MODIFIED GROUP NON-MEMBERSHIP IS IN PROMISE-AWPP RELATIVE TO GROUP ORACLES

TOMOYUKI MORIMAE
ASRLD Unit, Gunma University, 1-5-1 Tenjincho, Kiryushi, Gunma, 376-0052, Japan
morimae@gunma-u.ac.jp

HARUMICHI NISHIMURA
Graduate School of Information Science, Nagoya University
Furocho, Chikusaku, Nagoya, Aichi, 464-8601, Japan
hnishimura@is.nagoya-u.ac.jp

FRANÇOIS LE GALL
Department of Computer Science, The University of Tokyo
7-3-1 Hongo, Bunkyo, Tokyo, 113-8656, Japan
legall@is.s.u-tokyo.ac.jp

Received February 28, 2016
Revised January 20, 2017

It is known that the group non-membership problem is in QMA relative to any group oracle and in SPP∩BQP for solvable groups. We consider a modified version of the group non-membership problem where the order of the group is also given as an additional input. We show that the problem is in (the promise version of) AWPP relative to any group oracle. To show the result, we use the idea of postselected quantum computing.

Keywords: group non-membership problem; AWPP; postselection; group oracle

Communicated by: I Cirac & M Mosca

1 Introduction

The group non-membership (GNM) is the following problem:

- Input: Group elements $g_1, g_2, ..., g_k$, and $h$ in some finite group $G$.
- Question: Is $h \notin H \equiv \langle g_1, ..., g_k \rangle$?

Here, $H \equiv \langle g_1, ..., g_k \rangle$ is the group generated by $g_1, ..., g_k$. This problem has long been studied for black-box groups [1], which are finite groups whose elements are encoded as strings of a given length and whose group operations are performed by a group oracle. The GNM is known to be hard for classical computing: for some group oracle $B$, GNM is not in BPP$^B$ [2, 3]. Furthermore, it was also shown that for some group oracle $B$, GNM is not in NP$^B$ [2, 3], and for some group oracle $B$, GNM is not in MA$^B$ [4].

Upper bounds of GNM have also been derived. For example, it was shown that GNM is in coNP$^B$ [1], AM$^B$ [2, 3], and QMA$^B$ [4] for any group oracle $B$. If we restrict the group
to be solvable, upper bounds can be improved: it was shown that GNM is in BQP \cite{5} and SPP \cite{6}.

In this paper, to deepen our understanding of the upper bounds of GNM, we consider a slightly modified version of GNM, which we call modified GNM (MGNM):

- **Input**: A list of group elements \(g_1, g_2, \ldots, g_k\), and \(h\) in a finite group \(G\), and a number \(s\) in binary.
- **Promise**: \(s = |\langle g_1, \ldots, g_k \rangle|\).
- **Question**: Is \(h \not\in H \equiv \langle g_1, \ldots, g_k \rangle\)?

In other words, in MGNM, the order \(|\langle g_1, \ldots, g_k \rangle|\) of the generated group \(\langle g_1, \ldots, g_k \rangle\) is also given as an additional input.

We show that MGNM is in (the promise version of) AWPP relative to any group oracle. The class AWPP was introduced by Fenner, Fortnow, Kurtz, and Li \cite{7} to understand the structure of counting complexity classes (see also Refs. \cite{9, 8}). AWPP is also well-known among quantum information scientists, since it is one of the two best upper bounds of BQP \cite{10}. (The other one is QMA (or QCMA). No direct relation is known between QMA and AWPP. It is at least known that they share the same upper bound, SBQP, namely, QMA \(\subseteq\) SBQP \cite{11} and AWPP \(\subseteq\) SBQP.) Therefore, our result implies that if GNM is changed to an easier problem by adding an extra input, its upper bound is improved to the intersection of QMA and promise-AWPP.

The definition of promise-AWPP is as follows. (Here, we take a simpler definition of AWPP by Fenner \cite{8}.)

**Definition 1** A promise problem \(A = (A_{\text{yes}}, A_{\text{no}})\) is in promise-AWPP iff there exist \(f \in \text{FP}\) and \(g \in \text{GapP}\) such that for all \(w\), \(f(w) > 0\) and

1. If \(w \in A_{\text{yes}}\) then \(\frac{2}{3} \leq \frac{g(w)}{f(w)} \leq 1\),
2. If \(w \in A_{\text{no}}\) then \(0 \leq \frac{g(w)}{f(w)} \leq \frac{1}{3}\).

Here, \text{FP} is the class of functions from bit strings to integers that are computable in polynomial time by a Turing machine. A GapP function \cite{12} is a function from bit strings to integers that is equal to the number of accepting paths minus that of rejecting paths of a nondeterministic Turing machine which takes the bit strings as input. The FP function \(f\) can be replaced with \(2^{q(|w|)}\) for a polynomial \(q\) \cite{12, 9}, and the error bound \((\frac{1}{3}, \frac{2}{3})\) can be replaced with \((2^{-r(|w|)}), 1 - 2^{-r(|w|)})\) for any polynomial \(r\) \cite{7, 9}.

Note that this is a promise version of AWPP in close analogy with promise versions of other classes, such as promise-BPP and promise-BQP, which were previously defined in the literature.

Our proof is based on the idea of postselected quantum computing. The postselection is a fictitious ability that one can always obtain a specific measurement result even if its occurring probability is exponentially small. The class of languages that can be efficiently recognized by a quantum computer with the postselection is called postBQP, and it is known that postBQP = PP \cite{13}. If we consider a restricted version of postBQP where the postselection probability is close to an FP function divided by \(2^{\text{poly}}\), the class was shown to be equal to
Modified group non-membership is in promise-AWPP relative to group oracles

AWPP [14]. The original idea of our proof is based on this relation between postselected quantum computing and AWPP: if we first propose a postBQP algorithm that can solve MGNM, and next show that the postselection probability satisfies the condition, then we can show that MGNM is in promise-AWPP. In this paper, however, we show a more direct proof without explicitly using the modified postBQP class. Our quantum algorithm is based on that of Watrous [4]. He showed that if the state $\sum_{g \in H} |g\rangle$, which is believed to be hard to generate with a polynomial-size quantum circuit, is given as a witness, GNM is verified efficiently. In our algorithm, the witness is generated by a polynomial-size quantum circuit with postselection. This result itself means $\text{GNM} \in \text{postBQP} = \text{PP}$, which is trivial since it is already known that $\text{QMA} \subseteq \text{SBQP} \subseteq \text{PP}$. Our contribution is that we point out that the postselection probability satisfies a nice condition, and therefore if the GNM is modified as described above, it is in promise-AWPP.

Note that since promise-AWPP is closed under complement, modified group membership, which is defined by replacing the question of MGNM into “Is $h \in H$?”, is also in promise-AWPP.

2 Proof

Now we show our result that MGNM is in promise-AWPP relative to any group oracle. First, let us remember the group oracle and a theorem shown by Babai [2]. A group oracle $B$ can be represented by a family of bijections $\{B_n\}$ with each member having the form $B_n : \{0, 1\}^{2n+2} \rightarrow \{0, 1\}^{2n+2}$ and satisfying certain constraints that specify its operation (see Section 2 in Ref. [4] for the precise definition). We denote the group associated with each $B_n$ by $G(B_n)$. In other words, elements of $G(B_n)$ form some subset of $\{0, 1\}^n$ and the group structure of $G(B_n)$ is determined by the function $B_n$. The following theorem by Babai [2] (see also Ref. [4]) is a basis of our result.

**Theorem 1** For any group oracle $B = \{B_n\}$, there exists a randomized procedure $P$ acting as follows: On input $g_1, ..., g_k \in G(B_n)$ and $\epsilon > 0$, the procedure outputs an element of $H \equiv \langle g_1, ..., g_k \rangle$ in time polynomial in $n + \log \frac{1}{\epsilon}$ such that each $g \in H$ is output with probability in the range $(\frac{1}{|H|} - \epsilon, \frac{1}{|H|} + \epsilon)$.

As is explained in Ref. [4], we can simulate the classical randomized procedure $P$ in a “quantum way”: Let us assume that a random bit is generated $s(n, \epsilon)$ times during $P$, where $s$ is a polynomial in $n$ and $\log(1/\epsilon)$. For simplicity, we write $s \equiv s(n, \epsilon)$. We first generate the state

$$\frac{1}{\sqrt{N}} \sum_{z \in \{0, 1\}^s} |z\rangle,$$

where $N \equiv 2^n$, $|z\rangle$ is an $s$-qubit state, and each $z$ is an $s$-bit string representing random numbers generated during $P$. By coupling sufficiently many ancilla qubits and running $P$ for each branch controlled by $z$, we obtain

$$|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{z \in \{0, 1\}^s} |\eta_z\rangle \otimes |\phi_z\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{g \in H} \sqrt{\gamma_g} |g\rangle \otimes |\text{garbage}(g)\rangle,$$
where $\eta_z$ is an element of $H$, $\phi_z$ is a $t(n, \epsilon)$-bit string corresponding to the leftover of the procedure ($t$ is a polynomial in $n$ and $\log(1/\epsilon)$; for simplicity we write $t \equiv t(n, \epsilon)$, and

$$|\text{garbage}(g)\rangle \equiv \frac{1}{\sqrt{|g|}} \sum_{z: \eta_z = g} |\phi_z\rangle.$$  

Here, $\gamma_g$ is the normalization factor, i.e., the number of $z$ such that $\eta_z = g$. From Theorem 1,

$$\gamma_g \in \left(\frac{1}{|H|} - \epsilon, \frac{1}{|H|} + \epsilon\right).  \quad (1)$$  

Furthermore, due to the normalization of $|\Psi\rangle$,

$$\sum_{g \in H} \gamma_g = 1.$$  

Therefore if we write

$$\frac{\gamma_g}{N} = \frac{1}{|H|} + \epsilon_g,$$

where $-\epsilon \leq \epsilon_g \leq \epsilon$, we obtain $\sum_{g \in H} \epsilon_g = 0$. Hence,

$$\sum_{g \in H} \left(\frac{\gamma_g}{N}\right)^2 = \frac{1}{|H|} + \frac{2}{|H|} \sum_{g \in H} \epsilon_g + \sum_{g \in H} \epsilon_g^2 = \frac{1}{|H|} + \sum_{g \in H} \epsilon_g^2 \quad (2)$$

$$\geq \frac{1}{|H|}. \quad (3)$$

Let us couple $|\Psi\rangle$ with $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$ and apply a controlled multiplication by the element $h$ to obtain

$$|\Psi'\rangle \equiv \frac{1}{\sqrt{2N}} \sum_{g \in H} \sqrt{\gamma_g} \left(|g\rangle \otimes |0\rangle + |gh\rangle \otimes |1\rangle\right) \otimes |\text{garbage}(g)\rangle,$$

where the second register is the coupled qubit. Let us apply an Hadamard gate on the second register:

$$\frac{1}{2\sqrt{N}} \sum_{g \in H} \sqrt{\gamma_g} \left(|g\rangle + |gh\rangle\right)\left(00\rangle + (|g\rangle - |gh\rangle)\langle 0|1\rangle\right)\otimes |\text{garbage}(g)\rangle.$$

Let us prepare two copies of them, and add an ancilla qubit $|1\rangle_a$:

$$\frac{1}{4N} \sum_{g, g' \in H} \sqrt{\gamma_g} \sqrt{\gamma_{g'}} \left[ (|g\rangle + |gh\rangle)(|g'\rangle + |gh'\rangle)|00\rangle|1\rangle_a + (|g\rangle + |gh\rangle)(|g'\rangle - |gh'\rangle)|01\rangle|1\rangle_a + (|g\rangle - |gh\rangle)(|g'\rangle + |gh'\rangle)|10\rangle|1\rangle_a + (|g\rangle - |gh\rangle)(|g'\rangle - |gh'\rangle)|11\rangle|1\rangle_a \right] |\text{garbage}(g)\rangle |\text{garbage}(g')\rangle.$$
Modified group non-membership is in promise-AWPP relative to group oracles

Flip the ancilla qubit if the third register of the above state is in the state $|00\rangle$:

$$\frac{1}{4N} \sum_{g, g' \in H} \sqrt{\gamma_g \gamma_{g'}} \left[ (|g\rangle + |gh\rangle)(|g'\rangle + |g'h\rangle)|00\rangle|0\rangle_a 
+ (|g\rangle + |gh\rangle)(|g'\rangle - |g'h\rangle)|01\rangle|1\rangle_a 
+ (|g\rangle - |gh\rangle)(|g'\rangle + |g'h\rangle)|10\rangle|1\rangle_a 
+ (|g\rangle - |gh\rangle)(|g'\rangle - |g'h\rangle)|11\rangle|1\rangle_a \right] |\text{garbage}(g)\rangle |\text{garbage}(g')\rangle.$$  

Note that

$$\langle +^{\otimes t}|\text{garbage}(g)\rangle = \frac{1}{\sqrt{\gamma_g}} \sum_{z: n_z = g} \langle +^{\otimes t} |\phi_z\rangle$$

$$= \frac{1}{\sqrt{\gamma_g^{2^t}}} \gamma_g$$

$$= \frac{\sqrt{\gamma_g}}{\sqrt{2^t}}.$$  

Therefore, if we postselect garbage registers onto $|+\rangle^{\otimes 2^t}$, the (unnormalized) state after the postselection is

$$\frac{1}{4N^{2^t}} \sum_{g, g' \in H} \gamma_g \gamma_{g'} \left[ (|g\rangle + |gh\rangle)(|g'\rangle + |g'h\rangle)|00\rangle|0\rangle_a 
+ (|g\rangle + |gh\rangle)(|g'\rangle - |g'h\rangle)|01\rangle|1\rangle_a 
+ (|g\rangle - |gh\rangle)(|g'\rangle + |g'h\rangle)|10\rangle|1\rangle_a 
+ (|g\rangle - |gh\rangle)(|g'\rangle - |g'h\rangle)|11\rangle|1\rangle_a \right].$$  

Let us denote this state by

$$\frac{1}{4N^{2^t}} \left[ |h_+\rangle|h_+\rangle|00\rangle|0\rangle_a + |h_+\rangle|h_-\rangle|01\rangle|1\rangle_a + |h_-\rangle|h_+\rangle|10\rangle|1\rangle_a + |h_-\rangle|h_-\rangle|11\rangle|1\rangle_a \right],$$

where

$$|h_\pm\rangle = \sum_{g \in H} \gamma_g (|g\rangle \pm |gh\rangle).$$  

The square of the norm of the state, i.e., the postselection probability, is

$$P(p = 1) = \frac{1}{16N^{2^t}} \left( \langle h_+|h_+\rangle + \langle h_-|h_-\rangle \right)^2$$

$$= \frac{(\sum_{g \in H} \gamma_g^2)^2}{N^{2^t}2^{2^t}}$$

$$= \frac{N^2(\sum_{g \in H} \gamma_g^2)^2}{N^{4^t}2^{2^t}}$$

$$= \frac{N^2(\sum_{g \in H} \gamma_g^2)^2}{2^{2^t}}$$

$$= \frac{1}{2^{2^t-2^t}} \left( \frac{1}{|H|} + \sum_{g \in H} c_g^2 \right)^2,$$
where we mean $p = 1$ if the garbage registers are projected onto $|+\rangle^{\otimes 2t}$, and we have used $N = 2^s$, Eq. (2), and the relation

$$\langle h_+|h_+ \rangle + \langle h_-|h_- \rangle = 4 \sum_{g \in H} \gamma_g^2,$$

Therefore, from Eq. (4), the normalized state after the postselection is

$$\frac{1}{4 \sum_{g \in H} \gamma_g^2}[|h_+\rangle|h_+\rangle|00\rangle|0\rangle_a + |h_+\rangle|h_-\rangle|01\rangle|1\rangle_a + |h_-\rangle|h_+\rangle|10\rangle|1\rangle_a + |h_-\rangle|h_-\rangle|11\rangle|1\rangle_a].$$

If we project the ancilla qubit onto $|0\rangle_a$, the (unnormalized) state after the projection is

$$\frac{1}{4 \sum_{g \in H} \gamma_g^2}|h_+\rangle|h_+\rangle|00\rangle,$$

and therefore,

$$P(o = 0|p = 1) = \left(\frac{\langle h_+|h_+ \rangle}{4 \sum_{g \in H} \gamma_g^2}\right)^2.$$

Here, we mean $o = 0$ (resp., $o = 1$) if the ancilla qubit is projected onto $|0\rangle_a$ (resp., $|1\rangle_a$). If $h \notin H$,

$$\langle h_+|h_+ \rangle = 2 \sum_{g \in H} \gamma_g^2$$

and therefore,

$$P(o = 0|p = 1) = \frac{1}{4},$$

$$P(o = 1|p = 1) = 1 - P(o = 0|p = 1) = \frac{3}{4}.$$

If $h \in H$, on the other hand,

$$P(o = 1|p = 1) = 1 - P(o = 0|p = 1)$$

$$= 1 - \left(\frac{\langle h_+|h_+ \rangle}{4 \sum_{g \in H} \gamma_g^2}\right)^2$$

$$= 1 - \left(\frac{4 \sum_{g \in H} \gamma_g^2 - \langle h_-|h_- \rangle}{4 \sum_{g \in H} \gamma_g^2}\right)^2$$

$$= 1 - \left(1 - \frac{\langle h_-|h_- \rangle}{4 \sum_{g \in H} \gamma_g^2}\right)^2$$

$$= 1 - \left(1 - \frac{\langle h_-|h_- \rangle}{2 \sum_{g \in H} \gamma_g^2} + \left(\frac{\langle h_-|h_- \rangle}{4 \sum_{g \in H} \gamma_g^2}\right)^2\right)$$

$$\leq \frac{\langle h_-|h_- \rangle}{2 \sum_{g \in H} \gamma_g^2}$$

$$= \frac{\sum_{g \in H} (\gamma_g - \gamma_{gh^{-1}})^2}{2 \sum_{g \in H} \gamma_g^2}.$$
Modified group non-membership is in promise-AWPP relative to group oracles

\[ \text{Modified group non-membership is in promise-AWPP relative to group oracles} \]

\[ \leq \frac{4\epsilon^2 |H|}{2 \sum_{g \in H} \gamma_g^2} \leq 2\epsilon^2 |H|^2. \]

(6)

Here, we have used Eqs. (1) and (3), and

\[ \langle h_\perp | h_\perp \rangle = \sum_{g,g' \in H} \gamma_g \gamma_{g'}(|g\rangle - (gh)|g\rangle - |g'\rangle - |g'h\rangle) \]

\[ = \sum_{g,g' \in H} \gamma_g \gamma_{g'}(\delta_{g,g'} - \delta_{g,g'h} - \delta_{g'h} + \delta_{g,g'}) \]

\[ = \sum_{g \in H} \gamma_g^2 - \sum_{g \in H} \gamma_g \gamma_{gh^{-1}} - \sum_{g' \in H} \gamma_{g'h^{-1}} \gamma_{g'} + \sum_{g \in H} \gamma_g^2 \]

\[ = \sum_{g \in H} \gamma_g^2 - \sum_{g \in H} \gamma_g \gamma_{gh^{-1}} - \sum_{g \in H} \gamma_{gh^{-1}} \gamma_{g} + \sum_{g \in H} \gamma_{gh^{-1}}^2 \]

\[ = \sum_{g \in H} (\gamma_g - \gamma_{gh^{-1}})^2. \]

Now we use the result by Fortnow and Rogers [10]:

**Theorem 2** For any uniform family of polynomial-size quantum circuits, there exist \( g \in \text{GapP} \) and a polynomial \( q \) such that for any \( w \), the output probability of the quantum circuit on input \( w \) is equal to \( g(w) / 2^q(1) \). (Note that this theorem depends on the gate set. In this paper, we consider the Hadamard and Toffoli gates as a universal gate set.)

From this theorem, there exist a GapP function \( g \) and a polynomial \( q \) such that

\[ P(o = 1, p = 1) = \frac{g(w)}{2^q(n)}, \]

where \( w \) is an input of MGNM. In the above, we have shown that if \( w \) is a “yes” instance of MGNM, which means \( h \notin H \),

\[ \frac{3}{4} = P(o = 1 | p = 1) \leq 1, \]

which means

\[ \frac{3}{4} P(p = 1) = P(o = 1, p = 1) \leq P(p = 1). \]

From Eq. (7), it is

\[ \frac{3}{4} P(p = 1) = \frac{g(w)}{2^q(n)} \leq P(p = 1). \]

From Eq. (5) and \( |H| \leq 2^n \), this means

\[ \frac{1}{2^{2t-2s}} \left( \frac{1}{|H|} + \sum_{g \in H} \epsilon_g^2 \right)^{2} \leq \frac{1}{2^{2t-2s}} \left( \frac{1}{|H|} + \sum_{g \in H} \epsilon_g^2 \right)^{2} \]

\[ \Leftrightarrow \]

\[ \left( 1 + |H| \sum_{g \in H} \epsilon_g^2 \right)^{2} \leq \frac{g(w)2^{2t-2s} |H|^2}{2^q(n)} \leq \left( 1 + |H| \sum_{g \in H} \epsilon_g^2 \right)^{2} \]
\[ \frac{3}{4} \leq \frac{g(w)2^{2t-2s}|H|^2}{2^{q(n)}} \leq \left(1 + |H|^2 \epsilon^2 \right)^2 \]

\[ \frac{3}{4} \leq \frac{g(w)2^{2t-2s}|H|^2}{2^{q(n)}} \leq (1 + 2^{2n} \epsilon^2)^2 \]

\[ \frac{3}{4(1 + 2^{2n} \epsilon^2)^2} \leq \frac{g(w)2^{2t-2s}|H|^2}{2^{q(n)}(1 + 2^{2n} \epsilon^2)^2} \leq 1. \]

If we take \( \epsilon = 2^{-n-3} \) in Theorem 1,

\[ 2 \leq \frac{3}{4(1 + 2^{2n} \epsilon^2)^2}. \]

If we define

\[ G(w) = g(w)2^{2t-2s}|H|^2, \]

and

\[ F(w) = 2^{q(n)}(1 + 2^{2n} \epsilon^2)^2, \]

we thus obtain

\[ \frac{2}{3} \leq \frac{G(w)}{F(w)} \leq 1. \] (8)

By the definition of MGNM, \( |H| \in \text{FP}^B \subseteq \text{GapP}^B \). Since GapP functions are closed under multiplication, \( G \in \text{GapP}^B \). Furthermore, since we can assume \( q(n) \geq 12 \) for all \( n \) without loss of generality, we have \( F \in \text{FP}^B \) for our choice of \( \epsilon \).

On the other hand, if \( w \) is a “no” instance of MGNM, which means \( h \in H \), we obtain from Eqs. (7) and (6) that

\[ 0 \leq \frac{g(w)}{2^{q(n)}} \leq 2\epsilon^2|H|^2P(p = 1) \]

\[ 0 \leq \frac{g(w)}{2^{q(n)}} \leq 2\epsilon^2|H|^2 \frac{1}{2^{2t-2s}} \left( \frac{1}{|H|} + \sum_{g \in H} \epsilon_g \right)^2 \]

\[ 0 \leq \frac{g(w)2^{2t-2s}|H|^2}{2^{q(n)}} \leq 2\epsilon^2|H|^2 \left( 1 + \epsilon^2|H|^2 \right)^2 \]

\[ 0 \leq \frac{g(w)2^{2t-2s}|H|^2}{2^{q(n)}(1 + 2^{2n} \epsilon^2)^2} \leq 2\epsilon^2|H|^2. \]
Modified group non-membership is in promise-AWPP relative to group oracles

Since $\epsilon = 2^{-n-3}$,

$$2\epsilon^2|H|^2 \leq 2^{-5} \leq \frac{1}{3}.$$  

We thus obtain

$$0 \leq \frac{G(w)}{F(w)} \leq \frac{1}{3}.$$  

Since Eqs. (8) and (9) satisfy the definition of promise-AWPP, we conclude that MGNM is in promise-AWPP$^B$.

Acknowledgements

TM is supported by the JSPS Grant-in-Aid for Young Scientists (B) No.26730003 and the MEXT JSPS Grant-in-Aid for Scientific Research on Innovative Areas No.15H00850. HN is supported by the JSPS Grant-in-Aid for Scientific Research (A) Nos.23246071, 24240001, 26247016, and (C) No.25330012, and the MEXT JSPS Grant-in-Aid for Scientific Research on Innovative Areas No.24106009. FLG is supported by the JSPS Grant-in-Aid for Young Scientists (A) No. 16H05853, the JSPS Grant-in-Aid for Young Scientists (B) No. 24700005, the JSPS Grant-in-Aid for Scientific Research (A) No. 24240001, and the MEXT JSPS Grant-in-Aid for Scientific Research on Innovative Areas No. 24106009.

References

1. L. Babai and E. Szemerédi, On the complexity of matrix group problems I. Proc. of the 25th Ann. IEEE Sympo. on Found. of Comput. Sci. pp.229-240 (1984).
2. L. Babai, Local expansion of vertex-transitive graphs and random generation in finite groups. In Proc. of 23rd Ann. ACM Sympo. on Theor. of Comput. pp.164-174 (1991).
3. L. Babai, Bounded round interactive proofs in finite groups. SIAM J. Disc. Math. 5, pp.88-111 (1992).
4. J. Watrous, Succinct quantum proofs for properties of finite groups. Proc. of the 41st Ann. IEEE Sympo. on Found. of Comput. Sci. pp.537-546 (2000).
5. J. Watrous, Quantum algorithms for solvable groups. Proc. of the 33rd ACM Sympo. on Theor. of Comput. pp.60-67 (2001).
6. N. V. Vinodchandran, Counting complexity of solvable black-box group problems. SIAM J. Comput. 33, pp.852-869 (2004).
7. S. Fenner, L. Fortnow, S. Kurtz, and L. Li, An oracle builder’s toolkit. Inf. Comput. 182, 95-136 (2003); Earlier version in Proc. 8th IEEE Conference on Structure in Complexity Theory, pp.120-131 (1993).
8. S. A. Fenner, PP-lowness and a simple definition of AWPP. Theory Comput. Syst. 36, 199-212 (2003); ECCC Report TR02-036.
9. L. Li, On the counting functions. Ph.D. thesis, University of Chicago (1993).
10. L. Fortnow and J. Rogers, Complexity limitations on quantum computation. J. Comput. Syst. Sci. 59, 240-252 (1999).
11. M. N. Vyalyi, QMA = PP implies that PP contains PH. ECCC, Report No.21 (2003).
12. S. Fenner, L. Fortnow, and S. Kurtz, Gap-definable counting classes. J. Comput. Syst. Sci. 48, 116-148 (1994).
13. S. Aaronson, Quantum computing, postselection, and probabilistic polynomial-time. Proc. R. Soc. A 461, 3473-3482 (2005).
14. T. Morimae and H. Nishimura, Quantum interpretations of AWPP and APP. Quant. Inf. Comput. 16, 0498-0514 (2016).