根とする部分骨格式 $\mathbb{G}$ が $\mathbb{G} \geq \bar{\mathbb{G}}$ を満たすような骨格式のみを許すことにする．

三番目に，$\mathrm{MUX}(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3)$ と $\mathrm{MUX}(\bar{\mathbb{G}}_1, \mathbb{G}_3, \mathbb{G}_2)$ は一般的には異なる骨格式であるが，それらの表す関数は NP 同値である．この問題を解消するために，$\mathrm{OP}(u) \in \{\mathrm{MUX}\}$ である任意の内部頂点 u に対して，u を頂点とする部分骨格式を $\mathrm{MUX}(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3)$ とすると，$\mathbb{G}_2 \geq \mathbb{G}_3$ を満たすような骨格式のみを許すことにする．

これまで見てきたように，標準骨格式を定義する前に否定骨格式の定義を与える必要がある．

定義 5.9 骨格式 $\mathbb{F}$ が自己双対型であるとは，$\mathbb{F}$ の表す関数が自己双対であるときをいう．

定義 5.10 (否定骨格式) ある骨格式 $\mathbb{F}$ に対して，その否定骨格式 $\bar{\mathbb{F}}$ は以下の手続きで定義される．$\mathbb{F}$ が葉である場合は，$\bar{\mathbb{F}} = \mathbb{F}$ である．$\mathbb{F}$ が葉ではない場合は，$\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k$ をそれぞれ $\mathbb{F}$ の根の子の部分骨格式とする．$\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k$ を降順にソートして得られる骨格式の列を $\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k$ とする．また，$\bar{\mathbb{F}}_1, \bar{\mathbb{F}}_2, \ldots, \bar{\mathbb{F}}_k$ を降順にソートして得られる骨格式の列を $\mathbb{H}_1, \mathbb{H}_2, \ldots, \mathbb{H}_k$ とする．ここで，各 $\mathbb{F}_i$ $(1 \leq i \leq k)$ を $\mathbb{F}_i$ に対してこの手続きを再帰的に適用することによって得られる骨格式とする．

- $\mathbb{F} = \mathrm{AND}(\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k)$ である場合は，$\overline{\mathbb{F}} = \mathrm{OR}(\mathbb{H}_1, \mathbb{H}_2, \ldots, \mathbb{H}_k)$ とする．
- $\mathbb{F} = \mathrm{OR}(\mathbb{F}_1, , \mathbb{F}_2, \ldots, \mathbb{F}_k)$ である場合は，$\overline{\mathbb{F}} = \mathrm{AND}(\mathbb{H}_1, \mathbb{H}_2, \ldots, \mathbb{H}_k)$ とする．
- $\mathbb{F} = \mathrm{XOR}(\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k)$ である場合は，$\{\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k\}$ が自己双対型の骨格式を含まないならば，$\overline{\mathbb{F}} = \mathrm{NXOR}(\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k)$ とし，$\{\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k\}$ が少なくとも一つの自己双対型の骨格式を含むならば $\overline{\mathbb{F}} = \mathrm{XOR}(\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k)$ とする．

- $\mathbb{F} = \mathrm{NXOR}(\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k)$ である場合は，$\{\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k\}$ が自己双対型の骨格式を含まないならば，$\overline{\mathbb{F}} = \mathrm{XOR}(\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k)$ とする．$\{\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k\}$ が少なくとも一つの自己双対型の骨格式を含むならば $\overline{\mathbb{F}} = \mathrm{NXOR}(\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k)$ とする．

- $\mathbb{F} = \mathrm{MUX}(\mathbb{F}_1, \mathbb{F}_2, \mathbb{F}_3)$ である場合は，

$$\overline{\mathbb{F}} = \begin{cases} \mathrm{MUX}(\mathbb{F}_1, \overline{\mathbb{F}}_2, \overline{\mathbb{F}}_3) & \overline{\mathbb{F}}_2 \geq \overline{\mathbb{F}}_3 \text{ のとき} \\ \mathrm{MUX}(\overline{\mathbb{F}}_1, \overline{\mathbb{F}}_3, \overline{\mathbb{F}}_2) & \overline{\mathbb{F}}_2 < \overline{\mathbb{F}}_3 \text{ のとき} \end{cases}$$

  とする．

否定骨格式は明らかに骨格式の定義を満たすことに注意されたい．以下の命題に示すように，否定骨格式 $\bar{\mathbb{F}}$ の表す関数は，骨格式 $\mathbb{F}$ の表す関数の否定と NP 同値である．

命題 5.2 任意の骨格式 $\mathbb{F}$ に対して，$\mathbb{F}$ が表す関数を f とする．このとき，$\bar{\mathbb{F}} \simeq_{\mathrm{NP}} \bar{f}$ が成り立つ．

証明: $\mathbb{F}$ の深さ d に関する帰納法で証明する．

（基底段階）$d = 0$ のとき，$\mathbb{F}$ は葉のみの骨格式である．よって，$\mathbb{F}$ の表す関数は x_1 である．否定骨格式の定義 5.10 より，$\bar{\mathbb{F}}$ の表す関数も x_1 である．よって，$\bar{\mathbb{F}} \simeq_{\mathrm{NP}} \bar{f}$ である．

（帰納段階）$\mathbb{F}$ の根の子の部分骨格式を $\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k$ $(k \geq 2)$ とし，$\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k$ の表す関数をそれぞれ $f_1, f_2, \ldots, f_k$ とする．$\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k$ を降順にソートして得られる骨格式の列を $\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k$ とする．また，$\bar{\mathbb{F}}_1, \bar{\mathbb{F}}_2, \ldots, \bar{\mathbb{F}}_k$ を降順にソートして得られる骨格式の列を $\mathbb{H}_1, \mathbb{H}_2, \ldots, \mathbb{H}_k$ とする．$\mathbb{F}$ の根のラベルについての場合分けで証明を行う．

まず，$\mathbb{F}$ の根のラベルが AND である場合を考える．$\mathbb{F}$ の根のラベルが OR の場合も同様に証明できる．このとき，$f = \mathrm{AND}(f_1, f_2, \ldots, f_k)$ である．ド・モルガンの規則により，$\bar{f} = \mathrm{OR}(\bar{f}_1, \bar{f}_2, \ldots, \bar{f}_k)$ が成り立つ．一方，否定骨格式の定義 5.10 より，

$$\begin{aligned} \bar{\mathbb{F}} &= \mathrm{OR}(\mathbb{H}_1, \mathbb{H}_2, \ldots, \mathbb{H}_k) \\ &\simeq_{\mathrm{NP}} \mathrm{OR}(\bar{\mathbb{F}}_1, \bar{\mathbb{F}}_2, \ldots, \bar{\mathbb{F}}_k) \end{aligned}$$

である．二番目の等式は，OR が入力に対して対称な関数であることと NP 同値の定義から明らかである．帰納法の仮定より，各 $i \in \{1, 2, \ldots, k\}$ に対して，$\bar{\mathbb{F}}_i \simeq_{\mathrm{NP}} \bar{f}_i$ である．よって，命題 5.1 から，$\bar{\mathbb{F}} \simeq_{\mathrm{NP}} \bar{f}$ となる．

次に $\mathbb{F}$ の根のラベルが XOR である場合を考える．$\mathbb{F}$ の根のラベルが NXOR の場合も同様に証明できる．このとき，$\bar{f} = \mathrm{NXOR}(f_1, f_2, \ldots, f_k)$ が成り立つ．一方，否定骨格式の定義 5.10 より，$f_1, f_2, \ldots, f_k$ の中に自己双対関数が含まれていない場合は，

$$\begin{aligned} \bar{\mathbb{F}} &= \mathrm{NXOR}(\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k) \\ &\simeq_{\mathrm{NP}} \mathrm{NXOR}(\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k) \end{aligned} \tag{5.9}$$

である．式 (5.9) は，NXOR が入力に対して対称な関数であることと NP 同値の定義から明らかである．よって，命題 5.1 から，$\bar{\mathbb{F}} \simeq_{\mathrm{NP}} \bar{f}$ となる．$f_1, f_2, \ldots, f_k$ の中に自己双対関数が含まれている場合，一般性を欠くことなく $\mathbb{G}_1$ が自己双対型と仮定してよい．このとき，

$$\begin{aligned} \bar{\mathbb{F}} &= \mathrm{XOR}(\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k) \\ &\simeq_{\mathrm{NP}} \mathrm{XOR}(\bar{\mathbb{G}}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k) && (5.10) \\ &= \mathrm{NXOR}(\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k) && (5.11) \\ &\simeq_{\mathrm{NP}} \mathrm{NXOR}(\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k) && (5.12) \end{aligned}$$

である．ここで，式 (5.10) は $\mathbb{G}_1$ が自己双対型であることから，式 (5.11) は一つの入力否定が出力否定と等価であるという XOR の性質から，式 (5.12) は NXOR が入力に対して対称な関数であることと NP 同値の定義から，それぞれ成り立つ．よって，$\bar{\mathbb{F}} \simeq_{\mathrm{NP}} \bar{f}$ となる．

最後に $\mathbb{F}$ の根のラベルが MUX である場合を考える．このとき，$f = \mathrm{MUX}(f_1, f_2, f_3)$ である．$\bar{f} = \mathrm{MUX}(f_1, \bar{f}_2, \bar{f}_3)$ が成り立つ．一方，否定骨格式の定義 5.10 より，$\bar{\mathbb{F}}_2 \geq \bar{\mathbb{F}}_3$ であるときは

$$\bar{\mathbb{F}} = \mathrm{MUX}(\mathbb{F}_1, \bar{\mathbb{F}}_2, \bar{\mathbb{F}}_3)$$

である．よって，帰納法の仮定と命題 5.1 より $\bar{\mathbb{F}} \simeq_{\mathrm{NP}} \bar{f}$ となる．$\bar{\mathbb{F}}_2 < \bar{\mathbb{F}}_3$ であるときは

$$\bar{\mathbb{F}} = \mathrm{MUX}(\bar{\mathbb{F}}_1, \bar{\mathbb{F}}_3, \bar{\mathbb{F}}_2)$$

である．$\mathrm{MUX}(f_1, \bar{f}_2, \bar{f}_3) = \mathrm{MUX}(\bar{f}_1, \bar{f}_3, \bar{f}_2)$ であるから，帰納法の仮定と命題 5.1 より $\bar{\mathbb{F}} \simeq_{\mathrm{NP}} \bar{f}$ となる．

□

定義 5.11 (P 型，N 型) 自己双対型ではない骨格式 $\mathbb{F}$ に対して，$\mathbb{F} > \bar{\mathbb{F}}$ ならば $\mathbb{F}$ は P 型であり，$\mathbb{F} < \bar{\mathbb{F}}$ ならば $\mathbb{F}$ は N 型であるという．

命題 5.2 より，$\mathbb{F} = \bar{\mathbb{F}}$ ならば $\mathbb{F}$ は自己双対型であることに注意されたい．したがって，任意の骨格式は P 型，N 型，自己双対型のいずれかに分類される．

以上の準備のもとに，いよいよ標準骨格式の定義を与える．

定義 5.12 骨格式 $\mathbb{F}$ が標準形であるとは，以下の条件をすべて満たすときである．

- $\mathrm{OP}(u) \in \{\mathrm{AND}, \mathrm{OR}, \mathrm{XOR}, \mathrm{NXOR}\}$ であるような任意の内部頂点 u に対して，u の子の部分骨格式が左から右へ降順に並んでいる．
- ラベルが XOR の頂点の任意の子の部分骨格式は P 型か自己双対型である．ラベルが NXOR の頂点の任意の子の部分骨格式は P 型である．
- ラベルが MUX の頂点に対し，その子の部分骨格式を左から順に $\mathbb{F}_1$，$\mathbb{F}_2$，$\mathbb{F}_3$ とすると，
  1. $\mathbb{F}_2 > \mathbb{F}_3$，または．
  2. $\mathbb{F}_2 = \mathbb{F}_3$ かつ $\mathbb{F}_1$ は自己双対型か P 型である．

否定骨格式と標準骨格式の定義を用いると次の補題を示すことができる．

補題 5.6 任意の標準骨格式 $\mathbb{F}$ に対して，$\bar{\mathbb{F}}$ は標準骨格式である．

証明: $\mathbb{F}$ の深さ d に関する帰納法で証明する．

（基底段階）$d = 0$ のとき，$\mathbb{F}$ は葉のみの骨格式である．このとき，$\bar{\mathbb{F}}$ は明らかに標準骨格式である．

（帰納段階）$d \leq k$ のとき，題意が成立すると仮定して深さが $d = k+1$ のとき $\bar{\mathbb{F}}$ が標準骨格式であることを示す．$\mathbb{F}$ の根の子の部分骨格式を $\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k$ $(k \geq 2)$ とする．$\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k$ を降順にソートして得られる骨格式の列を $\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k$ とする．また，$\bar{\mathbb{F}}_1, \bar{\mathbb{F}}_2, \ldots, \bar{\mathbb{F}}_k$ を降順にソートして得られる骨格式の列を $\mathbb{H}_1, \mathbb{H}_2, \ldots, \mathbb{H}_k$ とする．否定骨格式の定義 5.10 より，$\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k$ は明らかにそれぞれ標準骨格式である．$\mathbb{F}$ の根のラベルについての場合分けで証明を行う．

まず，$\mathbb{F}$ の根のラベルが AND である場合を考える．OR の場合も同様に証明できる．否定骨格式の定義 5.10 より，$\bar{\mathbb{F}} = \mathrm{OR}(\mathbb{H}_1, \mathbb{H}_2, \ldots, \mathbb{H}_k)$ である．帰納法の仮定より $\mathbb{H}_1, \mathbb{H}_2, \ldots, \mathbb{H}_k$ はそれぞれ標準骨格式であり，降順に並んでいる．よって，$\bar{\mathbb{F}}$ は標準骨格式である．

次に，$\mathbb{F}$ の根のラベルが XOR である場合を考える．否定骨格式の定義 5.10 より，$\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k$ が全て P 型である場合は，$\bar{\mathbb{F}} = \mathrm{NXOR}(\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k)$ であり，$\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k$ の中に自己双対型の骨格式が存在する場合は，$\bar{\mathbb{F}} = \mathrm{XOR}(\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k)$ である．帰納法の仮定より $\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k$ はそれぞれ標準骨格式であり，降順に並んでいる．よって，どちらの場合も $\bar{\mathbb{F}}$ は標準骨格式である．

次に，$\mathbb{F}$ の根のラベルが NXOR である場合を考える．否定骨格式の定義 5.10 より，$\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k$ は全て P 型であり，$\bar{\mathbb{F}} = \mathrm{XOR}(\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k)$ である．帰納法の仮定より $\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k$ はそれぞれ標準骨格式であり，降順に並んでいる．よって，どちらの場合も $\bar{\mathbb{F}}$ は標準骨格式である．

最後に，$\mathbb{F}$ の根のラベルが MUX である場合を考える．否定骨格式の定義 5.10 より，$\mathbb{F}_2 \geq \mathbb{F}_3$ のとき $\bar{F} = \mathrm{MUX}(\mathbb{F}_1, \bar{\mathbb{F}}_2, \bar{\mathbb{F}}_3)$ であり，$\mathbb{F}_2 < \mathbb{F}_3$ のとき $\bar{F} = \mathrm{MUX}(\bar{\mathbb{F}}_1, \bar{\mathbb{F}}_3, \bar{\mathbb{F}}_2)$ である．ここで，帰納法の仮定より $\mathbb{F}_1, \mathbb{F}_2, F_3$ はそれぞれ標準骨格式である．以下の二つの場合を考える．骨格式の定義から $\mathbb{F}_2 \geq \mathbb{F}_3$ であることに注意されたい．

(1)$\mathbb{F}_2 > \mathbb{F}_3$ の場合を考える．$\mathbb{F}_2 \neq \mathbb{F}_3$ であるので，否定骨格式の定義 5.10 から明らかに $\bar{\mathbb{F}}_2 \neq \bar{\mathbb{F}}_3$ である．$\bar{\mathbb{F}}_2 > \bar{\mathbb{F}}_3$ であれば $\bar{\mathbb{F}} = \mathrm{MUX}(\mathbb{F}_1, \bar{\mathbb{F}}_2, \bar{\mathbb{F}}_3)$ であるから，$\mathbb{F}$ は標準骨格式である．$\bar{\mathbb{F}}_2 < \bar{\mathbb{F}}_3$ であれば $\bar{\mathbb{F}} = \mathrm{MUX}(\bar{\mathbb{F}}_1, \bar{\mathbb{F}}_3, \bar{\mathbb{F}}_2)$ であるから，やはり $\mathbb{F}$ は標準骨格式である．

(2)$\mathbb{F}_2 = \mathbb{F}_3$ の場合を考える．このとき $\mathbb{F}_1$ は P 型か自己双対型である．否定骨格式の定義 5.10 から明らかに $\bar{\mathbb{F}}_2 = \bar{\mathbb{F}}_3$ であり，$\bar{\mathbb{F}} = \mathrm{MUX}(\mathbb{F}_1, \bar{\mathbb{F}}_2, \bar{\mathbb{F}}_3)$ である．よって，$\mathbb{F}$ は標準骨格式である．

よって，どちらの場合も $\bar{\mathbb{F}}$ は標準骨格式である．

□

5.5.3　$\mathrm{ROF}(\mathfrak{B}^*)$ の NP 同値類の代表元

本小節では，(1) 標準骨格式が表す関数の集合がクラス $\mathrm{ROF}(\mathfrak{B}^*)$ の NP 同値類の代表元から成ること，(2) 各標準骨格式は NP 同値類のある代表元に一対一で対応すること，の二点を示す．以下では，(1) と (2) を示している二つの定理を与える．

定理 5.7 任意の一回読み $\mathfrak{B}^*$ 式 F に対して，$F \simeq_{\mathrm{NP}} \mathbb{F}$ であるような標準骨格式 $\mathbb{F}$ が存在する．

証明: 図 5.1 にアルゴリズム canonicalize を与える．canonicalize はある式 $F \in \mathrm{ROF}(\mathfrak{B}^*)$ を $F \simeq_{\mathrm{NP}} \mathbb{F}$ であるような標準骨格式に $\mathbb{F}$ に変形するアルゴリズムである．

アルゴリズム canonicalize の出力する骨格式 $\mathbb{F}$ が標準形であることは明らかである．よって，以下では F の深さに関する帰納法により $\mathbb{F} \simeq_{\mathrm{NP}} F$ を示す．

基底段階については，明らかに $\mathbb{F} \simeq_{\mathrm{NP}} F$ である．帰納段階については，F の根の演算子に基づくいくつかの場合を考える．どの場合についても帰納法の仮定より，

$$\mathbb{F}_i \simeq_{\mathrm{NP}} F_i, \quad 1 \leq i \leq k \tag{5.13}$$

が成立している．

最初に $h \in \{\mathrm{AND}, \mathrm{OR}\}$ の場合を考える．この場合，(5.13) と命題 5.1 より，

$$F = h(F_1, \ldots, F_k) \simeq_{\mathrm{NP}} h(\mathbb{F}_1, \ldots, \mathbb{F}_k) \simeq_{\mathrm{NP}} \mathbb{F}$$

を得る．

次に $h \in \{\mathrm{XOR}, \mathrm{NXOR}\}$ の場合を考える．一般性を欠くことなく，ある $0 \leq l \leq k$ に対して，$\mathbb{F}_1, \ldots, \mathbb{F}_l$ が全て N 型であり，$\mathbb{F}_{l+1}, \ldots, \mathbb{F}_k$ が P 型か自己双対型であると仮定する．命題 5.2 より，各 $1 \leq i \leq l$ に対して，$\mathbb{G}_i \simeq_{\mathrm{NP}} \overline{F}_i$ を得る．いま，ある $\mathbb{F}_i$（仮に $\mathbb{F}_{l+1}$ とする）が自己双対型である場合を考える．$\mathbb{G}_{l+1} \simeq_{\mathrm{NP}} F^0_{l+1} \simeq_{\mathrm{NP}} F^1_{l+1}$ に注意すると命題 5.1 より，$a \in \{0, 1\}$ を適切に選ぶことで

$$\begin{aligned}
\mathbb{F} &\simeq_{\mathrm{NP}} \mathrm{XOR}(\mathbb{G}_1, \ldots, \mathbb{G}_k) \\
&\simeq_{\mathrm{NP}} \mathrm{XOR}(\overline{F}_1, \ldots, \overline{F}_l, F^a_{l+1}, F_{l+2}, \ldots, F_k) \\
&= \mathrm{XOR}(F_1, \ldots, F_k) \oplus ((l + a) \bmod 2) \\
&= h(F_1, \ldots, F_k) \\
&= F
\end{aligned}$$

canonicalize(F)
{
　if F がリテラル, then return 単一の葉;
　ある演算子 h に対して $F = h(F_1, \ldots, F_k)$ と仮定する;
　for $i = 1$ to k, $\mathbb{F}_i = \text{canonicalize}(F_i)$;
　if $h \in \{\text{AND}, \text{OR}\}$, then return $h(\text{sort}(\mathbb{F}_1, \ldots, \mathbb{F}_k))$;
　if $h \in \{\text{XOR}, \text{NXOR}\}$, then
　　for $i = 1$ to k
　　　if $\mathbb{F}_i$ が P 型 or 自己双対型, then $\mathbb{G}_i = \mathbb{F}_i$;
　　　if $\mathbb{F}_i$ が N 型, then $\mathbb{G}_i = \overline{\mathbb{F}}_i$;
　　if ある $\mathbb{F}_i$ が自己双対型, then
　　　return XOR(sort($\mathbb{G}_1, \ldots, \mathbb{G}_k$));
　　if $\{\mathbb{F}_1, \ldots, \mathbb{F}_k\}$ に含まれる N 型の数が偶数, then
　　　return $h(\text{sort}(\mathbb{G}_1, \ldots, \mathbb{G}_k))$;
　　else return $\bar{h}(\text{sort}(\mathbb{G}_1, \ldots, \mathbb{G}_k))$,
　　　ただし $\bar{h}$ は $h = \text{XOR}$ ならば NXOR であり，そうでなければ XOR とする;
　if $h = \text{MUX}$, then
　　if $(\mathbb{F}_2 < \mathbb{F}_3)$ or $(\mathbb{F}_2 = \mathbb{F}_3$ かつ $\mathbb{F}_1$ が N 型), then
　　　$\mathbb{G}_1 = \overline{\mathbb{F}}_1$; $\mathbb{G}_2 = \mathbb{F}_3$; $\mathbb{G}_3 = \mathbb{F}_2$;
　　return MUX($\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3$);
}

図 5.1: アルゴリズム canonicalize

を得る．$\mathbb{F}_{l+1}, \ldots, \mathbb{F}_k$ がすべて P 型の場合，l が偶数ならば,

$$\begin{aligned}\mathbb{F} &\simeq_{\mathrm{NP}} h(\mathbb{G}_1, \ldots, \mathbb{G}_k)\\ &\simeq_{\mathrm{NP}} h(\overline{F}_1, \ldots, \overline{F}_l, F_{l+1}, \ldots, F_k)\\ &= h(F_1, \ldots, F_k)\\ &= F,\end{aligned}$$

l が奇数の場合ならば,

$$\begin{aligned}\mathbb{F} &\simeq_{\mathrm{NP}} \bar{h}(\mathbb{G}_1, \ldots, \mathbb{G}_k)\\ &\simeq_{\mathrm{NP}} \bar{h}(\overline{F}_1, \ldots, \overline{F}_l, F_{l+1}, \ldots, F_k)\\ &= h(F_1, \ldots, F_k)\\ &= F\end{aligned}$$

より，いずれの場合も $\mathbb{F} \simeq_{\mathrm{NP}} F$ を得る．

最後に $h = \mathrm{MUX}$ の場合を考える．$F = \mathrm{MUX}(F_1, F_2, F_3) = \mathrm{MUX}(\overline{F}_1, F_3, F_2)$ であるので，$F \simeq_{\mathrm{NP}} \mathrm{MUX}(\mathbb{F}_1, \mathbb{F}_2, \mathbb{F}_3) \simeq_{\mathrm{NP}} \mathrm{MUX}(\overline{\mathbb{F}}_1, \mathbb{F}_3, \mathbb{F}_2)$ を得る．

□

定理 5.8 任意の標準骨格式 $\mathbb{F}$ と $\mathbb{G}$ に対して，$\mathbb{F} \neq \mathbb{G}$ のときは $\mathbb{F} \not\simeq_{\mathrm{NP}} \mathbb{G}$.

次の小節では，この定理の証明のために必要となるいくつかの命題と補題を与え，定理の証明は 5.5.5 節で行う．

5.5.4　技術的な補題群

本小節では，定理 5.8 の証明のために必要となる二つの補題と，それら補題を示すために必要となる六つの命題を示す.

$\mathrm{ROF}(\mathfrak{B}^*)$ に含まれるある式 $F = (T, \mathrm{OP}, \mathrm{lit})$ を考える．F に現れるある変数 x に対して，x のラベルが付けられた葉から根へのパス上の頂点集合を $\mathrm{UP}(x)$ と記す．変数 x と y に対して，$\mathrm{UP}(x) \cap \mathrm{UP}(y)$ に含まれる内部頂点を x と y の共通祖先と呼ぶ．共通祖先の中で x（と y）に最も近い内部頂点を x と y の**最小共通祖先**と呼び，$x \sqcap_F y$ と記す．$|U| \geq 2$ である変数の集合 U とある内部頂点 v に対し，U の任意の二つの変数 $x, y \in U$ $(x \neq y)$ が $x \sqcap_F y = v$ を満たすとき，U は v で合流する

という．U が内部頂点 v で合流するとき，v を U の最小共通祖先と呼び，$v = \sqcap_F U$ と記す．

以下の命題群は NP 同値類の定義から得られるものである．以降では，演算子 h の引数の数 k を明示したい場合には，h_k のように演算子に引数の数を下付きで付加して書くこともある．例えば，AND_k は k 変数 AND 関数を表す．

命題 5.3 $f(x_1, \ldots, x_n)$ を $\mathrm{ROF}(\mathfrak{B}^*)$ に含まれる式によって表される関数とする．このとき，以下が成り立つ．

1. $\exists a \in \{0,1\}^n, f(a) = 1.$
2. $\exists a \in \{0,1\}^n, f(a) = 0.$
3. $1 \leq \forall i \leq n$，$\exists a \in \{0,1\}^{i-1}$，$\exists b \in \{0,1\}^{n-i}$，$\exists \epsilon \in \{0,1\}$，$f(a, x_i, b) = x_i^\epsilon$.

証明: 項目 1 と 2 が成立するは明らかである．項目 3 について示す．定数に固定しない変数を x_i $(1 \leq i \leq n)$ とする．x_i の各祖先 v に対し，v の子を根とする部分式で変数 x_i が現れないものの出力は，その部分式の入力変数に適当に定数を割り当てることで任意の値を取らせることができる．よって，項目 3 を示すためには，$\mathfrak{B}^*$ に含まれる各関数 $h_k(x_1, \ldots, x_k)$ に対して，一つの変数 x_i を除いて他の変数を定数に適当に固定することで，x_i にのみ依存する関数，すなわち，x_i または $\bar{x}_i$ が得られることを示せば良い．

AND の場合は，x_i 以外の変数を全て 1 に固定することで，関数 x_i が得られる．OR の場合は，x_i 以外の変数を全て 0 に固定することで，関数 x_i が得られる．XOR の場合は，x_i 以外の変数を全て 0 に固定することで，関数 x_i が得られる．NXOR の場合は，x_i 以外の変数を全て 0 に固定することで，関数 $\bar{x}_i$ が得られる．$\mathrm{MUX}(x_1, x_2, x_3)$ の場合は，$x_2 = 0, x_3 = 1$ とすると x_1 が，$x_1 = 0$ とすると x_2 が，$x_1 = 1$ とすると x_3 がそれぞれ得られる．

□

命題 5.4 $\mathrm{MUX}(x_1, x_2, x_3)$ に対する入力の部分割り当てを考える．このとき，得られる関数は XOR_2 と NXOR_2 のどちらとも NP 同値ではない．

証明: XOR_2 も NXOR_2 も 2 変数関数であるから，x_1, x_2, x_3 のうち一つの変数を定数に固定して得られる関数について考えれば十分である．$x_1 = 0$ と固定すると x_2

が得られ，$x_1 = 1$ と固定すると x_3 が得られる．$x_2 = 0$ と固定すると $x_1 \wedge x_3$ が得られ，$x_2 = 1$ と固定すると $\bar{x}_1 \vee x_3$ が得られる．$x_3 = 0$ と固定すると $\bar{x}_1 \wedge x_2$ が得られ，$x_3 = 1$ と固定すると $x_2 \wedge x_1$ が得られる．$\mathrm{XOR}_2^{-1}(0) \neq \mathrm{AND}_2^{-1}(0)$ かつ $\mathrm{XOR}_2^{-1}(0) \neq \mathrm{AND}_2^{-1}(1)$ であるから，事実 1 と事実 2 とド・モルガンの規則より，どの関数も XOR_2 とも NXOR_2 とも NP 同値ではないため，題意が成立する．

□

命題 5.5 MUX 演算子を用いない任意の式 $F \in \mathrm{ROF}(\mathfrak{B}^*)$ は MUX と NP 同値ではない．

証明: 事実 1 より，現れる変数の数が 3 である式についてのみ考えればよい．MUX を用いない任意の一回読み $\mathfrak{B}^*$ 式は，どの一つの変数を固定しても必ず残りの二つの変数に依存する関数を表す式となる．一方 MUX は第 1 入力変数を固定すると 1 つの変数のみに依存する関数が得られる．よって，事実 1 と事実 3 から MUX を用いない任意の一回読み $\mathfrak{B}^*$ 式は MUX と NP 同値ではない．

□

命題 5.6 任意の $k \geq 2$ に対し，AND と OR のみを用いる任意の式 $F \in \mathrm{ROF}(\mathfrak{B}^*)$ は XOR_k と NXOR_k のどちらとも NP 同値ではない．

証明: $\mathrm{AND}_2^{-1}(0) = 1$，$\mathrm{OR}_2^{-1}(0) = 3$，$\mathrm{XOR}_2^{-1}(0) = 2$，$\mathrm{NXOR}_2^{-1}(0) = 2$ と事実 2 より，AND_2 も OR_2 も XOR_2 と NXOR_2 のどちらとも NP 同値ではない．よって，事実 3 より，AND と OR のみを用いる任意の式 $F \in \mathrm{ROF}(\mathfrak{B}^*)$ は XOR_k と NXOR_k のどちらとも NP 同値ではない．

□

命題 5.7 任意の $k, l \geq 2$ に対して，AND_k は OR_l と NP 同値ではない．

証明: 事実 1 より，任意の $k \geq 2$ に対して AND_k と OR_k が NP 同値ではないことを示せば十分である．$\mathrm{AND}_k^{-1}(0) = 1$，$\mathrm{OR}_k^{-1}(0) = 2^k - 1$ である．よって，事実 2 より，AND_k と OR_k は NP 同値ではない．

□

命題 5.8 F を一回読み $\mathfrak{B}^*$ 式とする．式 F において，ある変数 x と y が存在して，x と y の共通祖先に含まれるどの内部頂点も AND か OR でラベルづけられていると仮定する．x と y 以外の全ての変数を任意の定数に固定して得られる関数を $g(x,y)$ とする．このとき，以下が成り立つ．$\mathrm{OP}(x \sqcap_F y) = \mathrm{AND}$ であるならば，$g(x,y)$ は OR_2 と NP 同値ではない．$\mathrm{OP}(x \sqcap_F y) = \mathrm{OR}$ であるならば，$g(x,y)$ は AND_2 と NP 同値ではない．

証明: 命題の仮定より，x と y の共通祖先に含まれる内部頂点は，AND か OR でラベルづけられている．AND も OR もある一つの変数 z 以外を定数に固定することによって得られる関数は，定数関数か z をそのまま出力する関数のみである．よって，ある入力変数に対する否定を出力することはできない．ゆえに，x と y 以外を定数に固定することで得られる関数は，$\mathrm{OP}(x \sqcap_F y) = \mathrm{AND}$ であるときは $x \wedge y$ か定数関数であり，これらは OR_2 と NP 同値ではない．また，$\mathrm{OP}(x \sqcap_F y) = \mathrm{OR}$ であるときは $x \vee y$ か定数関数であり，これらは AND_2 と NP 同値ではない．

□

ここで，定理 5.8 の証明をする際に重要な役割を担う二つの技術的な補題を与える．

補題 5.9 F_1 と F_2 を $\mathrm{ROF}(\mathfrak{B}^*)$ に含まれる，同じ関数を表す異なる二つの式とする．このとき，互いに異なる任意の変数 x,y,z に対して，以下が成り立つ．

$$\mathrm{OP}(\sqcap_{F_1}\{x,y,z\}) = \mathrm{MUX} \;\Leftrightarrow\; \mathrm{OP}(\sqcap_{F_2}\{x,y,z\}) = \mathrm{MUX}, \tag{5.14}$$

$$\mathrm{OP}(x \sqcap_{F_1} y) = \mathrm{MUX} \;\Leftrightarrow\; \mathrm{OP}(x \sqcap_{F_2} y) = \mathrm{MUX}, \tag{5.15}$$

$$\mathrm{OP}(x \sqcap_{F_1} y) \in \{\mathrm{XOR}, \mathrm{NXOR}\} \;\Leftrightarrow\; \mathrm{OP}(x \sqcap_{F_2} y) \in \{\mathrm{XOR}, \mathrm{NXOR}\}, \tag{5.16}$$

$$\mathrm{OP}(x \sqcap_{F_1} y) \in \{\mathrm{OR}, \mathrm{AND}\} \;\Leftrightarrow\; s\mathrm{OP}(x \sqcap_{F_2} y) \in \{\mathrm{OR}, \mathrm{AND}\}. \tag{5.17}$$

証明: $\mathrm{OP}(\sqcap_{F_1}\{x,y,z\}) = \mathrm{MUX}$ とし，背理法で式 (5.14) を示す．(5.14) が成立しない，つまり，(i)F_2 において $\{x,y,z\}$ がある一つの頂点で合流しない，または，(ii)$\mathrm{OP}(\sqcap_{F_2}\{x,y,z\}) \neq \mathrm{MUX}$ が成立していると仮定する．事実 5.3 より，F_1 において x,y,z 以外の変数を適当な定数に固定することにより，ある $\epsilon_1,\epsilon_2,\epsilon_3 \in \{0,1\}$ に対する関数 $\mathrm{MUX}(x^{\epsilon_1}, y^{\epsilon_2}, z^{\epsilon_3})$ を得る．変数に対するこの部分割り当てを，F_2 に

おいても行うことで得られる関数を $g(x,y)$ とすると，F_1 と F_2 は同じ関数を表すため，

$$g(x,y,z) = \mathrm{MUX}(x^{\epsilon_1}, y^{\epsilon_2}, z^{\epsilon_3}) \tag{5.18}$$

でなければならない．(ii) の場合は明らかに，(i) の場合は命題 5.4 から，g は MUX を用いない一回読み $\mathfrak{B}^*$ 式で表わされる．しかし，命題 5.5 より g は $\mathrm{MUX}(x,y,z)$ と NP 同値ではないため，式 (5.18) に矛盾する．よって，$\mathrm{OP}(\sqcap_{F_2}\{x,y,z\}) = \mathrm{MUX}$ である．

次に式 (5.15) を示す．$\mathrm{OP}(x \sqcap_{F_1} y) = \mathrm{MUX}$ とする．$\mathrm{OP}(\sqcap_{F_1}\{x,y,z\}) = \mathrm{MUX}$ であるような変数 z を一つ用意してから，上記の議論を行うと $\mathrm{OP}(x \sqcap_{F_2} y) = \mathrm{MUX}$ であることが示せる．

次に $\mathrm{OP}(x \sqcap_{F_1} y) = \mathrm{XOR}$ とし，背理法で式 (5.16) を示す．($\mathrm{OP}(x \sqcap_{F_1} y) = \mathrm{NXOR}$ としたときも同様の議論が可能である)．式 (5.16) が成立しない，つまり，$\mathrm{OP}(x \sqcap_{F_2} y) \neq \mathrm{XOR}$ かつ $\mathrm{OP}(x \sqcap_{F_2} y) \neq \mathrm{NXOR}$ と仮定する．事実 5.3 より，F_1 において x と y 以外の変数を適当な定数に固定することにより，ある $\epsilon_1, \epsilon_2 \in \{0,1\}$ に対する関数 $\mathrm{PARITY}(x^{\epsilon_1}, y^{\epsilon_2})$ を得る．変数に対するこの部分割り当てを，F_2 においても行うことで得られる関数を $g(x,y)$ とすると，F_1 と F_2 は同じ関数を表すため，

$$g(x,y) = \mathrm{PARITY}(x^{\epsilon_1}, y^{\epsilon_2}) \tag{5.19}$$

でなければならない．式 (5.19) と命題 5.4 より，$\mathrm{OP}(x \sqcap_{F_2} y) \neq \mathrm{MUX}$ であるため，背理法の仮定より $\mathrm{OP}(x \sqcap_{F_2} y) = \mathrm{OR}$ または $\mathrm{OP}(x \sqcap_{F_2} y) = \mathrm{AND}$ となる．よって，g は $\{\mathrm{AND}, \mathrm{OR}\}$ 上の一回読み $\mathfrak{B}^*$ 式で表現できる．しかし，命題 5.6 より．g は $\mathrm{PARITY}(x^{\epsilon_1}, y^{\epsilon_2})$ と NP 同値ではないため，式 (5.19) に矛盾する．

式 (5.17) については，式 (5.15) と式 (5.16) より明らかに成り立つ．

□

一回読み $\mathfrak{B}^*$ 式 F に対し，F を定義する順序木の根を $r(F)$ と書く．また，$r(F)$ の子 $v_1, \ldots, v_k$ をそれぞれ根とする部分式を $F_1, \ldots, F_k$ とするとき，変数集合の分割 $\{\mathrm{var}(F_1), \ldots, \mathrm{var}(F_k)\}$ を F の根による変数分割と言う．ただし，$\mathrm{var}(F_i)$ は式 F_i に現れる変数の集合である．

補題 5.10 *2つの一回読み $\mathfrak{B}^*$ 式 F_1 と F_2 が同じ関数を表すとする．このとき，根 $r(F_1), r(F_2)$ のラベルについて，以下が成り立つ．*

$$\mathrm{OP}(r(F_1)) \in \{\mathrm{XOR}, \mathrm{NXOR}\} \Leftrightarrow \mathrm{OP}(r(F_2)) \in \{\mathrm{XOR}, \mathrm{NXOR}\}, \tag{5.20}$$

$$\mathrm{OP}(r(F_1)) = \mathrm{AND} \Leftrightarrow \mathrm{OP}(r(F_2)) = \mathrm{AND}, \tag{5.21}$$

$$\mathrm{OP}(r(F_1)) = \mathrm{OR} \Leftrightarrow \mathrm{OP}(r(F_2)) = \mathrm{OR}. \tag{5.22}$$

$$\mathrm{OP}(r(F_1)) = \mathrm{MUX} \Leftrightarrow \mathrm{OP}(r(F_2)) = \mathrm{MUX}. \tag{5.23}$$

さらに，F_1 と F_2 の根による変数分割が等しい．特に，根のラベルが MUX である場合には，左の子の部分式に含まれる変数の集合は F_1 と F_2 で等しい．

証明: F_1 の根の子の部分式を $G_1, G_2, \ldots, G_k$ とし，F_2 の根の子の部分式を $H_1, H_2, \ldots, H_l$ とする．一般性を欠くことなく，$k \geq l$ と仮定してよい．

$\mathrm{OP}(r(F_1)) = \mathrm{XOR}$ であるとして，背理法で F_1 と F_2 の根による変数分割が等しいことと式 (5.20) を示す（$\mathrm{OP}(r(F_1)) = \mathrm{NXOR}$ である場合も同様に証明できる）．まず，F_1 と F_2 の根による変数分割が等しいことを示す．F_1 の根による変数分割と F_2 の根による変数分割が異なると仮定する．すなわち，F_1 において $x \sqcap_{F_1} y = r(F_1)$ であり，F_2 において $x \sqcap_{F_2} y \neq r(F_2)$ であるような変数 x と y が存在すると仮定する．補題 5.9 より．$\mathrm{OP}(x \sqcap_{F_2} y) \in \{\mathrm{XOR}, \mathrm{NXOR}\}$ である．よって，$x \sqcap_{F_2} y$ の親を w とすると，定義 5.8 の条件 4 より，$\mathrm{OP}(w) \notin \{\mathrm{XOR}, \mathrm{NXOR}\}$ である．このとき，$z \sqcap_{F_2} x = z \sqcap_{F_2} y = w$ であるような変数 z が存在する．一方，$z \sqcap_{F_1} x = r(F_1)$，または，$z \sqcap_{F_1} y = r(F_1)$ である．すなわち，$\mathrm{OP}(z \sqcap_{F_1} x) = \mathrm{XOR}$，または，$\mathrm{OP}(z \sqcap_{F_1} y) = \mathrm{XOR}$ である．補題 5.9 より，$\mathrm{OP}(z \sqcap_{F_2} x) \in \{\mathrm{XOR}, \mathrm{NXOR}\}$，または，$\mathrm{OP}(z \sqcap_{F_2} y) \in \{\mathrm{XOR}, \mathrm{NXOR}\}$ である．よって，何れの場合も $\mathrm{OP}(w) \in \{\mathrm{XOR}, \mathrm{NXOR}\}$ となり，矛盾する．根による変数分割が等しいことから，補題 5.9 より，明らかに $\mathrm{OP}(r(F_2)) \in \{\mathrm{XOR}, \mathrm{NXOR}\}$ である．

次に，$\mathrm{OP}(r(F_1)) = \mathrm{AND}$ であるとして，背理法で F_1 と F_2 の根による変数分割が等しいことと式 (5.21) を示す（$\mathrm{OP}(r(F_1)) = \mathrm{OR}$ とすれば同様に F_1 と F_2 の根による変数分割が等しいことと式 (5.22) とを示せる）．F_1 の根による変数分割と F_2 の根による変数分割が異なると仮定する．すなわち，F_1 において $x \sqcap_{F_1} y = r(F_1)$ であり，F_2 において $x \sqcap_{F_2} y \neq r(F_2)$ であるような変数 x と y が存在するとする．

場合 1: F_2 において，x と y のある共通祖先 w が存在して，$\mathrm{OP}(w) \notin \{\mathrm{OR}, \mathrm{AND}\}$ と仮定する．このとき，$z \sqcap_{F_2} x = z \sqcap_{F_2} y = w$ であるような変数 z が存在する．一方，$z \sqcap_{F_1} x = r(F_1)$，または，$z \sqcap_{F_1} y = r(F_1)$ である．すなわち，$\mathrm{OP}(z \sqcap_{F_1} x) = \mathrm{AND}$，または，$\mathrm{OP}(z \sqcap_{F_1} y) = \mathrm{AND}$ である．補題 5.9 より，$\mathrm{OP}(z \sqcap_{F_2} x) \in \{\mathrm{OR}, \mathrm{AND}\}$，または，$\mathrm{OP}(z \sqcap_{F_2} y) \in \{\mathrm{OR}, \mathrm{AND}\}$ である．よって，何れの場合も $\mathrm{OP}(w) \in \{\mathrm{OR}, \mathrm{AND}\}$ となり，矛盾する．

場合 2: F_2 において，x と y の任意の共通祖先 w に対し，$\mathrm{OP}(w) \in \{\mathrm{OR}, \mathrm{AND}\}$ と仮定する．定義 5.8 の条件 3 より，$\mathrm{OP}(x \sqcap_{F_2} y) = \mathrm{OR}$ であるか，$x \sqcap_{F_2} y$ の親の何れかの頂点 v について $\mathrm{OP}(v) = \mathrm{OR}$ である．このとき，一般性を欠くことなく，ある変数 z が存在して，$\mathrm{OP}(x \sqcap_{F_1} z) = \mathrm{AND}$ かつ $\mathrm{OP}(x \sqcap_{F_2} z) = \mathrm{OR}$ を仮定できる．このとき，F_1 において x と z 以外の変数を定数に固定すると，$x^{\epsilon_1} \wedge z^{\epsilon_2},\ \epsilon_1, \epsilon_2 \in \{0, 1\}$ という関数を得る．変数に対する同じ固定の仕方を F_2 において行って得られる関数を $g(x, z)$ とする．F_1 と F_2 は同じ関数を表すため，$g(x, z) = x^{\epsilon_1} \wedge z^{\epsilon_2}$ でなければならない．しかし，命題 5.8 により，g は $x \wedge z$ とは NP 同値ではないため，矛盾する．

根による変数分割が等しいことを用いて，補題 5.9 より，上記 2 と同様の議論により，$\mathrm{OP}(r(F_2)) = \mathrm{AND}$ でなければならない．

最後に，$\mathrm{OP}(r(F_1)) = \mathrm{MUX}$ であるとして，F_1 と F_2 の根による変数分割が等しいことと式 (5.23) を示す．式 (5.20)，(5.21)，(5.22) が成り立つことを示したので，$\mathrm{OP}(r(F_2)) = \mathrm{MUX}$ でなければならないため，式 (5.23) が成り立つ．次に F_1 と F_2 の根による変数分割が等しいことを背理法で示す．F_1 の根による変数分割と F_2 の根による変数分割が異なると仮定する．すなわち，$\sqcap_{F_1}\{x, y, z\} = r(F_1)$ であり，$\sqcap_{F_2}\{x, y, z\} \neq r(F_2)$ であるような変数 x と y と z が存在するとする．$r(F_1)$ に対する左，中央，右の部分木をそれぞれ G_1, G_2, G_3 とし，$r(F_2)$ に対する左，中央．右の部分木をそれぞれ H_1, H_2, H_3 とする．F_1 と F_2 の表す関数が等しいので，補題 5.9 により，$\sqcap_{F_2}\{x, y, z\} = v$ かつ $\mathrm{OP}(v) = \mathrm{MUX}$ であるような頂点 v がある $1 \leq i \leq 3$ に対する H_i の中に存在する．今，$\sqcap_{F_2}\{x, y, z\} \neq r(F_2)$ であるので，$a \sqcap_{F_2} x = r(F_2)$ かつ $a \sqcap_{F_2} y = r(F_2)$ かつ $a \sqcap_{F_2} z = r(F_2)$ であるような変数 a が存在する．a は F_1 において，G_1, G_2, G_3 の何れかに含まれる．a が G_1 に含まれると仮定する（G_2 や G_3 に含まれる場合も全く同様の議論が可能である）．このとき，$\sqcap_{F_1}\{a, y, z\} = r(F_1)$ である．一方，$\{a, y, z\}$ は一つの内部頂点で合流しないため，補題 5.9 より，矛盾する．

MUX は左の子による入力により，中央の子の出力か右の子の出力かを出力する，という関数であるため，F_1 の表す関数と F_2 の表す関数が等しくなるためには，$\mathrm{var}(G_1) = \mathrm{var}(H_1)$ でなければならないこともわかる．

□

5.5.5　定理 5.8 の証明

いよいよ定理 5.8 の証明を与える．

証明: $\mathbb{F}$ と $\mathbb{G}$ を $\mathbb{F} \simeq_{\mathrm{NP}} \mathbb{G}$ であるような標準骨格式とする．$\mathbb{F} = \mathbb{G}$ を骨格式の深さの帰納法によって示す．

NP 同値である二つの標準骨格式を $\mathbb{F}$ と $\mathbb{G}$ とする．標準骨格式の深さによる帰納法によって証明を行う．

（基底段階）$\mathbb{F}$ の深さが 0 の場合を考える．このとき，$\mathbb{F}$ は葉のみからなる．事実 1 より，$\mathbb{G}$ も葉のみでなければ $\mathbb{F}$ と NP 同値にならない．よって，$\mathbb{F}$ と $\mathbb{G}$ の骨格式は等しくなければならない．

（帰納段階）一般性を欠くことなく，$\mathbb{F}$ の深さが $\mathbb{G}$ の深さ以上であると仮定できる．$\mathbb{F}$ の深さを d とする．ある演算子 op_1 と op_2 に対して，$\mathbb{F} = op_1(\mathbb{F}_1, \ldots, \mathbb{F}_k)$ $(k \geq 2)$，$\mathbb{G} = op_2(\mathbb{G}_1, \ldots, \mathbb{G}_l)$ $(l \geq 2)$ である．$\mathbb{F} \simeq_{\mathrm{NP}} \mathbb{G}$ であるので，

$$\mathbb{F}(x_1, \ldots, x_n) = \mathbb{G}(x_{\pi(1)}^{\tau_I(1)}, \ldots, x_{\pi(n)}^{\tau_I(n)})$$

であるような $\boldsymbol{\tau}_I \in \{0,1\}^n$ と $\{1, \ldots, n\}$ 上の置換 π が存在する．上記の左辺の式と右辺の式をそれぞれ F，G とする．式 F については，各 $1 \leq i \leq k$ に対して $\mathbb{F}_i = F_i$ であるような $F = op_1(F_1, \ldots, F_k)$ であり，式 G については，各 $1 \leq i \leq l$ に対して $\mathbb{G}_i = G_i$ であるような $G = op_2(G_1, \ldots, G_l)$ であることに注意されたい．

ここで，帰納法の仮定を用いることで初めて示せる主張を以下に示す．この主張は後の議論で用いる．

主張 5.11 深さ $d-1$ 以下の任意の標準骨格式 $\mathbb{H}_1, \mathbb{H}_2$ に対し，$\mathbb{H}_1$ の表す関数を h_1，$\mathbb{H}_2$ の表す関数を h_2 とする．$h_1 \simeq_{\mathrm{NP}} \bar{h}_2$ のとき，

$$\mathbb{H}_1 = \overline{\mathbb{H}}_2$$

が成り立つ．さらに，$\mathbb{H}_1$ が P 型ならば $\mathbb{H}_2$ は N 型である．$\mathbb{H}_1$ が N 型ならば $\mathbb{H}_2$ は P 型である．

証明: 補題 5.6 より，$\overline{\mathbb{H}}_2$ は標準形である．また命題 5.2 より，$\overline{\mathbb{H}}_2$ の表す関数は $\bar{h}_2$ と NP 同値の関数である．よって $h_1 \simeq_{\mathrm{NP}} \bar{h}_2$ より，$\mathbb{H}_1$ と $\bar{\mathbb{H}}_2$ は NP 同値である．$\mathbb{H}_1$ と $\bar{\mathbb{H}}_2$ はともに深さが $d-1$ 以下であるため，帰納法の仮定から定理 5.8 が成立するので，$\mathbb{H}_1 = \bar{\mathbb{H}}_2$ となる．

□

根のラベルについての場合分けで証明を行う．

場合 1: $op_1 = \mathrm{AND}$ の場合．

$op_1 = \mathrm{OR}$ の場合も同様の議論で証明できる．F と G は同じ関数を表すので，補題 5.10 より $\mathrm{OP}(r(G)) = \mathrm{AND}$ であり，かつ，F と G の根による変数分割が等しくなければならない．よって，$k = l \geq 2$ であり，$\{\mathrm{var}(F_1), \mathrm{var}(F_2), \ldots, \mathrm{var}(F_k)\} = \{\mathrm{var}(G_1), \mathrm{var}(G_2), \ldots, \mathrm{var}(G_k)\}$ である．$op_1 = \mathrm{AND}$ であるので，F の出力が F_1 となるように F_1 に含まれる変数を除いた他の変数を定数に割り当てる，ある部分割り当てが存在する．変数に対する同様の部分割り当てを G においても行うと，G の変数分割が F と等しいことと，根のラベルが AND であることから，ある $1 \leq i \leq k$ に対する G_i を得る．F と G の表す関数が等しいことから，F_1 と G_i の表す関数も等しい．よって，帰納法の仮定から $\mathbb{F}_1 = \mathbb{G}_i$ を得る．このように，各 $F_j (1 \leq j \leq k)$ に対して，対応する骨格式が等しい $G_{i_j} (1 \leq i_j \leq k)$ が一意に存在する．$\mathbb{F}$ と $\mathbb{G}$ が標準骨格式であることから，$\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k$ $(k \geq 2)$ と $\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k$ はそれぞれ降順に並んでいるため，各 $1 \leq j \leq k$ に対して $\mathbb{F}_j = \mathbb{G}_j$ となる．よって，$\mathbb{F} = \mathbb{G}$ である．

場合 2: $op_1 = \mathrm{XOR}$ の場合．

$op_1 = \mathrm{NXOR}$ の場合も同様の議論で証明できる．F と G は同じ関数を表すので，補題 5.10 より，$op_2 = \mathrm{XOR}$ または $op_2 = \mathrm{NXOR}$ であり，かつ，F と G の根による変数分割が等しくなければならない．よって，$k = l \geq 2$ であり，$\{\mathrm{var}(F_1), \mathrm{var}(F_2), \ldots, \mathrm{var}(F_k)\} = \{\mathrm{var}(G_1), \mathrm{var}(G_2), \ldots, \mathrm{var}(G_k)\}$ である．$op_1 = \mathrm{XOR}$ であるので，場合 1 と同様の議論により，F_j $(1 \leq j \leq k)$ に対応する G_{i_j} $(1 \leq i_j \leq k)$ が一意に存在して，G_{i_j} の表す関数は F_j の表す関数か F_i の出力否定関数である．

まず，$op_2 \neq \mathrm{NXOR}$ であることを背理法で示す．$op_2 = \mathrm{NXOR}$ と仮定する．$op_1 = \mathrm{XOR}$ かつ $op_2 = \mathrm{NXOR}$ であるので，各 $1 \leq j \leq k$ に対する G_{i_j} が F_j と同じ関数を表すことはなく，少なくとも一つの G_{i_j} は F_j の表わす関数の出力否定関数を表す式でなければならない．$\mathbb{F}$ は標準骨格式であるため，$\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k$ はそれぞれ自己双対型か P 型である．$\{\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k\}$ の中に自己双対型の骨格式 F_i が存在した場合は，$\mathbb{G}_{i_j}$ も自己双対型でなければならない．これは，$\mathbb{G}$ が標準形であることに矛盾する．$\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k$ が全て P 型である場合は，主張 5.11 より $\mathbb{G}_i$ は N 型となるが，これは $\mathbb{G}$ が標準骨格式であることに矛盾する．ゆえに，$op_2 \neq \mathrm{NXOR}$

である．

よって，$op_2 = \mathrm{XOR}$ でなければならない．$\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k$ はそれぞれ自己双対型か P 型である．$\{\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k\}$ の中に自己双対型の骨格式 F_i が存在した場合は，$\mathbb{G}_{i_j}$ も自己双対型でなければならない．この場合，自己双対型の定義から $\mathbb{F}_i$ と $\mathbb{G}_{j_i}$ は NP 同値となるため，帰納法の仮定から $\mathbb{F}_i = \mathbb{G}_{j_i}$ となる．次に，$\{\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k\}$ の中に自己双対型の骨格式 F_i が存在しない場合，つまり，$\{\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k\}$ が全て P 型である場合を考える．$\mathbb{F}_i$ $(1 \leq i \leq k)$ が P 型であるとき，G_{j_i} が F_i の出力否定関数を表すと仮定すると，主張 5.11 により，$\mathbb{G}_{j_i}$ は N 型となる．これは $\mathbb{G}$ が標準骨格式であることに矛盾するため，F_i と G_{j_i} の表す関数が等しくなければならない．このとき，帰納法の仮定から F_i と G_{j_i} の骨格式は等しい．以上のことから，各 $F_j (1 \leq j \leq k)$ に対して，対応する骨格式が等しい $G_{i_j} (1 \leq i_j \leq k)$ が一意に存在する．$\mathbb{F}$ と $\mathbb{G}$ が標準骨格式であることから，$\mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_k$ と $\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k$ はそれぞれ降順に並んでいるため，各 $1 \leq j \leq k$ に対して $\mathbb{F}_j = \mathbb{G}_j$ となる．よって，$\mathbb{F} = \mathbb{G}$ である．

場合 3: $op_1 = \mathrm{MUX}$ の場合.

補題 5.10 により，$op_2 = \mathrm{MUX}$ かつ，F と G の変数分割が等しく，特に左の子供の部分式 F_1 に含まれる変数集合は等しい．すなわち，$F = \mathrm{MUX}(F_1, F_2, F_3)$，$G = \mathrm{MUX}(G_1, G_2, G_3)$ とすると，$\mathrm{var}(F_1) = \mathrm{var}(G_1)$，$\{\mathrm{var}(F_2), \mathrm{var}(F_3)\} = \{\mathrm{var}(G_2), \mathrm{var}(G_3)\}$ となる．F と G の表す関数は同じなので，$G_1 = F_1$ または $G_1 = \bar{F_1}$ である．まず $G_1 = F_1$ である場合を考える．このとき，F と G の表す関数は同じであるので $G_2 = F_2$ かつ $G_3 = F_3$ である．よって，帰納法の仮定より，$\mathbb{G}_1 = \mathbb{F}_1$ かつ $\mathbb{G}_2 = \mathbb{F}_2$ かつ $\mathbb{G}_3 = \mathbb{F}_3$ であるから，$\mathbb{F}$ と $\mathbb{G}$ は同じ骨格式である．次に $G_1 = \bar{F_1}$ の場合を考える．このとき，F と G の表す関数は同じであるので $G_2 = F_3$ かつ $G_3 = F_2$ である．よって，$\mathbb{F}_2 = \mathbb{F}_3$ でなければならない．なぜなら，$\mathbb{F}_2 \neq \mathbb{F}_3$ であるとした場合，F において $\mathbb{F}_2 > \mathbb{F}_3$ であるか，G において $\mathbb{G}_2 > \mathbb{G}_3$ であるか，のいずれかが生じるが，どちらも標準骨格式の定義を満たさないからである．さらに，$\mathbb{F}_1$ は自己双対型でなければならない．なぜなら，$\mathbb{F}_1$ が自己双対型でなければ，主張 5.11 より，$\mathbb{F}_1$ か $\mathbb{G}_1$ のどちらかが N 型となり，標準骨格式の定義を満たさないからである．以上より，$G_1 = F_1$ の場合も $G_1 = \bar{F_1}$ の場合も，$\mathbb{F}$ と $\mathbb{G}$ は等しい．

□

5.6　まとめと今後の課題

本章で示した結果は以下の二つである．一つ目は，ADV タイトな関数からなる任意の基底 $\mathfrak{B}$ 上の最簡化可能なブール式のクラス $C_{\mathfrak{B}}$ を定義したことである．二つ目は，標準骨格式を定義し，標準骨格式が $\mathrm{ROF}(\mathfrak{B})$ の NPN 同値類の代表とできることを示したことである．$C_{\mathfrak{B}^*}$ は $\mathrm{ROF}(\mathfrak{B})$ の部分集合であるので，$C_{\mathfrak{B}^*}$ に対しても標準形骨格式は NPN 同値類の代表とできる．$C_{\mathfrak{B}^*}$ と $\mathrm{ROF}(\mathfrak{B})$ に対する標準骨格式は計算機で容易に生成することができる．表 5.1 において，変数の数が 10 までの $C_{\mathfrak{B}^*}$ と $\mathrm{ROF}(\mathfrak{B})$ に対する標準骨格式の数を示す．

クラス $\mathrm{ROF}(\mathfrak{B}^*)$ は所属性質問と等価性質問を用いると多項式時間で学習可能であるという良い性質を持つ [8]．上記の結果と標準骨格式の性質を用いると，クラス $\mathrm{ROF}(\mathfrak{B}^*)$ に対する新たなブーリアンマッチングアルゴリズム A を与えることができる．ブーリアンマッチングとは与えられた二つのブール関数が NPN 同値であるかどうかを決定する問題であり，論理合成のテクノロジマッピングの分野において，与えられた部分回路と等価なライブラリセルを見つけるために用いられる．A は次のような非常に単純なアルゴリズムである．与えられた二つのブール関数に対してそれらを表す一回読み式を特定するために，Bshouty らの学習アルゴリズムを用いる．そして，得られた二つの式に対する標準骨格式が同じであるかどうかを調べる．

アルゴリズム $\mathrm{canonicalize}(F)$ は，次に述べる少し変更を加えることで，$O(n \log n)$ で動作させることができる．ここで，n は入力される式 F のサイズである．その変更とは，F の骨格式 $\mathbb{F}$ と同時に F の否定骨格式 $\bar{\mathbb{F}}$ も $\mathrm{canonicalize}(F)$ に出力させる．

今回我々が示した最簡化可能な式のクラスは一回読みという強い制約があるため，実際に生成することに対する利益はそれほど大きくないという欠点がある．今後の課題としては，より複雑な関数のクラスに対する最簡な式の導出法の確立することである．

表 5.1: $C_{\mathfrak{B}^*}$ と $\mathrm{ROF}(\mathfrak{B}^*)$ に対する標準骨格式の数.

変数の数	1	2	3	4	5	6	7	8	9	10
$C_{\mathfrak{B}^*}$ に対する標準骨格式の数	2	4	8	20	52	170	534	1840	6395	23252
$\mathrm{ROF}(\mathfrak{B}^*)$ に対する標準骨格式の数	2	4	10	32	122	449	2453	12654	65761	349036

第6章　結論

理論計算機科学の分野では，チューリング機械や論理回路などの計算モデル上で，与えられた問題を解くために必要となる時間的・空間的リソースの量を問題の複雑さと定め，多くの研究者たちが様々なブール関数の複雑さを解き明かそうと努力を続けている．

本研究では，論理回路から派生した計算モデルであるブール式モデル，量子回路を基とした計算モデルである量子質問モデルの下で，ブール関数の複雑さの下界を明らかにするというアプローチを取った．特に，量子質問モデルについては，2 乗ギャップ予想の真偽の究明に取り組んだ．2 乗ギャップ予想とは以下のようなものであった．

2 乗ギャップ予想 [5] 任意のブール関数 f と $\epsilon \in [0, 1/2)$ に対して，

$$Q_\epsilon(f) = \Omega(\sqrt{D(f)}).$$

この予想の解決に貢献できる結果として，第 3 章において，パリティノード付き一回読み決定木が計算する任意の関数に対して 2 乗ギャップ予想が成立すること（定理 3.6）を示した後，その結果を拡張し，一回読み $\mathcal{B}$ 式で表現される任意の関数に対しても 2 乗ギャップ予想が成立すること（定理 3.12）を示した．ここで，$\mathcal{B} = \{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}, \mathrm{XOR}, \mathrm{MUX}\}$ である．これらの結果は，2 乗ギャップ予想の正当性をさらに強める証拠を与えたといえる．2 乗ギャップ予想に関する定理の導出のために，まず，パリティノード付き一回読み決定木に対する複雑さ指標として，ソフトランクという指標を導入した（定義 3.2）．そして，ソフトランクが量子質問複雑さの下界を与えること（定理 3.5），および決定木の深さの 2 乗根がソフトランクの下界を与えること（命題 3.2）を示すことによって，2 乗ギャップ予想が成立すること（定理 3.6）を示した．次に，ソフトランクと決定木深さの定義域をブール式に拡張し（定義 3.4），パリティ付き一回読み決定木の場合と同様の議論を行うことによって一回読み $\mathfrak{B}$ 式のクラスに対しても 2 乗ギャップ予想が成立すること（定理 3.12）を示した．

ブール式モデルにおいては，まず第 4 章でブール式複雑さの下界を導出する新しい手法の提案を行った．具体的には，整数計画問題によって定式化されている従来の下界指標である長方形分割数を基に新たな下界指標としてシングルトン被覆数を提案した．k 入力マルチプレクサ関数に対して，長方形分割数を線形緩和した指標とそれを改良した Ueno の指標との比較を行った．我々が提案した指標は，コミュニケーション行列のシングルトンという特殊なセルに着目して提案した指標であり，整数計画問題である．一方，他の二つは線形計画問題であるため，扱いやすさでは他の二つの指標に劣るものの，整数計画問題であるがゆえに大きな下界を導出できる可能性があり，一方で長方形分割よりは扱いが容易であるという利点がある．実際，8 入力マルチプレクサ関数に対して，他の二つの指標より我々の指標の方が真に大きな下界を導出できることを示した（定理 4.8，定理 4.9）．

ブール式モデルにおいてはさらに，非常に困難ではあるが意義の大きい次のような問題に第 5 章で取り組んだ．それは，ある広いクラスのブール式の最小表現を導出する一般的手法の開発である．まず，Khrapchenko のパリティ関数に対する最簡な式の構成法を考察し，最簡化可能という概念を定義した．基底 $\mathfrak{B}$ 上のブール式が最簡化可能とは，現れる演算子をその演算子を表す最簡な標準基底ブール式で置き換えることで，最簡な標準基底ブール式が得られることである（定義 5.4）．本研究では，基底を $\mathfrak{B} = \{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}, \mathrm{XOR}, \mathrm{MUX}\}$ としたとき，ある条件を満たす任意の一回読みブール式が最簡化可能であること（定理 5.5）を示した．本研究で与えた最簡化可能なブール式のクラスはパリティ関数を含むので，定理 5.5 は Khrapchenko の結果の拡張と言えるだけではなく，最簡なブール式を導出する一般的手法開発の第一歩となったとは言えるだろう．次に，構造が本質的に異なる一回読み $\mathfrak{B}$ 式のみを含むクラスを，標準骨格式の概念を用いて構成した．具体的には，任意の一回読み $\mathfrak{B}$ 式 F は F と NPN 同値な関数を表す標準骨格式に変形できること（定理 5.7），異なる標準骨格式が表す関数は NPN 同値ではないことを示すことにより，標準骨格式のクラスが一回読み $\mathfrak{B}$ 式のクラスの NPN 代表元からなること（定理 5.8）を示した．定理 5.5，定理 5.7，定理 5.8 ををを全て用いると，対象のクラスを一回読み $\mathfrak{B}$ 式としたときの，最簡なブール式で本質的に構造の異なる式を特徴づけられる．また，最簡な式の形の一意性に関する結果でもあるので，Tarui の結果 [26] とも関係し，その方向でも今後貢献できる可能性がある．

今後の課題としては，本論文の第 3 章と第 5 章の結果は一回読み $\mathfrak{B}$ 式に対する結果であったが，基底 $\mathfrak{B}$ を拡張することにより，上記の章で導いた定理の適用範囲を広げるということがある．一回読みという制約は非常に強いものであるが，基

底 $\mathfrak{B}$ に新たにブール関数を加えることで，一回読み $\mathfrak{B}$ 式の表す関数のクラスを大きくすることができる．基底に加えるブール関数の性質は，ブール式複雑さの値と量子敵対者限界の 2 乗の値が一致する，もしくは，非常に近いことが望ましい．ブール式複雑さの値と量子敵対者限界の 2 乗の値が一致するブール関数を見つけるためには，5.2 節で示した最簡な式の生成アルゴリズムが有用である．ただし，このアルゴリズムの計算時間は，基とする下界指標の値を計算する時間に大きく依存する．ブール関数の入力変数の数が多くなってくると，下界指標によっては実際に計算することが困難になることがあることに注意されたい．例えば，入力変数の数が 7 以上になるとスーパーコンピューターを用いても，量子敵対者限界の値を計算することは困難である．

また，一回読みという制約を緩和することは挑戦的な課題である．一回読みの制約は，量子敵対者限界の合成関数に対する定理 2.7 を利用していることに起因する．よって，一回読みの制約を緩和するためには，定理 2.7 を改善する必要がある．しかし，量子計算の議論を用いた証明を行う必要があり，現時点では手掛かりは見つかっていない．

ブール式の分野における課題としては，超多項式のブール式複雑さの下界を導出することがある．この課題の解決のためには，大きな下界を与える下界指標を用いる必要がある．長方形分割数や本論文で提案したシングルトン被覆数は任意のブール関数に対する上界が知られていないため，超多項式の下界を導出できる可能性がある．一方，量子敵対者限界はそのまま用いるだけでは超多項式のブール式複雑さの下界の導出できない．なぜなら，任意のブール関数に対して，量子敵対者限界は入力変数の 2 乗が上界であるからである．これは，決定的質問複雑さの自明な上界が入力変数の数 n であることから直ちに導かれる．

謝辞

本研究を行うにあたり，多大なる御指導，御鞭撻を賜りました東北大学大学院情報科学研究科 西関隆夫教授に心から感謝致します．本研究の本研究への有益な御助言，熱心な御指導を頂きました九州大学大学院システム情報科学研究院 瀧本英二教授に深く感謝致します．本研究に対する貴重な御意見，御討論を頂きました群馬大学大学院工学研究科 天野一幸准教授に厚く御礼申し上げます．

そして，本論文の審査をしてくださり，有意義な御討論を頂きました東北大学大学院情報科学研究科 篠原歩教授，徳山豪教授に深く感謝致します．

有益な御討論を頂きました西関研究室の皆さま，特に内澤啓助教に心より感謝の意を表します．私が九州大学に特別研究学生として滞在した期間において，貴重な御討論を頂きました，竹田正幸教授，坂内英夫准教授，畑埜晃平助教に深く感謝致します．最後に，有意義な御討論を頂きました，九州大学の竹田研究室，鈴木研究室，池田研究室の皆さまに深く感謝致します．

参考文献

[1] S. Aaronson. The limits of quantum computers. *Scientific American*, 298(3):62–69, 2008.

[2] K. Amano. A procedure that generates a class of optimal boolean formulas. Technical Report 2006-AL-106, IPSJ SIG, 2006.

[3] A. Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002.

[4] A. Ambainis. Polynomial degree vs. quantum query complexity. *Journal of Computer and System Sciences*, 72(2):220–238, 2006.

[5] H. Barnum and M. Saks. A lower bound on the quantum query complexity of read-once functions. *Journal of Computer and System Sciences*, 69(2):244–258, 2004.

[6] H. Barnum, M. Saks, and M. Szegedy. Quantum decision trees and semidefinite programming. In *Proc. of 18th IEEE Conference on Computational Complexity*, pp.179–193, 2003.

[7] R. Beals, E. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4):778–797, 2001.

[8] N. Bshouty, T.Hancock, and L. Hellerstein. Learning boolean read-once formulas over generalized bases. *Journal of Computer and System Sciences*, 50(3):521–542, 1995.

[9] A. Ehrenfeucht and D. Haussler. Learning decision trees from random examples. *Information and Computation*, 82(3):231–246, 1989.

[10] L.K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. 28th ACM Symposium on Theory of Computing (STOC '96)*, pp.212–219, 1996.

[11] J. Håstad. The shrinkage exponent of de morgan formula is 2. *SIAM Journal on Computing*, 27(1):48–64, 1998.

[12] P. Høyer, T. Lee, and R. Špalek. Tight adversary bounds for composite functions. arXiv:quant-ph/0509067v3, 2006.

[13] P. Høyer, T. Lee, and R. Špalek. Negative weights make adversaries stronger. In *Proc. 39th ACM Symposium on Theory of Computing (STOC '07)*, pp.526–535, 2007.

[14] P. Høyer and R. Špalek. Lower bounds on quantum query complexity. *Bulletin of the EATCS*, 87, 2005.

[15] K. Iwama and H. Morizumi. An explicit lower bound of $5n - o(n)$ for boolean circuits. In *Proc. 27th MFCS*, pp.353–364, 2002.

[16] M. Karchmer, E. Kushilevitz, and N. Nisan. Fractional covers and communication complexity. *SIAM Journal on Discrete Mathematics*, 8(1):76–92, 1995.

[17] M. Karchmer and A. Wigderson. Monotone circuits for connectivity require super-logarithmic depth. *SIAM Journal on Discrete Mathematics*, 3(2):255–265, 1990.

[18] P. Kaye, R. Laflamme, and M. Mosca. *An Introduction to Quantum Computing*. Oxford University Press, 2007.

[19] V.M. Khrapchenko. Complexity of the realization of a linear function in the case of $\prod$-circuits. *Mathematical Notes of the Academy of Science*, 9:21–23, 1971.

[20] E. Koutsoupias. Improvements on Khrapchenko's theorem. *Theoretical Computer Science*, 116(2):399–403, 1993.

[21] S. Laplante, T. Lee, and M. Szegedy. The quantum adversary method and classical formula size lower bounds. In *Proc. 20th IEEE Conference on Computational Complexity*, pp.76–90, 2005.

[22] S. Laplante and F. Magniez. Lower bounds for randomized and quantum query complexity using kolmogorov arguments. In *Proc. 19th IEEE Conference on Computational Complexity*, pp.294–304, 2004.

[23] G. Midrijanis. Exact quantum query complexity for total boolean functions. arXiv:quant-ph/0403168v2, 2004.

[24] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[25] D. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26:1474–1483, 1997.

[26] J. Tarui. Smallest formulas for parity of 2^k variables are essentially unique. In *COCOON '08: Proceedings of the 14th Annual International Conference on Computing and Combinatorics*, pp.92–99. Lect.Note in Computer Science Vol.5092, Springer-Verlag, 2008.

[27] K. Ueno. A stronger LP bound for formula size lower bounds via clique constraints. In *Symposium on Theoretical Aspects of Computer Science 2009 (STACS 2009)*, pp.685–696, 2009.

[28] R. Špalek and M. Szegedy. All quantum adversary methods are equivalent. In *Proc. 32nd International Colloquium on Automata, Languages and Programming (ICALP 2005)*, pp.1299–1322, 2005.

[29] I. Wegner. *The Complexity of Boolean Functions*. Wiley-Teubner, 1991.

[30] A. Yao. Quantum circuit complexity. In *Proc. 34th Annual IEEE Symposium on Foundations of Computer Science*, pp.352–361, 1993.

公表目録

H. Fukuhara, E. Takimoto and K. Amano. NPN-representatives of a set of optimal Boolean formulas. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* (accepted).

H. Fukuhara and E. Takimoto. Lower bounds on quantum query complexity for read-once formulas with XOR and MUX operators. *IEICE Transactions on Information and Systems*, Vol.E93-D, No.2 (in press), Feb. 2010.

H. Fukuhara and E. Takimoto. Lower bounds on quantum query complexity for read-once formulas with XOR and MUX operators. *AAAC 09*, pp.8, 2009.

H. Fukuhara and E. Takimoto. Lower bounds on quantum query complexity for read-once decision trees with parity nodes. *Proceedings of the fifteenth Computing: The Australasian Theory Symposium*, pp.91–100, 2009.

H. Fukuhara and E. Takimoto. Lower bounds on quantum query complexity for decision trees. 電子情報通信学会技術研究報告 (コンピュテーション研究会), Vol.108, No.237 , pages 47–54, 2008 年.

H. Fukuhara, K. Amano and E. Takimoto. On formula size lower bounds for synthesis of Boolean functions over disjoint sets of variables. 電子情報通信学会 総合大会 COMP-NHC 学生シンポジウム, S3-S4, 2007 年.

H. Fukuhara, K. Amano and E. Takimoto. On formula size lower bounds for synthesis of Boolean functions over disjoint sets of variables. *Proceedings of the Joint International Conference of Fourth International Symposium on System Construc-*

tion of Global-Network-Oriented Information Electronics and Student-Organizing International Mini-conference on Information Electronics System, pp.364–365, 2007.

福原 秀明, 天野 一幸, 瀧本 英二. パリティ合成関数に対するブール式のサイズの下界について. 夏の LA シンポジウム, pp.22.1–22.7, 2006 年.