Article

The Connection between the PQ Penny Flip Game and the Dihedral Groups

Theodore Andronikos ^{1,*} and Alla Sirokofskich ^{2,†}¹ Department of Informatics, Ionian University, 7 Tsirigoti Square, 49100 Corfu, Greece² Department of History and Philosophy of Sciences, National and Kapodistrian University of Athens, 15771 Athens, Greece; asirokof@math.uoa.gr

* Correspondence: andronikos@ionio.gr

† These authors contributed equally to this work.

Abstract: This paper is inspired by the PQ penny flip game. It employs group-theoretic concepts to study the original game and its possible extensions. In this paper, it is shown that the PQ penny flip game can be associated, in a precise way, with the dihedral group D_8 and that within D_8 there exist precisely two classes of equivalent winning strategies for Q. This is achieved by proving that there are exactly two different sequences of states that can guarantee Q's win with probability 1.0. It is demonstrated that the game can be played in every dihedral group D_{8n} , where $n \geq 1$, without any significant change. A formal examination of what happens when Q can draw their moves from the entire $U(2)$, leads to the conclusion that, again, there are exactly two classes of winning strategies for Q, each class containing an infinite number of equivalent strategies, but all of them sending the coin through the same sequence of states as before. Finally, when general extensions of the game, with the quantum player having $U(2)$ at their disposal, are considered, a necessary and sufficient condition for Q to surely win against Picard is established: Q must make both the first and the last move in the game.

Citation: Andronikos, T.; Sirokofskich, A. The Connection between the PQ Penny Flip Game and the Dihedral Groups. *Mathematics* **2021**, *9*, 1115. <https://doi.org/10.3390/math9101115>

Academic Editor: David Barilla

Received: 27 April 2021

Accepted: 13 May 2021

Published: 14 May 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: quantum games; classical games; sequential quantum games; groups of actions; winning strategies

1. Introduction

It is rather unnecessary to stress the importance of game theory. It has been extensively used for decades now to help researchers and practitioners make sense of situations involving conflict, competition, and cooperation. The abstraction of players who antagonize each other in a specified framework by devising elaborate strategies has been employed in the fields of economics, political and social sciences, biology, and, naturally, computer science. Game theorists have developed an enormous technical machinery for the quantitative assessment of the players' strategies and their pay-offs. Of particular significance is the assumption that the players are rational, which means that they seek to maximize their pay-offs. In this paper, only very basic and easy to grasp notions from game theory are used. These can be found in all standard textbooks, such as [1–3]. The emergence of the quantum era in information and computation also brought about the creation of the field of quantum game theory. This recent field is devoted to the study of classical games in the quantum setting, giving an exciting new perspective and results that are beyond the grasp of the classical realm.

1.1. Related Work

The year 1999 was an important milestone for the creation of the field of quantum games. In that year, two influential works were published. In a seminal paper Meyer [4] introduced the PQ penny flip game, which can be considered the quantum analogue of the classical penny flip game. The other influential work from 1999 was by Eisert et al.

in [5]. There the authors presented a novel technique, known now as the Eisert–Wilkens–Lewenstein protocol, that has gained wide acceptance in the field.

In Meyer’s PQ penny flip game, the two players are the famous tv characters Picard and Q from the TV series Star Trek. They consecutively “toss” a quantum coin and if at the end of the game the coin is found heads up Q wins, otherwise Picard wins. There is a metaphor behind the two players: Picard represents the classical player and Q the quantum player. For Picard the game is perceived as the classical penny flip game, but for Q the quantumness of the coin is evident and can be exploited to their advantage. Meyer demonstrated that Q can always win with probability 1.0 by employing the Hadamard operator. Afterwards, many researchers generalized this game to n -dimensional quantum systems. Important results in this direction were obtained by [6–8]. These results indicated that under a specific set of rules, the quantum player does have an advantage over the classical player. Nonetheless, this need not always hold as the authors in [9] pointed out. There, it was shown that if the rules of the PQ penny flip game are appropriately modified, it is even possible that Picard may win the game. Another related problem, namely that of quantum gambling based on the Nash-equilibrium was examined in [10]. The association of every finite variant of the PQ penny flip game with finite automata, so that strategies are words accepted by the corresponding automaton, was established in [11]. In that work, the underlying assumption was that Q will always use the Hadamard operator. The present paper is also focused on the PQ penny flip game and its possible extensions, but this time without any limitations, as Q is free to choose their moves from the entire $U(2)$.

With respect to the Eisert–Wilkens–Lewenstein scheme, many important results have been obtained. Several quantum adaptations of the famous prisoners’ dilemma have been defined and studied, giving quantum strategies that are better than any classical strategy ([5]). Some recent results were presented in [12], where the correspondence of typical conditional strategies, used in the classical repeated prisoners’ dilemma game, to languages accepted by quantum automata was established, and in [13], where the Eisert–Wilkens–Lewenstein scheme was extended. Quantum games, especially coin tossing, have also been fruitfully utilized in many quantum cryptographic protocols. In such a setting, Alice and Bob assume the role of remote parties that, despite not trusting each other, have to agree on a random bit (see [14] and references therein). This has been extended in [15] to quantum dice rolling when multiple outcomes and parties are involved. In a different but quite similar line of thought, Parrondo games were studied via quantum lattice gas automata in [16] and in [17] it was shown that quantum automata accepting infinite words can capture winning strategies for abstract quantum games. Recently, abstract sequential quantum games were investigated in [18]. Games have been cast not only in a quantum setting, but also in a biological setting. Some well-known classical games, such as the prisoners’ dilemma, can be expressed via biological and bio-inspired concepts (see [19–21] for more references).

1.2. Contribution

This paper is inspired by previous research on the PQ penny flip game. Its novelty lies in the use of group-theoretic concepts to study the original game and its possible extensions. It is shown for the first time that the original PQ penny flip game can be associated in a precise way with the dihedral group D_8 . Interpreting the game in terms of stabilizers and fixed sets, which are basic and helpful group notions, facilitates the explanation and replication of Q’s strategy. Within D_8 there exist precisely two classes of winning strategies for Q. Each class contains many different strategies, but all these strategies are equivalent in the sense that they drive the coin through the same sequence of states. It is proven for the first time in the literature that there are precisely two different sequences of states that can guarantee Q’s win with probability 1.0. Subsequently, it is demonstrated that the same game can be played in the all dihedral groups D_{8n} , $n \geq 1$, without any significant change in the winning strategies of Q. Thus, the smallest group that captures the essence

of the game is D_8 . The most general setting, where Q can draw their moves from the entire $U(2)$, is examined next. The definitive answer is that, perhaps surprisingly, the situation remains the same. Again, there are exactly two classes of winning strategies for Q , each class containing now an infinite number of equivalent strategies, but all of them send the coin through the same sequence of states as before. Ultimately, the original PQ penny flip game can be succinctly summarized by saying that there are precisely two paths of states that lead to Q 's win and, of course, no path that leads to Picard's win. Finally, general extensions of the game in which Q has $U(2)$ at their disposal, are studied. Their examination uncovers a very important fact: for Q to surely win against the classical player the tremendous advantage of available quantum actions is not enough; he must also make both the first and last move, or else he is not certain to win.

1.3. Organization

The paper is structured as follows. Section 1 sets the stage and gives the most relevant references. Section 2 introduces the notation and terminology used in this article. Section 3 proves the connection of the game with the dihedral group D_8 and Section 4 analyzes Q 's strategy in terms of group concepts. Sections 5 and 6 analyze the characteristics and the possible extensions of the game in larger groups. A thorough discussion and evaluation of the results can be found in Section 7 and, finally, Section 8 provides a summary of the current work and sketches some ideas for future work.

2. Background

2.1. The PQ Penny Flip Game

In what is now regarded as a landmark paper [4], Meyer defined the penny flip game between the famous television personas Picard and Q from the TV series Star Trek. From now on, for brevity, the Picard– Q game is referred to as the PQG. This game is much more than a coin flipping game; its importance lies in the fact that it demonstrates the advantage of quantum strategies over classical strategies. The human player, Picard, can only employ classical strategies, while the quantum player, Q , is capable of using quantum strategies. This asymmetry is the reason why, no matter what Picard does, Q always wins with probability 1.0. Picard is confined to just the two classical moves available in a 2-dimensional system: he can either do nothing, or he can flip the coin. Doing nothing means that the coin remains in its current state, while flipping the coin changes its state from heads to tails or vice versa. Q 's advantage stems from the fact that he can potentially choose from an infinite pool of allowable moves; the only obvious restriction being that their move must be represented by a unitary operator. The game begins with the coin *heads up* and the two players act on the coin following a predetermined order. Q acts first, then Picard and last Q again. If, after Q 's last action, the coin is found *heads up*, then Q wins. If the coin is found *tails up*, then Picard wins.

In the context of the PQG and its extensions, it is convenient to employ the terminology outlined in Definition 1, adapted from [1,3]. Informally, the word strategy implies a rational plan on behalf of each player. This plan ultimately consists of actions, or moves that the player makes as the game evolves.

Definition 1 (Winning and dominant strategies).

- A strategy is a function that associates an admissible action to every round that the player makes a move. It is convenient to represent strategies as finite sequences of moves from the player's repertoire;
- A strategy σ_P for Picard is a winning strategy if for every strategy σ_Q of Q , Picard wins the game with probability 1.0;
- Symmetrically, a strategy σ_Q for Q is a winning strategy if for every strategy σ_P of Picard, Q wins the game with probability 1.0;

- A strategy for Picard or Q is dominated if there exists another strategy that has greater probability to win for every strategy of the other player. A strategy that dominates all other strategies is called dominant.

Of course, in the original PQG, Picard's strategy is just one move, e.g., (F) . Q's strategy on the other hand is a sequence of two moves: (H, H) . Moreover, a winning strategy for Q is also a dominant strategy. Meyer proved that the use of the Hadamard operator constitutes a winning strategy for Q. If Q uses the Hadamard operator, he will win with probability 1.0, irrespective of Picard's moves. In technical terms, the game takes place in the 2-dimensional complex Hilbert space $\mathcal{H}_2$. The computational basis of $\mathcal{H}_2$ is denoted by B and consists of the kets $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$:

$$B = \{|0\rangle, |1\rangle\}. \quad (1)$$

Typically, $|0\rangle$ and $|1\rangle$ capture the state of the coin being heads up or tails up, respectively. Picard's moves do nothing and flip the coin correspond to the identity I and the flip operator F , respectively. As already mentioned, Q's winning strategy is the Hadamard operator H . In $\mathcal{H}_2$ the players' moves are represented by the following 2×2 matrices:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad F = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \text{and} \quad H = \begin{bmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{bmatrix}. \quad (2)$$

F is, of course, one of the famous Pauli matrices, frequently denoted by σ_x or σ_1 . In this work the dynamics of the PQG and its extensions are studied through the actions available to the players.

Definition 2 (PQG moves and their composition). Let $M_P = \{I, F\}$ and $M_Q = \{H\}$ be the sets of permissible moves for Picard and Q, respectively, and let $M = M_P \cup M_Q = \{I, F, H\}$. The set of all finite compositions of moves from M , denoted by M^* , is called the operational space of the PQG.

Consider for instance the composition FH , that can arise in the PQG when Picard replies with F to Q's H . A simple matrix multiplication shows that

$$FH = \begin{bmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{bmatrix}. \quad (3)$$

The operational space M^* contains not only the above operator (3), but also every operator that results from a finite composition of the moves in M . Most of them are not realized in the actual PQG because its duration is just 3 rounds. Definition 2 can be generalized as follows:

Definition 3. Given any game V (e.g., an extension of the original PQG game), for which the set of moves is M_V , its operational space is M_V^* .

2.2. Dihedral Groups

The notation and definitions from group theory are based on standard textbooks such as [22,23]. The number of elements of the group G is called the *order* of G and is denoted by $|G|$. It is customary to employ the following notation regarding powers of an arbitrary element g of a group G .

- $g^0 = \mathbb{1}$,
- $g^n = \underbrace{g \circ g \circ \dots \circ g}_{n \text{ factors}}$, when $n > 0$, and

- $g^n = (g^{-1})^{|n|}$, when $n < 0$.

The symbol $\circ$ of the binary operation is omitted, particularly in view of the fact that in many occasions the group elements will be represented by 2×2 matrices and the operation $\circ$ will be matrix multiplication. Hence, instead of writing $f \circ g$, the juxtaposition of the two elements fg is used.

The groups that capture the symmetries of regular polygons are called dihedral groups. By *regular* polygon it is understood that all the sides of the polygon have the same length and all the interior angles are equal. Furthermore, it is assumed that the center of the regular polygon is located at the origin of the plane.

Definition 4 (Dihedral groups). *The group of symmetries of the regular n -gon, where $n \geq 3$, is called the dihedral group of order $2n$ and is denoted by D_n .*

Many authors denote the dihedral group of order $2n$ by D_{2n} to explicitly indicate its order. However, in this paper the notation D_n is preferred to emphasize the geometric intuition. From now on, when referring to the arbitrary dihedral group D_n , it will be assumed that $n \geq 3$. The group operation is composition of symmetries, i.e., composition of rotations and reflections. The $2n$ symmetries of a regular n -gon, where $n \geq 3$, can be categorized as follows.

- There are n rotational symmetries. These are the rotations about the center of the n -gon by $\frac{2\pi k}{n}$, with k taking the values $0, 1, \dots, n-1$. Figures 1 and 2 show the 7 and 8 rotational symmetries of the regular heptagon and octagon, respectively.
- There are also n reflection symmetries.
 - If n is odd these are the reflections in the lines defined by a vertex and the center of the regular n -gon. As an example, see Figure 3 depicting the reflection symmetries of the regular heptagon.
 - If n is even, these are $\frac{n}{2}$ reflections in the lines through opposite vertices and $\frac{n}{2}$ reflections in the lines passing through midpoints of opposite faces. An example that will play an important role in this study is given in Figure 4, showing the reflection symmetries of the regular octagon.

By fixing a vertex of the regular n -gon to lie on the x -axis (such a vertex 1 in Figures 3 and 4) and the center of the n -gon at the origin of the plane, the n reflection symmetries correspond to lines through the origin making an angle $\frac{\pi k}{n}$ with the positive x -axis, with k taking the values $0, 1, \dots, n-1$.

Figure 1. The rotational symmetries of the regular heptagon.

Figure 2. The rotational symmetries of the regular octagon.

Figure 3. The reflection symmetries of the regular heptagon.

Figure 4. The reflection symmetries of the regular octagon.

The general dihedral group contains the following $2n$ elements (for details the interested reader may consult [22,23] or [24])

$$D_n = \{1, r, r^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s\}, \quad (4)$$

where r is the rotation by $\frac{2\pi}{n}$ and s is *any* reflection. It is evident that each element of D_n can be *uniquely* written as $r^k s^l$ for some $k, 0 \leq k \leq n-1$, and l , where $l = 0$ or 1 . Elements $1, r, r^2, \dots, r^{n-1}$ are rotations, i.e., r^k is the rotation by $\frac{2\pi k}{n}$, and elements $s, rs, r^2s, \dots, r^{n-1}s$ are reflections.

In particular, the dihedral group D_8 contains the 16 elements

$$D_8 = \{1, r, r^2, \dots, r^7, s, rs, r^2s, \dots, r^7s\}, \quad (5)$$

where r is the rotation by $\frac{2\pi}{8}$ and s is *any* reflection. Referring to Figure 4, s can be taken to be the reflection in the line passing through the vertices 1 and 5, or the reflection in the line

passing through the midpoints A and A' , or the reflection in the line passing through the vertices 2 and 6, or any of the remaining reflections.

Definition 5 (Generators). Given a subset X of a group G , the smallest subgroup of G that contains X is denoted by $\langle X \rangle$. The elements of X are called generators for $\langle X \rangle$.

When X is finite, i.e., $X = \{x_1, \dots, x_n\}$, as will be the case in this work, it is customary to simply write $\langle x_1, \dots, x_n \rangle$.

A typical way to specify groups is via *presentations*. This amounts to using *generators* and *relations*, with the understanding that all group elements can be constructed as products of powers of the generators, and the relations are equations involving the generators and the group identity. The following presentation of D_n is especially convenient:

$$D_n = \langle s, t \mid s^2 = t^2 = (st)^n = \mathbb{1} \rangle. \quad (6)$$

This presentation demonstrates that D_n is generated by two reflections s and t . It appears in [22,25], where it is clarified that D_n can be generated by two reflections s, t in adjacent axes of symmetry passing through the origin and intersecting in an angle $\frac{\pi}{n}$. In this case, the product st is a rotation through an angle of $\pm \frac{2\pi}{n}$.

3. The Connection between PQG and D_8

3.1. Matrix Representations of Rotations and Reflections

A useful and quite common way to represent rotations and reflections in the plane is to use 2×2 matrices. Such matrices, which are often called *rotators* and *reflectors*, can be conveniently written in a form that is easy to recognize and manipulate (see [24,26,27] for more details). A rotator representing a counter-clockwise rotation through an angle φ about the origin is denoted by R_φ and, similarly, a reflector about a line through the origin that makes an angle φ with the positive x -axis is denoted by S_φ . R_φ and S_φ are given by the formulas shown below. Note that capital R and capital S are used to designate these 2×2 matrices, in order to avoid any confusion with the elements of the dihedral group that are denoted by small r and s .

$$R_\varphi = \begin{bmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{bmatrix} \quad (7)$$

$$S_\varphi = \begin{bmatrix} \cos 2\varphi & \sin 2\varphi \\ \sin 2\varphi & -\cos 2\varphi \end{bmatrix} \quad (8)$$

It is now quite straightforward to see that the F and H operators can be written as follows.

$$F = \begin{bmatrix} \cos 2\frac{2\pi}{8} & \sin 2\frac{2\pi}{8} \\ \sin 2\frac{2\pi}{8} & -\cos 2\frac{2\pi}{8} \end{bmatrix} \quad (9)$$

$$H = \begin{bmatrix} \cos 2\frac{\pi}{8} & \sin 2\frac{\pi}{8} \\ \sin 2\frac{\pi}{8} & -\cos 2\frac{\pi}{8} \end{bmatrix} \quad (10)$$

This form reveals that both are *reflectors*: F reflects about a line that makes an angle $\frac{\pi}{4}$ with the positive x -axis. To be exact, this is the line passing through the vertices 2 and 6 in Figure 4. Likewise, H reflects about a line that makes an angle $\frac{\pi}{8}$ with the positive x -axis, which is the line passing through the midpoints A and A' in Figure 4. Hence, their axes of symmetry intersect in an angle $\frac{\pi}{8}$, as shown in Figure 4. Moreover, their product FH , which is given in (3), is just the rotator $R_{\frac{2\pi}{8}}$, as can be verified by employing Formula (7).

Therefore, by invoking the presentation (6), associating s to F , and t to H , or vice versa, it becomes evident that F and H generate the dihedral group D_8 . This conclusion is stated as Theorem 1.

In an effort to enhance the readability of this paper, all the proofs have been relocated to the Appendix A.

Definition 6 (The ambient group). *Let V be a game with operational space M_V^* . If M_V^* is isomorphic to the group G , then G is called the ambient group of the game V .*

Theorem 1 (The ambient group of the PQG). *The ambient group of the PQG is D_8 .*

The above result tells us that Picard and Q's moves generate the group D_8 . This has important ramifications. As long as the two players are allowed to use only the aforementioned actions, no matter what specific game they play, the game will take place in the D_8 group. Every conceivable composition of moves by the players is just an element of D_8 . Therefore, although the rules of the game can change dramatically, e.g., the players' turn, the number of rounds, etc., the available moves will always be elements of D_8 .

Every element of the dihedral group D_n can be represented by 2×2 matrices of the form shown in (7) and (8) (see [23,28] or [29] for more details). One such representation is given below. In the literature it is usually referred to as the *standard* representation of D_n . In more technical terms, this is a faithful irreducible representation of dimension 2. To clear any potential misunderstanding, let us emphasize that in the standard representation s corresponds to the reflection in the line passing through the vertices 1 and 5, i.e., the x -axis of Figure 4.

$$r \mapsto R_{\frac{2\pi}{n}} = \begin{bmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{bmatrix} \quad (11)$$

$$s \mapsto S_0 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (12)$$

The above mapping of r and s uniquely determines the standard representation of the remaining reflections and rotations of D_n .

$$r^k \mapsto R_{\frac{2\pi k}{n}} = \begin{bmatrix} \cos \frac{2\pi k}{n} & -\sin \frac{2\pi k}{n} \\ \sin \frac{2\pi k}{n} & \cos \frac{2\pi k}{n} \end{bmatrix} \quad (13)$$

$$r^k s \mapsto S_{\frac{\pi k}{n}} = \begin{bmatrix} \cos \frac{2\pi k}{n} & \sin \frac{2\pi k}{n} \\ \sin \frac{2\pi k}{n} & -\cos \frac{2\pi k}{n} \end{bmatrix}, \quad (14)$$

where $0 \leq k \leq n-1$.

3.2. Orbits and Stabilizers

Definition 7 (Group action). *Let G be a group and let X be a non-empty set. A group action $\star$ of G on X is a function $\star : G \times X \rightarrow X$ that satisfies the following properties.*

(A₁) $1 \star x = x$ for every $x \in X$.

(A₂) $g_1 \star (g_2 \star x) = (g_1 g_2) \star x$, for all $g_1, g_2 \in G$ and all $x \in X$.

Under the standard representation of D_n , its action on a state of the quantum coin is computed by simply multiplying every matrix corresponding to an element of D_n with the ket describing the state of the coin. In what follows, in addition to speaking about an action, the expression that G acts on X will occasionally be employed. It is convenient to

just write gx instead of $g \star x$, since the action in this paper is that of operators on kets, i.e., of matrix-vector multiplication.

Definition 8 (Orbits and stabilizers). Suppose that a group G of linear operators, or their corresponding matrix representations, acts on a non-empty set of kets X . The next definitions, always taking into account that all kets of the form $e^{i\theta} |\psi\rangle$, with $\theta \in \mathbb{R}$, represent ket $|\psi\rangle$, will be useful.

1. Given $x \in X$, the G -orbit of x , denoted by $G \star x$, is the set $\{g \star x \in X : g \in G\}$.
2. Given $S \subset X$, the G -orbit of S , denoted by $G \star S$, is the union of the orbits $G \star x$, for each $x \in S$.
3. Given $x \in X$, the stabilizer of x , denoted by $G(x)$, is the set $\{g \in G : g \star x = x\}$.
4. Given $g \in G$, the fixed set of g , denoted by $\text{Fix}(g)$, is the set $\{x \in X : g \star x = x\}$.
5. Given $X \subset G$, the fixed set of X , denoted by $\text{Fix}(X)$, is the intersection of the fixed sets $\text{Fix}(g)$, for each $g \in X$.

In the next section these tools will be employed in the analysis of Q 's strategy to gain insight from a group theoretic perspective.

4. Analyzing Q 's Strategy in Terms of Groups

In this section, the PQG is interpreted using the aforementioned groups concepts. It is helpful to use the following abbreviations, which are very common in the literature.

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (15)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (16)$$

It is instructive to see the effect of the action of D_8 on the computational basis B . One easy way to do this is geometrically, by consulting Figures 2 and 4, to see where vertices 1 and 3 are sent when being acted upon by the elements of D_8 . Alternatively, one can arrive at the same result algebraically simply by multiplying the matrix representation of every member of D_8 with $|0\rangle$ and $|1\rangle$. The representations of the elements of D_8 can be readily found by setting $n = 8$ in the more general Formulas (13) and (14). In any event, for future reference the action of D_8 on the computational basis B is summarized in Proposition 1 (recall that $e^{i\theta} |\psi\rangle$, with $\theta \in \mathbb{R}$, and $|\psi\rangle$ represent the same state).

Proposition 1 (The action of D_8 on B).

1. $|0\rangle$ and $|1\rangle$ have the same orbit:

$$D_8 \star |0\rangle = D_8 \star |1\rangle = \{|0\rangle, |+\rangle, |1\rangle, |-\rangle\}. \quad (17)$$

2. The orbit of B is:

$$D_8 \star B = \{|0\rangle, |+\rangle, |1\rangle, |-\rangle\}. \quad (18)$$

Q 's first move aims to drive the coin into the state

$$H|0\rangle = |+\rangle. \quad (19)$$

Definition 8 is helpful in understanding the advantage of Q 's move in terms of group notions. In particular, there are certain elements of D_8 whose action on $|+\rangle$ has no effect whatsoever and which constitute the stabilizer of $|+\rangle$. These can be easily found either geometrically or algebraically, and are listed in Proposition 2.

Proposition 2 (The stabilizers of $|0\rangle, |+\rangle, |1\rangle$ and $|-\rangle$ in D_8).

- The stabilizers of $|0\rangle$ and $|1\rangle$ in D_8 are

$$D_8(|0\rangle) = \{I, R_\pi, S_0, S_{\frac{4\pi}{8}}\} \quad \text{and} \quad D_8(|1\rangle) = \{I, R_\pi, S_0, S_{\frac{4\pi}{8}}\}. \quad (20)$$

- The stabilizers of $|+\rangle$ and $|-\rangle$ are

$$D_8(|+\rangle) = \{I, R_\pi, F, S_{\frac{6\pi}{8}}\} \quad \text{and} \quad D_8(|-\rangle) = \{I, R_\pi, F, S_{\frac{6\pi}{8}}\}. \quad (21)$$

In a complementary manner, it can be surmised that Picard's set of moves fixes specific states in $\mathcal{H}_2$, as demonstrated in Proposition 3.

Proposition 3 (The fixed set of $\{I, F\}$ in D_8).

1. The fixed set of F in D_8 is the set

$$\text{Fix}(F) = \{|+\rangle, |-\rangle\}. \quad (22)$$

2. The fixed set of $M_P = \{I, F\}$ in D_8 is the set

$$\text{Fix}(\{I, F\}) = \{|+\rangle, |-\rangle\}. \quad (23)$$

Proposition 2 tells us that Picard's set of moves is a subset of $D_8(|+\rangle)$ and Proposition 3 completes the picture by revealing that ket $|+\rangle$ is among those that are fixed by Picard's moves. Thus, he is completely powerless to change the state $|+\rangle$ of the coin. From this perspective the progression of the PQG can be abstractly described as by the following "algorithm".

Picard symbolizes the classical player and as such it is quite appropriate to assume that their repertoire is the set $M_P = \{I, F\}$. This set is also a group, in particular the $\mathbb{Z}_2$ group of two elements (In the literature $\mathbb{Z}_2$ is more often denoted as $\{0, 1\}$ under addition modulo 2). In the rest of this paper it will be assumed that the classical player can only make use of these two actions. In the coming sections Algorithm 1 will be employed to discover winning strategies for Q in more general situations.

Algorithm 1: Q's Winning Strategy.

- 1 Q's first move sends the coin to an intermediate target state (in the actual game it happens to be $|+\rangle$) that satisfies the following property: *this state is fixed by Picard's moves or, equivalently, all of Picard's moves belong to the stabilizer of this state* (in the actual game $I, F \in D_8(|+\rangle)$).
 - 2 Picard acts on the coin, but no matter which move he makes, the quantum coin remains in the *same* state.
 - 3 Q's final move sends the coin to the desired state.
-

5. Enlarging the Operational Space of the Game

The operational space of the original PQG is indeed a group, and, in particular, the dihedral group D_8 , as established by Theorem 1. In this section, the ambient group of the PQG will be progressively enlarged and Q's winning strategies will be analyzed. The analysis is guided by the belief that the essence of the original PQG is the sharp distinction between the classical and the quantum player. From this perspective, the subsequent investigation relies on the following two assumptions.

1. Picard, who embodies the classical player, can flip the coin. If he is deprived of this ability, then the resulting game becomes trivial and meaningless. He should not be able to do more than that, as this would endow them with quantum capabilities. Formally, this is expressed by specifying:

$$M_P = \{I, F\}. \quad (24)$$

2. Q, who stands for the quantum player, must exhibit quantumness. Thus, at least one of their actions must lie outside the classical realm. In more technical terms, their repertoire M_Q must contain at least one operator from $U(2)$ other than I and F .

Under the above assumptions, the following properties are observed. These properties are quite general, as they are satisfied by every winning strategy of Q, no matter what the ambient group is. Therefore, they will be invoked when much larger dihedral groups and the unitary group $U(2)$ are considered.

Theorem 2 (Characteristic properties of winning strategies). *If (A_1, A_2) is a winning strategy for Q, then:*

$$A_2 I A_1 |0\rangle = A_2 F A_1 |0\rangle = |0\rangle, \quad \text{and} \quad (25)$$

$$A_1 |0\rangle \in \text{Fix}(\{F\}). \quad (26)$$

The notion of *equivalent strategies* greatly simplifies the classification of winning strategies. Two strategies are considered to be equivalent if, when acting on the same initial state of the coin, they produce the same sequence of states. In view of the extension of the original game that will be undertaken in Section , the next definition is general enough to deal with strategies for games with more than three number of rounds.

Definition 9 (Equivalent strategies). *Let $\sigma = (A_1, \dots, A_r)$ and $\sigma' = (A'_1, \dots, A'_r)$ be two strategies of the same player, and let $|q_0\rangle$ be the initial state of the coin. σ and σ' are equivalent with respect to $|q_0\rangle$, denoted by $\sigma \sim \sigma'$, if*

$$A_j \dots A_1 |q_0\rangle = A'_j \dots A'_1 |q_0\rangle, \text{ for every } j, 1 \leq j \leq r. \quad (27)$$

Q's strategies (H, H) and $(R_{\frac{2\pi}{8}}, R_{\frac{14\pi}{8}})$ are equivalent because they send the coin from state $|0\rangle$ first to $|+\rangle$ and then back to $|0\rangle$. It is obvious that $\sim$ is an equivalence relation that partitions the set of strategies into equivalence classes of strategies.

Definition 10 (Strategy classes).

1. *Given a strategy σ , $[\sigma]$ designates the equivalence class that contains σ . Any member of $[\sigma]$ is a representative of $[\sigma]$.*
2. *To every class $[\sigma]$ the state path $\tau_{[\sigma]}$ is associated as follows: if $(A_1, \dots, A_r)$ is any representative of $[\sigma]$, $\tau_{[\sigma]}$ is defined to be $(|q_0\rangle, |q_1\rangle, \dots, |q_r\rangle)$, where*

$$|q_j\rangle = A_j \dots A_1 |q_0\rangle, \text{ for every } j, 1 \leq j \leq r. \quad (28)$$

Clearly, the state path $\tau_{[\sigma]}$ is well-defined and unique for each class $[\sigma]$. The equivalence class $[(H, H)]$ contains 16 strategies, as will be explained in Example 1, and the corresponding state path is $(|0\rangle, |+\rangle, |0\rangle)$.

5.1. Inside D_8

Before delving into larger groups, the case where Q can chose their moves from the entire D_8 group is examined, i.e.,

$$M_Q = D_8. \quad (29)$$

The following Example 1 will be instructive.

Example 1. *In this example, Algorithm 1 facilitates the study all winning strategies of Q in the original PQG. Let (A_1, A_2) be Q's first and second move in a winning strategy. After Q's first*

move the quantum coin will in one of the states in the orbit $D_8 \star B$, where B is the computational basis. From (18) it follows that $D_8 \star B = \{|0\rangle, |+\rangle, |1\rangle, |-\rangle\}$.

- Let us first establish that if Q leaves the coin at state $|0\rangle$, or sends it to state $|1\rangle$, then he will not be able to win with probability 1.0. To see this more clearly, let us recall that, by Theorem 2, $A_2 I A_1 |0\rangle = A_2 F A_1 |0\rangle = |0\rangle$. If (A_1, A_2) leaves the coin at state $|0\rangle$, i.e., $A_1 |0\rangle = |0\rangle$, then $A_2 I |0\rangle = A_2 F |0\rangle = |0\rangle \Rightarrow A_2 |0\rangle = A_2 |1\rangle = |0\rangle$, which is impossible because A_2 represents an element of D_8 . The same reasoning shows that if Q 's first move sends the coin to state $|1\rangle$, then he will not be able to win with probability 1.0.
- In the original PQG, Q won by sending the coin to state $|+\rangle$. In D_8 , this can be achieved with 4 different ways: $H, R_{\frac{2\pi}{8}}, S_{\frac{5\pi}{8}}$, and $R_{\frac{10\pi}{8}}$. State $|+\rangle$ is fixed by I and F according to (23), which means that no matter what Picard plays, the coin will remain in this state. Finally, Q can send the coin back to the $|0\rangle$ state with 4 different ways: $H, R_{\frac{14\pi}{8}}, S_{\frac{5\pi}{8}}$, and $R_{\frac{6\pi}{8}}$. This means that Q has 16 different winning strategies, which, in view of Definition 9, are equivalent. Thus, they constitute one equivalence class of winning strategies. Strategy (H, H) is a representative of this class, but any other strategy would also do. For this class the corresponding state path is $(|0\rangle, |+\rangle, |0\rangle)$.
- Algorithm 1 enables us to discover one more winning strategy for Q . Q has another option, which is to drive the coin to state $|-\rangle$. This can also be achieved with 4 different ways: $S_{\frac{7\pi}{8}}, R_{\frac{14\pi}{8}}, S_{\frac{3\pi}{8}}$, or $R_{\frac{6\pi}{8}}$. Picard cannot change this state either because $|-\rangle$ is fixed by I and F , according to (23). During the final round Q has the opportunity to send the coin back to the $|0\rangle$ state with 4 different ways: $S_{\frac{7\pi}{8}}, R_{\frac{2\pi}{8}}, S_{\frac{3\pi}{8}}$, or $R_{\frac{10\pi}{8}}$. Hence, Q has 16 more winning strategies, which are equivalent. They make the second equivalence class of winning strategies and any one of them, e.g., $(S_{\frac{7\pi}{8}}, S_{\frac{7\pi}{8}})$ can be its representative. For this class, the corresponding state path is $(|0\rangle, |-\rangle, |0\rangle)$.
- Picard, unfortunately for him, has no winning strategy.

According to Definition 1, for Q a winning strategy is also a dominant strategy. Hence, Q has precisely two classes of winning and dominant strategies, each containing 16 individual strategies. These two classes correspond to exactly the 2 path states $(|0\rangle, |+\rangle, |0\rangle)$, and $(|0\rangle, |-\rangle, |0\rangle)$. $\triangleleft$

Table 1 and Figure 5 summarize these results.

Table 1. The two classes of winning and dominant strategies for Q in the original PQG.

The Evolution of the PQG				
	Initial State	Round 1	Round 2	Round 3
$(H, H), (R_{\frac{2\pi}{8}}, R_{\frac{14\pi}{8}}), (S_{\frac{5\pi}{8}}, S_{\frac{5\pi}{8}}), \dots$	$ 0\rangle$	$ +\rangle$	$ +\rangle$	$ 0\rangle$
$(S_{\frac{7\pi}{8}}, S_{\frac{7\pi}{8}}), (R_{\frac{14\pi}{8}}, R_{\frac{2\pi}{8}}), (S_{\frac{3\pi}{8}}, S_{\frac{3\pi}{8}}), \dots$	$ 0\rangle$	$ -\rangle$	$ -\rangle$	$ 0\rangle$

Figure 5. This figure depicts two different winning strategies for Q that represent the two winning strategy classes, as well as the corresponding path states.

Theorem 3 (The ambient group of the PQG is D_8). If $M_P = \{I, F\}$ and $M_Q = D_8$, i.e., the ambient group of the PQG is D_8 , then the following hold.

1. Q has exactly two classes of winning and dominant strategies, each containing 16 equivalent strategies:

$$C_+ = [(A_1, A_2)] \quad \text{and} \quad C_- = [(B_1, B_2)], \quad (30)$$

where

- A_1 is one of $H, R_{\frac{2\pi}{8}}, S_{\frac{5\pi}{8}}$ or $R_{\frac{10\pi}{8}}$,
- A_2 is one of $H, R_{\frac{14\pi}{8}}, S_{\frac{5\pi}{8}}$ or $R_{\frac{6\pi}{8}}$,
- B_1 is one of $S_{\frac{7\pi}{8}}, R_{\frac{14\pi}{8}}, S_{\frac{3\pi}{8}}$ or $R_{\frac{6\pi}{8}}$, and
- B_2 is one of $S_{\frac{7\pi}{8}}, R_{\frac{2\pi}{8}}, S_{\frac{3\pi}{8}}$ or $R_{\frac{10\pi}{8}}$.

2. The winning state paths corresponding to C_+ and C_- are

$$\tau_{C_+} = (|0\rangle, |+\rangle, |0\rangle) \quad \text{and} \quad \tau_{C_-} = (|0\rangle, |-\rangle, |0\rangle). \quad (31)$$

3. Picard has no winning strategy.

5.2. The Smaller Dihedral Groups D_3, D_4, D_5, D_6 and D_7

It is natural to ask whether any of the smaller dihedral groups D_3, D_4, D_5, D_6 , and D_7 can be an appropriate operational space for the PQG. The answer is no for the reasons outlined below.

- D_3, D_5, D_6 , and D_7 do not contain the reflection F . This can be verified by comparing Formula (9) with formula (14) for $n = 3, 5, 6$, and 7 and $k = 1, \dots, n-1$. This is based on the assumption that Picard, the classical player, must be able to flip the coin, as emphasized in (24).
- D_4 does contain the reflection F . However, the orbit $D_4 \star B$ is $\{|0\rangle, |1\rangle\}$. This means that Q can only flip the coin from heads to tails or vice versa. If $M_Q = D_4$, then the PQG degenerates to the classical coin tossing game. Q is no longer a quantum entity and, as explained in Example 1, no longer possesses a winning strategy. From this perspective, it becomes meaningless to play the PQG in D_4 .

These conclusions are contained in Table 2 for easy reference.

Table 2. In smaller dihedral groups, it is either impossible to play the PQG, or, in the event that it is possible (such as in D_4), Q lacks a winning strategy. The abbreviation WS stands for winning strategy.

Ambient Group	Is PQG Playable	WS for Picard	WS for Q
D_3	No ($F \notin M_P$)	—	—
D_4	Yes (classical coin tossing)	No	No
D_5	No ($F \notin M_P$)	—	—
D_6	No ($F \notin M_P$)	—	—
D_7	No ($F \notin M_P$)	—	—

Thus, assuming that the classical player should be able to flip the coin in order to have a non-trivial game, and that the quantum player must exhibit quantumness, then the smallest dihedral group for the PQG is D_8 . This is stated as Theorem 4.

Theorem 4 (The smallest dihedral group for the PQG is D_8). D_8 is the smallest dihedral group in which PQG can be meaningfully played and Q has a quantum winning strategy.

5.3. The Dihedral Groups D_{8n} , $n \geq 1$

The previous subsection demonstrated that the smallest meaningful group for the PQG is D_8 . This subsection examines what happens if Q can choose from a larger repertoire, and, more specifically, if

$$M_Q = D_n, n \geq 8. \quad (32)$$

A helpful observation is that when n is odd, then D_n does not contain F , which is proved as Proposition A4 in the Appendix A. Thus, these groups can be excluded when considering larger groups where the PQG can be successfully played. Another useful result about the orbit of B in general dihedral groups is contained in Theorem 5.

Theorem 5 (The action of D_n on B). *The action of the general dihedral group D_n , $n \geq 3$, on the computational basis B depends on whether n is a multiple of 4 or even but not a multiple of 4.*

1. if n is a multiple of 4, then the action of D_n on the computational basis B is

$$D_n \star |0\rangle = D_n \star |1\rangle = D_n \star B = \left\{ \cos \frac{2\pi k}{n} |0\rangle + \sin \frac{2\pi k}{n} |1\rangle : 0 \leq k < \frac{n}{2} \right\}, \quad (33)$$

2. if n is even but not a multiple of 4, then the action of D_n on the computational basis B is

$$D_n \star |0\rangle = \left\{ \cos \frac{2\pi k}{n} |0\rangle + \sin \frac{2\pi k}{n} |1\rangle : 0 \leq k < \frac{n}{2} \right\}, \quad (34)$$

$$D_n \star |1\rangle = \left\{ -\sin \frac{2\pi k}{n} |0\rangle + \cos \frac{2\pi k}{n} |1\rangle : 0 \leq k < \frac{n}{2} \right\}, \quad (35)$$

$$D_n \star B = \left\{ \cos \frac{2\pi k}{n} |0\rangle + \sin \frac{2\pi k}{n} |1\rangle : 0 \leq k < \frac{n}{2} \right\} \cup \left\{ -\sin \frac{2\pi k}{n} |0\rangle + \cos \frac{2\pi k}{n} |1\rangle : 0 \leq k < \frac{n}{2} \right\}. \quad (36)$$

Figures 6–8 provide intuitive visualizations of Theorem 5.

Figure 6. Kets $|0\rangle$ and $|1\rangle$ have the same orbit in case n is a 4-multiple. The antipodal points that arise represent the same state.

Figure 7. Kets $|0\rangle$ and $|1\rangle$ have different orbits in case n is even, but not a 4-multiple.

Figure 8. Kets $|0\rangle$ and $|1\rangle$ have different orbits in case in case n is odd. No antipodal points arise in this case.

In this setting, Algorithm 1 can be used to establish under what conditions Q still possesses winning strategies and, if so, which these are. This is facilitated by the next Theorem 6, which explains what happens to the fixed set of $\{I, F\}$ in D_n .

Theorem 6 (The fixed set of $\{I, F\}$ in D_n). *When the general dihedral group D_n , $n \geq 3$, acts on the computational basis B , the fixed set of $M_P = \{I, F\}$ depends on whether n is a multiple of 8 or not.*

1. If n is a multiple of 8, then:

$$\text{Fix}(\{I, F\}) = \text{Fix}(F) = \{|+\rangle, |-\rangle\}. \quad (37)$$

2. In every other case:

$$\text{Fix}(\{I, F\}) = \text{Fix}(F) = \emptyset. \quad (38)$$

The significance of Theorem 6 is twofold. First, from a negative perspective, disqualifies most of the dihedral groups as potential ambient groups for the PQG. Simultaneously, in a positive note, it ascertains that the PQG can be meaningfully played in every dihedral group D_n such that n is a multiple of 8. Theorem 7 explains what exactly happens in terms of winning strategies when the PQG is played in these groups.

Theorem 7 (The ambient group of the PQG is D_{8n}). *If $M_P = \{I, F\}$ and $M_Q = D_{8n}$, i.e., the ambient group of the PQG is D_{8n} , where $n \geq 1$, then the following hold.*

1. Q has exactly two classes of winning and dominant strategies, each containing 16 equivalent strategies:

$$\mathcal{C}_+ = [(A_1, A_2)] \quad \text{and} \quad \mathcal{C}_- = [(B_1, B_2)], \quad (39)$$

where

- A_1 is one of $H, R_{\frac{2\pi}{8}}, S_{\frac{5\pi}{8}}$ or $R_{\frac{10\pi}{8}}$,
- A_2 is one of $H, R_{\frac{14\pi}{8}}, S_{\frac{5\pi}{8}}$ or $R_{\frac{6\pi}{8}}$,
- B_1 is one of $S_{\frac{7\pi}{8}}, R_{\frac{14\pi}{8}}, S_{\frac{3\pi}{8}}$ or $R_{\frac{6\pi}{8}}$, and
- B_2 is one of $S_{\frac{7\pi}{8}}, R_{\frac{2\pi}{8}}, S_{\frac{3\pi}{8}}$ or $R_{\frac{10\pi}{8}}$.

2. The winning state paths corresponding to $\mathcal{C}_+$ and $\mathcal{C}_-$ are

$$\tau_{\mathcal{C}_+} = (|0\rangle, |+\rangle, |0\rangle) \quad \text{and} \quad \tau_{\mathcal{C}_-} = (|0\rangle, |-\rangle, |0\rangle). \quad (40)$$

3. Picard has no winning strategy.

This leads to a very important conclusion: nothing substantial will change if the game takes place in much larger groups than D_8 ; the winning strategies remain precisely the same. This realization begs the question whether things will turn out to be different when

Q has at their disposal the largest group possible, $U(2)$, which is examined in the next subsection.

5.4. The Entire $U(2)$

This section examines the situation when Q is free to choose from all of $U(2)$, which is the largest possible group that Q can draw their moves from. Therefore, the final assumption regarding Q's set of actions is that

$$M_Q = U(2) . \quad (41)$$

The major difference compared to the previous cases is that $U(2)$ contains infinitely many elements, whereas the previous groups were finite. Although, superficially, this might be expected to drastically enhance Q's capabilities, it turns out that in a certain sense everything remains the same. This can be attributed to the following very simple fact. Kets $|\psi\rangle$ and $e^{i\theta}|\psi\rangle$, where $\theta \in \mathbb{R}$, physically represent the same state. In turn, this implies that the action of the operator $A \in U(2)$ on a ket $|\psi\rangle$ is the same as the action of $e^{i\theta}A \in U(2)$ on $|\psi\rangle$ (see [30] for details). If $e^{i\theta}A$ is viewed as denoting a parametric family of operators, it is clear that all these operators can be considered equivalent and any of them, e.g., A , can be taken as the representative of the corresponding equivalence class. In order to simplify the notation, the following Definition 11 is useful.

Definition 11 (Families of unitary operators).

If $A \in U(2)$, then

$$A(\theta) = e^{i\theta}A , \theta \in \mathbb{R} . \quad (42)$$

denotes a one-parameter family of unitary operators.

Similarly, if R_φ and S_φ are rotators and reflectors, as given by (7) and (8), respectively, the following one-parameter families of operators are defined:

$$R_\varphi(\theta) = e^{i\theta}R_\varphi \quad (43)$$

$$S_\varphi(\theta) = e^{i\theta}S_\varphi , \quad (44)$$

where $\theta \in \mathbb{R}$. Analogously, if H is the Hadamard transform and $R_{\frac{2\pi k}{n}}$ and $S_{\frac{\pi k}{n}}$ are the matrix representations given by (13) and (14), the corresponding collections of operators are:

$$H(\theta) = e^{i\theta}H , \quad (45)$$

$$R_{\frac{2\pi k}{n}}(\theta) = e^{i\theta}R_{\frac{2\pi k}{n}} , \quad (46)$$

$$S_{\frac{\pi k}{n}}(\theta) = e^{i\theta}S_{\frac{\pi k}{n}} . \quad (47)$$

Again it is fruitful to turn to Algorithm 1 to establish under what conditions Q possesses winning strategies and which are these. This approach is guided by the next Theorem 8, which establishes the fixed set of $\{I, F\}$ in $U(2)$.

Theorem 8 (The fixed set of $\{I, F\}$ in $U(2)$). Under the action of $U(2)$ on the computational basis B , the fixed set of $M_P = \{I, F\}$ is

$$\text{Fix}(\{I, F\}) = \text{Fix}(F) = \{|+\rangle, |-\rangle\} . \quad (48)$$

This result is crucial in discovering and enumerating the winning strategies of Q in $U(2)$. Although, one might have hoped for more variety in discovering winning strategies, the result is not unexpected because the flip operator F cannot fix more than two states. The next Theorem 9 explains what exactly happens in terms of winning strategies when the PQG takes place in $U(2)$.

Theorem 9 (The ambient group of the PQG is $U(2)$). If $M_P = \{I, F\}$ and $M_Q = U(2)$, i.e., the ambient group of the PQG is $U(2)$, then the following hold.

1. Q has exactly two classes of winning and dominant strategies, each containing infinite equivalent strategies:

$$C_+ = [(A_1(\theta_1), A_2(\theta_2))] \quad \text{and} \quad C_- = [(B_1(\theta_3), B_2(\theta_4))], \quad (49)$$

where

- $A_1(\theta_1)$ is one of $H(\theta_1), R_{\frac{2\pi}{8}}(\theta_1), S_{\frac{5\pi}{8}}(\theta_1)$ or $R_{\frac{10\pi}{8}}(\theta_1)$,
 - $A_2(\theta_2)$ is one of $H(\theta_2), R_{\frac{14\pi}{8}}(\theta_2), S_{\frac{5\pi}{8}}(\theta_2)$ or $R_{\frac{6\pi}{8}}(\theta_2)$,
 - $B_1(\theta_3)$ is one of $S_{\frac{7\pi}{8}}(\theta_3), R_{\frac{14\pi}{8}}(\theta_3), S_{\frac{3\pi}{8}}(\theta_3)$ or $R_{\frac{6\pi}{8}}(\theta_3)$,
 - $B_2(\theta_4)$ is one of $S_{\frac{7\pi}{8}}(\theta_4), R_{\frac{2\pi}{8}}(\theta_4), S_{\frac{3\pi}{8}}(\theta_4)$ or $R_{\frac{10\pi}{8}}(\theta_4)$, and
 - $\theta_1, \theta_2, \theta_3, \theta_4$ are possibly different real parameters.
2. The winning state paths corresponding to C_+ and C_- are

$$\tau_{C_+} = (|0\rangle, |+\rangle, |0\rangle) \quad \text{and} \quad \tau_{C_-} = (|0\rangle, |-\rangle, |0\rangle). \quad (50)$$

3. Picard has no winning strategy.

This final conclusion is illuminating. Although there are infinitely many winning strategies, they are equivalent to the strategies found in D_8 . In this perspective nothing is really gained by enabling Q to pick moves from $U(2)$. In a certain sense the spirit of the game is completely captured when it is realized in D_8 . The next Table 3 contains the complete results about Q 's classes of winning strategies whether the ambient group belongs to the family of dihedral groups D_{8n} or is the entire $U(2)$.

Table 3. The two classes of winning strategies for Q when the PQG is played in a dihedral group $D_{8n}, n \geq 1$ and when the game is played in the largest possible group $U(2)$.

The Ambient Group is $D_{8n}, n \geq 1$				
	Initial State	Round 1	Round 2	Round 3
$(H, H), (R_{\frac{2\pi}{8}}, R_{\frac{14\pi}{8}}), (S_{\frac{5\pi}{8}}, S_{\frac{5\pi}{8}}), \dots$	$ 0\rangle$	$ +\rangle$	$ +\rangle$	$ 0\rangle$
$(S_{\frac{7\pi}{8}}, S_{\frac{7\pi}{8}}), (R_{\frac{14\pi}{8}}, R_{\frac{2\pi}{8}}), (S_{\frac{3\pi}{8}}, S_{\frac{3\pi}{8}}), \dots$	$ 0\rangle$	$ -\rangle$	$ -\rangle$	$ 0\rangle$
The Ambient Group is $U(2)$ ($\theta \in \mathbb{R}$)				
	Initial State	Round 1	Round 2	Round 3
$(H(\theta_1), H(\theta_2)), (R_{\frac{2\pi}{8}}(\theta_1), R_{\frac{14\pi}{8}}(\theta_2)), \dots$	$ 0\rangle$	$ +\rangle$	$ +\rangle$	$ 0\rangle$
$(S_{\frac{7\pi}{8}}(\theta_3), S_{\frac{7\pi}{8}}(\theta_4)), (R_{\frac{14\pi}{8}}(\theta_3), R_{\frac{2\pi}{8}}(\theta_4)), \dots$	$ 0\rangle$	$ -\rangle$	$ -\rangle$	$ 0\rangle$

In $U(2)$ the strategy classes contain infinite many strategies, but all these strategies are equivalent to the strategies encountered before.

6. Extending the Game

The original PQG can be extended in numerous ways. In each conceivable extension, the precise formulation of the rules of the game is of paramount importance. By drastically changing the rules it is even possible for Picard to win the game. This was accomplished in [9] where the authors exploited entanglement in a clever way, so that whether the system ends up in a maximally entangled or separable state determines the outcome. In [11], it was

shown that all possible finite extensions of the PQG can be expressed in terms of simple finite automata, provided that the allowable moves of Picard are either I or F and Q always uses the Hadamard transform H . The focus of the present investigation is enlarging the operational space of the game. Therefore, when considering extensions of the original PQG, not only the assumptions (24) and (41), i.e., $M_P = \{I, F\}$ and $M_Q = U(2)$ are valid, but, additionally, it is supposed that:

- at the start of the game the coin is in a predefined basis state, which is called the *initial* state and designate by $|q_0\rangle$,
- Picard and Q alternate turns acting on the coin following a specified order, and
- when the game ends, the coin is measured in the computational basis; if it is found in state $|q_P\rangle$ Picard wins, whereas if it is found in $|q_Q\rangle$ then Q wins.

It is convenient to refer to $|q_P\rangle$ as Picard's *target* state and to $|q_Q\rangle$ as Q 's *target* state. In a zero-sum game the target states $|q_P\rangle$ and $|q_Q\rangle$ are different. Furthermore, since both Picard and Q draw their moves from groups, nothing is lost in terms of generality if neither of them is allowed to make consecutive moves. Two or more successive moves by Q can be composed to give just one equivalent move, and the same holds for Picard.

Definition 12 (Extended games between Picard & Q). *An n -round game, $n \geq 2$, is a function that associates one of the players, i.e., Picard or Q , to every round of the game. An n -round game is conveniently represented as a sequence of length n from the alphabet $\{P, Q\}$, where the letters P and Q stand for Picard and Q , respectively. In accordance with the previous remarks it is assumed that if $(K_1, K_2, \dots, K_n)$ is an n -round game, then $K_i \neq K_{i+1}$, $1 \leq i < n$.*

Definition 1 is general enough to also hold for extended games. The next important Theorem 10 confirms that Picard cannot win any such game with probability 1.0. This negative result implies that for these extended games, Picard is at a permanent disadvantage.

Theorem 10 (Picard lacks a winning strategy). *Picard does not have a winning strategy in any n -round game, $n \geq 2$, as long as Q makes at least one move.*

The next couple of theorems explain in which games Q is unable to formulate a winning strategy. First, rather predictably, if Picard is given the opportunity to act last on the coin, then Q cannot surely win.

Theorem 11 (Q lacks a winning strategy when Picard plays last). *Q does not have a winning strategy in any n -round game, $n \geq 2$, in which Picard makes the last move.*

Symmetrically, it is also true that Q is unable to devise a winning strategy when Picard plays first, as the next Theorem 12 asserts.

Theorem 12 (Q lacks a winning strategy when Picard plays first). *Q does not have a winning strategy in any n -round game, $n \geq 2$, in which Picard makes the first move.*

Theorems 11 and 12 establish that Q cannot surely win in any game where Picard makes the first or the last move. Figures 9 and 10 provide a visual explanation of the validity of these two theorems.

The picture is completed by the next Theorem 13 which asserts that Q has a winning strategy if and only if Q makes the first and the last move. This result clarifies that the overwhelmingly larger repertoire of moves of the quantum player by itself is not enough. It has to be combined with the advantage of making both the first and the last move in order to guarantee that the quantum player will surely win. Figure 11 presents two typical situations where Q can surely win. In the first n -round game Q makes the first and the last move and the initial state of the coin and the target state for Q are both the same. In the

second n -round game Q makes the first and the last move, but the initial state of the coin is $|1\rangle$, whereas the target state for Q is $|0\rangle$.

Theorem 13 (When Q possesses a winning strategy). *In any n -round game, $n \geq 2$, Q has a winning strategy iff Q makes the first and the last move.*

Figure 9. To understand why Q cannot have a winning strategy if Picard plays last, it suffices to consider two of Picard's strategies: $\sigma_P = (I, \dots, I, I)$ and $\sigma'_P = (I, \dots, I, F)$. It is impossible for any single strategy $\sigma_Q = (A_1, \dots, A_{n/2})$ of Q to win with probability 1.0 against both of them. The "?" indicates that the outcome of the measurement is not known a priori with probability 1.0.

Figure 10. To see why Q does not have a winning strategy if Picard plays first, it suffices to consider two of Picard's strategies: $\sigma_P = (I, \dots, I, I)$ and $\sigma'_P = (F, \dots, I, I)$. It is impossible for any single strategy $\sigma_Q = (A_1, \dots, A_{n/2})$ of Q to win with probability 1.0 against both of them. The "?" indicates that the outcome of the measurement is not known a priori with probability 1.0.

Figure 11. This figure depicts two winning strategies for Q ; two n -round games where Q makes the first and the last move. In the first game the initial state of the coin and the target state for Q are both the same, i.e., $|1\rangle$. In the second game the initial state of the coin is also $|1\rangle$, but the target state for Q now is $|0\rangle$.

One last conclusion that may be drawn from the above theorems is about the initial state of the coin and the target states of the players. In the original PQG , both the initial state and Q 's target state were the same, namely $|0\rangle$. Clearly, the particular choice of the initial state and the target states is of no importance. If there exists a winning strategy for Q with respect to specific initial and target states, then there exists a winning strategy for every combination of initial and target states.

Corollary 1 (The impact of initial and target states). *In any n -round game, $n \geq 2$, if Q has a winning strategy, he has a winning strategy for any combination of initial and target states.*

7. Discussion

The important philosophical question behind the original *PQG* game is whether and under what precise conditions the quantum paradigm exhibits a definitive advantage against the classical paradigm. From this perspective, this section analyzes the results obtained here.

Theorem 1 sets the group theoretic background of the *PQG* by showing that Picard and Q's moves generate the group D_8 . The significance of groups is paramount because it implies that no matter what strategies are used the game will take place in the group. Even if the rules of the game change, the available actions will be elements of the group.

Theorem 3 builds on this result by enumerating and classifying the winning strategies of Q in D_8 . The notion of equivalent strategies simplifies this classification by identifying two strategies as equivalent if their action on the coin produces the same sequence of states. Hence, the winning strategies can be grouped into equivalent classes that are distinguished by their corresponding state path. Theorem 3 proves that Q has two classes of winning strategies, each containing 16 equivalent strategies, and the corresponding state paths are $(|0\rangle, |+\rangle, |0\rangle)$, and $(|0\rangle, |-\rangle, |0\rangle)$. In effect, these are the only paths that Q can take to surely win the game and each of them can be realized by 16 different ways.

Furthermore, assuming that Picard should, at the very least, be able to flip the coin and that Q must exhibit quantumness, then Theorem 4 establishes the smallest group in which the *PQG* can be meaningfully played is D_8 . When considering larger dihedral groups, Theorem 6 furnishes important information. From a prohibitive aspect, it disqualifies most of the dihedral groups as eligible groups for the *PQG*. In a more positive note, it ensures that the *PQG* can be played in every dihedral group D_{8n} . Theorem 7 analyzes this situation and concludes that the winning strategies remain precisely the same, despite the much larger repertoire of moves from which Q can choose their actions.

Theorem 9 completes the picture by examining $U(2)$, the largest group possible. $U(2)$ contains infinitely many elements, whereas the dihedral groups were finite. Superficially, this would seem to drastically enhance Q's capabilities. Nonetheless, everything remains practically the same. Although in $U(2)$ there are infinitely many winning strategies, they are all equivalent to the strategies found in D_8 . It seems that the essence of the *PQG* is captured by D_8 .

The original *PQG* can be extended in a plethora of ways. In each extension, the precise formulation of the rules of the game is crucial. In the study of finite extensions of the original game Theorem 13 provides an important clarification. It asserts that the overwhelmingly larger repertoire of moves of Q is not enough by itself, but it has to be combined with the advantage of making both the first and the last move in order to guarantee that Q will surely win. One last minor conclusion drawn from 1 is that whenever Q has a winning strategy for specific initial and target states, he has a winning strategy for every combination of initial and target states.

8. Conclusions

Quantum games not only pose many interesting questions, but also motivate research that can have important applications in other related fields such quantum algorithms and quantum key distribution. This work was inspired by the iconic PQ penny flip game that, undoubtedly, helped create the field. The approach advocated here is based on the use of concepts from group theory. This allowed us to uncover the interesting connection of the original game with the dihedral group D_8 . Interpreting the game in terms of stabilizers and fixed sets enabled us to easily explain and replicate Q's strategy. This in turn allowed to prove that there exist precisely two classes of winning strategies for Q. Each class contains many different strategies, but all these strategies are equivalent in the sense that they drive the coin through the same sequence of states. It was established that there are exactly two different sequences of states that can guarantee Q's win with probability 1.0. What is noteworthy is the realization that even when the game takes place in larger dihedral groups, or even in the entire $U(2)$, this fact remains true. The essence of the game can be

succinctly summarized by saying that there are precisely two paths that lead to Q's win and, of course, no path that leads to Picard's win. Finally, when extensions of the game without any restriction were examined, it was discovered that for the quantum player to surely win against the classical player the tremendous advantage of quantum actions is not enough. Q must also make the first and the last move, or else he is not certain to win.

There still many questions to be answered and a lot of important issues have to be addressed. These results were based on the assumption that the initial state of the coin and the target states of the players were one the the basis states. If this is not the case, and entanglement comes into play, how does that affect the progression of the game? This is a particularly interesting topic, worthy to be the subject of a future work.

Author Contributions: Conceptualization, T.A. and A.S.; methodology, T.A.; validation, A.S.; formal analysis, A.S.; investigation, T.A.; writing original draft preparation, T.A. and A.S.; writing review and editing, T.A. and A.S.; visualization, A.S.; supervision, T.A.; project administration, T.A. and A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

Abbreviations

The following abbreviations are used in this manuscript:

PQG The PQ penny flip game
 D_n The dihedral group of order $2n$
 $U(2)$ The unitary group of dimension 2

Appendix A. Proofs of the Main Results

Appendix A.1. Proofs for Section 3

Theorem A1 (The ambient group of the PQG). *The ambient group of the PQG is D_8 .*

Proof of Theorem A1. By recalling the presentation (6) for the general dihedral group D_n : $D_n = \langle s, t \mid s^2 = t^2 = (st)^n = \mathbb{1} \rangle$, and making the concrete associations

$$\mathbb{1} \mapsto I \stackrel{(2)}{=} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad s \mapsto F \stackrel{(2)}{=} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \text{and} \quad t \mapsto H \stackrel{(2)}{=} \begin{bmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{bmatrix}, \quad (\text{A1})$$

the following facts can be readily verified: $F^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$, $H^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$, $FH = \begin{bmatrix} \cos \frac{2\pi}{8} & -\sin \frac{2\pi}{8} \\ \sin \frac{2\pi}{8} & \cos \frac{2\pi}{8} \end{bmatrix} \stackrel{(7)}{=} R_{\frac{2\pi}{8}}$, $(FH)^k = \begin{bmatrix} \cos \frac{2\pi k}{8} & -\sin \frac{2\pi k}{8} \\ \sin \frac{2\pi k}{8} & \cos \frac{2\pi k}{8} \end{bmatrix} \stackrel{(7)}{=} R_{\frac{2\pi k}{8}}$, for $0 \leq k \leq 7$, and $(FH)^8 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$. Hence, presentation (6) is satisfied by F and H for $n = 8$, meaning that F and H generate the dihedral group D_8 : $D_8 = \langle F, H \rangle$. $\square$

Appendix A.2. Proofs for Section 4

It is straightforward to verify the proofs given below, by keeping in mind that:

- the action of a dihedral group on any state of the quantum coin can be determined by simply multiplying the matrices representing the elements of the group with the ket corresponding to the state; and
- a ket of the form $e^{i\theta} |\psi\rangle$, with $\theta \in \mathbb{R}$, represents the same state as the ket $|\psi\rangle$.

Proposition A1 (The action of D_8 on B).

1. $|0\rangle$ and $|1\rangle$ have the same orbit:

$$D_8 \star |0\rangle = D_8 \star |1\rangle = \{|0\rangle, |+\rangle, |1\rangle, |-\rangle\}. \quad (\text{A2})$$

2. The orbit of B is:

$$D_8 \star B = \{|0\rangle, |+\rangle, |1\rangle, |-\rangle\}. \quad (\text{A3})$$

Proof of Proposition A1.

1. By systematically multiplying the standard matrix representation of the rotations and reflections of D_8 , given by Formulas (13) and (14), with $|0\rangle$ one gets $|0\rangle, |+\rangle, |1\rangle, -|-\rangle, -|0\rangle, -|+\rangle, -|1\rangle$ and $|-\rangle$. Of course, $|0\rangle$ and $-|0\rangle$ represent the same state. This also applies to the pairs $|1\rangle$ and $-|1\rangle, |+\rangle$ and $-|+\rangle, |-\rangle$ and $-|-\rangle$. Thus, $D_8 \star |0\rangle = \{|0\rangle, |+\rangle, |1\rangle, |-\rangle\}$. In a symmetrical fashion, computing $D_8 \star |1\rangle$ verifies that (A2) holds.
2. Simply taking the union of the orbits $D_8 \star |0\rangle$ and $D_8 \star |1\rangle$ gives the desired result. $\square$

Proposition A2 (The stabilizers of $|0\rangle, |+\rangle, |1\rangle$ and $|-\rangle$ in D_8).

- The stabilizers of $|0\rangle$ and $|1\rangle$ in D_8 are

$$D_8(|0\rangle) = \{I, R_\pi, S_0, S_{\frac{4\pi}{8}}\} \quad \text{and} \quad D_8(|1\rangle) = \{I, R_\pi, S_0, S_{\frac{4\pi}{8}}\}. \quad (\text{A4})$$

- The stabilizers of $|+\rangle$ and $|-\rangle$ are

$$D_8(|+\rangle) = \{I, R_\pi, F, S_{\frac{6\pi}{8}}\} \quad \text{and} \quad D_8(|-\rangle) = \{I, R_\pi, F, S_{\frac{6\pi}{8}}\}. \quad (\text{A5})$$

Proof of Proposition A2. It suffices to show how to find the stabilizer of $|+\rangle$, since the proofs regarding the states $|0\rangle, |1\rangle$ and $|-\rangle$ are completely analogous. It suffices to exhaustively multiply the matrices as given by Formulas (13) and (14) with $|+\rangle$ and note for which matrices the outcome is again $|+\rangle$. The stabilizer of $|+\rangle$ will contain precisely these matrices. These are the two rotations I and R_π , through angles zero and π (see Figure 2), and the two reflections F , about the line passing through vertices 2 and 6, and $S_{\frac{6\pi}{8}}$, about the line passing through vertices 4 and 8 (see Figure 4). It is thus established that $D_8(|+\rangle) = \{I, R_\pi, F, S_{\frac{6\pi}{8}}\}$. $\square$

Proposition A3 (The fixed set of $\{I, F\}$ in D_8).

1. The fixed set of F in D_8 is the set

$$\text{Fix}(F) = \{|+\rangle, |-\rangle\}. \quad (\text{A6})$$

2. The fixed set of $M_P = \{I, F\}$ in D_8 is the set

$$\text{Fix}(\{I, F\}) = \{|+\rangle, |-\rangle\}. \quad (\text{A7})$$

Proof of Proposition A3.

1. (A3) implies that in D_8 the coin can be in one the states contained in $D_8 \star B = \{|0\rangle, |+\rangle, |1\rangle, |-\rangle\}$. By successively multiplying F with these states, it can be found that: $F|0\rangle = |1\rangle, F|+\rangle = |+\rangle, F|1\rangle = |0\rangle$, and $F|-\rangle = |-\rangle$. These results show that the action of F on the states $|+\rangle$ and $|-\rangle$ does not change the state of the coin. Hence, $\text{Fix}(F) = \{|+\rangle, |-\rangle\}$ and (A6) holds.

2. The identity I fixes every state in the orbit, so the intersection of $\text{Fix}(I)$ with $\text{Fix}(F)$ is just $\text{Fix}(F)$, which verifies (A7). □

Appendix A.3. Proofs for Section 5

Theorem A2 (Characteristic properties of winning strategies). *If (A_1, A_2) is a winning strategy for Q , then:*

$$A_2 I A_1 |0\rangle = A_2 F A_1 |0\rangle = |0\rangle, \quad \text{and} \quad (\text{A8})$$

$$A_1 |0\rangle \in \text{Fix}(\{F\}). \quad (\text{A9})$$

Proof of Theorem A2. By Definition 1 (A_1, A_2) is a winning strategy for Q if for every strategy of Picard, Q wins the game with probability 1.0. If the coin, just prior to measurement, is in a state $a|0\rangle + b|1\rangle$, with $b \neq 0$, then the probability that Q will win the game is strictly less than 1.0. Therefore, every winning strategy must eventually drive the coin to the state $|0\rangle$, no matter what Picard plays. This implies that $A_2 I A_1 |0\rangle = A_2 F A_1 |0\rangle = |0\rangle$.

Assuming, in order to reach a contradiction, that $|\psi\rangle = A_1 |0\rangle$ is not fixed by F . Then $F|\psi\rangle = |\psi'\rangle$, where state $|\psi'\rangle$ is different from state $|\psi\rangle$. However, according to (A8), $A_2 I A_1 |0\rangle = A_2 F A_1 |0\rangle \Rightarrow A_2 I |\psi\rangle = A_2 F |\psi\rangle \Rightarrow A_2 |\psi\rangle = A_2 |\psi'\rangle \Rightarrow |\psi\rangle = |\psi'\rangle$, which contradicts the assumption that $|\psi\rangle$ and $|\psi'\rangle$ are different states. The last implication is valid because A_2 , as a group element, has a unique inverse. □

Theorem A3 (The ambient group of the PQG is D_8). *Assuming that $M_P = \{I, F\}$ and $M_Q = D_8$, i.e., the ambient group of the PQG is D_8 , then the following hold.*

1. Q has exactly two classes of winning and dominant strategies

$$C_+ = [(H, H)] \quad \text{and} \quad C_- = [(S_{\frac{7\pi}{8}}, S_{\frac{7\pi}{8}})], \quad (\text{A10})$$

each containing 16 equivalent strategies.

2. The winning state paths corresponding to C_+ and C_- are

$$\tau_{C_+} = (|0\rangle, |+\rangle, |0\rangle) \quad \text{and} \quad \tau_{C_-} = (|0\rangle, |-\rangle, |0\rangle). \quad (\text{A11})$$

3. Picard has no winning strategy.

Proof of Theorem A3. If the ambient group is D_8 , the quantum coin will be in one of the states of the orbit $D_8 \star B$. From (A3) it follows that $D_8 \star B = \{|0\rangle, |+\rangle, |1\rangle, |-\rangle\}$. Let $\sigma = (A_1, A_2)$ be a winning strategy for Q . According to (A8), $A_2 I A_1 |0\rangle = A_2 F A_1 |0\rangle = |0\rangle$.

1. There are 4 cases to consider, depending on the state of the coin after Q 's first move A_1 .

- (i) If Q leaves the coin at state $|0\rangle$, i.e., $A_1 |0\rangle = |0\rangle$, then (A8) implies that $A_2 I |0\rangle = A_2 F |0\rangle = |0\rangle \Rightarrow A_2 |0\rangle = A_2 |1\rangle = |0\rangle \Rightarrow |0\rangle = |1\rangle$, which is absurd. To arrive at this contradiction, the fact that A_2 , as a group element, has a unique inverse was used. This result shows that the first move of every winning strategy for Q must drive the coin to a state other than $|0\rangle$.
- (ii) If Q sends the coin to state $|1\rangle$, i.e., $A_1 |0\rangle = |1\rangle$, then (A8) implies that $A_2 I |1\rangle = A_2 F |1\rangle = |0\rangle \Rightarrow A_2 |1\rangle = A_2 |0\rangle = |0\rangle \Rightarrow |1\rangle = |0\rangle$, which is also absurd for the same reason as in the previous case. Hence, the first move of every winning strategy for Q cannot send the coin to state $|1\rangle$.
- (iii) If Q sends the coin to state $|+\rangle$, which can be achieved through 4 different ways: $H, R_{\frac{2\pi}{8}}, S_{\frac{5\pi}{8}}$, and $R_{\frac{10\pi}{8}}$, then, no matter what Picard plays, the coin will remain in this state because $|+\rangle$ is fixed by I and F , according to (A7). Finally, Q can send the coin back to the $|0\rangle$ state with 4 different ways: $H, R_{\frac{14\pi}{8}}, S_{\frac{5\pi}{8}}$ and $R_{\frac{6\pi}{8}}$. This means that Q has 16 different winning strategies, which, in

view of Definition 9, are equivalent. Thus, they constitute one equivalence class of 16 winning strategies, which is designated by $\mathcal{C}_+$. Any one of them, e.g., (H, H) can be taken as a representative of this class, so it accurate to write $\mathcal{C}_+ = [(H, H)]$.

- (iv) In an analogous way, Q can send the coin to state $|-\rangle$ using 4 different moves: $S_{\frac{7\pi}{8}}, R_{\frac{14\pi}{8}}, S_{\frac{3\pi}{8}}$ or $R_{\frac{6\pi}{8}}$. Picard is unable to change this state because $|-\rangle$ is also fixed by I and F , according to (A7). This enables Q to send the coin back to $|0\rangle$ with 4 different ways: $S_{\frac{7\pi}{8}}, R_{\frac{2\pi}{8}}, S_{\frac{3\pi}{8}}$ or $R_{\frac{10\pi}{8}}$. Once again Q has 16 different winning strategies, which, in view of Definition 9, are equivalent. They make the second equivalence class of 16 winning strategies, which is denoted by $\mathcal{C}_-$. Any one of them, for instance $(S_{\frac{7\pi}{8}}, S_{\frac{7\pi}{8}})$, can be taken as a representative of this class, so it is also accurate to write $\mathcal{C}_- = [(S_{\frac{7\pi}{8}}, S_{\frac{7\pi}{8}})]$.

This concludes the proof of (A10).

2. Based on the above analysis of cases (iii) and (iv), it is straightforward to verify (A11).
3. By Definition 1, Picard has no winning strategy because if Q employs one of their winning strategies, Picard has 0.0 probability to win the game.

□

Theorem A4 (The smallest dihedral group for the PQG is D_8). D_8 is the smallest dihedral group in which PQG can be meaningfully played and Q has a quantum winning strategy.

Proof of Theorem A4. The two assumptions on which this result is based are:

1. Picard's set of moves M_P is $\{I, F\}$, according to assumption (24). As a classical player, Picard must certainly be able to flip the coin, or else the game will be meaningless. On the other hand, he should not be able to employ a true quantum move.
2. Q's actions M_Q should contain at least one unitary operator other than the classical I and F operators, in order to exhibit quantumness.

With the above clarifications in mind, none of the smaller dihedral groups D_3, D_4, D_5, D_6 , and D_7 can serve as the operational space for a meaningful, or at least non-trivial, realization of the PQG.

- The dihedral group D_3 does not contain the reflection F . One can verify this by comparing Formula (9) with Formula (14) for $n = 3$ and $k = 0, 1, 2$. This shows that D_3 does not satisfy assumption (24) and, hence, is an inappropriate stage for the PQG.
- D_4 contains the reflection F . However, the orbit $D_4 \star B$ is $\{|0\rangle, |1\rangle\}$. This means that Q can only flip the coin from heads to tails or vice versa. If $M_Q = D_4$, then the PQG degenerates to the classical coin tossing game. Q is unable to employ a truly quantum strategy, something that contradicts the second assumption at the beginning of Section 5 and goes against the spirit of the PQG. Moreover, in D_4 Q no longer possesses a winning strategy. For these reasons, it is meaningless to play the PQG in D_4 .
- The dihedral groups D_5, D_6 and D_7 do not contain the reflection F either. Once again the Formulas (9) and (14) for $n = 5, 6$ and 7 and $k = 0, 1, \dots, n - 1$ can be used to verify this fact. These groups do not satisfy assumption (24) and are also inadmissible for the PQG.

□

Proposition A4 (D_n does not contain F when n odd). If n is odd, then the dihedral group D_n does not contain F .

Proof of Proposition A4. Assuming to the contrary that there is an odd n so that D_n does contain F , then there must be a $k, 0 \leq k < n$, such that

$$F = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \stackrel{(14)}{=} \pm \begin{bmatrix} \cos \frac{2\pi k}{n} & \sin \frac{2\pi k}{n} \\ \sin \frac{2\pi k}{n} & -\cos \frac{2\pi k}{n} \end{bmatrix} \Rightarrow \left\{ \cos \frac{2\pi k}{n} = 0 \right\} \text{ or } \left\{ \cos \frac{2\pi k}{n} = 0 \right\} \text{ or } \left\{ \sin \frac{2\pi k}{n} = 1 \right\} \text{ or } \left\{ \sin \frac{2\pi k}{n} = -1 \right\}. \quad (\text{A12})$$

The fact that $0 \leq k < n$, implies that $0 \leq \frac{2\pi k}{n} < 2\pi$. Hence, either $\frac{2\pi k}{n} = \frac{\pi}{2}$ or $\frac{2\pi k}{n} = \frac{3\pi}{2}$. The former equation leads to $k = \frac{n}{4}$ and the latter to $k = \frac{3n}{4}$. Both are impossible because n is odd. This proves that F does not exist in D_n when n is odd. $\square$

It will also be helpful to recall some well-known trigonometric identities (see [31]):

$$\cos\left(\theta + \frac{\pi}{2}\right) = -\sin \theta \quad \sin\left(\theta + \frac{\pi}{2}\right) = \cos \theta \quad (\text{A13})$$

$$\cos(\theta + \pi) = -\cos \theta \quad \sin(\theta + \pi) = -\sin \theta \quad (\text{A14})$$

$$\sin \theta + \sin \varphi = 2 \sin\left(\frac{\theta + \varphi}{2}\right) \cos\left(\frac{\theta - \varphi}{2}\right) \quad \sin \theta - \sin \varphi = 2 \cos\left(\frac{\theta + \varphi}{2}\right) \sin\left(\frac{\theta - \varphi}{2}\right) \quad (\text{A15})$$

$$\cos(\theta + \varphi) = \cos \theta \cos \varphi - \sin \theta \sin \varphi \quad \cos(\theta - \varphi) = \cos \theta \cos \varphi + \sin \theta \sin \varphi \quad (\text{A16})$$

$$\sin(\theta + \varphi) = \sin \theta \cos \varphi + \cos \theta \sin \varphi \quad \sin(\theta - \varphi) = \sin \theta \cos \varphi - \cos \theta \sin \varphi \quad (\text{A17})$$

Lemma A1. Let G be any group of linear operators. Then

1. if $|1\rangle \in G \star |0\rangle$, then $G \star |0\rangle = G \star |1\rangle$, and
2. if $|0\rangle \in G \star |1\rangle$, then $G \star |0\rangle = G \star |1\rangle$.

Proof of Lemma A1.

1. By Definition 8, if $|1\rangle \in G \star |0\rangle$, then there exists an element $g_2 \in G$ such that $|1\rangle = g_2 \star |0\rangle$. Every member of $|x_1\rangle \in G \star |1\rangle$ has the form $|x_1\rangle = g_1 \star |1\rangle$ for some $g_1 \in G$. These combined with Definition 7, imply that $|x_1\rangle = (g_1 g_2) \star |0\rangle$, that is $|x_1\rangle \in G \star |0\rangle$ too. Hence, $G \star |1\rangle \subset G \star |0\rangle$.
At the same time, Definition 7 asserts that $|0\rangle = g_2^{-1} \star |1\rangle$. Every member of $|x_2\rangle \in G \star |0\rangle$ has the form $|x_2\rangle = g_3 \star |0\rangle$ for some $g_3 \in G$. Therefore, $|x_2\rangle = (g_3 g_2^{-1}) \star |1\rangle$, that is $|x_2\rangle \in G \star |1\rangle$ too, that is, $G \star |0\rangle \subset G \star |1\rangle$. This establishes that $G \star |0\rangle = G \star |1\rangle$.
2. The proof is completely symmetrical. $\square$

Lemma A2. The action of D_n on the basis kets $|0\rangle$ and $|1\rangle$ gives rise to the following two sequences of kets $|\varphi_k\rangle$ and $|\chi_k\rangle$, where $0 \leq k \leq n-1$:

$$|\varphi_k\rangle = \begin{bmatrix} \cos \frac{2\pi k}{n} \\ \sin \frac{2\pi k}{n} \end{bmatrix} \quad (\text{A18})$$

$$|\chi_k\rangle = \begin{bmatrix} -\sin \frac{2\pi k}{n} \\ \cos \frac{2\pi k}{n} \end{bmatrix} \quad (\text{A19})$$

Proof of Lemma A2. The action of the standard matrix representation of D_n on the computational basis B is given by the matrix-vector multiplication of the matrices (13) and (14) with the kets $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. The resulting products are the following.

$$\begin{bmatrix} \cos \frac{2\pi k}{n} & -\sin \frac{2\pi k}{n} \\ \sin \frac{2\pi k}{n} & \cos \frac{2\pi k}{n} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos \frac{2\pi k}{n} \\ \sin \frac{2\pi k}{n} \end{bmatrix} \quad (\text{A20})$$

$$\begin{bmatrix} \cos \frac{2\pi k}{n} & \sin \frac{2\pi k}{n} \\ \sin \frac{2\pi k}{n} & -\cos \frac{2\pi k}{n} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos \frac{2\pi k}{n} \\ \sin \frac{2\pi k}{n} \end{bmatrix} \quad (\text{A21})$$

$$\begin{bmatrix} \cos \frac{2\pi k}{n} & -\sin \frac{2\pi k}{n} \\ \sin \frac{2\pi k}{n} & \cos \frac{2\pi k}{n} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -\sin \frac{2\pi k}{n} \\ \cos \frac{2\pi k}{n} \end{bmatrix} \quad (\text{A22})$$

$$\begin{bmatrix} \cos \frac{2\pi k}{n} & \sin \frac{2\pi k}{n} \\ \sin \frac{2\pi k}{n} & -\cos \frac{2\pi k}{n} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \sin \frac{2\pi k}{n} \\ -\cos \frac{2\pi k}{n} \end{bmatrix} \quad (\text{A23})$$

Comparing (A20) and (A21) shows that the action of the rotations and the reflections of D_n on the basis ket $|0\rangle$ gives rise to precisely the same kets, specifically those that have the form shown in (A18). Symmetrically, (A22) and (A23), together with the fact that $|\psi\rangle$ and $-|\psi\rangle$ describe the same state, reveal that the action of the rotations and the reflections of D_n on the basis ket $|1\rangle$ leads to the same kets, namely those shown in (A19). $\square$

Lemma A3 (The action of D_n on B when $n = 4m$). *If $n \geq 3$ is a multiple of 4, then the action of the dihedral group D_n on the computational basis B is*

$$D_n \star |0\rangle = D_n \star |1\rangle = D_n \star B = \left\{ \cos \frac{2\pi k}{n} |0\rangle + \sin \frac{2\pi k}{n} |1\rangle : 0 \leq k < \frac{n}{2} \right\}. \quad (\text{A24})$$

Proof of Lemma A3. In this case $n = 4m$, $m \geq 1$, and (A18) and (A19) become:

$$|\varphi_k\rangle = \begin{bmatrix} \cos \frac{\pi k}{2m} \\ \sin \frac{\pi k}{2m} \end{bmatrix} \quad \text{and} \quad |\chi_k\rangle = \begin{bmatrix} -\sin \frac{\pi k}{2m} \\ \cos \frac{\pi k}{2m} \end{bmatrix}, \quad 0 \leq k \leq 4m - 1. \quad (\text{A25})$$

These kets are not all different. To understand this observe that

$$|\chi_k\rangle \stackrel{(\text{A25})}{=} \begin{bmatrix} -\sin \frac{\pi k}{2m} \\ \cos \frac{\pi k}{2m} \end{bmatrix} \stackrel{(\text{A13})}{=} \begin{bmatrix} \cos \left(\frac{\pi k}{2m} + \frac{\pi}{2} \right) \\ \sin \left(\frac{\pi k}{2m} + \frac{\pi}{2} \right) \end{bmatrix} = \begin{bmatrix} \cos \left(\frac{\pi(k+m)}{2m} \right) \\ \sin \left(\frac{\pi(k+m)}{2m} \right) \end{bmatrix}. \quad (\text{A26})$$

When k ranges from 0 to $3m - 1$, equations (A25) and (A26) immediately give that

$$|\chi_k\rangle = |\varphi_{k+m}\rangle, \quad 0 \leq k \leq 3m - 1. \quad (\text{A27})$$

It remains to ascertain what happens when k ranges from $3m$ to $4m - 1$. Then, $k + m$ ranges from $4m$ to $4m + (m - 1)$ and, according to (A27), the kets $|\chi_k\rangle$ assume the values

$$\begin{bmatrix} \cos \left(2\pi + \frac{\pi \cdot 0}{2m} \right) \\ \sin \left(2\pi + \frac{\pi \cdot 0}{2m} \right) \end{bmatrix} = \begin{bmatrix} \cos \frac{\pi \cdot 0}{2m} \\ \sin \frac{\pi \cdot 0}{2m} \end{bmatrix} \stackrel{(\text{A25})}{=} |\varphi_0\rangle, \dots, \begin{bmatrix} \cos \left(2\pi + \frac{\pi(m-1)}{2m} \right) \\ \sin \left(2\pi + \frac{\pi(m-1)}{2m} \right) \end{bmatrix} = \begin{bmatrix} \cos \frac{\pi(m-1)}{2m} \\ \sin \frac{\pi(m-1)}{2m} \end{bmatrix} \stackrel{(\text{A25})}{=} |\varphi_{m-1}\rangle. \quad (\text{A28})$$

By combining equations (A27) and (A28) it follows that $|\chi_k\rangle = |\varphi_{(k+m) \bmod n}\rangle$, $0 \leq k \leq 4m - 1$, which shows that all the kets of the $|\chi_k\rangle$ sequence also appear in the $|\varphi_k\rangle$ sequence. Another way to arrive at this conclusion is to observe that the D_n -orbits of $|0\rangle$ and $|1\rangle$ consist of kets appearing in the sequences $|\varphi_k\rangle$ and $|\chi_k\rangle$, respectively. In view of the fact that $|1\rangle = |\chi_0\rangle$ appears in the $|\varphi_k\rangle$ sequence as $|\varphi_m\rangle$, Lemma A1 asserts that $D_n \star |0\rangle = D_n \star |1\rangle = D_n \star B$. Furthermore, only $2m$ of the kets in the $|\varphi_k\rangle$ sequence are distinct ($|\psi\rangle$ and $-|\psi\rangle$ represent the same state). In particular,

$$|\varphi_k\rangle = -|\varphi_{k+2m}\rangle, \quad 0 \leq k \leq 2m - 1, \quad (\text{A29})$$

i.e., $|\varphi_k\rangle$ and $|\varphi_{k+2m}\rangle$ correspond to antipodal points in the unit circle (Figure 6 gives a geometric depiction of the situation). The latter is easily proved as follows:

$$|\varphi_k\rangle \stackrel{(A25)}{=} \begin{bmatrix} \cos \frac{\pi k}{2m} \\ \sin \frac{\pi k}{2m} \end{bmatrix} \stackrel{(A14)}{=} \begin{bmatrix} -\cos\left(\frac{\pi k}{2m} + \pi\right) \\ -\sin\left(\frac{\pi k}{2m} + \pi\right) \end{bmatrix} = \begin{bmatrix} -\cos \frac{\pi k + 2\pi m}{2m} \\ -\sin \frac{\pi k + 2\pi m}{2m} \end{bmatrix} \stackrel{(A25)}{=} -|\varphi_{k+2m}\rangle, \quad 0 \leq k \leq 2m-1.$$

When k ranges from 0 to $2m-1$, formula (A25) gives the first $2m$ kets in the $|\varphi_k\rangle$ sequence: $\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} \cos \frac{\pi}{2m} \\ \sin \frac{\pi}{2m} \end{bmatrix}, \dots, \begin{bmatrix} \cos \frac{\pi(2m-1)}{2m} \\ \sin \frac{\pi(2m-1)}{2m} \end{bmatrix}$. These are all distinct and correspond to different points on the upper semicircle of the unit circle making an angle $\frac{\pi k}{2m}$, where $0 \leq k \leq 2m-1$, with the positive x -axis, respectively. Finally, noting that $2m-1 < 2m = \frac{n}{2}$, shows that (A24) holds. $\square$

Lemma A4 (The action of D_n on B when $n = 2m$). *If $n \geq 3$ is even, but not a multiple of 4, then the action of the dihedral group D_n on the computational basis B is*

$$D_n \star |0\rangle = \left\{ \cos \frac{2\pi k}{n} |0\rangle + \sin \frac{2\pi k}{n} |1\rangle : 0 \leq k < \frac{n}{2} \right\}, \quad (A30)$$

$$D_n \star |1\rangle = \left\{ -\sin \frac{2\pi k}{n} |0\rangle + \cos \frac{2\pi k}{n} |1\rangle : 0 \leq k < \frac{n}{2} \right\}, \quad (A31)$$

$$D_n \star B = \left\{ \cos \frac{2\pi k}{n} |0\rangle + \sin \frac{2\pi k}{n} |1\rangle : 0 \leq k < \frac{n}{2} \right\} \cup \left\{ -\sin \frac{2\pi k}{n} |0\rangle + \cos \frac{2\pi k}{n} |1\rangle : 0 \leq k < \frac{n}{2} \right\}. \quad (A32)$$

Proof of Lemma A4. In this case $n = 2m$, where $m \geq 3$ is odd and (A18) and (A19) now give:

$$|\varphi_k\rangle = \begin{bmatrix} \cos \frac{\pi k}{m} \\ \sin \frac{\pi k}{m} \end{bmatrix} \quad \text{and} \quad |\chi_k\rangle = \begin{bmatrix} -\sin \frac{\pi k}{m} \\ \cos \frac{\pi k}{m} \end{bmatrix}, \quad 0 \leq k \leq 2m-1 \quad \text{and } m \text{ odd}. \quad (A33)$$

The kets in the above sequences are not all different. Only m of the kets in the $|\varphi_k\rangle$ sequence and only m of the kets in the $|\chi_k\rangle$ sequence are distinct. In particular,

$$|\varphi_k\rangle = -|\varphi_{k+m}\rangle, \quad 0 \leq k \leq m-1, \quad (A34)$$

that is kets $|\varphi_k\rangle$ and $|\varphi_{k+m}\rangle$ correspond to antipodal points in the unit circle (Figure 7 gives a geometric depiction of the situation). This can be shown as follows:

$$|\varphi_k\rangle \stackrel{(A33)}{=} \begin{bmatrix} \cos \frac{\pi k}{m} \\ \sin \frac{\pi k}{m} \end{bmatrix} \stackrel{(A14)}{=} \begin{bmatrix} -\cos\left(\frac{\pi k}{m} + \pi\right) \\ -\sin\left(\frac{\pi k}{m} + \pi\right) \end{bmatrix} = \begin{bmatrix} -\cos \frac{\pi k + \pi m}{m} \\ -\sin \frac{\pi k + \pi m}{m} \end{bmatrix} \stackrel{(A33)}{=} -|\varphi_{k+m}\rangle, \quad 0 \leq k \leq m-1.$$

When k ranges from 0 to $m-1$, Formula (A33) gives the first m kets in the $|\varphi_k\rangle$ sequence:

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} \cos \frac{\pi}{m} \\ \sin \frac{\pi}{m} \end{bmatrix}, \dots, \begin{bmatrix} \cos \frac{\pi(m-1)}{m} \\ \sin \frac{\pi(m-1)}{m} \end{bmatrix}. \quad (A35)$$

They correspond to m points that lie on the upper semicircle of the unit circle and make angles $0 < \frac{\pi}{m} < \frac{2\pi}{m} < \dots < \frac{\pi(m-1)}{m}$, respectively, with the positive x -axis. The associated angles lie in the interval $[0, \pi)$ because $\frac{\pi(m-1)}{m} < \pi$ and, therefore, these points are all distinct. (A30) holds, since $m-1 < m = \frac{n}{2}$. Analogously, it also holds that

$$|\chi_k\rangle = -|\chi_{k+m}\rangle, \quad 0 \leq k \leq m-1, \quad (A36)$$

that is kets $|\chi_k\rangle$ and $|\chi_{k+m}\rangle$ also correspond to antipodal points in the unit circle (again consult Figure 7). When k ranges from 0 to $m-1$, Formula (A33) gives the first m kets in the $|\chi_k\rangle$ sequence

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} -\sin \frac{\pi}{m} \\ \cos \frac{\pi}{m} \end{bmatrix}, \dots, \begin{bmatrix} -\sin \frac{\pi(m-1)}{m} \\ \cos \frac{\pi(m-1)}{m} \end{bmatrix}. \quad (\text{A37})$$

These kets correspond to m points that lie on the unit circle and make angles $\frac{\pi}{2} < \frac{\pi}{2} + \frac{\pi}{m} < \frac{\pi}{2} + \frac{2\pi}{m} < \dots < \frac{\pi}{2} + \frac{\pi(m-1)}{m}$, respectively, with the positive x -axis. The associated angles lie in the interval $[\frac{\pi}{2}, \frac{\pi}{2} + \pi)$ because $\frac{\pi(m-1)}{m} < \pi$, i.e., they are all distinct. The fact that $m-1 < m = \frac{n}{2}$, ascertains that (A31) holds. The important observation in this case is that

- no ket (or its opposite) from the sequence (A35) appears in the sequence (A37), that is $|\chi_{k_2}\rangle \neq \pm |\varphi_{k_1}\rangle$, $\forall k_1, k_2$, where $0 \leq k_1, k_2 \leq m-1$; and
- no ket (or its opposite) from the sequence (A37) appears in the sequence (A35), i.e., $|\varphi_{k_1}\rangle \neq \pm |\chi_{k_2}\rangle$, $\forall k_1, k_2$, where $0 \leq k_1, k_2 \leq m-1$.

Assuming towards a contradiction that there exist k_1, k_2 , where $0 \leq k_1, k_2 \leq m-1$, such that

$$\begin{bmatrix} \cos \frac{\pi k_1}{m} \\ \sin \frac{\pi k_1}{m} \end{bmatrix} = \pm \begin{bmatrix} -\sin \frac{\pi k_2}{m} \\ \cos \frac{\pi k_2}{m} \end{bmatrix} \Rightarrow \left\{ \begin{array}{l} \cos \frac{\pi k_1}{m} = -\sin \frac{\pi k_2}{m} \\ \sin \frac{\pi k_1}{m} = \cos \frac{\pi k_2}{m} \end{array} \right\} \text{ or } \left\{ \begin{array}{l} \cos \frac{\pi k_1}{m} = \sin \frac{\pi k_2}{m} \\ \sin \frac{\pi k_1}{m} = -\cos \frac{\pi k_2}{m} \end{array} \right\}, \quad (\text{A38})$$

leads to the following sequence of implications

$$\begin{aligned} & \left\{ \begin{array}{l} \cos \frac{\pi k_1}{m} + \sin \frac{\pi k_2}{m} = 0 \\ \sin \frac{\pi k_1}{m} - \cos \frac{\pi k_2}{m} = 0 \end{array} \right\} \text{ or } \left\{ \begin{array}{l} \cos \frac{\pi k_1}{m} - \sin \frac{\pi k_2}{m} = 0 \\ \sin \frac{\pi k_1}{m} + \cos \frac{\pi k_2}{m} = 0 \end{array} \right\} \xRightarrow{(\text{A13})} \\ & \left\{ \begin{array}{l} \sin\left(\frac{\pi k_1}{m} + \frac{\pi}{2}\right) + \sin \frac{\pi k_2}{m} = 0 \\ \sin \frac{\pi k_1}{m} - \sin\left(\frac{\pi k_2}{m} + \frac{\pi}{2}\right) = 0 \end{array} \right\} \text{ or } \left\{ \begin{array}{l} \sin\left(\frac{\pi k_1}{m} + \frac{\pi}{2}\right) - \sin \frac{\pi k_2}{m} = 0 \\ \sin \frac{\pi k_1}{m} + \sin\left(\frac{\pi k_2}{m} + \frac{\pi}{2}\right) = 0 \end{array} \right\} \xRightarrow{(\text{A15})} \\ & \left\{ \begin{array}{l} 2 \sin\left(\frac{\pi(k_1+k_2)}{2m} + \frac{\pi}{4}\right) \cos\left(\frac{\pi(k_1-k_2)}{2m} + \frac{\pi}{4}\right) = 0 \\ 2 \cos\left(\frac{\pi(k_1+k_2)}{2m} + \frac{\pi}{4}\right) \sin\left(\frac{\pi(k_1-k_2)}{2m} - \frac{\pi}{4}\right) = 0 \end{array} \right\} \text{ or } \left\{ \begin{array}{l} 2 \cos\left(\frac{\pi(k_1+k_2)}{2m} + \frac{\pi}{4}\right) \sin\left(\frac{\pi(k_1-k_2)}{2m} + \frac{\pi}{4}\right) = 0 \\ 2 \sin\left(\frac{\pi(k_1+k_2)}{2m} + \frac{\pi}{4}\right) \cos\left(\frac{\pi(k_1-k_2)}{2m} - \frac{\pi}{4}\right) = 0 \end{array} \right\} \end{aligned}$$

To proceed further it is convenient to distinguish the following cases.

- The first case gives the system $\left\{ \begin{array}{l} \sin\left(\frac{\pi(k_1+k_2)}{2m} + \frac{\pi}{4}\right) = 0 \\ \cos\left(\frac{\pi(k_1+k_2)}{2m} + \frac{\pi}{4}\right) = 0 \end{array} \right\}$, which is clearly impossible because there is no φ such that $\sin \varphi = \cos \varphi = 0$.
- The next case involves the system $\left\{ \begin{array}{l} \sin\left(\frac{\pi(k_1+k_2)}{2m} + \frac{\pi}{4}\right) = 0 \\ \sin\left(\frac{\pi(k_1-k_2)}{2m} - \frac{\pi}{4}\right) = 0 \end{array} \right\}$. Using (A17), this system can be transformed to the equivalent $\left\{ \begin{array}{l} \sin\left(\frac{\pi(k_1+k_2)}{2m}\right) \cos \frac{\pi}{4} + \cos\left(\frac{\pi(k_1+k_2)}{2m}\right) \sin \frac{\pi}{4} = 0 \\ \sin\left(\frac{\pi(k_1-k_2)}{2m}\right) \cos \frac{\pi}{4} - \cos\left(\frac{\pi(k_1-k_2)}{2m}\right) \sin \frac{\pi}{4} = 0 \end{array} \right\}$, which, in turn, implies that $\left\{ \begin{array}{l} \tan\left(\frac{\pi(k_1+k_2)}{2m}\right) = -1 \\ \tan\left(\frac{\pi(k_1-k_2)}{2m}\right) = 1 \end{array} \right\}$. The fact that $0 \leq k_1, k_2 \leq m-1$, means that $0 \leq \frac{\pi(k_1+k_2)}{2m} < \pi$ and $-\frac{\pi}{2} < -\frac{\pi(k_1-k_2)}{2m} \leq \frac{\pi(k_1-k_2)}{2m} \leq \frac{\pi(m-1)}{2m} < \frac{\pi}{2}$. Hence, $\frac{\pi(k_1+k_2)}{2m} = \frac{3\pi}{4}$ and $\frac{\pi(k_1-k_2)}{2m} = \frac{\pi}{4}$. Adding the last two equations gives that $\frac{2\pi k_1}{2m} = \pi \Rightarrow k_1 = m$, which is also impossible because $k_1 \leq m-1$.
- The remaining cases can be dealt with in an entirely analogous manner.

Thus, the first m kets in the $|\varphi_k\rangle$ sequence are all different from the first m kets in the $|\chi_k\rangle$ sequence, which establishes the validity of (A32). $\square$

The results of Lemmas A3 and A4 immediately prove Theorem A5.

Theorem A5 (The action of D_n on B). The action of the general dihedral group $D_n, n \geq 3$, on the computational basis B depends on whether n is a multiple of 4 or even but not a multiple of 4.

1. if n is a multiple of 4, then the action of D_n on the computational basis B is

$$D_n \star |0\rangle = D_n \star |1\rangle = D_n \star B = \left\{ \cos \frac{2\pi k}{n} |0\rangle + \sin \frac{2\pi k}{n} |1\rangle : 0 \leq k < \frac{n}{2} \right\}, \quad (\text{A39})$$

2. if n is even but not a multiple of 4, then the action of D_n on the computational basis B is

$$D_n \star |0\rangle = \left\{ \cos \frac{2\pi k}{n} |0\rangle + \sin \frac{2\pi k}{n} |1\rangle : 0 \leq k < \frac{n}{2} \right\}, \quad (\text{A40})$$

$$D_n \star |1\rangle = \left\{ -\sin \frac{2\pi k}{n} |0\rangle + \cos \frac{2\pi k}{n} |1\rangle : 0 \leq k < \frac{n}{2} \right\}, \quad (\text{A41})$$

$$D_n \star B = \left\{ \cos \frac{2\pi k}{n} |0\rangle + \sin \frac{2\pi k}{n} |1\rangle : 0 \leq k < \frac{n}{2} \right\} \cup \left\{ -\sin \frac{2\pi k}{n} |0\rangle + \cos \frac{2\pi k}{n} |1\rangle : 0 \leq k < \frac{n}{2} \right\}. \quad (\text{A42})$$

Theorem A6 (The fixed set of $\{I, F\}$ in D_n). The fixed set of $M_P = \{I, F\}$ in the general dihedral group $D_n, n \geq 3$, depends on whether n is a multiple of 8 or not.

1. If n is a multiple of 8, then:

$$\text{Fix}(\{I, F\}) = \text{Fix}(F) = \{|+\rangle, |-\rangle\}. \quad (\text{A43})$$

2. In every other case:

$$\text{Fix}(\{I, F\}) = \text{Fix}(F) = \emptyset. \quad (\text{A44})$$

Proof of Theorem A6.

1. If n is a multiple of 8, then $n = 8m, m \geq 1$, then (A18) and (A19) become:

$$|\varphi_k\rangle = \begin{bmatrix} \cos \frac{\pi k}{4m} \\ \sin \frac{\pi k}{4m} \end{bmatrix} \quad \text{and} \quad |\chi_k\rangle = \begin{bmatrix} -\sin \frac{\pi k}{4m} \\ \cos \frac{\pi k}{4m} \end{bmatrix}. \quad (\text{A45})$$

According to (A24) the range of k is $0 \leq k < 4m$. By setting $k = m$ and $k = 3m$ in (A24) it follows that $\cos \frac{2\pi m}{8m} |0\rangle + \sin \frac{2\pi m}{8m} |1\rangle = \cos \frac{\pi}{4} |0\rangle + \sin \frac{\pi}{4} |1\rangle = |+\rangle$ and $\cos \frac{2\pi 3m}{8m} |0\rangle + \sin \frac{2\pi 3m}{8m} |1\rangle = \cos \frac{3\pi}{4} |0\rangle + \sin \frac{3\pi}{4} |1\rangle = -|-\rangle$ belong to $D_n \star B$, i.e., the states $|+\rangle$ and $|-\rangle$ belong to the orbit of B . Proposition A3 asserts that F fixes these kets. What remains is to prove that F fixes no other state in the orbit of B . If F also fixes some ket other than $|+\rangle$ and $|-\rangle$, then there exists a $k, 0 \leq k < 4m$ but $k \neq m, 3m$, such that

$$F \begin{bmatrix} \cos \frac{\pi k}{4m} \\ \sin \frac{\pi k}{4m} \end{bmatrix} = \begin{bmatrix} \sin \frac{\pi k}{4m} \\ \cos \frac{\pi k}{4m} \end{bmatrix} = \pm \begin{bmatrix} \cos \frac{\pi k}{4m} \\ \sin \frac{\pi k}{4m} \end{bmatrix} \Rightarrow \begin{cases} \sin \frac{\pi k}{4m} = \cos \frac{\pi k}{4m} \\ \cos \frac{\pi k}{4m} = \sin \frac{\pi k}{4m} \end{cases} \text{ or } \begin{cases} \sin \frac{\pi k}{4m} = -\cos \frac{\pi k}{4m} \\ \cos \frac{\pi k}{4m} = -\sin \frac{\pi k}{4m} \end{cases} \Rightarrow$$

$$\tan\left(\frac{\pi k}{4m}\right) = 1 \quad \text{or} \quad \tan\left(\frac{\pi k}{4m}\right) = -1. \quad (\text{A46})$$

The fact that $0 \leq k < 4m$, implies that $0 \leq \frac{\pi k}{4m} < \pi$. Therefore, either $\frac{\pi k}{4m} = \frac{\pi}{4}$ or $\frac{\pi k}{4m} = \frac{3\pi}{4}$. The former equation leads to $k = m$ and the latter to $k = 3m$, which correspond to kets $|+\rangle$ and $|-\rangle$, respectively. No other values for k arise and, thus, F fixes no other state.

2. If n is not a multiple of 8, there are two cases to consider.

- n is a multiple of 4, but not a multiple of 8. This implies that $n = 4m$, where m is a positive *odd* integer. Therefore, (A18) and (A19) become:

$$|\varphi_k\rangle = \begin{bmatrix} \cos \frac{\pi k}{2m} \\ \sin \frac{\pi k}{2m} \end{bmatrix} \quad \text{and} \quad |\chi_k\rangle = \begin{bmatrix} -\sin \frac{\pi k}{2m} \\ \cos \frac{\pi k}{2m} \end{bmatrix}. \quad (\text{A47})$$

According to (A24), the range of k is $0 \leq k < 2m$. If there exists a k such that $\frac{\pi k}{2m} = \frac{\pi}{4}$, then k must be equal to $\frac{m}{2}$, which is absurd. Similarly, the existence of a k such that $\frac{\pi k}{2m} = \frac{3\pi}{4}$ is impossible because then k must be equal to $\frac{3m}{2}$. The previous calculations establish that $|+\rangle$ and $|-\rangle$ do not belong to the orbit of B . Moreover, F fixes no ket in the orbit of B . If F did fix some ket, then there would be a k , $0 \leq k < 2m$, such that

$$F \begin{bmatrix} \cos \frac{\pi k}{2m} \\ \sin \frac{\pi k}{2m} \end{bmatrix} = \begin{bmatrix} \sin \frac{\pi k}{2m} \\ \cos \frac{\pi k}{2m} \end{bmatrix} = \pm \begin{bmatrix} \cos \frac{\pi k}{2m} \\ \sin \frac{\pi k}{2m} \end{bmatrix} \Rightarrow \begin{cases} \sin \frac{\pi k}{2m} = \cos \frac{\pi k}{2m} \\ \cos \frac{\pi k}{2m} = \sin \frac{\pi k}{2m} \end{cases} \text{ or } \begin{cases} \sin \frac{\pi k}{2m} = -\cos \frac{\pi k}{2m} \\ \cos \frac{\pi k}{2m} = -\sin \frac{\pi k}{2m} \end{cases} \Rightarrow$$

$$\tan\left(\frac{\pi k}{2m}\right) = 1 \quad \text{or} \quad \tan\left(\frac{\pi k}{2m}\right) = -1. \quad (\text{A48})$$

The fact that $0 \leq k < 2m$, implies that $0 \leq \frac{\pi k}{2m} < \pi$. Therefore, either $\frac{\pi k}{2m} = \frac{\pi}{4}$ or $\frac{\pi k}{2m} = \frac{3\pi}{4}$. The former equation leads to $k = \frac{m}{2}$ and the latter to $k = \frac{3m}{2}$, which are both impossible. Hence, F fixes no state from the orbit of B .

- n is even, but not a multiple of 4, then it can be proved in an analogous manner that in this case too F fixes no state from the orbit of B .

□

Theorem A7 (The ambient group of the PQG is D_{8n}). If $M_P = \{I, F\}$ and $M_Q = D_{8n}$, i.e., the ambient group of the PQG is D_{8n} , where $n \geq 1$, then the following hold.

1. Q has exactly two classes of winning and dominant strategies

$$C_+ = [(H, H)] \quad \text{and} \quad C_- = [(S_{\frac{7\pi}{8}}, S_{\frac{7\pi}{8}})], \quad (\text{A49})$$

each containing 16 equivalent strategies.

2. The winning state paths corresponding to C_+ and C_- are

$$\tau_{C_+} = (|0\rangle, |+\rangle, |0\rangle) \quad \text{and} \quad \tau_{C_-} = (|0\rangle, |-\rangle, |0\rangle). \quad (\text{A50})$$

3. Picard has no winning strategy.

Proof of Theorem A7.

1. The two classes of winning strategies of Q , C_+ , and C_- , which were established by Theorem A3, are also present in every dihedral group D_{8n} .

If in some dihedral group larger than D_8 there exists a third class C' that contains the strategy $\sigma = (A_1, A_2)$, then the action of A_1 must drive the coin into some state other than $|+\rangle$ or $|-\rangle$. However, (A9) asserts that $A_1|0\rangle \in \text{Fix}(\{F\})$, which, in view of (A43), implies that $A_1|0\rangle \in \{|+\rangle, |-\rangle\}$, a contradiction. Hence, there are just two classes of winning strategies C_+ and C_- . It remains to prove that C_+ and C_- do not contain new winning strategies. Let $\sigma = (A_1, A_2)$ be such a “new winning” strategy, other than those established in D_8 . If A_1 is a rotation other than $R_{\frac{2\pi}{8}}$ and $R_{\frac{10\pi}{8}}$ that

sends the coin to state $|+\rangle$, then, according to (13), there exist $n \geq 1$ and $k, 0 \leq k < 8n$, such that $A_1 = \begin{bmatrix} \cos \frac{2\pi k}{8n} & -\sin \frac{2\pi k}{8n} \\ \sin \frac{2\pi k}{8n} & \cos \frac{2\pi k}{8n} \end{bmatrix}$. Therefore,

$$\begin{bmatrix} \cos \frac{2\pi k}{8n} & -\sin \frac{2\pi k}{8n} \\ \sin \frac{2\pi k}{8n} & \cos \frac{2\pi k}{8n} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \pm \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \Rightarrow \begin{bmatrix} \cos \frac{2\pi k}{8n} \\ \sin \frac{2\pi k}{8n} \end{bmatrix} = \pm \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \Rightarrow \begin{cases} \cos \frac{2\pi k}{8n} = \frac{1}{\sqrt{2}} \\ \sin \frac{2\pi k}{8n} = \frac{1}{\sqrt{2}} \end{cases} \text{ or } \begin{cases} \cos \frac{2\pi k}{8n} = -\frac{1}{\sqrt{2}} \\ \sin \frac{2\pi k}{8n} = -\frac{1}{\sqrt{2}} \end{cases}.$$

The fact that $0 \leq k < 8n$, implies that $0 \leq \frac{2\pi k}{8n} < 2\pi$. Hence, either $\frac{2\pi k}{8n} = \frac{\pi}{4}$ or $\frac{2\pi k}{8n} = \frac{5\pi}{4}$. The former equation leads to $k = n$ and the latter to $k = 5n$. This means that $A_1 = \begin{bmatrix} \cos \frac{2\pi}{8} & -\sin \frac{2\pi}{8} \\ \sin \frac{2\pi}{8} & \cos \frac{2\pi}{8} \end{bmatrix} = R_{\frac{2\pi}{8}}$ or $A_1 = \begin{bmatrix} \cos \frac{10\pi}{8} & -\sin \frac{10\pi}{8} \\ \sin \frac{10\pi}{8} & \cos \frac{10\pi}{8} \end{bmatrix} = R_{\frac{10\pi}{8}}$, which contradicts the assumption that A_1 is different from $R_{\frac{2\pi}{8}}$ and $R_{\frac{10\pi}{8}}$. Similar contradictions arise by assuming that A_1 is a reflection different from H or $S_{\frac{5\pi}{8}}$ or that A_1 drives the coin to state $|-\rangle$. Thus, other than those already existing in D_8 , there are no more winning strategies for Q in the larger dihedral groups D_{8n} .

2. Based on the above analysis it is straightforward to see that (A50) holds.
3. By Definition 1, Picard has no winning strategy.

□

The next two theorems settle the general case, where the ambient group is $U(2)$.

Theorem A8 (The fixed set of $\{I, F\}$ in $U(2)$). Under the action of $U(2)$ on the computational basis B , the fixed set of $M_P = \{I, F\}$ is

$$\text{Fix}(\{I, F\}) = \text{Fix}(F) = \{|+\rangle, |-\rangle\}. \quad (\text{A51})$$

Proof of Theorem A8. In this most general case the eigenvalues and the eigenkets of the flip operator F must be computed. The well-known relations

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |+\rangle = |+\rangle \quad \text{and} \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |-\rangle = -|-\rangle, \quad (\text{A52})$$

immediately imply that the two eigenvalues of F are $\lambda = 1$ and $\lambda = -1$. Furthermore, the eigenkets corresponding to the eigenvalues 1 and -1 are $|+\rangle$ and $|-\rangle$, respectively. This proves that F fixes both $|+\rangle$ and $|-\rangle$. □

Theorem A9 (The ambient group of the PQG is $U(2)$). If $M_P = \{I, F\}$ and $M_Q = U(2)$, i.e., the ambient group of the PQG is $U(2)$, then the following hold.

1. Q has exactly two classes of winning and dominant strategies, each containing infinite equivalent strategies:

$$C_+ = [(A_1(\theta_1), A_2(\theta_2))] \quad \text{and} \quad C_- = [(B_1(\theta_3), B_2(\theta_4))], \quad (\text{A53})$$

where

- $A_1(\theta_1)$ is one of $H(\theta_1), R_{\frac{2\pi}{8}}(\theta_1), S_{\frac{5\pi}{8}}(\theta_1)$ or $R_{\frac{10\pi}{8}}(\theta_1)$,
- $A_2(\theta_2)$ is one of $H(\theta_2), R_{\frac{14\pi}{8}}(\theta_2), S_{\frac{5\pi}{8}}(\theta_2)$ or $R_{\frac{6\pi}{8}}(\theta_2)$,
- $B_1(\theta_3)$ is one of $S_{\frac{7\pi}{8}}(\theta_3), R_{\frac{14\pi}{8}}(\theta_3), S_{\frac{3\pi}{8}}(\theta_3)$ or $R_{\frac{6\pi}{8}}(\theta_3)$,
- $B_2(\theta_4)$ is one of $S_{\frac{7\pi}{8}}(\theta_4), R_{\frac{2\pi}{8}}(\theta_4), S_{\frac{3\pi}{8}}(\theta_4)$ or $R_{\frac{10\pi}{8}}(\theta_4)$, and
- $\theta_1, \theta_2, \theta_3, \theta_4$ are possibly different real parameters.

2. The winning state paths corresponding to $\mathcal{C}_+$ and $\mathcal{C}_-$ are

$$\tau_{\mathcal{C}_+} = (|0\rangle, |+\rangle, |0\rangle) \quad \text{and} \quad \tau_{\mathcal{C}_-} = (|0\rangle, |-\rangle, |0\rangle). \quad (\text{A54})$$

3. Picard has no winning strategy.

Proof of Theorem A9.

1. The two classes of winning strategies of $\mathcal{Q}$, $\mathcal{C}_+$ and $\mathcal{C}_-$, which were established by Theorem A3, are present in $U(2)$. However, they now contain infinitely many equivalent strategies. To see why this is so, consider a winning strategy $\sigma = (A_1, A_2)$ in $\mathcal{C}_+$. To this strategy corresponds the collection of infinitely many strategies $(A_1(\theta_1), A_2(\theta_2))$, where $\theta_1, \theta_2 \in \mathbb{R}$. Every strategy in this collection is equivalent to (A_1, A_2) because the action of every operator $A \in U(2)$ on a ket $|\psi\rangle$ is the same as the action of $e^{i\theta} A \in U(2)$ on $|\psi\rangle$. This holds for every strategy in $\mathcal{C}_-$. Hence, in $U(2)$ the two classes $\mathcal{C}_+$ and $\mathcal{C}_-$ contain infinitely many equivalent strategies.

Assuming that there exists a third class $\mathcal{C}'$, let $\sigma = (A_1, A_2)$ be a strategy in this class. Then the action of A_1 must drive the coin into some state other than $|+\rangle$ or $|-\rangle$. However, (A9) asserts that $A_1|0\rangle \in \text{Fix}(\{F\})$, which, in view of (A51), implies that $A_1|0\rangle \in \{|+\rangle, |-\rangle\}$, a contradiction. Consequently, there are just two classes of winning strategies $\mathcal{C}_+$ and $\mathcal{C}_-$. It remains to prove that $\mathcal{C}_+$ and $\mathcal{C}_-$ do not contain new winning strategies, i.e., strategies that are not of the form stated in (A53). To arrive at a contradiction, suppose that $\sigma = (A_1, A_2)$ is a “new winning” strategy. If $A_1 = \begin{bmatrix} z_1 & w_1 \\ z_2 & w_2 \end{bmatrix}$, then its columns form an orthonormal basis for $\mathcal{H}_2$ because it is a unitary operator. This means that they satisfy the following relations:

$$z_1^* z_1 + z_2^* z_2 = 1, \quad (\text{A55})$$

$$w_1^* w_1 + w_2^* w_2 = 1, \quad (\text{A56})$$

$$z_1^* w_1 + z_2^* w_2 = 0. \quad (\text{A57})$$

If A_1 sends the coin to state $|+\rangle$, assuming that A_1 is not of the form $H(\theta_1)$, $R_{\frac{2\pi}{8}}(\theta_1)$, $S_{\frac{5\pi}{8}}(\theta_1)$ or $R_{\frac{10\pi}{8}}(\theta_1)$, then

$$\begin{bmatrix} z_1 & w_1 \\ z_2 & w_2 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = e^{i\theta_1} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \Rightarrow \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = e^{i\theta_1} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}, \quad \text{for some } \theta_1 \in \mathbb{R}. \quad (\text{A58})$$

Together (A58) and (A57) imply that

$$z_1^* w_1 + z_2^* w_2 = 0 \Rightarrow \frac{e^{-i\theta_1}}{\sqrt{2}} (w_1 + w_2) = 0 \Rightarrow w_2 = -w_1. \quad (\text{A59})$$

In view of (A59), (A57) becomes

$$2|w_1|^2 = 1 \Rightarrow |w_1| = \frac{1}{\sqrt{2}}. \quad (\text{A60})$$

All complex numbers of the form $e^{i\varphi} \frac{1}{\sqrt{2}}$, where $\varphi \in \mathbb{R}$, are solutions of the Equation (A60).

By choosing $\varphi = \theta_1$ and setting $w_1 = \frac{e^{i\theta_1}}{\sqrt{2}}$, w_2 becomes $-\frac{e^{i\theta_1}}{\sqrt{2}}$. Hence, A_1 is in fact

$e^{i\theta_1} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$, which means that A_1 is of the form $H(\theta_1)$, $R_{\frac{2\pi}{8}}(\theta_1)$, $S_{\frac{5\pi}{8}}(\theta_1)$ or $R_{\frac{10\pi}{8}}(\theta_1)$, in stark contrast to the initial assumption. Similar contradictions arise by

assuming that A_1 drives the coin to state $|-\rangle$. Thus, the resulting conclusion is that other than the strategies described by (A53), there are no more winning strategies for Q.

2. Based on the above analysis it is straightforward to see that (A54) holds.
3. By Definition 1, Picard has no winning strategy because if Q employs one of their winning strategies, Picard has 0.0 probability to win the game.

□

Appendix A.4. Proofs for Section 6

Theorem A10 (Picard lacks a winning strategy). *Picard does not have a winning strategy in any n -round game, $n \geq 2$, as long as Q makes at least one move.*

Proof of Theorem A10. According to Definition 12 and the assumptions at the beginning of Section 6, in every n -round game with $n \geq 2$, Q makes at least one move. As a matter of fact, any n -round game has one of the following forms.

1. $(Q, P, \dots, Q, P)$, in which case if Q employs the strategy $(H, I, \dots, I)$, the state of the coin prior to measurement will either be $|+\rangle$, if the initial state of the coin is $|0\rangle$, or $|-\rangle$, if the initial state of the coin is $|1\rangle$. This is because $\text{Fix}(\{I, F\}) = \{|+\rangle, |-\rangle\}$, so the coin will stay in one of these states no matter which strategy Picard uses. When the coin is measured, Picard will have exactly 0.5 probability to win irrespective of which is their target state. Thus, Picard does not possess a winning strategy because, by Definition 1, a winning strategy means that he wins the game with probability 1.0.
2. $(P, Q, \dots, P, Q)$, where again, if the same strategy $(H, I, \dots, I)$ is used by Q, it will prevent Picard from surely winning the game. The coin will be in one of its basis states (which one depends on the initial state and Picard's first move) when Q acts on it for the first time. His action will drive the coin to state $|+\rangle$ (if the coin was at state $|0\rangle$) or $|-\rangle$ (if the coin was at state $|1\rangle$). This will be the state of the coin prior to measurement no matter which strategy Picard uses because $\text{Fix}(\{I, F\}) = \{|+\rangle, |-\rangle\}$. When the coin is measured, Picard will have exactly 0.5 probability to win irrespective of their target state. Hence, Picard does not have a winning strategy because, by Definition 1, a winning strategy means that he wins the game with probability 1.0.
3. $(Q, P, \dots, Q, P, Q)$, in which case Q has a winning strategy. If the initial state is the same as Q's target state, then Q's winning strategy is $(H, I, \dots, I, H)$; if it is different, then Q's winning strategy is $(H, I, \dots, I, FH)$. In this case Picard has precisely 0.0 probability to win, so Picard certainly does not possess a winning strategy.
4. $(P, Q, \dots, P, Q, P)$, where once more the strategy $(H, I, \dots, I)$ can be used by Q to prevent Picard from surely winning the game. The coin will be in one of its basis states (which one depends on the initial state and Picard's first move) when Q acts on it for the first time. His action will drive the coin to state $|+\rangle$ (if the coin was at state $|0\rangle$) or $|-\rangle$ (if the coin was at state $|1\rangle$). This will be the state of the coin prior to measurement because $\text{Fix}(\{I, F\}) = \{|+\rangle, |-\rangle\}$. When the coin is measured, Picard will have exactly 0.5 probability to win irrespective of which is their target state. Therefore, Picard does not have a winning strategy because, by Definition 1, a winning strategy means that he wins the game with probability 1.0.

□

Theorem A11 (Q lacks a winning strategy when Picard plays last). *Q does not have a winning strategy in any n -round game, $n \geq 2$, in which Picard makes the last move.*

Proof of Theorem A11. Any n -round game in which Picard makes the last move has one of the following two forms.

1. $(Q, P, \dots, Q, P)$, where n is even and both Picard and Q make $\frac{n}{2}$ moves. Assuming to the contrary that there exists a winning strategy $\sigma_Q = (A_1, \dots, A_{\frac{n}{2}})$ for Q, Definition 1,

implies that for every strategy of Picard, Q wins the game with probability 1.0. Since this holds for every strategy of Picard, it must also hold for the strategies $\sigma_P = (I, \dots, I, I)$ and $\sigma'_P = (I, \dots, I, F)$. The former implies that after Q's last action the coin must be at the basis state $|q_Q\rangle$, whereas the latter implies that after Q's last action the coin must be at the opposite basis state, which is absurd. Thus, Q does not possess a winning strategy.

2. $(P, Q, \dots, P, Q, P)$, where n is odd, Q makes $\frac{n}{2}$ moves and Picard makes $\frac{n}{2} + 1$ moves. Let $\sigma_Q = (A_1, \dots, A_{\frac{n}{2}})$ be a winning strategy for Q. By Definition 1, if Q employs σ_Q , he will win the game with probability 1.0 no matter which strategy Picard chooses. If Picard uses $\sigma_P = (I, \dots, I, I)$, then after Q's last action the coin must be at the basis state $|q_Q\rangle$. On the other hand, if Picard uses $\sigma_P = (I, \dots, I, F)$, then after Q's last action the coin must be at the opposite basis state. This contradiction proves that Q does not possess a winning strategy.

□

Theorem A12 (Q lacks a winning strategy when Picard plays first). *Q does not have a winning strategy in any n -round game, $n \geq 2$, in which Picard makes the first move.*

Proof of Theorem A12. Any n -round game in which Picard makes the first move has one of the following two forms.

1. $(P, Q, \dots, P, Q)$, where n is even and both Picard and Q make $\frac{n}{2}$ moves. Assuming to the contrary that there exists a winning strategy $\sigma_Q = (A_1, \dots, A_{\frac{n}{2}})$ for Q, then Definition 1 implies that for every strategy of Picard, Q wins the game with probability 1.0. Since this holds for every strategy of Picard, it must also hold for the strategies $\sigma_P = (I, \dots, I, I)$ and $\sigma'_P = (F, \dots, I, I)$. The former implies that

$$A_{\frac{n}{2}} \dots A_1 |q_0\rangle = |q_Q\rangle \Rightarrow C |q_0\rangle = |q_Q\rangle, \quad (\text{A61})$$

where $C = A_{\frac{n}{2}} \dots A_1$. Since the composition of unitary operators produces a unitary operator, C is unitary. On the other hand, the latter implies that

$$A_{\frac{n}{2}} \dots A_1 F |q_0\rangle = |q_Q\rangle \Rightarrow CF |q_0\rangle = |q_Q\rangle. \quad (\text{A62})$$

If $|q_0\rangle = |0\rangle$, then $F |q_0\rangle = |1\rangle$, whereas if $|q_0\rangle = |1\rangle$, then $F |q_0\rangle = |0\rangle$. By combining this last result with (A61) and (A62), it follows that

$$C |0\rangle = C |1\rangle = |q_Q\rangle, \quad (\text{A63})$$

which is impossible because C is unitary. Thus, Q does not possess a winning strategy.

2. $(P, Q, \dots, P, Q, P)$, where n is odd, Q makes $\frac{n}{2}$ moves and Picard makes $\frac{n}{2} + 1$ moves. Let $\sigma_Q = (A_1, \dots, A_{\frac{n}{2}})$ be a winning strategy for Q. By Definition 1, if Q employs σ_Q , he will win the game with probability 1.0. If Picard uses $\sigma_P = (I, \dots, I, I)$, then after Q's last action the coin must be at the basis state $|q_Q\rangle$. On the other hand, if Picard uses $\sigma_P = (I, \dots, I, F)$, then after Q's last action the coin must be at the opposite basis state. This contradiction proves that Q does not possess a winning strategy.

□

The next Theorem A13 gives a positive answer to the question of whether Q, and in effect the quantum player, can surely win and under what circumstances.

Theorem A13 (When Q possesses a winning strategy). *In any n -round game, $n \geq 2$, Q has a winning strategy iff Q makes the first and the last move.*

Proof of Theorem A13. The one direction, i.e., if Q has a winning strategy then he must make the first and the last move, is an immediate consequence of Theorems A11 and A12.

It remains to prove the other direction, that is if Q makes the first and the last move, then Q possesses a winning strategy. If the initial state $|q_0\rangle$ is the same as the target state of Q , then $\sigma_Q = (H, I, \dots, I, H)$ is a winning strategy for Q . Q 's first action will drive the coin to either $|+\rangle$ (if the initial state is $|0\rangle$) or $|-\rangle$ (if the initial state is $|1\rangle$). Both $\{|+\rangle, |-\rangle\}$ are fixed by $\{I, F\}$, as Theorem A8 asserts. Q 's last move will send the coin back to $|q_0\rangle$. If the initial state of the coin $|q_0\rangle$ is different from the target state of Q , then it is trivial to check that $\sigma_Q = (H, I, \dots, I, FH)$ a winning strategy for Q . $\square$

Corollary A1 (The impact of initial and target states). *In any n -round game, $n \geq 2$, if Q has a winning strategy, he has a winning strategy for any combination of initial and target states.*

Proof of Corollary A1. An immediate consequence of Theorem A13. $\square$

References

- Maschler, M. *Game Theory*; Cambridge University Press: Cambridge, UK, 2020.
- Dixit, A. *Games of Strategy*; W.W. Norton & Company: New York, NY, USA, 2015.
- Myerson, R. *Game Theory*; Harvard University Press: Cambridge, MA, USA, 1997.
- Meyer, D.A. Quantum strategies. *Phys. Rev. Lett.* **1999**, *82*, 1052.
- Eisert, J.; Wilkens, M.; Lewenstein, M. Quantum games and quantum strategies. *Phys. Rev. Lett.* **1999**, *83*, 3077.
- Wang, X.B.; Kwek, L.; Oh, C. Quantum roulette: an extended quantum strategy. *Phys. Lett. A* **2000**, *278*, 44–46.
- Ren, H.F.; Wang, Q.L. Quantum game of two discriminable coins. *Int. J. Theor. Phys.* **2008**, *47*, 1828–1835.
- Salimi, S.; Soltanzadeh, M. Investigation of quantum roulette. *Int. J. Quantum Inf.* **2009**, *7*, 615–626.
- Anand, N.; Benjamin, C. Do quantum strategies always win? *Quantum Inform. Process.* **2015**, *14*, 4027–4038.
- Zhang, P.; Zhou, X.Q.; Wang, Y.L.; Liu, B.H.; Shadbolt, P.; Zhang, Y.S.; Gao, H.; Li, F.L.; O'Brien, J.L. Quantum gambling based on Nash-equilibrium. *NPJ Quantum Inform.* **2017**, *3*, doi:10.1038/s41534-017-0021-7.
- Andronikos, T.; Sirokofskich, A.; Kastampolidou, K.; Varvouzou, M.; Giannakis, K.; Singh, A. Finite Automata Capturing Winning Sequences for All Possible Variants of the PQ Penny Flip Game. *Mathematics* **2018**, *6*, 20.
- Giannakis, K.; Theocharopoulou, G.; Papalitsas, C.; Fanarioti, S.; Andronikos, T. Quantum Conditional Strategies and Automata for Prisoners' Dilemmata under the EWL Scheme. *Appl. Sci.* **2019**, *9*, 2635.
- Rycerz, K.; Frackiewicz, P. A quantum approach to twice-repeated 2×2 game. *Quantum Inf. Process.* **2020**, *19*, doi:10.1007/s11128-020-02743-0.
- Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11.
- Aharon, N.; Silman, J. Quantum dice rolling: A multi-outcome generalization of quantum coin flipping. *New J. Phys.* **2010**, *12*, 033027.
- Meyer, D.A.; Blumer, H. Parrondo games as lattice gas automata. *J. Stat. Phys.* **2002**, *107*, 225–239.
- Giannakis, K.; Papalitsas, C.; Kastampolidou, K.; Singh, A.; Andronikos, T. Dominant Strategies of Quantum Games on Quantum Periodic Automata. *Computation* **2015**, *3*, 586–599.
- Andronikos, T. Conditions that Enable a Player to Surely Win in Sequential Quantum Games. *Preprints* **2021**, 2021040298, doi:10.20944/preprints202104.0298.v1.
- Kastampolidou, K.; Nikiforos, M.N.; Andronikos, T. A Brief Survey of the Prisoners' Dilemma Game and Its Potential Use in Biology. In *Advances in Experimental Medicine and Biology*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 315–322.
- Theocharopoulou, G.; Giannakis, K.; Papalitsas, C.; Fanarioti, S.; Andronikos, T. Elements of Game Theory in a Bio-inspired Model of Computation. In Proceedings of the 2019 10th International Conference on Information, Intelligence, Systems and Applications (IISA), Patras, Greece, 15–17, July 2019.
- Kastampolidou, K.; Andronikos, T. A Survey of Evolutionary Games in Biology. In *Advances in Experimental Medicine and Biology*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 253–261.
- Artin, M. *Algebra*; Pearson Prentice Hall: Hoboken, NJ, USA, 2011.
- Dummit, D.; Foote, R. *Abstract Algebra*; Wiley: Hoboken, NJ, USA, 2004.
- Lovett, S. *Abstract Algebra: Structures and Applications*; Taylor & Francis: Abingdon, UK, 2015.
- Meier, J. *Groups, Graphs and Trees*; Cambridge University Press: Cambridge, UK, 2011.
- Meyer, C.D. *Matrix Analysis and Applied Linear Algebra*; Society for Industrial and Applied Mathematics: Philadelphia, PA, USA, 2000.
- Anton, H.; Rorres, C. *Elementary Linear Algebra: Applications Version*, 11th ed.; Wiley Global Education: Hoboken, NJ, USA, 2013.
- Hodge, J.K. *Abstract Algebra*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2013.
- Machi, A. *Groups*; Springer: Milan, Italy, 2012.
- Hall, B. *Quantum Theory for Mathematicians*; Graduate Texts in Mathematics; Springer, New York, NY, USA, 2013.
- Beecher, J. *Algebra and Trigonometry*; Pearson: London, UK, 2016.