社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

量子版NPと量子版AMの計算複雑さ

西村　治道†

† 名古屋大学大学院情報科学研究科
〒 464-8601 愛知県名古屋市千種区不老町
E-mail: †hnishimura@is.nagoya-u.jp

あらまし　本講演では，計算量理論の代表的クラスである NP と AM の量子版についてその計算複雑さに関する研究の進展を報告する．とくに，講演者が小林弘忠氏（国立情報学研究所），ルガルフランソワ氏（東京大学）と共同で研究を行った２編の論文の成果を詳細に報告する．
キーワード　量子計算，計算複雑さ，QMA，量子 Arthur-Merlin 証明

Computational Complexity of Quantum NP and Quantum AM

Harumichi NISHIMURA†

† Graduate School of Information Science, Nagoya University
Furo-cho, Chikusa-ku, Nagoya, Aichi
E-mail: †hnishimura@is.nagoya-u.jp

Abstract　In this talk, we report some progresses of research on the computational complexity of quantum versions of two representative complexity classes NP and AM in computational complexity theory. In particular, we mainly report the results in two papers which are joint works with Hirotada Kobayashi (National Institute of Informatics) and François Le Gall (Tokyo University).
Key words　quantum computation, computational complexity, QMA, quantum Arthur-Merlin proof

1. NP と AM

NP は P とともに計算機科学の枠を超えて広く知られており，情報学の中でも基礎知識の１つといってよい概念であるが，通信プロトコルとしては以下のようにとらえることができる．ある決定問題 A が NP に属するとは，多項式時間の計算能力を持つ検証者 V が存在して，次の２条件をみたす．

- （完全性）入力 x が A の Yes 入力（x に対する A の答えが Yes であるような入力）であるとき，無限の計算能力を持つ証明者 P が V に適切なビット列 y（証明）を送ることで，V は受理する．
- （健全性）x が A の No 入力であるとき，どんな y が送られてきても V は拒否する．

この自然な拡張としてまず考えられるのは，検証者 V がコインを投げて動作を決める確率的なアルゴリズム（多項式時間乱択アルゴリズム）を使って高確率で受理，拒否を判定するといったように NP を変形した計算量クラスである．この計算量クラスは導入した Babai [3] が証明者を魔法使い Merlin，検証者を Arthur 王と見立てたことから MA と名づけられ，とくに改名されることなくそのまま今日に至っている．

さらに NP（や MA）が証明者から検証者への一方向通信による通信プロトコルであると鑑みると，やはり自然な拡張として双方向通信による通信プロトコルのもとで同様の拡張概念が考えられる．これが対話型証明であり，1985 年に前述の Babai と，同時に Goldwasser ら [7] によって導入された．通信回数が入力長の多項式であるような対話型証明によって検証される問題のクラスは IP と呼ばれ，このクラスは多項式メモリで計算可能な問題のクラス PSPACE と一致することが知られている [25], [29].

では通信回数を制限した場合はどうか？ここで対話型証明を導入した Babai と Goldwasser らの定式化の違いによって２種類の計算量クラスが考えられる．Goldwasser らの定式化によるクラス IP(k) は，通信回数が k 回 (注1) の対話型証明で検証される問題のクラスであるが，検証者は多項式時間の乱択アルゴリズムの範囲でどんな戦略をとってもよい．とくに，検証者はメッセージ生成のために自分で投げたコインの値を証明者に教えることなく通信プロトコルを進めてもよい．一方で，Babai

(注1)：対話型証明において，最初にメッセージを送るのがどちらかは k の偶奇で変わるが，最後にメッセージを送るのは常に証明者である．

の定式化によるクラス AM(k) では，検証者が証明者に送るメッセージは（前後の文脈に関係なく）単なるランダムなビット列である．一聞するとこの 2 つはかなり検証能力に差が出そうな気がするが，実際には Goldwasser と Sipser によって IP(k) が AM($k+2$) に含まれることが示されている [8]．さらに Babai によって，k が定数である限り AM(k) は通信が 2 回のクラス AM := AM(2) に一致すること（Babai の崩壊定理）が示されている．これらの事実によって，通信回数が定数回の対話型証明はすべて AM，つまり「検証者がランダムビット列を送って証明者がメッセージを返す」という簡素化された通信プロトコルによる対話型証明と検証能力が変わらないことになる．このため，AM は NP の拡張クラスの中で比較的堅牢なものであり，計算量理論における最重要なクラスの 1 つとして脱乱択化のトピック（例えば [2] 参照）などで盛んに研究されている．

2. QMA: 量子版 NP

NP の重要性からしてその量子版が Shor のブレークスルーから数年で考察されたことは驚くにはあたらないだろう．1990 年代後半に Knill [17] によって量子版 NP の概念が触れられ，その後数年で Kitaev [14], [15] と Watrous [31] によって量子版 NP（厳密にいえば MA の量子版）の定式化が導入された．決定問題 A が QMA（Quantum Merlin-Arthur の略）に属するとは，多項式時間量子アルゴリズムを実行可能な検証者 V が存在して，以下の 2 条件をみたすことを指す．

- （完全性）入力 x が A の Yes 入力であるとき，証明者 P が V に適切な量子状態 $|\psi\rangle$（量子証明）を送ることで，V は高確率（例えば 2/3）で受理する．
- （健全性）x が A の No 入力であるとき，どんな $|\psi\rangle$ が送られてきても V は高確率で拒否する．

Kitaev は LH（local Hamiltonian problem），Watrous は GNM（group non-membership problem）という NP ないし MA に属することが知られていない問題に対してそれぞれ QMA プロトコルを与えたが，とくに Kitaev により LH が QMA に属するのみならず QMA 完全問題であると示されたことは，今日のハミルトニアン計算量の精力的な研究（例えば [6] 参照）の出発点となっている．一方で，QMA という計算量クラスの他のクラスとの関係やクラスが持つ性質については：

- QMA は PSPACE の部分クラスである PP，さらにはその部分クラス A_0PP（あるいは等価なクラス SBQP [22]）に含まれる [26], [30]
- QMA は証明サイズを保存したままで検証の成功率を増幅できる [26]
- QMA は検証者の能力を Clifford 回路と古典計算に制限しても不変である [27]

など幾らかの事実が知られているが，MA と比較して量子特有の困難さから解明されていない関係・性質も多い．とくに，以下の 3 つのクラスの QMA との等価性に関する課題はいずれも 10 年以上未解決のまま残っている（いずれも MA の場合は成立するかそもそもクラスの定義が無意味になる）．

- QMA = QMA_1?： QMA_1 は QMA の定義において完全性の受理確率が 1 である（つまり完全性は誤りがない）という制限を持つ部分クラスである．
- QMA = QCMA?： QCMA（しばしば MQA とも呼ばれる）は，QMA の定義において証明者が量子状態でなくビット列を送るという制限を持つ部分クラスである．なお QCMA については完全性に誤りがない場合に対応する部分クラス QCMA_1 との計算量的等価性（QCMA = QCMA_1）が示されている [13]．
- QMA = QMA(2)?： QMA(2)(注2) は QMA の定義において「証明者が 2 人いてそれぞれが量子状態 $|\psi_1\rangle, |\psi_2\rangle$ を送る」と変形することで定義される QMA の拡張クラス [21] である（最近の研究状況については例えば [9], [10], [23], [24]）．

3. 量子対話型証明

量子対話型証明は文字通り対話型証明の量子版である．多項式時間の能力しかない検証者も無限の能力を持つ証明者も量子的に生成・変換された量子状態を送りあうことで，検証者が決定問題を検証するプロトコルを指す．量子対話型証明は QMA と同時期にやはり Watrous [34] によって導入されたが，その最初の論文でいきなり「PSPACE が量子対話型証明を使うとたった 3 回の通信で検証可能」という驚くべき事実が証明された．この結果はすぐに Kitaev と Watrous によって「すべての量子対話型証明で検証可能な問題は，通信が 3 回に限定された量子対話型証明で検証可能」という結果に改良された [16]．より正確には，QIP を量子対話型証明で検証可能な問題のクラス，QIP(k) および $\mathrm{QIP}_1(k)$ をそれぞれ通信回数が k 回の量子対話型証明で検証可能な問題のクラスおよびその完全性が誤りのない場合に対応する部分クラスとすれば，[34] では PSPACE $\subseteqq$ $\mathrm{QIP}_1(3)$ が示され，[16] では QIP = QIP(3) = $\mathrm{QIP}_1(3)$ が示されたということになる．古典の場合，通信回数が定数なら AM の能力で止まり，AM は IP = PSPACE より小さいクラスと考えられている（AM = NP という予想もある）ので，量子だと検証能力を制限することなく通信を 3 回に制限できるというのは，古典の場合と非常に対照的な結果であると考えられる．

一方で「QIP は IP より真に検証能力が高いのか」という問題は否定的に解決された．Jain ら [12] は，QIP のそれまでの上界 EXP [16] を改良して，QIP $\subseteqq$ PSPACE（従って，QIP = IP）を証明した．この結果を以って量子対話型証明のクラス QIP は古典のクラスで特徴付けられた．しかしながら，QIP(2) や QMA (= QIP(1)) のような 2 回以下の通信に限定された場合は，依然として十分にその検証能力が明らかになったとは言い難い．とくに QIP(2) についてはわかっていることは非常に限られていて例えば，QMA の場合と同様に，QIP(2) と $\mathrm{QIP}_1(2)$ が一致するかどうかは未解決である．

4. QMA vs QMA_1 に関する進展

2 章で述べたように，QMA と完全性に誤りのない部分クラス QMA_1 が等しいか否かは，QMA が導入された当初からの

(注2)：ここでの (2) は通信回数でなく証明者の人数が 2 であることを指す（QMA プロトコルは通信が一方向なので誤解は生じないと思われるが）．

未解決問題である．この問題はその数学的興味だけでなく，ハミルトニアン計算量や量子版 PCP（例えば [1] 参照）の研究の観点からも重要である．とくに NP 完全問題 SAT（与えられた CNF 論理式が充足可能か否かを問う問題）の量子版として Kitaev が導入した QMA 完全問題 LH（定数個の粒子にしか作用しない局所的なハミルトニアン (注3) の和の最低エネルギーがある閾値以上かどうかを問う問題）は，実際には MAX-SAT（与えられた CNF 論理式においてある閾値以上の個数の節が充足可能か否かを問う問題）の量子版に対応しており，本当の意味で SAT の量子版に対応する QSAT（定数個の粒子にしか作用しない局所的な射影作用素の和の最低エネルギーが 0 かを問う問題 [4]）が QMA_1 完全であることを鑑みると，$\mathrm{QMA} = \mathrm{QMA}_1$ を証明することは 2 つに分かれた量子版 NP の完全問題を統一することに繋がる．

論文 [19] では，$\mathrm{QMA} = \mathrm{QMA}_1$ の肯定的解決の方向への進展を与えた．平たく言うと「検証者と証明者が高々定数個の EPR ペアを共有していれば QMA プロトコルは誤りのない完全性をみたすように変形できる」という事実が証明された．より厳密には，$\mathrm{QMA}^{\text{const-EPR}}$ を QMA の定義において検証者と証明者が定数個の EPR ペアを事前に共有しているという条件を加える (注4) ことで定義される拡張クラスとする．また，$\mathrm{QMA}_1^{\text{const-EPR}}$ をそのクラスの完全性に誤りがない場合に対応する部分クラスとする．このとき，以下の定理が示された．

定理 1. $\mathrm{QMA} \subseteqq \mathrm{QMA}_1^{\text{const-EPR}} = \mathrm{QMA}^{\text{const-EPR}}$.

また，上記の定理からは QMA に対する（既存の上界 $\mathrm{A_0PP}$ とは異なる）新しい上界を得ることができる．

定理 2. $\mathrm{QMA} \subseteqq \mathrm{QIP}_1(2)$.

5. 量子版 AM とその一般化

QIP(2) は通信回数が 2 回という点では AM の量子版といえるが，検証者が証明者に送るメッセージを（検証者が多項式量子アルゴリズムであるという以外に）何も制限していないという意味では，むしろ（AM と等価ではあるものの）IP(2) の量子版といえる．Marriott と Watrous [26] は，検証者の送るメッセージを AM 同様にランダムビット列に制限することで定義される量子対話型証明を量子 Arthur-Merlin 証明と名付け，以下の事実を証明した．

- $\mathrm{QIP}(3) = \mathrm{QMAM}$： QMAM は通信回数が 3 回の量子 Arthur-Merlin 証明で検証可能な問題のクラスである．この事実によって任意の量子対話型証明は通信回数が 3 回の量子 Arthur-Merlin 証明と検証能力において等価である．この等価性は QIP = PSPACE の証明 [12] などで有効に利用されている．
- $\mathrm{QAM} \subseteqq \mathrm{BP{\cdot}PP}$: QAM は通信回数が 2 回の量子 Arthur-Merlin 証明で検証可能な問題のクラスである．$\mathrm{BP \cdot PP}$ は PP と PSPACE の間にあるクラスであり，論文 [20] 以前は QAM に対する唯一の非自明な上界であった．

問題	計算複雑さ
Image vs Image	QIP 完全 [28]
Image vs State	QIP(2) 完全 [11], [32]
Image vs Identity	qq-QAM 完全 [20]
State vs State	QSZK 完全 [33], [35]
State vs Identity	NIQSZK 完全 [5], [18]

表 1　量子回路の出力に関する完全問題：Image vs Image は与えられた 2 つの量子回路の像が近いかを問う問題，Image vs State は量子回路の像が別の量子回路が生成する状態に近いかを問う問題，Image vs Identity は量子回路の像が完全混合状態に近いかを問う問題，State vs State は 2 つの量子回路が生成する状態が近いかを問う問題，そして State vs Identity は量子回路が生成する状態が完全混合状態に近いかを問う問題である．

論文 [20] は [26] の量子 Arthur-Merlin 証明を次のような形で一般化した．

- 検証者から証明者への各メッセージはランダムなビット列 (c) か EPR ペアの片割れの列 (q)，すなわち検証者は高々多項式個の EPR ペアを用意してその各々の片割れを証明者に送る，かのモードがある．
- 証明者から検証者への各メッセージは古典のビット列 (c) か量子状態 (q) かのモードがある．

このとき，$t_m \cdots t_1$-QAM(m) は m 回の通信による量子対話型証明で最後から数えて j 回目のメッセージがモード t_j に制限されたものによって検証可能な問題のクラスを表す．なおクラス記法の簡潔性のため (m) は m が明らかな場合は省略する．例えば [26] による QAM は cq-QAM と表され，QMAM は qcq-QAM と表される．

とくに既存のクラス QAM と QIP(2) の間にあるクラス qq-QAM は，検証者の操作がランダムビット列を送るという古典操作でなく，その量子拡張として自然と考えられる操作（EPR ペアの片割れを送るという操作）に制限されているため，AM の完全な量子版と考えられるものである．[20] では qq-QAM について以下のような成果を得た．

- qq-QAM は自然な完全問題を持つ： 量子回路の（写像とみなしたときの）像が完全混合状態に近いか（すなわち与えられた量子回路の出力が完全混合状態に近くなるような入力が存在するか）を判定する問題は qq-QAM にとって完全問題である．表 1 に示されるように，この問題は一連の先行研究で得られている他のクラスの完全問題から考えうる問題の 1 つである．また，与えられた量子通信路の最大出力エントロピーがある閾値より大きいかを判定する問題も qq-QAM 完全である．
- 任意の $m \geqq 3$ について $\mathrm{c}\cdots\mathrm{cqq}(m)$-QAM = qq-QAM：qq-QAM は定数回の古典の Arthur-Merlin 的対話を最初に加えても検証能力は変わらない．これは Babai の崩壊定理のクラス qq-QAM に対応するものとみなせる．
- $\mathrm{QAM} \subseteqq \mathrm{qq\text{-}QAM}_1$： $\mathrm{qq\text{-}QAM}_1$ は qq-QAM の完全性が誤りのない場合に対応する部分クラスである．この結果は

(注3)：実際は射影作用素に制限しても問題の計算複雑さは変わらない．

(注4)：逆にいうと，QMA の定義では証明者と検証者はエンタングルメントを事前共有していないことが暗に仮定されている．

QAM $\subseteqq$ $\mathrm{QIP}_1(2)$ を意味するので，QAM に対する（BP · PP とは異なる）新しい上界を与えている．

さらに，一般化された量子 Arthur-Merlin 証明のクラスは，計算量的等価性において cc-QAM, QAM = cq-QAM, qq-QAM, PSPACE の 4 種類のクラスに分類されることが示された．これは一般化された量子 Arthur-Merlin 証明に対する Babai の崩壊定理のアナロジーと位置付けられる．

定理 3. （*1*） 任意の $m \geqq 3$ に対して，$\mathrm{c}\cdots\mathrm{ccc\text{-}QAM}(m) = \mathrm{cc\text{-}QAM}$.

（*2*） 任意の $m \geq 3$ に対して，$\mathrm{c}\cdots\mathrm{ccq\text{-}QAM}(m) = \mathrm{cq\text{-}QAM}\ (= \mathrm{QAM})$.

（*3*） 任意の $t_1 \in \{\mathrm{c},\mathrm{q}\}$ および $m \geq 3$ に対して，$\mathrm{c}\cdots\mathrm{cq}t_1\mathrm{\text{-}QAM}(m) = \mathrm{qq\text{-}QAM}$.

（*4*） それ以外は PSPACE と一致する．すなわち，任意の $m \geqq 3$ および $t_1, \ldots, t_m \in \{\mathrm{c},\mathrm{q}\}$ に対して，ある $j \geqq 3$ が存在して $t_j = \mathrm{q}$ なら，$t_m \cdots t_1\mathrm{\text{-}QAM}(m) = \mathrm{QMAM}\ (= \mathrm{PSPACE})$.

謝　辞

本講演で報告する論文 [19], [20] を通じての共同研究全般について小林弘忠氏とルガルフランソワ氏に深く感謝します．本研究は科研費 23246071, 24240001, 24106009, 25330012, 26247016 の助成を受けたものです．

文　献

[1] Dorit Aharonov, Itai Arad, and Thomas Vidick. The quantum PCP conjecture, *SIGACT News*, 44(2):47–79, 2013. arXiv:1309.7495.

[2] Barış Aydinlioğlu, Dan Gutfreund, John M. Hitchcock, and Akinori Kawachi. Derandomizing Arthur-Merlin games and approximate counting implies exponential-size lower bounds. *Computational Complexity*, 20(2):329–366, 2011. Earlier version in *Proceedings of the 25th Annual IEEE Conference on Computational Complexity (CCC'10)*, pages 38–49, 2010.

[3] László Babai. Trading group theory for randomness. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing (STOC'85)*, pages 421–429, 1985.

[4] Sergey Bravyi. Efficient algorithm for a quantum analogue of 2-SAT. arXiv:quant-ph/0602108.

[5] André Chailloux, Dragos Florin Ciocan, Iordanis Kerenidis, and Salil Vadhan. Interactive and noninteractive zero knowledge are equivalent in the help model. In *Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008*, volume 4948 of *Lecture Notes in Computer Science*, pages 501–534, 2008. A full version available as Cryptology ePrint Archive, Report 2007/467, 2007.

[6] Sevag Gharibian, Yichen Huang, and Zeph Landau. Quantum Hamiltonian complexity. arXiv:1401.3916.

[7] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989. Earlier version in *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing (STOC'85)*, pages 291–304, 1985.

[8] Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In Silvio Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 73–90. JAI Press, 1989. Earlier version in *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing (STOC'86)*, pages 59–68, 1986.

[9] Gus Gutoski, Patrick Hayden, Kevin Milner, and Mark M. Wilde. Quantum interactive proofs and the complexity of separability testing. *Theory of Computing*, 11:59–103 (article 3), 2015.

[10] Aram W. Harrow and Ashley Montanaro. Testing product states, quantum Merlin-Arthur games and tensor optimization. *Journal of the ACM*, 60(1):article 3, 2013. Earlier version in *51st Annual IEEE Symposium on Foundations of Computer Science (FOCS'10)*, pages 633–642, 2010.

[11] Patrick Hayden, Kevin Milner, and Mark M. Wilde. Two-message quantum interactive proofs and the quantum separability problem. *Quantum Information and Computation*, 14(5–6):0384–0416, 2014. Earlier version in *Proceedings of the 28th Conference on Computational Complexity (CCC'13)*, pages 156–167, 2013.

[12] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. *Journal of the ACM*, 58(6):article 30, 2011. Earlier version in *Proceedings of the 42nd ACM Symposium on Theory of Computing (STOC'10)*, pages 573–582, 2010.

[13] Stephen P. Jordan, Hirotada Kobayashi, Daniel Nagaj, and Harumichi Nishimura. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Information and Computation*, 12(5–6):0461–0471, 2012.

[14] Alexei Yu. Kitaev. Quantum NP. Talk at the 2nd Workshop on Algorithms in Quantum Information Processing, DePaul University, Chicago, January 1999.

[15] Alexei Yu. Kitaev, Alexander H. Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

[16] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing (STOC'00)*, pages 608–617, 2000.

[17] Emanuel Knill. Quantum randomness and nondeterminism. Technical Report LAUR-96-2186, Los Alamos National Laboratory, 1996. arXiv:quant-ph/9610012.

[18] Hirotada Kobayashi. Non-interactive quantum perfect and statistical zero-knowledge. In *Algorithms and Computation, 14th International Symposium, ISAAC 2003*, volume 2906 of *Lecture Notes in Computer Science*, pages 178–188, 2003.

[19] Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura. Stronger methods of making quantum interactive proofs perfectly complete. *SIAM Journal on Computing*, 44(2):243–289, 2015. Earlier version in *Proceedings of the 4th Innovations in Theoretical Computer Science (ITCS'13)*, pages 329–352, 2013.

[20] Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura. Generalized quantum Arthur-Merlin games. In *Proceedings of the 30th Conference on Computational Complexity (CCC'15)*, pages 488–511, 2015.

[21] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? *Chicago Journal of Theoretical Computer Science*, 2009:article 3, 2009. Earlier version in *Algorithms and Computation, 14th International Symposium, ISAAC 2003*, volume 2906 of *Lecture Notes in Computer Science*, pages 189–198, 2003.

[22] Greg Kuperberg. How hard is it to approximate the Jones polynomial? *Theory of Computing*, 11:183–219 (article 6), 2015.

[23] François Le Gall, Shota Nakagawa, and Harumichi Nishimura. On QMA protocols with two short quantum proofs. *Quantum Information and Computation*, 12(7–8):0589–0600, 2012.

[24] Ke Li and Graeme Smith. Quantum de Finetti theorem un-

der fully-one-way adaptive measurements. *Physical Review Letters*, 114:article 160503, 2015.

[25] Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, 1992. Earlier version in *Proceedings of the 31st Annual Symposium on Foundations of Computer Science (FOCS'90)*, pages 2–10, 1990.

[26] Chris Marriott and John Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005. Earlier version in *Proceedings of the 19th IEEE Conference on Computational Complexity (CCC'04)*, pages 275–285, 2004.

[27] Tomoyuki Morimae, Masahito Hayashi, Harumichi Nishimura, and Keisuke Fujii. Quantum Merlin-Arthur with Clifford Arthur. *Quantum Information and Computation*, 15(15–16):1420–1430, 2015.

[28] Bill Rosgen and John Watrous. On the hardness of distinguishing mixed-state quantum computations. In *Twentieth Annual IEEE Conference on Computational Complexity (CCC'05)*, pages 344–354, 2005.

[29] Adi Shamir. IP = PSPACE. *Journal of the ACM*, 39(4):869–877, 1992. Earlier version in *Proceedings of the 31st Annual Symposium on Foundations of Computer Science (FOCS'90)*, pages 11–15, 1990.

[30] Mikhail N. Vyalyi. QMA = PP implies that PP contains PH. Electronic Colloquium on Computational Complexity, Report TR03-021, 2003.

[31] John Watrous. Succinct quantum proofs for properties of finite groups. In *41st Annual Symposium on Foundations of Computer Science (FOCS'00)*, pages 537–546, 2000.

[32] John Watrous. Capturing quantum complexity classes via quantum channels. Talk at the 6th Workshop on Quantum Information Processing, December 2002.

[33] John Watrous. Limits on the power of quantum statistical zero-knowledge. In *43rd Annual Symposium on Foundations of Computer Science (FOCS'02)*, pages 459–468, 2002.

[34] John Watrous. PSPACE has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, 2003. Earlier version in *40th Annual Symposium on Foundations of Computer Science (FOCS'99)*. pages 112–119, 1999.

[35] John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009. Earlier version in *Proceedings of the 38th Annual ACM Symposium on Theory of Computing (STOC'06)*, pages 296–305, 2006.