Blier-Tapp QMA プロトコルの健全性について

中川　翔太 * 西村　治道 *
mu301012@edu.osakafu-u.ac.jp　hnishimura@mi.s.osakafu-u.ac.jp
*大阪府立大学
〒 599-8531 大阪府堺市中区学園町１－１
TEL: 072-252-9693　FAX: 072-254-9930

あらまし　Blier と Tapp は，エンタングルメントを持たない２人の証明者から短い量子証明を受け取るような **QMA**(量子 **NP**) プロトコルとして，**NP** 完全問題を完全性と健全性のギャップが $\frac{1}{n^6}$ 程度となるように解く方法を考案した．本論文では，このプロトコルをもとにして，完全性と健全性のギャップを改良する．

キーワード　量子計算量，QMA，エンタングルメント

On the Soundness of the Blier-Tapp QMA Protocol

Shota Nakagawa * Harumichi Nishimura *
mu301012@edu.osakafu-u.ac.jp　hnishimura@mi.s.osakafu-u.ac.jp
*Osaka Prefecture University
1-1 Gakuen-cho Naka-ku Sakai-shi Osaka Pref.
TEL: +81-72-252-9693　FAX: +81-72-254-9930

Abstract　Blier and Tapp developed the method of solving a **NP**-complete problem as a **QMA** protocol which receives short quantum proofs from two provers without entanglement so that the gap between completeness and soundness may become approximately $\frac{1}{n^6}$. This paper shows that the gap is improved based on this protocol.

key words　quantum computational complexity, QMA, entanglement

1 はじめに

QMA とは，クラス **NP**(厳密にはその確率版である **MA**) を量子版に拡張した量子計算量クラスである．つまり，それは証明者から送られた多項式長の量子証明をもとに, 検証者が量子コンピュータにより効率的にチェックできる言語のクラスである (詳細は論文 [7] を参照)．**QMA** の亜種として, Kobayashi, Matsumoto, Yamakami によって, 証明者が 2 人になった $\mathbf{QMA}(\mathbf{2})$ というクラスが導入された [5]．古典のクラス **MA** は，証明者が 1 人でも 2 人でも能力に差異がないことが知られている．一方，$\mathbf{QMA} = \mathbf{QMA}(\mathbf{2})$ が成り立つか否かは，今のところ知られていない．つまり，証明者が 1 人よりも 2 人の方が，(証明者間にエンタングルメントがないことを検証者が利用することで) 能力が高くなる可能性が大いにあるということである．一方，**QMA** の別の亜種として，量子証明の長さが高々 $O(\log n)$ であるようなクラス $\mathbf{QMA}_{\log}$ も考えられるが，これは有界誤り量子多項式時間で解ける言語のクラス **BQP** と一致することが証明されている [6].

では，証明者が 2 人いて，量子証明長が $O(\log n)$ である場合はどうか？この場合に対応するクラスは $\mathbf{QMA}_{\log}(\mathbf{2})$ と呼ばれ，Blier と Tapp によって研究された [3]．驚くべきことに，彼らは $\mathbf{NP} \subseteq \mathbf{QMA}_{\log}(\mathbf{2})$ であること，より具体的には，3 彩色問題が $\mathbf{QMA}_{\log}(\mathbf{2})$ に属することを示した [3]．但し，そのときの完全性は 1，健全性は $1-\Omega\left(\frac{1}{n^6}\right)$ であった．自然な疑問として，完全性と健全性のギャップがどの程度まで広げられるか，という問題が考えられる．現に，$\sqrt{n}$ 人証明者がいると，健全性は定数になることが知られている [1]．Beigi は，3 充足可能性問題 (**3SAT**) に対し, 完全性が a, 健全性が $a-\Omega\left(\frac{1}{n^{3+\epsilon}}\right)$ (但し，ϵ は任意の正の定数) となる $\mathbf{QMA}_{\log}(\mathbf{2})$ に関するプロトコルを与え，論文 [3] のギャップを改良した [2].

本論文では，Blier と Tapp のプロトコルをもとに **3SAT** に対し，$\mathbf{QMA}_{\log}(\mathbf{2})$ に関する完全性 1，健全性 $1-\Omega\left(\frac{1}{n^2}\right)$ のプロトコルが存在することを示す.

2 定義と結果

まず，この論文で用いる $\mathbf{QMA}_{\log}(2,a,b)$ を定義する．以下では，$\mathcal{H}_n = \mathrm{span}\{|0\rangle, |1\rangle, \ldots, |n-1\rangle\}$ とする.

定義 1 以下の 2 つの条件を満たす量子多項式時間アルゴリズム V，定数 c が存在するなら，言語 L は $\mathbf{QMA}_{\log}(2,a,b)$ に属するという：
任意の長さ n の入力 x に対して，
1) (完全性) $x \in L$ なら，$\Pr[V(x,|w\rangle) = accept] \geq a$ を満たす状態 $|w\rangle = |w_1\rangle \otimes |w_2\rangle \in \left(\mathcal{H}_2^{c\log(n)}\right)^{\otimes 2}$ が存在する．
2) (健全性) $x \notin L$ なら，全ての状態 $|w\rangle = |w_1\rangle \otimes |w_2\rangle \in \left(\mathcal{H}_2^{c\log(n)}\right)^{\otimes 2}$ に対し, $\Pr[V(x,|w\rangle) = accept] \leq b$.

本論文の結果は，以下の定理で記述される．

定理 1 $\mathbf{3SAT} \in \mathbf{QMA}_{\log}\left(2,1,1-\frac{1}{2.4\times 10^{11}n^2}\right)$.

以降，定理 1 を証明する．検証者のアルゴリズムは 2.1 章で記述され，定理 2 が完全性を，定理 3 が健全性を与える．以下の証明の方針は，概ね Blier と Tapp の論文 [3] に従うが，本論文では **3SAT** を扱い，解析はより詳細になされる.

2.1 プロトコルと完全性

まず，**3SAT** に対する検証者を記述する．以下，ϕ は **3SAT** の入力を表し，n は ϕ の節の数を表す.

与えられるべき証明の形

素直に考えると，**3SAT** の証明は「各変数に対する割当て」とするのが 1 つの方法である．しかし，その証明の形を採用してしまうと，以下で記述するプロトコルのテスト 2 b) の構成がうまくいかない．そこで今回は，「各節に対する割当て」を証明の形として採用した．例えば，節 $c_i = l_{i,0} \vee l_{i,1} \vee l_{i,2}$ の割当てが 5(2 進表記で 101) であるとは，$l_{i,0}$ に 1，$l_{i,1}$ に 0，$l_{i,2}$ に 1 を割当てる，ということである．この形にすることで，以下のようにうまくプロトコルが組める.

$\phi, |\Psi\rangle, |\Phi\rangle$ に対する検証者

2 つの証明 $|\Psi\rangle, |\Phi\rangle$ が送られるとする．検証者は $\mathcal{H}_n \otimes \mathcal{H}_8$ 上で，等確率で以下の 3 つのテストのうち 1 つを行う．拒否しないときは受理する．ここで，$\mathcal{H}_n$ の部分を節レジスタ，$\mathcal{H}_8$ の部分を割当レジスタと呼ぶことにする.

- **テスト 1：**(2 つの証明の同一性) $|\Psi\rangle$ と $|\Phi\rangle$ に *swap-test* [4] を行う．テストが失敗ならば拒否.
- **テスト 2：**(論理式の妥当性) $|\Psi\rangle$ と $|\Phi\rangle$ を計算基底で測定し，(c,d) と (c',d') を得る.
  a) $c = c'$ なら，$d = d'$ かどうかをみて，$d \neq 0$ かどうかをみる．$d \neq d'$ または $d = 0$ ならば拒否.

b) $c \neq c'$ なら，$d \neq 0$ かつ $d' \neq 0$ かどうかをみて，c と c' もしくは同じ節に同じリテラル (否定関係も含む) があれば矛盾なく割当てられているかをみる．$d = 0$ または $d' = 0$ または矛盾した割当てがあるならば拒否.

- **テスト３：**(位相に変な施しがなされていないかの確認) $|\Psi\rangle$ と $|\Phi\rangle$ に以下のことを行う．
  節レジスタにフーリエ逆変換 $F_n^\dagger$，割当レジスタにフーリエ変換 F_8 を施し，それぞれ計算基底で測定する．節レジスタが 0 でないかつ割当レジスタが 0 ならば拒否.

以下の定理はこのプロトコルの完全性を示している．

定理 2 $\phi \in$ **3SAT** なら検証者が確率 1 で受理する証明が存在する．

証明． 証明を $|\Psi\rangle = |\Phi\rangle = \frac{1}{\sqrt{n}} \sum_c |c\rangle |A(c)\rangle$ (但し，A は ϕ の各節への適切な割当て) とする．$|\Psi\rangle = |\Phi\rangle$ なので，テスト 1 は確率 1 で成功する．また，A は適切な割当てなので，テスト 2 も確率 1 で成功する．最後にテスト 3 の成功確率を見る．割当レジスタにフーリエ変換 F_8 を施すと，

$$\begin{aligned}&(I \otimes F_8) \frac{1}{\sqrt{n}} \sum_c |c\rangle |A(c)\rangle \\ =&\frac{1}{\sqrt{n}} \sum_c |c\rangle \frac{1}{\sqrt{8}} \sum_k \exp\left(\frac{2\pi i A(c) k}{8}\right) |k\rangle\end{aligned}$$

となる．よって，割当レジスタで 0 が測定されれば，測定後の割当レジスタの状態は $\frac{1}{\sqrt{n}} \sum_c |c\rangle = F_n |0\rangle$ になる．故に，テスト 3 も確率 1 で成功する． ■

2.2 健全性

ここでは，$\phi \notin$ **3SAT** の場合を考える．定理 3 で，この場合は少しの確率で 3 つのテストの 1 つは失敗することを示す．これを示すために以下で 5 つの補題を示す.

まず，証明者から与えられた 2 つの証明はエンタングルしていないので，それぞれ

$$\begin{aligned}|\Psi\rangle &= \sum_c \alpha_c |c\rangle \sum_l \beta_{c,l} |l\rangle \\ |\Phi\rangle &= \sum_c \alpha'_c |c\rangle \sum_l \beta'_{c,l} |l\rangle\end{aligned}$$

(但し，$\sum_c |\alpha_c|^2 = 1$ かつ，任意の c に対して，$\sum_l |\beta_{c,l}|^2 = 1$．$|\Phi\rangle$ も同様．) と書くことができる．このもとで 5 つの補題を示していく．

最初の補題は，もしテスト 1 を成功すれば，2 つの証明はほぼ同じである，ということを意味している．

補題 1 $\left||\alpha_i \beta_{i,j}|^2 - |\alpha'_i \beta'_{i,j}|^2\right| \geq \frac{1}{1\times 10^5 n}$ なる i と j が存在するなら，テスト 1 は少なくとも確率 $\frac{1}{8\times 10^{10} n^2}$ で失敗する．

証明． Blier と Tapp の論文 [3] の補題 2.9 と同様に証明できる． ■

次の補題は，テスト 2 をパスすれば，各節は高い確率で well-defined な割当てがあること意味している．

補題 2 与えられた証明がテスト 1 とテスト 2 a) を $\frac{1}{8\times 10^{10} n^2}$ より小さい確率で失敗するとする．このとき，$|\alpha_c|^2 \geq \frac{1}{50n}$ となる任意の c に対し，$|\beta_{c,l}|^2 \geq \frac{99}{100}$ となる l が一意に存在する．

証明． 背理法で示す．$|\alpha_c|^2 \geq \frac{1}{50n}$ かつ全ての l で $|\beta_{c,l}|^2 < \frac{99}{100}$ を満たす c が存在すると仮定する．このとき，2 つの l で $|\beta_{c,l}|^2 > \frac{1}{700}$ となる．今，一般性を失うことなく $|\beta_{c,1}|^2 > \frac{1}{700}$ かつ $|\beta_{c,2}|^2 > \frac{1}{700}$ とできる．補題 1 の対偶より，$|\Phi\rangle$ で $(c,2)$ を得る確率は，少なくとも

$$\begin{aligned}&|\alpha'_c \beta'_{c,2}|^2 = |\alpha'_c|^2 |\beta'_{c,2}|^2 \geq |\alpha_c|^2 |\beta_{c,2}|^2 - \frac{1}{1\times 10^5 n} \\ \geq &\frac{1}{3.5\times 10^4 n} - \frac{1}{1\times 10^5 n} > \frac{1}{1\times 10^5 n}.\end{aligned}$$

また，$|\Psi\rangle$ で $(c,1)$ を得る確率は，少なくとも $|\alpha_c \beta_{c,1}|^2 = |\alpha_c|^2 |\beta_{c,1}|^2 \geq \frac{1}{3.5\times 10^4 n}$．よって，$n$ が十分大きいとき，$|\Psi\rangle$ で $(c,1)$ を得て，かつ $|\Phi\rangle$ で $(c,2)$ を得る確率は，少なくとも $\frac{1}{3.5\times 10^4 n} \times \frac{1}{1\times 10^5 n} = \frac{1}{3.5\times 10^9 n^2}$ である．これは，テスト 2 a) を $\frac{1}{8\times 10^{10} n^2}$ より小さい確率で失敗するという仮定に矛盾．故に，$|\alpha_c|^2 \geq \frac{1}{50n}$ となる任意の c に対し，$|\beta_{c,l}|^2 \geq \frac{99}{100}$ となる l が一意に存在する． ■

残る 3 つの補題は，証明者が位相部分に手を加えたときでも，ある程度の確率で検証者が拒否できることを意味している．

補題 3 与えられた証明がテスト 1 とテスト 2 a) を $\frac{1}{8\times 10^{10} n^2}$ より小さい確率で失敗するとする．このとき，割当レジスタにフーリエ変換 F_8 を施して計算基底で測定したときに 0 を得る確率は，n が十分大きいとき，$\frac{1}{20}$ より大きい．

証明． $|\Psi\rangle$ について考える ($|\Phi\rangle$ も同様)．先に節レジスタが測定され，c を得たとする．このとき，残った状態は $\sum_l \beta_{c,l} |l\rangle$ なので，これにフーリエ変換 F_8 を施して計算基底で測定したときに 0 を得る確率は，

$$\Pr[0] = \frac{1}{8} |\beta_{c,0} + \cdots + \beta_{c,7}|^2$$

である．ここで，$|\alpha_c|^2 \geq \frac{1}{50n}$ となる全ての c に対して補題 2 を適用する．このとき，一般性を失うことなく，$|\beta_{c,7}|^2 \geq \frac{99}{100}$ かつ $|\beta_{c,0}|^2 + \cdots + |\beta_{c,6}|^2 \leq \frac{1}{100}$ とできる．三角不等式とコーシー・シュワルツの不等式より，

$$\begin{aligned}\Pr[0] \geq & \frac{1}{8}\left||\beta_{c,7}| - |\beta_{c,0} + \cdots + \beta_{c,6}|\right|^2 \\ \geq & \frac{1}{8}\left||\beta_{c,7}| - \sqrt{7\left(|\beta_{c,0}|^2 + \cdots + |\beta_{c,6}|^2\right)}\right|^2 \\ \geq & \frac{1}{8}\left|\sqrt{\frac{99}{100}} - \sqrt{\frac{7}{100}}\right|^2 \geq \frac{1}{18}\end{aligned}$$

を得る．今，$|\alpha_c|^2 < \frac{1}{50n}$ となる c は高々 $n-1$ 個しかない．[*1] よって，補題 2 が使える確率は，少なくとも $1-(n-1)\frac{1}{50n}$ である．故に，n が十分大きいとき，割当レジスタで 0 を得る確率は，少なくとも $\left(1-(n-1)\frac{1}{50n}\right)\frac{1}{18} \geq \frac{1}{20}$ である． ■

補題 4 状態 $|X\rangle = \sum_c \gamma_c |c\rangle$ を $|\gamma_i|^2 < \frac{1}{2n}$ となる i が存在する状態とする．このとき，フーリエ逆変換 $F_n^\dagger$ を施して計算基底で測定したとき 0 を得ない確率は，少なくとも $\frac{1}{16n^2}$.

証明. Blier と Tapp の論文 [3] の補題 2.12 と同様に証明できる． ■

補題 5 与えられた証明がテスト 1 とテスト 2 a) とテスト 3 を $\frac{1}{8\times 10^{10}n^2}$ より小さい確率で失敗するとする．このとき，任意の c に対して，$|\alpha_c|^2 \geq \frac{1}{40n}$.

証明. 補題 3 より，テスト 3 において割当レジスタで 0 を得る確率は少なくとも $\frac{1}{20}$．$|X\rangle = \sum_c \gamma_c |c\rangle$ を割当レジスタで 0 を得た後の節レジスタの状態とする．以下，背理法で示す．$|\alpha_c|^2 < \frac{1}{40n}$ なる c が存在すると仮定する．このとき，補題 3 より，$|\gamma_c|^2 < \frac{1}{2n}$ が成り立つ．[*2] さらに補題 4 より，節レジスタで 0 を得ないかつ割当レジスタで 0 を得る確率 $\geq \frac{1}{16n^2} \times \frac{1}{20} = \frac{1}{320n^2}$．これは，テスト 3 を $\frac{1}{8\times 10^{10}n^2}$ より小さい確率で失敗するという仮定に矛盾．故に，任意の c に対して，$|\alpha_c|^2 \geq \frac{1}{40n}$． ■

補題 1，補題 2，補題 5 を使って，健全性を示すことができる．

定理 3 $\phi \notin$ **3SAT** なら，全ての量子証明に対し，少なくとも確率 $\frac{1}{2.4\times 10^{11}n^2}$ で失敗する．

証明. $\phi \notin$ **3SAT** とし，テスト 1 とテスト 2 a) とテスト 3 を $\frac{1}{8\times 10^{10}n^2}$ より小さい確率で失敗するとする．$A(c) = \max_l |\beta_{c,l}|$ を割当てとすると，補題 2，補題 5 より well-defined である．今，$\phi \notin$ **3SAT** なので，(1)「どれかの節が 0」又は (2)「同じリテラル (否定関係も含む) に対して矛盾した割当てがなされている」のどちらかになる．まず，(1) の場合の失敗確率を見る．補題 2，補題 5 より，そのような節 c とその割当て $A(c)$ を得る確率は，少なくとも $\frac{1}{40n} \times \frac{99}{100} = \frac{99}{4000n}$． 次に，(2) の場合の失敗確率を見る．同じ節内で矛盾が起こっている場合，先程と同様にして，矛盾となる節とその割当てを得る確率は，少なくとも $\frac{1}{40n} \times \frac{99}{100} = \frac{99}{4000n}$．異なる節で矛盾が起こっている場合，補題 1，補題 2，補題 5 より，そのような 2 節 c, c' とその割当て $A(c), A(c')$ を得る確率は，少なくとも

$$\frac{1}{40n} \times \frac{99}{100}\left(\frac{1}{40n} \times \frac{99}{100} - \frac{1}{1\times 10^5 n}\right) = \frac{99\times 2474}{4\times 10^8 n^2}$$

である．いずれも $\frac{1}{8\times 10^{10}n^2}$ より大きいので，テスト 2 b) の失敗確率は $\frac{1}{8\times 10^{10}n^2}$ より大きい．故に，$\phi \notin$ **3SAT** なら，全ての量子証明に対し，少なくとも確率 $\frac{1}{2.4\times 10^{11}n^2}$ で失敗する． ■

参考文献

[1] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman and P. W. Shor. The Power of Unentanglement. *Theory of Computing* **5(1)** (2009) 1–42.

[2] S. Beigi. NP vs $\mathrm{QMA}_{\log}(2)$ *Quantum Information & Computation* **10** (2010) 141–151. arXiv:0810.5109, 2008.

[3] H. Blier and A. Tapp. All languages in NP have very short quantum proofs. *Proceedings of the 3rd ICQNM*, pp.34–37, 2009.

[4] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. In *Phys. Rev. Lett.* **87** (2001) 167902.

[5] H. Kobayashi, K. Matsumoto and T. Yamakami. Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur? *Chicago Journal of Theoretical Computer Science* (2009) 3. arXiv:quant-ph/0306051, 2003.

[6] C. Marriott and J. Watrous. Quantum Arthur-Merlin games. *Computational Complexity* **14(2)** (2005) 122–152.

[7] J. Watrous. *Quantum Computational Complexity.* arXiv:0804.3401, 2008.

[*1] もし $|\alpha_c|^2 < \frac{1}{50n}$ となる c が n 個だとすると，$\sum_c |\alpha_c|^2 < \frac{1}{5}$ となり，$\sum_c |\alpha_c|^2 = 1$ に矛盾．

[*2] フーリエ変換後の状態は，$\sum_c \alpha_c |c\rangle \sum_l \beta_{c,l} F_8 |l\rangle = \sum_c \alpha_c |c\rangle \sum_l \beta_{c,l} \frac{1}{\sqrt{8}} \sum_k \exp\left(\frac{2\pi i l k}{8}\right)|k\rangle$ である．よって，$\sum_c \gamma_c |c\rangle = \frac{\frac{1}{\sqrt{8}}\sum_c \alpha_c |c\rangle \sum_l \beta_{c,l}}{\left\|\frac{1}{\sqrt{8}}\sum_c \alpha_c |c\rangle \sum_l \beta_{c,l}\right\|}$ なので，補題 3 より，$|\gamma_c|^2 = \frac{\frac{1}{8}|\alpha_c|^2\left|\sum_l \beta_{c,l}\right|^2}{\left\|\frac{1}{\sqrt{8}}\sum_c \alpha_c |c\rangle \sum_l \beta_{c,l}\right\|^2} \leq \frac{\frac{1}{8}\times\frac{1}{40n}\times 8}{\frac{1}{20}} = \frac{1}{2n}$.