Strategies for Quantum Races

Troy Lee
Centre for Quantum Software and Information, School of Software,
Faculty of Engineering and Information Technology, University of Technology Sydney, Australia
troyjlee@gmail.com

Maharshi Ray
Centre for Quantum Technologies, National University of Singapore, Singapore
maharshi91@gmail.com

Miklos Santha
IRIF, Univ. Paris Diderot, CNRS, 75205 Paris, France; and
Centre for Quantum Technologies and MajuLab,
National University of Singapore, Singapore 117543
miklos.santha@gmail.com

Abstract

We initiate the study of *quantum races*, games where two or more quantum computers compete to solve a computational problem. While the problem of dueling algorithms has been studied for classical deterministic algorithms [12], the quantum case presents additional sources of uncertainty for the players. The foremost among these is that players do not know if they have solved the problem until they measure their quantum state. This question of "when to measure?" presents a very interesting strategic problem. We develop a game-theoretic model of a multiplayer quantum race, and find an approximate Nash equilibrium where all players play the same strategy. In the two-party case, we further show that this strategy is nearly optimal in terms of payoff among all symmetric Nash equilibria. A key role in our analysis of quantum races is played by a more tractable version of the game where there is no payout on a tie; for such races we completely characterize the Nash equilibria in the two-party case.

One application of our results is to the stability of the Bitcoin protocol when mining is done by quantum computers. Bitcoin mining is a race to solve a computational search problem, with the winner gaining the right to create a new block. Our results inform the strategies that eventual quantum miners should use, and also indicate that the collision probability – the probability that two miners find a new block at the same time – would not be too high in the case of quantum miners. Such collisions are undesirable as they lead to forking of the Bitcoin blockchain.

2012 ACM Subject Classification Theory of computation → Algorithmic game theory

Keywords and phrases Game theory, Bitcoin mining, Quantum computing, Convex optimization

Digital Object Identifier 10.4230/LIPIcs.ITCS.2019.51

Related Version A full version of the paper is available at [14], `https://arxiv.org/abs/1809.03671`.

Acknowledgements We would like to thank Gavin Brennen, Hartmut Klauck, and Marco Tomamichel for very useful discussions about game theory and quantum Bitcoin mining. We would also like to thank Or Sattath for sharing an early version of his work [18] and discussions about its implications.
Part of this work was done while Troy Lee was at the School of Physical and Mathematical Sciences, Nanyang Technological University and the Centre for Quantum Technologies, Singapore. Troy Lee and Maharshi Ray were supported in part by the Singapore National Research

10th Innovations in Theoretical Computer Science (ITCS 2019).
Editor: Avrim Blum; Article No. 51; pp. 51:1–51:21
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Fellowship under NRF RF Award No. NRF-NRFF2013-13. This research was further partially funded by the Singapore Ministry of Education and the National Research Foundation under grant R-710-000-012-135, and in part by the QuantERA ERA-NET Cofund project QuantAlgo.

1 Introduction

We study the scenario of two or more quantum computers competing to solve a computational task, which we call a *quantum race*. This setting presents a different problem to finding the fastest algorithm for a task, as the only goal is to solve the task before the competitors. For example, imagine a search race where Alice and Bob, each armed with identical quantum computers, compete to find a marked item in a database. The first person to find the marked item wins \$1, with the payout being split in the case of a tie. The first natural idea is for Alice to run Grover's algorithm [11], which can find a marked item in a database of size N with high probability in time $O(\sqrt{N})$. However, if Alice's strategy is to run Grover's algorithm and measure after the specified number of steps to maximize her success probability, Bob will have an advantage by measuring after running Grover's algorithm for a few less steps. Although this way Bob has a slightly lower success probability, he gains a huge advantage in always answering first. This simple example shows that the optimal algorithm to solve a problem can be different from the optimal strategy to employ when the goal is to solve the problem before an opponent.

The scenario of competing algorithms has been studied before in the classical deterministic setting [12]. In a classical game, the uncertainty is provided by an unknown probability distribution over the inputs: depending on what the input is, one algorithm may perform better than another. The quantum setting inherently has additional sources of uncertainty, most interestingly that players do not know if they have solved the problem until they *measure* their quantum state. Going back to the search game, in the classical version the players know at every instant if they have found the marked item or not. This is not the case in the quantum setting, where a player can only tell if she has found the desired item by measuring her quantum state. Furthermore, if she measures her state and does not find the marked item, then she must begin the search again from scratch. In the quantum case there is a natural tension between waiting to measure, and thereby building up the probability of success upon measuring, and measuring sooner, to answer before one's competitors. We study this game theoretic problem to develop strategies for players to use in quantum races.

One of our main motivations for studying quantum races is to model quantum computers mining the decentralized currency Bitcoin [16]. Mining is the process by which new blocks of transactions are added to the history of Bitcoin transactions, called the blockchain. The winner of a race to solve a computational search problem gains the right to add a new block of transactions to the blockchain, and participants in this race are called miners. Quantum miners could use Grover's algorithm to solve the search problem with quadratically fewer search queries than needed classically. But what should the strategy of quantum miners be when competing against each other?

▶ **Question 1.** *What is the optimal strategy for quantum miners?*

Figuring out the optimal strategy for quantum miners is important to analyze the impact of quantum mining on the stability of the Bitcoin protocol. When two miners solve the computational search problem at (nearly) the same time, the blockchain can fork as it is unclear which new block is the "correct" history of Bitcoin transactions. Forking is bad for the security of Bitcoin as it can decrease the cost of attacks [10], increase the gain from deviating from the intended mining protocol [9], and generally decreases chain growth and wastes resources. In the classical case, each search query has the same probability of success. In the quantum case, however, because of Grover's algorithm the success probability grows roughly quadratically with the number of search queries. Does this lead to many quantum miners finding blocks at the same time?

▶ **Question 2.** *What is the probability that two or more quantum miners playing the optimal strategy find a block at the same time?*

In the next subsections, we describe our model and results in more detail and the impact it has on these questions.

1.1 The model and results

In a *symmetric* game all players have the same payoff function. In his original paper defining a Nash equilibrium, Nash showed that every symmetric multiparty finite game has a symmetric equilibrium, i.e. one where all players play the same strategy [17]. When all players have identical quantum computers, a quantum race is naturally a symmetric race, and we describe this scenario first.

We model a symmetric multiplayer quantum race in the following way. The pure strategies available to a player are the possible times at which she can measure $1, 2, 3, \ldots, K$. For each time t, a player has an algorithm that she can run for t steps and for which the success probability is p_t. Without loss of generality, we assume that these probabilities form an increasing sequence $0 < p_1 < p_2 < \cdots < p_K \leq 1$. A general strategy is a probability distribution over the possible times to measure. The player who succeeds first receives a payoff of 1. In the case of a tie, the payoff is split amongst all players who succeed first at the same time. Our model can be thought of as a "one-shot" race, as if a player measures and does not succeed, she does not get a chance to restart and try again. While a race where players are allowed to repeatedly restart until someone wins would be more realistic, it becomes much more difficult to analyze due to the proliferation of possible stategies, and we leave this for future work.

Two-player case

We begin explaining our model and results in more detail in the two-player case. In this case, a game defined by the probabilities $p_1, \ldots, p_K$ can be represented by the payoff matrix for Alice, given by the K-by-K matrix A, and the payoff matrix for Bob B. The (s, t) entry of A gives Alice's payoff when she runs an algorithm for time s and Bob plays time t. In the case of a quantum race, this is defined as

$$A(s,t) = \begin{cases} p_s & \text{if } s < t \\ p_s(1-p_s) + \frac{1}{2}p_s^2 & \text{if } s = t \\ p_s(1-p_t) & \text{if } s > t \ . \end{cases} \qquad (1)$$

As the game is symmetric, Bob's payoff matrix is $B = A^{\mathrm{T}}$.

Our analysis of quantum races begins in Section 3 by analyzing a more tractable variant of the game we call a *stingy* quantum race. In a stingy quantum race, there is no payout in the case of a tie (the game organizer is stingy). A Nash equilibrium of a two-party stingy quantum race has very strong constraints on its support structure (see Corollary 16). In particular, if (x, y) is a Nash equilibrium in a two-party stingy quantum race, then the union of the supports of x and y must be an interval $\{T, T+1, \dots, K\}$ that contains the maximum running time K. There are 3 possible types of Nash equilibria in a two-party stingy quantum race, and we characterize all of them (see Theorem 22, and Appendix of [14].

One particularly nice type of equilibrium is what we call a *coinciding* equilibrium. In a coinciding equilibrium, the support of all player's strategies is the same, but the strategies do not have to be identical. This is a more general notion than a symmetric equilibrium where all strategies are the same. In a coinciding equilibrium for a stingy quantum race, the support of each player's strategy is an interval $\{T, T+1, \dots, K\}$. This leaves the problem of determining the starting point T of this interval in a Nash equilibrium. We are able to show that there is always exactly one T such that there is a Nash equilibrium with support $\{T, T+1, \dots, K\}$.

▶ **Theorem 3** (Informal, see Theorem 22). *In a two-party stingy quantum race defined by probabilities $p_1, \dots, p_K$, there is a unique coinciding Nash equilibrium. In this equilibrium all players play the same strategy, and the support of the strategies is an interval $\{T^*, T^*+1, \dots, K\}$.*

We also explicitly find this Nash equilibrium.

This result begs the question: what is this value of T^*? At what success probability does it become worthwhile to start measuring? By putting an additional restriction on the probabilities $p_1, \dots, p_K$, we can give quite a precise answer to this question. We say $p_1, \dots, p_K$ is an ℓ-*dense* sequence (see Definition 13) if $p_1 \le \frac{\ell}{K}, p_K \ge 1 - \frac{\ell}{K}$, and $p_{i+1} - p_i \le \frac{\ell}{K}$ for $i = 2, \dots, K-1$. This is quite a natural restriction that is satisfied for many races. In the quantum search race, where the p_i are the Grover success probabilities, and therefore also in the application to Bitcoin, the ℓ-density condition is satisfied with $\ell = \pi/2$. In the ℓ-dense case, we can give the following bound on T^*.

▶ **Theorem 4** (Informal, see Corollary 25 and Corollary 28). *Let $p_1, \dots, p_K$ be an ℓ-dense sequence with $K \ge 6\ell$. Then the starting point T^* of the unique coinciding Nash equilibrium in the stingy quantum race defined by these probabilities is such that $p_{T^*} = \sqrt{2} - 1 + \Theta\left(\frac{\ell}{K}\right)$.*

Thus it is worthwhile to start measuring once the success probability becomes around $\sqrt{2}-1$, and this is largely independent of the actual values of $p_1, \dots, p_K$.

In Section 4, we apply our analysis of two-player stingy quantum races to the case of general quantum races. As the only difference between a stingy quantum race and a quantum race is the payout on ties, intuitively strategies in these two kinds of races should have similar payoffs when the probability of ties is small. We follow this intuition and show that when $p_1, \dots, p_K$ form an ℓ-dense sequence the probability of a tie is $O(\frac{\ell}{K})$ (see Theorem 27) when players use the unique coinciding equilibrium from the stingy race, and this strategy is an $O(\frac{\ell}{K})$-approximate Nash equilibrium of the corresponding quantum race.

Approximate Nash equilibria are naturally an imperfect lens into true Nash equilibria. The approximate Nash equilibrium we give would not be a reasonable suggestion for the actual strategies of quantum players if there were other equilibria with much higher payoff, for example. We show that this is not the case, and the approximate Nash equilibrium we give is nearly optimal in terms of payoff amongst all symmetric equilibria.

▶ **Theorem 5** (Informal, see Theorem 31 and Theorem 33). *Let $p_1, \dots, p_k$ be an ℓ-dense sequence with $K \ge 6\ell$. Then the unique coinciding equilibrium of the two-player stingy quantum race defined by these probabilities is an $O(\frac{\ell}{K})$-approximate Nash equilibrium in the corresponding quantum race. Moreover, the payoff achieved by this strategy is within $O(\sqrt{\frac{\ell}{K}})$ of the largest payoff achievable by any symmetric Nash equilibrium.*

To show that the approximate Nash equilibrium we give is nearly optimal in terms of payoff (Theorem 33), we use the bilinear programming formulation of Nash equilbria due to Mangasarian and Stone [15]. We exploit the properties of the sum of Alice's and Bob's payoff matrices $A + A^{\mathrm{T}}$ (from Eq. (1)). More specifically, It turns out that over a probability simplex x, the quadratic form $x^{\mathrm{T}}(A + A^{\mathrm{T}})x$ is a negative-definite plus linear function. When optimizing over symmetric strategies this makes the Mangasarian and Stone bilinear program (which is a maximization problem) into a convex quadratic program. We then use Dorn's [8] equivalent dual formulation of a convex quadratic program (see Eq. (17)), which is a minimization problem. We explicitly construct a feasible solution to this dual minimization problem to upper bound the payoff of any symmetric Nash equilibrium. Our construction of this dual solution again makes use of our analysis of stingy quantum races.

Multiplayer case

The case of many players is what we are interested in for the application to Bitcoin. Luckily, we are able to recover analogs of many of the results from the two-player case in the multiplayer case as well. We start in Section 5 by analyzing n-player stingy quantum races, and show the following.

▶ **Theorem 6** (Informal, see Theorem 41)**.** *Let $p_1, \ldots, p_K$ define an n-player stingy quantum race. This race has a unique coinciding Nash equilibrium, and in this equilibrium all players play the same strategy. The support of each strategy is an interval $\{T^*, T^* + 1, \ldots, K\}$.*

To show that an n-player stingy quantum race has a unique coinciding Nash equilibrium, our proof proceeds through a 2-player *asymmetric* stingy quantum race. In a 2-player asymmetric race, Alice has probabilities $p_1, \ldots, p_K$ of succeeding after t steps and Bob has a (potentially different) sequence of probabilities $P_1, \ldots, P_K$. An asymmetric race models the case where Alice and Bob have quantum computers of potentially different speeds. We relate the payoff for Alice in a n-player stingy quantum race to the payoff for Alice in a 2-player quantum race against a more powerful opponent (see Lemma 40). We can then refer to Theorem 21 in Section 3 which completely characterizes coinciding equilibria in asymmetric 2-player stingy quantum races. This gives Theorem 6.

When the sequence $p_1, \ldots, p_K$ is ℓ-dense, we can also say something about the starting point T^* of the n-player coinciding equilibrium, though not as precisely as in the two-party case.

▶ **Theorem 7** (Informal, see Theorem 44)**.** *Let $p_1, \ldots, p_K$ be an ℓ-dense sequence defining a stingy n-player quantum race with $n \geq 2$. If $K \geq 4e\ell n$ then the starting point T^* of the unique coinciding equilibrium is such that $p_{T^*} = \Theta(\frac{1}{n})$.*

This means that the more players there are in a game, the earlier one starts to measure in the unique coinciding equilibrium.

In light of Question 2 we also want to see what the probability of more than one player succeeding at the same time in this unique coinciding equilibrium. We show the following.

▶ **Theorem 8.** *Let $P_1, ..., P_K$ define an ℓ-dense stingy n-player quantum race such that $4en\ell \leq K$. When the players play the coinciding equilibrium of the stingy race, the probability that two or more players succeed at the same time is at most $\frac{8en\ell}{K}$.*

Finally, as in the two-party case, we show that the unique coinciding equilibrium of a stingy race is also an approximate Nash equilibrium in the corresponding quantum race, provided the sequence of probabilities is ℓ-dense.

▶ **Theorem 9.** *Let $P_1, ..., P_K$ define an ℓ-dense stingy n-player quantum race, $n \geq 2$, with $4en\ell \leq K$. If $x = (x_1, ..., x_n)$ is the coinciding Nash equilibrium for this stingy race, then x is an $\frac{8e\ell}{K}$- approximate Nash equilibrium of the corresponding quantum race.*

1.2 Application to Bitcoin

One application of our study of quantum races is to the decentralized digital currency Bitcoin, developed in 2008 by Satoshi Nakamoto [16]. Bitcoin transactions are packaged into blocks and stored in a public ledger called the blockchain. A major obstacle in creating a decentralized currency is to find a way for all parties to agree on the history of transactions. In Bitcoin, this is done through *Nakamoto consensus*: the right to create a new block is decided through proof-of-work, a contest to solve a computational problem. The winner of this contest has the right to make a new block of transactions, is given a reward in bitcoin, and then the process repeats itself. The players competing in this process are called miners. Nakamato consensus remains the primary means of achieving consensus across all cryptocurrencies, although there are coins using other consensus mechanisms such as proof-of-stake [13] or Byzantine agreement [6].

The proof-of-work task used in Bitcoin (originally developed in a system called Hashcash [2]) is essentially a search problem. The problem is to find a value x (called a nonce) such that $h(H \parallel x) \leq t$, where h is a hash function (doubly iterated SHA-256 in the case of Bitcoin), H is the header of the block of transactions to be processed, and t is a hardness parameter that can be varied so that the entire network takes 10 minutes to solve this task, on average.

Several works have studied the impact that quantum computers would have on the Bitcoin protocol [5, 1, 18], both on the mining process we have described above and on the digital signatures used in Bitcoin to authenticate ownership of coins. We will focus here on the impact of quantum computers on Bitcoin mining.

As the Bitcoin proof-of-work is a search task, quantum miners could use Grover's algorithm to find a nonce x satisfying $h(H \parallel x) \leq t$ with quadratically fewer evaluations of the hash function h than is needed by a classical computer [1]. The use of Grover's algorithm creates new issues for proof-of-work that do not exist in the classical case. Desirable properties of a proof-of-work task have been studied from an axiomatic point of view by Biryukov and Khovratovich [3]. One property they give is *progress-freeness*: the probability of a miner solving the proof-of work task in any moment is independent of previous events. This is achieved for a classical miner in the Bitcoin proof of work, as every call to the hash function is equally likely to find a good nonce x. Progress-freeness is not achieved for a quantum miner running Grover's algorithm, as the success probability grows roughly quadratically with the amount of time the algorithm is run.

Sattath [18] points out that this gives a way for quantum miners to deviate from the prescribed protocol in order to increase their chance of winning a block. To explain this deviation, imagine a simplified case where the proof-of-work is to find a unique marked item in a database of size N. Say that Alice, a quantum miner, receives a new block from the network which was found by Bob. When Alice receives this block she will be in the middle of running Grover's algorithm to find the marked item herself. The prescribed protocol says that she should immediately halt this run of Grover's algorithm and begin working

[1] While this seems to give quantum computers a huge advantage for Bitcoin mining, specialized classical Bitcoin mining hardware currently can perform14 trillion hashes per second [4] and would outperform a near-term quantum computer with gate speeds of 100MHz [1]

on a new search problem by mining on top of Bob's new block. However, if Alice has run Grover algorithm for $c\sqrt{N}$ steps, for a constant c, she will have already built up a constant probability of finding the marked item upon measuring. From the point of view of maximizing her payoff, there is no harm in just measuring to see if she finds the marked item. If Alice gets lucky and indeed finds the marked item, then she can broadcast her new block to the network. Depending on her connectivity to the network, some other miners may receive Alice's block before Bob's, and there is some probability that Alice's new block eventually becomes the block accepted by the network rather than Bob's, meaning that Alice will receive the bitcoin reward. Note that this does not happen in the classical case, where after Alice receives Bob's block she would still just have probability $1/N$ to find the marked item with each additional search query. In this case it makes sense to immediately start mining on top of the new block.

Luckily, Sattath also provides an easy fix for the Bitcoin protocol to remedy this problem. Without going into the technical details, this fix essentially forces miners to commit to how long they will run Grover's algorithm *before they begin.* Thus if Alice commits to running Grover's algorithm for time $\sqrt{N}/100$, yet receives Bob's block after time $\sqrt{N}/200$, if she tries to immediately measure and publish her own block, the network will reject it because of the timing discrepancy. This fix fits in very well with our model of quantum races, as a strategy is exactly a probability distribution over choices of times to measure.

The quantum race that captures the case of Bitcoin mining is what we call the *Grover race* (see Definition 12). In this race, the success probability p_t is given by the success probability of t-iterations of Grover's algorithm [2]. This race is an ℓ-dense race for $\ell = \pi/2$. The size of the search space, and thus the maximum number of iterations K to run Grover's algorithm, is determined by the *difficulty* setting of the Bitcoin protocol. Currently the difficulty (as of September 7, 2018) is approximately $7 \cdot 10^{12}$, which, by Bitcoin's definition of difficulty, means that the network has to do roughly $2^{32} \cdot 7 \cdot 10^{12}$ many hashes to succeed, in expectation. This leads to a value of K of approximately 10^{11}. Thus for this application $\frac{\ell}{K}$ is very small, and Theorem 9 implies that the unique coinciding equilibrium for the stingy Grover race is an ϵ-approximate Nash equilibrium in the Grover race for $\epsilon \leq 3 \cdot 10^{-10}$. This gives a reasonable answer to Question 1 for what a good strategy would be for quantum miners, and moreover has the desirable property that all miners run the same algorithm. By Theorem 8, when there are n miners running this strategy the probability of a tie is at most $3n \cdot 10^{-10}$. This gives an answer to Question 2, that quantum mining is not likely to produce a high forking rate and thereby destabilize the Bitcoin protocol.

2 Preliminaries

We use e ≈ 2.71828 for Euler's number. For a probability $0 \leq p \leq 1$, we set $\bar{p} = 1 - p$. For a natural number n, we let $[n] = \{1, \ldots, n\}$. We let $\Delta_n = \{x \in \mathbb{R}^n : x \geq 0, \sum_{i=1}^{n} x_i = 1\}$ be the probability simplex. For $x \in \Delta_n$ we let $\sup(x) = \{i \in [n] : x_i > 0\}$ be the support of x.

▶ **Definition 10** (quantum race). A 2-*player quantum race* is specified by two sequences of increasing probabilities $0 < p_1 < p_2 < \cdots < p_K \leq 1$, and $0 < P_1 < P_2 < \cdots < P_K \leq 1$ for some integer $K \geq 2$. The set of pure strategies of both players is $[K]$. The $K \times K$ payoff

[2] It is known that t queries of Grover's algorithm maximizes the probability of success in a search problem over all t-query quantum algorithms [7].

matrix A of Alice and B of Bob are defined as

$$A(i,j) = \begin{cases} p_i & \text{if } i < j, \\ p_i \bar{P}_j + \frac{1}{2} p_i P_i & \text{if } i = j, \\ p_i \bar{P}_j & \text{otherwise.} \end{cases} \qquad B(i,j) = \begin{cases} P_j & \text{if } j < i, \\ P_j \bar{p}_i + \frac{1}{2} p_i P_i & \text{if } i = j, \\ P_j \bar{p}_i & \text{otherwise.} \end{cases}$$

If $p_i = P_i$ for all $i = 1, \ldots, K$ then we call the game a *symmetric* quantum race. Note that in this case $B = A^{\mathrm{T}}$.

In our study of quantum races, a key role will be played by an auxiliary game that is easier to analyze called a stingy quantum race. A stingy quantum race differs from a quantum race only in that no payout is given in the case of a tie.

▶ **Definition 11** (stingy quantum race). A 2-*player stingy quantum race* is specified by two sequences of increasing probabilities $0 < p_1 < p_2 < \cdots < p_K \leq 1$, and $0 < P_1 < P_2 < \cdots < P_K \leq 1$ for some integer $K \geq 2$. The set of pure strategies of both players is $[K]$. The $K \times K$ payoff matrix A_0 of Alice is defined as

$$A_0(i,j) = \begin{cases} p_i & \text{if } i < j, \\ p_i \bar{P}_j & \text{otherwise.} \end{cases}$$

The payoff matrix of Bob B_0 is defined as

$$B_0(i,j) = \begin{cases} P_j & \text{if } j < i, \\ P_j \bar{p}_i & \text{otherwise.} \end{cases}$$

If $p_i = P_i$ for all $i = 1, \ldots, K$ then we call the game a *symmetric* stingy quantum race. Note that in this case $B_0 = A_0^{\mathrm{T}}$.

The main specific quantum race we will be interested in is the *Grover race.* This results from two players competing to find a marked item in a database and playing by running Grover's algorithm for a certain amount of time and then measuring. Formally, the race is defined as follows.

▶ **Definition 12** (Grover race). We define the (stingy) Grover race on N items as the symmetric (stingy) quantum race with $K = \left\lceil \frac{\pi}{4}\sqrt{N} - 3/2 \right\rceil$ and $p_t = \sin^2\left(2(t+1/2)\arcsin\left(\frac{1}{\sqrt{N}}\right)\right)$, for $1 \leq t \leq K$.

Here p_t is the success probability of Grover's algorithm of finding a unique marked item in a database of N items. It is known that p_t is the highest success probability for finding a marked item for any quantum algorithm making t many calls to the database [7].

The Grover race has many nice properties, and we will abstract out one of them here. This allows us to show results for a general class of quantum races, rather than just the Grover race.

▶ **Definition 13** (dense race). Let $p_1 < p_2 < \cdots < p_K \leq 1$. We call the sequence $(p_1, \ldots, p_K)$ ℓ-dense if $p_1 \leq \frac{\ell}{K}$, $p_K \geq 1 - \frac{\ell}{K}$, and $p_{i+1} - p_i \leq \frac{\ell}{K}$ for all $i = 1, \ldots, K-1$. For a dense sequence $(p_1, \ldots, p_K)$ will similarly call the symmetric (stingy) quantum race defined by this sequence a symmetric (stingy) ℓ-dense quantum race.

The (stingy) Grover race is an ℓ-dense race with $\ell = \pi/2$.

3 Two-player stingy quantum races

We will first analyze Nash equilibria in stingy quantum races. We can show several structural properties about the support of Nash equilibria in stingy quantum races that make them easier to analyze than quantum races. After our analysis in this section, we will bootstrap our knowledge of Nash equilibria in stingy quantum races to find an approximate Nash equilibrium for quantum races.

Consider a stingy quantum race given by the probabilities $0 < p_1 < p_2 < \cdots < p_K \leq 1$ and $0 < P_1 < P_2 < \cdots < P_K$, and let y be a mixed strategy of Bob. For $t \leq K$, we let $\sup_{\leq t}(y) = \{j \in \sup(y) : j \leq t\}$ be the set of times played by Bob that are at most t, and similarly, we let $\sup_{>t}(y) = \{j \in \sup(y) : j > t\}$ be the set of times played by Bob that are greater than t. Observe that when Alice plays the pure strategy t against y, her payoff is

$$e_t^{\mathrm{T}} Ay = p_t \left(\sum_{j \in \sup_{\leq t}(y)} y_j \bar{P}_j + \sum_{j \in \sup_{>t}(y)} y_j \right).$$

▶ **Claim 14.** *Let (x, y) be a Nash equilibrium of a 2-player stingy quantum race. If $t_1 \in \sup(x)$ then there does not exist $t_2 > t_1$ with $\sup_{\leq t_1}(y) = \sup_{\leq t_2}(y)$.*

Proof. Say that the game is defined by probabilities $0 < p_1 < p_2 < \cdots < p_K \leq 1$ and $0 < P_1 < P_2 < \cdots < P_k$ If $\sup_{\leq t_1}(y) = \sup_{\leq t_2}(y)$ then

$$e_{t_2}^{\mathrm{T}} Ay = \frac{p_{t_2}}{p_{t_1}} e_{t_1}^{\mathrm{T}} Ay.$$

As $p_{t_1} < p_{t_2}$, the payoff for playing t_2 is strictly larger than that for playing t_1. Therefore t_1 is not a best response for y, in contradiction with the definition of a Nash equilibrium. ◀

This claim implies that the support structure of Nash equilibria in stingy quantum races is relatively simple. We first make the following definition.

▶ **Definition 15.** A pair of strategies (x, y) is called *coinciding* if $\sup(x) = \sup(y)$. A pair of strategies (x, y) is called *alternating* if there exists $1 \leq t_1 < t_2 \leq K$ such that the support of one player is $\{t_1, t_1 + 2, \ldots, t_2 - 1\}$ and the support of the other is $\sup(y) = \{t_1 + 1, t_1 + 3, \ldots, t_2\}$. A pair of strategies (x, y) is called (t_1, c, t_2)*-alternating-coinciding* if there are natural numbers $1 \leq t_1 < t_2 \leq K$ and $t_1 + 2 \leq c \leq t_2$ such that the support of one player is $\{t_1, t_1 + 2, \ldots, c - 2, c, c + 1, c + 2, \ldots, t_2\}$ and the support of the other is $\sup(y) = \{t_1 + 1, t_1 + 3, \ldots, c - 3, c - 1, c, c + 1, c + 2, \ldots, t_2\}$.

▶ **Corollary 16.** *Let (x, y) be a Nash equilibrium of a stingy quantum race specified by probabilities $0 < p_1 < p_2 < \cdots < p_K \leq 1$ and $0 < P_1 < P_2 < \cdots < P_k$. Then there is some $1 \leq T \leq K$ such that*

- $\sup(x) \cup \sup(y) = [T, K]$,
- *(x, y) is either coinciding, alternating, or alternating-coinciding.*

Proof. From Claim 14 we can easily derive the following two statements:

- $\sup(x) \cup \sup(y)$ is an interval containing the time with maximum success probability,
- For every $t_1, t_2 \in \sup(x)$ there must be $t \in \sup(y)$ with $t_1 < t \leq t_2$.

These statements immediately imply the claim. ◀

We now study the particularly simple coinciding equilibria. Due to space constraints we do not discuss the other types of equilibria here. However, we give a full characterization of all Nash equilibria in a symmetric stingy quantum race in the full version of the paper [14].

3.1 Unique coinciding equilibrium

We first look for Nash equilibria where the mixed strategies of Alice and Bob have the same support. If the number of strategies is K, we know by Corollary 16 that this support must be a set $\{T, T+1, \ldots, K\}$, for some $1 \leq T \leq K$.

▶ **Lemma 17.** *Consider a stingy quantum race defined by $0 < p_1 < \ldots < p_K \leq 1$ and $0 < P_1 < P_2 < \cdots < P_k$. Let $x, y \in \mathbb{R}^K$. Then (x, y) is a Nash equilibrium for this game with support $\{T, T+1, \ldots, K\}$, for some $1 \leq T \leq K$, if and only if x and y satisfy the following system of equations and inequalities.*

$$\begin{aligned}
e_t^{\mathrm{T}} Ay &= e_T^{\mathrm{T}} Ay, && \textit{for } \; T < t \leq K \;, && (2)\\
e_{T-1}^{\mathrm{T}} Ay &\leq e_T^{\mathrm{T}} Ay, && && (3)\\
y_t &= 0 && \textit{for } \; 0 < t < T \;, && (4)\\
y_t &> 0 && \textit{for } \; T \leq t \leq K \;, && (5)\\
\sum_{t=T}^{K} y_t &= 1 && && (6)\\
x^{\mathrm{T}} B e_t &= x^{\mathrm{T}} B e_T, && \textit{for } \; T < t \leq K \;, && (7)\\
x^{\mathrm{T}} B e_{T-1} &\leq x^{\mathrm{T}} B e_T, && && (8)\\
x_t &= 0 && \textit{for } \; 0 < t < T \;, && (9)\\
x_t &> 0 && \textit{for } \; T \leq t \leq K \;, && (10)\\
\sum_{t=T}^{K} x_t &= 1 \;. && && (11)
\end{aligned}$$

Proof. Eq. (4)–(6) and (9)–(11) express that x and y are probability distributions with support $\{T, T+1, \ldots, K\}$. The other conditions for a Nash equilibrium are that all strategies in the support of x are best responses against y and vice versa. That all strategies in the support of x are best responses against y means

$$\begin{aligned}
e_t^{\mathrm{T}} Ay &= e_T^{\mathrm{T}} Ay, && \text{for } \; T < t \leq K \;,\\
e_{t-1}^{\mathrm{T}} Ay &\leq e_t^{\mathrm{T}} Ay, && \text{for } \; 1 \leq t < T.
\end{aligned}$$

The first equation here is exactly Eq. (2). The inequality here is implied by Eq. (3). This is because for $t < T-1$, $e_t^{\mathrm{T}} Ay = \frac{p_t}{p_{T-1}} e_{T-1}^{\mathrm{T}} Ay$, as $\sup_{\leq T-1}(y) = \sup_{\leq t}(y)$. A similar argument show that Eq. (7)–(8) show that all strategies in the support of y are best responses against x. ◀

When $P_K = 1$, then Alice has zero payoff on playing time K. Thus as long as $K \geq 2$, when $P_K = 1$ there is no coinciding Nash equilibrium (x, y) where $\sup(x) = \sup(y) = \{K\}$. A similar argument applies when $p_K = 1$. We will therefore exclude the case $T = K$ and either $p_K = 1$ or $P_K = 1$ for the next definition and Lemma 19.

▶ **Definition 18.** We define the values q_T^A, q_T^B, for $T = 2, \ldots, K$, and $r_T^A, r_T^B, z_T^A, z_T^B$, for $T = 1, \ldots, K-1$. The values z_K^A, r_K^A are not defined when $T = K, p_K = 1$ and z_K^B, r_K^B are not defined when $T = K, P_K = 1$.

$$q_i^A = \frac{1}{p_i}\left(\frac{1}{P_{i-1}} - \frac{1}{P_i}\right), \qquad q_i^B = \frac{1}{P_i}\left(\frac{1}{p_{i-1}} - \frac{1}{p_i}\right),$$

$$r_T^A = \frac{1}{\bar{p}_T}\left(\frac{1}{P_K} - \sum_{i=T+1}^{K} \bar{p}_i q_i^A\right), \qquad r_T^B = \frac{1}{\bar{P}_T}\left(\frac{1}{p_K} - \sum_{i=T+1}^{K} \bar{P}_i q_i^B\right),$$

$$z_T^A = r_T^A + \sum_{i=T+1}^{K} q_i^A, \qquad z_T^B = r_T^B + \sum_{i=T+1}^{K} q_i^B.$$

▶ **Lemma 19.** *For every $1 \leq T \leq K-1$, and the case $T = K$ and $P_K \neq 1$, the system of linear equations composed of the Eq.* (2)*, (4) and (6) of Lemma 17 has a unique solution given by*

$$y_t = \begin{cases} r_T^B / z_T^B & \textit{if} \quad t = T, \\ q_t^B / z_T^B & \textit{if} \quad T < t \leq K, \\ 0 & \textit{otherwise} \ . \end{cases}$$

Proof. For convenience, we drop the normalization condition $\sum_{t=T}^{K} y_t = 1$ and instead scale y such that the expected payoff of a best response is 1. That is, we replace Eq. (6) by Eq. (12):

$$e_T^{\mathrm{T}} A y = 1. \tag{12}$$

Clearly the solutions of Eq. (2),(4),(6) and the solutions of Eq. (2),(4),(12) differ only by a constant multiplicative factor, and from a solution of the latter system a solution of the former one can be obtained by dividing it coordinate-wise by $\sum_{t=T}^{K} y_t$.

We first want to find the solutions of Eq. (2) and (12). Together, they can be expressed in matrix form as:

$$\begin{bmatrix} p_T \bar{P}_T & p_T & p_T & \cdots & p_T \\ p_{T+1}\bar{P}_T & p_{T+1}\bar{P}_{T+1} & p_{T+1} & \cdots & p_{T+1} \\ p_{T+2}\bar{P}_T & p_{T+2}\bar{P}_{T+1} & p_{T+2}\bar{P}_{T+2} & \cdots & p_{T+2} \\ \vdots & & & \ddots & \vdots \\ p_K \bar{P}_T & p_K \bar{p}_{T+1} & p_K \bar{P}_{T+2} & \cdots & p_K \bar{P}_K \end{bmatrix} \begin{bmatrix} y_T \\ y_{T+1} \\ y_{T+2} \\ \vdots \\ y_K \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}. \tag{13}$$

We can simplify the above system of linear equations as follows:

$$\begin{bmatrix} 0 & P_{T+1} & 0 & \cdots & 0 \\ 0 & 0 & P_{T+2} & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ \bar{P}_T & \bar{P}_{T+1} & \bar{P}_{T+2} & \cdots & \bar{P}_K \end{bmatrix} \begin{bmatrix} y_T \\ y_{T+1} \\ y_{T+2} \\ \vdots \\ y_K \end{bmatrix} = \begin{bmatrix} 1/p_T - 1/p_{T+1} \\ 1/p_{T+1} - 1/p_{T+2} \\ 1/p_{T+2} - 1/p_{T+3} \\ \vdots \\ 1/p_K \end{bmatrix}.$$

From this we can see that, for every $1 \leq T \leq K$, Eq. (13) has a unique solution, given by $y_T = r_T^B$, and $y_t = q_t^B$, for $T < t \leq K$. ◀

▶ **Definition 20.** Define T_A^* (respectively T_B^*) as the smallest integer $1 \leq T \leq K$ such that $r_T^A > 0$ (respectively $r_T^B > 0$). When $T_A^* = T_B^*$ we denote their common value as T^*.

This definition makes sense as in the case $p_K = 1$ (when r_K^A is not defined) we see that $r_{K-1}^A > 0$ and otherwise $r_K^A = \frac{1}{\bar{p}_K P_K} > 0$. A similar argument applies for r_K^B.

▶ **Lemma 21.** *Eq.* (2)*–*(6) *have a solution if and only if* $T = T_B^*$*. In the case* $T = T_B^*$*, the solution is unique and is given by*

$$y_t = \begin{cases} r^B_{T_B^*}/z^B_{T_B^*} & \textit{if} \quad t = T_B^*, \\ q^B_t/z^B_{T_B^*} & \textit{if} \quad T_B^* < t \leq K. \end{cases}$$

Proof. Refer [14]. ◀

The following theorem characterizes the coinciding Nash equilibria in a stingy quantum race.

▶ **Theorem 22.** *A stingy quantum race defined by probabilities* $0 < p_1 < \ldots < p_K \leq 1$ *and* $0 < P_1 < \ldots < P_K \leq 1$ *has a coinciding Nash equilibrium if and only if* $T_A^* = T_B^*$*. In this case, letting* $T^* = T_A^* = T_B^*$ *there is a unique coinciding equilibrium given by*

$$x_t = \begin{cases} r^A_{T^*}/z^A_{T^*} & \textit{if} \quad t = T^*, \\ q^A_t/z^A_{T^*} & \textit{if} \quad T^* < t \leq K \end{cases}, \qquad y_t = \begin{cases} r^B_{T^*}/z^B_{T^*} & \textit{if} \quad t = T^*, \\ q^B_t/z^B_{T^*} & \textit{if} \quad T^* < t \leq K \end{cases}.$$

In particular, when $p_i = P_i$ *for all* $1 \leq i \leq K$ *then* (x, x) *is the unique coinciding Nash equilibrium.*

Proof. By Lemma 17 a coinciding Nash equilibrium (x, y) supported on $\{T, T+1, \ldots, K\}$ must satisfy Eq. (2)–(11). By Theorem 21, Eq. (2)–(6) are satisfied if and only if $T = T_B^*$ and y is given as in the Lemma. We can also apply Theorem 21 to (the transpose of) Eq. (7)–(11) to see that they have a solution if and only if $T = T_A^*$ and x is given by

$$x_t = \begin{cases} r^A_{T_A^*}/z^A_{T_A^*} & \text{if} \quad t = T_A^*, \\ q^A_t/z^A_{T_A^*} & \text{if} \quad T_A^* < t \leq K, \\ 0 & \text{otherwise.} \end{cases}$$

As x and y must have the same support in a coinciding Nash equilibrium, there can only exist a coinciding Nash equilibrium if $T_A^* = T_B^*$.

When $p_i = P_i$ for all $1 \leq i \leq K$ then clearly $r^A_T = r^B_T$ and $q^A_i = q^B_i$ and it will always be the case that $T_A^* = T_B^*$. Thus there will always exist a Nash equilibrium in this case, given by the unique solution to Eq. (2)–(11). ◀

3.2 Payoff and collision probability

In this section we will explore the consequences of the coinciding Nash equilibrium we have found for the payoff of the game and for the probability that the two players win at the same time, the collision probability. For these results, we will only consider the symmetric case when there is always a unique symmetric equilibrium whose support begins at $T^* = T_A^* = T_B^*$. Note that the payoff for each player with this strategy is $\frac{1}{z_{T^*}}$. Since a player receives payoff 1 upon winning, $\frac{1}{z_{T^*}}$ is also exactly the each player's winning probability.

To investigate the collision probability, we will also make the following definitions.

▶ **Definition 23** (Unnormalized collision probability)**.** Define

$$\sigma(T) = p_T^2 r_T^2 + \sum_{i=T+1}^{K} p_i^2 q_i^2 \ .$$

With this definition, $\frac{1}{z_{T^*}^2}\sigma(T^*)$ is the collision probability we are interested in. First we analyze the payoff in a symmetric stingy quantum race.

▶ **Theorem 24.** *Let $p_1 < p_2 < \cdots < p_K$ define a stingy symmetric quantum race. Then $z_{T^*} = 1 + \sqrt{1 + \frac{1}{p_K^2} + \sigma(T^*)}$. In particular, $\frac{1}{z_{T^*}} \leq \sqrt{2} - 1$.*

Proof. Refer [14]. ◀

▶ **Corollary 25.** *If $T^* \geq 2$ then*

$$p_{T^*-1} \leq \sqrt{2} - 1 \ .$$

Proof. As can be seen from Bob playing time $T^* - 1$, we have $p_{T^*-1} z_{T^*} \leq 1$, thus $p_{T^*-1} \leq \sqrt{2} - 1$ by Theorem 24. ◀

Although Theorem 24 gives an exact expression for the payoff, we would like to get a general lower bound on the payoff. This requires showing an upper bound on the collision probability. Showing an upper bound on the collision probability is also important for the application to Bitcoin, to estimate the forking probability amongst quantum miners.

The first step to upper bounding the collision probability is to get a rough lower bound on p_{T^*}. This is our initial bootstrap, which will then let us upper bound the collision probability and then in turn get a sharper lower bound on p_{T^*} in Corollary 28. For these results we restrict to ℓ-dense stingy quantum races.

▶ **Lemma 26.** *Let $p_1, \ldots, p_K$ define an ℓ-dense symmetric stingy quantum race. If $K \geq 6\ell$ then $p_{T^*} > \frac{5}{21}$. In particular, $T^* \geq 2$.*

Proof. Refer [14]. ◀

▶ **Theorem 27.** *Let $p_1, \ldots, p_K$ define an ℓ-dense symmetric stingy quantum race. If $K \geq 6\ell$ then*

$$\frac{\sigma(T^*)}{z_{T^*}^2} \leq \frac{6\ell}{K} \qquad \textit{and} \qquad \sigma(T^*) \leq \frac{196\ell}{K} \ .$$

Proof. Refer [14]. ◀

Now that we have an upper bound on the collision probability, we obtain the following corollary to Theorem 24.

▶ **Corollary 28.** *Let $p_1, \ldots, p_K$ define an ℓ-dense symmetric stingy quantum race. Let $\tau = \frac{50\sqrt{2}\ell}{K}$. If $K \geq 6\ell$ then*

$$z_{T^*} \leq \sqrt{2} + 1 + \tau, \qquad \frac{1}{z_{T^*}} \geq \sqrt{2} - 1 - \tau(\sqrt{2} - 1)^2, \qquad p_{T^*} \geq \sqrt{2} - 1 - \tau(\sqrt{2} - 1)^2 \ .$$

Proof. Refer [14]. ◀

4 Two-player quantum races

In this section, we bootstrap our results about symmetric stingy quantum races to analyze symmetric quantum races. Our main results are two-fold.

1. The unique coinciding Nash equilibrium in an ℓ-dense symmetric stingy quantum race is an approximate Nash equilibrium in the corresponding quantum race.
2. The approximate Nash equilibrium from (1) achieves a payoff which is nearly optimal among all symmetric Nash equilibria in a symmetric quantum race.

The intuition for item (1) is clear. The only difference between a stingy quantum race and a quantum race is the payoff on ties. For the unique coinciding Nash equilibrium we have shown that the collision probability is $O(\ell/K)$, thus the change in payoff on ties will make only a small change to the payoffs under this strategy.

For item (2), we use the quadratic programming characterization of Nash equilibria [15]. Consider a game (A, B) where A, B are m-by-n matrices. The program

$$\begin{aligned} \underset{x\in\Delta^m, y\in\Delta^n, \alpha,\beta\in\mathbb{R}}{\text{maximize}} \quad & x^T(A+B)y - \alpha - \beta \\ \text{subject to} \quad & Ay \leq \alpha\mathbf{1}, \\ & B^T x \leq \beta\mathbf{1}, \end{aligned} \tag{14}$$

has an optimal value of 0, and any (x, y) attaining the value 0 is a Nash equilibrium. In the case of a symmetric quantum race (A, A^T), when we restrict to symmetric strategies (x, x) the objective function in Eq. (14) becomes negative definite plus linear, making this a standard quadratic program. We then use the tight dual formulation of a quadratic program [8] to give an upper bound on the payoff of any symmetric Nash equilibrium, by explicitly constructing solutions to the dual problem. This allows us to show that the payoff of the unique coinciding equilibrium in a stingy race achieves a payoff which is within $O(\sqrt{\ell/K})$ of optimal amongst all symmetric equilibria in the corresponding quantum race.

We now proceed to show these two results.

4.1 Approximate Nash equilibrium

▶ **Definition 29.** A two-player game described by payoff matrices (A, B) is said to have an ϵ-approximate Nash equilibrium (p, q), for $\epsilon \geq 0$, if the following two conditions hold

$$p^{\mathrm{T}}Aq \geq v^{\mathrm{T}}Aq - \epsilon \text{ for all } v \in \Delta_m \tag{15}$$

$$p^{\mathrm{T}}Bq \geq p^{\mathrm{T}}Bu - \epsilon \text{ for all } u \in \Delta_n \quad . \tag{16}$$

▶ **Definition 30.** A two-player game described by payoff matrices (A, B) is said to have an ϵ-well supported Nash equilibrium (p, q), for $\epsilon \geq 0$ if

$$e_i^{\mathrm{T}}Aq \geq e_j^{\mathrm{T}}Aq - \epsilon \text{ for all } i \in \sup(p) \text{ and } j \in [m]$$

$$p^{\mathrm{T}}Be_i \geq p^{\mathrm{T}}Be_j - \epsilon \text{ for all } i \in \sup(q) \text{ and } j \in [n] \quad .$$

Note that an ϵ-well supported Nash equilibrium is also an ϵ-approximate Nash equilibrium, but the reverse does not hold.

▶ **Theorem 31.** *Let $p_1, \ldots, p_K$ be an ℓ-dense sequence defining the symmetric stingy quantum race (A_0, A_0^T) and the symmetric quantum race (A, A^T). Let (x, x) be the unique coinciding Nash equilibrium for the stingy quantum race (A_0, A_0^T) given by Theorem 22. Then (x, x) is a $\frac{7(\sqrt{2}-1)\ell}{K}$-well supported Nash equilibrium in the quantum race (A, A^T).*

Proof. To show that (x, x) is an ϵ-well supported Nash equilibrium in the quantum race (A, A^T) it suffices to show that $e_i^{\mathrm{T}} Ax \geq e_j^{\mathrm{T}} Ax - \epsilon$ for all $T^* \leq i \leq K$ and $j \in [K]$. We omit the details of the proof here and refer the readers to [14]. ◀

4.2 Upper bound on payoff

Let (x, x) be the unique coinciding Nash equilibrium in an ℓ-dense symmetric stingy quantum race (A_0, A_0^{T}). We have just shown that (x, x) is a $\frac{7(\sqrt{2}-1)\ell}{K}$-well supported Nash equilibrium in the corresponding quantum race (A, A^{T}). By Corollary 28, (x, x) achieves payoff at least $\sqrt{2} - 1 - 50\sqrt{2}(\sqrt{2} - 1)^2 \frac{\ell}{K}$ in the game (A, A^{T}). In this section, we show that this payoff is within $O(\sqrt{\ell/K})$ of optimal among all symmetric strategies (y, y) for the game (A, A^{T}).

Our starting point is to use the program in Eq. (14) to provide a means to upper bound the value of any symmetric equilibrium.

▶ **Lemma 32.** *Let (A, A^T) be a symmetric game and define for $c \geq 0$*

$$\begin{aligned} \gamma_A(c) = \underset{x}{\mathit{maximize}} \quad & \frac{1}{2} x^T (A + A^T) x \\ \mathit{subject\ to} \quad & Ax \leq c\mathbf{1}, \\ & \mathbf{1}^{\mathrm{T}} x = 1, x \geq \mathbf{0}. \end{aligned}$$

For all c_0, such that $\gamma_A(c) < c$ for all $c \geq c_0$, the payoff of any symmetric Nash equilibrium in the game (A, A^{T}) is less than c_0.

Proof. We show the contrapositive. Suppose there is a symmetric Nash equilibrium (x, x) with payoff $c \geq c_0$. Then (x, x, c, c) is a feasible solution to the program in Eq. (14) with objective value 0. Thus $Ax \leq c$ and $\frac{1}{2} x^{\mathrm{T}} (A + A^{\mathrm{T}}) x = c$. ◀

This is the approach we take to upper bounding the payoff of symmetric Nash equilibria in a quantum race.

▶ **Theorem 33.** *Let $p_1, \ldots, p_K$ be an ℓ-dense sequence with $K \geq 6\ell$. Then any symmetric Nash equilibrium (x, x) in the two-player quantum race defined by $p_1, \ldots, p_K$ has payoff at most $\sqrt{2} - 1 + 5\sqrt{\frac{\ell}{K}}$.*

Proof. Let (A, A^{T}) be the payoff matrices of a two-player quantum race defined by $p_1, \ldots, p_K$. We will show that $\gamma_A(c) < c$ for all $c > \sqrt{2} - 1 + 5\sqrt{\frac{\ell}{K}}$. By Lemma 32 this proves the theorem.

In the case of a quantum race $A + A^{\mathrm{T}} = p\mathbf{1}^{\mathrm{T}} + \mathbf{1}p^{\mathrm{T}} - pp^{\mathrm{T}}$. This means that over the probability simplex, the quadratic form $x^{\mathrm{T}}(A + A^{\mathrm{T}})x = -x^{\mathrm{T}}(pp^{\mathrm{T}})x + 2p^{\mathrm{T}}x$ is a negative-definite plus linear function. In this case, $\gamma_A(c)$ is in the standard form of a quadratic program and has a dual program with matching value [8].

$$\begin{aligned} \gamma_A(c) = \underset{v \in \mathbb{R}^K, \lambda, d \in \mathbb{R}}{\text{minimize}} \quad & \frac{1}{2}\lambda^2 + c \cdot \mathbf{1}^{\mathrm{T}} v + d \\ \text{subject to} \quad & A^T v \geq (1 - \lambda)p - d\mathbf{1} \quad , \\ & v \geq \mathbf{0}. \end{aligned} \tag{17}$$

Our approach will be to construct a feasible solution to Eq. (17) to demonstrate that $\gamma_A(c) < c$ for all $c > \sqrt{2} - 1 + 5\sqrt{\frac{\ell}{K}}$.

First note that for $c > \frac{1}{2}$ there is a trivial solution where $\lambda = 1, d = 0$ and v is the all-zero vector which shows that $\gamma(c) < c$. We now focus on the case $c \leq \frac{1}{2}$. Let $\sqrt{2} - 1 \leq c \leq \frac{1}{2}$. We will develop a lower bound on c which implies $\gamma_A(c) < c$.

Let S be the smallest index i such that $p_i \geq c$. Note that as A is an ℓ-dense quantum race we have $p_S \leq c + \frac{\ell}{K}$. We let

$$d = (1-\lambda)\left(1 + p_K - \frac{p_K}{p_S}\right)$$

and

$$v(i) = \begin{cases} 0 & \text{if } 1 \leq i < S \\ (1-\lambda-d)\frac{p_S}{\bar{p}_S}\frac{1}{p_i}\left(\frac{1}{p_i} - \frac{1}{p_{i+1}}\right) & \text{if } S \leq i < K \\ (1-\lambda-d)\frac{p_S}{p_K^2 \bar{p}_S} - \frac{(1-\lambda)}{p_K} & \text{if } i = K \ . \end{cases}$$

The choice of v comes from solving the system of linear equations $(A_0^{\mathrm{T}} v)_i = (1-\lambda)p_i - d$ for $S \leq i \leq K$. The parameter λ will be chosen later.

Let us see that v satisfies the constraints of Eq. (17). Note that $1 - \lambda - d = (1-\lambda)p_K \frac{\bar{p}_S}{p_S}$. Thus $v(K) = 0$ and $v \geq 0$ so long as $\lambda \leq 1$.

As mentioned, by construction v satisfies $(A_0^T v)_i = (1-\lambda)p_i - d$ for $S \leq i \leq K$. Thus as $A = A_0 + \frac{1}{2}\mathrm{diag}(p)^2$ and $v \geq 0$ we also have $(A^T v)_i \geq (1-\lambda)p_i - d$ for $S \leq i \leq K$.

For $i < S$ we have that

$$(A^T v)_i \geq (A_0^T v)_i = \bar{p}_i p^T v \geq \bar{p}_S p^T v = (1-\lambda)p_S - d \geq (1-\lambda)p_i - d \ .$$

Thus the constraint $A_0^T v \geq (1-\lambda)p - d\mathbf{1}$ is satisfied. We have shown that v is a feasible solution for any choice of $\lambda \leq 1$. We now choose λ to minimize the objective value. Substituting our choices of v, d into the objective value we have

$$\begin{aligned}\gamma_A(c) &\leq \frac{1}{2}\lambda^2 + (1-\lambda)\left(1 + p_K - \frac{p_K}{p_S}\right) + c(1-\lambda)p_K \sum_{i=S}^{K-1} \frac{1}{p_i}\left(\frac{1}{p_i} - \frac{1}{p_{i+1}}\right) \\ &= \frac{1}{2}\lambda^2 + (1-\lambda)\left(1 + p_K\left(-\frac{\bar{p}_S}{p_S} + c \cdot \sum_{i=S}^{K-1} \frac{1}{p_i}\left(\frac{1}{p_i} - \frac{1}{p_{i+1}}\right)\right)\right)\end{aligned}$$

Define

$$\beta(c) = 1 + p_K\left(-\frac{\bar{p}_S}{p_S} + c \cdot \sum_{i=S}^{K-1} \frac{1}{p_i}\left(\frac{1}{p_i} - \frac{1}{p_{i+1}}\right)\right) \ .$$

The objective value $\frac{1}{2}\lambda^2 + (1-\lambda)\beta(c)$ is minimized over λ by taking $\lambda = \beta(c)$. This makes the objective value $\beta(c) - \beta(c)^2/2$. We have now reduced the problem to showing $\beta(c) - \beta(c)^2/2 - c < 0$. The roots of the corresponding quadratic equation are $1 \pm \sqrt{1-2c}$. Note that $c \leq 1/2$, thus the square root term will be real. Thus we will simultaneously have $\beta(c) \leq 1$ and $\beta(c) - \beta(c)^2/2 < c$ when $\beta(c) < 1 - \sqrt{1-2c}$. In Lemma 34, we show that $\beta(c) < 1 - \sqrt{1-2c}$ when $\sqrt{2} - 1 + 5\sqrt{\frac{\ell}{K}} \leq c \leq \frac{1}{2}$. This will conclude the proof. ◀

▶ **Lemma 34.** *$\beta(c) < 1 - \sqrt{1-2c}$ for any $\sqrt{2} - 1 + 5\sqrt{\frac{\ell}{K}} \leq c \leq \frac{1}{2}$.*

Proof. Refer [14]. ◀

5 Multiplayer quantum races

5.1 Basic properties

For an integer $n \geq 2$, an *n-player game* is specified by a set of *pure strategies* S_i, and *payoff* functions $u_i : S \to \mathbb{R}$, for each player $i \in [n]$, where by definition $S = S_1 \times \cdots \times S_n$ is the set of *pure strategy profiles.* For $s \in S$, the value $u_i(s)$ is the payoff of player i for pure strategy profile s. Let $S_{-i} = S_1 \times \cdots \times S_{i-1} \times S_{i+1} \times \cdots \times S_n$ be the set of all pure strategy profiles of players other than i. For $s \in S$ and $i \in [n]$, we set the *partial* pure strategy profile $s_{-i} \in S_{-i}$ to be $(s_1, \dots s_{i-1}, s_{i+1}, \dots, s_n)$. For s' in S_{-i}, and $s_i \in S_i$, we denote by (s', s_i) the *combined* pure strategy profile $(s'_1, \dots, s'_{i-1}, s_i, s'_{i+1}, \dots, s'_n) \in S$. We will suppose that each player has m pure strategies and that $S_i = \{e_1, \dots, e_m\}$, the canonical basis of the vector space $\mathbb{R}^m$, for all $i \in [n]$, and therefore $S = \{e_1, \dots, e_m\}^n$. For simplicity, instead of e_j we often say strategy j.

A *mixed strategy* for player i is a probability distribution over S_i that we identify with a vector $x_i = (x_i^1, \dots x_i^m)$ such that $x_i^j \geq 0$, for all $j \in [m]$, and $\sum_{j\in[m]} x_i^j = 1$. We denote by Δ_i the set of mixed strategies for i, and we call $\Delta = \Delta_1 \times \cdots \times \Delta_r$ the set of *mixed strategy profiles.* For a mixed strategy profile $x = (x_1, \dots, x_n)$ and pure strategy profile $s \in S$, the product $x^s = x_1^{s_1} x_2^{s_2} \cdots x_n^{s_n}$ is the probability of s in x. We will consider the multilinear extension of the payoff functions from S to Δ defined by $u_i(x) = \sum_{s\in S} x^s u_i(s)$. The set Δ_{-i}, the partial mixed strategy profile x_{-i}, for $x \in \Delta$ and $i \in [n]$, and the combined mixed strategy profile (x', x_i) for $x' \in \Delta_{-i}$ and $x_i \in \Delta_i$ are defined analogously to the pure case.

The pure strategy s_i is a *best response* for player i against the partial mixed strategy profile $x' \in \Delta_{-i}$ if it maximizes $u_i(x', \cdot)$. For $x \in \Delta$ and $i \in [n]$, we will denote by $\mathrm{br}(x_{-i})$ the set of best responses of player i against x_{-i}. A *Nash equilibrium* is a mixed strategy profile $x = (x_1, \dots, x_n)$ such that $\sup(x_i) \subseteq \mathrm{br}(x_{-i})$, for all $i \in [n]$.

▶ **Definition 35** (n-party stingy quantum race)**.** Let $n \geq 2$ be a positive integer. An *n-party stingy quantum race* is defined by a sequence of increasing probabilities $0 < P_1 < P_2 < \ldots < P_K \leq 1$, for some positive integer K. The set of pure strategies of all players is $[K]$. For every i, the utility function of the i^{th} player is defined as

$$u_i(s_1, \dots, s_n) = P_{s_i} \prod_{k\neq i, s_k \leq s_i} \bar{P}_{s_k}.$$

Consider an n-party stingy quantum race given by the probabilities $0 < P_1 < \ldots < P_K \leq 1$, and let $x_{-i} \in \Delta_{-i}$ for some $i \in [n]$. If player i plays the pure strategy s against x_{-i}, her payoff is

$$u_i(x_{-i}, s) = P_s \prod_{k\neq i} \left(\sum_{s_k \in \sup_{\leq s}(x_k)} x_k^{s_k} \bar{P}_{s_k} + \sum_{s_k \in \sup_{>s}(x_k)} x_k^{s_k} \right). \qquad (18)$$

The following is the multiparty analog of Claim 14.

▶ **Claim 36.** *Let $x = (x_1, \dots x_n)$ be a Nash equilibrium of an n-party stingy quantum race defined by probabilities $P_1 < \ldots < P_K$. If $s_1 \in \sup(x_i)$, for some $i \in [n]$, then for all $s_2 > s_1$ there exists $k \neq i$ such that $\sup_{\leq s_1}(x_k) \neq \sup_{\leq s_2}(x_k)$.*

Proof. If $\sup_{\leq s_1}(x_k) = \sup_{\leq s_2}(x_k)$, for all $k \neq i$ then

$$u_i(x_{-i}, s_2) = \frac{P_{s_2}}{P_{s_1}} u_i(x_{-i}, s_1).$$

As $p_{s_1} < p_{s_2}$, the payoff for playing s_2 is strictly larger than that for playing s_1. Therefore s_1 is not a best response for x_{-i}, in contradiction with the definition of a Nash equilibrium. ◀

This claim implies the following properties for the supports of Nash equilibria in a multiplayer stingy quantum race.

▶ **Corollary 37.** *Let x be a Nash equilibrium of an n-party stingy quantum race defined by probabilities $0 < P_1 < P_2 < \ldots < P_K \leq 1$. Then we have:*

- *$\bigcup_{i=1}^{n} \sup(x_i)$ is an interval containing K,*
- *for every $i \in [n]$, for every $s_1, s_2 \in \sup(x_i)$ there exists $s \in \bigcup_{k \neq i} \sup(x_k)$ with $s_1 < s \leq s_2$.*

Let x be a Nash equilibrium of an n-party stingy quantum race. We say that x is *coinciding* if $\sup(x_i) = \sup(x_k)$, for all $i, k \in [n]$. We call this common support in a coinciding Nash equilibrium the *support* of the equilibrium. In the multiparty case we will only study coinciding Nash equilibria.

5.2 Coinciding Nash equilibria of stingy multiplayer races

By Corollary 37 we know that in a coinciding Nash equilibrium of an n-party stingy quantum race the support of the equilibrium is of the form $\{T, T+1, \ldots, K\}$, for some $1 \leq T \leq K$. We would like to characterize these coinciding equilibria.

▶ **Lemma 38.** *Let $x = (x_1, \ldots, x_n)$, where x_i is a K-dimensional real vector for every $i \in [n]$, and let $1 \leq T \leq K$. Then x is a Nash equilibrium of support $\{T, T+1, \ldots, K\}$ in an n-party stingy quantum race defined by $0 < P_1 < \ldots < P_K \leq 1$ if and only x satisfies the following system, for all $i \in [n]$:*

$$u_i(x_{-i}, t) = u_i(x_{-i}, T) \qquad \text{for } \; T < t \leq K \; , \tag{19}$$

$$u_i(x_{-i}, T-1) \leq u_i(x_{-i}, T) \; , \tag{20}$$

$$x_i^t = 0 \qquad \text{for } \; 0 < t < T \; , \tag{21}$$

$$x_i^t > 0 \qquad \text{for } \; T \leq t \leq K \; , \tag{22}$$

$$\sum_{t=T}^{K} x_i^t = 1 \; . \tag{23}$$

Proof. For every $i \in [n]$, Eq. (21)–(23) express that x_i is a probability distribution of support $\{T, T+1, \ldots, K\}$. For $T \geq 2$, when playing a strategy $t < T$ against the partial mixed strategy profile x_{-i}, the ith player's payoff is maximized if she plays $T-1$. Therefore Eq. (19) and (20) express that the strategies in her support are all best responses against x_{-i}. ◀

▶ **Definition 39.** For an n-party stingy quantum race defined by $0 < P_1 < \ldots < P_K \leq 1$ we define its *reduced game* as the 2-party stingy quantum race defined by the two sequences of probabilities $p_1 < \ldots < p_K$, and $P_1 < \ldots < P_K$ where $p_j = P_j^{1/(n-1)}$, for $1 \leq j \leq K$.

We denote by A the payoff matrix of the first player in the reduced game

▶ **Lemma 40.** *Let an n-party stingy quantum race be defined by $0 < P_1 < \ldots < P_K \leq 1$, let $x = (x_1, \ldots, x_n)$, where x_i is a K-dimensional vector, and let $1 \leq T \leq K$. Then Eq. (19)–(23) are satisfied by x, for every $i \in [n]$ if and only if Eq. (2)–(6) for the reduced game are satisfied by x_i, for every $i \in [n]$.*

Proof. Refer [14]. ◀

The following theorem characterizes the coinciding Nash equilibria in an n-party stingy quantum race.

▶ **Theorem 41.** *An n-party stingy quantum race always has a unique coinciding Nash equilibrium $x = (x_1, \ldots, x_n)$, where $x_1 = \cdots = x_n$. If the game is defined by the probabilities $0 < P_1 < P_2 < \cdots < P_K$ then the coinciding equilibrium has support $\{T^*, T^* + 1, \ldots, K\}$, where $T^* = T^*_B$ of the reduced game, and for all $i \in [n]$, the distribution x_i is defined on its support as*

$$x_i^t = \begin{cases} r^B_{T^*}/z^B_{T^*} & \textit{if} \quad t = T^*, \\ q^B_t/z^B_{T^*} & \textit{if} \quad T^* < t \le K. \end{cases}$$

Proof. Combining Lemma 38 and Lemma 40, we get that x is a coinciding Nash equilibrium of support $\{T, T + 1, \ldots, K\}$ if and only if x_i satisfies Eq. (2)–(6) for the reduced game, for all $i \in [n]$. By Theorem 21 this happens if and only if $T = T^*_B$ of the reduced game, and the unique solution for x_i, for $i \in [n]$, is the one stated by the Theorem. ◀

5.3 Collision probability of the stingy coinciding equilibrium

Our main objective in this section is to upper bound the collision probability – the probability that two or more players succeed at the same time – in the coinciding equilibrium found in the last section for an ℓ-dense stingy n-player quantum race. To help with this, we make the following definition.

▶ **Definition 42.** For a joint probability distribution $y = (y_1, \ldots, y_n) \in \Delta$, let $\mathrm{cp}^m_i(y)$ denote the probability that player i succeeds first and that exactly m players (including i) succeed at the same time under the joint strategy y. Let $\mathrm{cp}_i(y) = \sum_{m=2}^n \mathrm{cp}^m_i(y)$ denote the probability that player i succeeds first and at least one other player succeeds at the same time.

Let us also set up notation to describe the coinciding equilibrium in a stingy multiplayer race. Define the following quantities

$$q_i = \frac{1}{P_i}\left(\frac{1}{P_{i-1}^{1/(n-1)}} - \frac{1}{P_i^{1/(n-1)}}\right), r_T = \frac{1}{\bar{P}_T}\left(\frac{1}{P_K^{1/(n-1)}} - \sum_{i=T+1}^{K} \bar{P}_i q_i\right), z_T = r_T + \sum_{i=T+1}^{K} q_i \ .$$

Let T^* be the starting point of the support of the coinciding equilibrium. Then by Theorem 41, the strategy of player i in the coinciding equilibrium is given by

$$x_i^t = \begin{cases} r_{T^*}/z_{T^*} & \text{if} \quad t = T^*, \\ q_t/z_{T^*} & \text{if} \quad T^* < t \le K, \\ 0 & \text{if} \quad t < T^* \ . \end{cases} \tag{24}$$

To obtain concrete bounds on the collision probability, we will need bounds on z_{T^*} and P_{T^*-1}.

▶ **Lemma 43.** *In any stingy multiplayer quantum race with n players $(1/z_{T^*})^{n-1} < 1/n$.*

Proof. Refer [14]. ◀

▶ **Theorem 44.** *Let $P_1, \ldots, P_K$ define a stingy n-player quantum race with $n \ge 2$. Then $P_{T^*-1} < \frac{1}{n}$. If in addition $P_1, \ldots., P_K$ form an ℓ-dense sequence and $4\mathrm{e}\ell n \le K$ then $P_{T^*-1} \ge \frac{1}{2\mathrm{e}n}$, where e is Euler's number.*

Proof. Refer [14]. ◀

The next lemma bounds the collision probability for player i when all players but player i play according to the coinciding equilibrium, and player i plays an arbitrary strategy v. We will use this lemma to bound the total collision probability and also in Section 5.4 to show that the stingy coinciding equilibrium is an approximate equilibrium in a multiparty race.

▶ **Lemma 45.** *Let $P_1, ..., P_K$ define an ℓ-dense stingy n-player quantum race, $n \geq 2$, with $4en\ell \leq K$, and let x be the unique coinciding equilibrium given by Eq.* (24)*. Then $\mathrm{cp}_i(x_{-i}, v) \leq \frac{8e\ell}{K}$ for any $i \in [n]$ and $v \in \Delta_i$.*

Proof. Refer [14]. ◀

▶ **Theorem 8.** *Let $P_1, ..., P_K$ define an ℓ-dense stingy n-player quantum race such that $4en\ell \leq K$. When the players play the coinciding equilibrium of the stingy race, the probability that two or more players succeed at the same time is at most $\frac{8en\ell}{K}$.*

Proof. By Lemma 45, the probability that two or more players succeed at the same time is at most

$$\sum_{i=1}^{n} \mathrm{cp}_i(x) \leq \frac{8en\ell}{K} \quad .$$ ◀

5.4 Multiplayer quantum races

In this section we use our results about the stingy multiplayer quantum race to analyse the multiplayer quantum race. Namely, we show that the coinciding equilibrium in a stingy multiplayer quantum race is an approximate equilibrium in a multiplayer race. The difference between a stingy multiplayer race and a multiplayer race is that in a multiplayer race, the payoff is equally divided amongst all players who succeed first at the same time.

▶ **Definition 46** (Multiplayer quantum race)**.** Let u_i be the payoff function for player $i \in [n]$ in the n-player stingy race defined by $P_1 < \cdots < P_k$, as given by Eq. (18). The payoff function u_i' in the n-player quantum race defined by $P_1, \ldots, P_k$ is

$$u_i'(x) = u_i(x) + \sum_{m=2}^{n} \frac{\mathrm{cp}_i^m(x)}{m} \quad .$$

While the tie-splitting payoff in Definition 46 is quite natural, one could imagine other definitions in-between stingy multiplayer races and the definition of multiplayer races we have given. Our results in this section depend very weakly on the exact definition of how ties are split in a multiplayer race. In fact, the only property we use is $u_i'(x) \leq u_i(x) + \mathrm{cp}_i(x)$. This property holds under any reasonable definition of tie-splitting.

Now we show Theorem 9 from the introduction that the coinciding Nash equilibrium in a multiplayer stingy quantum race is an approximate Nash equilibrium in a multiplayer quantum race.

▶ **Theorem 9.** *Let $P_1, ..., P_K$ define an ℓ-dense stingy n-player quantum race, $n \geq 2$, with $4en\ell \leq K$. If $x = (x_1, ..., x_n)$ is the coinciding Nash equilibrium for this stingy race, then x is an $\frac{8e\ell}{K}$- approximate Nash equilibrium of the corresponding quantum race.*

Proof. Refer [14]. ◀

References

1 Divesh Aggarwal, Gavin Brennen, Troy Lee, Miklos Santha, and Marco Tomamichel. Quantum attacks on Bitcoin and how to prevent against them. Technical report, arXiv, 2017. arXiv:1710.10377.

2 Adam Back. Hashcash – a denial of service counter-measure, 2002. Available at: http://www.hashcash.org/papers/hashcash.pdf.

3 Alex Biryukov and Dmitry Khovratovich. Equihash: Asymmetric proof-of-work based on the generalized birthday problem. *Ledger*, 2:1–30, 2017.

4 Bitmain. Bitmain Antminer S9. https://shop.bitmain.com/antminer_s9_asic_bitcoin_miner.html, 2018. Accessed 2018-02-16.

5 Vitalik Buterin. Bitcoin is not quantum safe, and how we can fix it when needed. https://bitcoinmagazine.com/articles/bitcoin-is-not-quantum-safe-and-how-we-can-fix-1375242150/, 2013.

6 Miguel Castro and Barbara Liskov. Practical Byzantine Fault Tolerance. In *Third Symposium on Operating Systems Design and Implementation*, 1999.

7 Catalin Dohotaru and Peter Høyer. Exact quantum lower bound for Grover's problem. Technical report, arXiv, 2008. arXiv:0810.3647.

8 William S. Dorn. Duality in quadratic programming. *Quarterly of applied mathematics*, 18(2):155–162, 1960.

9 Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *18th International Conference on Financial Cryptography and Data Security*, 2014.

10 Arthur Gervais, Ghassan Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Compute and Communications Security (CCS'16)*, pages 3–16, 2016.

11 Lov K. Grover. A Fast Quantum Mechanical Algorithm for Database Search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, New York, NY, USA, 1996. ACM. doi:10.1145/237814.237866.

12 Nicole Immorlica, Adam Tauman Kalai, Brendan Lucier, Ankur Moitra, Andrew Postlewaite, and Moshe Tennenholtz. Dueling algorithms. In *Proceedings of the forty-third annual ACM symposium on theory of computing (STOC'11)*, pages 215–224, 2011.

13 Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *CRYPTO*, pages 357–388, 2017.

14 T. Lee, M. Ray, and M. Santha. Strategies for quantum races. *ArXiv e-prints*, September 2018. arXiv:1809.03671.

15 Olvi L. Mangasarian and H. Stone. Two-person nonzero-sum games and quadratic programming. *Journal of mathematical analysis and applications*, 9:348–355, 1964.

16 Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009. Available at: http://www.bitcoin.org/pdf.

17 John F. Nash. Non-cooperative Games. *Annals of Mathematics*, 54(2):286–295, 1951.

18 Or Sattath. On the insecurity of quantum Bitcoin mining. Technical report, arXiv, 2018. Appeared in QCRYPT 2018. arXiv:1804.08118.