論文内容の要旨

論文題目　Complexity-Theoretical Aspects
of Quantum Computational Models
(計算量的観点における量子計算モデルの計算能力)

氏名　小林 弘忠

Deutsch によって初めて量子計算の数学的モデルが提案されて以来，多くの研究によって量子計算の古典計算に対する計算能力の優位性が示されてきた．その代表例が，Shor の素因数分解アルゴリズムである．一方で，計算モデルによっては，その量子モデル版を考えても優位性が得られない場合や，逆に古典モデルより能力が弱くなってしまう場合があることも知られている．さらに，対話型証明のように高等なモデルや有限状態オートマトンのように能力が制限されたモデルにおいては，量子モデル化がどのような効果をもたらすかが不明な場合が多く，このようなモデルの量子版の能力を解析することは，量子計算が古典計算に比べどの程度優れているのか，あるいは，どのような状況下で量子計算が優位性を発揮できるのか，といった疑問を解明する糸口として重要と考えられる．そこで，本論文では，対話型証明に関連深い計算モデルとしては，多証明者対話型証明に，有限状態オートマトンに関連深いモデルとしては，カウンタオートマトンにそれぞれ焦点を当て，その量子版の能力を解析する．

証明者が一人だけの対話型証明に関しては，その量子版が Watrous によって定義され，複数の研究により，古典モデルより強力なことを示すいくつかの性質が分かっている．しかしながら，証明者が複数いる場合のモデルの量子版はこれまで未定義であるため，本論文ではまず，量子多証明者対話型証明の定義を，Watrous の定義を拡張することにより与える．量子多証明者対話型証明としては，証明者間に事前の量子相関を許す場合と許さない場

合の二つの自然なモデルが考えられる．本論文では特に後者に焦点を当て，証明者間に事前の量子相関のない量子多証明者対話型証明を持つ言語クラスが古典計算量クラス NEXP と一致することを示す．この結果は，証明者が一人の場合とは対照的に，多証明者対話型証明においては，証明者間の事前量子相関がなければ，量子モデルと古典モデルの間に計算量的な能力の差が出ないことを意味する．これに関連して，証明者が一人だけの対話型証明においても，証明者が自分だけが扱える量子空間を持たない場合には，量子対話型証明を持つ言語クラスは NEXP と一致することも示す．これらの結果は，古典計算量のクラスを量子計算の観点から正確に特徴付けた数少ない例の一つとしても非常に興味深い．さらに，証明者間に高々多項式で抑えられる数の量子ビット数の事前量子相関を許しても，量子多証明者対話型証明を持つ言語クラスは NEXP に含まれることも示す．

これらの結果とは対照的に，本論文ではさらに，以下のような多証明者対話型証明の特殊な場合，つまり，証明者達が検証者に最初に各 1 回のみ証拠を送り，検証者には質問が許されない場合には，量子モデルと古典モデルの間に構造的な違いがあることを指摘する．この場合，古典モデルにおいては，証明者が複数いることと一人だけいること，つまり，証拠が複数送られることとただ一つのみ送られることは本質的に同等である．しかしながら，量子モデルにおいては，証拠が量子状態として複数独立に送られる場合，全体としての証拠列は各証拠のテンソル積として表されるため，検証者はそのテンソル積の構造を検証に利用できる可能性がある．この理由から，量子モデルにおいては，証拠が複数送られることとただ一つのみ送られることは本質的に異なると考えられる．そこで本論文では，証拠が複数送られる場合の検証者の計算能力をさらに追求し，任意の定数 k に対し，k 個の量子状態の証拠を受け取って “no” 側の片側有限誤り確率で効率的に検証できる言語は，2 個の量子状態の証拠を受け取るのみでも “no” 側片側有限誤り確率で検証できることを示す．また，正確な検証や “yes” 側片側誤りでの検証の場合には，量子証拠を複数利用しても検証能力は変わらないことも示す．さらに，量子証拠を用いて正確に検証可能な，あるいは “yes” 側片側誤りで検証可能な言語クラスは，NP のもう一つの量子的一般化であるクラス NQP に含まれることも示す．

一方，能力が限定されたモデルであるカウンタオートマトンに関しては，本論文では 1 方向 1 カウンタオートマトンと 2 方向 1 カウンタオートマトンの二つを考える．1 方向 1 カウンタオートマトンに関しては，その量子版が Kravtsev によって定義され，いくつかの非文脈自由言語を有限誤り確率で認識できることが示されている．本論文では，1 方向量子 1 カウンタオートマトンの性質をさらに解明するために，その能力を 1 方向決定性 1 カウンタオートマトン，及び，1 方向確率可逆 1 カウンタオートマトンと比較する．本論文ではまず，新たな非文脈自由言語の族 $\{L_{\mathrm{eq}(k)}\}$, $L_{\mathrm{eq}(k)} = \{a_1^m a_2^m \cdots a_k^m \mid m \geq 1\}, k \geq 1$, が 1 方向確率可逆 1 カウンタオートマトンで有限誤り確率で認識できることを示し，さらに量子干渉効果をうまく用いることにより，1 方向量子 1 カウンタオートマトンで受理確率を改善できることを示す．一方で，1 方向量子 1 カウンタオートマトンでは有限誤り確率で認識できない正則言語 $L_{\mathrm{last}} = \{\{a,b\}^* a\}$ の存在も示す．これらの結果は，ごく最近に Bonner, Freivalds, Kravtsev によって得られた，1 方向量子 1 カウンタオートマトンでは有限誤り

確率で認識可能だが，1 方向確率 1 カウンタオートマトンでは有限誤り確率では認識できない言語の存在を示す結果と合わせて，1 方向量子 1 カウンタオートマトンと各古典 1 方向 1 カウンタオートマトンの間の認識可能な言語クラスの関係を完全に解明する．

さらに，本論文では，2 方向量子 1 カウンタオートマトンを定義し，その能力を 2 方向決定性 1 カウンタオートマトンと比較する．まず，カウンタ用のテープの長さが有界であれば，2 方向決定性 1 カウンタオートマトンが 2 方向可逆 1 カウンタオートマトンで模倣可能なことを示し，さらに，2 方向決定性 1 カウンタオートマトンでは認識できない非文脈自由言語 $L_{\mathrm{square}} = \{a^m b^{m^2} \mid m \geq 1\}$ と $L_{\mathrm{prod}} = \{a^{m_1} b^{m_2} c^{m_1 m_2} \mid m_1, m_2 \geq 1\}$ が，2 方向量子 1 カウンタオートマトンで任意に小さい “no” 側片側定数誤り確率で，多項式時間内に認識可能なことを示す．すなわち，有界な長さのカウンタテープを用いた実際的なモデルにおいては，2 方向量子 1 カウンタオートマトンは 2 方向決定性 1 カウンタオートマトンより真に強力であることが示される．他にも，$L_{\mathrm{power}} = \{a^m b^{2^m} \mid m \geq 1\}$ などの非文脈自由言語が 2 方向量子 1 カウンタオートマトンで任意に小さい “no” 側片側定数誤り確率で認識可能なことも示す．