Schrödinger’s Ballot: Quantum Information and the Violation of Arrow’s Impossibility Theorem

Xin Sun
Department of the Foundations of Computer Science, the John Paul II Catholic University of Lublin, Lublin, Poland
Quantum Blockchains Inc., Pulawy, Poland
xin.sun.logic@gmail.com

Feifei He*
Institute of Logic and Cognition, Sun Yat-sen University, Guangzhou, China
heff5@mail2.sysu.edu.cn

Piotr Kulicki
Department of the Foundations of Computer Science, the John Paul II Catholic University of Lublin, Lublin, Poland
Quantum Blockchains Inc., Pulawy, Poland
kulicki@kul.pl

Mirek Sopek
MakoLab SA, Lodz, Poland
Quantum Blockchains Inc., Pulawy, Poland
sopek@makolab.com

In this paper we study Arrow’s Impossibility Theorem in the quantum setting. Our work is based on the work of Bao and Halpern [3], in which it is proved that the quantum analogue of Arrow’s Impossibility Theorem is not valid. However, we feel unsatisfied about the proof presented in [3]. Moreover, the definition of Quantum Independence of Irrelevant Alternatives (QIIA) in [3] seems not appropriate to us. In this paper, we give a better definition of QIIA, which properly captures the idea of the independence of irrelevant alternatives, and a detailed proof of the violation of Arrow’s Impossibility Theorem in the quantum setting with the modified definition.

Keywords: vote, quantum information, Arrow’s Impossibility Theorem, social choice

1 Introduction

Many voting protocols based on classical cryptography have been developed and successfully applied since Chaum et al. [5]. However, the security of protocols based on classical cryptography is based on the unproven complexity of some computational algorithms, such as factoring of large numbers. The research in quantum computation shows that quantum computers are able to factor large numbers in a short time, which means that classical protocols based on such algorithms are already insecure. To react to the risk posed by forthcoming quantum computers, a number of quantum voting protocols have been developed in the last decade [8, 24, 11, 9, 10, 22, 25, 21, 20].

While all these works have focused on the security problems of voting from a cryptographic perspective, Bao and Halpern [3] studied quantum voting from a social choice theoretic perspective by showing

*Corresponding author
that the quantum analog of Arrow’s Impossibility Theorem is violated in the quantum setting. Bao and Halpern’s [3] idea and results are equally interesting. However, we feel unsatisfied about the proof presented in [3]. Moreover, the definition of the Quantum Independence of Irrelevant Alternatives (QIIA) in [3] seems not appropriate to us. In this paper, we give a better definition of QIIA, which properly captures the idea of independence of irrelevant alternatives, and a detailed proof of the violation of Arrow’s Impossibility Theorem in the quantum setting with the modified definition.

The structure of this paper is as follows. We review some background knowledge on classical and quantum voting in Section 2. In section 3 we introduce a voting rule called quantum Condorcet voting and prove that Arrow’s Impossibility Theorem is violated by quantum Condorcet voting. We discuss related work in Section 4 and conclude this paper with the plan for the future work in Section 5. Some primitives of the quantum information theory which are used in this paper are collected in the appendix.

2 Background

2.1 Classical voting system

Now we succinctly review the theory of classical voting. A more detailed introduction to the classical voting and social choice theory can be found in Zwicker [28], Pacuit [15] and Brandt et al. [4].

Let $\mathcal{V} = \{v_1, \ldots, v_n\}$ be a finite set of (at least two) voters and $\mathcal{C} = \{c_1, c_2, \ldots, c_n\}$ be a non-empty set of candidates. Each voter $v_i \in \mathcal{V}$ is endowed with preference $\succ_i$ over $\mathcal{C}$. The preference $\succ_i$ is a binary relation on $\mathcal{C}$ that is irreflexive, transitive, and complete. In other words, $\succ_i$ is a linear order on $\mathcal{C}$. Let $\mathcal{L}(\mathcal{C})$ denote the set of all linear orders on $\mathcal{C}$. A profile $R = (R_1, \ldots, R_n) \in \mathcal{L}(\mathcal{C})^n$ is a vector of linear orders (i.e., preferences), where $R_i$ is the linear order supplied by voter $v_i$. We write $\mathcal{V}^R_{x\succ y}$ to denote the set of voters that rank candidate $x$ above candidate $y$ under profile $R$. A Social Welfare Function (SWF) is a function $F : \mathcal{L}(\mathcal{C})^n \rightarrow \mathcal{L}(\mathcal{C})$. Two widely accepted properties of SWF are unanimity and independence of irrelevant alternatives.

**Definition 1 (Unanimity)** A SWF $F$ satisfies the unanimity condition if, whenever all voters rank $x$ above $y$, then so does society:

$$\mathcal{V}^R_{x\succ y} = \mathcal{V} \implies (x, y) \in F(R).$$

**Definition 2 (Independence of Irrelevant Alternatives (IIA))** An SWF $F$ satisfies IIA if the relative social ranking of two candidates only depends on their relative voter rankings:

$$\mathcal{V}^R_{x\succ y} = \mathcal{V}^R_{x\succ y} \implies (x, y) \in F(R) \iff (x, y) \in F(R').$$

The intuition about IIA is that two ballot profiles that are similar according to $(x, y)$ should produce the same ranking. This intuition will be used later to define the quantum analogue of IIA.

The celebrated Arrow’s Impossibility Theorem states that any SWF that satisfies both unanimity and the IIA must also satisfy a property which any SWF should not satisfy: dictatorship.

**Definition 3 (Dictatorship)** An SWF $F$ satisfies dictatorship if there is a voter $v_i \in \mathcal{V}$ such that $F(R) = R_i$ for every profile $R = (R_1, \ldots, R_n)$.

**Theorem 1 (Arrow [2])** Any SWF for three or more candidates that satisfies unanimity and the IIA cannot satisfy nondictatorship.
2.2 Quantum voting system

Now we introduce our formalism of quantum voting system, which is similar to the formalism of Bao and Halpern [3]. In a quantum voting system with candidates \( \mathcal{C} = \{c_1, c_2, \ldots, c_n\} \), we specify a Hilbert space \( H \) of which the dimension is \( |\mathcal{C}| \). That is, \( H = \mathbb{C}^{\mathcal{C}} \). Every voter \( v_i \in \mathcal{V} \) is associated with a Hilbert space \( H_i \) which is isomorphic to \( H \). Every linear order \( R \in \mathcal{L}(\mathcal{C}) \) is naturally viewed as basis vector \( |R\rangle \) of \( H \). The basis \( \mathcal{B} = \{|R_1^1\rangle, \ldots, |R_{|\mathcal{C}|}^{|\mathcal{C}|}\rangle\rangle \) is called the preference basis for \( H_i \).

Consider a pair \((x, y)\) of candidates. \( H \) decomposes into subspaces associated with the possible relationships between \( x \) and \( y \). By \( S^{x>y} \), we denote the subspace spanned by the \( B \) elements that encode \( x \succ y \) (e.g. \([x \succ y \succ z], [z \succ x \succ y] \) ). We use \( \Pi^{x>y} \) to denote the projector onto the subspace \( S^{x>y} \).

A quantum ballot of voter \( v_i \) is a density operator \( \rho \in D(H_i) \). A quantum ballot profile is a density operator \( \rho \in H_1 \otimes \ldots \otimes H_n \). A basis quantum ballot profile is a profile in which every component is a density operator of a basis vector. A quantum social welfare function (QSWF) is linear map \( \mathcal{E} : D(H_1 \otimes \ldots \otimes H_n) \rightarrow D(H) \). The result of voting with quantum ballot profile \( \rho \) is obtained by measuring \( \mathcal{E}(\rho) \) on the preference basis.

**Definition 4 (Quantum Unanimity [3])** A QSWF \( \mathcal{E} \) satisfies the sharp unanimity condition if it satisfies the following:

- For all quantum ballot profile \( \rho \) and all pairs of candidates \((x, y)\), if \( \text{Tr}(\Pi^{x>y}(\text{Tr}_{\neq i}(\rho))) = 1 \) for each voter \( v_i \), then \( \text{Tr}(\Pi^{x>y}(\mathcal{E}(\rho))) = 1 \).

A QSWF \( \mathcal{E} \) satisfies the unsharp unanimity condition if it satisfies the following:

- For all quantum ballot profile \( \rho \) and all pairs of candidates \((x, y)\), if \( \text{Tr}(\Pi^{x>y}(\text{Tr}_{\neq i}(\rho))) > 0 \) for each voter \( v_i \), then \( \text{Tr}(\Pi^{x>y}(\mathcal{E}(\rho))) > 0 \).

A QSWF \( \mathcal{E} \) satisfies the quantum unanimity condition if it satisfies both sharp and unsharp unanimity conditions.

**Definition 5 (Quantum Independence of Irrelevant Alternatives (QIIA))** A QSWF \( \mathcal{E} \) satisfies the sharp IIA condition if it satisfies the following:

- For all quantum ballot profile \( \rho \) and \( \rho' \) and all pairs of candidates \((x, y)\), if \( \text{Tr}(\Pi^{x>y}(\text{Tr}_{\neq i}(\rho))) = \text{Tr}(\Pi^{x>y}(\text{Tr}_{\neq i}(\rho'))) \) and \( \text{Tr}(\Pi^{x>y}(\text{Tr}_{\neq i}(\rho))) = \text{Tr}(\Pi^{x'y}(\text{Tr}_{\neq i}(\rho'))) \) for each voter \( v_i \), then \( \text{Tr}(\Pi^{x>y}(\mathcal{E}(\rho))) = 1 \) implies that \( \text{Tr}(\Pi^{x>y}(\mathcal{E}(\rho'))) = 1 \).

A QSWF \( \mathcal{E} \) satisfies unsharp IIA if the following condition is satisfied:

- For all quantum ballot profile \( \rho, \rho' \) and all pairs of candidates \((x, y)\), if \( \text{Tr}(\Pi^{x>y}(\text{Tr}_{\neq i}(\rho))) = \text{Tr}(\Pi^{x'y}(\text{Tr}_{\neq i}(\rho'))) \) and \( \text{Tr}(\Pi^{x'y}(\text{Tr}_{\neq i}(\rho))) = \text{Tr}(\Pi^{x'y}(\text{Tr}_{\neq i}(\rho'))) \) for each voter \( v_i \), then \( \text{Tr}(\Pi^{x>y}(\mathcal{E}(\rho))) > 0 \) implies that \( \text{Tr}(\Pi^{x'y}(\mathcal{E}(\rho'))) > 0 \).

A QSWF \( \mathcal{E} \) satisfies the QIIA condition if it satisfies both sharp and unsharp IIA conditions.

Note that QIIA in our definition is different from the QIIA in [3]. QIIA in [3] states that whether \( \mathcal{E}(\rho) \) has support on \( S^{x>y} \) only depends on whether each \( \rho_i \) has support on \( S^{x>y} \) and \( S^{x'y} \). More precisely, it states that for all quantum ballot profile \( \rho, \rho' \) and all pairs of candidates \((x, y)\), if \( \text{Tr}(\Pi^{x>y}(\text{Tr}_{\neq i}(\rho))) > 0 \) iff \( \text{Tr}(\Pi^{x>y}(\text{Tr}_{\neq i}(\rho'))) > 0 \) and \( \text{Tr}(\Pi^{x'y}(\text{Tr}_{\neq i}(\rho))) > 0 \) iff \( \text{Tr}(\Pi^{x'y}(\text{Tr}_{\neq i}(\rho'))) > 0 \) for each voter \( v_i \), then \( \text{Tr}(\Pi^{x>y}(\mathcal{E}(\rho))) > 0 \) implies that \( \text{Tr}(\Pi^{x'y}(\mathcal{E}(\rho'))) > 0 \).
4 Quantum Information and the Violation of Impossibility Theorems of Voting in Social Choice Theory

The intuition of QIIA is the same as the intuition of classical IIA: it states that two ballot profiles that are similar according to \((x, y)\) should produce the same ranking for \((x, y)\). It seems Bao and Halpern [3] considered two ballot profiles \(\rho\) and \(\rho'\) to be similar according to \((x, y)\) as long as \(\text{Tr}(\Pi^{x>y}(\text{Tr}_\rho(\rho'))) > 0\) iff \(\text{Tr}(\Pi^{y>x}(\text{Tr}_\rho(\rho'))) > 0\) and \(\text{Tr}(\Pi^{x->}(\text{Tr}_\rho(\rho'))) > 0\) iff \(\text{Tr}(\Pi^{y->}(\text{Tr}_\rho(\rho'))) > 0\). To us this requirement is too weak. For example, \(\rho = 0.99|x > y > z|\) \((x > y > z) \cup 0.01|y > x > z|\) and \(\rho' = 0.01|x > y > z|\) \((x > y > z) \cup 0.99|y > x > z|\) are similar according to \((x, y)\) in our definition, but intuitively they should not be. On the other hand, \(\rho\) and \(\rho'\) are not similar according to \((x, y)\) in our definition. Indeed, two profiles \(\rho\) and \(\rho'\) are similar according to \((x, y)\) in our definition only if \(\text{Tr}(\Pi^{x>y}(\text{Tr}_\rho(\rho'))) = 1\) and \(\text{Tr}(\Pi^{y>x}(\text{Tr}_\rho(\rho'))) = 1\) and \(\text{Tr}(\Pi^{x->}(\text{Tr}_\rho(\rho'))) = 1\) and \(\text{Tr}(\Pi^{y->}(\text{Tr}_\rho(\rho'))) = 1\).

We believe our definition of QIIA properly capture the idea of independence of irrelevant alternatives. That’s why we use it to replace the QIIA of Bao and Halpern [3].

**Definition 6 (Quantum Dictatorship [3])** A QSWF \(\mathcal{E}\) satisfies sharp dictatorship if there is a voter \(v_i\) such that:

- For all quantum ballot profile \(\rho = (\rho_1, \ldots, \rho_n)\) and all pairs of candidates \((x, y)\), \(\text{Tr}(\Pi^{x>y}(\mathcal{E}(\rho))) = 1\) iff \(\text{Tr}(\Pi^{y>x}(\mathcal{E}(\rho))) = 1\).

A QSWF \(\mathcal{E}\) satisfies unsharp dictatorship if there is a voter \(v_i\) such that:

- For all quantum ballot profile \(\rho = (\rho_1, \ldots, \rho_n)\) and all pairs of candidates \((x, y)\), \(\text{Tr}(\Pi^{x>y}(\mathcal{E}(\rho))) > 0\) iff \(\text{Tr}(\Pi^{y>x}(\mathcal{E}(\rho))) > 0\).

A QSWF \(\mathcal{E}\) satisfies quantum dictatorship if it satisfies both sharp and unsharp dictatorship.

3 Quantum Condorcet voting and Arrow’s Impossibility Theorem

We will use a special voting rule called Quantum Condorcet Voting \(\mathcal{E}_\text{qcv}\) to disprove Arrow’s Impossibility Theorem in the quantum setting. Since \(\mathcal{E}_\text{qcv}\) is a linear map from \(D(H_1 \otimes \ldots \otimes H_n)\) to \(D(H)\), we only need to specify how \(\mathcal{E}_\text{qcv}\) operates on a basis quantum ballot profile.

**Definition 7 (Quantum Condorcet Voting)** Let \(\rho_1 \otimes \ldots \otimes \rho_n\) be a basis quantum ballot profile. The Quantum Condorcet Voting \(\mathcal{E}_\text{qcv}\) operates in the following steps:

1. **Calculate the Condorcet score of each candidate according to \(\rho_1 \otimes \ldots \otimes \rho_n\).** The Condorcet score of a candidate is the number of winning in pairwise comparison with other candidates. That is, for a candidate \(x\), his Condorcet score \(S_c(x)\) is \(|\{y \in \mathcal{E} : |\Pi_{x>y}^{R} \geq |\Pi_{y>x}^{R}\}|\) where \(R\) is the classical ballot profile corresponding to \(\rho_1 \otimes \ldots \otimes \rho_n\).

2. **Generate a weak order \(\succeq\) over all candidates according to their Condorcet score.** That is, \(x \succeq y\) iff \(S_c(x) \geq S_c(y)\).

3. **Complete the weak order.** That is, generate the set \(\{\succ, \ldots, \succ^m\}\) in which each \(\succ^i\) is a linear order that extends \(\succeq\) and \(\{\succ^1, \ldots, \succ^m\}\) contains all extensions of \(\succeq\).

4. **Transform the linear order into quantum states.** That is, for \(\{\succ^1, \ldots, \succ^m\}\) we create a quantum state \(\sigma^1 = \frac{1}{m} \sum_i \sigma_i\), where each \(\sigma_i\) is a basis ballot corresponds to \(\succ^i\).

5. **Give the minority a shot.** For any candidate pair \((x, y)\), which is encoded by at least one \(\rho_n\), we spread an amount \(\delta \in (0, 1)\) of weight across the \(x \succ y\) subspace. That is, \(\sigma^1\) is changed to \(\sigma^2 = (1 - k\delta)\sigma^1 + \delta \Pi_{x>y} \rho_1 + \ldots + \delta \Pi_{y>x} \rho_n\), where \((x_1, y_1), \ldots, (x_k, y_k)\) ranges over all candidate pairs that are encoded by at least one \(\rho_i\). The parameter \(\delta\) is required to satisfy that \(\delta < \frac{1}{|E|}\).
6. Enforce unanimity. For any candidate pair \((x, y)\) which is encoded by all \(\rho_i\), we project \(\sigma^2\) onto the \(x \succ y\) subspace. That is, \(\sigma^2\) is changed to \(\sigma^2 = \Pi^{x \succ y}_1 \ldots \Pi^{x \succ y}_n \sigma^2 \Pi^{x \succ y}_1 \ldots \Pi^{x \succ y}_n\), where \((x_1, y_1), \ldots, (x_k, y_k)\) ranges over all candidate pairs that are encoded by all \(\rho_i\).

Both giving the minority a shot and enforcing unanimity are first introduced in Bao and Halpern [3]. While they may look strange at first sight, both of them will be useful in disproving Arrow’s Impossibility Theorem.

**Theorem 2** The Quantum Condorcet Voting \(E_{qc}\) satisfies sharp unanimity.

**Proof:** Let \(\rho = \rho_1 \otimes \ldots \otimes \rho_n\) be a basis quantum ballot profile. If \(Tr(\Pi^{x \succ y}_i(\rho_i)) = 1\) for each voter \(v_i\), then each \(\rho_i\) encodes \(x \succ y\) since \(\rho_i\) is a basis ballot. Then the projector \(\Pi^{x \succ y}_i\) will be applied in the step of enforcing unanimity. Therefore, \(Tr(\Pi^{x \succ y}_i(E_{qc}(\rho))) = 1\).

Now let \(\rho\) be a quantum ballot profile such that \(Tr(\Pi^{x \succ y}_i(Tr_{\noti}(\rho))) = 1\) for each voter \(v_i\). Note that \(Tr(\Pi^{x \succ y}_i(Tr_{\noti}(\rho))) = 1\) implies that \(Tr(\Pi^{x \succ y}_i(\rho)) = x_i |\phi_i^{+}\rangle\langle \phi_i^{+}| + \ldots + x_m |\phi_m^{+}\rangle\langle \phi_m^{+}|\) where each \(\phi_j^{+}\) is a basis vector that encodes \(x \succ y\) and \(\sum_j x_j = 1\). Therefore, \(\rho = x_1^{+} \ldots x_n^{+} |\phi_1^{+}\rangle\langle \phi_1^{+}| \ldots \otimes |\phi_n^{+}\rangle\langle \phi_n^{+}|\) + \ldots + \(x_1^{+} \ldots x_m^{+} |\phi_1^{+}\rangle\langle \phi_1^{+}| \ldots \otimes |\phi_m^{+}\rangle\langle \phi_m^{+}|\). It then follows that \(Tr(\Pi^{x \succ y}_i(Tr_{\noti}(\rho)))(|\phi_1^{+}\rangle\langle \phi_1^{+}| \ldots \otimes |\phi_i^{+}\rangle\langle \phi_i^{+}|) = 1\) for all \(i\). Then we know that \(Tr(\Pi^{x \succ y}_i(E_{qc}(\rho)))(|\phi_1^{+}\rangle\langle \phi_1^{+}| \ldots \otimes |\phi_i^{+}\rangle\langle \phi_i^{+}|) = 1\) because \(|\phi_1^{+}\rangle\ldots \otimes |\phi_i^{+}\rangle\langle \phi_1^{+}\rangle\ldots \otimes |\phi_i^{+}\rangle\) is a basis quantum ballot profile. Therefore, we have \(Tr(\Pi^{x \succ y}_i(E_{qc}(\rho))) = x_1^{+} \ldots x_i^{+} \ldots + x_m^{+} \ldots = 1\).

**Theorem 3** The Quantum Condorcet Voting \(E_{qc}\) satisfies unsharp unanimity.

**Proof:** Let \(\rho = \rho_1 \otimes \ldots \otimes \rho_n\) be a basis quantum ballot profile where each \(\rho_i\) is a basis vector of \(H_i\). If \(Tr(\Pi^{x \succ y}_i(\rho_i)) > 0\) for each voter \(v_i\), then each \(\rho_i\) encodes \(x \succ y\) since \(\rho_i\) is a basis ballot. Then the projector \(\Pi^{x \succ y}_i\) will be applied in the step of enforcing unanimity. Therefore, \(Tr(\Pi^{x \succ y}_i(E_{qc}(\rho))) = 1 > 0\).

Now let \(\rho\) be a quantum ballot profile such that \(Tr(\Pi^{x \succ y}_i(Tr_{\noti}(\rho))) > 0\) for each voter \(v_i\). Note that \(Tr(\Pi^{x \succ y}_i(Tr_{\noti}(\rho))) > 0\) implies that \(Tr_{\noti}(\rho) = x_i |\phi_i\rangle\langle \phi_i| \ldots + \) for some basis vector \(|\phi_i\rangle\) which encodes \(x \succ y\) and \(0 < x_i \leq 1\). Hence \(\rho = x_1 \ldots x_n |\phi_1 \ldots \otimes |\phi_n\rangle\langle \phi_1 \ldots \otimes \phi_n| + \ldots + |\phi_1 \ldots \otimes \phi_n\rangle\langle \phi_1 \ldots \otimes \phi_n|\) is a basis quantum ballot profile in which each \(\phi_i\) encode \(x \succ y\). It then follows that \(Tr(\Pi^{x \succ y}_i(E_{qc}(\rho)))(|\phi_1 \ldots \otimes \phi_n\rangle\langle \phi_1 \ldots \otimes \phi_n|) = 1\). From \(0 < x_1 \ldots x_n \leq 1\) we now know that \(Tr(\Pi^{x \succ y}_i(E_{qc}(\rho))) > 0\).

**Theorem 4** The Quantum Condorcet Voting \(E_{qc}\) satisfies sharp IIA.

**Proof:** Let \(\rho = \rho_1 \otimes \ldots \otimes \rho_n\) and \(\rho' = \rho'_1 \otimes \ldots \otimes \rho'_n\) be two basis quantum ballot profiles. Assume \(Tr(\Pi^{x \succ y}_i(\rho_i)) = Tr(\Pi^{x \succ y}_i(\rho'_i))\) and \(Tr(\Pi^{x \prec y}_i(\rho_i)) = Tr(\Pi^{x \prec y}_i(\rho'_i))\) for each voter \(v_i\). If \(Tr(\Pi^{x \succ y}_i(E_{qc}(\rho))) = 1\), then we know \(x \succ y\) is encoded by all \(\rho_i\). For otherwise \(\Pi^{x \prec y}_i\) will appear in \(\sigma^2\) in the step of giving the minority a shot, making \(Tr(\Pi^{x \prec y}_i(E_{qc}(\rho))) < 1\). Since \(Tr(\Pi^{x \succ y}_i(\rho_i)) = Tr(\Pi^{x \succ y}_i(\rho'_i))\) and \(Tr(\Pi^{x \prec y}_i(\rho_i)) = Tr(\Pi^{x \prec y}_i(\rho'_i))\) for each voter \(v_i\), we know that \(x \succ y\) is encoded by all \(\rho'_i\). Hence \(Tr(\Pi^{x \succ y}_i(E_{qc}(\rho'_i))) = 1\).

Now, let \(\rho\) and \(\rho'\) be quantum ballot profiles such that \(Tr(\Pi^{x \succ y}_i(Tr_{\noti}(\rho))) = Tr(\Pi^{x \succ y}_i(Tr_{\noti}(\rho')))\) and \(Tr(\Pi^{x \prec y}_i(Tr_{\noti}(\rho))) = Tr(\Pi^{x \prec y}_i(Tr_{\noti}(\rho')))\) for each voter \(v_i\). If \(Tr(\Pi^{x \succ y}_i(E_{qc}(\rho))) = 1\), then we know \(x \succ y\) is encoded by all \(\rho_i\). For otherwise \(\Pi^{x \prec y}_i\) will appear in \(\sigma^2\) in the step of giving the minority a shot and \(\Pi^{x \prec y}_i\) will not appear in \(\sigma^3\) in the step of enforcing unanimity, making \(Tr(\Pi^{x \prec y}_i(E_{qc}(\rho))) < 1\). Since \(Tr(\Pi^{x \succ y}_i(\rho_i)) = Tr(\Pi^{x \succ y}_i(\rho'_i))\) and \(Tr(\Pi^{x \prec y}_i(\rho_i)) = Tr(\Pi^{x \prec y}_i(\rho'_i))\) for each voter \(v_i\), we know that \(x \succ y\) is encoded by all \(\rho'_i\). Hence \(Tr(\Pi^{x \succ y}_i(E_{qc}(\rho'_i))) = 1\).

**Theorem 5** The Quantum Condorcet Voting \(E_{qc}\) satisfies unsharp IIA.
Proof: Let $\rho = \rho_1 \otimes \ldots \otimes \rho_n$ and $\rho' = \rho'_1 \otimes \ldots \otimes \rho'_n$ be two basis quantum ballot profiles. Assume $\text{Tr}((\Pi^{y\succ x}(\rho_i))) = \text{Tr}((\Pi^{y\succ x}(\rho'_i)))$ and $\text{Tr}((\Pi^{x\succ z}(\rho_i))) = \text{Tr}((\Pi^{x\succ z}(\rho'_i)))$ for each voter $v_i$. Now, if $\text{Tr}((\Pi^{y\succ x}(\mathcal{E}(\rho)))) > 0$, then $y > x$ is not encoded by all candidates. Without loss of generality, let’s assume $\rho_1$ encodes $x > y$ but not $y > x$. Then $\rho'_1$ also encodes $x > y$ but not $y > x$. Hence $\text{Tr}((\Pi^{y\succ x}(\mathcal{E}(\rho')))) > 0$.

Now, let $\rho$ and $\rho'$ be quantum ballot profiles such that $\text{Tr}((\Pi^{y\succ x}(\mathcal{E}(\rho)))) = \text{Tr}((\Pi^{y\succ x}(\mathcal{E}(\rho'))))$ and $\text{Tr}((\Pi^{x\succ z}(\mathcal{E}(\rho)))) = \text{Tr}((\Pi^{x\succ z}(\mathcal{E}(\rho'))))$ for each voter $v_i$. If $\text{Tr}((\Pi^{y\succ x}(\mathcal{E}(\rho)))) > 0$, then we know $y > x$ is not encoded by all $\rho_i$. Since $\text{Tr}((\Pi^{y\succ x}(\rho_i))) = \text{Tr}((\Pi^{y\succ x}(\rho'_i)))$ and $\text{Tr}((\Pi^{x\succ z}(\rho_i))) = \text{Tr}((\Pi^{x\succ z}(\rho'_i)))$ for each voter $v_i$, we know that $y > x$ is not encoded by all $\rho'_i$. Hence $\text{Tr}((\Pi^{y\succ x}(\mathcal{E}(\rho')))) > 0$. □

Theorem 6 The Quantum Condorcet Voting $\mathcal{E}_{qcv}$ does not satisfy sharp dictatorship.

Proof: We will construct a ballot profile in which no candidate is a dictator. Let $\{x, y, z\}$ be the set of candidates. Let $\rho = \rho_1 \otimes \rho_2 \otimes \rho_3$ be a quantum ballot profile where $\rho_1 = |x > y > z\rangle (x > y > z\rangle, \rho_2 = |y > z > x\rangle (y > z > x\rangle, \rho_3 = |z > x > y\rangle (z > x > y\rangle$. Then the weak order generated by $\mathcal{E}_{qcv}$ according to the Condorcet score is $x \equiv y \equiv z$. The completion of $x \equiv y \equiv z$ is $\{x > y > z, x > z > y, y > x > z, y > z > x, z > x > y, z > y > x\}$. Therefore the quantum state generated in step 4 of quantum Condorcet voting is $\sigma = \frac{1}{6}(|x > y > z\rangle (x > y > z\rangle + |x > z > y\rangle (x > z > y\rangle + |y > x > z\rangle (y > x > z\rangle + |y > z > x\rangle (y > z > x\rangle + |z > x > y\rangle (z > x > y\rangle + |z > y > x\rangle (z > y > x\rangle)$. Therefore, we have $\text{Tr}((\Pi^{x\succ y}(\rho_1)) = 1$ but $\text{Tr}((\Pi^{y\succ x}(\mathcal{E}_{qcv}(\rho))) < 1$, $\text{Tr}((\Pi^{x\succ z}(\rho_2)) = 1$ but $\text{Tr}((\Pi^{x\succ z}(\mathcal{E}_{qcv}(\rho))) < 1$, $\text{Tr}((\Pi^{y\succ z}(\rho_3)) = 1$ but $\text{Tr}((\Pi^{y\succ z}(\mathcal{E}_{qcv}(\rho))) < 1$. This violates sharp dictatorship. □

Theorem 7 The Quantum Condorcet Voting $\mathcal{E}_{qcv}$ does not satisfy unsharp dictatorship.

Proof: Consider again the profile constructed in the above proof. We have $\text{Tr}((\Pi^{x\succ y}(\mathcal{E}_{qcv}(\rho))) > 0$ but $\text{Tr}((\Pi^{y\succ z}(\mathcal{E}_{qcv}(\rho))) > 0$ but $\text{Tr}((\Pi^{y\succ z}(\mathcal{E}_{qcv}(\rho))) > 0$ but $\text{Tr}((\Pi^{y\succ z}(\mathcal{E}_{qcv}(\rho))) > 0$. This violates unsharp dictatorship. □

By combining theorems 2-7 we conclude that Quantum Condorcet Voting satisfies Quantum Unanimity and the QIIA but does not Quantum Dictatorship. In other words, we can infer the following corollary:

Corollary 1 Arrow’s impossibility theory is not valid in quantum voting.

4 Related work

Most of the related work on quantum voting focus on the security of voting. The first quantum voting protocol was proposed by Hillery et al. [8]. They proposed two voting modes, namely traveling ballot and distributed ballot to ensure the security of voting. The protocol designed by Vaccaro et al. [24] uses entangled states to ensure that the votes are anonymous and to allow the votes to be tallied. The entanglement is distributed over separated sites; the physical inaccessibility of any site is sufficient to guarantee the anonymity of the votes. Horoshko and Kilin [9] proposed a quantum anonymous voting scheme based on Bell-state. Their protocol protects both the voters from a curious tallyman and all the participants from a dishonest voter in an unconditionally secure way. Wang et al. [25] proposed a quantum anonymous voting protocol assisted by two kinds of entangled quantum states. They provided a mechanism of opening and permuting the ordered votes of all the voters in an anonymous manner; any party who is interested in the voting results can obtain the voting result through a simple calculation. Their protocol possesses the properties of privacy, self-tallying, nonreusability, verifiability, and fairness at the same time.
In our previous work [20] a simple voting protocol based on Quantum Blockchain was proposed. Despite its simplicity, our protocol satisfies the most important properties of secure voting protocols: is anonymous, binding, non-reusable, verifiable, eligible, fair and self-tallying. The protocol could also be implemented using presently available technology. One limitation of this protocol is that it works for only 2 candidates. In a recent paper [19] we overcame this limitation by realizing classical Condorcet voting on Quantum Blockchain.

5 Conclusion and future work

In this paper, we study Arrow’s Impossibility Theorem in the quantum setting. We first modify the definition of QIIA such that it precisely captures the idea of independence of irrelevant alternatives. Then we present a detailed proof of the violation of Arrow’s Impossibility Theorem with our modified definition.

In [19], we have demonstrated that Condorcet voting on Quantum Blockchain significantly simplifies the task of electronic voting and in the same time ensures many desired security properties. In the future, we will further improve Quantum Condorcet Voting such that it has advantages for both security and the quality of the democratic processes. We will also investigate the validity of other theorems of classical social choice theory in the quantum setting. Those theorems include Sen’s Theorem on the impossibility of a Paretian Liberal [18], the Muller-Satterthwaite Theorem on surjective monotonicity [13] and the Gibbard-Satterthwaite Theorem on strategic manipulation [7]. The third direction of research we are interested in is quantum logic for social choice. Modal logic has been used as a powerful tool to model and reason about social choice [23, 11, 6, 16]. It is both natural and valuable to develop a quantum logic to model and reason about quantum social choice.
Appendix: basics of quantum information

Some primitives of quantum information which are used in this paper are collected in this appendix. The readers who are interested in quantum information are recommended to textbooks such as Yanofsky and Mannucci [27], Scherer [17], Nielsen and Chuang [14] and Watrous [26].

Definition 8 (Hilbert space) A (finite-dimensional) Hilbert space \( H \) is a

1. complex vector space, that is, \( \phi, \psi \in H \) and \( a, b \in \mathbb{C} \Rightarrow a\phi + b\psi \in H \),

2. with a (positive-definite) scalar product \( \langle \cdot | \cdot \rangle : H \times H \mapsto \mathbb{C} \) such that for all \( \phi, \psi, \phi_1, \phi_2 \in H \) and \( a, b \in \mathbb{C} \)

   (a) \( \langle \phi | \psi \rangle = \overline{\langle \psi | \phi \rangle} \)

   (b) \( \langle \phi | \phi \rangle \geq 0 \)

   (c) \( \langle \phi | \psi \rangle = 0 \iff \phi = 0 \)

   (d) \( \langle \psi | a\phi_1 + b\phi_2 \rangle = a\langle \psi | \phi_1 \rangle + b\langle \psi | \phi_2 \rangle \)

In quantum computation and quantum information, we only consider finite-dimensional Hilbert spaces. A vector \( \phi \) of a Hilbert space is usually represented in the Dirac notion as \( | \phi \rangle \) in quantum computing. A Hilbert space \( H \) induces a norm \( \| \cdot \| \) defined by \( \| \phi \| = \sqrt{\langle \phi | \phi \rangle} \) for any \( \phi \in H \).

Definition 9 (orthonormal basis and dimension) An orthonormal basis \( \{ | \phi_i \rangle \} \) for a Hilbert space \( H \) is a basis of \( H \) whose vectors are unit vectors and are orthogonal to each other, that is, for any \( | \phi_i \rangle, | \phi_j \rangle \), \( \| \phi_i \| = 1 \) and \( \langle \phi_i | \phi_j \rangle = 0 \). The dimension of a Hilbert space is the number of vectors of an orthonormal basis.

Definition 10 (tensor product) Given Hilbert spaces \( V \) and \( W \) of dimension \( m \) and \( n \) respectively, their tensor product, denoted \( V \otimes W \), is a \( mn \)-dimensional space consisting of linear combinations of outer products \( | v \rangle \otimes | w \rangle \) of vectors \( | v \rangle = (v_1, v_2, \ldots, v_m)^T \in V \) and \( | w \rangle = (w_1, w_2, \ldots, w_n)^T \in W \), where

\[
| v \rangle \otimes | w \rangle = \begin{bmatrix} v_1 w_1 \\ v_1 w_2 \\ \vdots \\ v_m w_n \end{bmatrix}
\]

Definition 11 (subspace) A subspace of a Hilbert space \( V \) is a subset \( W \) of \( V \) such that \( W \) is also a Hilbert space.

Definition 12 (operator) A linear map \( A : H \mapsto H \) is called an operator on \( H \).

We use \( L(H) \) to denote the set of all operators on \( H \).

Definition 13 (adjoint) The operator \( A^* : H \mapsto H \) that satisfies \( \langle A^* \phi | \psi \rangle = \langle \phi | A \psi \rangle \) for all \( \phi, \psi \in H \) is called the adjoint operator to \( A \).

Definition 14 (projector) A projector of a Hilbert space \( H \) is a linear map \( P : H \mapsto H \) such that \( P^2 = P \) and \( P^* = P \).
Projectors are related to projective measurements in quantum mechanics. We use an operator $M$ to represent an observable of the quantum system being observed, with a decomposition $M = \sum_m P_m$, where $P_m$ is the projector onto the eigenspace of $M$ with eigenvalue $m$. The result of measuring the state $|\psi\rangle$ will be one of $M$’s eigenvalues, and the probability of getting result $m$ is $p(m) = \langle \psi | P_m | \psi \rangle$.

**Definition 15 (trace)** Let $\mathcal{H}$ be a Hilbert space and $\rho$ be an operator on $\mathcal{H}$. The trace of $\rho$ is defined by

$$
\text{Tr}(\rho) = \sum_i \langle i | \rho | i \rangle
$$

where $\{|i\rangle\}$ is an orthonormal basis of $\mathcal{H}$.

**Definition 16 (positive semidefinite operator)** An operator $A : \mathcal{H} \rightarrow \mathcal{H}$ is positive semidefinite if it holds that $A = B^* B$ for some operator $B \in \mathcal{L}(\mathcal{H})$.

**Definition 17 (density operator)** A positive semidefinite operator $\rho$ on $\mathcal{H}$ is a density operator if it holds that $\rho = \rho^*$ and $\text{Tr}(\rho) = 1$.

**Definition 18 (partial trace)** Suppose the composite system of two subsystems $A$ and $B$ is described by the density operator $\rho_{AB}$. The partial trace over $B$ is defined by

$$
\rho_A = \text{Tr}_B(\rho_{AB}) = \sum_i (I_A \otimes \langle i |) \rho_{AB} (I_A \otimes | i \rangle)
$$

where $\{|i\rangle\}$ is an orthonormal basis of the Hilbert space $\mathcal{H}_B$. $\rho_A$ is called the reduced density operator of the subsystem $A$. The partial trace over $A$ can be defined in a similar way.
References

[1] Thomas Ågotnes, Wiebe van der Hoek & Michael J. Wooldridge (2011): On the logic of preference and judgment aggregation. Auton. Agents Multi Agent Syst. 22(1), pp. 4–30, doi:10.1007/s10458-009-9115-8 Available at https://doi.org/10.1007/s10458-009-9115-8

[2] Kenneth J. Arrow (1951): Social Choice and Individual Values. John Wiley and Sons.

[3] Ning Bao & Nicole Yunger Halpern (2017): Quantum voting and violation of Arrow’s impossibility theorem. Phys. Rev. A 95, p. 062306, doi:10.1103/PhysRevA.95.062306 Available at https://link.aps.org/doi/10.1103/PhysRevA.95.062306

[4] Felix Brandt, Vincent Conitzer, Ulle Endriss, Jérôme Lang & Ariel D. Procaccia, editors (2016): Handbook of Computational Social Choice. Cambridge University Press.

[5] David Chaum, Claude Crépeau & Ivan Damgård (1988): Multiparty Unconditionally Secure Protocols (Extended Abstract). In Janos Simon, editor: Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA, ACM, pp. 11–19, doi:10.1145/62212.62214 Available at http://doi.acm.org/10.1145/62212.62214

[6] Giovanni Cínà & Ulle Endriss (2016): Proving classical theorems of social choice theory in modal logic. Auton. Agents Multi Agent Syst. 30(5), pp. 963–989, doi:10.1007/s10458-016-9328-6 Available at https://doi.org/10.1007/s10458-016-9328-6

[7] Allan Gibbard (1973): Manipulation of Voting Schemes: A General Result. Econometrica 41(4), pp. 587–601. Available at http://www.jstor.org/stable/1914083

[8] Mark Hillery, Mário Ziman, Vladimír Bužek & Martina Bieliková (2006): Towards quantum-based privacy and voting. Physics Letters A 349(1), pp. 75 – 81, doi:https://doi.org/10.1016/j.physleta.2005.09.010 Available at http://www.sciencedirect.com/science/article/pii/S0375960105014738

[9] Dmitri Horoshko & Sergei Kilin (2011): Quantum anonymous voting with anonymity check. Physics Letters A (375), pp. 1172–1175.

[10] Lang Jiang, Guangqiang He, Ding Nie, Jin Xiong & Guihua Zeng (2012): Quantum anonymous voting for continuous variables. Phys. Rev. A 85, p. 042309, doi:10.1103/PhysRevA.85.042309 Available at https://link.aps.org/doi/10.1103/PhysRevA.85.042309

[11] Yuan Li & Guihua Zeng (2008): Quantum anonymous voting systems based on entangled state. Optical Review 15(5), pp. 219–223, doi:10.1007/s10043-008-0034-8 Available at https://doi.org/10.1007/s10043-008-0034-8

[12] Yuan Li & Guihua Zeng (2012): Anonymous quantum network voting scheme. Optical Review 19(3), pp. 121–124, doi:10.1007/s10043-012-0021-y Available at https://doi.org/10.1007/s10043-012-0021-y

[13] Eitan Muller & Mark A Satterthwaite (1977): The equivalence of strong positive association and strategy-proofness. Journal of Economic Theory 14(2), pp. 412–418, doi:https://doi.org/10.1016/0022-0531(77)90140-5 Available at https://www.sciencedirect.com/science/article/pii/0022053177901405

[14] Michael A. Nielsen & Isaac L. Chuang (2010): Quantum Computation and Quantum Information. Cambridge University Press, doi:10.1017/CBO9780511976667

[15] Eric Pacuit (2019): Voting Methods. In Edward N. Zalta, editor: The Stanford Encyclopedia of Philosophy, fall 2019 edition, Metaphysics Research Lab, Stanford University.

[16] Erik Parmann & Thomas Ågotnes (2021): Reasoning about strategic voting in modal logic quickly becomes undecidable. Journal of Logic and Computation. https://doi.org/10.1093/logcom/exab001

[17] Wolfgang Scherer (2019): Mathematics of Quantum Computing: An Introduction. Springer.
[18] Amartya Sen (1970): *The Impossibility of a Paretian Liberal*. Journal of Political Economy 78(1), pp. 152–157. Available at http://www.jstor.org/stable/1829633

[19] Xin Sun, Piotr Kulicki, Mirek Sopek & Feifei He (2021): A Still Simple Multi-candidate Voting Protocol on Quantum Blockchain. Submitted to Quantum Information Processing.

[20] Xin Sun, Quanlong Wang, Piotr Kulicki & Mirek Sopek (2019): A Simple Voting Protocol on Quantum Blockchain. *International Journal of Theoretical Physics* 58(1), pp. 275–281, doi:10.1007/s10773-018-3929-6 Available at https://doi.org/10.1007/s10773-018-3929-6

[21] Kishore Thapliyal, Rishi Dutt Sharma & Anirban Pathak (2017): Protocols for quantum binary voting. *International Journal of Quantum Information* 15(01), p. 1750007, doi:10.1142/S0219749917500071 Available at https://www.worldscientific.com/doi/abs/10.1142/S0219749917500071

[22] Juan-Hong Tian, Jian-Zhong Zhang & Yan-Ping Li (2016): A Voting Protocol Based on the Controlled Quantum Operation Teleportation. *International Journal of Theoretical Physics* 55(5), pp. 2303–2310, doi:10.1007/s10773-015-2868-8 Available at https://doi.org/10.1007/s10773-015-2868-8

[23] Nicolas Troquard, Wiebe van der Hoek & Michael J. Wooldridge (2011): Reasoning About Social Choice Functions. *J. Philos. Log.* 40(4), pp. 473–498, doi:10.1007/s10992-011-9189-z Available at https://doi.org/10.1007/s10992-011-9189-z

[24] J. A. Vaccaro, Joseph Spring & Anthony Chefles (2007): Quantum protocols for anonymous voting and surveying. *Phys. Rev. A* 75, p. 012333, doi:10.1103/PhysRevA.75.012333 Available at https://link.aps.org/doi/10.1103/PhysRevA.75.012333

[25] Qingle Wang, Chaohua Yu, Fei Gao, Haoyu Qi & Qiaoyan Wen (2016): Self-tallying quantum anonymous voting. *Phys. Rev. A* 94, p. 022333, doi:10.1103/PhysRevA.94.022333 Available at https://link.aps.org/doi/10.1103/PhysRevA.94.022333

[26] John Watrous (2018): *The Theory of Quantum Information*. Cambridge University Press.

[27] Noson Yanofsky & Mirco Mannucci (2008): *Quantum Computing for Computer Scientists*. Cambridge University Press.

[28] William S. Zwicker (2006): *Handbook of Computational Social Choice*, chapter Introduction to the Theory of Voting, pp. 23–56. Cambridge University Press.