Cloning Games, Black Holes and Cryptography

Alexander Poremba* MIT
Seyoon Ragavan† MIT
Vinod Vaikuntanathan‡ MIT

Abstract

Quantum no-cloning (Wootters and Zurek, *Nature*, 1982) is one of the most fundamental properties of quantum information. In this work, we introduce a new toolkit for analyzing *cloning games*; these games capture more quantitative versions of no-cloning and are central to unclonable cryptography. Previous works rely on the framework laid out by Tomamichel, Fehr, Kaniewski and Wehner (*New Journal of Physics*, 2013) to analyze both the n-qubit BB84 game and the subspace coset game. Their constructions and analysis face the following inherent limitations:

1. The existing bounds on the values of these games are at least $2^{-0.25n}$; on the other hand, the trivial adversarial strategy wins with probability 2^{-n}. Not only that, the BB84 game does in fact admit a highly nontrivial winning strategy. This raises the natural question: *are there cloning games which admit no non-trivial winning strategies*?
2. The existing constructions are not multi-copy secure; the BB84 game is not even $2 \mapsto 3$ secure, and the subspace coset game is not $t \mapsto t+1$ secure for a polynomially large t. Moreover, we provide evidence that the existing technical tools do not suffice to prove multi-copy security of even completely different constructions. This raises the natural question: *can we design new cloning games that achieve multi-copy security, possibly by developing a new analytic toolkit*?

Inspired by the literature on pseudorandom states, we study a new cloning game based on *binary phase states* and show that it is t-copy secure when $t = o(n/\log n)$. Moreover, for constant t, we obtain the *first* asymptotically optimal bounds of $O(2^{-n})$. To accomplish this, we introduce a new analytic toolkit based on of *binary subtypes* and combine this with novel bounds on the operator norms of block-wise tensor products of matrices. We also show a *worst-case to average-case reduction* for a large class of cloning games, which allows us to show the same quantitative results for *Haar cloning games*. These technical ingredients together enable two new applications which have previously been out of reach:

- In the area of black-hole physics, our cloning games reveal that, in an idealized model of a black hole which features Haar random (or *pseudorandom*) scrambling dynamics, the information from infalling qubits can only be recovered from either the interior or the exterior of the black hole—but never from both places at the same time. To demonstrate this result, it turns out to be crucial to prove an asymptotically optimal bound and to overcome the first limitation above.
- In the area of quantum cryptography, our worst-case to average-case reduction helps us construct succinct unclonable encryption schemes from the existence of *pseudorandom unitaries*, thereby, for the first time, bridging the gap between "MicroCrypt" and unclonable cryptography. We also propose and provide evidence for the security of multi-copy unclonable encryption schemes, which requires us to overcome the second limitation above.

*poremba@mit.edu
†sragavan@mit.edu
‡vinodv@mit.edu

Contents

1 Introduction **1**
- 1.1 Our Contributions . . . 2
- 1.2 Technical Overview . . . 5
  - 1.2.1 Previous Techniques and Their Limitations . . . 6
  - 1.2.2 Section 7: Haar Cloning Games and Worst-Case to Average-Case Reductions . . . 10
  - 1.2.3 Sections 4 and 5: Construction and Analysis from Binary Phase States . . . 11
- 1.3 Application I: Black Hole Cloning Games . . . 14
- 1.4 Application II: Unclonable Cryptography . . . 19
- 1.5 Open Questions . . . 23

2 Preliminaries **24**
- 2.1 Quantum Computation . . . 24
- 2.2 Unitary Designs . . . 26
- 2.3 Pseudorandom Unitaries . . . 27
- 2.4 Operator Norm Bounds . . . 27
  - 2.4.1 Blockwise Tensor Products . . . 29
  - 2.4.2 Consequences . . . 33

3 Monogamy of Entanglement and Oracular Cloning Games **35**
- 3.1 Monogamy of Entanglement Games . . . 35
- 3.2 Oracular Cloning Games . . . 37

4 Types and Subtypes **40**
- 4.1 Binary Types . . . 40
- 4.2 Phase Twirling . . . 41
- 4.3 Binary Subtypes . . . 42
  - 4.3.1 Definitions and Combinatorial Properties . . . 42
  - 4.3.2 Relating Subtype Projectors to Type Projectors . . . 43

5 Cloning Game Construction from Binary Phase States **45**
- 5.1 Setup and Notation . . . 45
- 5.2 Expanding out Ξ using Subtypes . . . 47
- 5.3 Bounding $\|\mathbf{B}_{\boldsymbol{\mu}}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{t+1})\|_\infty$ . . . 49
- 5.4 Combinatorial Lemmas about Free Variable Symbols . . . 53
- 5.5 Putting Everything Together . . . 54

6 Limitations of Analyzing Monogamy Games Using Existing Techniques **55**
- 6.1 Limitations of Bounding the Operator Norm Directly . . . 56
- 6.2 Limitations of Bounding Pairwise Overlaps . . . 57
- 6.3 Monogamy Bounds from Binary Phase States . . . 58

7 Worst-Case to Average-Case Reduction **62**
- 7.1 Preliminary: Mixed Unitary Designs . . . 62
- 7.2 Proof of the Reduction . . . 65

8 Black Hole Cloning Games **66**
8.1 Definition 66
8.2 Bounds On the Value of a Black Hole Cloning Game 68

9 Search-Secure Unclonable Encryption **73**
9.1 Definitions 73
9.2 Constructions 75

A Relating Cloning Games to Monogamy-Like Games **83**

1 Introduction

Quantum no-cloning [WZ82] is one of the most fundamental properties of quantum information. Roughly speaking, it states that no quantum procedure can create an exact copy of an arbitrary unknown quantum state. The principle of no-cloning has profound implications in quantum information processing [BB84, BBC+93, Ron19, CBTW17] and has even inspired entirely new cryptographic primitives, starting with Wiesner's remarkable quantum money scheme [Wie83] and many subsequent primitives which are collectively known as *unclonable cryptography* [Sat22]; these include unclonable quantum encryption [BL20, AKL23, KT23, AKY24], encryption with unclonable decryption keys [GZ20, APV23], quantum copy-protection [AKL+22, CMP22, CLLZ21], unclonable commitments and proofs [GMR23], and many more.

Because the standard no-cloning theorem [WZ82] merely precludes the possibility of creating *exact* copies, several lines of work have since explored other quantitative variants of no-cloning which are far less restrictive; for example, Bužek and Hillery [BH96] initiated the study of *approximate* no-cloning, whereas Molina, Vidick and Watrous [MVW13] studied the limitations of counterfeiting attacks against Wiesner's quantum money. In the context of money, the latter offers a much more meaningful notion of no-cloning as as it not only prohibits the act of copying a banknote, but also the possibility of *forging* possibly different quantum states that merely pass verification by the bank. Following a long-standing tradition of studying quantum mechanical phenomena through the lens of interactive games [Mer90, Ara02, Har93, GHZ89, RUV12, TFKW13, JNV+21, KLVY23], the field of unclonable cryptography [Sat22] today relies on abstract games as a means of capturing no-cloning; as in the case of quantum money, these games enable much stronger notions of no-cloning which not only capture the difficulty of *copying* the states themselves, but merely copying *properties* of quantum states, such as a choice of basis which is used to generate the state.

Cloning Games. The class of interactive games which are relevant for unclonable cryptography are known as *cloning games* [AKL23]. These types of games first emerged in the context of unclonable encryption schemes [BL20] but the general framework[1] also applies many other fundamental unclonable primitives, such as copy-protection, single-decryptor encryption, quantum money, and more [AKL23].

A basic $1 \mapsto 2$ cloning game $\mathsf{G}_{1\mapsto 2}$ with respect to the question set Θ, answer set $\mathcal{X}$, and ensemble of unitaries $\{U_\theta\}_{\theta\in\Theta}$ of dimension $|\mathcal{X}|$ is the following interactive game played by a trusted challenger, say Alice, as well as an adversary consisting of a cloner Φ and two additional players, say Bob and Charlie.

1. (**Setup phase**) Alice samples random $x \sim \mathcal{X}$ and $\theta \sim \Theta$, and sends $U_\theta |x\rangle_{\mathsf{A}}$ to the cloner Φ.

   The cloner Φ splits the state into two registers B and C, which he then forwards to Bob and Charlie, respectively. Afterwards, the players may no longer communicate for the rest of the game.

2. (**Question phase**) Bob and Charlie both receive the string θ.

3. (**Answer phase**) Bob and Charlie independently output a guess for the element x.

4. (**Outcome phase**) Bob and Charlie win if they both guess x correctly.

We illustrate the cloning game $\mathsf{G}_{1\mapsto 2}$ in Figure 1. A strategy S for the game $\mathsf{G}_{1\mapsto 2}$ consists of a cloning map Φ and a pair of positive operator-valued measurements $\mathcal{B} = \{\mathbf{B}_x^\theta\}_{\theta\in\Theta,x\in\mathcal{X}}$ and $\mathcal{C} = \{\mathbf{C}_x^\theta\}_{\theta\in\Theta,x\in\mathcal{X}}$. The *value* of a particular strategy S for the cloning game $\mathsf{G}_{1\mapsto 2}$ is defined as the average winning probability

$$\omega_{\mathsf{S}}(\mathsf{G}_{1\mapsto 2}) = \mathop{\mathbb{E}}_{\theta\sim\Theta}\mathop{\mathbb{E}}_{x\sim\mathcal{X}} \mathrm{Tr}\left[\left(\mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta\right)\Phi_{\mathsf{A}\to\mathsf{BC}}(U_\theta |x\rangle\langle x|_{\mathsf{A}} U_\theta^\dagger)\right].$$

[1] We note that our notion of a basic cloning game is slightly more specific than the general framework studied in [AKL23]; we discuss these differences in more detail in Remark 7.

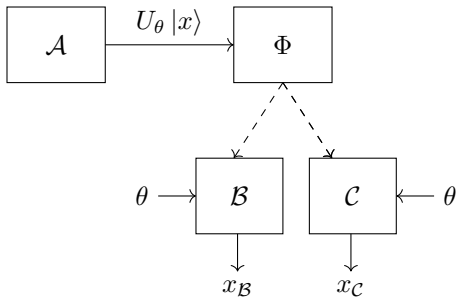

Figure 1: A basic $1 \mapsto 2$ cloning game.

Here, we use $\omega(\mathsf{G}_{1\mapsto 2})$ to denote the optimal winning probability over all joint strategies which are specified by Φ, $\mathcal{B}$ and $\mathcal{C}$. Note that there always exists a trivial strategy that succeeds with probability $1/|\mathcal{X}|$: the cloner Φ simply forwards the state $U_\theta |x\rangle$ to Bob, who can easily recover x once θ becomes available, whereas Charlie simply guesses a random element in $\mathcal{X}$.

We emphasize that an upper bound on the success probability of a cloning game implies something stronger than the conventional no-cloning theorem [WZ82] or even its approximate variant [BH96]: if the cloner Φ can copy the state $U_\theta |x\rangle$, then Φ can certainly also send the two copies to Bob and Charlie and ensure that they win the game. However, there may be other strategies which do not involve direct cloning but may nevertheless provide the players with enough information to win the game. In fact, the only property of the state that Φ needs to clone is its measurement statistics with respect to the bases specified by Θ (or more weakly, just x itself). As it turns out, this basic notion of unclonability is already sufficient for most applications in unclonable cryptography [Sat22].

To this day, the majority of unclonable cryptography is rooted in either n-qubit BB84 states with $U_\theta = \mathsf{H}^\theta$ [TFKW13, BL20] or subspace coset states over $\mathbb{F}_2^n$, where U_θ encodes a shift of a random $n/2$-dimensional subspace $A \subset \mathbb{F}_2^n$ [CLLZ21, CV22, SS25]. In both cases, the optimal winning probability for the corresponding cloning game decays exponentially in the number of qubits [BL20, CV22, SS25].

1.1 Our Contributions

Despite extensive study and multiple successful applications in unclonable cryptography, several important gaps in our understanding of cloning games remain. Our contributions to this effect are several fold:

1. We show that existing techniques for analyzing cloning games are severely limited; in particular, they prevent us from making progress on many fundamental open questions in the field. We formally expose these limitations with counterexamples and concrete, quantitative proofs.

2. We study several new cloning games and develop a whole suite of techniques for analyzing them; crucially, these techniques allow us to circumvent some of the limitations of previous approaches.

3. Finally, we present two applications of our results which have previously been out of reach; one in the area of *black hole physics* and one in the field of *unclonable cryptography*. Both of these applications provably require us to overcome several technical barriers which are inherent in prior work.

We now discuss each of these contributions in some more detail.

Exposing Limitations on Cloning Games. Our first contribution is to expose several important gaps in our understanding of cloning games; more importantly, we also show that existing techniques for analyzing cloning games appear fundamentally insufficient at addressing them. We list some of these gaps below:

1. **Optimal games:** Prior work on cloning games over $\mathcal{X} = \{0,1\}^n$ has shown the upper bounds of $\cos^2\left(\frac{\pi}{8}\right)^n$ and $2^{-n/4}$ in the case of BB84 states [TFKW13] and subspace coset states [CV22, SS25], respectively. In contrast, a trivial strategy always succeeds with probability 2^{-n}, and this holds for any cloning game. Are there *especially hard* cloning games which admit no non-trivial strategies and have asymptotically optimal bounds of the form $O(2^{-n})$? Closing this gap has important consequences for certain applications of cloning games which we discuss in Section 1.3.

   Not only are all known cloning games far from optimal, we prove that existing techniques can at best only produce upper bounds of the form $2^{-n/2}$. We discuss this in detail in Section 1.2.1.

2. **Multi-copy games:** Quantum states become *learnable* once many identical copies are available, as the literature on quantum tomography [BCG13] suggests. Does cloning also become significantly easier in the presence of multiple copies? Can we extend $1 \mapsto 2$ cloning games towards $t \mapsto t+1$ cloning games, where the cloner Φ receives t identical copies of the initial state, i.e., $(U_\theta |x\rangle)^{\otimes t}$, and there are $t+1$ players $\mathcal{P}_1, \ldots, \mathcal{P}_{t+1}$ who simultaneously seek to recover x? This was posed as an open question in [MPSY24, AMP24], where the latter initiated the study of multi-copy security in the context of revocable cryptography. Not only is prior work limited to $1 \mapsto 2$ cloning games, all existing unclonable cryptography becomes completely insecure if t is allowed to grow polynomially.

   We discuss these limitations in Section 1.2.1. Moreover, we also provide strong evidence that existing techniques seem fundamentally insufficient for analyzing multi-copy games more generally.

3. **Unclonable cryptography in MicroCrypt:** A number of recent works [Kre21, AQY22, AGQY22, BCQ23] showed how to build quantum cryptography from *pseudorandom states and unitaries*, which exist in "MicroCrypt" and are potentially even weaker than one-way functions [Kre21]. To this day, however, the worlds of unclonable cryptography and MicroCrypt have been completely disconnected, as was recently observed in [MPSY24, AMP24]. Do pseudorandom unitaries, which have so far eluded major cryptographic application, give rise to interesting unclonable cryptography?

   The analysis of *Haar cloning games*, where U_θ is a *Haar* unitary (or, a unitary sampled from a unitary design), seems far beyond the scope of existing techniques, as we explain in Sections 1.2.1 and 1.2.2.

4. **Applications beyond cryptography:** While cloning games appear quite fundamental, their use case has so far been limited to cryptography. Can cloning games offer new insights in other scenarios where no-cloning and monogamy of entanglement play an important role, such as in black hole physics? Recent works studied idealized models of black holes which rely on Haar random or pseudorandom unitary dynamics [HP07, KP23, EFL+24], which raises the question: can cloning games with Haar random unitaries help us understand how information gets scrambled inside of a black hole?

   An application to black hole physics once again seems to require new insights into *Haar cloning games* which, as mentioned before, are currently out of reach. We refer to Sections 1.2.1 and 1.2.2.

Given these inherent limitations on cloning games, it seems that fundamentally new techniques are needed in order to advance the field. This is where our next contribution comes in.

A New Suite of Techniques for Analyzing Cloning Games. Our approach towards overcoming both limitations 1 and 2 is to focus on entirely new cloning games altogether. Inspired by the recent literature on pseudorandom quantum states [JLS18, BS19, Col23], we study a cloning game based on *binary phase states*. The pseudorandomness property of these states makes them excellent candidates for multi-copy unclonability [Wer98], in the sense of a traditional no-cloning theorem. In order to extend this to a stronger cloning game bound, we take the existing formalism of binary types [AGQY22] and extend it to a new notion of binary *subtypes*, proving new standalone spectral bounds along the way. For technical reasons, our results only apply to a restricted model: rather than receiving the string θ in the clear, each player receives a oracle access and is allowed to make a query to either U_θ or $U_\theta^\dagger$. While this constitutes a weaker model, it already implies something much stronger than a conventional $t \mapsto t+1$ no-cloning bound.[2]

Ultimately, we prove the following theorem (see Section 1.2.3 for more details):

Theorem 1.1 (Informal, see Theorem 5.15 for a formal statement)**.** *Let $n, t \in \mathbb{N}$. Then, the one-query $t \mapsto t+1$ binary phase cloning game $\mathsf{G}_{t\mapsto t+1}$ over $\mathcal{X} = \{0,1\}^n$, where each of the players is allowed to make one oracle query, has a value of $\omega(\mathsf{G}_{t\mapsto t+1}) \leq \exp(O(t\log t)) \cdot 2^{-n}$.*

For constant t, this is asymptotically optimal and thus overcomes limitation 1. For $t = o(n/\log n)$, this is still negligible in n and thus makes significant progress towards overcoming limitation 2. However, we believe that this construction is plausibly secure when t is *any* polynomial in n (unlike previous constructions based on BB84 [TFKW13, BL20] and coset states [CLLZ21, CV22, SS25]), and view our results as providing evidence towards this conjecture. Our justification for the plausible security of this construction is the fact that binary phase states are pseudorandom [JLS18, BS19] and hence multi-copy unclonable [Wer98]. We discuss our binary phase state construction more in Section 1.2.3.

Secondly, we study the new and natural notion of a *Haar cloning game*. Here, the unitary U_θ is sampled according to the *Haar measure* and the players receive oracle access to U_θ and $U_\theta^\dagger$. We show that the Haar cloning game is the *hardest* cloning game by exhibiting a *worst-case to average-case reduction*; this allows us to use an upper bound on the value of *any* cloning game, including our binary phase state game, in order to bound the value of the Haar cloning game. As a consequence, we additionally obtain the following:

Corollary 1.2 (Informal)**.** *Let $n, t \in \mathbb{N}$. As a consequence of our worst-case to average-case reduction (Theorem 7.5), we can show the following bounds on the Haar cloning game:*

- *In the single-copy setting, the Haar game $\mathsf{G}_{1\mapsto 2}$ has a value of $\omega(\mathsf{G}_{1\mapsto 2}) \leq \left(\cos^2(\pi/8)\right)^n \approx 2^{-0.228n}$.*
  (Here, the players are free to make arbitrarily many adaptive queries to U_θ or $U_\theta^\dagger$.)
- *In the multi-copy setting, the Haar game $\mathsf{G}_{t\mapsto t+1}$ has a value of $\omega(\mathsf{G}_{t\mapsto t+1}) \leq \exp(O(t\log t)) \cdot 2^{-n}$.*
  (Here, the players are restricted to making a single query to U_θ or $U_\theta^\dagger$.)

We will see next that Haar cloning games are central to the applications previously listed in items 3 and 4. We will discuss Haar cloning games and our worst-case to average-case reduction more in Section 1.2.2.

Opening Up New Applications. To demonstrate the full potential of our new insights into cloning games, we give two applications of our techniques which help resolve fundamental open questions in the field. We will see that these applications crucially require us to overcome the aforementioned limitations 1 and 2 in the existing constructions and analyses of cloning games.

[2] As we explain in Remark 6, approximate $t \mapsto t+1$ no-cloning emerges as a special case of our one-query cloning game, whereby each player makes a single query to $U_\theta^\dagger$ and immediately measures in the computational basis (with no post-processing whatsoever). In this case, the value of the cloning game is precisely equal to the maximum *average* cloning fidelity for $t \mapsto t+1$.

- **Black Hole Cloning Games.** In Section 8, we analyze a new three-player game which is designed to capture cloning and entanglement monogamy in the context of evaporating black holes (see Figure 2). Our results offer new quantitative insights into the *black hole information paradox* [Haw76, Pre92, HP07] and suggest that, in an idealized model of a black hole which features Haar random (or pseudorandom) scrambling dynamics, the information from infalling qubits can only be recovered from either the interior or the exterior of the black hole—but never from both places at the same time.

  At a technical level, this requires us to essentially show a bound of $O(2^{-n})$ for the $1 \mapsto 2$ Haar cloning game. We thus crucially need to overcome the aforementioned limitation 1, and we also need to make use of the aforementioned worst-case to average-case reduction. We will discuss this application in more detail in Section 1.3, taking care to provide context on relevant prior work in black hole physics.

- **Unclonable Cryptography: "MicroCrypt" and the Multi-Copy Setting.** In Section 9, we give an affirmative answer to an open question which was recently posed in [MPSY24]; namely: do interesting unclonable cryptographic primitives exist, even in a world in which $\mathsf{P} = \mathsf{NP}$? We construct succinct unclonable encryption schemes from the existence of pseudorandom unitaries; thereby, for the first time, bridging the gap between the worlds of MicroCrypt and unclonable cryptography. A crucial ingredient for this result is the aforementioned worst-case to average-case reduction.

  Secondly, we propose a candidate multi-copy unclonable encryption scheme based on the aforementioned binary phase cloning game. We view Theorem 1.1 as evidence and a first step towards proving its security in the stronger setting where t can be an a priori unbounded polynomial in n and the players are free to make polynomially many queries to the encryption and decryption functionality (or even more strongly, are given the secret key θ in the clear). Considering the pseudorandomness of the binary phase states that we use as ciphertexts, we believe this stronger security guarantee to be plausible. Obtaining multi-copy security clearly requires us to overcome limitation 2.

  We will discuss these applications to unclonable cryptography in some more detail in Section 1.4.

We now turn to a detailed overview of our techniques.

1.2 Technical Overview

This technical overview is organized as follows:

- In Section 1.2.1, we discuss previous constructions [BL20, CLLZ21] and explain the limitations of these constructions and the underlying techniques [TFKW13, CV22, SS25] in both the multi-copy and single-copy settings.

- In Section 1.2.2, we discuss a natural construction using Haar random unitaries, the obstacles to directly analyzing this construction, and our worst-case to average-case reduction as a means of indirectly studying this construction.

- In Section 1.2.3, we present our construction based on binary phase states (previously put forth by [JLS18, BS19] as a quantum pseudorandom state), and our new tools for analyzing this. Our tools significantly extend the previous notion of *binary types* introduced by [AGQY22] for analyzing binary phase states.

We remark at the outset that, when considering cloning games, we will consider a few different models for how the players (Bob and Charlie) access θ:

- *Strong cloning games:* Bob and Charlie are given θ in the clear;
- *Oracular cloning games:* Bob and Charlie are given oracle access to U_θ and $U_\theta^\dagger$, and are free to make an a priori unbounded polynomial number of queries.
- *Bounded-query-oracular cloning games:* Bob and Charlie are given some a priori bound q on the number of queries they can adaptively make.

  We note that, even when $q = 1$, this model is still quite expressive; as noted in Remark 6, it captures conventional and approximate $t \mapsto t + 1$ no-cloning bounds as a special case.

We will also sometimes consider Bob and Charlie who are required to run in quantum polynomial time.

1.2.1 Previous Techniques and Their Limitations

Let us now dive a little deeper into the shortcomings of our current understanding of cloning games. Here, it is instructive to start with limitation 2; namely, that of multi-copy games.

Multi-Copy Insecurity of BB84 and Coset States. One can extend cloning games as defined in Figure 1 to *multi-copy* cloning games: in this variant, the cloner Φ receives t copies i.e. the state $(U_\theta |x\rangle)^{\otimes t}$. In the place of Bob and Charlie, there are now $t+1$ players $\mathcal{P}_1, \ldots, \mathcal{P}_{t+1}$ who wish to all simultaneously guess x. It is easy to see that this game becomes provably easier for the adversaries as t increases.

In the case of BB84 states, where $U_\theta |x\rangle = \mathsf{H}^\theta |x\rangle$, we claim that the adversaries can win with probability 1 for any $t \geq 2$. The attack is simple: Φ will measure one copy in the standard basis and one copy in the Hadamard basis, and forward these results to all players. Upon receiving θ, the players can mix-and-match these results to recover x. The intuitive issue here is that the measurement basis is entirely disentangled across qubits; in fact, [AK21] describes a generic attack on cloning games with this disentangled structure.

The case of coset states [CLLZ21, CV22, SS25] is similar, albeit only once $t \gg n$. Here, we will interpret the basis θ as a subspace $A \subseteq \mathbb{F}_2^n$ of dimension $n/2$, and the input $x \in \{0,1\}^n$ as a pair of cosets $s + A, s' + A^\perp$. Then the cloner will receive copies of the state

$$|A_{s,s'}\rangle = \frac{1}{2^{n/4}} \sum_{a \in A} (-1)^{\langle a, s' \rangle} |a + s\rangle .$$

The cloner can measure half the copies in the standard basis and half the copies in the Hadamard basis, and forward these results to all players. Upon receiving A, they can all identify the cosets $s + A$ and $s' + A^\perp$ with high probability.

As stated, the above attacks only apply in the strong cloning setting. However, the situation is more grim for a very simple reason: *these families of states are both learnable given* $\mathsf{poly}(n)$ *copies*, whereas most states require exponentially many copies to become learnable, as the state of the art in quantum tomography [BCG13] suggests. Hence, the cloner Φ can simply learn a classical description of the state and subsequently forward both the basis θ and the message x to the $t+1$ players; the players do not even require the challenger to send them θ. In other words, these attacks even hold in the bounded-query-oracular model with $q = 0$ or $q = 1$. Nevertheless, our technical starting point, which we discuss next, is the toolkit used by previous works to analyze cloning games in the single copy ($t = 1$) case. We will pin down where exactly it fails to work in the multi-copy case and remedy these problems. To provide the necessary background, we begin by introducing the notion of a monogamy of entanglement game.

Monogamy of Entanglement Games. We now take a brief detour and discuss the concept of *monogamy of entanglement games*; we will see shortly that they are closely related to cloning games. Monogamy of entanglement games were introduced by Tomamichel, Fehr, Kaniewski and Wehner [TFKW13] in order to characterize entanglement monogamy [Ter04] using the language of non-local games. Informally, quantum correlations are "monogamous", and thus cannot be shared freely among multiple parties.

A monogamy of entanglement (MOE) game G with respect to the question set Θ, answer set $\mathcal{X}$ and measurement set $\{\mathbf{A}_x^\theta\}_{\theta\in\Theta,x\in\mathcal{X}}$ is an interactive game played by three players: a trusted referee called Alice, as well as two colluding and adversarial parties called Bob and Charlie.

1. (**Setup phase**) Bob and Charlie prepare a tripartite quantum state $\rho \in \mathcal{D}(\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B} \otimes \mathcal{H}_\mathsf{C})$. They send register A to Alice, and hold onto registers B and C, respectively. Afterwards, they are no longer allowed to communicate for the remainder of the game.

2. (**Question phase**) Alice samples a random question $\theta \sim \Theta$, and then applies the corresponding measurement $\{\mathbf{A}_x^\theta\}_{x\in\mathcal{X}}$ to her register A. Afterwards, Alice announces the question θ to both Bob and Charlie, and keeps the measurement outcome in $\mathcal{X}$ to herself.

3. (**Answer phase**) Bob and Charlie independently output a guess for Alice's outcome by applying the measurements $\{\mathbf{B}_x^\theta\}_{x\in\mathcal{X}}$ and $\{\mathbf{C}_x^\theta\}_{x\in\mathcal{X}}$ to their registers B and C, respectively.

4. (**Outcome phase**) Bob and Charlie win if they both guess Alice's outcome correctly.

Here, we associate a particular *strategy* S employed by Bob and Charlie with the tuple consisting of the initial shared state ρ and the positive operator-valued measurements $\{\mathbf{B}_x^\theta\}_{\theta\in\Theta,x\in\mathcal{X}}$ and $\{\mathbf{C}_x^\theta\}_{\theta\in\Theta,x\in\mathcal{X}}$. The *value* of a particular strategy S for the monogamy game G is defined as the average winning probability

$$\omega_\mathsf{S}(\mathsf{G}) := \mathop{\mathbb{E}}_{\theta\sim\Theta} \sum_{x\in\mathcal{X}} \mathrm{Tr}\left[(\mathbf{A}_x^\theta \otimes \mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta)\rho_{\mathsf{ABC}}\right].$$

We let $\omega(\mathsf{G})$ denote the maximal value of the game, i.e., the optimal winning probability over all strategies. An upper bound on the value of a monogamy game therefore limits the extent to which Bob and Charlie can simultaneously maintain a quantum correlation with Alice who holds a register outside of their view. *We emphasize that in general monogamy of entanglement games, the shared state ρ is completely arbitrary and adversarially chosen by Bob and Charlie; as we will see, this is the main way in which cloning games deviate from the monogamy of entanglement setting.*

Appendix A: Connecting Cloning and Monogamy Games. The standard tool for analyzing cloning games is to recast them as a special type of monogamy game. Together with the techniques laid out by [TFKW13] for analyzing monogamy games, this has found numerous applications in unclonable cryptography, including unclonable encryption [BL20], quantum copy-protection [Aar09, CMP22, CLLZ21, AKL+22], unclonable decryption keys [GZ20], and unclonable proofs [GMR23].

We now explain this connection between cloning and MOE games. In a cloning game, Alice sends the cloner Φ the state $U_\theta|x\rangle$. Instead, we could imagine that Alice and Φ share several EPR pairs, and later on in the game (even after the cloning phase) Alice can apply a measurement $\left\{\mathbf{A}_x^\theta := \bar{U}_\theta|x\rangle\langle x|\bar{U}_\theta^\dagger\right\}_{x\in\{0,1\}^n}$ on her side to induce the state $U_\theta|x\rangle$ on the cloner's side, where $\bar{U}$ denotes the complex conjugate of U. This yields a monogamy of entanglement game with the following two restrictions:

- As already mentioned, Alice's measurements $\mathbf{A}_x^\theta$ must take the form $\bar{U}_\theta|x\rangle\langle x|\bar{U}_\theta^\dagger$.

- The tripartite state ρ shared by Alice, Bob, and Charlie is the *Choi state* of the cloning channel Φ. Concretely, we must have the special form

$$\rho_{\mathsf{ABC}} = (\mathbb{I}_{\mathsf{A}} \otimes \Phi_{\mathsf{A}' \to \mathsf{BC}})(|\mathsf{EPR}\rangle\langle\mathsf{EPR}|_{\mathsf{AA}'}). \tag{1}$$

  In words, *ρ can be adversarially chosen subject to the constraint that its marginal state on Alice's system is maximally mixed.*

This equivalence, which we formally show in Lemma A.1, was first observed in the context of BB84 states by Broadbent and Lord [BL20]. On a high level, the statement is a consequence of the *ricochet property* of EPR pairs, which we formally state in Section 2.1. The technical benefit of doing this is that it enables us to get a handle on the cloning channel Φ by absorbing it into the state shared by the players in the equivalent monogamy game. Now we can focus on Bob and Charlie's measurements which, as we will see, can be handled using spectral bounds as first observed by [TFKW13].

Although the equivalence observed by [BL20] is in the single-copy setting, it turns out that this idea readily generalizes to the multi-copy setting, as we show in Lemma A.2. The differences are as follows:

- In the cloning game, Alice and the cloner Φ now share nt EPR pairs, and Alice will measure each of the t copies in the basis specified by $\left\{\bar{U}_\theta |x\rangle\langle x| \bar{U}_\theta^\dagger\right\}_{x\in\{0,1\}^n}$.
- In the equivalent monogamy-like game, we only say that the adversaries win if Alice's t measurements and the $t+1$ players' outputs are all equal to the same string x. In other words, we need to essentially post-select on Alice's measured string $x \in \{0,1\}^n$ being the same for each of the t copies, which means the value of this monogamy-like game is immediately upper bounded by $2^{-n(t-1)}$.

Because of this post-selection, what we end up with is an equality of the following form:

$$\omega(\mathsf{G}_{\text{cloning}}) = 2^{n(t-1)} \cdot \omega(\mathsf{G}_{\text{monogamy-like}}). \tag{2}$$

Note that when $t = 1$, the $2^{n(t-1)}$ term is 1 and we recover the equivalence used by [BL20]. Our goal is hence to upper bound the value of $\mathsf{G}_{\text{monogamy-like}}$ by $2^{-n(t-1)} \cdot \mathsf{negl}(n)$, ideally even $O(2^{-nt})$.

Section 6: [TFKW13] and its Limitations. The work by [TFKW13] analyzes MOE games and later focuses on the BB84 case (i.e. $U_\theta = \mathsf{H}^\theta$) and uses two beautiful ideas, which for simplicity we state in the single-copy setting:

1. The value of a particular monogamy game can be bounded *independently* of the state ρ_{ABC} shared by the 3 players, noting that ρ_{ABC} is PSD and has trace 1. Concretely, one can show that

$$\mathop{\mathbb{E}}_{\theta\sim\Theta} \sum_{x\in\mathcal{X}} \mathrm{Tr}\left[(\mathbf{A}_x^\theta \otimes \mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta)\rho_{\mathsf{ABC}}\right] \leq \left\| \mathop{\mathbb{E}}_{\theta\sim\Theta} \sum_{x\in\mathcal{X}} \mathbf{A}_x^\theta \otimes \mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta \right\|_\infty.$$

   This reduces the task of bounding the value of a monogamy game to bounding an operator norm. In general monogamy games as formulated by [TFKW13], the shared state ρ_{ABC} is adversarially chosen so this step is tight. However, we will see soon that this step is too lossy when restricting attention to the special monogamy-like games that are equivalent to cloning games.

2. This operator norm can in turn be bounded just in terms of *pairwise overlaps* between the $\mathbf{A}_x^\theta$'s, which the designer of the game is free to choose. As we restate in Theorem 6.1, the authors of [TFKW13] show that

$$\left\| \mathop{\mathbb{E}}_{\theta\sim\Theta} \sum_{x\in\mathcal{X}} \mathbf{A}_x^\theta \otimes \mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta \right\|_\infty \leq \frac{1}{|\Theta|} + \frac{|\Theta|-1}{|\Theta|} \cdot \max_{\substack{\theta,\theta'\in\Theta \\ \theta\neq\theta'}} \max_{x,x'\in\mathcal{X}} \left\| \mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'} \right\|_\infty .$$

   We refer the reader to Theorem 6.1 for a formal statement.

In the BB84 monogamy game where $\Theta = \mathcal{X} = \{0,1\}$ and $\mathbf{A}_x^\theta = \mathsf{H}^\theta |x\rangle\langle x| \mathsf{H}^\theta$, it is straightforward to see that $\left\| \mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'} \right\|_\infty = \frac{1}{\sqrt{2}}$, and hence $\omega(\mathsf{G}_{\text{BB84}}) \leq \frac{1}{2} + \frac{1}{2\sqrt{2}}$. The work by [TFKW13] also extends this to "parallel-repeated" BB84 games with $|\Theta| = |\mathcal{X}| = \{0,1\}^n$ (see Theorem 3.4) for a formal definition, and show that

$$\omega(\mathsf{G}_{\text{BB84}}^{\otimes n}) \leq \cos^2\left(\frac{\pi}{8}\right)^n \approx 2^{-0.228n}.$$

Hence the BB84 monogamy game has value $\leq 2^{-0.228n}$, and in fact this is tight; [TFKW13] exhibits a simple strategy achieving this bound. Similar techniques were used by [CV22] and improved upon by [SS25] to analyze subspace coset states, ultimately proving an upper bound of $O(2^{-n/4})$; it is not known whether or not this is tight.[3] However, the techniques laid out by [TFKW13] *provably* do not suffice for our applications:

- In the multi-copy case, recall from Equation (2) that we need to prove a bound on $\mathsf{G}_{\text{monogamy-like}}$ of $\ll 2^{-n(t-1)}$. Item 1 of the [TFKW13] methodology proposes to ignore the structure of the state shared by Alice and $\mathcal{P}_1, \ldots, \mathcal{P}_{t+1}$, in order to reduce our task to bounding an operator norm.

  This is likely too lossy in our setting, as evidenced by the following simple counterexample (assume $t > 1$ is even for simplicity) that holds against any cloning game where the unitaries U_θ have real entries. Alice will hold $tn/2$ EPR pairs (which are unentangled from the states held by $\mathcal{P}_1, \ldots, \mathcal{P}_{t+1}$). The $t+1$ players will each deterministically output 0^n as their guess (note that once again this strategy does not depend at all on θ). The winning probability is now just the probability that Alice measures 0 on each of her $tn/2$ EPR pairs (in whatever basis she samples), which is $2^{-nt/2} \geq 2^{-n(t-1)}$. We formalize this counterexample in Section 6.1.

  We note that this does not rule out the possibility of the [TFKW13] technique being adaptable to the multi-copy setting for a construction that uses unitaries with complex entries. However, the pre-existing constructions based on BB84 states or coset states — as well as our main construction based on binary phase states (which we sketch in Section 1.2.3) — only use unitaries with real entries. Thus we still view our result as a bound against the adaptability of existing construction and techniques to the multi-copy setting.

- Even in the single-copy case, there is another inherent limitation that arises from using Item 2 of the [TFKW13] methodology: the maximal pairwise overlap $\max_{\theta\neq\theta'} \left\| \mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'} \right\|_\infty$ is provably at least $2^{-n/2}$ for any monogamy game, as we show in Section 6.2. For completeness, we also show in Section 6.3 that our binary phase state construction (which we will discuss more in Section 1.2.3) essentially attains this maximum pairwise overlap.

[3] Previous work [SSS24] proved an upper bound of $O(2^{-n/2})$ in a setting where the cloner Φ is restricted to splitting the state as is into two equal-sized halves, sending one to Bob and the other to Charlie. We cite $O(2^{-n/4})$ as the state of the art, as we are interested in games where the cloner Φ is unrestricted.

Howeover, we would ideally like to prove a tight bound (up to constant factors) of $O(2^{-n})$. This is not just a matter of aesthetic taste; this is actually crucial for our application to black hole physics, as we explain in Section 1.3.

We next turn our attention to our construction and our new techniques for analyzing it, which make progress towards overcoming both of these barriers.

1.2.2 Section 7: Haar Cloning Games and Worst-Case to Average-Case Reductions

Given our previous observations on the multi-copy insecurity of BB84 and coset states, it is clear that we need to look for entirely new constructions. Ideally, such a candidate ensemble of states would also remain *unlearnable* in the presence of an arbitrary polynomial amount of identical copies. A natural idea is to consider Haar random states, which Werner [Wer98] showed to be multi-copy unclonable. This suggests the following very natural approach: Alice will take $\{U_\theta : \theta \in \Theta\}$[4] to be a Haar random ensemble and send the cloner $(U_\theta |x\rangle)^{\otimes t}$. We call this the $t \mapsto t+1$ *Haar cloning game*. However, existing techniques for analyzing the Haar measure, which we outline below, appear severely limited for our purposes:

- Prior works [MPSY24, CDX+24, ACG+24] often rely on representation-theoretic techniques. In our setting, we would roughly need to prove spectral bounds on the *mixed Haar twirl* of a certain operator Ξ; informally, in the $1 \mapsto 2$ case, these amount to expressions of the form:

$$\left\| \mathop{\mathbb{E}}_{U \sim \mathrm{U}(d)} \left[\left(U \otimes U \otimes \bar{U}\right) \Xi \left(U \otimes U \otimes \bar{U}\right)^\dagger \right] \right\|_\infty .$$

  General expressions of this form have been studied by [EW01, GO23, GBO23] using the machinery of *mixed Schur-Weyl duality*, but their techniques appear to be very unwieldy in our more complicated setting with multiple non-communicating parties.

- The recent breakthrough result by Ma and Huang [MH24] uses a technically involved purification argument [MH24] that once again does not seem to adapt easily to the multi-party setting.

- Finally, the recent beautiful work by Bhattacharya and Culf [BC25] analyzes the Haar measure in the single-copy case using a modular application of the one-shot decoupling theorem [DBWR14], but in the process only establishes a cloning bound of $\tilde{O}(1/n)$, whereas we would like a bound that is $O(2^{-n})$ or at the very least exponentially small in n.

Instead, we take a two-step approach which is based on the following insight: cloning games instantiated with a Haar (pseudo)random unitary are, in some sense, *strictly harder to win* than any other cloning game. We prove this via a *worst-case to average-case reduction* which, at a high level, follows from Haar invariance and some additional new insights into *mixed* unitary designs, which we explain in more detail below.

Our observation immediately suggests the following approach for analyzing a Haar cloning game:

1. Argue that for *any* distribution $\mathfrak{D}$ supported on $\mathrm{U}(2^n)$, we have:

$$\sup_{\text{strategies } \mathsf{S}} \omega_{\mathsf{S}}(\mathsf{G}; U \sim \mathrm{U}(2^n)) \leq \sup_{\text{strategies } \mathsf{S}} \omega_{\mathsf{S}}(\mathsf{G}; U \sim \mathfrak{D}). \tag{3}$$

[4] The Haar random ensemble is infinite so this is not well-defined; this technicality can be circumvented by using a higher order unitary design or a pseudorandom unitary [MPSY24, MH24] in its place.

2. Find a convenient distribution $\mathcal{D}$ such that we can more easily show that

$$\sup_{\text{strategies } \mathsf{S}} \omega_{\mathsf{S}}(\mathsf{G}; U \sim \mathfrak{D}) \leq O(2^{-n}),$$

perhaps by passing first to an equivalent monogamy game as stated earlier.

We prove the aforementioned *worst-case-to-average-case reduction* which is captured in Item 1 in Section 7. To instantiate this argument, we need to be able to sample V that appears Haar random, together with a classical description of it. This can be done using either a *mixed unitary design* (in the bounded-query-oracular setting) or a pseudorandom unitary [MPSY24, MH24] (in the oracular setting with computationally bounded players). We formally define mixed unitary designs in Section 7.1, and—as a bonus—we also prove that the standard notion of an exact unitary t-design will also work as a mixed unitary design without modification. To the best of our knowledge, this was not previously observed in the literature, and we hope that this contribution might be of independent interest. We leave the task of adapting this reduction to the strong cloning game setting as a direction for future work.

It now remains to address Item 2 i.e. find some other cloning game that we can more easily show an upper bound of $O(2^{-n})$ for. We address this next.

1.2.3 Sections 4 and 5: Construction and Analysis from Binary Phase States

Our Construction Inspired by Quantum Pseudorandom States. We begin from a simple starting point: in Section 1.2.2, we suggested having Alice send a Haar random state $U_\theta |x\rangle$ to the cloner. Instead, what if Alice were to send a *pseudorandom* state [JLS18, BS19]? These are also multi-copy unclonable by a trivial hybrid argument combined with Werner's result [Wer98] in the Haar case. The advantage of working with binary phase states is that we have much simpler constructions that, as we will see, are easier to analyze.

It was shown by [JLS18, BS19] that if $\mathfrak{F}$ is a family of post-quantum pseudorandom functions [Zha21a] $f : \{0,1\}^n \to \{0,1\}$, then the *binary phase state*

$$|\psi^f\rangle := 2^{-n/2} \sum_{y \in \{0,1\}^n} (-1)^{f(y)} |y\rangle$$

is pseudorandom. To use this in a cloning game, we follow the approach in [Col23] in order to encode $x \in \{0,1\}^n$ into this state, which we do by taking:

$$|\psi^f_x\rangle := 2^{-n/2} \sum_{y \in \{0,1\}^n} (-1)^{f(y)+\langle x,y\rangle} |y\rangle = \mathsf{U}_f \mathsf{H}^{\otimes n} |x\rangle, \quad \text{where} \quad \mathsf{U}_f := \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle\langle x|$$

is a phase oracle for f. In other words, we are proposing to define a cloning game with $\Theta = \mathfrak{F}$ and $U_\theta = \mathsf{U}_f \mathsf{H}^{\otimes n}$. Thus in the equivalent monogamy game, Alice's projectors will be defined by

$$\mathbf{A}^f_x := \mathsf{U}_f \mathsf{H}^{\otimes n} |x\rangle\langle x| \mathsf{H}^{\otimes n} \mathsf{U}_f.$$

The question is now how one should go about analyzing this game. As mentioned in Section 1.2.1, the usual [TFKW13] methodology for analyzing cloning games is firstly limited to the single-copy setting, and secondly even in this setting can only prove a bound of $2^{-n/2}$. For completeness, we show that in Section 6.3 that plugging our binary phase construction into [TFKW13] "saturates" this technique and yields a single-copy cloning bound of $\widetilde{O}(2^{-n/2})$, which is stronger than the previous results on BB84 [TFKW13, BL20] and coset [CLLZ21, CV22, SS25] states.

Compressed Oracles and Binary Types. The techniques discussed up to this point draw on the machinery of [TFKW13] and thus suffice to establish cloning bounds even in the setting where a classical description of the measurement basis θ (in the binary phase case, the function f) is sent to all players $\mathcal{P}_1, \ldots, \mathcal{P}_{t+1}$ in the clear. To our knowledge, the only other technique that works in this strong regime is the decoupling technique by [BC25]. However, as we explained in Sections 1.2.1 and 1.2.2, both of these techniques run into limitations with respect to the multi-copy setting and/or attaining an optimal bound of $O(2^{-n})$.

We hence propose to migrate to the oracular setting, where each player can make oracle queries to U_f, but is not given a description of f in the clear. Note that this still suffices to recover x from $\mathsf{U}_f\mathsf{H}^{\otimes n}|x\rangle$. In fact, we only need one query: a single query to U_f would leave us with $\mathsf{H}^{\otimes n}|x\rangle$, and now measuring in the Hadamard basis yields x. We explain this in the case of general cloning games in Remark 6.

We now want to reason about algorithms that make oracle queries to U_f for a random (or pseudorandom) function f. The natural candidate technique for such a task is Zhandry's compressed oracle technique [Zha19]. The crucial idea is to purify the cloning game by adding a register that stores the function f. One can then argue that queries to U_f for a random $f : \{0,1\}^n \to \{0,1\}$ can be simulated as follows:

- We will add a purifying "database" register to the system that we initialize to $|\emptyset\rangle$. In general, it will store some subset $S \subseteq \{0,1\}^n$.
- If the algorithm wishes to query the string $y \in \{0,1\}^n$, simply update $|S\rangle \leftarrow |S \oplus \{y\}\rangle$ (note that if y is in S before the query, this will remove y from S.)

Let us see how this technique would play out in our setting. Alice and $\mathcal{P}_1, \ldots, \mathcal{P}_{t+1}$ all share some global state, and act as follows:

- Alice queries each of her t n-qubit states, then applies a Hadamard to each copy. Her local transformation can be written as $\bigotimes_{i=1}^{t}\left(\sum_{y_i\in\{0,1\}^n}\mathsf{H}^{\otimes n}|y_i\rangle\langle y_i|\right)$, and she will XOR $\{y_1\}\oplus\ldots\oplus\{y_t\}$ into the database register.
- For each $i \in [t+1]$, let the adversary $\mathcal{P}_i$ make q adaptive queries represented by unitaries $V_{i,1}, \ldots, V_{i,q}$. Their local transformation can be written as a sum of terms of the form

$$V_{i,q}|z_{i,q}\rangle\langle z_{i,q}|V_{i,q-1}|z_{i,q-1}\rangle\langle z_{i,q-1}|\ldots V_{i,1}|z_{i,1}\rangle\langle z_{i,1}|,$$

  and they will XOR $\{z_{i,1}\}\oplus\ldots\oplus\{z_{i,q}\}$ into the database register.

In summary, the database register will contain the set:

$$\bigoplus_{i=1}^{t}\{y_i\}\oplus\bigoplus_{i=1}^{t+1}\bigoplus_{j=1}^{q}\{z_{i,j}\}. \tag{4}$$

At this point, it is unclear how to proceed, for the following simple conceptual reason: the utility of Zhandry's compressed oracle technique [Zha19] lies in the fact that it connects an algorithm's success probability with the contents of the database register in some way. For example, when reproving the [BBBV97] lower bound showing the optimality of Grover search, Zhandry shows that the success probability of the algorithm is essentially upper bounded by the probability of a solution x to the search problem appearing in the database register. However, there is no analogous notion in our setting, because we are considering a problem with *inherently quantum inputs*; a successful adversary likely needs to query U_f on every input in superposition.

Instead, we will deviate from Zhandry's compressed oracle formalism by simply tracing out (or equivalently, measuring) the database register. This effectively conditions our superposition on the collection of strings that are listed an odd number of times in Equation (4). This is exactly the notion of *binary types* introduced by [AGQY22]. In order to get a better handle on the binary type's combinatorial structure, we will restrict each of the $t+1$ players to only make *one oracle query* to U_f; as explained in Remark 6, this is still sufficiently expressive to admit a trivial strategy attaining value 2^{-n}.

In this case, a binary type $\boldsymbol{\lambda}$ is specified by a subset $T_{\boldsymbol{\lambda}} \subseteq [2^n]$ with $|T_{\boldsymbol{\lambda}}| \leq 2t+1$. For $\mathbf{x} \in [2^n]^{2t+1}$, we say that $\mathsf{BinType}(\mathbf{x}) = \boldsymbol{\lambda}$, or equivalently that $\mathbf{x}$ *matches* $\boldsymbol{\lambda}$, if every string in $T_{\boldsymbol{\lambda}}$ appears an odd number of times in $\mathbf{x}$, while every string outside $T_{\boldsymbol{\lambda}}$ appears an even number of times in $\mathbf{x}$. Thus, if Alice and the players jointly hold a standard basis state $|\mathbf{x}\rangle$, a simultaneous query to U_f by all parties will write $\mathsf{BinType}(\mathbf{x})$ into the database register. Finally, we let $\Pi_{\boldsymbol{\lambda}}$ denote the projector onto standard basis vectors $\mathbf{x}$ that match $\boldsymbol{\lambda}$. We provide more precise definitions and properties of binary types in Section 4.2. We now model each player's projector as follows:

$$\mathbf{P}^f_{i,x} = \mathsf{U}_f V_i^\dagger \, |x\rangle\langle x| \, V_i \mathsf{U}_f,$$

for unitaries Q_i.[5] This simplification together with the aforementioned binary type formalism allows us to succinctly characterize the value of the cloning game: if we define

$$\Xi := \sum_{x \in \{0,1\}^n} \left[\left(\mathsf{H}^{\otimes n} \, |x\rangle\langle x| \, \mathsf{H}^{\otimes n} \right)^{\otimes t} \otimes \bigotimes_{i=1}^{t+1} \left(V_i^\dagger \, |x\rangle\langle x| \, V_i \right) \right], \text{ then}$$

$$\omega(\mathsf{G}) = \sum_{\boldsymbol{\lambda}} \mathrm{Tr}\left[\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}} \rho\right],$$

where ρ is the shared state from the monogamy-like game that we introduced in Section 1.2.1. We face two challenges in bounding expressions of this form. We state them below and then describe how we address these challenges:

1. The [TFKW13] paradigm of discarding the tripartite state ρ and simply bounding this expression by $\max_{\boldsymbol{\lambda}} \|\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}}\|_\infty$[6] is provably too lossy, as we explained in Section 1.2.1.

2. Even if it were somehow sufficient to bound $\|\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}}\|_\infty$ for each $\boldsymbol{\lambda}$, to the best of our knowledge, it appears difficult to directly establish such a bound. Informally, the reason is that the combinatorial structure arising from a type $\boldsymbol{\lambda}$ entangles registers together; if we consider the $t = 1$ case and the type defined by $T_{\boldsymbol{\lambda}} = \{x^*\}$ for some string x^*, then strings of the form (x^*, y, y), (y, x^*, y), or (x^*, y, y) would all match $\boldsymbol{\lambda}$. It would be much cleaner if we could just analyze strings from one of these categories at a time.

Idea 1 (Section 5.4): Staring at the Shared State. To address Item 1, we take a closer look at the structure of the shared state ρ. It is the result of applying some (adversarially chosen) channel to the right half of tn EPR pairs. This can be seen from Equation (1) (appropriately generalized to the multi-copy setting). In other words, if we apply a partial trace to remove the $\mathsf{P}_{1 \to t+1}$ registers of the $t+1$ players, the residual state on Alice's register A will always be proportional to $\mathbb{I}_{2^n \times 2^n}$.

[5] In reality, we later also allow these players additional ancillary workspace qubits; we define this generalization in Definition 3.8. Moreover, we assume without loss of generality that the players do not perform any preprocessing before making their query to U_f, by absorbing this preprocessing into the cloning channel Φ that constructs their initial states.

[6] This bound holds by noting that the projectors $\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}}$ are mutually orthogonal.

This structure may seem mild, but it turns out to be enough to complete our analysis; we present this in Sections 5.4 and 5.5. This is perhaps not surprising; in the counterexample we presented in Section 1.2.1 showing that just bounding the operator norm would be insufficient, Alice's local state was very far from maximally mixed. In fact, it was a pure state consisting of $t/2$ EPR qudit pairs.

At a high level, our analysis to use this structure of ρ proceeds by showing that for any type $\boldsymbol{\lambda}$ such that $\Pi_{\boldsymbol{\lambda}}\Xi\Pi_{\boldsymbol{\lambda}}$ has high operator norm, the shared state ρ must place *low* weight on the image of Π_λ. These effects roughly cancel each other out.

Idea 2 (Sections 4.3 and 5.3): From Types to Subtypes. We now turn to the issue stated in Item 2. Continuing with the $t = 1$ example, reasoning about $\boldsymbol{\lambda}$ directly requires simultaneously handling three categories of strings: $(x^*, y, y), (y, x^*, y)$, or (x^*, y, y). Instead, we simplify matters by focusing on just one of these categories at a time — we call such a category a *subtype*, a novel notion we define formally in Section 4.3. We denote subtypes by $\boldsymbol{\mu}$ and their corresponding subtype projectors by $\Pi_{\boldsymbol{\mu}}$. In Section 4.3.2, we show that instead of bounding $\|\Pi_{\boldsymbol{\lambda}}\Xi\Pi_{\boldsymbol{\lambda}}\|_\infty$ for a type $\boldsymbol{\lambda}$, it suffices to bound $\|\Pi_{\boldsymbol{\mu}}\Xi\Pi_{\boldsymbol{\mu}}\|_\infty$ for a *subtype* $\boldsymbol{\mu}$. This added structure allows us to prove better spectral bounds, which we present in Section 5.3.

It turns out that this technique allows us to prove the desired bound of $O(2^{-n})$ for $1 \mapsto 2$ cloning games, albeit with the restriction that Bob and Charlie can only make one query each to U_f. At a very high level, the "product structure" of subtypes enables us to leverage a simple but novel spectral bound on the column-wise tensor product of several matrices, which we present in Lemma 2.18.

Technical Tool (Section 2.4): Spectral Bounds on Blockwise Tensor Products. In order to prove spectral bounds on the norm of $\Pi_{\boldsymbol{\mu}}\Xi\Pi_{\boldsymbol{\mu}}$ for any subtype $\boldsymbol{\mu}$, and accommodate the possibility of the $t+1$ players using ancilla qubits, we require a novel bound on the norm of a blockwise tensor product of $d \times d$ block matrices. As a simple example, the $d = 2$ case is the following: we need to show that

$$\left\| \begin{bmatrix} c_{1,1}\mathbf{A}_{1,1} \otimes \mathbf{B}_{1,1} & c_{1,2}\mathbf{A}_{1,2} \otimes \mathbf{B}_{1,2} \\ c_{2,1}\mathbf{A}_{2,1} \otimes \mathbf{B}_{2,1} & c_{2,2}\mathbf{A}_{2,2} \otimes \mathbf{B}_{2,2} \end{bmatrix} \right\|_\infty \leq 1,$$

provided that $\begin{bmatrix} \mathbf{A}_{1,1} & \mathbf{A}_{1,2} \\ \mathbf{A}_{2,1} & \mathbf{A}_{2,2} \end{bmatrix}, \begin{bmatrix} \mathbf{B}_{1,1} & \mathbf{B}_{1,2} \\ \mathbf{B}_{2,1} & \mathbf{B}_{2,2} \end{bmatrix}$ are unitary and $|c_{i,j}| \leq 1$ for all i, j. Proving this turns out to be rather technically challenging; we present this result and its proof in Theorem 2.15. We also discuss at the end of Section 2.4.1 why existing techniques fail to prove the general result we need. Given that this theorem is a purely linear algebraic statement unrelated to monogamy games, we are hopeful that it might be useful elsewhere in quantum information and even in other areas.

Putting these ideas together, we manage to prove a multi-copy cloning bound of $O_t(2^{-n})$, overcoming the limitations of previous techniques explained in 1.2.1 with a complete overhaul of the technical framework laid out by [TFKW13], albeit at the expense of restricting the $t + 1$ players to make a single oracle query to U_f.

1.3 Application I: Black Hole Cloning Games

As one application of our techniques on cloning games, we study the notion of a *black hole cloning game*—a three-player interactive game which is designed to capture no-cloning and entanglement monogamy which arises naturally in the context of evaporating black holes. The main result we discuss in this section is an asymptotically tight upper bound on the success probability of a variant of the game. In particular, we observe that the analysis of black hole cloning games is inextricably linked to the existence of standard cloning

games which have asymptotically optimal bounds of the form $O(2^{-n})$—well beyond the pre-existing upper bound of $2^{-0.25n}$ from the analysis by [SS25] of the coset state game [CLLZ21, CV22]. Our new contributions on *optimal* games allow us to fill this gap, and to complete the analysis.

In this section, we first provide some relevant context on black holes, and then give an overview of how we revisit the problem using the language of cloning games. We present more detailed context and results in Section 8.

Hayden-Preskill thought experiment. Hawking [Haw76] made the remarkable prediction that black holes are not completely black—they slowly emit what is now known as *Hawking radiation*. But if black holes evaporate, what happens to information that falls inside of a black hole? Does it get destroyed, or is it effectively conserved and eventually radiated out in some scrambled form? This question has puzzled physicists for many decades. The endeavour of trying to reconcile the predictions of quantum mechanics and general relativity has led to the famous *black hole information paradox* [Haw76, Pre92].

Hayden and Preskill [HP07] proposed a thought experiment that illustrates the black-hole information loss problem: Suppose that Alice throws k qubits into a black hole, which are maximally entangled with a second register in her possession. For simplicity, we assume that the black hole initially consists of $n - k$ qubits. After a long period of time, another distant observer, say Bob, uses the intercepted Hawking radiation (say, in the form of photons) which he has collected in the meantime, feeds it into his quantum computer and applies an appropriate computation in an attempt to recover Alice's quantum state. Hayden and Preskill asked: how long would Bob have to wait before he finally starts to observe correlations between the outgoing Hawking radiation and the entangled infalling matter near the boundary? To answer this question, they made the following crucial assumption: black holes are extremely strong and efficient *information scramblers*—their internal dynamics can be modeled as a more or less *Haar random* unitary time-evolution.[7] This view has since been widely adopted as an idealized mathematical model of black hole evolution [AMPS13, HH13, KP23, EFL+24]. Concretely, it assumes that, from the perspective of an outside observer, Alice's infalling information is scrambled by a random unitary and effectively spread across the entire horizon of the black hole, whereby the total amount of information—accounting for both the internal degrees of freedom, as well as Alice's infalling information—is encoded in qubits which lie at the surface of the black hole. Here, the *surface* of the black hole refers to the *stretched horizon*—a tiny region of space which is located "just outside" of the black hole horizon [STU93, HH13] and is typically considered to be part of the black hole.

Hayden and Preskill [HP07] showed that after slightly more than half of the black hole has evaporated (sometimes called the *Page time*), Bob can in principle completely recover the information from Alice's infalling qubits by intercepting the outgoing Hawking radiation. This led them to conclude that black holes act as *information mirrors*: while Alice's information remains concealed up until the half-way point, it then starts to emerge fairly quickly in the form of scrambled Hawking radiation.

Do Black Holes Clone Information? While the Hayden-Preskill thought experiment [HP07] suggests that the information from Alice's infalling qubits is ultimately preserved and encoded in the form of scrambled radiation, it does raise the question: how much of Alice's information is still retained by the black hole? Could it be that a distant observer, say Bob, can recover Alice's information from the outgoing radiation, and yet a "second copy" of Alice's information somehow also survives in the black hole interior?

Suppose that we partition the relevant qubits which result from the evolution of the black hole into two registers H and R, where H corresponds to the qubits near the horizon which are still retained by the black

[7] Note that genuine *Haar* dynamics have exponential circuit complexity with high probability [Kni00]. Hayden and Preskill opted for a weaker notion than Haar randomness which nevertheless suffices for their purposes; namely, that of a *unitary 2-design.*

hole, and where R corresponds to emitted Hawking radiation. Hayden and Preskill [HP07] consider two regimes: at the beginning of the experiment, H is significantly larger than R and virtually all of Alice's information is contained in H; however, by the end of the experiment, when the black hole has evaporated long past the Page time (and most of the qubits have been transformed into radiation), R is now significantly larger than H and must therefore be highly correlated with Alice's infalling qubits. Is it possible that Alice's information is retained by the black hole (and thus present in H) but simultaneously also encoded in R—even long after the Page time? Could it be that black holes *clone* information?[8] Note that the standard no-cloning theorem [WZ82] and its approximate variants [BH96] do not suffice to immediately answer this question; for example, if Alice's infalling information is *classical* rather than *quantum*, the black hole may not even need to fully clone a quantum state to retain her information; it merely needs to maintain a classical correlation with Alice's infalling bits. Therefore, to answer this question, a new approach is necessary.

This Work: Revisiting the Black Hole Information Paradox. We seek to extend our existing understanding of the black hole information paradox in two ways. The first is that we would like to provide a new and *quantitative* characterization of cloning and entanglement monogamy which arises in the context of evaporating black holes. Many seminal works [CHSH69, TFKW13] have quantified and enhanced our understanding of physical principles (e.g., the nature of entanglement) through the formulation and analysis of certain interactive games; our first goal is to do the same for the black hole information paradox:

> ***Question One**: Can we give a quantitative trade-off for how much of Alice's infalling information can be retained by the black hole, and how much can be present in its radiation?*

Note that such a trade-off would significantly extend the analysis by Hayden and Preskill [HP07] who merely studied two extreme cases, i.e., when when most of the qubits are either retained by the black hole or when most of the qubits have been converted into Hawking radiation. As it turns out, however, such an information-theoretic analysis seems to lie way beyond the scope of existing techniques. (We will discuss the limitations of existing these techniques later in this section, as well as in Sections 1.2.1 and 1.2.2.)

Secondly, we aim to revisit prior attempts for how to model the decoder's knowledge of the internal dynamics of the black hole. In the seminal Hayden-Preskill thought experiment [HP07], the authors assume that the decoder (say, Bob) holds a quantum memory that is maximally entangled with the qubits in the interior of the black hole. In other words, Bob is an extremely powerful observer that has complete control over the black hole and its resulting radiation. As noted by Hayden and Preskill, we would ideally like a more realistic model that captures Bob's knowledge of the black hole dynamics without giving him direct control over the black hole, which raises the question:

> ***Question Two:** Are there alternative—and perhaps more reasonable—models that capture the fact that the decoder has knowledge of the internal dynamics of the black hole?*

We believe that an affirmative answer to these two questions could offer new and valuable insights into the black-hole information paradox.

[8] Hayden and Preskill [HP07] explored this question using another and much more radical thought experiment: suppose that Bob quickly decodes Alice's information from the intercepted Hawking radiation, and then immediately jumps inside of the black hole and crosses the event horizon in an attempt to find a "second copy" of Alice's information. A series of follow-up works [AMPS13, HH13, Aar16] have since exposed and studied paradoxes which emerge out of this experiment, and which have led to the belief that black-hole radiation decoding must necessarily be *computationally intractable* [HH13, Bra23, BEM+23].

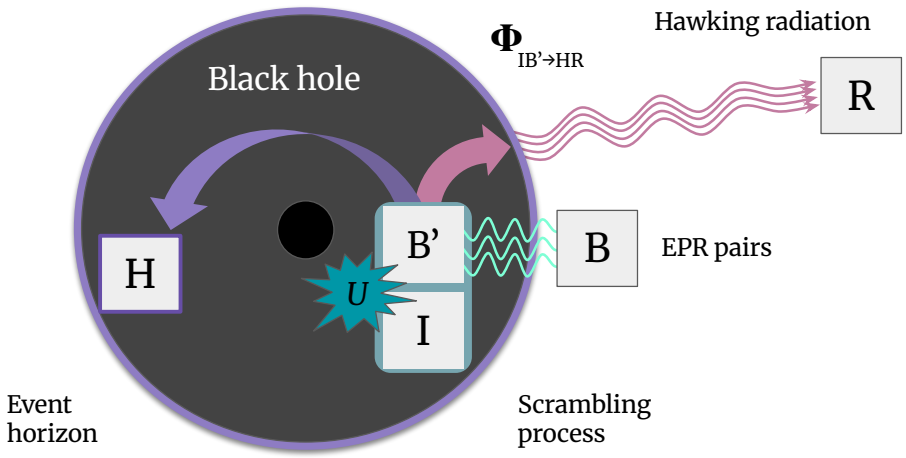

Figure 2: **Black Hole Cloning Game**. Entangled particles emerge near the boundary and form a k-qubit EPR pair $|\mathsf{EPR}\rangle_{\mathsf{B}'\mathsf{B}}$, of which register B' falls inside of the black hole, and register B is given to Alice. The interior of the black hole, modeled as $|0^{n-k}\rangle_{\mathsf{I}}$, together with the k infalling qubits in register B', undergo a *scrambling process*. Here, the internal dynamics of the black hole are described by a random n-qubit unitary time-evolution operator $U \sim \nu$ which gets applied to registers $\mathsf{B}'\mathsf{I}$. A quantum channel $\Phi_{\mathsf{IB}'\to\mathsf{HR}}$ processes the internal qubits into two registers: a register H corresponding to the qubits at the event horizon which are retained by the black hole, and a register R corresponding to the emitted Hawking radiation. Charlie (who is anchored at the horizon) receives H, whereas Bob (who is a distant observer) receives R. The two observers are allowed to have some knowledge of the internal dynamics U, and thus receive oracles for U and $U^\dagger$. Finally, Alice measures B, and Bob and Charlie win if they simultaneously guess her outcome correctly.

Our Approach: Black Hole Cloning Games. To address *Question One*, we cast the famous black-hole information paradox into the form of a cloning game (see Figure 2). At the beginning of the game, Alice throws her entangled qubits into the black hole. Later, at the end of the game, two spatially separated "adversaries" called Bob and Charlie will attempt to recover Alice's information—either as a *distant observer* with access to the emitted Hawking radiation (say, Bob), or as an *anchored observer* (say, Charlie) who remains at the event horizon and has access to remaining qubits which are retained by the black hole. Concretely, we imagine that Alice measures her half of the entangled state at the end of the experiment, and Bob and Charlie are asked to simultaneously predict her measurement outcome. In our setting, Alice's infalling information should be thought of as being *classical* rather than *quantum*; indeed, our black hole cloning game in Figure 6 is equivalent to a game in which Alice throws random classical bits into the black hole[9].

[9]This is an important distinction compared to the Hayden and Preskill experiment, where Alice's information can actually be thought of as being *quantum* and where Bob attempts to decode it in a coherent fashion by exploiting entanglement as a resource. Nevertheless, our setting captures the inherent trade-off between Alice's system and the registers H and R in a similar spirit.

We work with the purified picture for purely aesthetic purposes; it helps us keep the notation consistent with Hayden and Preskill, and also makes the analysis via monogamy of entanglement games much more direct.

In line with prior works [HP07, HH13, KP23, EFL+24], we model the black hole's internal evolution in between as a "scrambling process" which is the result of some random unitary time-evolution U, followed by an arbitrary quantum channel Φ that processes the internal qubits into two systems: one corresponding to the qubits near the event horizon of the black hole (denoted by H), and another corresponding to the emitted Hawking radiation (denoted by R). In the work of Hayden and Preskill [HP07], Φ is essentially just a simple unitary channel that randomly partitions the scrambled qubits into two subsystems H and R of different sizes (in particular, where R is typically much larger than H), whereas in our work we let Φ be an arbitrary (and possibly unitary) completely-positive and trace-preserving map. This significantly generalizes the setting considered by Hayden and Preskill [HP07] and, in particular, includes *all possible partitionings* into two systems H and R. As in a conventional cloning game, it is also crucial that Bob and Charlie do not communicate while the decoding phase is taking place, which also consistent with our modeling assumption that Charlie is anchored at the horizon of the black hole, whereas Bob remains a distant observer.

To address *Question Two*, we grant Bob and Charlie *oracle access* to the internal scrambling dynamics U, as well as its inverse $U^\dagger$. Additionally, we assume that Bob and Charlie have a complete description of the physical process Φ that results in the outgoing radiation. While Bob (and similarly, also Charlie) no longer has the ability to exercise direct control over the black hole dynamics (as in the Hayden-Preskill model), he does have the power (via the oracle for $U^\dagger$) to instantaneously "unscramble" the black hole's time evolution at will. Here, the oracle access to the unitaries $U, U^\dagger$ is meant to reflect the possibility that Bob and Charlie are powerful observers that have obtained some knowledge on the physical equations and parameters governing the black hole's evolution (see Figure 7 for a quantum circuit representation).

Analyzing Black Hole Cloning Games. Given the similarity between our black hole cloning game and the games studied in [TFKW13, BL20], this raises the question of whether one can indeed interpret one as an instance of the other. Our main technical insight is that the analysis of black hole cloning games is inextricably linked to the existence of standard $1 \mapsto 2$ cloning games which have asymptotically optimal bounds of the form $O(2^{-n})$—well beyond the pre-existing upper bound of $2^{-0.25n}$ from the analysis by [SS25] of the coset state game [CLLZ21, CV22]. In Theorem 8.4, we prove the following result without any restrictions on the choice of quantum channel Φ; however, for technical reasons, we let ν be a unitary 3-design and we assume that Bob and Charlie employ single-query strategies only. We visualize what Bob and Charlie's strategies might look like in Figure 7, and we mention further potential improvements in Section 1.5.

Theorem 1.3 (Informal, see Theorem 8.4 for formal statement)**.** *Let $n, k \in \mathbb{N}$ be integers with $n \geq k$ and let $\nu = \{U_\theta\}_{\theta\in\Theta}$ be an n-qubit unitary 3-design. Then, for any quantum channel Φ (of appropriate dimensions), the maximal single-query value $\omega(\mathsf{G}_{BH})$ of the black hole cloning game G_{BH} (as illustrated in Figure 2) with respect to ν and Φ is at most $O(2^{-k})$.*

The bulk of our work in Section 8 is to show that the maximal value $\omega(\mathsf{G}_{\text{BH}})$ (see Definition 8.3 for a formal definition) can always be related to the maximal value of a related (but standard) cloning game $\mathsf{G}_{\text{clone}}$. Specifically, we show that the game G_{BH} emerges as a special case of $\mathsf{G}_{\text{clone}}$ in which we post-select on the event that Alice's sampled message y takes the form $y = x||0^{n-k}$, for some $x \in \{0,1\}^k$. Because this event occurs with probability 2^{-n+k}, this allows us to deduce that

$$\sup_{\text{strategies } \mathsf{S}} \omega_{\mathsf{S}}(\mathsf{G}_{\text{clone}}) \geq 2^{-n+k} \cdot \omega(\mathsf{G}_{\text{BH}}).$$

Therefore, in order to obtain an asymptotically optimal bound of the form $\omega(\mathsf{G}_{\text{BH}}) = O(2^{-k})$, it suffices to show that the related cloning game $\mathsf{G}_{\text{clone}}$ has a maximal value of $\sup_{\text{strategies } \mathsf{S}} \omega_{\mathsf{S}}(\mathsf{G}_{\text{clone}}) = O(2^{-n})$. **Crucially, we require an $O(2^{-n})$ bound; a bound of the form $O(2^{-cn})$ for any $c < 1$ is insufficient.** This would yield $\omega(\mathsf{G}_{\text{BH}}) \leq 2^{-k} \cdot 2^{n(1-c)}$, which is a completely trivial bound if we assume $n \gg k$ (which is likely since presumably the black hole is a much larger system than the set of qubits Alice throws inside). As briefly mentioned in the introduction and elaborated in Section 1.2.1, our work is the first to show that a cloning game (even if in a restricted query model) admits an asymptotically optimal bound of the form $O(2^{-n})$. We explain this final point some more in Remark 14.

Implications for Black-Hole Physics. Theorem 1.3 yields the first quantitative trade-off for how much of Alice's information in the form of k infalling entangled qubits can be retained by the black hole, and how much can be present in its emitted Hawking radiation. In fact, our bound of $O(2^{-k})$ is also optimal (up to constant factors), since there always exists a particular Hawking radiation channel Φ together with a trivial strategy that attains it: we can consider a variant of the black hole cloning game where Φ is the channel that converts the entirety of all the qubits inside of the black hole into radiation (i.e., acting as the identity), which would allow Bob to perfectly recover the information from Alice's system by simply applying the inverse of the scrambling unitary. Now Charlie can guess randomly and succeed with probability 2^{-k}.

We believe that our bound has several interesting implications. First, it suggests that the moment Bob has produced a register which is nearly maximally correlated with Alice's infalling qubits, then any additional qubits that lie in the interior of the black hole (i.e., in Charlie's system), must be almost completely uncorrelated from them. Second, such a strong decoupling result is achieved for *any* choice of Hawking radiation channel Φ—it arises precisely because of the strong scrambling properties of the unitary 3-design itself. By contrast, the same would not be true for a *classical* model of black-hole scrambling [HP07], say in the form of a random reversible circuit or a random permutation[10]. Despite the fact that a random permutation is already exponentially complex (i.e., requires exponential-sized circuits with overwhelming probability), it is simply *not sufficiently scrambling* to allow for a similar decoupling to hold.

In summary, our results suggest that, in an idealized model of a black hole which features Haar random (or pseudorandom) scrambling dynamics, the information from infalling entangled qubits can only be recovered from either the interior (specifically, at the event horizon) or the exterior of the black hole (i.e., in the form of distant Hawking radiation), though never from both places at the same time.

1.4 Application II: Unclonable Cryptography

In this section, we describe our applications to quantum cryptography; specifically, for how to construct succinct unclonable encryption schemes from the existence of *pseudorandom unitaries*. This allows us to fully bridge the gap between the world of quantum pseudorandomness and unclonable cryptography.

Unclonable Encryption. Cloning games have played a foundational role in the field of *unclonable cryptography*—a branch of quantum cryptography that capitalizes on quantum no-cloning [WZ82] to achieve guarantees of "unclonable security" which are completely impossible classically. These include unclonable encryption [BL20, AKL23, KT23, AKY24], encryption with unclonable decryption keys [GZ20], unclonable commitments and proofs [GMR23], quantum copy-protection [AKL+22, CMP22], and unclonable

[10] Interestingly, one could interpret the one-round variant of the *sponge construction* which underlies the international hash standard SHA-3 [BDPA11, CP24, CPZ24] as a classical model of black hole scrambling, where the scrambling unitary is given by a random permutation and the Hawking radiation channel is an erasure channel that selects a subset of the final output bits.

quantum advice [BKL23]. Most of these constructions rely at minimum on the existence of post-quantum one-way functions, placing unclonable cryptography in "Post-Quantum MiniCrypt" [Imp95].[11]

Of particular interest to us is unclonable encryption, which is very closely related to cloning games. Indeed, any cloning game with value $\mathsf{negl}(n)$ immediately implies an unclonable encryption scheme with message space $\mathcal{X} = \{0,1\}^n$ that satisfies unclonable search security: to encrypt x under secret key θ, output $U_\theta |x\rangle$. This scheme has the obvious shortcoming that it is deterministic, and hence does not satisfy the ideal notions of indistinguishable or unclonable-indistinguishable security.

However, Broadbent and Lord [BL20] proposed the following transformation that plausibly transforms an unclonable search secure scheme $\mathsf{SearchEnc}$ to an unclonable indistinguishable secure scheme: to encrypt $x \in \{0,1\}^n$ under secret keys k, θ, sample a random PRF seed $r \in \{0,1\}^\lambda$ and output the classical string $x \oplus \mathsf{PRF}(k,r)$ together with the quantum state $|\mathsf{SearchEnc}(\theta, r)\rangle$. Broadbent and Lord [BL20] also provided some mild evidence that this may be secure if the PRF is instantiated with a random oracle. We emphasize that *proving* the unclonable-indistinguishable security of this transformation (or a similar one) is a notoriously difficult open problem [KT23, AKL23, AKY24]. Our point is just that studying unclonable encryption in the weaker search-secure setting is still an interesting and relevant cryptographic problem.

Multi-Copy Unclonable Cryptography. Previous works on unclonable cryptography have exclusively focused exclusively on the case of $1 \mapsto 2$ cloning games, e.g. in the case of unclonable encryption [BL20], the adversarial cloner is given only one copy of a ciphertext state and aims to provide two receivers, say Bob and Charlie, with sufficient information to later recover the plaintext message.

These cryptographic primitives could naturally be extended to $t \mapsto t+1$ security: in the case of unclonable encryption, the cloner receives t identical copies of a ciphertext state and aims to provide $t+1$ receivers with enough information to later recover the plaintext message. This raises the following question:

Can we construct $t \mapsto t+1$ unclonable cryptography from well-founded assumptions?

As explained in Section 1.2.1, existing constructions and techniques have little to say about this question. Answering this would resolve a question which was recently left open in [AMP24], who asked whether the desirable property of multi-copy security is within reach in unclonable cryptography more generally.

Quantum Cryptography in "MicroCrypt". Meanwhile, another line of work [JLS18, BS19, MPSY24, MH24, BHHP24] has introduced and constructed notions of *pseudorandom quantum states and unitaries*. These are implied by the existence of post-quantum one-way functions; however, the reverse implication is not known. In fact, recent work [Kre21, AIK22, KQST23] has provided evidence that such an implication is unlikely to exist. This has led to the development of new and *inherently quantum* assumptions [BHHP24, PQS24]. As a result, the quantum cryptographic landscape includes yet another world, sometimes referred to as "MicroCrypt", which is potentially even weaker than that of MiniCrypt.

Moreover, pseudorandom states have proven to be powerful cryptographic tools in quantum cryptography, implying commitments [MY22] and oblivious transfer [BCKM21, GLSV21], and more. The fact that such powerful primitives live in MicroCrypt raises the following question:

Does unclonable cryptography exist in MicroCrypt?

In fact, the authors of [MPSY24] explicitly asked whether pseudorandom unitaries (which have eluded major cryptographic application so far) imply the existence of unclonable cryptographic primitives.

[11] The work by [BL20] does imply an information-theoretic construction of unclonable encryption based on BB84 states; however, this lacks succinctness as the size of the encryption and decryption keys scales with the message length n rather than just the security parameter λ.

Our Results. In this work, we make progress towards these foundational questions, and give an affirmative answer to both of them. Our main result of this section is the following:

Theorem 1.4 (Informal, see Theorems 9.4 and 9.5 for formal statements)**.** *We show the following statements:*

1. *Assuming the existence of pseudorandom unitaries, there exists an unclonable encryption scheme with succinct keys which satisfies oracular $1 \mapsto 2$ search security (i.e., the adversaries are computationally bounded and only given oracle access to encryption and decryption functionality).*

2. *If the message space is $\mathcal{X} = \{0,1\}^n$ and we fix $t = o(n/\log n)$ then, assuming the existence of post-quantum pseudorandom functions, there exists an unclonable encryption scheme with succinct keys satisfies oracular $t \mapsto t+1$ search security, **provided** that the adversaries are computationally bounded and can only make **a single oracle query** to either the encryption or decryption functionality.*

Remark 1. *Although we are only able to prove security for $t = o(n/\log n)$, we remark that our construction is plausibly secure for t that is an arbitrary polynomial in n (unlike previous constructions based on BB84 states [BL20] and coset states [CLLZ21]). Our justification for the plausible security of this construction is the fact that binary phase states are pseudorandom [JLS18, BS19] and hence multi-copy unclonable [Wer98].*

Remark 2. *Broadbent and Lord [BL20] prove a result that appears similar to our result for the $1 \mapsto 2$ case. The main difference is that they assume the existence of post-quantum PRFs, while we only need PRUs which is likely a weaker assumption [Kre21]. Additionally, they assume a different oracle model; they instantiate their PRF as a random oracle, while we give the adversaries oracle access to unitaries for encryption and decryption.*

Our proof of the first result uses the BB84 cloning game [TFKW13] and its analysis by [BL20], together with the worst-case to average-case reduction outlined in Section 1.2.2 and fleshed out in Section 7. The latter can be thought of as an additional cryptographic application of pseudorandom unitaries[12] which was previously not known. While this gives us a security bound of $2^{-0.228n} + \mathsf{negl}(\lambda)$ rather than the ideal $O(2^{-n}) + \mathsf{negl}(\lambda)$, this is not a crucial difference for this application (unlike in the black hole setting); moreover, the analysis of the subspace coset monogamy game has the advantage that it does not need to restrict the queries made by the players.[13]

Our proof of the second result uses our machinery outlined in Section 1.2.3 and fleshed out in Sections 4 and 5 for analyzing cloning games based on binary phase states. We emphasize that our construction is the first that could even be plausibly secure in the setting where t can be an a priori unbounded polynomial in λ, n and the $t+1$ players are given the secret key θ in the clear. While our results are far from this ideal goal, we view our techniques as providing a stepping stone towards an ideal security result for unclonable encryption. We are also optimistic that our results and techniques might be adaptable to other problems in unclonable cryptography.

We visualize the landscape of some unclonable cryptographic primitives relative to the worlds of MicroCrypt, Post-Quantum Minicrypt, and Post-Quantum Obfustopia in Figure 3.

[12] To the best of our knowledge, the use of pseudorandom unitaries in the context of efficient worst-case to average-case reductions has not previously appeared.

[13] We note for completeness that we could just as easily have used the analysis by [SS25] of the subspace coset monogamy game [CLLZ21, CV22] in the place of the BB84 game and thus obtained a marginally stronger bound of $O(2^{-0.25n}) + \mathsf{negl}(\lambda)$. We comment on this more in Remark 18.

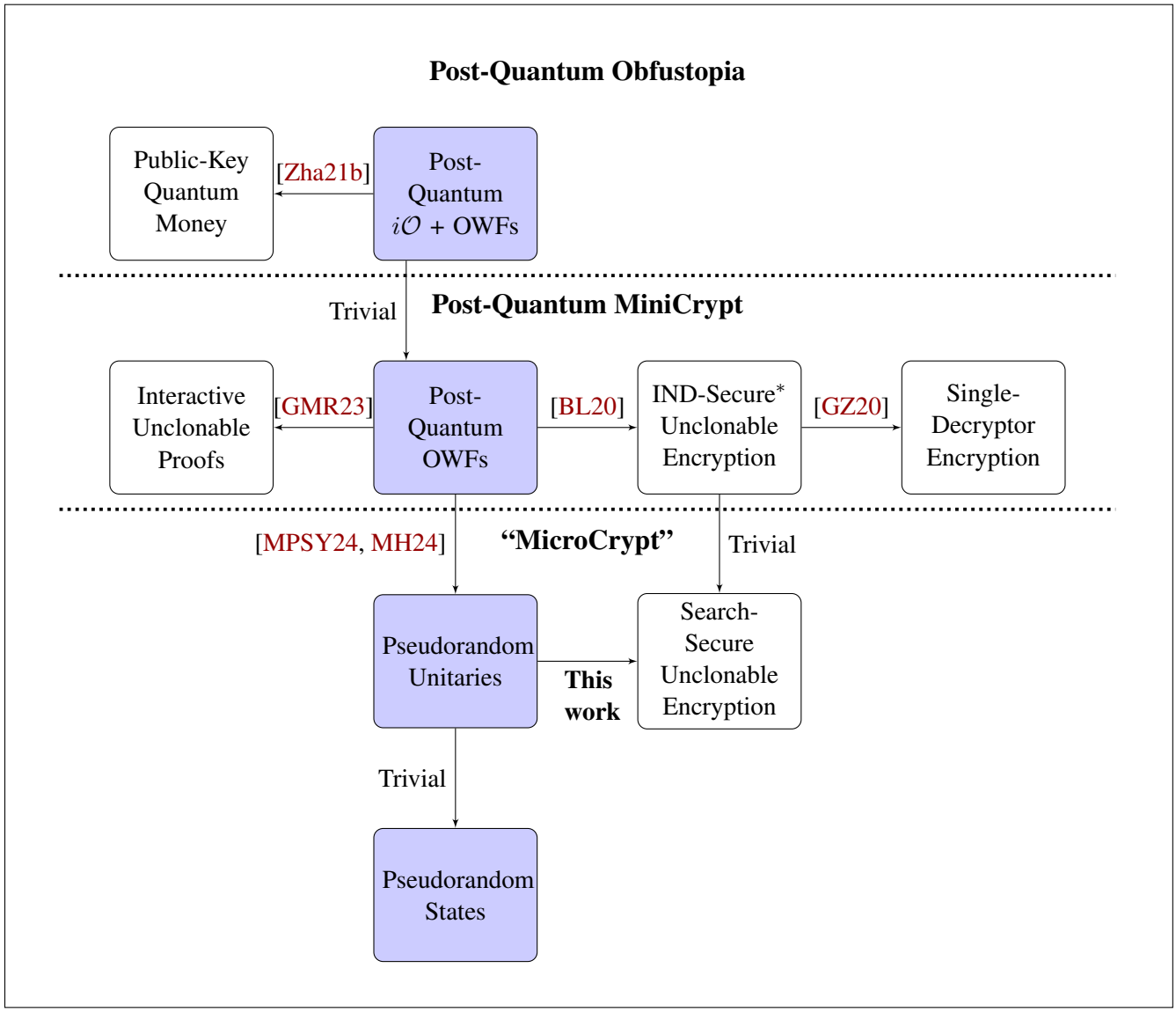

Figure 3: A visualization of some primitives in unclonable cryptography and the assumptions that are known to imply them (we focus here on primitives that are relatively well-understood and related to monogamy of entanglement games). We segment these assumptions into three worlds, loosely following [Imp95]: Obfustopia, MiniCrypt, and MicroCrypt. MicroCrypt is a world where we only assume the existence of pseudorandom states and unitaries, which could plausibly hold even if $\mathsf{P} = \mathsf{NP}$ [KQST23]. Powerful cryptographic primitives such as bit commitments [MY22] and oblivious transfer [BCKM21, GLSV21] have been shown to exist in MicroCrypt; however, prior to our work, it was not known how to instantiate any unclonable cryptography *with succinct keys* in MicroCrypt. Our work takes a first step in this direction by showing that pseudorandom unitaries imply search-secure succinct unclonable encryption in an oracle model.
(*We note for clarity that the existing results on indistinguishability-secure unclonable encryption all come with some kind of caveat e.g. existing in an oracle model and requiring that the adversaries are disentangled [BL20], or requiring quantum decryption keys [AKY24].)

1.5 Open Questions

Cloning Games in General. We first list some open questions related to cloning games in general; these would immediately yield applications to either or both of the black hole and unclonable encryption settings. We list some of these questions here:

1. Can the security of the underlying $1 \mapsto 2$ oracular cloning game (i.e., as in Construction 1) be proven even if the two players (say, Bob and Charlie) can adaptively make *any* polynomial number of queries to the encoding underlying unitary and its inverse?

   This would immediately imply the security of our black hole cloning game against *arbitrary* Bob and Charlie strategies, when instantiated with a pseudorandom unitary (PRU) rather than a unitary design. Due to their highly efficient (and yet strong) scrambling properties, pseudorandom unitaries are believed to be an excellent theoretical model of black hole dynamics [KP23, EFL+24].

2. More tantalizingly, can this security be shown if the measurement basis θ (either a PRU or PRF secret key, depending on whether we are considering the PRU or binary phase construction) is given to Bob and Charlie in the clear, rather than in the form of an oracle? This still plausibly satisfies unclonable security (as demonstrated by [TFKW13, BL20, CV22, SS25] for BB84 and coset state cloning games), but is highly counterintuitive; the PRU/PRF security guarantees do not say anything about what could happen in a game where the secret key θ is eventually leaked.

   In our black hole cloning game, this would allow us to prove much stronger quantitative statements, even in the scenario in which Bob and Charlie have *complete* knowledge of the internal scrambling dynamics of the black hole.

3. Can we achieve any of the above stronger security guarantees for $t \mapsto t+1$ cloning games? Or as a starting point: can we prove security against players $\mathcal{P}_1, \ldots, \mathcal{P}_{t+1}$ that are free to make multiple *non-adaptive* queries to $U_\theta, U_\theta^\dagger$?

Applications to Black Hole Physics and Beyond. Here, we list some questions specific to our black hole application:

1. Can we make our modeling assumptions in our definition of black hole cloning games in Section 8 more physically realistic? For example, can we model the (initial) internal qubits of the black hole as a more general quantum state (potentially even entangled with the exterior) rather than as the all-zero state $|0^{n-k}\rangle$? What if the scrambling dynamics do not just affect internal qubits, but also external qubits? And lastly, what if the scrambling dynamics is in the form of a Haar random isometry?

2. Can we use the language of interactive games to offer new quantitative insights into information scrambling in other chaotic quantum systems, besides black holes?

Applications to Unclonable Cryptography. Finally, we present some questions specific to our applications to unclonable cryptography:

1. What other unclonable cryptography primitives can be instantiated in MicroCrypt?

2. Can we obtain unclonable encryption with the stronger notion of indistinguishability security that we usually require of encryption schemes? (Our notion of unclonable security takes the form of "search security", which as we argue in Section 1.4 offers a plausible but not yet proven path towards

indistinguishable security.) This is an important but difficult problem that recent works have made some progress on [BL20, KT23, AKL23, AKY24].

3. Which unclonable cryptography primitives have natural, constructible, and applicable $t \mapsto t+1$ analogues, besides unclonable encryption?

Organization of the Paper. The remainder of this paper is organized as follows:

- In Section 2, we present some preliminaries including our novel spectral bounds in Section 2.4 on blockwise tensor products of matrices.
- In Section 3, we formally define monogamy of entanglement games and cloning games.
- In Sections 4 and 5, we introduce our novel notion of binary subtypes and apply this to prove $O_t(2^{-n})$ cloning bounds for our binary phase state cloning game in the single-query-oracular setting.
- In Section 6, we revisit pre-existing techniques for analyzing cloning and monogamy games, and demonstrate that there are inherent limitations that likely prevent them from being adaptable to our applications in either black hole physics or unclonable cryptography.
- In Section 7, we prove a worst-case to average-case reduction for cloning games that allows us to adapt our result for binary phase state cloning games to Haar cloning games. This is integral both to our application to black hole physics, and to proving the existence of $1 \mapsto 2$ unclonable encryption assuming only PRUs.
- In Section 8, we formally define black hole cloning games, and use our aforementioned technical results on cloning games to prove an upper bound on the value of the black hole cloning game.
- Finally, in Section 9, we define the notion of succinct unclonable encryption schemes and show that it exists in an oracle model, assuming the existence of pseudorandom unitaries. We also provide a first result towards establishing multi-copy security of the same scheme.

Acknowledgements. The authors would like to thank Aditya Nema, Aparna Gupte, Aram Harrow, Fermi Ma, Henry Yuen, Jiahui Liu, John Bostanci, Jonas Haferkamp, Jonathan Lu, Joseph Carolan, Lisa Yang, Makrand Sinha, Netta Engelhardt, Peter Shor, Prabhanjan Ananth, Ran Canetti, Saachi Mutreja, Soonwon Choi, Thomas Vidick, Tony Metger, William Kretschmer, and Yael Tauman Kalai for useful discussions. AP is supported by the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Co-design Center for Quantum Advantage (C2QA) under contract number DE-SC0012704. SR is supported by an Akamai Presidential Fellowship and the grants of VV. VV is supported by DARPA under Agreement No. HR00112020023, NSF CNS-2154149 and a Simons Investigator Award. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Government or DARPA.

2 Preliminaries

2.1 Quantum Computation

For a comprehensive background, we refer to [NC16]. We denote a finite-dimensional complex Hilbert space by $\mathcal{H}$, and we use subscripts to distinguish between different systems (or registers). For example, we

let $\mathcal{H}_{\mathsf{A}}$ be the Hilbert space corresponding to a system A. The tensor product of two Hilbert spaces $\mathcal{H}_{\mathsf{A}}$ and $\mathcal{H}_{\mathsf{B}}$ is another Hilbert space denoted by $\mathcal{H}_{\mathsf{AB}} = \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$. The Euclidean norm of a vector $|\psi\rangle \in \mathcal{H}$ over the finite-dimensional complex Hilbert space $\mathcal{H}$ is denoted as $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$. Let $\mathrm{L}(\mathcal{H})$ denote the set of linear operators over $\mathcal{H}$. A quantum system over the 2-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^2$ is called a *qubit*. For $n \in \mathbb{N}$, we refer to quantum registers over the Hilbert space $\mathcal{H} = \left(\mathbb{C}^2\right)^{\otimes n}$ as n-qubit states. We use the word *quantum state* to refer to both pure states (unit vectors $|\psi\rangle \in \mathcal{H}$) and density matrices $\rho \in \mathcal{D}(\mathcal{H})$, where we use the notation $\mathcal{D}(\mathcal{H})$ to refer to the space of positive semidefinite matrices of unit trace acting on $\mathcal{H}$. The *trace distance* of two density matrices $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ is given by

$$\mathsf{TD}(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1.$$

A quantum channel $\Phi : \mathrm{L}(\mathcal{H}_{\mathsf{A}}) \to \mathrm{L}(\mathcal{H}_{\mathsf{B}})$ is a linear map between linear operators over the Hilbert spaces $\mathcal{H}_{\mathsf{A}}$ and $\mathcal{H}_{\mathsf{B}}$. Oftentimes, we use the compact notation $\Phi_{\mathsf{A}\to\mathsf{B}}$ to denote a quantum channel between $\mathrm{L}(\mathcal{H}_{\mathsf{A}})$ and $\mathrm{L}(\mathcal{H}_{\mathsf{B}})$. We say that a channel Φ is *completely positive* if, for a reference system R of arbitrary size, the induced map $\mathbb{I}_{\mathsf{R}} \otimes \Phi$ is positive, and we call it *trace-preserving* if $\mathrm{Tr}\left[\Phi(X)\right] = \mathrm{Tr}\left[X\right]$, for all $X \in \mathrm{L}(\mathcal{H})$. A quantum channel that is both completely positive and trace-preserving is called a quantum CPTP channel. A *unitary* $U : \mathrm{L}(\mathcal{H}_{\mathsf{A}}) \to \mathrm{L}(\mathcal{H}_{\mathsf{A}})$ is a special case of a quantum channel that satisfies $U^\dagger U = UU^\dagger = \mathbb{I}_{\mathsf{A}}$. When U acts on a density matrix ρ, it maps $\rho \mapsto U\rho U^\dagger$, and we will denote this channel by $U \cdot U^\dagger$. Whenever $d = 2^n$, we refer to the group of unitaries acting on n qubits as $\mathrm{U}(d)$. An isometry is a linear map $V : \mathrm{L}(\mathcal{H}_{\mathsf{A}}) \to \mathrm{L}(\mathcal{H}_{\mathsf{B}})$ with $\dim(\mathcal{H}_{\mathsf{B}}) \geq \dim(\mathcal{H}_{\mathsf{A}})$ and $V^\dagger V = \mathbb{I}_{\mathsf{A}}$. A *projector* Π is a Hermitian operator such that $\Pi^2 = \Pi$, and a *projective measurement* is a collection of projectors $\{\Pi_i\}_i$ such that $\sum_i \Pi_i = \mathbb{I}$. A positive-operator valued measure (POVM) is a set of Hermitian positive semidefinite operators $\{M_i\}$ acting on a Hilbert space $\mathcal{H}$ such that $\sum_i M_i = \mathbb{I}$.

Given a bipartite state ρ_{AB}, the *partial trace* Tr_{B} captures the residual state of the system on just the A register. Tr_{B} is thus defined as a linear map from $\mathrm{L}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}) \to \mathrm{L}(\mathcal{H}_{\mathsf{A}})$ that maps $R \otimes S \mapsto \mathrm{Tr}\left[S\right] \cdot R$. Given a multipartite operator $X \in \mathrm{L}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}})$, the *partial transpose* applies a transpose to only some of these systems. For example, the partial transpose $X \mapsto X^{\mathsf{T}_{\mathsf{B}}}$ with respect to the second system is defined as a linear map satisfying $X_1 \otimes X_2 \otimes X_3 \mapsto X_1 \otimes X_2^\top \otimes X_3$. We can also define a SWAP operator that acts on say registers A and C; this is a linear map that will map $X_1 \otimes X_2 \otimes X_3 \mapsto X_3 \otimes X_2 \otimes X_1$.

Operators. Define the following unitary operators:

- Phase oracle: For $f : \{0,1\}^n \to \{0,1\}$ we let

$$\mathsf{U}_f = \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \left|x\right\rangle\!\left\langle x\right|.$$

- Multi-bit Pauli operator: For $m \in \{0,1\}^n$, let

$$\mathsf{Z}^m = \sum_{x \in \{0,1\}^n} (-1)^{\langle x, m\rangle} \left|x\right\rangle\!\left\langle x\right|.$$

- Hadamard: The n-qubit Hadamard operator is defined by

$$\mathsf{H}^{\otimes n} = 2^{-n/2} \sum_{x,y \in \{0,1\}^n} (-1)^{\langle x, y\rangle} \left|x\right\rangle\!\left\langle y\right|.$$

Choi-Jamiołkowski isomorphism. Let $\mathcal{H}_{\mathsf{A}}$ be a d-dimensional Hilbert space with an orthonormal basis denoted by $\{|1\rangle, \ldots, |d\rangle\}$. Let $|\Omega\rangle = \sum_{i\in[d]} |i\rangle \otimes |i\rangle$ be the vectorization of the identity $\mathbb{I}_d = \sum_{i\in[d]} |i\rangle\langle i|$. Then, the Choi-Jamiołkowski isomorphism $J(\Phi) \in \mathrm{L}(\mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{A}'})$ with respect to a linear map of the form $\Phi : \mathrm{L}(\mathcal{H}_{\mathsf{A}}) \to \mathrm{L}(\mathcal{H}_{\mathsf{B}})$ is defined as

$$J(\Phi) = (\Phi_{\mathsf{A}\to\mathsf{B}} \otimes \mathbb{I}_{\mathsf{A}'})(|\Omega\rangle\langle\Omega|) = \sum_{i,j\in[d]} \Phi(|i\rangle\langle j|) \otimes |i\rangle\langle j| \,.$$

We use the following well known fact.

Lemma 2.1. *Let $\Phi : \mathrm{L}(\mathcal{H}_{\mathsf{A}}) \to \mathrm{L}(\mathcal{H}_{\mathsf{B}})$ be a linear map. Then, for any $|\psi\rangle \in \mathrm{S}(\mathcal{H}_{\mathsf{A}})$ and $|\phi\rangle \in \mathrm{S}(\mathcal{H}_{\mathsf{B}})$,*

$$\langle\phi| \Phi(|\psi\rangle\langle\psi|) |\phi\rangle = \langle\phi| \otimes \langle\bar{\psi}| J(\Phi) |\phi\rangle \otimes |\bar{\psi}\rangle \ ,$$

where the complex conjugation is taken with respect to the computational basis. Equivalently, we have:

$$\mathrm{Tr}\left[|\phi\rangle\langle\phi| \Phi(|\psi\rangle\langle\psi|)\right] = \mathrm{Tr}\left[\left(|\phi\rangle\langle\phi| \otimes |\bar{\psi}\rangle\langle\bar{\psi}|\right) J(\Phi)\right] .$$

By linearity, we immediately obtain the following corollary:

Corollary 2.2. *Let $\Phi : \mathrm{L}(\mathcal{H}_{\mathsf{A}}) \to \mathrm{L}(\mathcal{H}_{\mathsf{B}})$ be any linear map. Then, for any Hermitian operators $\mathbf{P} \in \mathrm{L}(\mathcal{H}_{\mathsf{B}})$ and $\mathbf{Q} \in \mathrm{L}(\mathcal{H}_{\mathsf{A}})$, it holds that*

$$\mathrm{Tr}\left[\mathbf{P}\Phi(\mathbf{Q})\right] = \mathrm{Tr}\left[\left(\mathbf{P} \otimes \bar{\mathbf{Q}}\right) J(\Phi)\right] .$$

2.2 Unitary Designs

In this section, we formally define the *Haar measure* [Sim95] and also define a new and more general version of a *mixed* unitary t-design which also allows for inverses with respect to the adjoint of the unitary.

Definition 2.3 (Haar measure)**.** *Let $d \in \mathbb{N}$ denote the dimension. The Haar measure μ_H is the unique left and right unitarily-invariant measure over the unitary group $\mathrm{U}(d)$; that is, for every (possibly matrix-valued) integrable function f with domain $\mathrm{L}(\mathbb{C}^d)$ and every unitary $V \in \mathrm{U}(d)$,*

$$\int_{\mathrm{U}(d)} f(U)\, \mathrm{d}_{\mu_H} U = \int_{\mathrm{U}(d)} f(U \cdot V)\, \mathrm{d}_{\mu_H} U = \int_{\mathrm{U}(d)} f(V \cdot U)\, \mathrm{d}_{\mu_H} U.$$

For brevity, we oftentimes denote the expectation of f over the Haar measure by

$$\mathop{\mathbb{E}}_{U\sim\mathrm{U}(d)}[f(U)] = \int_{\mathrm{U}(d)} f(U)\, \mathrm{d}_{\mu_H} U.$$

Non-Adaptive Mixed Unitary Designs. In this section, we introduce a generalization of the standard notion of a unitary t-design which also accounts for inverse queries (to the adjoint of the unitary). We exclusively consider exact designs; in particular, exact unitary 3-designs via the Clifford group [Web16].

Definition 2.4 (Non-Adaptive Mixed Unitary (p,q)-Design)**.** *Let ν be an ensemble of unitary operators over $\mathbb{C}^d$. Then, ν is a (non-adaptive) unitary (p,q)-design if, for every $\mathbf{O} \in \mathrm{L}((\mathbb{C}^d)^{\otimes(p+q)})$,*

$$\mathop{\mathbb{E}}_{U\sim\nu}\left[(U^{\otimes p} \otimes (U^\dagger)^{\otimes q})\mathbf{O}(U^{\otimes p} \otimes (U^\dagger)^{\otimes q})^\dagger\right] = \mathop{\mathbb{E}}_{U\sim\mathrm{U}(d)}\left[(U^{\otimes p} \otimes (U^\dagger)^{\otimes q})\mathbf{O}(U^{\otimes p} \otimes (U^\dagger)^{\otimes q})^\dagger\right] .$$

Note that a unitary t-design is a special case of the above definition.

Definition 2.5 (Non-Adaptive Unitary t-Design)**.** *Let ν be an ensemble of unitary operators over $\mathbb{C}^d$. Then, ν is a (non-adaptive) unitary t-design if it is a (non-adaptive) unitary (t,q)-design for $q = 0$.*

Adaptive Mixed Unitary Designs. In this section, we generalize the notion of mixed unitary designs to algorithms which may query a unitary (and possibly its inverse) adaptively, rather than in parallel.

Definition 2.6 (Adaptive Mixed Unitary (p,q)-Design)**.** *Let ν be an ensemble of unitary operators over $\mathbb{C}^d$. Then, ν is an adaptive unitary (p,q)-design if, for every single-bit output (possibly adaptive) quantum algorithm $\mathcal{A}$ making at most p many queries to a unitary and q many queries to its adjoint,*

$$\Pr\left[1 \leftarrow \mathcal{A}^{U,U^\dagger}(1^{\lceil \log d \rceil}) \,:\, U \sim \nu\right] = \Pr\left[1 \leftarrow \mathcal{A}^{U,U^\dagger}(1^{\lceil \log d \rceil}) \,:\, U \sim \mathrm{U}(d)\right].$$

We say that ν is an adaptive mixed unitary t-design if the property above holds for any adaptive quantum query algorithm $\mathcal{A}$ which submits no more than t queries to either U or $U^\dagger$.

2.3 Pseudorandom Unitaries

Pseudorandom unitaries are ensembles of unitary operators that look indistinguishable from Haar random unitaries for all computationally bounded observers. These ensembles of unitaries have been first proposed in [JLS18], and have only very recently been constructed assuming the existence of post-quantum one-way functions [MPSY24, MH24]. We give a formal definition below.

Definition 2.7 (Pseudorandom Unitary)**.** *Let λ be the security parameter, $n := n(\lambda) \in \mathbb{N}$ be some polynomial, and $d = 2^n$. An infinite sequence $\mathfrak{U} = \{\mathfrak{U}_n\}_{n\in\mathbb{N}}$ of n-qubit unitary ensembles $\mathfrak{U}_n = \{U_{\theta,n}\}_{\theta\in\{0,1\}^\lambda}$ is a pseudorandom unitary if it satisfies the following conditions:*

- *(**Efficient computation**) For all λ, n, there exists a polynomial-time quantum algorithm $\mathcal{Q}$ such that for all keys $\theta \in \{0,1\}^\lambda$, and any $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$, it holds that*

$$\mathcal{Q}(\theta, |\psi\rangle) = U_{\theta,n} |\psi\rangle \ .$$

- *(**Pseudorandomness**) The unitary $U_{\theta,n}$, for a random key $\theta \sim \{0,1\}^\lambda$, is computationally indistinguishable from a Haar random unitary $U \sim \mathrm{U}(d)$. In other words, for any QPT algorithm $\mathcal{A}$, it holds that*

$$\left| \Pr_{\theta\sim\{0,1\}^\lambda}[\mathcal{A}^{U_{\theta,n},U_{\theta,n}^\dagger}(1^\lambda,1^n)=1] - \Pr_{U\sim\mathrm{U}(d)}[\mathcal{A}^{U_{\theta,n},U_{\theta,n}^\dagger}(1^\lambda,1^n)=1] \right| \leq \mathsf{negl}(\lambda).$$

Remark 3. *We note that this definition of pseudorandom unitary is quite strong; the adversary $\mathcal{A}$ is free to make its queries adaptively, and moreover it is allowed to query both U and $U^\dagger$, in analogy to strong pseudorandom permutations. This notion was constructed in recent work by Ma and Huang [MH24].*

2.4 Operator Norm Bounds

In this section, we lay out some tools for bounding the operator norm $\|\mathbf{A}\|_\infty$ of operators $A \in \mathbb{C}^{d\times d}$. For matrices $\mathbf{A}, \mathbf{B}$ of the same dimensions, we use $\mathbf{A} \circ \mathbf{B}$ to denote their entrywise product.

Lemma 2.8 (Well-known)**.** *For any matrix $\mathbf{A} \in \mathbb{C}^{d_1\times d_2}$, we have*

$$\|\mathbf{A}\|_\infty = \sqrt{\lambda_{\max}(\mathbf{A}^\dagger\mathbf{A})} = \sqrt{\lambda_{\max}(\mathbf{A}\mathbf{A}^\dagger)} = \max\{\|\mathbf{A}x\|_2 : \|x\|_2 = 1\}.$$

Moreover, if $\mathbf{A}$ has rank ≤ 1, then we have $\lambda_{\max}(\mathbf{A}^\dagger\mathbf{A}) = \mathrm{Tr}\left[\mathbf{A}^\dagger\mathbf{A}\right]$.

Lemma 2.9 (Well-known)**.** *For any pair of matrices $\mathbf{A} \in \mathbb{C}^{d_1 \times d_2}$ and $\mathbf{A}' \in \mathbb{C}^{d_1' \times d_2'}$ such that $\mathbf{A}'$ is a submatrix of $\mathbf{A}$, we have $\|\mathbf{A}'\|_\infty \leq \|\mathbf{A}\|_\infty$.*

Lemma 2.10 (Well-known)**.** *For $\mathbf{A} \in \mathbb{C}^{d_1 \times d_2}$ and $\mathbf{B} \in \mathbb{C}^{d_3 \times d_4}$, we have $\|\mathbf{A} \otimes \mathbf{B}\|_\infty = \|\mathbf{A}\|_\infty \cdot \|\mathbf{B}\|_\infty$.*

Lemma 2.11. *Let $\mathbf{A}_1, \ldots, \mathbf{A}_k \in \mathbb{C}^{d \times d}$ be unitary matrices with $k \geq 2$. Then, the rows and columns of $\mathbf{C} = \mathbf{A}_1 \circ \ldots \circ \mathbf{A}_k$ all have ℓ_1 norm ≤ 1.*

Proof. In the case of rows, we have:

$$\begin{aligned}
\sum_{j=1}^{d} |C_{i,j}| &= \sum_{j=1}^{d} |A_{1;(i,j)}| \cdot \ldots \cdot |A_{k;(i,j)}| \\
&\leq \sum_{j=1}^{d} |A_{1;(i,j)}| \cdot |A_{2;(i,j)}| \text{ (all entries of a unitary are } \leq 1) \\
&\leq \sqrt{\left(\sum_{j=1}^{d} |A_{1;(i,j)}|^2\right) \cdot \left(\sum_{j=1}^{d} |A_{2;(i,j)}|^2\right)} \text{ (Cauchy-Schwarz)} \\
&= 1.
\end{aligned}$$

The case of columns is analogous. □

Lemma 2.12. *Let $\mathbf{C} \in \mathbb{C}^{d_1 \times d_2}$ be such that the ℓ_1 norm of each row is $\leq a$ and the ℓ_1 norm of each column is $\leq b$. Then $\|\mathbf{C}\|_\infty \leq \sqrt{ab}$.*

Proof. For any row i of $\mathbf{C}^\dagger \mathbf{C} \in \mathbb{C}^{d_2 \times d_2}$, we have:

$$\begin{aligned}
\sum_{j=1}^{d_2} |(\mathbf{C}^\dagger \mathbf{C})_{i,j}| &= \sum_{j=1}^{d_2} |\sum_{k=1}^{d_1} C_{i,k}^\dagger C_{k,j}| \\
&\leq \sum_{j=1}^{d_2} \sum_{k=1}^{d_1} |C_{k,i}||C_{k,j}| \\
&\leq a \cdot \sum_{k=1}^{d} |C_{k,i}| \\
&\leq ab.
\end{aligned}$$

Since the maximum eigenvalue of a square matrix is at most the maximum ℓ_1 norm of its rows, we have $\left\|\mathbf{C}^\dagger \mathbf{C}\right\|_\infty \leq ab \Rightarrow \|\mathbf{C}\|_\infty \leq \sqrt{ab}$. □

We also define and state some simple properties of matrix inner products:

Definition 2.13. *For matrices $\mathbf{A}, \mathbf{B} \in \mathbb{C}^{d_1 \times d_2}$, define the inner product*

$$\langle \mathbf{A}, \mathbf{B} \rangle = \sum_{i \in [d_1], j \in [d_2]} \overline{A_{i,j}} \cdot B_{i,j} = \mathrm{Tr}\left[\mathbf{A}^\dagger \mathbf{B}\right].$$

We also define the Frobenius norm $\|\mathbf{A}\|_F = \sqrt{\langle \mathbf{A}, \mathbf{A} \rangle}$.

Lemma 2.14. *For matrices $\mathbf{A}, \mathbf{B} \in \mathbb{C}^{d \times d}$, we have:*

- *(Cauchy-Schwarz)* $|\langle \mathbf{A}, \mathbf{B} \rangle| \leq \|\mathbf{A}\|_F \cdot \|\mathbf{B}\|_F$.
- *(Well-known) If $\mathbf{A}$ is Hermitian and $\mathbf{B}$ is Hermitian PSD, then we have* $|\langle \mathbf{A}, \mathbf{B} \rangle| \leq \|\mathbf{A}\|_\infty \cdot \mathrm{Tr}[\mathbf{B}]$.

2.4.1 Blockwise Tensor Products

This section is devoted to stating and proving Theorem 2.15, which will serve as our central linear algebraic workhorse. We will make some comments about this theorem and its proof at the end of this section. We will then present some straightforward consequences of this theorem in Section 2.4.2, which we will use directly when analyzing $t \mapsto t+1$ cloning games.

Theorem 2.15. *Let R, C be positive integers. Let $r_1, r_2, \ldots, r_R, r'_1, r'_2, \ldots, r'_R, c_1, \ldots, c_C, c'_1, \ldots, c'_C$ be positive integers. For each $i \in [R], k \in [C]$, let $\mathbf{A}_{i,k} \in \mathbb{C}^{r_i \times c_k}$ and $\mathbf{B}_{i,k} \in \mathbb{C}^{r'_i \times c'_k}$ be matrices. Additionally, for each $i \in [R], k \in [C]$, let $\gamma_{i,k} \in \mathbb{C}$ be a scalar of magnitude at most 1, i.e. $|\gamma_{i,k}| \leq 1$.*

Define the following block matrices:

$$\mathbf{A} := \begin{bmatrix} \mathbf{A}_{1,1} & \ldots & \mathbf{A}_{1,C} \\ \vdots & \ddots & \vdots \\ \mathbf{A}_{R,1} & \ldots & \mathbf{A}_{R,C} \end{bmatrix} \in \mathbb{C}^{(r_1+\ldots+r_R)\times(c_1+\ldots+c_C)}$$

$$\mathbf{B} := \begin{bmatrix} \mathbf{B}_{1,1} & \ldots & \mathbf{B}_{1,C} \\ \vdots & \ddots & \vdots \\ \mathbf{B}_{R,1} & \ldots & \mathbf{B}_{R,C} \end{bmatrix} \in \mathbb{C}^{(r'_1+\ldots+r'_R)\times(c'_1+\ldots+c'_C)}$$

$$\mathbf{M} := \begin{bmatrix} \gamma_{1,1}\mathbf{A}_{1,1} \otimes \mathbf{B}_{1,1} & \ldots & \gamma_{1,C}\mathbf{A}_{1,C} \otimes \mathbf{B}_{1,C} \\ \vdots & \ddots & \vdots \\ \gamma_{R,1}\mathbf{A}_{R,1} \otimes \mathbf{B}_{R,1} & \ldots & \gamma_{R,C}\mathbf{A}_{R,C} \otimes \mathbf{B}_{R,C} \end{bmatrix} \in \mathbb{C}^{(r_1 r'_1+\ldots+r_R r'_R)\times(c_1 c'_1+\ldots+c_C c'_C)}.$$

Suppose both of the following conditions hold:

1. $\|\mathbf{A}\|_\infty \leq 1$.
2. *Each block column of $\mathbf{B}$ has operator norm ≤ 1 i.e. for all $k \in [C]$, we have*

$$\left\| \begin{bmatrix} \mathbf{B}_{1,k} \\ \vdots \\ \mathbf{B}_{R,k} \end{bmatrix} \right\|_\infty \leq 1.$$

Then, it holds that $\|\mathbf{M}\|_\infty \leq 1$.

High-level proof idea. The main idea is as follows: it suffices to show that for any unit vectors x, y of the right dimensions that $|x^\dagger \mathbf{M} y| \leq 1$. As a function of B, $x^\dagger \mathbf{M} y$ is linear. We can hence express this as the inner product of $\mathbf{B}$ with some other matrix. It turns out that this matrix has a simple form; reformulating the problem in these terms will allow us to use the standard bounds stated in Lemma 2.14.

Notation. We begin by setting up some notation. If we have a sequence of matrices $\{\mathbf{A}_I : I \in \mathcal{I}\}$ indexed by I with rows and columns indexed by $r \in \mathcal{R}$ and $c \in \mathcal{C}$, we use $(\mathbf{A}_I)_{r;c}$ to denote the entry in row r and column c of matrix $\mathbf{A}_I$.

Now let us define $\widetilde{\mathbf{B}}$ as follows, and let $\mathbf{B}'$ be its entrywise conjugate:

$$\begin{aligned}\widetilde{\mathbf{B}} &:= \begin{bmatrix} \widetilde{\mathbf{B}_{1,1}} & \dots & \widetilde{\mathbf{B}_{1,C}} \\ \vdots & \ddots & \vdots \\ \widetilde{\mathbf{B}_{R,1}} & \dots & \widetilde{\mathbf{B}_{R,C}} \end{bmatrix} \\ &= \begin{bmatrix} \gamma_{1,1}\mathbf{B}_{1,1} & \dots & \gamma_{1,C}\mathbf{B}_{1,C} \\ \vdots & \ddots & \vdots \\ \gamma_{R,1}\mathbf{B}_{R,1} & \dots & \gamma_{R,C}\mathbf{B}_{R,C} \end{bmatrix} \in \mathbb{C}^{(r'_1+\ldots+r'_R)\times(c'_1+\ldots+c'_C)}.\end{aligned}$$

As outlined earlier, it suffices to show for any unit vectors $x \in \mathbb{C}^{r_1r'_1+\ldots+r_Rr'_R}$ and $y \in \mathbb{C}^{c_1c'_1+\ldots+c_Cc'_C}$ that $|x^\dagger \mathbf{M} y| \le 1$. We index the entries of x by an index $i \in [R]$ and then values $j \in [r_i]$ and $j' \in [r'_i]$. We similarly index the entries of y by (k, l, l'). We can also apply this same indexing to the rows and columns of $\mathbf{M}$. Thus for $i \in [R]$ and $k \in [C]$, we can define $\mathbf{M}_{i,k} \in \mathbb{C}^{r_ir'_i\times c_kc'_k}$ by $\mathbf{M}_{i,k} = \gamma_{i,k}\mathbf{A}_{i,k} \otimes \mathbf{B}_{i,k}$ (i.e. this is one block of $\mathbf{M}$).

For each $i \in [R]$, let $\mathbf{X}_i \in \mathbb{C}^{r_i\times r'_i}$ be defined by $(\mathbf{X}_i)_{j;j'} = x_{(i,j,j')}$. Similarly define $\mathbf{Y}_k \in \mathbb{C}^{c_k\times c'_k}$ for each $k \in [C]$. We also defined the following matrices:

$$\mathbf{X} := \begin{bmatrix} \mathbf{X}_1 & 0 & \dots & 0 \\ 0 & \mathbf{X}_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \mathbf{X}_R \end{bmatrix} \in \mathbb{C}^{(r_1+\ldots+r_R)\times(r'_1+\ldots+r'_R)}$$

$$\mathbf{Y} := \begin{bmatrix} \mathbf{Y}_1 & 0 & \dots & 0 \\ 0 & \mathbf{Y}_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \mathbf{Y}_C \end{bmatrix} \in \mathbb{C}^{(c_1+\ldots+c_C)\times(c'_1+\ldots+c'_C)}.$$

It is straightforward to see that $\|\mathbf{X}\|_F = \|\mathbf{Y}\|_F = 1$, since the nonzero entries in $\mathbf{X}$ are exactly the same as in x, and similarly for Y and y.

Finally, over $\mathbb{C}_{c'_1+\ldots+c'_C}$, for each $k \in [C]$ define the projector Π'_k to be onto the natural c'_k coordinates (more precisely, all coordinates z such that $c'_1 + \ldots + c'_{k-1} < z \le c'_1 + \ldots + c'_k$. Note then that the block-diagonal structure of Y implies that:

$$\mathbf{Y}^\dagger\mathbf{Y} = \sum_{k\in[C]} \Pi'_k\mathbf{Y}^\dagger\mathbf{Y}\Pi'_k. \tag{5}$$

Rewriting $x^\dagger\mathbf{M}\,y$ as a linear function of $\mathbf{B}'$. We now show that $x^\dagger\mathbf{M}\,y$ can be written as a linear function of B'. This is captured in the following lemma:

Lemma 2.16. *We have*

$$x^\dagger\,\mathbf{M}\,y = \mathrm{Tr}\left[\mathbf{X}^\dagger\mathbf{A}\mathbf{Y}(\mathbf{B}')^\dagger\right].$$

Proof. We proceed as follows:

$$\begin{aligned}
x^\dagger \mathbf{M}\, y &= \sum_{i\in[R],k\in[C]} \sum_{j\in[r_i],j'\in[r'_i],l\in[c_k],l'\in[c'_k]} \overline{x_{(i,j,j')}}\, (\mathbf{M}_{i,k})_{(j,j');(l,l')}\, y_{(k,l,l')} \\
&= \sum_{i\in[R],k\in[C]} \sum_{j\in[r_i],j'\in[r'_i],l\in[c_k],l'\in[c'_k]} \overline{x_{(i,j,j')}} \left(\mathbf{A}_{i,k} \otimes \widetilde{\mathbf{B}_{i,k}}\right)_{(j,j');(l,l')} y_{(k,l,l')} \\
&= \sum_{i\in[R],k\in[C]} \sum_{j\in[r_i],j'\in[r'_i],l\in[c_k],l'\in[c'_k]} \overline{x_{(i,j,j')}}\, (\mathbf{A}_{i,k})_{j;l} \left(\widetilde{\mathbf{B}}_{i,k}\right)_{j';l'} y_{(k,l,l')} \\
&= \sum_{i\in[R],k\in[C]} \sum_{j'\in[r'_i],l'\in[c'_k]} \left(\widetilde{\mathbf{B}}_{i,k}\right)_{j';l'} \cdot \left(\sum_{j\in[r_i],l\in[c_k]} \overline{x_{(i,j,j')}}\, (\mathbf{A}_{i,k})_{j;l}\, y_{(k,l,l')} \right) \\
&= \sum_{i\in[R],k\in[C]} \sum_{j'\in[r'_i],l'\in[c'_k]} \left(\widetilde{\mathbf{B}}_{i,k}\right)_{j';l'} \cdot \left(\sum_{j\in[r_i],l\in[c_k]} \overline{(\mathbf{X}_i)_{j;j'}}\, (\mathbf{A}_{i,k})_{j;l}\, (\mathbf{Y}_k)_{l;l'} \right) \\
&= \sum_{i\in[R],k\in[C]} \sum_{j'\in[r'_i],l'\in[c'_k]} \left(\widetilde{\mathbf{B}}_{i,k}\right)_{j';l'} \cdot \left(\sum_{j\in[r_i],l\in[c_k]} \left(\mathbf{X}_i^\dagger\right)_{j';j}\, (\mathbf{A}_{i,k})_{j;l}\, (\mathbf{Y}_k)_{l;l'} \right) \\
&= \sum_{i\in[R],k\in[C]} \sum_{j'\in[r'_i],l'\in[c'_k]} \left(\widetilde{\mathbf{B}}_{i,k}\right)_{j';l'} \cdot \left(\mathbf{X}_i^\dagger \mathbf{A}_{i,k} \mathbf{Y}_k\right)_{j';l'} \\
&= \sum_{i\in[R],k\in[C]} \sum_{j'\in[r'_i],l'\in[c'_k]} \widetilde{\mathbf{B}}_{(i,j');(k,l')} \cdot (\mathbf{X}^\dagger \mathbf{A} \mathbf{Y})_{(i,j');(k,l')} \\
&= \langle \mathbf{B}', \mathbf{X}^\dagger \mathbf{A} \mathbf{Y} \rangle \;=\; \mathrm{Tr}\left[(\mathbf{B}')^\dagger \mathbf{X}^\dagger \mathbf{A} \mathbf{Y}\right] \;=\; \mathrm{Tr}\left[\mathbf{X}^\dagger \mathbf{A} \mathbf{Y} (\mathbf{B}')^\dagger\right].
\end{aligned}$$

□

Bounding the operator norm of $B'\Pi'_k$. Our second ingredient will be the following straightforward observation:

Lemma 2.17. *For any $k \in [C]$, we have $\|\mathbf{B}'\Pi'_k\|_\infty \leq 1$.*

Proof. After removing zero columns, $\mathbf{B}'\Pi'_k$ is just the following block matrix:

$$\begin{bmatrix} \overline{\gamma_{1,k}}\, \overline{\mathbf{B}_{1,k}} \\ \vdots \\ \overline{\gamma_{R,k}}\, \overline{\mathbf{B}_{R,k}} \end{bmatrix}.$$

This is the result of taking $\begin{bmatrix} \mathbf{B}_{1,k} \\ \vdots \\ \mathbf{B}_{R,k} \end{bmatrix}$, multiplying each row by a scalar of magnitude ≤ 1, then conjugating all entries. The latter two operations do not increase operator norm, and we are assuming that the starting matrix has operator norm ≤ 1. The conclusion follows. □

Completing the proof. We are now ready to complete the proof of Theorem 2.15; this will follow from the standard inequalities stated in Lemma 2.14, in addition to using the block-diagonal structure of Y (as in Equation (5)).

Proof of Theorem 2.15. Starting from Lemma 2.16, we have:

$$\begin{aligned}
|x^\dagger \mathbf{M}\, y| &= \left|\mathrm{Tr}\left[\mathbf{X}^\dagger \mathbf{A}\mathbf{Y}(\mathbf{B}')^\dagger\right]\right| \\
&\leq \|\mathbf{X}\|_F \cdot \left\|\mathbf{A}\mathbf{Y}(\mathbf{B}')^\dagger\right\|_F \text{ (Lemma 2.14)} \\
&= \left\|\mathbf{A}\mathbf{Y}(\mathbf{B}')^\dagger\right\|_F.
\end{aligned}$$

Continuing from here, we have:

$$\begin{aligned}
\left\|\mathbf{A}\mathbf{Y}(\mathbf{B}')^\dagger\right\|_F^2 &= \mathrm{Tr}\left[\mathbf{B}'\mathbf{Y}^\dagger \mathbf{A}^\dagger \mathbf{A}\mathbf{Y}(\mathbf{B}')^\dagger\right] \\
&= \mathrm{Tr}\left[\mathbf{A}^\dagger \mathbf{A}\mathbf{Y}(\mathbf{B}')^\dagger \mathbf{B}'\mathbf{Y}^\dagger\right] \\
&\leq \mathrm{Tr}\left[\mathbf{Y}(\mathbf{B}')^\dagger \mathbf{B}'\mathbf{Y}^\dagger\right] \text{ (Lemma 2.14; } \|\mathbf{A}\|_\infty \leq 1) \\
&= \mathrm{Tr}\left[\mathbf{Y}^\dagger \mathbf{Y}(\mathbf{B}')^\dagger \mathbf{B}'\right] \\
&= \sum_{k\in[C]} \mathrm{Tr}\left[\Pi'_k \mathbf{Y}^\dagger \mathbf{Y}\Pi'_k (\mathbf{B}')^\dagger \mathbf{B}'\right] \text{ (Equation (5))} \\
&= \sum_{k\in[C]} \mathrm{Tr}\left[\left(\Pi'_k \mathbf{Y}^\dagger \mathbf{Y}\Pi'_k\right)\left(\Pi'_k (\mathbf{B}')^\dagger \mathbf{B}'\Pi'_k\right)\right] \\
&\leq \sum_{k\in[C]} \mathrm{Tr}\left[\Pi'_k \mathbf{Y}^\dagger \mathbf{Y}\Pi'_k\right] \cdot \left\|\Pi'_k (\mathbf{B}')^\dagger \mathbf{B}'\Pi'_k\right\|_\infty \text{ (Lemma 2.14)} \\
&\leq \sum_{k\in[C]} \mathrm{Tr}\left[\Pi'_k \mathbf{Y}^\dagger \mathbf{Y}\Pi'_k\right] \text{ (Lemma 2.17)} \\
&= \sum_{k\in[C]} \mathrm{Tr}\left[\Pi'_k \mathbf{Y}^\dagger \mathbf{Y}\right] \\
&= \mathrm{Tr}\left[\mathbf{Y}^\dagger \mathbf{Y}\right] \\
&= \|\mathbf{Y}\|_F^2 \\
&= 1,
\end{aligned}$$

thus completing the proof of the theorem. □

Discussion. Given the simplicity of the statement of Theorem 2.15, one might wonder why our proof is so involved. Here, we present some justification that this theorem is actually quite strong, and discuss some obstacles to more intuitive proof strategies. First, we note that our theorem captures some simple special cases:

- When $R = C = 1$, this is immediate from Lemma 2.10.

- When $\gamma_{i,k} = 1$ for all i, k (or more generally $\gamma_{i,k}$ is constant) and $\|\mathbf{B}\|_\infty \leq 1$, this can be shown by noting that the matrix $\mathbf{M}$ would be a submatrix of $\mathbf{A} \otimes \mathbf{B}$, and then appealing to Lemma 2.10. (We rigorously argue this fact as part of the proof of Lemma 2.19.)

  However, this argument completely breaks down if $\gamma_{i,k}$ is allowed to vary between blocks.

- When $r_i = r'_i = c_k = c'_k = 1$ for all i, k, this boils down to bounding the operator norm of any complex $R \times C$ matrix with the entry in row i and column k having magnitude equal to $|A_{i;k} B_{i;k}|$ (noting that in this setting $A_{i;k}, B_{i;k}$ are scalars). This is not straightforward but still easier to handle; one can argue by Cauchy-Schwarz that the rows and columns of such a matrix must have ℓ_1 norm ≤ 1, and it is well-known that such a matrix must have operator norm ≤ 1 (see Lemmas 2.11 and 2.12 for details).

  This argument also breaks down as soon as the block matrices $A_{i,k}, B_{i,k}$ are not just scalars; the ℓ_1 norms of the rows and columns of M will end up growing polynomially in $\max(r_1, \ldots, r_R, r'_1, \ldots, r'_R, c_1, \ldots, c_C, c'_1, \ldots, c'_C)$ in the worst case. (Jumping ahead, in the setting of oracular cloning games, this would yield a bound that degrades exponentially in the number of ancilla qubits that each adversary is allowed to use, which is of course undesirable.)

One could imagine "interpolating" between these two techniques by considering the operator norm of each block of $\mathbf{M}$ individually, and using this to obtain a bound on $\|\mathbf{M}\|_\infty$. Perhaps surprisingly, this is also *provably* insufficient. Suppose $R = C = n$ for some n, and $r_i = r'_i = c_k = c'_k = n$ for all i, k. Then let us take $\mathbf{A}, \mathbf{B}$ to be $n^2 \times n^2$ permutation matrices with exactly one 1 in each block. Now we will have $\|\mathbf{A}_{i,k}\|_\infty = \|\mathbf{B}_{i,k}\|_\infty = 1 \Rightarrow \|\mathbf{A}_{i,k} \otimes \mathbf{B}_{i,k}\|_\infty = 1$ for all i, k. However, there exist $n \times n$ block matrices (i.e. containing n^2 blocks in total) with each block having operator norm 1, but where the overall matrix has operator norm growing with n; one such example is the $n \times n$ all 1's matrix (appropriately padded with zero rows and columns to obtain the right dimensions). This counterexample implies that just considering the operator norm of each block of $\mathbf{M}$ is too lossy.

Thus Theorem 2.15 is quite strong and there are natural barriers to proof strategies that might feel more simple and intuitive. The proof we have presented is the simplest one that we are aware of.

2.4.2 Consequences

We now state some corollaries of Theorem 2.15 that we will later directly apply when bounding the operator norms relevant to cloning games in Section 5.3.

Lemma 2.18. *Let $\mathbf{A}_1, \ldots, \mathbf{A}_k$ be block matrices of d columns. More formally, for each $i \in [k]$ set*

$$\mathbf{A}_i = \begin{bmatrix} \mathbf{A}_{i,1} & \ldots & \mathbf{A}_{i,d} \end{bmatrix},$$

for some block matrices $\mathbf{A}_{i,1}, \ldots, \mathbf{A}_{i,d}$ that have the same number of rows but not necessarily the same number of columns. (Note that we do not require $\mathbf{A}_{i,1}$ and $\mathbf{A}_{j,1}$ to have the same number of rows when $i \neq j$.) Assume the following preconditions:

1. *For all $i \in [k]$ and $j \in [d]$, we have $\|\mathbf{A}_{i,j}\|_\infty \leq 1$; and*
2. *There exists some $i \in [k]$ such that $\|\mathbf{A}_i\|_\infty \leq 1$.*

Let

$$\mathbf{A} = \begin{bmatrix} \bigotimes_{i=1}^k \mathbf{A}_{i,1} & \bigotimes_{i=1}^k \mathbf{A}_{i,2} & \ldots & \bigotimes_{i=1}^k \mathbf{A}_{i,d} \end{bmatrix}$$

be defined as a "block column-wise tensor product" of $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_d$. Then $\|\mathbf{A}\|_\infty \leq 1$.

Proof. Firstly, if $k = 1$ then we will have $\mathbf{A} = \mathbf{A}_1$ so the conclusion will follow from the second precondition. From now on, assume that $k \geq 2$. Also, by symmetry, let us assume without loss of generality that $\|\mathbf{A}_1\|_\infty \leq 1$.

Now define the matrix $\mathbf{M}$ as follows:

$$\mathbf{M} = \begin{bmatrix} \bigotimes_{i=2}^k \mathbf{A}_{i,1} & \bigotimes_{i=2}^k \mathbf{A}_{i,2} & \dots & \bigotimes_{i=2}^k \mathbf{A}_{i,d} \end{bmatrix}.$$

Notice that, for each $j \in [d]$, the jth block column of $\mathbf{M}$ has operator norm equal to $\prod_{i=1}^k \|\mathbf{A}_{i,j}\|_\infty \leq 1$. Since we also have $\|\mathbf{A}_1\|_\infty \leq 1$, we can apply Theorem 2.15 to $\mathbf{A}_1$ and $\mathbf{M}$ (with $R = 1$, $C = d$, and $\gamma_{i,j} = 1$ for all i, j) to immediately obtain that $\|A\|_\infty \leq 1$, as desired. □

Lemma 2.19. *Let R, C be positive integers. Let $r_1, \dots, r_R, c_1, \dots, c_C$ be positive integers. Fix some integer $d \geq 2$. For each $t \in [d], i \in [R], k \in [C]$, let $\mathbf{A}_{t,i,k} \in \mathbb{C}^{r_i \times c_k}$ be a matrix. Additionally, for each $i \in [R], k \in [C]$, let $\gamma_{i,k} \in \mathbb{C}$ be a scalar of magnitude at most 1 i.e. $|\gamma_{i,k}| \leq 1$. Then define the following block matrices:*

$$\mathbf{A}_t := \begin{bmatrix} \mathbf{A}_{t,1,1} & \dots & \mathbf{A}_{t,1,C} \\ \vdots & \ddots & \vdots \\ \mathbf{A}_{t,R,1} & \dots & \mathbf{A}_{t,R,C} \end{bmatrix} \in \mathbb{C}^{(r_1+\dots+r_R)\times(c_1+\dots+c_C)}, \text{ for each } t \in [d]$$

$$\mathbf{M} := \begin{bmatrix} \gamma_{1,1} \bigotimes_{t=1}^d \mathbf{A}_{t,1,1} & \dots & \gamma_{1,C} \bigotimes_{t=1}^d \mathbf{A}_{t,1,C} \\ \vdots & \ddots & \vdots \\ \gamma_{R,1} \bigotimes_{t=1}^d \mathbf{A}_{t,R,1} & \dots & \gamma_{R,C} \bigotimes_{t=1}^d \mathbf{A}_{t,R,C} \end{bmatrix} \in \mathbb{C}^{(r_1^d+\dots+r_R^d)\times(c_1^d+\dots+c_C^d)}.$$

Suppose that for all $t \in [d]$, we have $\|\mathbf{A}_t\|_\infty \leq 1$. Then $\|\mathbf{M}\|_\infty \leq 1$. (Note that the $d = 2$ case is immediate from Theorem 2.15.)

Proof. Define the matrix

$$\mathbf{B} = \begin{bmatrix} \bigotimes_{t=2}^d \mathbf{A}_{t,1,1} & \dots & \bigotimes_{t=2}^d \mathbf{A}_{t,1,C} \\ \vdots & \ddots & \vdots \\ \bigotimes_{t=2}^d \mathbf{A}_{t,R,1} & \dots & \bigotimes_{t=2}^d \mathbf{A}_{t,R,C} \end{bmatrix} \in \mathbb{C}^{(r_1^{d-1}+\dots+r_R^{d-1})\times(c_1^{d-1}+\dots+c_C^{d-1})}.$$

We claim that $\mathbf{B}$ is a submatrix of $\mathbf{A}_2 \otimes \dots \otimes \mathbf{A}_d$. This is intuitive, but nevertheless we justify this rigorously before completing the proof. To this end, let us index each row of each A_t by an index $i \in [R]$ together with an index $\alpha \in [i]$. Similarly, we can index each column by an index $k \in [C]$ together with $\beta \in [k]$. We can hence index rows of $\mathbf{A}_2 \otimes \dots \otimes \mathbf{A}_d$ by $(i_2, \dots, i_t, \alpha_2, \dots, \alpha_d)$ and similarly the columns by $(k_2, \dots, k_d, \beta_2, \dots, \beta_d)$; so that:

$$(\mathbf{A}_2 \otimes \dots \otimes \mathbf{A}_d)_{(i_2,\dots,i_d,\alpha_2,\dots,\alpha_d);(k_2,\dots,k_d,\beta_2,\dots,\beta_d)} = \prod_{t=2}^d (\mathbf{A}_{t,i_t,k_t})_{\alpha_t;\beta_t}.$$

On the other hand, we can index the rows of $\mathbf{B}$ by one index $i \in [R]$ and indices $\alpha_2, \dots, \alpha_d \in [i]$, and similarly the columns by $k, \beta_2, \dots, \beta_d$, so that:

$$B_{(i,\alpha_2,\dots,\alpha_d);(k,\beta_2,\dots,\beta_d)} = \prod_{t=2}^d (\mathbf{A}_{t,i,k})_{\alpha_t;\beta_t}.$$

Game 1 (Monogamy of Entanglement Game)**.**
A monogamy of entanglement game $\mathsf{G} = (\mathcal{H}_{\mathsf{A}}, \Theta, \mathcal{X}, \{\mathbf{A}_x^\theta\}_{\theta\in\Theta, x\in\mathcal{X}})$ *for a quantum strategy* $\mathsf{S} = (\mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{C}}, \rho_{\mathsf{ABC}}, \{\mathbf{B}_x^\theta\}_{\theta\in\Theta, x\in\mathcal{X}}, \{\mathbf{C}_x^\theta\}_{\theta\in\Theta, x\in\mathcal{X}})$ *is the following game between a trusted referee (called Alice) and two collaborating players (called Bob and Charlie):*

1. *(**Setup phase**) Bob and Charlie prepare a tripartite quantum state* $\rho \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}})$*. They send register* A *to Alice, and hold onto registers* B *and* C*, respectively. Afterwards, they are no longer allowed to communicate for the remainder of the game.*
2. *(**Question phase**) Alice first samples a uniformly random question* $\theta \sim \Theta$*, and then applies the corresponding measurement* $\{\mathbf{A}_x^\theta\}_{x\in\mathcal{X}}$ *to her register* A*. Afterwards, Alice announces the question* θ *to both Bob and Charlie.*
3. *(**Answer phase**) Bob and Charlie independently output a guess for Alice's outcome by applying the measurements* $\{\mathbf{B}_x^\theta\}_{x\in\mathcal{X}}$ *and* $\{\mathbf{C}_x^\theta\}_{x\in\mathcal{X}}$ *to their registers* B *and* C*, respectively.*
4. *(**Outcome phase**) Bob and Charlie win if they both guess Alice's outcome correctly.*

Figure 4: A monogamy of entanglement game.

It is now clear that $\mathbf{B}$ can be obtained by restricting $\mathbf{A}_2 \otimes \ldots \otimes \mathbf{A}_d$ to rows where $i_2 = \ldots = i_d$ and columns where $k_2 = \ldots = k_d$. This establishes our claim.

We now complete the proof as follows. By Lemma 2.9, our claim implies that

$$\|\mathbf{B}\|_\infty \leq \prod_{t=2}^{d} \|\mathbf{A}_t\|_\infty \leq 1.$$

The conclusion now follows by applying Theorem 2.15 to $\mathbf{A}_1$ and $\mathbf{B}$ for the choices of R, C, and scalars $\gamma_{i,k}$. This proves the claim. □

3 Monogamy of Entanglement and Oracular Cloning Games

In this section, we formally define monogamy of entanglement games, as well as the closely related notion of (oracular) cloning games, which is the central object of study in this work.

3.1 Monogamy of Entanglement Games

A monogamy of entanglement game [TFKW13] is an interactive game which is played by three players: a trusted referee called Alice, and two colluding and adversarial parties Bob and Charlie.

Definition 3.1 (Monogamy of Entanglement Game)**.** *A monogamy of entanglement (MOE) game is specified by a tuple* $\mathsf{G} = (\mathcal{H}_{\mathsf{A}}, \Theta, \mathcal{X}, \{\mathbf{A}_x^\theta\}_{\theta\in\Theta, x\in\mathcal{X}})$ *which consists of the following elements:*

- *A finite dimensional Hilbert space* $\mathcal{H}_{\mathsf{A}}$ *corresponding to a register* A *that Alice holds;*
- *A finite set* Θ *corresponding to the set of possible questions;*

- *A finite set $\mathcal{X}$ corresponding to the set of all possible answers;*
- *A set of positive operator-valued measurements $\left\{\mathbf{A}_x^\theta\right\}_{\theta\in\Theta,x\in\mathcal{X}}$ to be performed on Alice's system.*

Definition 3.2 (Quantum Strategy)**.** *A quantum strategy $\mathsf{S} = (\mathcal{H}_\mathsf{B}, \mathcal{H}_\mathsf{C}, \rho_\mathsf{ABC}, \{\mathbf{B}_x^\theta\}_{\theta\in\Theta,x\in\mathcal{X}}, \{\mathbf{C}_x^\theta\}_{\theta\in\Theta,x\in\mathcal{X}})$ for a monogamy of entanglement game $\mathsf{G} = (\mathcal{H}_\mathsf{A}, \Theta, \mathcal{X}, \{\mathbf{A}_x^\theta\}_{\theta\in\Theta,x\in\mathcal{X}})$ consists of*

- *A finite dimensional Hilbert space $\mathcal{H}_\mathsf{B}$ corresponding to a register B that Bob holds;*
- *A finite dimensional Hilbert space $\mathcal{H}_\mathsf{C}$ corresponding to a register C that Charlie holds;*
- *A tripartite quantum state $\rho \in \mathcal{D}(\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B} \otimes \mathcal{H}_\mathsf{C})$;*
- *A set of positive operator-valued measurements $\left\{\mathbf{B}_x^\theta\right\}_{\theta\in\Theta,x\in\mathcal{X}}$ to be performed on Bob's system.*
- *A set of positive operator-valued measurements $\left\{\mathbf{C}_x^\theta\right\}_{\theta\in\Theta,x\in\mathcal{X}}$ to be performed on Charlie's system.*

Definition 3.3 (Value of a Monogamy Game)**.** *Let $\mathsf{G} = (\mathcal{H}_\mathsf{A}, \Theta, \mathcal{X}, \{\mathbf{A}_x^\theta\}_{\theta\in\Theta,x\in\Sigma})$ be monogamy game. Then, the winning probability of a quantum strategy $\mathsf{S} = (\mathcal{H}_\mathsf{B}, \mathcal{H}_\mathsf{C}, \rho_\mathsf{ABC}, \{\mathbf{B}_x^\theta\}_{\theta\in\Theta,x\in\mathcal{X}}, \{\mathbf{C}_x^\theta\}_{\theta\in\Theta,x\in\mathcal{X}})$ for the particular monogamy game G is defined by the quantity*

$$\omega_\mathsf{S}(\mathsf{G}) := \mathop{\mathbb{E}}_{\theta\sim\Theta} \sum_{x\in\mathcal{X}} \mathrm{Tr}\left[(\mathbf{A}_x^\theta \otimes \mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta)\rho_\mathsf{ABC}\right].$$

Moreover, we define the value of the monogamy game G as the optimal winning probability

$$\omega(\mathsf{G}) := \sup_{\mathsf{S}=(\mathcal{H}_\mathsf{B},\mathcal{H}_\mathsf{C},\rho_\mathsf{ABC},\{\mathbf{B}_x^\theta\},\{\mathbf{C}_x^\theta\})} \omega_\mathsf{S}(\mathsf{G}).$$

Remark 4. *As noted in [TFKW13], a standard purification argument and Neumark's dilation theorem show that we can assume without loss of generality that all POVMs are projective. We will assume this going forward.*

Definition 3.4 (Parallel-Repeated Monogamy Game)**.** *Let $r \in \mathbb{N}$ be a parameter. For any monogamy game $\mathsf{G} = (\mathcal{H}_\mathsf{A}, \Theta, \mathcal{X}, \left\{\mathbf{A}_x^\theta\right\}_{\theta\in\Theta,x\in\mathcal{X}})$, we define the r-*fold parallel-repeated monogamy game *$\mathsf{G}^{\times r}$ as follows:*

- *The Hilbert space for Alice's register will be $\mathcal{H}_\mathsf{A}^{\otimes r}$.*
- *The set of questions will now be Θ^r.*
- *The set of answers will be $\mathcal{X}^r$.*
- *For any $(x_1, \ldots, x_r) \in \mathcal{X}^r$ and $(\theta_1, \ldots, \theta_r) \in \Theta^r$, we define Alice's measurement to be*

$$\mathbf{A}_{(x_1,\ldots,x_r)}^{(\theta_1,\ldots,\theta_r)} = \bigotimes_{i=1}^r \mathbf{A}_{x_i}^{\theta_i}.$$

Informally, Alice will carry out r parallel measurements and Bob and Charlie succeed if they successfully guess the outcomes of all r measurements.

Example (BB84 Monogamy Game)**.** *As a simple example, the following monogamy game is known as the "BB84 monogamy game":*

- *The Hilbert space* $\mathcal{H}_{\mathsf{A}}$ *is* $\mathbb{C}^2$.
- *The sets of questions* Θ *and answers* $\mathcal{X}$ *are both* $\{0,1\}$.
- *For any* $x, \theta \in \{0,1\}$*, we have*

$$\mathbf{A}_x^\theta = \mathsf{H}^\theta \left|x\right\rangle\!\left\langle x\right| \mathsf{H}^\theta.$$

Remark 5. *We note that any MOE game admits a trivial strategy with success probabiliy* $1/|\mathcal{X}|$*. Bob and Charlie could set up the state* ρ_{ABC} *so that Bob and Alice are maximally entangled. This would enable Bob to always guess* x *correctly, and now Charlie can guess randomly. (He cannot do better as in this case he must be completely decoupled from Alice and Bob.)*

3.2 Oracular Cloning Games

The monogamy of entanglement games which we encounter in physics and cryptography often deal with some restrictions on the types of strategies that can be employed. Motivated by this, in this section, we introduce the notion of a $t \mapsto t+1$ *cloning game*. In the case when $t = 1$, this notion turns out to be a special case of a monogamy of entanglement game in Section 3.1, with the following additional restrictions:

- The tripartite state $\rho \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}})$ which is shared between Alice, Bob and Charlie is the result of applying a cloning channel $\Phi_{\mathsf{A}' \to \mathsf{BC}}$ to one half of an EPR pair, i.e.,

$$\rho_{\mathsf{ABC}} = (\mathbb{I}_{\mathsf{A}} \otimes \Phi_{\mathsf{A}' \to \mathsf{BC}})(|\mathsf{EPR}\rangle\langle\mathsf{EPR}|_{\mathsf{AA}'}).$$

  In other words, ρ_{ABC} is the normalized Choi state of some channel $\Phi_{\mathsf{A}' \to \mathsf{BC}}$.

- Alice's measurement $\left\{\mathbf{A}_x^\theta\right\}_{\theta \in \Theta, x \in \mathcal{X}}$ on register A is a projective measurement of the form

$$\mathbf{A}_x^\theta = \bar{U}_\theta \left|x\right\rangle\!\left\langle x\right| \bar{U}_\theta^\dagger,$$

  for some family of unitary operators $\{U_\theta\}_{\theta \in \Theta}$ acting on $\mathcal{H}_{\mathsf{A}}$.

- (If we are in the oracular setting) Bob and Charlie's measurements can only depend on oracle queries to U_θ and $U_\theta^\dagger$, rather than directly on θ.

This equivalence was first observed and used by Broadbent and Lord [BL20] for analyzing BB84 cloning games; for completeness, we give a proof of the general case (which proceeds along almost identical lines) in Lemma A.1. For $t \geq 2$, the notion of a $t \mapsto t+1$ cloning game includes $t+1$ colluding parties and thus starts to become incomparable to a monogamy of entanglement game in Section 3.1. However, a similar argument still allows us to establish an equivalence between $t \mapsto t+1$ cloning games and another game that resembles a monogamy game, and we will use this equivalence in our analysis. This equivalence is demonstrated in Lemma A.2.

Let us now give a formal definition of a $t \mapsto t+1$ cloning game.

Definition 3.5 ((Oracular) Cloning Game)**.** *Let* $t \in \mathbb{N}$ *be an integer. A* $t \mapsto t+1$ *(oracular) cloning game* ($(\mathsf{O})\mathsf{CG}$) *is a tuple* $\mathsf{G}_{t \mapsto t+1} = (t, \mathcal{H}_{\mathsf{A}^t}, \Theta, \mathcal{X}, \{U_\theta\}_{\theta \in \Theta})$ *which consists of the following elements:*

- *A finite dimensional Hilbert space* $\mathcal{H}_{\mathsf{A}^t}$ *consisting of registers* $\mathsf{A}^t := \mathsf{A}_1 \cdots \mathsf{A}_t$ *given to the cloner;*
- *A finite set* Θ *corresponding to the set of possible questions;*

- *A finite set $\mathcal{X}$ corresponding to the set of all possible answers;*
- *A finite ensemble of unitary operators $\{U_\theta\}_{\theta\in\Theta}$ acting on the A systems.*

Definition 3.6 (Quantum Strategy for Cloning Games)**.** *Let $t \in \mathbb{N}$ and let $\mathsf{G}_{t\mapsto t+1} = (t, \mathcal{H}_{\mathsf{A}^t}, \Theta, \mathcal{X}, \{U_\theta\}_{\theta\in\Theta})$ be a cloning game. A quantum strategy $\mathsf{S} = (\mathcal{H}_{\mathsf{B}^{t+1}}, \Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}, \{\mathbf{P}^\theta_{1,x}\}_{\theta\in\Theta,x\in\mathcal{X}}, \ldots, \{\mathbf{P}^\theta_{t+1,x}\}_{\theta\in\Theta,x\in\mathcal{X}})$ for the game $\mathsf{G}_{t\mapsto t+1}$ is characterized by the following elements:*

- *A finite dimensional Hilbert space $\mathcal{H}_{\mathsf{B}^{t+1}}$ consisting of registers $\mathsf{B}^{t+1} := \mathsf{B}_1\cdots\mathsf{B}_{t+1}$ which are held by the $k+1$ many players in the game;*
- *A completely positive and trace-preserving channel $\Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}$ performed by the cloner;*
- *A sequence of measurements $\{\mathbf{P}^\theta_{1,x}\}_{\theta\in\Theta,x\in\mathcal{X}}, \ldots, \{\mathbf{P}^\theta_{t+1,x}\}_{\theta\in\Theta,x\in\mathcal{X}}$ which are to be performed by the $t+1$ players on the registers $\mathsf{B}_1, \cdots, \mathsf{B}_{t+1}$, respectively.*

Definition 3.7 (Quantum Strategy for **Oracular** Cloning Games)**.** *A quantum strategy for an **oracular** cloning game is the same as a quantum strategy for a cloning game, with the following crucial restriction: the measurements by the $t+1$ players will now be* oracle-aided*. We denote these as*

$$\left\{\mathbf{P}^{U_\theta,U_\theta^\dagger}_{1,x}\right\}_{\theta\in\Theta,x\in\mathcal{X}}, \ldots, \left\{\mathbf{P}^{U_\theta,U_\theta^\dagger}_{t+1,x}\right\}_{\theta\in\Theta,x\in\mathcal{X}}.$$

Informally, an oracular cloning game is one where the players are only given oracle access to $U_\theta, U_\theta^\dagger$, whereas in Definition 3.6 the players are given the question θ in the clear.

Definition 3.8 (**Restricted** Quantum Strategy for Oracular Cloning Games)**.** *Assume $\mathcal{X} = \{0,1\}^n$. Then a **restricted** quantum strategy for an oracular cloning game further restricts the players in the following way. For each $i \in [t+1]$, player $\mathcal{P}_i$ must output their guess $x \in \{0,1\}^n$ after applying some quantum algorithm that makes **at most one query** to either U_θ or $U_\theta^\dagger$.*

We let $\mathcal{S}_{\text{rest}}$ denote the collection of restricted quantum strategies S for the oracular cloning game G.

We first observe that we can impose some structure on the $t+1$ players' strategies without loss of generality; this will make our analysis easier:

Lemma 3.9. *Without loss of generality, a restricted quantum strategy for G may be taken to the have the following much more restricted structure: Each player $\mathcal{P}_i$ will hold a register B_i that splits into the following registers:*

- *A query register C_i of n qubits;*
- *An ancilla register D_i of a qubits (we allow a to be arbitrary, but assume WLOG that it is the same for all the players); and*
- *A classical control bit b_i from the cloning channel Φ, which we store in a single-qubit register E_i for formality's sake.*

The player $\mathcal{P}_i$ will then proceed as follows:

1. *They first make **exactly one query** to either U_θ or $U_\theta^\dagger$, which will be applied to the C_i register. Which of these unitaries they query will be controlled by b_i.*

2. *They can then apply a unitary Q_i of their choice to their entire system B_i. (We assume without loss of generality that the same unitary Q_i is applied regardless of the value of the control bit b_i; the cloner could simply include a copy of the control bit in register D_i as well, which Q_i acts on.)*

3. *They now measure the n qubits in the C_i register to obtain a string $x \in \{0,1\}^n$.*

4. *They output x.*

Formally: for every $i \in [t+1]$ and $x \in \{0,1\}^n$, player $\mathcal{P}_i$'s projector has the form:

$$\mathbf{P}_{i,x}^{U_\theta, U_\theta^\dagger} = \left[(U_\theta^\dagger \otimes \mathbb{I}_{\mathsf{D}_\mathsf{i}}) Q_i^\dagger (|x\rangle\langle x| \otimes \mathbb{I}_{D_i}) Q_i (U_\theta \otimes \mathbb{I}_{\mathsf{D}_\mathsf{i}})\right] \otimes |0\rangle\langle 0|_{\mathsf{E}_\mathsf{i}} + \left[(U_\theta \otimes \mathbb{I}_{\mathsf{D}_\mathsf{i}}) Q_i^\dagger (|x\rangle\langle x| \otimes \mathbb{I}_{D_i}) Q_i (U_\theta^\dagger \otimes \mathbb{I}_{\mathsf{D}_\mathsf{i}})\right] \otimes |1\rangle\langle 1|_{\mathsf{E}_\mathsf{i}} .$$

Proof. Any preprocessing that player $\mathcal{P}_i$ might carry out before their query can be absorbed into the cloning channel Φ, including the decision about which of $U_\theta, U_\theta^\dagger$ to query, which we represent in the control bit b_i. (If the player does not want to query either, we can just treat C_i as dummy qubits and make a query there.)

The conclusion now follows from the Stinespring and Neumark dilation theorems [NC16]. □

Remark 6. *Some comments are in order about Definition 3.8:*

- *The cloner Φ remains entirely unrestricted; they can apply an arbitrary quantum channel to $(U_\theta |x\rangle)^{\otimes t}$.*
- *While quite restrictive, this model is still sufficiently expressive and captures a standard approximate no-cloning bound as a special case: once the cloning map Φ has been applied, each player $\mathcal{P}_i$ immediately makes a query to $U_\theta^\dagger$ and measures in the computational basis. In this case, it is easy to check that the winning probability corresponds precisely to the average cloning fidelity for $t \mapsto t+1$.*

Definition 3.10 (Value of a (Oracular) Cloning Game)**.** *Let $t \in \mathbb{N}$. The winning probability of a quantum strategy $\mathsf{S} = (\mathcal{H}_{\mathsf{B}^{t+1}}, \Phi_{\mathsf{A}^t \to \mathsf{B}^{t+1}}, \{\mathbf{P}_{1,x}^{U_\theta, U_\theta^\dagger}\}_{\theta\in\Theta, x\in\mathcal{X}}, \ldots, \{\mathbf{P}_{t+1,x}^{U_\theta, U_\theta^\dagger}\}_{\theta\in\Theta, x\in\mathcal{X}})$ for a particular $t \mapsto t+1$ oracular cloning game $\mathsf{G}_{t\mapsto t+1} = (t, \mathcal{H}_{\mathsf{A}^t}, \Theta, \mathcal{X}, \{U_\theta\}_{\theta\in\Theta})$ is defined by the quantity*

$$\omega_\mathsf{S}(\mathsf{G}_{t\mapsto t+1}) := \mathop{\mathbb{E}}_{\theta\sim\Theta} \mathop{\mathbb{E}}_{x\sim\mathcal{X}} \mathrm{Tr}\left[\left(\mathbf{P}_{1,x}^{U_\theta, U_\theta^\dagger} \otimes \ldots \otimes \mathbf{P}_{t+1,x}^{U_\theta, U_\theta^\dagger}\right) \Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}\left((U_\theta |x\rangle\langle x| U_\theta^\dagger)_{\mathsf{A}^t}^{\otimes t}\right)\right].$$

Moreover, we define the value of the oracular cloning game G as the optimal winning probability

$$\omega(\mathsf{G}_{t\mapsto t+1}) := \sup_{\mathsf{S}=(\mathcal{H}_{\mathsf{B}^{t+1}}, \Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}, \{\mathbf{P}_{1,x}\}, \ldots, \{\mathbf{P}_{t+1,x}\})} \omega_\mathsf{S}(\mathsf{G}_{t\mapsto t+1}).$$

We analogously define the value of a cloning game G, using the measurements $\left\{\mathbf{P}_{i,x}^\theta\right\}$ instead.

Remark 7 (Comparison with [AKL23])**.** *Our definition of cloning games (in the single copy setting) is much more specific than that in [AKL23, Definitions 2-6]. Using their terminology, the secret key is θ and each of the steps has the following structure:*

- *The secret key sk will be the basis θ.*
- *Token generation $\mathsf{GenT}(\mathsf{sk}, x)$ is restricted to deterministically output the pure state $U_\theta |x\rangle$.*

- *Challenge generation* $\mathsf{GenC}(\mathsf{sk}, x)$ *simply releases* $\theta = \mathsf{sk}$*, either in the clear or in the form of an oracle.*
- *For verification, we specialize to the* cloning search *setting (see [AKL23, Definition 4]), where the players win if they all output the string* x *as their answer.*

Our reason for focusing on games of this form is because we are primarily concerned with the difficulty of cloning one very specific property of a quantum state, namely its measurement statistics with respect to the bases specified by Θ *(or even more weakly, just the string* x*).*

We also make the straightforward observation that cloning games are closely related to unclonable encryption (UE) schemes (which we will formally define in Section 9):

Lemma 3.11. *Consider a cloning game with* t *players,* $\mathcal{X} = \{0,1\}^n$*, and* $\Theta = \{0,1\}^\lambda$*. Then all of the following hold:*

- *If the corresponding cloning game has value* $\leq \epsilon$ *with computationally unbounded (respectively, computationally bounded)* $(\Phi, \mathcal{P}_1, \ldots, \mathcal{P}_{t+1})$*, then there exists a* UE *scheme satisfying statistical (respectively, computational)* $t \mapsto t+1$ ϵ*-*UE *security.*
- *If the corresponding* oracular *cloning game has value* $\leq \epsilon$ *with computationally unbounded (respectively, computationally bounded)* $(\Phi, \mathcal{P}_1, \ldots, \mathcal{P}_{t+1})$*, then there exists a* UE *scheme satisfying (statistical, respectively computational)* $t \mapsto t+1$ (ϵ, ∞)-UE oracular *security.*
- *If in the corresponding oracular cloning game, any computationally unbounded (respectively, computationally bounded)* restricted *strategy* $(\Phi, \mathcal{P}_1, \ldots, \mathcal{P}_{t+1})$ *has value* $\leq \epsilon$*, then there exists a* UE *scheme satisfying (statistical, respectively computational)* $t \mapsto t+1$ $(\epsilon, 1)$-UE *oracular security.*

Proof. In all cases, the construction proceeds as follows: we will take $\mathsf{Enc}(\theta, x) = U_\theta |x\rangle$, and Dec will apply $U_\theta^\dagger$ and measure in the standard basis. The conclusions are now straightforward to verify. □

4 Types and Subtypes

In order to improve on the limitations of the [TFKW13] framework for bounding the value of monogamy games, we essentially restrict attention to oracular cloning games, and restrict each player to only make one query. This allows us to analyze this game using the language of *binary phase twirls* (defined and analyzed in Section 4.2). To effectively capture the effect of binary phase twirls on an operator, we revisit the formalism of *types* introduced by [AGQY22] in Section 4.1 and extend this to *subtypes* in Section 4.3. Later, in Section 5, we will leverage these tools to analyze our construction using binary phase states and prove cloning bounds of $O_t(2^{-n})$.

4.1 Binary Types

Let $N, M \in \mathbb{N}$ and $r \in \mathbb{N}$. For a vector $\mathbf{x} = (x_1, \ldots, x_r) \in [N]^r$ and an ancilla input $y \in [M]$, we denote by $\mathsf{Type}(\mathbf{x}, y) \in [0:r]^N$ the so-called *type vector* in which the i-th entry corresponds to the number of occurrences of $i \in [N]$ in $\mathbf{x}$. Note that the ancillary information y is just representing some auxiliary input that we do not consider when evaluating Type. We denote by $\mathsf{BinType}(\mathbf{x}, y) \in \{0,1\}^N$ the *binary type*

Game 2 (Oracular Cloning Game)**.**
A $t \mapsto t+1$ oracular cloning game $\mathsf{G}_{t\mapsto t+1} = (k, \mathcal{H}_{\mathsf{A}^t}, \Theta, \mathcal{X}, \{U_\theta\}_{\theta\in\Theta})$ for a quantum strategy of the form $\mathsf{S} = (\mathcal{H}_{\mathsf{B}^{t+1}}, \Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}, \{\mathbf{P}_{1,x}^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\mathcal{X}}, \ldots, \{\mathbf{P}_{t+1,x}^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\mathcal{X}})$ is the following game between a trusted challenger, a cloner and $t+1$ many players:

1. *(**Setup phase**) The challenger samples a random $x \sim \mathcal{X}$ and a random $\theta \sim \Theta$, and sends the state $(U_\theta |x\rangle)^{\otimes t}$ consisting of registers $\mathsf{A}^t := \mathsf{A}_1 \cdots \mathsf{A}_t$ to the cloner.*

   The cloner applies the channel $\Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}$ to $(U_\theta |x\rangle)^{\otimes t}$ and sends the resulting registers $\mathsf{B}^{t+1} = \mathsf{B}_1 \cdots \mathsf{B}_{t+1}$ to the $t+1$ many players, respectively. Afterwards, the players may no longer communicate with each other for the remainder of the game.

2. *(**Question phase**) Each of the players receives oracles for both U_θ and $U_\theta^\dagger$.*

3. *(**Answer phase**) The players independently output a guess for the element x by applying the measurements $\{\mathbf{P}_{1,x}^{U_\theta,U_\theta^\dagger}\}_{x\in\mathcal{X}}, \ldots, \{\mathbf{P}_{t+1,x}^{U_\theta,U_\theta^\dagger}\}_{x\in\mathcal{X}}$ to their registers, respectively.*

4. *(**Outcome phase**) The players win if they all guess x correctly.*

Figure 5: A $t \mapsto t+1$ oracular cloning game. A regular cloning game is defined analogously, except the measurements are now $\mathbf{P}_{i,x}^{\theta}$ and free to depend on θ in any way. Informally, in a standard cloning game θ is revealed to the $t+1$ players in the clear, while in the oracular cloning game the players are only given oracle access to U_θ and $U_\theta^\dagger$.

vector in which the i-th entry corresponds to the parity of the number of occurrences of $i \in [N]$ in $\mathbf{x}$. In other words, we let

$$\mathsf{BinType}(\mathbf{x}, y) = \mathsf{Type}(\mathbf{x}, y) \pmod 2.$$

We note that our definition of Type and BinType is a natural extension of the standard definition in the literature (which does not consider auxiliary input); in particular, when $M = 0$ and y is the empty string, our definitions and the standard definitions coincide.

BinType **decomposition.** When working with the vector space $\mathcal{H} = (\mathbb{C}^N)^{\otimes r} \otimes \mathbb{C}^M$, we use the following BinType decomposition into orthogonal subspaces $V_{\boldsymbol{\lambda}}$ indexed by binary types $\boldsymbol{\lambda} \in \{0,1\}^N$ such that

$$(\mathbb{C}^N)^{\otimes r} \otimes \mathbb{C}^M \cong \bigoplus_{\boldsymbol{\lambda}} V_{\boldsymbol{\lambda}}\,,$$

where each subspace $V_{\boldsymbol{\lambda}} \subseteq \mathcal{H}$ corresponds to vectors with a particular binary type $\boldsymbol{\lambda}$, i.e.,

$$V_{\boldsymbol{\lambda}} = \mathrm{span}_{\mathbb{C}}\{|v_1, \ldots, v_r, w\rangle \,:\, \mathsf{BinType}((v_1, \ldots, v_r), w) = \boldsymbol{\lambda}\}.$$

4.2 Phase Twirling

For a binary function $f : [N] \to \{0,1\}$, we let U_f define the phase unitary

$$\mathsf{U}_f = \sum_{x\in[N]} (-1)^{f(x)} |x\rangle\langle x|\,.$$

Using the BinType decomposition, we can show the following identity for the r-wise twirl with U_f. We note that the below lemma is also immediate from Zhandry's compressed oracle technique [Zha19]; although we do not present our results in these terms here, we outline this formulation in Section 1.2.3.

Lemma 4.1. *Let $O \in L(\mathcal{H})$ be a linear operator acting on the vector space $\mathcal{H} = (\mathbb{C}^N)^{\otimes r} \otimes \mathbb{C}^M$. Then,*

$$\mathop{\mathbb{E}}_{f\sim\mathcal{F}_n}\left[\left(\mathsf{U}_f^{\otimes r}\otimes\mathbb{I}\right)O\left(\mathsf{U}_f^{\otimes r}\otimes\mathbb{I}\right)\right] = \sum_{\boldsymbol{\lambda}\in\{0,1\}^N}\Pi_{\boldsymbol{\lambda}}O\Pi_{\boldsymbol{\lambda}}\,,$$

where $\Pi_{\boldsymbol{\lambda}}$ projects onto $V_{\boldsymbol{\lambda}} = \mathrm{span}_{\mathbb{C}}\{|x_1,\ldots,x_r,v\rangle \in (\mathbb{C}^N)^{\otimes r}\otimes\mathbb{C}^M \,:\, \mathsf{BinType}((x_1,\ldots,x_r),v) = \boldsymbol{\lambda}\}$.

Proof. Expanding O in the standard basis and using the linearity of expectation, we get

$$\begin{aligned}
&\mathop{\mathbb{E}}_{f\sim\mathcal{F}_n}\left[\left(\mathsf{U}_f^{\otimes r}\otimes\mathbb{I}\right)O\left(\mathsf{U}_f^{\otimes r}\otimes\mathbb{I}\right)\right]\\
&= \sum_{\substack{\mathbf{x},\mathbf{y}\in[N]^r\\ v,w\in[M]}} O_{(\mathbf{x},v);(\mathbf{y},w)}\mathop{\mathbb{E}}_{f\sim\mathcal{F}_n}\left[\mathsf{U}_f^{\otimes r}|\mathbf{x}\rangle\langle\mathbf{y}|\,\mathsf{U}_f^{\otimes r}\otimes|v\rangle\langle w|\right]\\
&= \sum_{\substack{\mathbf{x},\mathbf{y}\in[N]^r\\ v,w\in[M]}} O_{(\mathbf{x},v);(\mathbf{y},w)}\mathop{\mathbb{E}}_{f\sim\mathcal{F}_n}\left[(-1)^{f(x_1)+\ldots+f(x_r)+f(y_1)+\ldots+f(y_r)}\right]|\mathbf{x}\rangle\langle\mathbf{y}|\otimes|v\rangle\langle w|\\
&= \sum_{\substack{\mathbf{x},\mathbf{y}\in[N]^r\\ v,w\in[M]\\ \mathsf{BinType}(\mathbf{x},v)=\mathsf{BinType}(\mathbf{y},w)}} O_{(\mathbf{x},v);(\mathbf{y},w)}|\mathbf{x},v\rangle\langle\mathbf{y},w| \;=\; \sum_{\boldsymbol{\lambda}\in\{0,1\}^N}\Pi_{\boldsymbol{\lambda}}O\Pi_{\boldsymbol{\lambda}}.
\end{aligned}$$

□

4.3 Binary Subtypes

4.3.1 Definitions and Combinatorial Properties

While BinType is very simple to define, it comes with an "entangled"[14] combinatorial structure that is difficult to work with. As a simple example, consider the case where $r = 3, M = 0$, and the binary type $\boldsymbol{\lambda}$ is $(1,0,0,\ldots,0)$. There are a few different ways for a vector in $[N]^3$ to attain this BinType: the vector could be of the form $(0,x,x)$ for any $x \in [N]$ or any permutation of this, and moreover these collections of vectors will overlap on $(0,0,0)$.

Instead of working with the BinType directly, it is more natural and convenient to address each of these different collections of vectors separately. Within each of these collections, there is now a very clean combinatorial structure that we will be able to exploit.

To formalize the above intuition, we will work with the notion of *subtypes*. As in Section 4.1, let N, M, r be positive integer parameters:

Definition 4.2. *A* subtype *of a given type $\boldsymbol{\lambda} = (c_1,\ldots,c_N) \in \{0,1\}^N$ is a string $\boldsymbol{\mu}$ of length r. Each entry of $\boldsymbol{\mu}$ is either an integer $i \in [N]$ such that $\boldsymbol{\lambda}_i = 1$, or a* variable symbol *x_i for some index i. We have the following constraints:*

- *For each $i \in [N]$ such that $\boldsymbol{\lambda}_i = 1$, i should appear an odd number of times in $\boldsymbol{\mu}$.*

[14] This comment is qualitative, and does not relate in any way to quantum entanglement.

- *For any i such that x_i appears at least once in $\boldsymbol{\mu}$, the first i distinct variable symbols that appear in $\boldsymbol{\mu}$ are $x_1, x_2, \ldots, x_i$ in that order.*
- *Each variable symbol x_i appears an even number of times in $\boldsymbol{\mu}$.*

Definition 4.3. *For a vector $(\mathbf{x}, y) \in [N]^r \times [M]$, define its* query restriction *to be $\mathbf{x} \in [N]^r$. (Informally, the query restriction discards any auxiliary information.)*

Definition 4.4. *We say a vector $(\mathbf{x}, y) \in [N]^r \times [M]$ matches a subtype $\boldsymbol{\mu}$ if there exist assignments of values in $[N]$ to the variable symbols in $\boldsymbol{\mu}$ to yield the query restriction $\mathbf{x}$ of $(\mathbf{x}, y)$.*

For a subtype $\boldsymbol{\mu}$, we define $S_{\boldsymbol{\mu}} \subseteq [N]^r \times [M]$ to be the set of vectors $(\mathbf{x}, y)$ that match $\boldsymbol{\mu}$, and let $\Pi_{\boldsymbol{\mu}}$ denote the projection onto standard basis vectors in $S_{\boldsymbol{\mu}}$.

Definition 4.5. *For any subtype $\boldsymbol{\mu}$ with variable symbols $x_1, \ldots, x_k$ and some specific values $y_1, \ldots, y_k \in [N]$ and $z \in [M]$, define $\mathsf{Reconstruct}(\boldsymbol{\mu}, (y_1, \ldots, y_k), z)$ to be the vector in $[N]^r \times [M]$ obtained by taking $\boldsymbol{\mu}$ and replacing the variable symbol x_i with y_i for each i, then finally appending z.*

At this point, we make some straightforward observations. Firstly, membership of a vector $(\mathbf{x}, y)$ in a subtype $\boldsymbol{\mu}$ or a type $\boldsymbol{\lambda}$ depends only on its query restriction. Also, any vector $(\mathbf{x}, y)$ that matches a subtype $\boldsymbol{\mu}$ of a type $\boldsymbol{\lambda}$ must have type $\boldsymbol{\lambda}$. This is due to the parity constraints in Definition 4.2. Conversely, for any vector $(\mathbf{x}, y)$ of type $\boldsymbol{\lambda}$, there is at least one subtype $\boldsymbol{\mu}$ of $\boldsymbol{\lambda}$ that $(\mathbf{x}, y)$ matches: we can take $\mathbf{x}$, leave entries i such that $\boldsymbol{\lambda}_i = 1$ as they are, and replace all other distinct values by variable symbols $x_1, x_2, \ldots$. This suggests that we might be able to relate the collection of vectors in a given $\mathsf{BinType}$ to the collection of vectors in a given subtype.

Lemma 4.6. *Any type $\boldsymbol{\lambda}$ has at most $(2r)^r$ subtypes.*

Proof. Consider a subtype $\boldsymbol{\mu}$ of $\boldsymbol{\lambda}$. Any entry in the string defining $\boldsymbol{\mu}$ must be one of the following:

- A fixed integer $i \in [N]$ such that $\boldsymbol{\lambda}_i = 1$. There are at most r such integers.
- A variable symbol x_i, where $i \leq r$.

$\boldsymbol{\mu}$ has r entries, so the conclusion follows. □

4.3.2 Relating Subtype Projectors to Type Projectors

It turns out that our main technical task to prove bounds on monogamy games in Section 5 is to bound expressions of the form

$$\mathrm{Tr}\left[\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}} \rho\right],$$

where ρ is some quantum mixed state in $\mathrm{S}((\mathbb{C}^N)^{\otimes r} \otimes \mathbb{C}^M)$, Ξ is some PSD operator, and $\boldsymbol{\lambda}$ is a $\mathsf{BinType}$. Here, we will use the combinatorial machinery we just introduced in Section 4.3.1 to reduce this to bounding expressions of the form

$$\left\|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\right\|_\infty \cdot \mathrm{Tr}\left[\Pi_{\boldsymbol{\mu}} \rho\right],$$

where $\boldsymbol{\mu}$ is now a subtype. Our starting point is the following lemma:

Lemma 4.7. *For any type $\boldsymbol{\lambda}$, there exist projectors $P_{\boldsymbol{\mu}}$ for each subtype $\boldsymbol{\mu}$ of $\boldsymbol{\lambda}$ such that both of the following are true:*

1. *We have*
$$\Pi_{\boldsymbol{\lambda}} = \sum_{\boldsymbol{\mu}} P_{\boldsymbol{\mu}}.$$
2. *For every $\boldsymbol{\mu}$, we have $P_{\boldsymbol{\mu}} \leq \Pi_{\boldsymbol{\mu}}$ (with respect to the PSD ordering).*

Proof. Let $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2, \ldots, \boldsymbol{\mu}_K$ be all the subtypes of $\boldsymbol{\lambda}$ in an arbitrary order. For each $i \in [K]$, let $P_{\boldsymbol{\mu}_i}$ be the projector onto the span of standard basis vectors in the set
$$T_{\boldsymbol{\mu}_i} := S_{\boldsymbol{\mu}_i} \setminus \bigcup_{j<i} S_{\boldsymbol{\mu}_j}.$$
First, we check condition 1: the sets $T_{\boldsymbol{\mu}_i}$ are disjoint by construction and clearly contained in the set of vectors of type $\boldsymbol{\lambda}$. Conversely, any vector of type $\boldsymbol{\lambda}$ is contained in at least one $S_{\boldsymbol{\mu}_i}$ (and hence some $T_{\boldsymbol{\mu}_i}$). Hence the disjoint union of $\{T_{\boldsymbol{\mu}_i} : i \in [K]\}$ is exactly the collection of standard basis vectors with type $\boldsymbol{\lambda}$. The claim follows. Finally, condition 2 is immediate from the fact that $T_{\boldsymbol{\mu}_i} \subseteq S_{\boldsymbol{\mu}_i}$. □

Finally, we completely reduce our problem to working with subtypes instead of types via the following lemma:

Lemma 4.8. *For any PSD matrix A, type $\boldsymbol{\lambda}$, and mixed state ρ, we have*
$$\operatorname{Tr}\left[\Pi_{\boldsymbol{\lambda}} A \Pi_{\boldsymbol{\lambda}} \rho\right] \leq (2r)^r \cdot \left(\sum_{\boldsymbol{\mu} \text{ subtype of } \boldsymbol{\lambda}} \left\|\Pi_{\boldsymbol{\mu}} A \Pi_{\boldsymbol{\mu}}\right\|_\infty \cdot \operatorname{Tr}\left[\Pi_{\boldsymbol{\mu}} \rho\right] \right).$$

Proof. By linearity, it suffices to prove the result when ρ is a pure state $|\phi\rangle\langle\phi|$. Moreover, let us write $A = B^\dagger B$ for some matrix B. Then we have:
$$\begin{aligned}
\operatorname{Tr}\left[\Pi_{\boldsymbol{\lambda}} A \Pi_{\boldsymbol{\lambda}} \rho\right] &= \langle\phi|\Pi_{\boldsymbol{\lambda}} B^\dagger B \Pi_{\boldsymbol{\lambda}}|\phi\rangle \\
&= \left\|B \Pi_{\boldsymbol{\lambda}} |\phi\rangle\right\|^2 \\
&= \left\| \sum_{\boldsymbol{\mu} \text{ subtype of } \boldsymbol{\lambda}} B P_{\boldsymbol{\mu}} |\phi\rangle \right\|^2 \text{ (Lemma 4.7, condition 1)} \\
&\leq (2r)^r \cdot \sum_{\boldsymbol{\mu} \text{ subtype of } \boldsymbol{\lambda}} \left\|B P_{\boldsymbol{\mu}} |\phi\rangle\right\|^2 \text{ (Cauchy-Schwarz; Lemma 4.6)} \\
&= (2r)^r \cdot \sum_{\boldsymbol{\mu} \text{ subtype of } \boldsymbol{\lambda}} \langle\phi| P_{\boldsymbol{\mu}} B^\dagger B P_{\boldsymbol{\mu}} |\phi\rangle \\
&= (2r)^r \cdot \sum_{\boldsymbol{\mu} \text{ subtype of } \boldsymbol{\lambda}} \operatorname{Tr}\left[P_{\boldsymbol{\mu}} A P_{\boldsymbol{\mu}} \rho\right] \\
&\leq (2r)^r \cdot \sum_{\boldsymbol{\mu} \text{ subtype of } \boldsymbol{\lambda}} \left\|P_{\boldsymbol{\mu}} A P_{\boldsymbol{\mu}}\right\|_\infty \cdot \operatorname{Tr}\left[P_{\boldsymbol{\mu}} \rho\right] \\
&\leq (2r)^r \cdot \sum_{\boldsymbol{\mu} \text{ subtype of } \boldsymbol{\lambda}} \left\|\Pi_{\boldsymbol{\mu}} A \Pi_{\boldsymbol{\mu}}\right\|_\infty \cdot \operatorname{Tr}\left[\Pi_{\boldsymbol{\mu}} \rho\right]. \text{ (Lemma 4.7, condition 2)}
\end{aligned}$$

In more detail, the final step follows from two straightforward observations. Firstly: $\mathrm{Tr}\left[P_{\boldsymbol{\mu}}\rho\right] \leq \mathrm{Tr}\left[\Pi_{\boldsymbol{\mu}}\rho\right]$ is clear since $\Pi_{\boldsymbol{\mu}} - P_{\boldsymbol{\mu}}$ is PSD. Secondly: since $P_{\boldsymbol{\mu}}$ is a projector, we have that:

$$\left\|P_{\boldsymbol{\mu}}AP_{\boldsymbol{\mu}}\right\|_\infty = \max_{|\phi\rangle \in \mathrm{im}P_{\boldsymbol{\mu}}} \langle\phi|A|\phi\rangle \text{ ; and similarly}$$
$$\left\|\Pi_{\boldsymbol{\mu}}A\Pi_{\boldsymbol{\mu}}\right\|_\infty = \max_{|\phi\rangle \in \mathrm{im}\Pi_{\boldsymbol{\mu}}} \langle\phi|A|\phi\rangle .$$

Now we have $P_{\boldsymbol{\mu}} \leq \Pi_{\boldsymbol{\mu}} \Rightarrow \mathrm{im}P_{\boldsymbol{\mu}} \subseteq \mathrm{im}\Pi_{\boldsymbol{\mu}} \Rightarrow \left\|P_{\boldsymbol{\mu}}AP_{\boldsymbol{\mu}}\right\|_\infty \leq \left\|\Pi_{\boldsymbol{\mu}}A\Pi_{\boldsymbol{\mu}}\right\|_\infty$. This completes our proof. □

5 Cloning Game Construction from Binary Phase States

In this section, we prove upper bounds on the value of restricted oracular cloning games (defined in Definition 3.8). This section is organized as follows:

- In Section 5.1, we formally state our binary phase construction and prove some preliminary lemmas, in particular relating the cloning game to a monogamy-like game with some state ρ shared between the challenger and the $t+1$ players $\mathcal{P}_1, \ldots, \mathcal{P}_{t+1}$.
- In Section 5.2, we expand out the relevant operators and states in terms of *subtypes* (defined in Section 4.3).
- In Section 5.3, we prove spectral bounds on the operator norms of the relevant operators.
- In Sections 5.4 and 5.5, we provide some additional tools — namely, an analysis of the structure of the shared state ρ and how it splits across subtypes — that are necessary for handling $t \mapsto t+1$ cloning games when $t > 1$. We then put everything together to prove our desired bounds in the restricted oracular cloning setting.

5.1 Setup and Notation

We begin by presenting our construction. Note the qualitative similarity of this construction with Construction 2; both rely centrally on binary phase states.

Construction 1. *Let $\mathfrak{F} = \{f_\theta : \{0,1\}^n \to \{0,1\}\}_{\theta\in\Theta}$ be a family of functions parametrized by elements $\Theta = \{0,1\}^\lambda$. Consider the following $t \mapsto t+1$ oracular cloning game (as defined in Definition 3.5) $\mathsf{G}_{\mathfrak{F},t}$ with question set Θ and answer set $\mathcal{X} := \{0,1\}^n$. For any θ, we will take the unitary U_θ to be $\mathsf{U}_{f_\theta}\mathsf{H}^{\otimes n}$. (Here, U_{f_θ} is the phase oracle for f_θ as defined in Section 2.1.) In other words, for any $x \in \{0,1\}^n$, we have*

$$U_\theta\left|x\right\rangle = 2^{-n/2}\sum_{u\in\{0,1\}^n}(-1)^{f_\theta(u)\oplus\langle x,u\rangle}\left|u\right\rangle .$$

Remark 8. *We are being intentionally vague about the choice of function family $\mathfrak{F}$. One could imagine instantiating it with a post-quantum PRF family, to obtain a construction that is plausibly secure against arbitrary polynomial-time adversaries in the oracular cloning game. (We believe this construction would be plausibly secure because $U_\theta\left|x\right\rangle$ is pseudorandom [JLS18, BS19] for any fixed $x \in \{0,1\}^n$, and hence multi-copy unclonable [Wer98].)*

Since we only prove oracular security in the case where $t = O(1)$ and each player can make $q = 1$ query in total, we will instead instantiate $\mathfrak{F}$ as an $O(1)$-wise uniform function family, which is statistically

indistinguishable from the family of all functions from $\{0,1\}^n \to \{0,1\}$ in this query bounded game. We will reiterate this formally when establishing our final theorem in Section 5.5.

We will consider restricted quantum strategies (defined in Definition 3.8). Recall that we use $\mathcal{S}_{\text{rest}}$ to denote the collection of all such strategies. We now make a crucial observation:

Remark 9. *Since $U_\theta^\dagger = \mathsf{H}^{\otimes n}\mathsf{U}_{f_\theta}$ and each player $\mathcal{P}_i$ is given a control bit in register E_i dictating whether they will query U_θ or $U_\theta^\dagger$, we can assume without loss of generality that each player simply makes one non-adaptive query to U_{f_θ} as their first step. (In the event that the player is querying $U_\theta = \mathsf{U}_{f_\theta}\mathsf{H}^{\otimes n}$, they would technically need to query $\mathsf{H}^{\otimes n}$ first. We can get around this by absorbing this query to $\mathsf{H}^{\otimes n}$ into the cloning channel Φ.)*

Recall from Definition 3.8 that each player's register B_i splits into a query register C_i, an ancilla register D_i, and a control qubit register E_i. Recalling the setup in Definition 3.8 together with Lemma 3.9 and Remark 9, we can write

$$\mathbf{P}_{i,x}^{U_\theta, U_\theta^\dagger} = (\mathsf{U}_{f_\theta} \otimes \mathbb{I}_{\mathsf{D}_i\mathsf{E}_i}) Q_i^\dagger (|x\rangle\langle x| \otimes \mathbb{I}_{\mathsf{D}_i\mathsf{E}_i}) Q_i (\mathsf{U}_{f_\theta} \otimes \mathbb{I}_{\mathsf{D}_i\mathsf{E}_i}), \tag{6}$$

for some unitaries $Q_1, \dots, Q_{t+1}$ such that Q_i acts on all the three registers $\mathsf{C}_i\mathsf{D}_i\mathsf{E}_i$.

With this in mind, we now switch from a cloning-based formulation to an entanglement-based formulation. At a high level, this follows from the ricochet property of EPR pairs (formally, Lemma 2.1). Substituting $\mathbf{P}_{i,x}$ as defined in Equation (6) and $U_\theta = \mathsf{U}_{f_\theta}\mathsf{H}^{\otimes n}$ (note that all entries of this unitary are real) into Lemma A.2 implies that:

$$\begin{aligned}\omega_{\mathsf{S}}(\mathsf{G}) =& 2^{n(t-1)} \cdot \mathop{\mathbb{E}}_{\theta} \sum_{x\in\{0,1\}^n} \operatorname{Tr}\Bigg[\Bigg(\Bigg(\bigotimes_{i\in[t+1]} (\mathsf{U}_{f_\theta} \otimes \mathbb{I}_{\mathsf{D}_i\mathsf{E}_i}) Q_i^\dagger (|x\rangle\langle x| \otimes \mathbb{I}_{\mathsf{D}_i\mathsf{E}_i}) Q_i (\mathsf{U}_{f_\theta} \otimes \mathbb{I}_{\mathsf{D}_i\mathsf{E}_i})\Bigg) \\ &\otimes \left(\mathsf{U}_{f_\theta}\mathsf{H}^{\otimes n} |x\rangle\langle x| \mathsf{H}^{\otimes n}\mathsf{U}_{f_\theta}\right)^{\otimes t}_{\mathsf{A}'_{1:t}}\Bigg)\rho\Bigg],\end{aligned}$$

where ρ is the Choi state

$$\rho_{\mathsf{B}_{1:t+1}\mathsf{A}'_{1:t}} := (\Phi_{\mathsf{A}_1\dots\mathsf{A}_t\to\mathsf{B}_1\dots\mathsf{B}_{t+1}} \otimes \mathbb{I}_{\mathsf{A}'_{1:t}}) \left(|\mathsf{EPR}^n\rangle\langle\mathsf{EPR}^n|^{\otimes t}\right). \tag{7}$$

Now define the projector

$$\Xi = \sum_{x\in\{0,1\}^n} \left(\left(\bigotimes_{i\in[t+1]} Q_i^\dagger \left(|x\rangle\langle x|_{\mathsf{C}_i} \otimes \mathbb{I}_{\mathsf{D}_i\mathsf{E}_i}\right) Q_i\right) \otimes \left(\mathsf{H}^{\otimes n} |x\rangle\langle x| \mathsf{H}^{\otimes n}\right)^{\otimes t}_{\mathsf{A}'_{1:t}}\right). \tag{8}$$

Let $d = 2^n$, $r = 2t+1$, $d' = 2^{a+1}$, and $r' = t+1$. Recall that $(\mathbb{C}^d)^{\otimes r} \otimes (\mathbb{C}^{d'})^{\otimes r'} \cong \bigoplus_{\boldsymbol{\lambda}} V_{\boldsymbol{\lambda}}$ decomposes into a collection of subspaces corresponding to binary type vectors $\boldsymbol{\lambda} \in \{0,1\}^d$. Here, $(\mathbb{C}^{d'})^{\otimes r'}$ serves as an auxiliary register; in terms of the notation in Section 4.1, we are taking $N = d$ and $M = d'^{r'}$ (in other words, we are packing all the players' ancillary registers into one auxiliary input).

Moreover, we assume going forward that $\mathfrak{F}$ is a $(4t+2)$-wise uniform family of functions from $\{0,1\}^n \to \{0,1\}$. As noted in Remark 8, this is statistically indistinguishable from instantiating $\mathfrak{F}$ as the family of all functions from $\{0,1\}^n \to \{0,1\}$, since the expression in Lemma A.2 has degree $4t+2$ in U_{f_θ}.

Then using Lemma A.2 and then Lemma 4.1, we get:

$$\begin{aligned}\omega_{\mathsf{S}}(\mathsf{G}) &= 2^{n(t-1)}\mathrm{Tr}\left[\mathop{\mathbb{E}}_{f}\left[\left(\mathsf{U}_f^{\otimes r}\otimes \mathbb{I}_{\mathsf{D}_{1:t+1}}\right)\,\Xi\,\left(\mathsf{U}_f^{\otimes r}\otimes \mathbb{I}_{\mathsf{D}_{1:t+1}}\right)\right]\rho\right] \\ &= 2^{n(t-1)}\sum_{\boldsymbol{\lambda}\in\{0,1\}^d}\mathrm{Tr}\left[\Pi_{\boldsymbol{\lambda}}\Xi\Pi_{\boldsymbol{\lambda}}\rho\right], \end{aligned} \tag{9}$$

where $\Pi_{\boldsymbol{\lambda}}$ is the projector onto the subspace of $(\mathbb{C}^d)^{\otimes r}\otimes(\mathbb{C}^{d'})^{\otimes(t+1)}$ given by

$$V_{\boldsymbol{\lambda}} = \mathrm{span}_{\mathbb{C}}\{|(v_1,\ldots,v_r,a_1,\ldots,a_{t+1})\rangle \,:\, \mathsf{BinType}(v_1,\ldots,v_r,a_1,\ldots,a_{t+1}) = \boldsymbol{\lambda}\}.$$

We now state a simple high-level bound on $\omega(\mathsf{G})$ in terms of *subtypes* $\boldsymbol{\mu}$. Unlike the bounds obtained using techniques in [TFKW13], this bound will depend on the Choi state ρ. This is *provably* necessary for any $t \geq 2$, as we will show in Section 6.1.

Lemma 5.1. *We have*

$$\omega(\mathsf{G}) \leq \exp(O(t\log t))\cdot 2^{n(t-1)}\cdot\sum_{\boldsymbol{\mu}}\mathrm{Tr}\left[\Pi_{\boldsymbol{\mu}}\rho\right]\cdot\left\|\Pi_{\boldsymbol{\mu}}\Xi\Pi_{\boldsymbol{\mu}}\right\|_{\infty}.$$

Proof. This follows immediately by plugging Lemma 4.8 into Equation (9). □

5.2 Expanding out Ξ using Subtypes

We now set up some additional notation. For each $i \in [t+1]$ and $j_1, j_2 \in [d]$ and $l_1, l_2 \in [d']$, we let $Q^{\dagger}_{i,(j_1,l_1);(j_2,l_2)}$ denote the entry in the (j_1,l_1)-th row and (j_2,l_2)-th column of the unitary $Q_i^{\dagger}$. To keep track of the ancillary indices in registers $\mathsf{D}_{1:t+1}$, we will introduce the values $z_1,\ldots,z_{t+1}\in[d']$ and denote $\mathbf{z} = (z_1,\ldots,z_{t+1})$ for brevity. We can now write the projector Ξ in Equation (8) as:

$$\Xi = \sum_{\substack{x\in\{0,1\}^n \\ z_1,\ldots,z_{t+1}\in\{0,1\}^a}} |\Xi^{x,\mathbf{z}}\rangle\langle\Xi^{x,\mathbf{z}}|\,, \text{ where}$$

$$\begin{aligned}|\Xi^{x,\mathbf{z}}\rangle &= Q_1^{\dagger}\left(|x\rangle\otimes|z_1\rangle\right)\otimes\cdots\otimes Q_{t+1}^{\dagger}\left(|x\rangle\otimes|z_{t+1}\rangle\right)\otimes\left(\mathsf{H}^{\otimes n}|x\rangle\right)^{\otimes t} \\ &= 2^{-nt/2}\sum_{\substack{v_1,\ldots,v_r\in[d] \\ w_1,\ldots,w_{t+1}\in[d']}}\left((-1)^{\langle v_{t+2}+\cdots+v_r,x\rangle}\prod_{i=1}^{t+1}Q^{\dagger}_{i,(v_i,w_i);(x,z_i)}\right)|v_1,\ldots,v_r\rangle\otimes|w_1,\ldots,w_{t+1}\rangle\,.\end{aligned}$$

We now begin unpacking the operator $\Pi_{\boldsymbol{\mu}}\Xi\Pi_{\boldsymbol{\mu}}$, using the formalism of subtypes introduced in Section 4.3. Recall that we have:

$$\begin{aligned}\Xi &= \sum_{\substack{x\in\{0,1\}^n \\ z_1,\ldots,z_{t+1}\in\{0,1\}^a}} |\Xi^{x,\mathbf{z}}\rangle\langle\Xi^{x,\mathbf{z}}| \\ \Rightarrow \Pi_{\boldsymbol{\mu}}\Xi\Pi_{\boldsymbol{\mu}} &= \sum_{\substack{x\in\{0,1\}^n \\ z_1,\ldots,z_{t+1}\in\{0,1\}^a}} \Pi_{\boldsymbol{\mu}}|\Xi^{x,\mathbf{z}}\rangle\langle\Xi^{x,\mathbf{z}}|\Pi_{\boldsymbol{\mu}}.\end{aligned}$$

Therefore we can define a matrix $\mathbf{A} \in \mathbb{C}^{d_1 \times d_2}$, where $d_1 = 2^{rn+(t+1)a}$ is the dimension of $|\Xi^{x,\mathbf{z}}\rangle$ and $d_2 = 2^{n+(t+1)a}$ is the number of possible values of $x, \mathbf{z}$. The columns of $\mathbf{A}$ are indexed by $x, \mathbf{z}$ and the corresponding column is exactly $\Pi_{\boldsymbol{\mu}} |\Xi^{x,\mathbf{z}}\rangle$. Then we have $\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}} = \mathbf{A}\mathbf{A}^\dagger \Rightarrow \|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\|_\infty = \|\mathbf{A}\|_\infty^2$.

Recall also that we have:

$$|\Xi^{x,\mathbf{z}}\rangle = 2^{-nt/2} \sum_{\substack{v_1,\dots,v_r \in [d] \\ w_1,\dots,w_{t+1} \in [d']}} \left((-1)^{\langle v_{t+2}+\cdots+v_r, x\rangle} \prod_{i=1}^{t+1} Q^\dagger_{i,(v_i,w_i);(x,z_i)} \right) |v_1,\dots,v_r\rangle \otimes |w_1,\dots,w_{t+1}\rangle .$$

Therefore, once we project onto the subspace corresponding to the subtype $\boldsymbol{\mu}$, we get the state

$$\Pi_{\boldsymbol{\mu}} |\Xi^{x,\mathbf{z}}\rangle = 2^{-nt/2} \sum_{\substack{v_1,\dots,v_r \in [d] \\ w_1,\dots,w_{t+1} \in [d'] \\ (\mathbf{v},\mathbf{w}) \in S_{\boldsymbol{\mu}}}} \left((-1)^{\langle v_{t+2}+\cdots+v_r, x\rangle} \prod_{i=1}^{t+1} Q^\dagger_{i,(v_i,w_i);(x,z_i)} \right) |v_1,\dots,v_r\rangle \otimes |w_1,\dots,w_{t+1}\rangle . \tag{10}$$

Now note that any row of $\mathbf{A}$ that does not correspond to a standard basis vector in $S_{\boldsymbol{\mu}}$ will be 0. We can discard all such rows without affecting the operator norm of A. We can therefore re-index the rows of $\mathbf{A}$ by the variable symbols $x_1, \dots, x_l$ of $\boldsymbol{\mu}$ and the ancilla indices $w_1, \dots, w_{t+1}$, so that $\mathbf{A}$ is effectively a $2^{nl+a(t+1)} \times 2^{n+a(t+1)}$ matrix.

With this setup in mind, we introduce a couple more definitions that will help us complete our analysis:

Definition 5.2. *Let $\ell \in [0,t]$ be an integer parameter (typically we will work with $\ell = t$). Let $\boldsymbol{\mu}$ be a subtype of $(\mathbb{C}^d)^{\otimes(t+1+\ell)} \otimes (\mathbb{C}^{d'})^{\otimes r'}$ with variable symbols $x_1, \dots, x_l$. Then, define the matrix*

$$\mathbf{B} := \mathbf{B}_{\boldsymbol{\mu}}(\mathbf{Q}_1, \dots, \mathbf{Q}_{t+1})$$

with dimensions $2^{nl+a(t+1)} \times 2^{n+a(t+1)}$ as follows:

Its rows are indexed by $y_1, \dots, y_l \in [d]$ and $w_1, \dots, w_{t+1} \in [d']$. Its columns are indexed by $x \in [d]$ and $z_1, \dots, z_{t+1} \in [d']$. For any such indices, take

$$(v_1, \dots, v_{t+1+\ell}, w_1, \dots, w_{t+1}) = \mathsf{Reconstruct}(\boldsymbol{\mu}, (y_1, \dots, y_l), (w_1, \dots, w_{t+1})) \in [d]^{t+1+\ell} \times [d']^{t+1}.$$

(The function Reconstruct *is defined in Definition 4.5.) Then we define the entry*

$$\mathbf{B}_{(y_1,\dots,y_l,w_1,\dots,w_{t+1});(x,z_1,\dots,z_{t+1})} = (-1)^{\langle v_{t+2}+\dots+v_{t+1+\ell}, x\rangle} \prod_{i=1}^{t+1} Q^\dagger_{i,(v_i,w_i);(x,z_i)}. \tag{11}$$

We remark that when $\ell = t$, this definition coincides with the matrix $2^{nt/2}A$. The reason we generalize to $\ell < t$ is for technical reasons; there could be variable symbols that only appear in the "phase entries" $v_{t+2}, \dots, v_{t+1+\ell}$, in which case they appear an even number of times and do not have any effect on the value of that entry in the matrix B. These variable symbols artificially blow up the operator norm of B and will need to be dealt with separately. To capture this, we have the following notion:

Definition 5.3. *For a subtype $\boldsymbol{\mu}$ with respect to $(\mathbb{C}^d)^{\otimes(t+1+\ell)} \otimes (\mathbb{C}^{d'})^{\otimes r'}$ and variable symbol x_i, we say x_i is a* free variable symbol *of $\boldsymbol{\mu}$ if it only appears in entries $t+2, t+3, \dots, t+1+\ell$ of $\boldsymbol{\mu}$. (Informally, a free variable symbol is one that only appears in the phase.)*

5.3 Bounding $\|\mathbf{B}_{\boldsymbol{\mu}}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{t+1})\|_\infty$

In this section, we provide estimates on the operator norm of $\mathbf{B}_{\boldsymbol{\mu}}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{t+1})$. We first begin with a lemma that allows us to dispose of free variable symbols:

Lemma 5.4. *Suppose $\boldsymbol{\mu}$ is a subtype with respect to $(\mathbb{C}^d)^{\otimes(2t+1)} \otimes (\mathbb{C}^{d'})^{\otimes r'}$, and suppose it has b free variable symbols that appear in a total of p positions in indices $k+2, k+3, \ldots, 2k+1$.*

Then define $\ell := t - p$, and $\boldsymbol{\mu}'$ to be the subtype with respect to $(\mathbb{C}^d)^{\otimes(t+1+\ell)} \otimes (\mathbb{C}^{d'})^{\otimes r'}$ obtained by taking $\boldsymbol{\mu}$ and removing all free variable symbols. Then we have

$$\|\mathbf{B}_{\boldsymbol{\mu}}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{t+1})\|_\infty = 2^{nb/2} \left\|\mathbf{B}_{\boldsymbol{\mu}'}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{t+1})\right\|_\infty.$$

Proof. For brevity, write $\mathbf{B} = \mathbf{B}_{\boldsymbol{\mu}}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{t+1})$ and $\mathbf{B}' = \mathbf{B}_{\boldsymbol{\mu}'}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{t+1})$. Let the variable symbols of $\boldsymbol{\mu}$ be $y_1, \ldots, y_l$, so that its free variable symbols are $y_{l-b+1}, \ldots, y_l$. Note that $\boldsymbol{\mu}'$ will have $l - b$ variable symbols, none of which are free variable symbols. Now since each free variable symbol appears an even number of times in the phase, we have for any indices that

$$B_{(y_1,\ldots,y_l,w_1,\ldots,w_{t+1});(x,z_1,\ldots,z_{t+1})} = B'_{(y_1,\ldots,y_{l-b},w_1,\ldots,w_{t+1});(x,z_1,\ldots,z_{t+1})}.$$

In other words, the matrix $\mathbf{B}$ is obtained by vertically stacking 2^{nb} copies of $\mathbf{B}'$ (up to a permutation of rows). Put another way, $\mathbf{B}$ is equal to B' tensored with a column vector consisting of 2^{nb} 1's. It follows by Lemma 2.10 that:

$$\|\mathbf{B}\|_\infty = \left\|\mathbf{B}'\right\|_\infty \cdot \left\| \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \right\|_\infty = 2^{nb/2} \left\|\mathbf{B}'\right\|_\infty.$$

□

For most of the remainder of this section, we focus on subtypes $\boldsymbol{\mu}$ that do not have any free variable symbols. We first set up some more notation. At a high level, the idea is to cluster the terms being multiplied in Equation (11) according to which of the variable symbols they depend on. This allows us to write B as a block column-wise tensor product of several much simpler block matrices, and then we will appeal to Lemma 2.18.

To this end, let $\boldsymbol{\mu}$ have variable symbols $x_1, \ldots, x_l$. For each for $i \in [l]$, let $I_i = \{j \in [t+1+\ell] : \boldsymbol{\mu}_j = x_i\}$ and $J = \{j \in [t+1+\ell] : \boldsymbol{\mu}_j \text{ is fixed}\}$. Note that $[t+1+\ell]$ is the disjoint union of $I_1, I_2, \ldots, I_l, J$. Also, for convenience we will make the following abuse of notation: for any integer h, subset $I \subseteq [h]$, and vector $\mathbf{b}$ with h entries, we use $\mathbf{b}_I$ to denote the sub-vector of length $|I|$ obtained by taking only the indices in I from $\mathbf{b}$. With this in mind, for each $i \in [l]$ define the following matrix $\mathbf{M}_i$ of dimensions $2^{n+a(|I_i|\cap[t+1])} \times 2^{n+a(|I_i|\cap[t+1])}$:

$$M_{i,(y_i,\mathbf{w}_{I_i\cap[t+1]});(x,\mathbf{z}_{I_i\cap[t+1]})} = \prod_{j\in I_i\cap[t+2,t+1+\ell]} (-1)^{\langle y_i,x\rangle} \cdot \prod_{j\in I_i\cap[t+1]} Q^\dagger_{j,(y_i,w_j);(x,z_j)}.$$

Additionally, define the following matrix $\mathbf{T}$ of dimensions $2^{a(|J|\cap[t+1])} \times 2^{n+a(|J|\cap[t+1])}$:

$$\mathbf{T}_{\mathbf{w}_{J\cap[t+1]};(x,\mathbf{z}_{J\cap[t+1]})} = \prod_{j\in J\cap[t+2,t+1+\ell]} (-1)^{\langle \boldsymbol{\mu}_j,x\rangle} \cdot \prod_{j\in J\cap[t+1]} Q^\dagger_{j,(\boldsymbol{\mu}_j,w_j);(x,z_j)}.$$

It is clear by inspection that $\mathbf{B}_{\boldsymbol{\mu}}$ is the result of applying the block column-wise tensoring operation described in Lemma 2.18 to $\mathbf{M}_1, \ldots, \mathbf{M}_l, \mathbf{T}$. Here, the block columns are indexed by x. We will proceed by applying this lemma to these matrices. We thus need to check that the preconditions of the lemma apply, which we do in the next few lemmas:

Lemma 5.5. *For any $x^* \in [2^n]$, consider the matrix $\mathbf{T}_{x^*}$ obtained by restricting $\mathbf{T}$ to columns where $x = x^*$. Then $\|\mathbf{T}_{x^*}\|_\infty \leq 1$. Moreover, if $J \cap [t+1]$ is nonempty, then we have $\|\mathbf{T}\|_\infty \leq 1$.*

Proof. We have:

$$T_{\mathbf{w}_{J\cap[t+1]};(x,\mathbf{z}_{J\cap[t+1]})} = \prod_{j\in J\cap[t+2,t+1+\ell]} (-1)^{\langle \boldsymbol{\mu}_j, x\rangle} \cdot \prod_{j\in J\cap[t+1]} Q^\dagger_{j,(\boldsymbol{\mu}_j,w_j);(x,z_j)}.$$

Now consider the matrix T' with the same dimensions as T defined by:

$$T'_{\mathbf{w}_{J\cap[t+1]};(x,\mathbf{z}_{J\cap[t+1]})} = \prod_{j\in J\cap[t+1]} Q^\dagger_{j,(\boldsymbol{\mu}_j,w_j);(x,z_j)}.$$

Since $\boldsymbol{\mu}_j$ is fixed for $j \in J$, $\mathbf{T}'$ can be obtained from $\mathbf{T}$ by just flipping the signs of some columns. This preserves the operator norm (this can be seen from Lemma 2.8 for example), so we have $\|\mathbf{T}'\|_\infty = \|\mathbf{T}\|_\infty$. It also follows analogously that $\|\mathbf{T}'_{x^*}\|_\infty = \|\mathbf{T}_{x^*}\|_\infty$, where we analogously define $\mathbf{T}'_{x^*}$ as the result of restricting $\mathbf{T}'$ to columns where $x = x^*$. At this point, we split into two cases:

- If $J \cap [t+1]$ is nonempty, we claim that $\mathbf{T}'$ is a submatrix of $\mathbf{Q} := \bigotimes_{j\in J\cap[t+1]} Q^\dagger_j$. Indeed, we can index the rows of $\mathbf{Q}$ by $(\mathbf{a}, \mathbf{b})$ and the columns by $(\mathbf{c}, \mathbf{d})$, and write

  $$Q_{(\mathbf{a},\mathbf{b});(\mathbf{c},\mathbf{d})} = \prod_{j\in J\cap[t+1]} Q^\dagger_{j,(a_j,b_j);(c_j,d_j)}.$$

  Then $\mathbf{T}'$ is the submatrix of $\mathbf{Q}$ obtained by restricting to rows $(\mathbf{a}, \mathbf{b})$ such that $a_j = \boldsymbol{\mu}_j$ for all $j \in J \cap [t+1]$ and columns $(\mathbf{c}, \mathbf{d})$ such that $c_{j_1} = c_{j_2}$ for any $j_1, j_2 \in J \cap [t+1]$.

  Since the operator norm of a unitary matrix is 1 and there is at least one unitary matrix in this tensor product, it follows from Lemmas 2.9 and 2.10 that $\|\mathbf{T}'\|_\infty \leq 1 \Rightarrow \|\mathbf{T}\|_\infty \leq 1$. Then, it also follows that $\|\mathbf{T}_{x^*}\|_\infty \leq 1$ by Lemma 2.9.

- If $J \cap [t+1]$ is empty then T' is really just a vector of 2^n many 1's. Hence T'_{x^*} is just the scalar 1, which trivially has operator norm ≤ 1.

□

Lemma 5.6. *Assume $\boldsymbol{\mu}$ does not have free variable symbols. For any $x^* \in [2^n]$ and $i \in [l]$, consider the matrix $\mathbf{M}_{i,x^*}$ obtained by restricting M_i to columns where $x = x^*$. Then $\|\mathbf{M}_{i,x^*}\|_\infty \leq 1$.*

Proof. We have:

$$\mathbf{M}_{i,(y_i,\mathbf{w}_{I_i\cap[t+1]});(x^*,\mathbf{z}_{I_i\cap[t+1]})} = \prod_{j\in I_i\cap[t+2,t+1+\ell]} (-1)^{\langle y_i, x^*\rangle} \cdot \prod_{j\in I_i\cap[t+1]} Q^\dagger_{j,(y_i,w_j);(x^*,z_j)}.$$

We can now define another matrix $\mathbf{M}'_{i,x^*}$ with the same dimensions as $\mathbf{M}_{i,x^*}$ defined by:

$$\mathbf{M}'_{(i,x^*),(y_i,\mathbf{w}_{I_i\cap[t+1]});\mathbf{z}_{I_i\cap[t+1]}} = \prod_{j\in I_i\cap[t+1]} Q^\dagger_{j,(y_i,w_j);(x^*,z_j)}.$$

Since we are fixing x^*, $\mathbf{M}'_{i,x^*}$ can be obtained from $\mathbf{M}_{i,x^*}$ by just flipping the signs of some rows. It follows that $\left\|\mathbf{M}'_{i,x^*}\right\|_\infty = \|\mathbf{M}_{i,x^*}\|_\infty$. Now to finish, we argue that $\mathbf{M}'_{i,x^*}$ is a submatrix of $\mathbf{Q} := \bigotimes_{j\in I_i\cap[t+1]} \mathbf{Q}^\dagger_j$. Note that $I_i \cap [t+1]$ must be non-empty as otherwise x_i would be a free variable symbol. Given this, this claim would imply the conclusion by Lemmas 2.9 and 2.10.

To see this claim, note that we can index the rows of $\mathbf{Q}$ by $(\mathbf{a},\mathbf{b})$ and the columns by $(\mathbf{c},\mathbf{d})$, and write:

$$Q_{(\mathbf{a},\mathbf{b});(\mathbf{c},\mathbf{d})} = \prod_{j\in I_i\cap[t+1]} Q^\dagger_{j,(a_j,b_j);(c_j,d_j)}.$$

Then $\mathbf{M}'_{i,x^*}$ is the submatrix of $\mathbf{Q}$ obtained by restricting to rows $(\mathbf{a},\mathbf{b})$ where $a_{j_1} = a_{j_2}$ for any $j_1, j_2 \in I_i \cap [t+1]$ and columns $(\mathbf{c},\mathbf{d})$ where $c_j = x^*$ for all $j \in I_i \cap [t+1]$. This completes the proof of the lemma. □

Lemma 5.7. *Assume $\boldsymbol{\mu}$ does not have free variable symbols. Consider some $i \in [l]$ such that the integer $|I_i \cap [t+2, t+1+\ell]|$ is even. Then, it holds that $\|\mathbf{M}_i\|_\infty \le 1$.*

Proof.

$$\begin{aligned} M_{i,(y_i,\mathbf{w}_{I_i\cap[t+1]});(x,\mathbf{z}_{I_i\cap[t+1]})} &= \prod_{j\in I_i\cap[t+2,t+1+\ell]} (-1)^{\langle y_i,x\rangle} \cdot \prod_{j\in I_i\cap[t+1]} Q^\dagger_{j,(y_i,w_j);(x,z_j)} \\ &= \prod_{j\in I_i\cap[t+1]} Q^\dagger_{j,(y_i,w_j);(x,z_j)}, \end{aligned}$$

since there are an even number of identical terms being multiplied together in the first product. In this case, we just argue that $\mathbf{M}_i$ is a submatrix of $\mathbf{Q} := \bigotimes_{j\in I_i\cap[t+1]} \mathbf{Q}^\dagger_j$. This is a non-empty tensor product since otherwise x_i would be a free variable symbol. Given this, this claim would imply the conclusion by Lemmas 2.9 and 2.10.

To see this claim, we once again index the rows of $\mathbf{Q}$ by $(\mathbf{a},\mathbf{b})$ and the columns by $(\mathbf{c},\mathbf{d})$, and write:

$$Q_{(\mathbf{a},\mathbf{b});(\mathbf{c},\mathbf{d})} = \prod_{j\in I_i\cap[t+1]} Q^\dagger_{j,(a_j,b_j);(c_j,d_j)}.$$

Then, $\mathbf{M}_i$ is the submatrix of $\mathbf{Q}$ obtained by restricting to rows $(\mathbf{a},\mathbf{b})$ such that $a_{j_1} = a_{j_2}$ for any $j_1, j_2 \in I_i \cap [t+1]$ and columns $(\mathbf{c},\mathbf{d})$ such that $c_{j_1} = c_{j_2}$ for any $j_1, j_2 \in I_i \cap [t+1]$. This completes the proof of the lemma. □

Our final technical lemma handles the case where a variable symbol appears multiple times among $v_1, \ldots, v_{t+1}$:

Lemma 5.8. *Consider some $i \in [l]$ be such that $|I_i \cap [t+1]| \ge 2$ (we are assuming that such i exists; this may not always be the case). Then*

$$\|\mathbf{M}_i\|_\infty \le 1.$$

Proof. Firstly, if $|I_i \cap [t+1]|$ is even, then by the parity constraints (the variable symbol x_i should appear an even number of times in $\boldsymbol{\mu}$), we must also have that $|I_i \cap [t+2, t+1+\ell]|$ is even. In this case, the conclusion would follow from Lemma 5.7. Hence from now on we assume that $|I_i \cap [t+1]|$ is odd. We hence have:

$$\mathbf{M}_{i,(y_i,\mathbf{w}_{I_i\cap[t+1]});(x,\mathbf{z}_{I_i\cap[t+1]})} = \prod_{j\in I_i\cap[t+2,t+1+\ell]} (-1)^{\langle y_i,x\rangle} \cdot \prod_{j\in I_i\cap[t+1]} Q^\dagger_{j,(y_i,w_j);(x,z_j)}$$

$$= (-1)^{\langle y_i, x\rangle} \cdot \prod_{j \in I_i \cap [t+1]} Q^{\dagger}_{j,(y_i,w_j);(x,z_j)}.$$

The conclusion now follows by applying Lemma 2.19 with the following inputs:

- We will take $R = C = 2^n$, and $d = |I_i \cap [t+1]| \geq 2$. (In fact, $d \geq 3$ since $|I_i \cap [t+1]|$ is odd, but this will not matter for us.)
- The matrices will be $\left\{\mathbf{Q}_j^{\dagger} \in \mathbb{C}^{2^{n+a} \times 2^{n+a}}\right\}_{j \in I_i \cap [t+1]}$. Accordingly, we will have

  $$r_1 = \ldots = r_R = c_1 = \ldots = c_C = d'.$$

  These matrices are unitary so they have operator norm exactly 1.
- For each $y_i, x \in \{0,1\}^n$, the scalar $\gamma_{y_i,x}$ will be $(-1)^{\langle y_i, x\rangle}$, which clearly has magnitude 1.

□

Finally, we can put these lemmas together to prove the bounds that we want:

Lemma 5.9. *Suppose $\boldsymbol{\mu}$ is a subtype with respect to $(\mathbb{C}^d)^{\otimes 2t+1} \otimes (\mathbb{C}^{d'})^{r'}$ with b free variable symbols. Then we have $\|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\|_{\infty} \leq 2^{-nt+nb}$.*

Moreover, when $t = 1$, we must have $b = 0$ and hence $\|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\|_{\infty} \leq 2^{-n}$.

Proof. We first address the final claim about the $t = 1$ case. Indeed, a subtype with respect to $(\mathbb{C}^d)^{\otimes 2t+1} \otimes (\mathbb{C}^{d'})^{\otimes t+1} = (\mathbb{C}^d)^{\otimes 3} \otimes (\mathbb{C}^{d'})^{\otimes 2}$ cannot have free variable symbols. Definition 5.3 states that a free variable symbol of $\boldsymbol{\mu}$ could only appear in entry 3 of $\boldsymbol{\mu}$. But a free variable symbol must appear an even number of times (as specified by Definition 4.2), so in fact it cannot appear at all. Now let us turn to proving the desired bound.

Now let $\boldsymbol{\mu}'$ be defined as in the statement of Lemma 5.4 i.e. it is $\boldsymbol{\mu}$ but with free variable symbols removed. Then we would like to show:

$$\begin{aligned} \|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\|_{\infty} &\leq 2^{-nt+nb} \\ \Leftrightarrow \|\mathbf{A}\|_{\infty}^2 &\leq 2^{-nt+nb} \\ \Leftrightarrow \|\mathbf{B}_{\boldsymbol{\mu}}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{k+1})\|_{\infty}^2 &\leq 2^{nb} \\ \Leftrightarrow \left\|\mathbf{B}_{\boldsymbol{\mu}'}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{k+1})\right\|_{\infty} &\leq 1. \text{ (Lemma 5.4)} \end{aligned}$$

Let $\boldsymbol{\mu}'$ have l variable symbols. As hinted at earlier, we will bound this by applying Lemma 2.18 to the matrices $\mathbf{M}_1, \ldots, \mathbf{M}_l$ and $\mathbf{T}$ defined with respect to $\boldsymbol{\mu}'$. The first precondition follows from Lemmas 5.5 and 5.6. To check the second precondition, we need only show that $\min(\|\mathbf{M}_1\|_{\infty}, \ldots, \|\mathbf{M}_l\|_{\infty}, \|\mathbf{T}\|_{\infty}) \leq 1$. For this, we have some light casework:

1. If at least one of $\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_{t+1}$ is fixed, then $J \cap [t+1]$ is nonempty, so it follows that $\|T\|_{\infty} \leq 1$ by Lemma 5.5.
2. Otherwise, all of $\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_{t+1}$ must be variable symbols. However, every variable symbol must appear at least twice and we only have $2t+1$ entries in total, so the total number of variable symbols must be $\leq t$. Therefore by the pigeonhole principle, some two of $\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_{t+1}$ are the same variable symbol i.e. there exists $i \in [l]$ such that $|I_i \cap [t+1]| \geq 2$. In this case, Lemma 5.8 tells us that $\|\mathbf{M}_i\|_{\infty} \leq 1$.

□

5.4 Combinatorial Lemmas about Free Variable Symbols

In the case where $t > 1$, free variable symbols could exist, and as indicated by Lemma 5.9, they can blow up the operator norms we care about. To mitigate this, we establish some simple lemmas about free variable symbols:

Definition 5.10. *For any $l \in [t]$, define the projector Γ_l over $(\mathbb{C}^d)^{\otimes r} \otimes (\mathbb{C}^{d'})^{\otimes(t+1)}$ as the projector onto*

$$W_l := \mathrm{span}_{\mathbb{C}}\{|(v_1, \ldots, v_r, a_1, \ldots, a_{t+1})\rangle \ : \ \textit{exactly } l \textit{ distinct values among } v_{t+2}, \ldots, v_r\}.$$

Lemma 5.11. *We have*

$$\sum_{b \le t/2} \sum_{\boldsymbol{\mu} \textit{ with } b \textit{ free variable symbols}} 2^{nb} \Pi_{\boldsymbol{\mu}} \le \exp(O(t \log t)) \cdot \sum_{l \le t} 2^{n(t-l)} \Gamma_l,$$

with respect to the PSD ordering.

Proof. Note that the LHS and RHS are both diagonal in the standard basis. Hence it suffices to show for any $\mathbf{x} = (v_1, \ldots, v_r, a_1, \ldots, a_{t+1})$ that:

$$\sum_{b \le t/2} \sum_{\boldsymbol{\mu} \text{ with } b \text{ free variable symbols}} 2^{nb} \langle \mathbf{x} | \Pi_{\boldsymbol{\mu}} | \mathbf{x} \rangle \le \exp(O(t \log t)) \cdot \sum_{l \le t} 2^{n(t-l)} \langle \mathbf{x} | \Gamma_l | \mathbf{x} \rangle .$$

Let l^* be the number of distinct values among $v_{t+2}, \ldots, v_r$, then the RHS is $\exp(O(t \log t)) \cdot 2^{n(t-l^*)}$. On the other hand, the LHS is equal to:

$$\sum_{b \le t/2} \sum_{\substack{\boldsymbol{\mu} \text{ with } b \text{ free variable symbols} \\ \mathbf{x} \in S_{\boldsymbol{\mu}}}} 2^{nb}.$$

Now consider any subtype $\boldsymbol{\mu}$ with b free variable symbols such that $\mathbf{x} \in S_{\boldsymbol{\mu}}$. Each of its b free variable symbols must appear at least twice among $v_{t+2}, \ldots, v_r$ due to the parity constraint, which implies that we must have $l^* \le t - b \Leftrightarrow b \le t - l^*$. Hence every term in the above sum is at most $2^{n(t-l^*)}$. Moreover, by Lemma 4.6, there are at most $\exp(O(t \log t))$ subtypes $\boldsymbol{\mu}$ with $\mathbf{x} \in S_{\boldsymbol{\mu}}$, so there are at most $\exp(O(t \log t))$ terms in the above sum. It follows that the LHS is at most $\exp(O(t \log t)) \cdot 2^{n(t-l^*)}$, which is exactly the RHS, as desired. □

We make one more observation:

Lemma 5.12. *The number of tuples $(x_1, \ldots, x_t) \in [2^n]^t$ with l distinct values is at most $\exp(t \log t) \cdot 2^{nl}$.*

Proof. There are at most 2^{nl} ways to choose the l distinct values. Then there are $l^t \le t^t = \exp(t \log t)$ ways to assign a value to each individual x_i. The conclusion follows. □

Next, we present the only specific property of the shared state ρ that we need. In the following, we partition the Hilbert space $(\mathbb{C}^d)^{\otimes r} \otimes (\mathbb{C}^{d'})^{\otimes t+1}$ as the tensor product of Hilbert spaces on the following systems:

- R_1: this consists of the values $(v_{t+2}, \ldots, v_r)$. Thus $\mathcal{H}_{\mathsf{R}_1} \cong (\mathbb{C}^d)^{\otimes t}$.
- R_2: all other values i.e. $(v_1, \ldots, v_{t+1}, a_1, \ldots, a_{t+1})$. Thus $\mathcal{H}_{\mathsf{R}_2} \cong (\mathbb{C}^d)^{\otimes t+1} \otimes (\mathbb{C}^{d'})^{\otimes t+1}$.

Lemma 5.13. *We have*

$$\mathrm{Tr}_{\mathsf{R}_2}[\rho] = 2^{-nt} \cdot \mathbb{I}_{\mathsf{R}_1}.$$

Informally, if we take ρ and trace out the system R_2, we are left with a maximally mixed state.

Proof. We have by definition that:

$$\begin{aligned}
\rho &= (\mathbb{I}_{\mathsf{R}_1} \otimes \Phi_{\mathsf{R}_2}) \left(|\mathsf{EPR}\rangle\langle\mathsf{EPR}|^{\otimes nt}_{\mathsf{R}_1,\mathsf{R}_2} \right) \\
&= 2^{-nt} \cdot \sum_{\mathbf{x},\mathbf{y} \in [2^n]^t} (\mathbb{I}_{\mathsf{R}_1} \otimes \Phi) \left(|\mathbf{x}\rangle\langle\mathbf{y}|_{\mathsf{R}_1} \otimes |\mathbf{x}\rangle\langle\mathbf{y}|_{\mathsf{R}_2} \right) \\
&= 2^{-nt} \cdot \sum_{\mathbf{x},\mathbf{y} \in [2^n]^t} |\mathbf{x}\rangle\langle\mathbf{y}|_{\mathsf{R}_1} \otimes \Phi(|\mathbf{x}\rangle\langle\mathbf{y}|)_{\mathsf{R}_2} \\
\Rightarrow \mathrm{Tr}_{\mathsf{R}_2}[\rho] &= 2^{-nt} \cdot \sum_{\mathbf{x},\mathbf{y} \in [2^n]^t} |\mathbf{x}\rangle\langle\mathbf{y}|_{\mathsf{R}_1} \cdot \mathrm{Tr}\left[\Phi(|\mathbf{x}\rangle\langle\mathbf{y}|)_{\mathsf{R}_2}\right] \\
&= 2^{-nt} \cdot \sum_{\mathbf{x} \in [2^n]^t} |\mathbf{x}\rangle\langle\mathbf{x}|_{\mathsf{R}_1},
\end{aligned}$$

which implies the conclusion. In the last step, we are using the fact that Φ is trace-preserving. □

Finally, we put these two together to show the following:

Lemma 5.14. *For any integer $l \in [1, t]$, we have*

$$\mathrm{Tr}[\Gamma_l \rho] \leq \exp(t \log t) \cdot 2^{-nt+nl}.$$

Proof. We can clearly write

$$\Gamma_l = \Gamma'_{l,\mathsf{R}_1} \otimes \mathbb{I}_{\mathsf{R}_2},$$

where Γ'_l is the projector onto standard basis vectors $|v_{t+2}, \ldots, v_r\rangle$ with exactly l distinct values. We hence have:

$$\begin{aligned}
\mathrm{Tr}[\Gamma_l \rho] &= \mathrm{Tr}\left[\left(\Gamma'_{l,\mathsf{R}_1} \otimes \mathbb{I}_{\mathsf{R}_2}\right) \rho\right] \\
&= \mathrm{Tr}\left[\Gamma'_{l,\mathsf{R}_1} \left(\mathrm{Tr}_{\mathsf{R}_2} \rho\right)\right] \\
&= 2^{-nt} \cdot \mathrm{Tr}\left[\Gamma'_{l,\mathsf{R}_1}\right] \text{ (Lemma 5.13)} \\
&\leq \exp(t \log t) \cdot 2^{-nt+nl},
\end{aligned}$$

where in the last step we are using the fact that Γ'_{l,R_1} is a projector together with Lemma 5.12. □

5.5 Putting Everything Together

In this section, we complete our treatment of the case of $t \mapsto t+1$ cloning games for $t > 1$. Our bounds here are once again independent of the number of ancilla qubits a used by each player.

Theorem 5.15. *Let $\mathfrak{F}$ be a $(4t+2)$-wise uniform family of functions from $\{0,1\}^n \to \{0,1\}$. Then for all n, we have*

$$\sup_{\mathsf{S} \in \mathcal{S}_{\mathrm{rest}}} \omega_{\mathsf{S}}(\mathsf{G}_{\mathfrak{F},t}) \leq \exp(O(t \log t)) \cdot 2^{-n}.$$

Proof. For any strategy $\mathsf{S} \in \mathcal{S}_{\text{rest}}$, we have:

$$\begin{aligned}
\omega_{\mathsf{S}}(\mathsf{G}) &\leq \exp(O(t \log t)) \cdot 2^{n(t-1)} \cdot \sum_{\boldsymbol{\mu}} \operatorname{Tr}\left[\Pi_{\boldsymbol{\mu}} \rho\right] \cdot \left\|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\right\|_{\infty} \text{ (Lemma 5.1)} \\
&\leq \exp(O(t \log t)) \cdot 2^{n(t-1)} \cdot \sum_{b \leq t/2} \sum_{\boldsymbol{\mu} \text{ with } b \text{ free variable symbols}} 2^{-nt+nb} \cdot \operatorname{Tr}\left[\Pi_{\boldsymbol{\mu}} \rho\right] \text{ (Lemma 5.9)} \\
&\leq \exp(O(t \log t)) \cdot 2^{-n} \cdot \sum_{l \leq t} 2^{n(t-l)} \cdot \operatorname{Tr}\left[\Gamma_l \rho\right] \text{ (Lemma 5.11)} \\
&\leq \exp(O(t \log t)) \cdot 2^{-n} \cdot \sum_{l \leq t} 2^{n(t-l)} \cdot 2^{-nt+nl} \text{ (Lemma 5.14)} \\
&\leq \exp(O(t \log t)) \cdot 2^{-n},
\end{aligned}$$

as desired. □

6 Limitations of Analyzing Monogamy Games Using Existing Techniques

In this section, we revisit the existing techniques laid out by [TFKW13] for upper bounding the value of monogamy games (and hence cloning games in particular). We begin by summarizing their technique and main result, modifying the presentation to accommodate the multi-copy setting. For a particular strategy S, define the operator

$$\Pi^{\theta} := |\mathcal{X}|^{t-1} \cdot \sum_{x \in \mathcal{X}} \left(\bigotimes_{i=1}^{t+1} \mathbf{P}_{i,x}^{\theta} \otimes (\mathbf{A}_x^{\theta})^{\otimes t} \right), \text{ where we define} \tag{12}$$

$$\mathbf{A}_x^{\theta} := \bar{U}_{\theta} |x\rangle\langle x|_{\mathsf{A}} \bar{U}_{\theta}^{\dagger}.$$

Then, by Lemma A.2, we have:

$$\begin{aligned}
\omega_{\mathsf{S}}(\mathsf{G}) &= \mathop{\mathbb{E}}_{\theta \sim \Theta} \left[\operatorname{Tr}\left[\Pi^{\theta} \rho \right] \right] \\
&\leq \left\| \mathop{\mathbb{E}}_{\theta \sim \Theta} \left[\Pi^{\theta} \right] \right\|_{\infty},
\end{aligned} \tag{13}$$

since ρ has trace 1 (by Lemma 2.14). To bound this in the $t = 1$ case, they show the following result:

Theorem 6.1 (Essentially [TFKW13], Theorem 4)**.** *When $t = 1$, we have*

$$\begin{aligned}
\left\| \mathop{\mathbb{E}}_{\theta \sim \Theta} \left[\Pi^{\theta} \right] \right\|_{\infty} &\leq \frac{1}{|\Theta|} + \frac{|\Theta| - 1}{|\Theta|} \cdot \max_{\substack{\theta, \theta' \in \Theta \\ \theta \neq \theta'}} \max_{x, x' \in \mathcal{X}} \left\| \sqrt{\mathbf{A}_x^{\theta}} \sqrt{\mathbf{A}_{x'}^{\theta'}} \right\|_{\infty} \\
&= \frac{1}{|\Theta|} + \frac{|\Theta| - 1}{|\Theta|} \cdot \max_{\substack{\theta, \theta' \in \Theta \\ \theta \neq \theta'}} \max_{x, x' \in \mathcal{X}} \left\| \mathbf{A}_x^{\theta} \mathbf{A}_{x'}^{\theta'} \right\|_{\infty}.
\end{aligned}$$

(The second line holds because $\mathbf{A}_x^{\theta}$ is always a projector.)

Using this theorem, they are able to show that the BB84 monogamy game has value $\frac{1}{2} + \frac{1}{2\sqrt{2}}$. Moreover, they show that the n-fold parallel repetition of the BB84 monogamy game has value $\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n$. These techniques have since been adapted by [CV22, SS25] to cloning games based on coset states as well. In this section, we will demonstrate three things that we previously alluded to in Section 1.2.1:

- Section 6.1: In the case of the case of multi-copy cloning games (i.e. $t > 1$), we will show that ignoring the shared state ρ can *provably* lose too much. Specifically, we will show for any $\{U_\theta\}$ with real entries, there exist projectors $\mathbf{P}^\theta_{i,x}$ such that

$$\left\| \mathop{\mathbb{E}}_{\theta\sim\Theta} \left[\Pi^\theta\right] \right\|_\infty \geq 1.$$

  Moreover, we will show this even if $\mathbf{P}^\theta_{i,x}$ does not even depend on θ. (This can informally be thought of as the case where the players $\mathcal{P}_1, \ldots, \mathcal{P}_{t+1}$ are never given access to the basis θ in any form.)

  Since previous constructions [TFKW13, BL20, CLLZ21, CV22, SS25] as well as our binary phase state construction only make use of unitaries with real entries, this justifies the necessity of our finer analysis in Section 5.4 of the specific structure imposed on the shared state ρ by the oracular cloning setting.

- Section 6.2: For the single-copy case, we will demonstrate another inherent limitation that arises from the [TFKW13] approach of bounding a spectral norm in terms of the maximal pairwise overlap $\max_{\theta\neq\theta'} \left\|\mathbf{A}^\theta_x \mathbf{A}^{\theta'}_{x'}\right\|_\infty$. Namely, we will show that this pairwise overlap is provably at least $1/\sqrt{|\mathcal{X}|} = 2^{-n/2}$ (as opposed to the ideal $O(2^{-n})$ for any monogamy game). Recall from Section 1.3 that this is crucial for our application to black hole physics (we will elaborate on this more in Section 8 and Remark 14 in particular).

  Thus, in order to bypass this limitation of Theorem 6.1, we need entirely new techniques. This is yet another reason why we restrict attention to *oracular cloning games* (defined in Section 3.2) and analyze these with a completely different technique based on binary subtypes in Section 5.

- Finally, for completeness, we show in Section 6.3 that this bound of $2^{-n/2}$ is essentially tight in the single-copy case; we will show that a slight tweak of our binary phase state construction — introduced in Section 1.2.3 and fleshed out in Section 5 — yields a different monogamy game with $\mathcal{X} = \{0,1\}^n$ and maximal pairwise overlap $\leq 2^{-n/2+o(n)}$. This only requires the existence of sub-exponentially *classically* secure PRFs.

6.1 Limitations of Bounding the Operator Norm Directly

Recall that, in Section 5, we proved a multi-copy cloning bound with the assistance of a careful analysis (in Section 5.4) of the structure of the shared state ρ defined in Equation (7), namely the structure specified by Lemma 5.13. In this section, we argue that this more careful approach is likely *necessary*:

Lemma 6.2. *Consider any $t > 1$ and projectors $\left\{\mathbf{A}^\theta_x = \bar{U}_\theta |x\rangle\langle x| \bar{U}^\dagger_\theta\right\}$ such that U_θ has real entries for all θ i.e. $U_\theta = \bar{U}_\theta$. Then there exist projectors $\mathbf{P}^\theta_{i,x}$ such that, if Π^θ is defined as in Equation (12), then we have:*

$$\left\| \mathop{\mathbb{E}}_{\theta\sim\Theta} \left[\Pi^\theta\right] \right\|_\infty \geq |\mathcal{X}|^{\lfloor t/2 \rfloor - 1}.$$

Moreover, this bound can be attained even if these projectors need not depend at all on θ. Note that for any $t \geq 2$, the RHS is ≥ 1 so this implies that Equation (13) does not give any non-trivial bound on the value of the corresponding cloning game.

Proof. Fix some element $y \in \mathcal{X}$. For all i, θ, we will define $\mathbf{P}_{i,x}^{\theta}$ to be $\mathbb{I}$ if $x = y$ and 0 otherwise. In other words, each player is simply going to guess $x = y$ deterministically. Then Equation (12) tells us that:

$$\Pi^{\theta} = |\mathcal{X}|^{t-1} \cdot \left(\bigotimes_{i=1}^{t+1} \mathbb{I} \otimes \left(\mathbf{A}_y^{\theta}\right)^{\otimes t} \right)$$
$$\Rightarrow \left\| \mathop{\mathbb{E}}_{\theta \sim \Theta} \left[\Pi^{\theta}\right] \right\|_{\infty} = |\mathcal{X}|^{t-1} \cdot \left\| \mathop{\mathbb{E}}_{\theta \sim \Theta} \left[\left(\mathbf{A}_y^{\theta}\right)^{\otimes t} \right] \right\|_{\infty}.$$

To finish, it suffices to exhibit some mixed state ρ such that:

$$\mathrm{Tr}\left[\mathop{\mathbb{E}}_{\theta \sim \Theta} \left[\left(\mathbf{A}_y^{\theta}\right)^{\otimes t} \right] \rho \right] \geq |\mathcal{X}|^{\lfloor t/2 \rfloor - t}. \tag{14}$$

Define the bit $b = t \bmod 2$, and let

$$\rho := \left(\bigotimes_{i=1}^{\lfloor t/2 \rfloor} |\mathsf{EPR}_{\mathcal{X}}\rangle\langle \mathsf{EPR}_{\mathcal{X}}| \right) \otimes \left(\frac{1}{|\mathcal{X}|} \mathbb{I}_{\mathcal{X}} \right)^{\otimes b}.$$

In other words, we let ρ comprise $\lfloor t/2 \rfloor$ EPR qudits supported on $\mathcal{X}$, and in the event that t is odd we also include one qudit that is maximally mixed on $\mathcal{X}$. Intuitively, we will use the entanglement between each EPR pair to increase the probability that the t measurements specified by $\left\{\mathbf{A}_x^{\theta}\right\}$ measurements all output y. Indeed, for any particular θ we have:

$$\begin{aligned}
\mathrm{Tr}\left[\left(\mathbf{A}_y^{\theta}\right)^{\otimes t} \rho \right] &= \left(\mathrm{Tr}\left[\left(\mathbf{A}_y^{\theta}\right)^{\otimes 2} |\mathsf{EPR}_{\mathcal{X}}\rangle\langle \mathsf{EPR}_{\mathcal{X}}| \right] \right)^{\lfloor t/2 \rfloor} \cdot \frac{1}{|\mathcal{X}|^b} \\
&= \left(\frac{1}{|\mathcal{X}|} \mathrm{Tr}\left[\mathbf{A}_y^{\theta} \overline{\mathbf{A}_y^{\theta}} \right] \right)^{\lfloor t/2 \rfloor} \cdot \frac{1}{|\mathcal{X}|^b} \text{ (Corollary 2.2)} \\
&= \left(\frac{1}{|\mathcal{X}|} \mathrm{Tr}\left[\mathbf{A}_y^{\theta} \mathbf{A}_y^{\theta} \right] \right)^{\lfloor t/2 \rfloor} \cdot \frac{1}{|\mathcal{X}|^b} \text{ (U_θ has real entries)} \\
&= |\mathcal{X}|^{-\lfloor t/2 \rfloor - b} \cdot \left(\mathrm{Tr}\left[U_\theta |y\rangle\langle y| U_\theta^{\dagger} U_\theta |y\rangle\langle y| U_\theta^{\dagger} \right] \right)^{\lfloor t/2 \rfloor} \\
&= |\mathcal{X}|^{-\lfloor t/2 \rfloor - b} \\
&= |\mathcal{X}|^{\lfloor t/2 \rfloor - t}.
\end{aligned}$$

In the above application of Corollary 2.2, we are taking $\mathbf{P} = \mathbf{A}_y^{\theta}, \mathbf{Q} = \overline{\mathbf{A}_y^{\theta}}$, and Φ to be the identity map. Now taking expectation over θ immediately yields Equation (14), as desired. □

6.2 Limitations of Bounding Pairwise Overlaps

Here, we show that the framework laid out by [TFKW13] of using Theorem 6.1 to bound monogamy games cannot prove a better bound than $1/\sqrt{|\mathcal{X}|}$ (see the statement of Theorem 6.1).

Lemma 6.3. *If $|\Theta| \geq 2$, then we have*

$$\max_{\substack{\theta,\theta' \in \Theta \\ \theta \neq \theta'}} \max_{x,x' \in \mathcal{X}} \left\| \sqrt{\mathbf{A}_x^\theta} \sqrt{\mathbf{A}_{x'}^{\theta'}} \right\|_\infty = \max_{\substack{\theta,\theta' \in \Theta \\ \theta \neq \theta'}} \max_{x,x' \in \mathcal{X}} \left\| \mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'} \right\|_\infty \geq \frac{1}{\sqrt{|\mathcal{X}|}}.$$

Proof. The first equality follows since the measurements are projective, so $\sqrt{\mathbf{A}_x^\theta} = \mathbf{A}_x^\theta$. Now for any distinct $\theta, \theta' \in \Theta$, we will show that

$$\max_{x,x' \in \mathcal{X}} \left\| \mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'} \right\|_\infty \geq \frac{1}{\sqrt{|\mathcal{X}|}}.$$

Indeed, fix any $x' \in \mathcal{X}$ such that $\mathbf{A}_{x'}^{\theta'}$ is nonzero (such x' exists since $\sum_{x'} \mathbf{A}_{x'}^{\theta'} = \mathbb{I}$) and consider an arbitrary state $|\psi\rangle$ in the image of $\mathbf{A}_{x'}^{\theta'}$. Then we have:

$$\begin{aligned} |\psi\rangle &= \sum_{x \in \mathcal{X}} \mathbf{A}_x^\theta |\psi\rangle \\ &= \sum_{x \in \mathcal{X}} \mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'} |\psi\rangle \\ \Rightarrow 1 &= \left\| \sum_{x \in \mathcal{X}} \mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'} |\psi\rangle \right\|_2^2. \end{aligned}$$

For each $x \in \mathcal{X}$, let $|\psi_x\rangle = \mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'} |\psi\rangle$, where $|\psi_x\rangle$ may not be normalized. Note for any $x \neq y$ that $\langle \psi_x | \psi_y \rangle = \langle \psi | \mathbf{A}_{x'}^{\theta'} \mathbf{A}_x^\theta \mathbf{A}_y^\theta \mathbf{A}_{x'}^{\theta'} | \psi \rangle = 0$, since $\mathbf{A}_x^\theta \mathbf{A}_y^\theta = 0$. Hence the $|\psi_x\rangle$'s are mutually orthogonal, implying that:

$$\begin{aligned} 1 &= \left\| \sum_{x \in \mathcal{X}} |\psi_x\rangle \right\|_2^2 \\ &= \sum_{x \in \mathcal{X}} \| |\psi_x\rangle \|_2^2. \end{aligned}$$

Hence there exists $x \in \mathcal{X}$ such that $\| |\psi_x\rangle \|_2^2 \geq 1/|\mathcal{X}| \Rightarrow \| |\psi_x\rangle \|_2 \geq 1/\sqrt{|\mathcal{X}|}$. For this x, we have:

$$\begin{aligned} \frac{1}{\sqrt{|\mathcal{X}|}} &\leq \| |\psi_x\rangle \|_2 \\ &= \left\| \mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'} |\psi\rangle \right\|_2 \\ &\leq \left\| \mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'} \right\|_\infty, \end{aligned}$$

as desired. □

6.3 Monogamy Bounds from Binary Phase States

We just showed in Section 6.2 that using Theorem 6.1 to bound a monogamy game with $\mathcal{X} = \{0,1\}^n$, we can only hope to prove a bound of $2^{-n/2}$. On the other hand, no existing analyses saturate this bound:

the best known upper bound for the coset monogamy game is $O(2^{-n/4})$, due to [SS25][15], and the BB84 monogamy game attains value $\approx 2^{-0.228n}$.

In this section, we close this gap. Specifically, we will show that a variant of our binary phase construction used in Section 5 satisfies $\omega(\mathsf{G}) \leq 2^{-n/2+o(n)}$, and that this can be shown following the [TFKW13] methodology and using Theorem 6.1. For details on how exactly our results in this section differ from those in Section 5, we refer the reader to Remark 13.

Lemma 6.4. *Suppose we have $\mathbf{A}_x^\theta = \mathsf{V}_\theta |x\rangle\langle x| \mathsf{V}_\theta^\dagger$ for some unitaries V_θ. Then for any $x, x' \in \mathcal{X}$ and $\theta, \theta' \in \Theta$, we have*

$$\left\| \sqrt{\mathbf{A}_x^\theta} \sqrt{\mathbf{A}_{x'}^{\theta'}} \right\|_\infty = \left\| \mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'} \right\|_\infty = \left| \langle x | \mathsf{V}_\theta^\dagger \mathsf{V}_{\theta'} | x' \rangle \right|.$$

Proof. Note firstly that the ℓ_∞ norm of any rank 1 Hermitian PSD matrix is equal to its trace (see Lemma 2.8). Bearing this in mind, we have:

$$\begin{aligned}
\left\| \mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'} \right\|_\infty^2 &= \left\| \mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'} \mathbf{A}_{x'}^{\theta'\dagger} \mathbf{A}_x^{\theta\dagger} \right\|_\infty \\
&= \left\| \mathsf{V}_\theta |x\rangle\langle x| \mathsf{V}_\theta^\dagger \cdot \mathsf{V}_{\theta'} |x'\rangle\langle x'| \mathsf{V}_{\theta'}^\dagger \cdot \mathsf{V}_{\theta'} |x'\rangle\langle x'| \mathsf{V}_{\theta'}^\dagger \cdot \mathsf{V}_\theta |x\rangle\langle x| \mathsf{V}_\theta^\dagger \right\|_\infty \\
&= \mathrm{Tr}\left[\mathsf{V}_\theta |x\rangle\langle x| \mathsf{V}_\theta^\dagger \cdot \mathsf{V}_{\theta'} |x'\rangle\langle x'| \mathsf{V}_{\theta'}^\dagger \cdot \mathsf{V}_{\theta'} |x'\rangle\langle x'| \mathsf{V}_{\theta'}^\dagger \cdot \mathsf{V}_\theta |x\rangle\langle x| \mathsf{V}_\theta^\dagger \right] \\
&= \left| \langle x | \mathsf{V}_\theta^\dagger \mathsf{V}_{\theta'} | x' \rangle \right|^2 \cdot \mathrm{Tr}\left[\mathsf{V}_\theta |x\rangle \langle x'| \mathsf{V}_{\theta'}^\dagger \cdot \mathsf{V}_{\theta'} |x'\rangle \langle x| \mathsf{V}_\theta^\dagger \right] \\
&= \left| \langle x | \mathsf{V}_\theta^\dagger \mathsf{V}_{\theta'} | x' \rangle \right|^2,
\end{aligned}$$

which implies the conclusion. □

We now describe our PRF-based construction. We stress that we only require the PRF to be secure against classical adversaries, and we do not assume that Bob and Charlie are computationally bounded. The reasons for this will become clear later, and are summarized in Remark 12. Some other helpful remarks on this construction and its analysis can be found in Remark 13.

Construction 2. *Let $\mathfrak{F} = \left\{ F_k : \{0,1\}^{m+n} \to \{0,1\} \right\}_{k \in \{0,1\}^\lambda}$ be a PRF family. (Here, $m := m(\lambda)$ and $n := n(\lambda)$ should be thought of as small polynomials in the security parameter λ e.g. $\lambda^{0.1}$.) For any $k \in \{0,1\}^\lambda$ and $\theta \in \{0,1\}^m$, define the "salted" function $f_{k,s} : \{0,1\}^n \to \{0,1\}$ by $f_{k,\theta}(x) = F_k(\theta || x)$.*

Then for any $k \in \{0,1\}^\lambda$, we define the monogamy game $\mathsf{G}_{\mathfrak{F},k}$ as follows:

- *The Hilbert space $\mathcal{H}_\mathsf{A}$ is $\mathcal{C}^{2^n}$.*
- *The set of questions Θ is $\{0,1\}^m$.*
- *The set of answers $\mathcal{X}$ is $\{0,1\}^n$.*
- *For any $\theta \in \{0,1\}^m$ and $x \in \{0,1\}^n$, we define the following:*

$$\mathsf{V}_\theta = \mathsf{U}_{f_{k,\theta}} \mathsf{H}^{\otimes n}, \text{ and}$$

[15] Previous work [SSS24] proved an upper bound of $O(2^{-n/2})$ in a setting where the cloner Φ is restricted to splitting the state as is into two equal-sized halves, sending one to Bob and the other to Charlie. We cite $O(2^{-n/4})$ as the state of the art, as we are interested in games where the cloner Φ is unrestricted.

$$\mathbf{A}_x^\theta = \mathsf{V}_\theta \left|x\right\rangle\!\left\langle x\right| \mathsf{V}_\theta^\dagger,$$

where $\mathsf{U}_{f_{k,\theta}}$ is the phase unitary defined in Section 4.2.

Remark 10. *Our use of PRF security is already quite unconventional; the PRF key k should be thought of here as a public parameter that is known to all parties (including Bob and Charlie) before the monogamy game commences.*

Remark 11. *At first glance, this "salting" construction appears unnatural; it would be much more natural to consider a PRF family $\{F_k : \{0,1\}^n \to \{0,1\}\}_{k\in\{0,1\}^\lambda}$, set $\Theta = \{0,1\}^\lambda$, and set $\mathsf{V}_\theta = \mathsf{U}_{F_\theta}\mathsf{H}^{\otimes n}$ (where $\theta \in \{0,1\}^\lambda$ is the PRF key).*

The problem with this is that we will be analyzing this construction using Theorem 6.1, which considers the worst-case *overlap across different $\theta, \theta' \in \{0,1\}^\lambda$, while PRF security would only give us a "with high probability" guarantee with respect to θ, which is insufficient for us.*

To remedy this, we salt the PRF so that the "with high probability" guarantee is absorbed into the setup phase of the construction. In other words, this can be thought of as a "randomized monogamy game" (where the new randomization occurs during the setup phase). We can now obtain the desired worst-case overlap bounds using simple concentration bounds, as we will see next.

Our starting point to analyze Construction 2 is the following lemma:

Lemma 6.5 (Essentially [O'D21], Exercise 5.8)**.** *Let $F : \{0,1\}^{m+n} \to \{-1,1\}$ be a random function. For any $s \in \{0,1\}^m$, define $f_s : \{0,1\}^n \to \{-1,1\}$ by $f_s(u) = F(s,u)$. Then with probability $1 - O(2^{-n})$ over the randomness of F, we have*

$$\max_{r\neq s} \max_{w\in\{0,1\}^n} \left|\mathbb{E}_u \left[(-1)^{\langle w,u\rangle} f_r(u) f_s(u)\right]\right| \leq 2\cdot 2^{-n/2}\sqrt{m+n}.$$

Proof. We will first argue for any fixed r, s, w then take a union bound at the end. If we let $G(u) = f_r(u)f_s(u) = F(r,u)F(s,u)$, it is clear that G is itself a random function from $\{0,1\}^n \to \{-1,1\}$ (noting that we get independence because $r \neq s$). Hence we just want to bound

$$\left|\mathbb{E}_u \left[(-1)^{\langle w,u\rangle} G(u)\right]\right|.$$

For each u, $(-1)^{\langle w,u\rangle}G(u)$ is an independent and uniformly random sample from $\{-1,1\}$, so this quantity can be bounded with a straightforward Chernoff bound. Indeed, Hoeffding's inequality tells us that:

$$\begin{aligned}\Pr\left[\left|\mathbb{E}_u \left[(-1)^{\langle w,u\rangle} G(u)\right]\right| > 2\cdot 2^{-n/2}\sqrt{m+n}\right] &\leq 2\exp\left(\frac{-4\cdot 2^n\cdot(m+n)}{2^{n+1}}\right)\\ &= 2\exp(-2(m+n)).\end{aligned}$$

Taking a union bound over 2^m choices of r, 2^m choices of s, and 2^n choices of w implies that:

$$\begin{aligned}\Pr\left[\max_{r\neq s}\max_{w\in\{0,1\}^n}\left|\mathbb{E}_u \left[(-1)^{\langle w,u\rangle} G(u)\right]\right| > 2\cdot 2^{-n/2}\sqrt{m+n}\right] &\leq 2^{2m+n}\cdot 2\exp(-2(m+n))\\ &= O(2^{-n}).\end{aligned}$$

□

Corollary 6.6. *Assume that the PRF family $\mathfrak{F}$ is $(2^{m+n}, \epsilon(\lambda))$-classically secure i.e. a classical distinguisher that runs in time $\mathsf{poly}(2^{m+n})$ can only distinguish a function sampled from $\mathfrak{F}$ from a truly random function with advantage $\leq \epsilon(\lambda)$. Then with probability $1 - O(2^{-n}) - \epsilon(\lambda)$ over the randomness of $k \leftarrow \{0,1\}^\lambda$, we have*

$$\max_{r \neq s} \max_{w \in \{0,1\}^n} \left| \mathbb{E}_u \left[(-1)^{\langle w,u \rangle + f_{k,r}(u) + f_{k,s}(u)} \right] \right| \leq 2 \cdot 2^{-n/2} \sqrt{m+n}.$$

Proof. Consider the following PRF distinguisher given oracle access to some function F: it simply iterates over all r, s, w, u and computes

$$\max_{r \neq s} \max_{w \in \{0,1\}^n} \left| \mathbb{E}_u \left[(-1)^{\langle w,u \rangle + F(r,u) + F(s,u)} \right] \right|,$$

and outputs 1 if the result is $> 2 \cdot 2^{-n/2} \sqrt{m+n}$. This distinguisher runs in time $\mathsf{poly}(2^{m+n})$. By Lemma 6.5, it outputs 1 given a random function with probability at most $O(2^{-n})$ (noting that the outputs of F are in $\{0,1\}$, so the outputs of $(-1)^{F(\cdot)}$ are in $\{-1,1\}$ as in Lemma 6.5). Hence by PRF security, it outputs 1 given a function sampled from $\mathfrak{F}$ with probability at most $O(2^{-n}) + \epsilon(\lambda)$. The conclusion follows. □

Note that a PRF with this security guarantee can be instantiated assuming sub-exponentially secure PRFs since λ is a large polynomial in $m+n$. With this corollary, we can prove an upper bound on the value of our monogamy game:

Theorem 6.7. *Assume (as in Corollary 6.6) that the PRF family $\mathfrak{F}$ is $(2^{m+n}, \epsilon(\lambda))$-classically secure i.e. a classical distinguisher that runs in time $\mathsf{poly}(2^{m+n})$ can only distinguish a function sampled from $\mathfrak{F}$ from a truly random function with advantage $\leq \epsilon(\lambda)$. Then with probability $1 - O(2^{-n}) - \epsilon(\lambda)$ over the randomness of $k \leftarrow \{0,1\}^\lambda$, we have:*

$$\omega(\mathsf{G}_{\mathfrak{F},k}) \leq O(2^{-m} + 2^{-n/2}\sqrt{m+n}).$$

Proof. By Theorem 6.1 and the analysis preceding it, we have:

$$\omega(\mathsf{G}_{\mathfrak{F},k}) \leq 2^{-m} + (1 - 2^{-m}) \cdot \max_{\substack{\theta,\theta' \in \{0,1\}^m \\ \theta \neq \theta'}} \max_{x,x' \in \{0,1\}^n} \left\| \sqrt{\mathbf{A}_x^\theta} \sqrt{\mathbf{A}_{x'}^{\theta'}} \right\|_\infty.$$

Hence it suffices to show that

$$\max_{\substack{\theta,\theta' \in \{0,1\}^m \\ \theta \neq \theta'}} \max_{x,x' \in \{0,1\}^n} \left\| \sqrt{\mathbf{A}_x^\theta} \sqrt{\mathbf{A}_{x'}^{\theta'}} \right\|_\infty \leq O(2^{-n/2}\sqrt{m+n}).$$

Indeed, we have:

$$\begin{aligned}
\left\| \sqrt{\mathbf{A}_x^\theta} \sqrt{\mathbf{A}_{x'}^{\theta'}} \right\|_\infty &= \left| \langle x | \mathsf{V}_\theta^\dagger \mathsf{V}_{\theta'} | x' \rangle \right| \text{ (Lemma 6.4)} \\
&= \left| \langle x | \mathsf{H}^{\otimes n} \mathsf{U}_{f_{k,\theta}} \mathsf{U}_{f_{k,\theta'}} \mathsf{H}^{\otimes n} | x' \rangle \right| \\
&= \frac{1}{2^n} \left| \sum_{y,y' \in \{0,1\}^n} (-1)^{\langle x,y \rangle + \langle x',y' \rangle} \langle y | \mathsf{U}_{f_{k,\theta}} \mathsf{U}_{f_{k,\theta'}} | y' \rangle \right|
\end{aligned}$$

$$= \frac{1}{2^n} \left| \sum_{y,y' \in \{0,1\}^n} (-1)^{\langle x,y\rangle + \langle x',y'\rangle + f_{k,\theta}(y) + f_{k,\theta'}(y')} \langle y|y'\rangle \right|$$

$$= \left| \mathop{\mathbb{E}}_{y \leftarrow \{0,1\}^n} \left[(-1)^{\langle x+x',y\rangle + f_{k,\theta}(y) + f_{k,\theta'}(y)} \right] \right|$$

$$\Rightarrow \max_{\substack{\theta,\theta' \in \{0,1\}^m \\ \theta \neq \theta'}} \max_{x,x' \in \{0,1\}^n} \left\| \sqrt{\mathbf{A}_x^\theta} \sqrt{\mathbf{A}_{x'}^{\theta'}} \right\|_\infty = \max_{\substack{\theta,\theta' \in \{0,1\}^m \\ \theta \neq \theta'}} \max_{x,x' \in \{0,1\}^n} \left| \mathop{\mathbb{E}}_{y \leftarrow \{0,1\}^n} \left[(-1)^{\langle x+x',y\rangle + f_{k,\theta}(y) + f_{k,\theta'}(y)} \right] \right|$$

$$\leq O(2^{-n/2}\sqrt{m+n}),$$

with probability at least $1 - O(2^{-n}) - \epsilon(\lambda)$ over the randomness of k by Corollary 6.6 (noting that we can consolidate the max over x and x' into a single max over $w := x + x'$). □

Remark 12. *Our use of PRF security is only to prove the concentration bound in Corollary 6.6, and hence we only need security against classical adversaries. Once we have this bound, we are applying Theorem 6.7 which holds against computationally unbounded Bob and Charlie. Therefore, although our construction is based on a cryptographic assumption, it is secure even against computationally unbounded adversaries Bob and Charlie.*

Remark 13. *We make some other comparisons between this construction and other constructions:*

- *Compared with the very similar construction (Construction 1) based on binary phase states in Section 5:*
  - *Theorem 6.7 only establishes a bound of $\tilde{O}(2^{-n/2})$ in the single-copy setting. In comparison, in Section 5 we show a bound of $O_t(2^{-n})$ in the t-copy setting.*
  - *On the other hand, Theorem 6.7 holds in a much stronger attack model; the players Bob and Charlie are given the basis θ in the clear and are computationally unbounded. On the other hand, in Section 5 we restrict the players to each make a single query to U_f.*
- *Compared with the BB84 [TFKW13, BL20] and coset state [CLLZ21, CV22, SS25] constructions, we show a better bound in the same attack model. However, we need to use a cryptographic assumption (sub-exponentially classically secure PRFs).*

7 Worst-Case to Average-Case Reduction

In this section, we show that $t \mapsto t+1$ oracular cloning games admit a worst-case to average-case reduction: even the hardest games which are specified by some worst-case unitary U_w can be won by a strategy for the average-case version of the game that involves a Haar-like unitary U_a from an appropriate unitary design, or alternatively from a pseudorandom unitary ensemble.

We begin with a technical background section on mixed unitary designs; equipped with this machinery, we can then complete the proof of our worst-case to average-case reduction.

7.1 Preliminary: Mixed Unitary Designs

We first review some relevant background on the vectorization technique.

Vectorization Formalism. For a linear operator $\mathbf{\Lambda} \in \mathrm{L}(\mathbb{C}^d)$, we consider the corresponding vectorization map $\mathrm{vec} : \mathrm{L}(\mathbb{C}^d) \to (\mathbb{C}^d)^{\otimes 2}$ which is defined as follows:

$$\mathbf{\Lambda} = \sum_{i,j\in[d]} \Lambda_{(i,j)} |i\rangle\langle j| \quad \mapsto \quad \mathrm{vec}(\mathbf{\Lambda}) := |\mathbf{\Lambda}\rangle\!\rangle = \sum_{i,j\in[d]} \Lambda_{(i,j)} |i\rangle \otimes |j\rangle \,.$$

We are also going to use the so-called ABC-rule [Mel24]: for any linear operators $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathrm{L}(\mathbb{C}^d)$,

$$|\mathbf{ABC}\rangle\!\rangle = (\mathbf{A} \otimes \mathbf{C}^\intercal)\, |\mathbf{B}\rangle\!\rangle.$$

We now introduce a "mixed variant" of the regular vectorized moment operator [Mel24].

Definition 7.1 (Mixed-Adjoint Moment Operator)**.** *Let ν be an ensemble of unitary operators over $\mathbb{C}^d$. Then, we define the mixed-adjoint (p,q)-moment operator $\mathcal{M}^{(p,q)}_{\nu,\mathsf{adj}} : \mathrm{L}(\mathbb{C}^d) \to \mathrm{L}(\mathbb{C}^d)$ by*

$$\mathcal{M}^{(p,q)}_{\nu,\mathsf{adj}}(\mathbf{O}) := \mathop{\mathbb{E}}_{U\sim\nu} \left[(U^{\otimes p} \otimes (U^\dagger)^{\otimes q})\mathbf{O}(U^{\otimes p} \otimes (U^\dagger)^{\otimes q})^\dagger\right]$$

for a linear operator $\mathbf{O} \in \mathrm{L}((\mathbb{C}^d)^{\otimes(p+q)})$. Similarly, we let $\mathcal{M}^{(p,q)}_{\mathrm{U}(d),\mathsf{adj}}$ denote the mixed-adjoint (p,q)-moment operator with respect to the Haar measure over the unitary group $\mathcal{U}_d$.

It turns out that the mixed-adjoint moment operator allows for a particularly neat characterization of mixed unitary designs introduced in Section 2.2. In particular, we show the following equivalence.

Lemma 7.2. *A unitary ensemble ν over $\mathbb{C}^d$ is a (non-adaptive) unitary (p,q)-design if and only if*

$$\mathop{\mathbb{E}}_{U\sim\nu} \left[U^{\otimes p} \otimes (U^\dagger)^{\otimes q} \otimes \bar{U}^{\otimes p} \otimes (U^\intercal)^{\otimes q}\right] = \mathop{\mathbb{E}}_{U\sim\mathrm{U}(d)} \left[U^{\otimes p} \otimes (U^\dagger)^{\otimes q} \otimes \bar{U}^{\otimes p} \otimes (U^\intercal)^{\otimes q}\right].$$

Proof. Suppose that ν is a unitary (p,q)-design. Then, for all $\mathbf{O} \in \mathrm{L}((\mathbb{C}^d)^{\otimes(p+q)})$, it holds that

$$\mathcal{M}^{(p,q)}_{\nu,\mathsf{adj}}(\mathbf{O}) = \mathcal{M}^{(p,q)}_{\mathrm{U}(d),\mathsf{adj}}(\mathbf{O}).$$

By applying the vectorization $\mathrm{vec} : \mathrm{L}((\mathbb{C}^d)^{\otimes(p+q)}) \to ((\mathbb{C}^d)^{\otimes(p+q)})^{\otimes 2}$ on both sides, we get

$$|\mathcal{M}^{(p,q)}_{\nu,\mathsf{adj}}(\mathbf{O})\rangle\!\rangle = |\mathcal{M}^{(p,q)}_{\mathrm{U}(d),\mathsf{adj}}(\mathbf{O})\rangle\!\rangle.$$

By linearity and the ABC-rule for $\mathrm{vec}(\cdot)$, this is equivalent to

$$\mathop{\mathbb{E}}_{U\sim\nu} \left[U^{\otimes p} \otimes (U^\dagger)^{\otimes q} \otimes \bar{U}^{\otimes p} \otimes (U^\intercal)^{\otimes q}\right] |\mathbf{O}\rangle\!\rangle = \mathop{\mathbb{E}}_{U\sim\mathrm{U}(d)} \left[U^{\otimes p} \otimes (U^\dagger)^{\otimes q} \otimes \bar{U}^{\otimes p} \otimes (U^\intercal)^{\otimes q}\right] |\mathbf{O}\rangle\!\rangle.$$

Because $\mathrm{vec}(\cdot)$ is a bijection between $\mathrm{L}((\mathbb{C}^d)^{\otimes(p+q)})$ and $((\mathbb{C}^d)^{\otimes(p+q)})^{\otimes 2}$, the operators above must be identical on the entire vector space $((\mathbb{C}^d)^{\otimes(p+q)})^{\otimes 2}$. The converse statement can be shown analogously. □

Lemma 7.3. *A unitary t-design ν is a mixed unitary (p,q)-design for any p, q with $t = p + q$.*

Proof. Let $t = p + q$. According to Theorem 7.2, it suffices to show that ν satisfies

$$\mathop{\mathbb{E}}_{U\sim\nu}\left[U^{\otimes p}\otimes(U^\dagger)^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes(U^\intercal)^{\otimes q}\right] = \mathop{\mathbb{E}}_{U\sim\mathrm{U}(d)}\left[U^{\otimes p}\otimes(U^\dagger)^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes(U^\intercal)^{\otimes q}\right].$$

By inserting the partial transpose with respect to the 2nd and 4th system, this is equivalent to

$$\mathop{\mathbb{E}}_{U\sim\nu}\left[U^{\otimes p}\otimes\bar{U}^{\otimes q}\otimes\bar{U}^{\otimes q}\otimes U^{\otimes p}\right]^{\mathsf{T}_{2,4}} = \mathop{\mathbb{E}}_{U\sim\mathrm{U}(d)}\left[U^{\otimes p}\otimes\bar{U}^{\otimes q}\otimes\bar{U}^{\otimes q}\otimes U^{\otimes p}\right]^{\mathsf{T}_{2,4}}.$$

After inserting a SWAP between the 2nd and 4th system via $\mathbb{F}_{2,4}$, it is also equivalent to showing that

$$\left[\mathbb{F}_{2,4}^\dagger\mathop{\mathbb{E}}_{U\sim\nu}\left[U^{\otimes p}\otimes U^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes\bar{U}^{\otimes q}\right]\mathbb{F}_{2,4}\right]^{\mathsf{T}_{2,4}} = \left[\mathbb{F}_{2,4}^\dagger\mathop{\mathbb{E}}_{U\sim\mathrm{U}(d)}\left[U^{\otimes p}\otimes U^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes\bar{U}^{\otimes q}\right]\mathbb{F}_{2,4}\right]^{\mathsf{T}_{2,4}}.$$

By assumption, ν is a unitary t-design for $t = p + q$, and hence it holds that

$$\mathop{\mathbb{E}}_{U\sim\nu}\left[U^{\otimes p}\otimes U^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes\bar{U}^{\otimes q}\right] = \mathop{\mathbb{E}}_{U\sim\mathrm{U}(d)}\left[U^{\otimes p}\otimes U^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes\bar{U}^{\otimes q}\right]$$

which yields the desired equality from before. □

Finally, we show that an (exact) non-adaptive mixed unitary t-design is automatically also an (exact) adaptive mixed unitary t-design. In the approximate case, this conversion incurs an exponential blow-up.

Theorem 7.4. *Any exact non-adaptive unitary t-design is also an exact adaptive mixed unitary t-design.*

Proof. Let ν be a non-adaptive unitary t-design over $\mathbb{C}^d$. Suppose that $\mathcal{A}^{U,U^\dagger}(1^{\lceil\log d\rceil})$ is an adaptive t-query quantum algorithm that makes p many queries to U and q queries to $U^\dagger$, for $U \in \mathrm{U}(d)$ and $t = p + q$.

The idea is to use a standard gate teleportation approach, similar to [AMR19, Kre21]. Concretely, we can argue that, for any $U \in \mathrm{U}(d)$, there exists a non-adaptive algorithm $\mathcal{B}^{U,U^\dagger}(1^{\lceil\log d\rceil})$ that makes p many parallel queries to U and q many parallel queries to $U^\dagger$ such that

$$\Pr\left[1 \leftarrow \mathcal{A}^{U,U^\dagger}(1^{\lceil\log d\rceil})\right] = d^{2(p+q)}\Pr\left[1 \leftarrow \mathcal{B}^{U,U^\dagger}(1^{\lceil\log d\rceil})\right].$$

This essentially follows from [Kre21, Lemma 23], since the non-adaptive query algorithm has access to both U and $U^\dagger$. Because ν is a non-adaptive unitary t-design, we know from Theorem 7.3 that ν is also mixed unitary (p, q)-design. Putting everything together, we get that

$$\begin{aligned}\Pr\left[1 \leftarrow \mathcal{A}^{U,U^\dagger}(1^{\lceil\log d\rceil}) \,:\, U\sim\nu\right] &= d^{2(p+q)}\Pr\left[1 \leftarrow \mathcal{B}^{U,U^\dagger}(1^{\lceil\log d\rceil}) \,:\, U\sim\nu\right]\\ &= d^{2(p+q)}\Pr\left[1 \leftarrow \mathcal{B}^{U,U^\dagger}(1^{\lceil\log d\rceil}) \,:\, U\sim\mathrm{U}(d)\right]\\ &= \Pr\left[1 \leftarrow \mathcal{A}^{U,U^\dagger}(1^{\lceil\log d\rceil}) \,:\, U\sim\mathrm{U}(d)\right].\end{aligned}$$

This proves the claim. □

7.2 Proof of the Reduction

Using the technical machinery on mixed unitary designs from the previous section, we can finally prove our worst-case to average-case reduction for cloning games.

Theorem 7.5 (Worst-Case to Average-Case Reduction)**.** *Let $n, t \in \mathbb{N}$ and let $\nu = \{U_a\}_{a\in\Theta}$ be an ensemble of n-qubit unitaries to be specified later. Suppose there exists a quantum strategy*

$$\mathsf{S}^{\mathsf{avg}} = (\mathcal{H}_{\mathsf{B}^{t+1}}, \Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}, \{\mathbf{P}_{1,x}^{U_a,U_a^\dagger}\}_{a\in\Theta,\, x\in\{0,1\}^n}, \ldots, \{\mathbf{P}_{t+1,x}^{U_a,U_a^\dagger}\}_{a\in\Theta,\, x\in\{0,1\}^n})$$

for the average-case $t \mapsto t+1$ oracular cloning game $\mathsf{G}^{\mathsf{avg}}_{t\mapsto t+1} = (t, \mathcal{H}_{\mathsf{A}^t}, \Theta, \{0,1\}^n, \{U_a\}_{a\in\Theta})$, where the $t+1$ players make no more than a total of q many oracle queries to either U_a or $U_a^\dagger$ combined, and

$$\omega_{\mathsf{S}^{\mathsf{avg}}}(\mathsf{G}^{\mathsf{avg}}_{t\mapsto t+1}) = \epsilon.$$

Then, there exists a quantum strategy (in which the $t+1$ many players make the same number of queries)

$$\mathsf{S}^{\mathsf{wst}} = (\mathcal{H}_{\tilde{\mathsf{B}}^{t+1}}, \tilde{\Phi}_{\mathsf{A}^t\to\tilde{\mathsf{B}}^{t+1}}, \{\tilde{\mathbf{P}}_{1,x}^{V_w,V_w^\dagger}\}_{x\in\{0,1\}^n}, \ldots, \{\tilde{\mathbf{P}}_{t+1,x}^{V_w,V_w^\dagger}\}_{x\in\{0,1\}^n})$$

for any $t \mapsto t+1$ oracular cloning game $\mathsf{G}^{\mathsf{wst}}_{t\mapsto t+1} = (t, \mathcal{H}_{\mathsf{A}^t}, \Theta', \{0,1\}^n, \{V_w\}_{w\in\Theta'})$ in the worst-case (i.e., for any adversarially chosen ensemble of n-qubit unitaries $\{V_w\}_{w\in\Theta'}$), such that:

- *If ν is an exact unitary r-design, for $r = t + q$ and $q \in \mathbb{N}$: we will have*

$$\omega_{\mathsf{S}^{\mathsf{wst}}}(\mathsf{G}^{\mathsf{wst}}_{t\mapsto t+1}) = \epsilon.$$

- *If ν is a pseudorandom unitary family with security parameter λ, and the adversaries $(\Phi, \mathcal{P}_1, \ldots, \mathcal{P}_{t+1})$ are computationally bounded: we will have*

$$\omega_{\mathsf{S}^{\mathsf{wst}}}(\mathsf{G}^{\mathsf{wst}}_{t\mapsto t+1}) \geq \epsilon - \mathsf{negl}(\lambda).$$

Proof. Let $\mathsf{G}^{\mathsf{wst}}_{t\mapsto t+1} = (t, \mathcal{H}_{\mathsf{A}^t}, \Theta', \{0,1\}^n, \{V_w\}_{w\in\Theta'})$ be a worst-case $t \mapsto t+1$ oracular cloning game for ensemble of unitaries $\{V_w\}$. Consider the quantum strategy $\mathsf{S}^{\mathsf{wst}}$ for the game $\mathsf{G}^{\mathsf{wst}}_{t\mapsto t+1}$ which internally uses $\mathsf{S}^{\mathsf{avg}}$ and proceeds as follows:

- (Cloning Channel:) on input $(V_w |x\rangle)^{\otimes t}$ in register A^t, the channel $\tilde{\Phi}_{\mathsf{A}^t\to\tilde{\mathsf{B}}^{t+1}}$ proceeds as follows:
  1. Sample a uniformly random unitary $U_a \sim \nu$ from the unitary ensemble ν.
  2. Apply U_a to each copy of $V_w |x\rangle$, resulting in a state $(U_a V_w |x\rangle)^{\otimes t}$ in register A^t.
  3. Run $\Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}$ on $(U_a V_w |x\rangle)^{\otimes t}$, and let $\mathsf{B}^{t+1} = \mathsf{B}_1 \cdots \mathsf{B}_{t+1}$ denote the resulting registers.
  4. Output $\tilde{\mathsf{B}}^{t+1} := \tilde{\mathsf{B}}_1 \cdots \tilde{\mathsf{B}}_{t+1}$, where $\tilde{\mathsf{B}}_i$ consists of B_i together with $\mathsf{B}'_i = |a\rangle\langle a|$, for $i \in [t+1]$.
- (i-th Player:) On input $\tilde{\mathsf{B}}_i$, the measurement $\{\tilde{\mathbf{P}}_{i,x}^{V_w,V_w^\dagger}\}_{x\in\{0,1\}^n}$ proceeds as follows:
  1. Parse $\tilde{\mathsf{B}}_i$ as $\mathsf{B}_i\mathsf{B}'_i$. Measure B'_i to obtain the string a.
  2. Run the oracle-aided measurement $\{\mathbf{P}_{i,x}^{U,U^\dagger}\}_{x\in\{0,1\}^n}$ with respect to $U := U_a V_w$ in such a way that, whenever one of the q-many oracle queries to U or $U^\dagger$ is submitted:

– If the query is to U: the query is first submitted to the available oracle V_w, then the unitary U_a is applied to the resulting outcome.
– If the query is to $U^\dagger$: the unitary $U_a^\dagger$ is applied, and the resulting outcome submitted to the available oracle $V_w^\dagger$.

Let us now analyze the success probability $\omega_{\mathsf{S}^{\mathsf{wst}}}(\mathsf{G}^{\mathsf{wst}}_{t\mapsto t+1})$ of the strategy $\mathsf{S}^{\mathsf{wst}}$. We first address the case where ν is an exact unitary r-design. Recall from Theorem 7.4 that any exact (non-adaptive) unitary r-design is also an exact adaptive r-design. Therefore, using that ν is an adaptive unitary r-design, for $r = t + q$, as well as the right-invariance of the Haar measure over the unitary group $\mathrm{U}(2^n)$, we get:

$$
\begin{aligned}
&\mathop{\mathbb{E}}_{\substack{x\sim\{0,1\}^n\\ w\sim\Theta'}} \mathrm{Tr}\left[\left(\tilde{\mathbf{P}}^{V_w,V_w^\dagger}_{1,x}\otimes\ldots\otimes\tilde{\mathbf{P}}^{V_w,V_w^\dagger}_{t+1,x}\right)\tilde{\Phi}_{\mathsf{A}^t\to\tilde{\mathsf{B}}^{t+1}}\left((V_w\left|x\right\rangle\!\left\langle x\right|V_w^\dagger)^{\otimes t}_{\mathsf{A}^t}\right)\right]\\
&=\mathop{\mathbb{E}}_{U_a\sim\nu}\mathop{\mathbb{E}}_{\substack{x\sim\{0,1\}^n\\ w\sim\Theta'}}\mathrm{Tr}\left[\left(\mathbf{P}^{U_aV_w,(U_aV_w)^\dagger}_{1,x}\otimes\ldots\otimes\mathbf{P}^{U_aV_w,(U_aV_w)^\dagger}_{t+1,x}\right)\Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}\left((U_aV_w\left|x\right\rangle\!\left\langle x\right|(U_aV_w)^\dagger)^{\otimes t}_{\mathsf{A}^t}\right)\right]\\
&=\mathop{\mathbb{E}}_{W\sim\mathrm{U}(2^n)}\mathop{\mathbb{E}}_{\substack{x\sim\{0,1\}^n\\ w\sim\Theta'}}\mathrm{Tr}\left[\left(\mathbf{P}^{WU_w,(WU_w)^\dagger}_{1,x}\otimes\ldots\otimes\mathbf{P}^{WU_w,(WU_w)^\dagger}_{t+1,x}\right)\Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}\left((WV_w\left|x\right\rangle\!\left\langle x\right|(WV_w)^\dagger)^{\otimes t}_{\mathsf{A}^t}\right)\right]\\
&=\mathop{\mathbb{E}}_{U\sim\mathrm{U}(2^n)}\mathop{\mathbb{E}}_{x\sim\{0,1\}^n}\mathrm{Tr}\left[\left(\mathbf{P}^{U,U^\dagger}_{1,x}\otimes\ldots\otimes\mathbf{P}^{U,U^\dagger}_{t+1,x}\right)\Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}\left((U\left|x\right\rangle\!\left\langle x\right|U^\dagger)^{\otimes t}_{\mathsf{A}^t}\right)\right]\\
&=\mathop{\mathbb{E}}_{U_a\sim\nu}\mathop{\mathbb{E}}_{x\sim\{0,1\}^n}\mathrm{Tr}\left[\left(\mathbf{P}^{U_a,U_a^\dagger}_{1,x}\otimes\ldots\otimes\mathbf{P}^{U_a,U_a^\dagger}_{t+1,x}\right)\Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}\left((U_a\left|x\right\rangle\!\left\langle x\right|U_a^\dagger)^{\otimes t}_{\mathsf{A}^t}\right)\right].
\end{aligned}
$$

Therefore, we get that $\omega_{\mathsf{S}^{\mathsf{wst}}}(\mathsf{G}^{\mathsf{wst}}_{t\mapsto t+1}) = \omega_{\mathsf{S}^{\mathsf{avg}}}(\mathsf{G}^{\mathsf{avg}}_{t\mapsto t+1}) = \epsilon$, which proves the claim. In the case that ν is a PRU family and the adversary is computationally bounded, we can apply essentially the same calculation, but we will incur a potential additive loss of $\mathsf{negl}(\lambda)$ when passing from U_a to the Haar measure. (Note that we can appeal to PRU security because the strategy $\mathsf{S}^{\mathsf{wst}}$ can be simulated using only oracle access to $U_a, U_a^\dagger$.) □

8 Black Hole Cloning Games

Hayden and Preskill [HP07] put forward the idea that the dynamics of a black hole are well-described by a random unitary time-evolution operator, e.g., via a *unitary design*. Does such a scrambling process limit the extent to which black holes clone information? In this section, we seek to give a quantitative answer to this question. We formally state and discuss our model for this problem in terms of *black hole cloning games* in Section 8.1, and then turn to proving a bound on the value of black hole cloning games in Section 8.2.

8.1 Definition

Inspired by the monogamy game of Tomamichel, Fehr, Kaniewski and Wehner [TFKW13], we formalize the notion of a *black hole cloning game* as follows:

Definition 8.1 (Black Hole Cloning Game)**.** *A black hole cloning game is specified by a tuple of the form* $\mathsf{G}_{BH} = (\mathcal{H}_{\mathsf{I}}, \mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{B}'}, \mathcal{H}_{\mathsf{H}}, \mathcal{H}_{\mathsf{R}}, \Theta, \{U_\theta\}_{\theta\in\Theta}, \Phi_{\mathsf{IB}'\to\mathsf{HR}})$ *and consists of the following elements:*

- *A finite dimensional Hilbert space* $\mathcal{H}_{\mathsf{I}}$ *associated with the internal degrees of the freedom of the black hole; in particular, where* $\mathcal{H}_{\mathsf{I}}$ *contains the* $(n-k)$*-qubit initial state of the black hole;*

- *A pair of isomorphic finite dimensional Hilbert spaces $\mathcal{H}_{\mathsf{B}}$ and $\mathcal{H}_{\mathsf{B}'}$ which are associated with k-qubit* EPR *pairs that emerge near the boundary of the black hole;*

- *A finite dimensional Hilbert space $\mathcal{H}_{\mathsf{H}}$ associated with the final state of the black hole that comprises all of the qubits at its event horizon;*

- *A finite dimensional Hilbert space $\mathcal{H}_{\mathsf{R}}$ associated with the emitted Hawking radiation;*

- *A finite set of indices Θ over the set of all possible scrambling unitaries;*

- *A finite ensemble of scrambling unitaries $\{U_\theta^\dagger\}_{\theta\in\Theta}$ indexed by Θ which is associated with the internal time-evolution of the black hole within its event horizon;*

- *A completely positive and trace-preserving channel $\Phi_{\mathsf{IB}'\to\mathsf{HR}}$ associated with the physical process that maps the internal registers IB' of the black hole into a final internal register H and a register R associated with the emitted Hawking radiation.*

We remark that the modeling assumptions behind our *black hole cloning game* (see Figure 6) appear consistent with the postulates of black hole complementarity [STU93, 't 85]; all of the components of our game are modeled according to the existing understanding of physics and Hawking radiation:

- we model the entire process of black hole evolution as a (possibly unitary) quantum channel which takes as input the set of qubits belonging to the interior—together with Alice's infalling qubits—and converts them into a global (possibly pure) state of which a subsystem constitutes outgoing radiation;

- we assume that Hawking radiation is a valid phenomenon—it enables Bob to intercept outgoing radiation in the form of qubits that he can process on his quantum computer; meanwhile, Charlie is simply another observer that is anchored at the event horizon and has access to the remaining qubits; and

- we assume that Bob and Charlie have knowledge of the internal dynamics of the black hole, say as the result of statistical mechanical and thermodynamic considerations—in analogy to how deciphering the contents of a burning book is possible, at least in principle, by observing its smoke and ashes.[16]

Therefore, we believe that black hole cloning games offer a reasonable characterization of quantum cloning in the context of evaporating black holes. In Section 1.5, we discuss further improvements to our modeling assumptions which could potentially make our game even more realistic from a physical perspective.

Definition 8.2 (Quantum Strategy)**.** *A quantum strategy* $\mathsf{S} = (\{\mathbf{H}_x^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\{0,1\}^k}, \{\mathbf{R}_x^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\{0,1\}^k})$ *for a black hole cloning game* $\mathsf{G}_{BH} = (\mathcal{H}_{\mathsf{I}}, \mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{B}'}, \mathcal{H}_{\mathsf{H}}, \mathcal{H}_{\mathsf{R}}, \Theta, \{U_\theta\}_{\theta\in\Theta}, \Phi_{\mathsf{IB}'\to\mathsf{HR}})$ *consists of*

- *An ensemble of oracle-aided positive operator-valued measurements*

$$\left\{\mathbf{H}_x^{U_\theta,U_\theta^\dagger}\right\}_{\theta\in\Theta,x\in\{0,1\}^k}$$

  which are to be performed on Charlie's system $\mathcal{H}_{\mathsf{H}}$.

[16] This analogy was also used in the work of Hayden and Preskill [HP07].

- *An ensemble of oracle-aided positive operator-valued measurements*

$$\left\{\mathbf{R}_x^{U_\theta,U_\theta^\dagger}\right\}_{\theta\in\Theta,x\in\{0,1\}^k}$$

which are to be performed on Bob's system $\mathcal{H}_{\mathsf{R}}$.

Next, we define the value of a black hole cloning game, which can be thought of as the maximal winning probability over all admissible strategies.

Definition 8.3 (Value of a Black Hole Cloning Game)**.** *Consider a black hole cloning game of the form* $\mathsf{G}_{BH} = (\mathcal{H}_{\mathsf{I}}, \mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{B}'}, \mathcal{H}_{\mathsf{H}}, \mathcal{H}_{\mathsf{R}}, \Theta, \{U_\theta\}_{\theta\in\Theta}, \Phi_{\mathsf{IB}'\to\mathsf{HR}})$*. Then, the winning probability of a quantum strategy* $\mathsf{S} = (\{\mathbf{H}_x^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\{0,1\}^k}, \{\mathbf{R}_x^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\{0,1\}^k})$ *for* G_{BH} *is defined by the quantity*

$$\omega_{\mathsf{S}}(\mathsf{G}_{BH}) := \mathop{\mathbb{E}}_{\theta\sim\Theta}\Bigg\{\sum_{x\in\{0,1\}^k}\mathrm{Tr}\Bigg[\left(\mathbf{H}_x^{U_\theta,U_\theta^\dagger}\otimes\mathbf{R}_x^{U_\theta,U_\theta^\dagger}\otimes|x\rangle\langle x|_{\mathsf{B}}\right)\left(\Phi_{\mathsf{IB}'\to\mathsf{HR}}\otimes\mathbb{I}_{\mathsf{B}}\right)$$
$$\left(\left(U_\theta\cdot U_\theta^\dagger\right)_{\mathsf{IB}'\to\mathsf{IB}'}\otimes\mathbb{I}_{\mathsf{B}}\right)\left(|0^{n-k}\rangle\langle 0^{n-k}|_{\mathsf{I}}\otimes|\mathsf{EPR}^k\rangle\langle\mathsf{EPR}^k|_{\mathsf{B}'\mathsf{B}}\right)\Bigg]\Bigg\}.$$

Moreover, we define the value of the monogamy game G_{BH} *as the optimal winning probability*

$$\omega(\mathsf{G}_{BH}) := \sup_{\mathsf{S}=\left(\left\{\mathbf{H}_x^{U_\theta,U_\theta^\dagger}\right\},\left\{\mathbf{R}_x^{U_\theta,U_\theta^\dagger}\right\}\right)}\omega_{\mathsf{S}}(\mathsf{G}_{BH}).$$

Let us remark that the initial quantum state is not adversarially prepared by Bob and Charlie (unlike in typical monogamy games [TFKW13]); rather, it is generated by an external process (say, nature) over which the players have no control. While this is also true of the $\Phi_{\mathsf{IB}'\to\mathsf{HR}}$ cloning channel in practice, our bounds will hold even if Φ is chosen *adversarially* by Bob and Charlie.

8.2 Bounds On the Value of a Black Hole Cloning Game

In this section, we bound the maximal value $\omega(\mathsf{G}_{\mathsf{BH}}) = \sup_{\mathsf{S}}\omega_{\mathsf{S}}(\mathsf{G}_{\mathsf{BH}})$ of a particular black hole cloning game G_{BH} for a unitary 3-design $\{U_\theta\}_{\theta\in\Theta}$ and where we restrict the set of oracle-aided strategies

$$\mathsf{S} = \left(\{\mathbf{H}_x^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\{0,1\}^k}, \{\mathbf{R}_x^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\{0,1\}^k}\right)$$

such that Charlie and Bob only make a single oracle query (to either U_θ or $U_\theta^\dagger$), for any given $\theta\in\Theta$.

Let us first give a brief overview of the idea behind our proof. We refer the reader to our technical overview (Section 1.2) and the associated technical sections for details on each of these steps.

Overview of the proof. To obtain a bound, we consider a sequence of *hybrid games*:

- G_{BH}: This is a black hole cloning game of the form

$$\mathsf{G}_{\mathsf{BH}} = (\mathcal{H}_{\mathsf{I}}, \mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{B}'}, \mathcal{H}_{\mathsf{H}}, \mathcal{H}_{\mathsf{R}}, \Theta, \{U_\theta\}_{\theta\in\Theta}, \Phi_{\mathsf{IB}'\to\mathsf{HR}})$$

where $\nu = \{U_\theta\}_{\theta\in\Theta}$ is an n-qubit unitary 3-design and $\Phi_{\mathsf{IB}'\to\mathsf{HR}}$ is an arbitrary CPTP map.

Game 3 (Black Hole Cloning Game)**.**
A black hole cloning game $\mathsf{G}_{BH} = (\mathcal{H}_{\mathsf{I}}, \mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{B}'}, \mathcal{H}_{\mathsf{H}}, \mathcal{H}_{\mathsf{R}}, \Theta, \{U_\theta\}_{\theta\in\Theta}, \Phi_{\mathsf{IB}'\to\mathsf{HR}})$ *for a quantum strategy* $\mathsf{S} = (\{\mathbf{H}_x^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\{0,1\}^k}, \{\mathbf{R}_x^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\{0,1\}^k})$ *is the following game between a trusted referee called Alice and two colluding and adversarial parties Bob and Charlie.*

1. *(**Setup phase**) A tripartite quantum state* $\rho \in \mathcal{D}(\mathcal{H}_{\mathsf{I}} \otimes \mathcal{H}_{\mathsf{B}'} \otimes \mathcal{H}_{\mathsf{B}})$ *is prepared, where*

$$\rho = \Big(|0^{n-k}\rangle\langle 0^{n-k}|_{\mathsf{I}} \otimes |\mathsf{EPR}^k\rangle\langle \mathsf{EPR}^k|_{\mathsf{B}'\mathsf{B}} \Big).$$

   Here, k *denotes the number of qubits in the registers* B *and* B'*. Next, Alice receives register* B*.*

2. *(**Time-evolution phase**) A random scrambling unitary* U_θ *is selected, where* $\theta \sim \Theta$ *is chosen uniformly at random, and the internal registers of the black hole evolve according to the unitary channel* $\left(U_\theta \cdot U_\theta^\dagger\right)_{\mathsf{IB}'\to\mathsf{IB}'}$ *which is applied to registers* IB' *of the state* ρ*.*

   Afterwards, the channel $\Phi_{\mathsf{IB}'\to\mathsf{HR}}$ *is applied to registers* IB' *and produces registers* HR*.*

3. *(**Guessing phase**) Charlie and Bob receive the registers* H *and* R*, respectively. They also receive oracles for both* U_θ *and* $U_\theta^\dagger$*, but may no longer communicate. They independently perform the measurements* $\{\mathbf{H}_x^{U_\theta,U_\theta^\dagger}\}_{x\in\mathcal{X}}$ *and* $\{\mathbf{R}_x^{U_\theta,U_\theta^\dagger}\}_{x\in\mathcal{X}}$ *and output a* k*-bit string.*

4. *(**Outcome phase**) Alice measures* B *is measured in the computational basis, resulting in an outcome* $x \in \{0,1\}^k$*. Charlie and Bob win if they both guessed* x *correctly.*

Figure 6: A black hole cloning game.

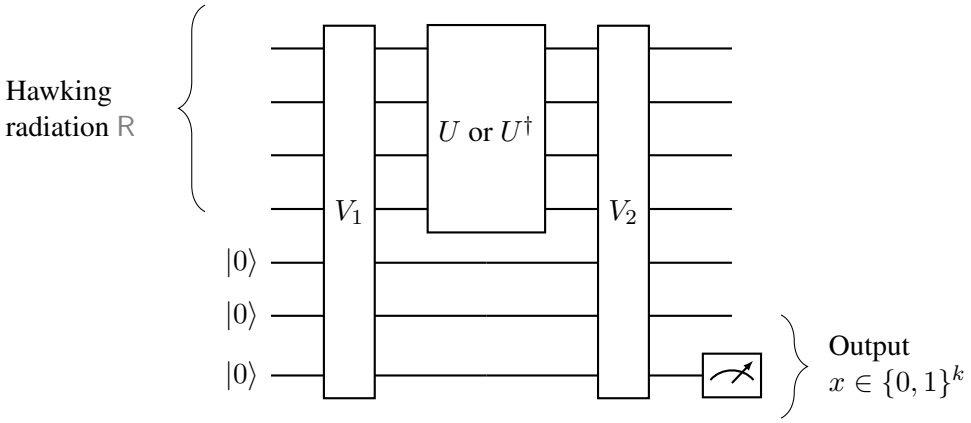

Figure 7: Visualization of Bob's quantum computation in our black hole cloning game. He takes the intercepted Hawking radiation in register R as input, adds any number of ancilla qubits (in the $|0\rangle$ state) of his choosing, and applies an initial unitary V_1 to the entire system. He then makes one oracle query to either U or $U^\dagger$, where U is the black hole's scrambling unitary. Finally, he applies an additional unitary V_2 then measures the last k qubits to produce his guess $x \in \{0,1\}^k$. The diagram for Charlie's strategy would be similar, except the input would consist of the black hole's interior qubits in register H.

- G_{MOE}: This is a (regular) monogamy of entanglement game (as in Section 3.1), where

$$\mathsf{G}_{\text{MOE}} = (\mathcal{H}_{\mathsf{A}}, \Theta, \{0,1\}^n, \{\mathbf{A}_y^\theta\}_{\theta\in\Theta, x\in\{0,1\}^n})$$

  where Alice performs a set of projective measurements $\{\mathbf{A}_y^\theta\}_{\theta\in\Theta,\, y\in\{0,1\}^n}$ acting on the Hilbert space $\mathcal{H}_{\mathsf{A}} = (\mathbb{C}^2)^{\otimes n}$, for some rank-1 projectors $\mathbf{A}_y^\theta = \bar{U}_\theta \left|y\right\rangle\!\left\langle y\right| \bar{U}_\theta^\dagger$.

- $\mathsf{G}_{1\mapsto 2}$: This is a $1 \mapsto 2$ oracular cloning game (as in Section 3.2), where

$$\mathsf{G}_{1\mapsto 2} = (1, \mathcal{H}_{\mathsf{A}}, \Theta, \{0,1\}^n, \{U_\theta\}_{\theta\in\Theta}).$$

- $\mathsf{G}_{\mathfrak{F},1}$: This is a different $1 \mapsto 2$ oracular cloning game (as in Section 3.2), where

$$\mathsf{G}_{\mathfrak{F},1} = (1, \mathcal{H}_{\mathsf{A}}, \{0,1\}^\lambda, \{0,1\}^n, \{\mathsf{U}_{f_\theta}\mathsf{H}^{\otimes n}\}_{\theta\in\{0,1\}^\lambda}).$$

  and $\mathfrak{F} = \{f_\theta : \{0,1\}^n \to \{0,1\}\}_{\theta\in\Theta}$ is a family of 6-wise uniform functions.

First, we show that the game G_{BH} emerges as a special case of G_{MOE} in which we post-select on the event that Alice measures $\{\mathbf{A}_y^\theta\}_{\theta\in\Theta,\, y\in\{0,1\}^n}$ and obtains the outcome $y = x||0^{n-k}$, for some $x \in \{0,1\}^k$. Informally, because this event occurs with probability 2^{-n+k}, we can deduce that that:

$$\sup_{\hat{\mathsf{S}}}\, \omega_{\hat{\mathsf{S}}}(\mathsf{G}_{\text{MOE}}) \;\geq\; 2^{-n+k} \;\cdot\; \sup_{\mathsf{S}} \omega_{\mathsf{S}}(\mathsf{G}_{\text{BH}}),$$

where we maximize over the choice of strategies $\hat{\mathsf{S}}$ selected by Bob and Charlie which consist of a tripartite state ρ, where ρ is the normalized *Choi state* of the quantum channel Φ, and where Bob and Charlie perform oracle aided measurements with single-query access to U_θ and $U_\theta^\dagger$) on an enlarged Hilbert space. Therefore, in order to obtain an asymptotically optimal bound of the form $\omega(\mathsf{G}_{\text{BH}}) = O(2^{-k})$, it suffices to show that the related monogamy game G_{MOE} has a maximal value of $\sup_{\hat{\mathsf{S}}} \omega_{\hat{\mathsf{S}}}(\mathsf{G}_{\text{MOE}}) = O(2^{-n})$. **Note that analyses of monogamy games preceding this work [TFKW13, BL20, CLLZ21, CV22, SS25] would not suffice here, since they only prove bounds of the form $O(2^{-cn})$ for $c < 1$.** (We will discuss this in some more detail in Remark 14.)

Second, we relate the game G_{MOE} to the $1 \mapsto 2$ cloning game $\mathsf{G}_{1\mapsto 2}$. Here, we use the general result in Theorem A.1 which allows us to relate this particular class of monogamy games to cloning games. As a result, we find that $\sup_{\hat{\mathsf{S}}}\, \omega_{\hat{\mathsf{S}}}(\mathsf{G}_{\text{MOE}}) = \sup_{\mathsf{S}'}\, \omega_{\mathsf{S}'}(\mathsf{G}_{1\mapsto 2})$, where S' ranges over the set of analogous oracular cloning strategies, but which involve Φ as a cloning channel.

Third, we use the insight from our worst-case to average-case reduction in Theorem 7.5 in order to argue that the $\mathsf{G}_{1\mapsto 2}$ is at least as hard as the cloning game $\mathsf{G}_{\mathfrak{F},1}$. In particular, we observe that the winning probabilities satisfy $\sup_{\hat{\mathsf{S}}'}\, \omega_{\hat{\mathsf{S}}'}(\mathsf{G}_{1\mapsto 2}) \leq \sup_{\mathsf{S}'}\, \omega_{\mathsf{S}'}(\mathsf{G}_{\mathfrak{F},1})$, where the set of strategies $\hat{\mathsf{S}}'$ remains the same.

Finally, we invoke Theorem 5.15 which gives an explicit bound on the game $\mathsf{G}_{\mathfrak{F},1}$. Specifically, we prove that $\sup_{\mathsf{S}'}\, \omega_{\mathsf{S}'}(\mathsf{G}_{\mathfrak{F},1}) \leq O(2^{-n})$, if $\mathfrak{F}$ is a family of 6-wise uniform functions. **As remarked above, proving a bound this strong requires the new techniques that we introduced earlier in this work.**

Putting everything together, we then obtain the aforementioned asymptotically optimal bound of the form $\omega(\mathsf{G}_{\text{BH}}) = O(2^{-k})$ on the black hole cloning game G_{BH}. Let us now state our main theorem.

Theorem 8.4. *Let $n, k \in \mathbb{N}$ be integers such that $n \geq k$ and let $\nu = \{U_\theta\}_{\theta\in\Theta}$ be a unitary 3-design on n-qubits. Then, for any quantum channel $\Phi_{\mathsf{IB}'\to\mathsf{HR}}$, the maximal single-query value of the black hole cloning game $\mathsf{G}_{BH} = (\mathcal{H}_{\mathsf{I}}, \mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{B}'}, \mathcal{H}_{\mathsf{H}}, \mathcal{H}_{\mathsf{R}}, \Theta, \{U_\theta\}_{\theta\in\Theta}, \Phi_{\mathsf{IB}'\to\mathsf{HR}})$ is at most*

$$\sup_{\mathsf{S}}\, \omega_{\mathsf{S}}(\mathsf{G}_{BH}) \;=\; O(2^{-k})\,,$$

where the supremum ranges over all oracle-aided strategies

$$\mathsf{S} = \left(\{\mathbf{H}_x^{U_\theta, U_\theta^\dagger}\}_{\theta\in\Theta, x\in\{0,1\}^k}, \{\mathbf{R}_x^{U_\theta, U_\theta^\dagger}\}_{\theta\in\Theta, x\in\{0,1\}^k}\right)$$

that only make a single oracle query (to either U_θ or $U_\theta^\dagger$), for any given $\theta \in \Theta$.

Proof. Let S be any single-query strategy. For convenience, we also assume there exists an auxiliary register E (say, the exterior of the black hole) which is initialized to $|0^{n-k}\rangle_{\mathsf{E}}$ and not touched by any of the processes in the black hole cloning game. This is without loss of generality, since it can always be absorbed into Φ by re-defining the quantum channel appropriately. Then, it follows that:

$$\begin{aligned}
\omega_{\mathsf{S}}(\mathsf{G}_{\mathrm{BH}}) =& \mathop{\mathbb{E}}_{U\sim\nu}\Bigg\{\sum_{x\in\{0,1\}^k} \mathrm{Tr}\Bigg[\left(\mathbf{H}_x^{U,U^\dagger}\otimes\mathbf{R}_x^{U,U^\dagger}\otimes|x0^{n-k}\rangle\langle x0^{n-k}|_{\mathsf{BE}}\right)\left(\Phi_{\mathsf{IB}'\to\mathsf{HR}}\otimes\mathbb{I}_{\mathsf{BE}}\right)\\
&\left(\left(U\cdot U^\dagger\right)_{\mathsf{IB}'\to\mathsf{IB}'}\otimes\mathbb{I}_{\mathsf{BE}}\right)\left(|0^{n-k}\rangle\langle 0^{n-k}|_{\mathsf{I}}\otimes|\mathsf{EPR}^k\rangle\langle\mathsf{EPR}^k|_{\mathsf{B}'\mathsf{B}}\otimes|0^{n-k}\rangle\langle 0^{n-k}|_{\mathsf{E}}\right)\Bigg]\Bigg\}\\
=& 2^{n-k}\mathop{\mathbb{E}}_{U\sim\nu}\Bigg\{\sum_{x\in\{0,1\}^k} \mathrm{Tr}\Bigg[\left(\mathbf{H}_x^{U,U^\dagger}\otimes\mathbf{R}_x^{U,U^\dagger}\otimes|x0^{n-k}\rangle\langle x0^{n-k}|_{\mathsf{BE}}\right)\left(\Phi_{\mathsf{IB}'\to\mathsf{HR}}\otimes\mathbb{I}_{\mathsf{BE}}\right)\\
&\left(\left(U\cdot U^\dagger\right)_{\mathsf{IB}'\to\mathsf{IB}'}\otimes\mathbb{I}_{\mathsf{BE}}\right)\left(|\mathsf{EPR}^n\rangle\langle\mathsf{EPR}^n|_{\mathsf{IB}'\mathsf{BE}}\right)\Bigg]\Bigg\}.
\end{aligned}$$

The above step holds because in the second line the projector $|0^{n-k}\rangle\langle 0^{n-k}|_{\mathsf{E}}$ will act on one half of the EPR pair $|\mathsf{EPR}^{n-k}\rangle\langle\mathsf{EPR}^{n-k}|_{\mathsf{IE}}$, thus collapsing it to $|0^{n-k}\rangle\langle 0^{n-k}|_{\mathsf{I}}\otimes|0^{n-k}\rangle\langle 0^{n-k}|_{\mathsf{E}}$ and pulling out a factor of 2^{k-n}.

We continue by using the ricochet property of EPR pairs (formally, Corollary 2.2) to pull $U, U^\dagger$ "out" of the cloning channel to obtain something that will look more like a monogamy game. First, consider the channel $\Psi_{\mathsf{IB}'\to\mathsf{HR}}$ defined as $\Phi\circ(U\cdot U^\dagger)$ (here, $\circ$ denotes composition). Applying Corollary 2.2 to the channel Ψ yields the following:

$$\begin{aligned}
&2^{n-k}\mathop{\mathbb{E}}_{U\sim\nu}\Bigg\{\sum_{x\in\{0,1\}^k} \mathrm{Tr}\Bigg[\left(\mathbf{H}_x^{U,U^\dagger}\otimes\mathbf{R}_x^{U,U^\dagger}\otimes|x0^{n-k}\rangle\langle x0^{n-k}|_{\mathsf{BE}}\right)\left(\Phi_{\mathsf{IB}'\to\mathsf{HR}}\otimes\mathbb{I}_{\mathsf{BE}}\right)\\
&\left(\left(U\cdot U^\dagger\right)_{\mathsf{IB}'\to\mathsf{IB}'}\otimes\mathbb{I}_{\mathsf{BE}}\right)\left(|\mathsf{EPR}^n\rangle\langle\mathsf{EPR}^n|_{\mathsf{IB}'\mathsf{BE}}\right)\Bigg]\Bigg\}\\
=&2^{-k}\mathop{\mathbb{E}}_{U\sim\nu}\Bigg\{\sum_{x\in\{0,1\}^k} \mathrm{Tr}\Bigg[\left(\mathbf{H}_x^{U,U^\dagger}\otimes\mathbf{R}_x^{U,U^\dagger}\otimes|x0^{n-k}\rangle\langle x0^{n-k}|_{\mathsf{BE}}\right)J(\Psi)\Bigg]\Bigg\}\\
=&2^{-k}\mathop{\mathbb{E}}_{U\sim\nu}\Bigg\{\sum_{x\in\{0,1\}^k} \mathrm{Tr}\Bigg[\left(\mathbf{H}_x^{U,U^\dagger}\otimes\mathbf{R}_x^{U,U^\dagger}\right)\Psi(|x0^{n-k}\rangle\langle x0^{n-k}|)\Bigg]\Bigg\}\\
=&2^{-k}\mathop{\mathbb{E}}_{U\sim\nu}\Bigg\{\sum_{x\in\{0,1\}^k} \mathrm{Tr}\Bigg[\left(\mathbf{H}_x^{U,U^\dagger}\otimes\mathbf{R}_x^{U,U^\dagger}\right)\Phi(U|x0^{n-k}\rangle\langle x0^{n-k}|U^\dagger)\Bigg]\Bigg\}.
\end{aligned}$$

Next, we apply Corollary 2.2 once more, this time to the channel Φ:

$$
\begin{aligned}
&2^{-k} \mathop{\mathbb{E}}_{U\sim\nu} \left\{ \sum_{x\in\{0,1\}^k} \mathrm{Tr}\left[\left(\mathbf{H}_x^{U,U^\dagger} \otimes \mathbf{R}_x^{U,U^\dagger} \right) \Phi(U\left|x0^{n-k}\right\rangle\!\left\langle x0^{n-k}\right| U^\dagger) \right] \right\} \\
=&2^{-k} \mathop{\mathbb{E}}_{U\sim\nu} \left\{ \sum_{x\in\{0,1\}^k} \mathrm{Tr}\left[\left(\mathbf{H}_x^{U,U^\dagger} \otimes \mathbf{R}_x^{U,U^\dagger} \otimes \bar{U}\left|x0^{n-k}\right\rangle\!\left\langle x0^{n-k}\right|_{\mathsf{BE}} \bar{U}^\dagger \right) J(\Phi) \right] \right\} \\
=&2^{n-k} \mathop{\mathbb{E}}_{U\sim\nu} \left\{ \sum_{x\in\{0,1\}^k} \mathrm{Tr}\left[\left(\mathbf{H}_x^{U,U^\dagger} \otimes \mathbf{R}_x^{U,U^\dagger} \otimes \bar{U}\left|x0^{n-k}\right\rangle\!\left\langle x0^{n-k}\right|_{\mathsf{BE}} \bar{U}^\dagger \right) \right.\right. \\
&\qquad \left.\left. \left(\Phi_{\mathsf{IB}'\to\mathsf{HR}} \otimes \mathbb{I}_{\mathsf{BE}} \right) \left(\left|\mathsf{EPR}^n\right\rangle\!\left\langle \mathsf{EPR}^n\right|_{\mathsf{IB}'\mathsf{BE}} \right) \right] \right\}.
\end{aligned}
$$

For the remainder of the proof, we will bound the final quantity in the expression above; specifically, by relating it to the value of a related monogamy of entanglement game. To this end, we now observe that

$$
\begin{aligned}
&2^{n-k} \mathop{\mathbb{E}}_{U\sim\nu} \left\{ \sum_{x\in\{0,1\}^k} \mathrm{Tr}\left[\left(\mathbf{H}_x^{U,U^\dagger} \otimes \mathbf{R}_x^{U,U^\dagger} \otimes \bar{U}\left|x0^{n-k}\right\rangle\!\left\langle x0^{n-k}\right|_{\mathsf{BE}} \bar{U}^\dagger \right) \right.\right. \\
&\qquad \left.\left. \left(\Phi_{\mathsf{IB}'\to\mathsf{HR}} \otimes \mathbb{I}_{\mathsf{BE}} \right) \left(\left|\mathsf{EPR}^n\right\rangle\!\left\langle \mathsf{EPR}^n\right|_{\mathsf{IB}'\mathsf{BE}} \right) \right] \right\} \\
=\ &2^{n-k} \mathop{\mathbb{E}}_{U\sim\nu} \left\{ \sum_{x\in\{0,1\}^k} \mathrm{Tr}\left[\left(\tilde{\mathbf{H}}_{x||0^{n-k}}^{U,U^\dagger} \otimes \tilde{\mathbf{R}}_{x||0^{n-k}}^{U,U^\dagger} \otimes \bar{U}\left|x0^{n-k}\right\rangle\!\left\langle x0^{n-k}\right|_{\mathsf{BE}} \bar{U}^\dagger \right) \right.\right. \\
&\qquad \left.\left. \left(\Phi_{\mathsf{IB}'\to\mathsf{HR}} \otimes \mathbb{I}_{\mathsf{BE}} \right) \left(\left|\mathsf{EPR}^n\right\rangle\!\left\langle \mathsf{EPR}^n\right|_{\mathsf{IB}'\mathsf{BE}} \right) \right] \right\} \\
\leq\ &2^{n-k} \sup_{\tilde{\mathsf{S}}=\left(\left\{\hat{\mathbf{H}}_y^{U,U^\dagger}\right\},\left\{\hat{\mathbf{R}}_y^{U,U^\dagger}\right\}\right)} \mathop{\mathbb{E}}_{U\sim\nu} \left\{ \sum_{y\in\{0,1\}^n} \mathrm{Tr}\left[\left(\hat{\mathbf{H}}_y^{U,U^\dagger} \otimes \hat{\mathbf{R}}_y^{U,U^\dagger} \otimes \bar{U}\left|y\right\rangle\!\left\langle y\right|_{\mathsf{BE}} \bar{U}^\dagger \right) \right.\right. \\
&\qquad \left.\left. \left(\Phi_{\mathsf{IB}'\to\mathsf{HR}} \otimes \mathbb{I}_{\mathsf{BE}} \right) \left(\left|\mathsf{EPR}^n\right\rangle\!\left\langle \mathsf{EPR}^n\right|_{\mathsf{IB}'\mathsf{BE}} \right) \right] \right\}. \qquad (15)
\end{aligned}
$$

We have now transitioned successfully to G_{MOE}. Because the bound in Equation (15) applies to any single-query strategy S, we can therefore complete the proof by bounding the black hole cloning game as follows:

$$
\begin{aligned}
\omega(\mathsf{G}_{\text{BH}}) &= \sup_{\mathsf{S}=\left(\{\mathbf{H}_x^{U,U^\dagger}\},\{\mathbf{R}_x^{U,U^\dagger}\}\right)} \omega_{\mathsf{S}}(\mathsf{G}_{\text{BH}}) \\
&\leq 2^{n-k} \sup_{\hat{\mathsf{S}}=\left(\mathcal{H}_{\mathsf{H}},\mathcal{H}_{\mathsf{R}},\rho_{\mathsf{AHR}},\{\hat{\mathbf{H}}_y^{U,U^\dagger}\},\{\hat{\mathbf{R}}_y^{U,U^\dagger}\}\right)} \omega_{\hat{\mathsf{S}}}(\mathsf{G}_{\text{MOE}}) && \text{(by Equation (15))} \\
&= 2^{n-k} \sup_{\mathsf{S}'=\left(\mathcal{H}_{\mathsf{H}}\otimes\mathcal{H}_{\mathsf{R}},\Phi_{\mathsf{IB}'\to\mathsf{HR}},\{\hat{\mathbf{H}}_y^{U,U^\dagger}\},\{\hat{\mathbf{R}}_y^{U,U^\dagger}\}\right)} \omega_{\mathsf{S}'}(\mathsf{G}_{1\mapsto 2}) && \text{(Lemma A.1)} \\
&\leq 2^{n-k} \sup_{\mathsf{S}'=\left(\mathcal{H}_{\mathsf{H}}\otimes\mathcal{H}_{\mathsf{R}},\Phi_{\mathsf{IB}'\to\mathsf{HR}},\{\hat{\mathbf{H}}_y^{U,U^\dagger}\},\{\hat{\mathbf{R}}_y^{U,U^\dagger}\}\right)} \omega_{\mathsf{S}'}(\mathsf{G}_{\mathfrak{F},1}) && \text{(Theorem 7.5)}
\end{aligned}
$$

$$\leq 2^{n-k} \cdot O(2^{-n}) \;=\; O(2^{-k}). \qquad \text{(Theorem 5.15)}$$

□

We conclude this section with the following remark.

Remark 14 (Comparison with the Cloning Game Bound by [BL20])**.** *Earlier, we made the claim that we require a construction of a cloning game with value $\leq O(2^{-n})$, and that our work is the first to achieve this. At the surface, it might appear that the construction of Broadbent and Lord [BL20] also achieves this (even if their unclonable encryption construction does not strictly conform to the syntax in Definition 3.5): they provide a construction with $\mathcal{X} = \{0,1\}^n$ and $\Theta = \{0,1\}^\lambda$ with value $\leq \left(\cos^2(\pi/8)\right)^\lambda + O(2^{-n})$. Thus, if $\lambda \geq cn$ for some $c > 1$, this value will be $O(2^{-n})$.*

However, the result by [BL20] still does not suffice for our black hole application. The reason is that their ciphertext states comprise $\lambda > n$ qubits and are thus not succinct. Looking through our proof of Theorem 8.4, what we really need is a cloning game such that messages $x \in \{0,1\}^n$ are "encrypted" using m qubits and where we can prove a bound of $O(2^{-m})$, which the [BL20] construction does not satisfy as $m = \lambda$. The reason for this is that an adaptation of our worst-case to average-case reduction in Section 7 would have proceed by applying a Haar random (or pseudorandom) unitary to the entire *ciphertext state. This forces the Haar random unitary to act on m qubits, so our goal would be to prove a bound of $O(2^{-m})$.*

9 Search-Secure Unclonable Encryption

In this section, we formally define (succinct, deterministic, search-secure) unclonable encryption, loosely following the terminology introduced by Broadbent and Lord [BL20]. We will use $\theta \in \{0,1\}^\lambda$ (rather than k, which we are already using in Section 8 to denote the number of EPR pairs in a black hole cloning game) to denote the secret key.

9.1 Definitions

Definition 9.1 (Unclonable Encryption)**.** *Let $\lambda \in \mathbb{N}$ be the security parameter and let $n := n(\lambda)$ be some polynomial in λ. A* ***succinct and deterministic*** *unclonable encryption scheme* (UE) *is a tuple* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *consisting of the following QPT algorithms:*

- $\mathsf{KeyGen}(1^\lambda, 1^n)$ *: takes as input $1^\lambda, 1^n$ and outputs $\theta \in \{0,1\}^\lambda$.*
- $\mathsf{Enc}(\theta \in \{0,1\}^\lambda, x \in \{0,1\}^n)$ *: on input (θ, x), it outputs a pure ciphertext state $|\psi_x^\theta\rangle$.* ***We require*** $\mathsf{Enc}(\theta, x)$ ***to deterministically output*** $U_\theta |x\rangle$***, for some unitary*** $U_{\theta,n} \in \mathcal{U}(2^n)$***.*** *Thus the ciphertext state must also comprise n qubits.*
- $\mathsf{Dec}(1^n, \theta \in \{0,1\}^\lambda, \rho)$*: on input θ and a quantum state ρ, it outputs $x' \in \{0,1\}^n$.*

We require the following correctness property: for any λ, n, it holds that

$$\Pr\left[\mathsf{Dec}\big(1^n, \theta, |\psi_x^\theta\rangle\langle\psi_x^\theta|\big) = x \;:\; \begin{smallmatrix}\theta \leftarrow \mathsf{KeyGen}(1^\lambda, 1^n) \\ |\psi_x^\theta\rangle \leftarrow \mathsf{Enc}(\theta, x)\end{smallmatrix}\right] = 1.$$

Succinctness *is implicit in our requirement that the key length only depends on λ rather than n.*

Definition 9.2 ($t \mapsto t+1$ UE security)**.** *Let* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be a* UE *scheme, and* $t \in \mathbb{N}$ *a positive integer. Consider the following experiment between a challenger and an adversary* $(\Phi, \mathcal{P}_1, \ldots, \mathcal{P}_{t+1})$ *consisting of a cloner* Φ *and* $t+1$ *players* $\mathcal{P}_1, \ldots \mathcal{P}_{t+1}$ *who are not allowed to communicate:*

1. *The challenger runs* $\theta \leftarrow \mathsf{KeyGen}(1^\lambda, 1^n)$*. Next, the challenger samples* $x \leftarrow \{0,1\}^n$ *and runs* $\mathsf{Enc}(\theta, x)$ *to obtain the ciphertext* $|\psi_x^\theta\rangle$*, and sends* t *copies* $|\psi_x^\theta\rangle^{\otimes t}$ *of the state to the cloner* Φ*.*
2. *The cloner* Φ *applies any quantum channel to* $|\psi_x^\theta\rangle^{\otimes t}$ *in registers* $\mathsf{A}_1 \ldots \mathsf{A}_t$ *and then splits the resulting state into* $t+1$ *registers* $\mathsf{B}_1, \ldots, \mathsf{B}_{t+1}$*. Finally,* Φ *sends* B_i *to player* $\mathcal{P}_i$*.*
3. *The players* $\mathcal{P}_1, \ldots, \mathcal{P}_{t+1}$ *receive* θ *and output their guesses for* x*, and win if they all guess correctly.*

We say that $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *satisfies statistical (respectively, computational)* $t \mapsto t+1$ *and* $\epsilon(t, \lambda, n)$-UE *security if, for any computationally unbounded (respectively, computationally bounded) adversary* $(\Phi, \mathcal{P}_1, \ldots, \mathcal{P}_{t+1})$*, where each* $\mathcal{P}_i$ *is an ensemble of positive-operator valued measurements* $\{\mathbf{P}_{i,x}^\theta\}_{x,\theta}$*,*

$$\mathop{\mathbb{E}}_{(x,\theta)\sim\mathsf{KeyGen}(1^n)} \mathrm{Tr}\left[\left(\mathbf{P}_{1,x}^\theta \otimes \ldots \otimes \mathbf{P}_{t+1,x}^\theta\right) \Phi_{\mathsf{A}_1\ldots\mathsf{A}_t\to\mathsf{B}_1\ldots\mathsf{B}_{t+1}}\left(|\psi_x^\theta\rangle\langle\psi_x^\theta|_{\mathsf{A}_1\ldots\mathsf{A}_t}^{\otimes t}\right)\right] \leq O\left(\epsilon(t,\lambda,n)\right).$$

The $1 \mapsto 2$ UE security experiment is visualized in Figure 8. In the following definition, we also define an *oracular* version of this security experiment.

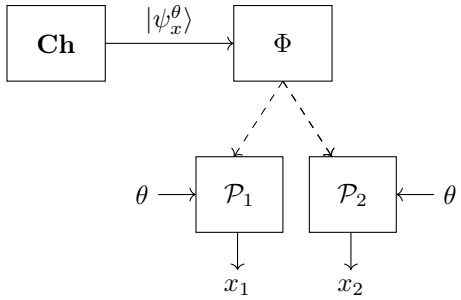

Figure 8: The $1 \mapsto 2$ UE experiment. A cloner Φ splits a state $|\psi_x^\theta\rangle$ prepared by the challenger **Ch** into two parts, one is sent to $\mathcal{P}_1$ and one is sent to $\mathcal{P}_2$. Given θ, $\mathcal{P}_1$ and $\mathcal{P}_2$ then output their guesses x_1 and x_2 for x.

Definition 9.3 ($t \mapsto t+1$ oracular UE security)**.** *We say that* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *satisfies statistical (respectively, computational)* $t \mapsto t+1$ ϵ-UE *oracular security under the same conditions as Definition 9.2, with the following modification: in the final phase, the players* $\mathcal{P}_1, \ldots \mathcal{P}_{t+1}$ *do not receive* θ *directly. Instead, they receive query access to the unitary* $U_{\theta,n}$ *computing* $\mathsf{Enc}(\theta, \cdot)$ *as well as its inverse* $U_{\theta,n}^\dagger$*.*

We say that $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *satisfies the weaker notion of* (ϵ, q)-UE *oracular security if each of the players may only make a total of* $\leq q$ *queries to* $U_{\theta,n}$ *and* $U_{\theta,n}^\dagger$*.*

Remark 15. *We emphasize that our work is the first to consider* $t \mapsto t+1$ *cloning games for* $t > 1$*: not only is prior work limited to* $1 \mapsto 2$ *cloning games, all existing unclonable cryptography (based on BB84 states or coset states) becomes completely insecure if* t *is allowed to grow polynomially (see Section 1.2.1 and [AMP24] for more details).*

While we are only able to prove security for $t = o(n/\log n)$ *(see Theorem 9.5), we reiterate that our construction could very well be secure for* t *that is an arbitrary polynomial in* n *(unlike previous constructions based on BB84 states [BL20] and coset states [CLLZ21]).*

Remark 16 (Comparison with [BL20])**.** *At first glance, in the $t = 1$ case this notion may already appear to have been achieved by the construction by Broadbent and Lord [BL20], which achieves a security bound of $\epsilon(\lambda, n) = \frac{9}{2^n} + \left(\cos^2 \frac{\pi}{8}\right)^\lambda$. At a high level, they compose a λ-bit BB84 cloning game as in [TFKW13] with a PRF-based one-time pad (see Remark 17 below for details). However, their construction has two aspects which we would like to improve on:*

- *Their construction assumes the existence of post-quantum pseudorandom functions. We would like to instantiate a* UE *scheme assuming the milder notions of pseudorandom quantum states or unitaries.*
- *Their encryption is randomized. The natural deterministic analogue of this would be the BB84-based encryption scheme without the PRF, which has security $\left(\cos^2 \frac{\pi}{8}\right)^n$ but is no longer succinct as this would use keys of length n.*

We note that a common shortcoming of both the work by [BL20] and our work is the reliance on oracles for proving security.

Remark 17 (Justifying Deterministic Encryption)**.** *Our reason for focusing on* UE *schemes with* deterministic unitary *encryption is in order to be able to naturally instantiate the oracular security setting. Regardless, any such scheme comes with the obvious shortcoming that it is deterministic, and hence does not satisfy the ideal notions of indistinguishable or unclonable-indistinguishable security (as defined in [BL20]). Nevertheless, we argue that a deterministic scheme satisfying unclonable search security can plausibly be bootstrapped to a scheme satisfying unclonable-indistinguishable security.*

One such bootstrapping transformation was proposed by Broadbent and Lord [BL20]: suppose we have an unclonable search-secure scheme $\mathsf{SearchEnc}$*. Then to encrypt $x \in \{0,1\}^n$ under secret keys $(k, \theta) \in \{0,1\}^\lambda \times \{0,1\}^\lambda$, sample a random PRF seed $r \in \{0,1\}^\lambda$ and output the classical string $x \oplus \mathsf{PRF}(k, r)$ together with the quantum state $|\mathsf{SearchEnc}(\theta, r)\rangle$. Broadbent and Lord [BL20] also provided some mild evidence that this may be secure if the PRF is instantiated with a random oracle.*

We emphasize that proving *the unclonable-indistinguishable security of this transformation (or a similar one) is a notoriously difficult open problem [KT23, AKL23, AKY24]. Our point is just that studying unclonable encryption in the weaker search-secure setting is still an interesting and relevant cryptographic problem, and hence that restricting attention to the case of deterministic unclonable encryption is also interesting.*

Finally, we recall from Remark 6 that the oracular UE setting is still quite expressive, even if we only allow each player *one* query. In particular, it would be sufficient for recovering x from $|\psi_x^\theta\rangle$, and thus there is still a trivial strategy that succeeds with probability 2^{-n}: the cloner forwards their copies to the first t players, and nothing to player $t + 1$. The first t players can decrypt and output x, and player $t + 1$ will simply guess randomly.

9.2 Constructions

Construction 3. *Let $\mathfrak{U} = \{\mathfrak{U}_n\}_{n\in\mathbb{N}}$ be some ensemble of unitaries (we will specify what $\mathfrak{U}$ should be later). Recall that $\mathfrak{U}_n = \{U_{\theta,n}\}_{\theta\in\{0,1\}^\lambda}$. Our construction proceeds as follows:*

- $\mathsf{KeyGen}(1^\lambda, 1^n)$*: sample and output uniformly random $\theta \in \{0,1\}^\lambda$.*
- $\mathsf{Enc}(\theta, x)$*: output $U_{\theta,n} |x\rangle$.*

- $\mathsf{Dec}(1^n, \theta, \rho)$. *First apply the unitary channel* $U_{\theta,n}^\dagger \cdot U_{\theta,n}$ *to obtain the state* $U_{\theta,n}^\dagger \rho U_{\theta,n}$. *Now measure in the standard basis and output the result.*

Correctness is clear, so we now prove security in two different settings. First, we show $1 \mapsto 2$ security assuming the existence of pseudorandom unitaries, thus placing unclonable encryption in MicroCrypt:

Theorem 9.4. *If* $\mathfrak{U}$ *is a pseudorandom unitary (as defined in Definition 2.7), then the* UE *scheme specified in Construction 3 satisfies computational* $1 \mapsto 2$ ϵ-UE *oracular security, where* $\epsilon = \mathsf{negl}(\lambda) + \left(\cos^2 \frac{\pi}{8}\right)^n$.

Proof. We consider a series of hybrid games:

- Hyb_0: This is the $1 \mapsto 2$ oracular UE security game, as defined in Definition 9.3.
- Hyb_1: In step 1 of the UE security game, the challenger also only has oracle access to $U_{\theta,n}, U_{\theta,n}^\dagger$. To generate the ciphertext state $|\psi_x^\theta\rangle$, they query the oracle for $U_{\theta,n}$ on input $|x\rangle$.
- Hyb_2: Now, the unitary U is sampled as follows: sample a string $b \leftarrow \{0,1\}^n$ uniformly at random, and output H^b (which applies a Hadamard at every position where the corresponding entry of b is 1).

For $i = 0, 1, 2$, let $\omega(\mathsf{Hyb}_i)$ denote the probability of the players winning the security game in Hyb_i. Then we observe the following:

- $\omega(\mathsf{Hyb}_0) = \omega(\mathsf{Hyb}_1)$, as these two are functionally equivalent.
- $|\omega(\mathsf{Hyb}_1) - \omega(\mathsf{Hyb}_2)| \leq \mathsf{negl}(\lambda)$ by the worst-case to average-case reduction in Section 7.
- $\omega(\mathsf{Hyb}_2) \leq \cos^2\left(\frac{\pi}{8}\right)^n$: this is exactly the BB84 security game. This security bound essentially follows from analysis by [TFKW13], and was formally shown in [BL20, Corollary 2].

The conclusion follows. □

Remark 18. *We note that we could just as easily have used the subspace coset monogamy game [CLLZ21, CV22] and its analysis by [SS25] in the place of the BB84 cloning game in* Hyb_2 *to obtain a slightly stronger upper bound of* $\mathsf{negl}(\lambda) + O(2^{-n/4})$.

In some more detail: the unitary will be indexed by a linear subspace A *of* $\mathbb{F}_2^n$ *with* $\dim A = n/2$. *The unitary will be that which takes an* n*-bit string* x *as input, interprets this as a pair of cosets* $s + A, s' + A^\perp$, *and outputs*

$$|A_{s,s'}\rangle = \frac{1}{2^{n/4}} \sum_{a \in A} (-1)^{\langle a, s' \rangle} |a + s\rangle .$$

Secondly, we show assuming the existence of post-quantum one-way functions that Construction 3 can be instantiated to satisfy multi-copy security against query-bounded adversaries:

Theorem 9.5. *For any* λ, n, *let* $n' = n - \omega(\log \lambda)$ *and consider* t *such that*

$$t \leq O\left(\frac{n'}{\log n'}\right) \Leftrightarrow \exp(O(t \log t)) \leq 2^{n'} = 2^n \cdot \mathsf{negl}(\lambda).$$

Let $\left\{f_{\theta,n} : \theta \in \{0,1\}^\lambda\right\}$ *be a post-quantum pseudorandom function family from* $\{0,1\}^n \to \{0,1\}$. *Then we define* $\mathfrak{U}$ *by*

$$U_{\theta,n} = \mathsf{U}_{f_{\theta,n}} \mathsf{H}^{\otimes n}.$$

Then the UE *scheme specified in Construction 3 satisfies computational* $t \mapsto t + 1$ $(\epsilon, 1)$-UE *oracular security, where*

$$\epsilon = \exp(O(t \log t)) \cdot 2^{-n} + \mathsf{negl}(\lambda) = \mathsf{negl}(\lambda).$$

Proof. We first pass from a pseudorandom function $f_{\theta,n}$ to a truly random function f at the expense of an additive $\mathsf{negl}(\lambda)$ security loss. A random function is $(4t+2)$-wise uniform, so we can then finish using Lemma 3.11 and Theorem 5.15.

□

References

[Aar09] Scott Aaronson. Quantum copy-protection and quantum money. In *2009 24th Annual IEEE Conference on Computational Complexity*, page 229–242. IEEE, July 2009. 7

[Aar16] Scott Aaronson. The complexity of quantum states and transformations: From quantum money to black holes, 2016. 16

[ACG+24] Rene Allerstorfer, Matthias Christandl, Dmitry Grinko, Ion Nechita, Maris Ozols, Denis Rochette, and Philip Verduyn Lunel. Monogamy of highly symmetric states, 2024. 10

[AGQY22] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. Pseudorandom (function-like) quantum state generators: New definitions and applications. In Eike Kiltz and Vinod Vaikuntanathan, editors, *Theory of Cryptography - 20th International Conference, TCC 2022, Chicago, IL, USA, November 7-10, 2022, Proceedings, Part I*, volume 13747 of *Lecture Notes in Computer Science*, pages 237–265. Springer, 2022. 3, 4, 5, 13, 40

[AIK22] Scott Aaronson, DeVon Ingram, and William Kretschmer. The acrobatics of BQP. In Shachar Lovett, editor, *37th Computational Complexity Conference, CCC 2022, July 20-23, 2022, Philadelphia, PA, USA*, volume 234 of *LIPIcs*, pages 20:1–20:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. 20

[AK21] Prabhanjan Ananth and Fatih Kaleoglu. Unclonable encryption, revisited. In Kobbi Nissim and Brent Waters, editors, *Theory of Cryptography - 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, Proceedings, Part I*, volume 13042 of *Lecture Notes in Computer Science*, pages 299–329. Springer, 2021. 6

[AKL+22] Prabhanjan Ananth, Fatih Kaleoglu, Xingjian Li, Qipeng Liu, and Mark Zhandry. On the feasibility of unclonable encryption, and more. In *Advances in Cryptology – CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part II*, page 212–241, Berlin, Heidelberg, 2022. Springer-Verlag. 1, 7, 19

[AKL23] Prabhanjan Ananth, Fatih Kaleoglu, and Qipeng Liu. Cloning games: A general framework for unclonable primitives. In *Advances in Cryptology – CRYPTO 2023: 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part V*, page 66–98, Berlin, Heidelberg, 2023. Springer-Verlag. 1, 19, 20, 24, 39, 40, 75

[AKY24] Prabhanjan Ananth, Fatih Kaleoglu, and Henry Yuen. Simultaneous Haar indistinguishability with applications to unclonable cryptography. *CoRR*, abs/2405.10274, 2024. 1, 19, 20, 22, 24, 75

[AMP24] Prabhanjan Ananth, Saachi Mutreja, and Alexander Poremba. Revocable encryption, programs, and more: The case of multi-copy security, 2024. 3, 20, 74

[AMPS13] Ahmed Almheiri, Donald Marolf, Joseph Polchinski, and James Sully. Black holes: complementarity or firewalls? *Journal of High Energy Physics*, 2013(2), February 2013. 15, 16

[AMR19] Gorjan Alagic, Christian Majenz, and Alexander Russell. Efficient simulation of random states and random unitaries. Cryptology ePrint Archive, Paper 2019/1204, 2019. 64

[APV23] Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan. Revocable cryptography from learning with errors. Cryptology ePrint Archive, Paper 2023/325, 2023. 1

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*, pages 208–236, Cham, 2022. Springer Nature Switzerland. 3

[Ara02] P. K. Aravind. Bell's theorem without inequalities and only two distant observers, 2002. 1

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984. 1

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997. 12

[BBC+93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical Review Letters*, 70(13):1895–1899, 1993. 1

[BC25] Archishna Bhattacharyya and Eric Culf. Uncloneable encryption from decoupling, 2025. 10, 12

[BCG13] K Banaszek, Marcus Cramer, and D Gross. Focus on quantum tomography. *New Journal of Physics*, 15:5020–, 12 2013. 3, 6

[BCKM21] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*, volume 12825 of *Lecture Notes in Computer Science*, pages 467–496. Springer, 2021. 20, 22

[BCQ23] Zvika Brakerski, Ran Canetti, and Luowen Qian. On the Computational Hardness Needed for Quantum Cryptography. In Yael Tauman Kalai, editor, *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*, volume 251 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:21, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. 3

[BDPA11] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. The keccak sha-3 submission. Submission to NIST (Round 3), 2011. 19

[BEM+23] John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. Unitary complexity and the uhlmann transformation problem, 2023. 16

[BH96] V. Bužek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Physical Review A*, 54(3):1844–1852, September 1996. 1, 2, 16

[BHHP24] John Bostanci, Jonas Haferkamp, Dominik Hangleiter, and Alexander Poremba. Efficient quantum pseudorandomness from hamiltonian phase states, 2024. 20

[BKL23] Anne Broadbent, Martti Karvonen, and Sébastien Lord. Uncloneable quantum advice, 2023. 20

[BL20] Anne Broadbent and Sébastien Lord. Uncloneable Quantum Encryption via Oracles. In Steven T. Flammia, editor, *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, volume 158 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 4:1–4:22, Dagstuhl, Germany, 2020. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. 1, 2, 4, 5, 7, 8, 11, 18, 19, 20, 21, 22, 23, 24, 37, 56, 62, 70, 73, 74, 75, 76, 83

[Bra23] Zvika Brakerski. Black-hole radiation decoding is quantum cryptography. In *Advances in Cryptology – CRYPTO 2023: 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part V*, page 37–65, Berlin, Heidelberg, 2023. Springer-Verlag. 16

[BS19] Zvika Brakerski and Omri Shmueli. (pseudo) random quantum states with binary phase, 2019. 4, 5, 11, 20, 21, 45

[CBTW17] Patrick J. Coles, Mario Berta, Marco Tomamichel, and Stephanie Wehner. Entropic uncertainty relations and their applications. *Rev. Mod. Phys.*, 89:015002, Feb 2017. 1

[CDX+24] Chi-Fang Chen, Jordan Docter, Michelle Xu, Adam Bouland, Fernando G.S.L. Brandão, and Patrick Hayden. Efficient unitary designs from random sums and permutations. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, page 476–484. IEEE, October 2024. 10

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, October 1969. 16

[CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 556–584, Cham, 2021. Springer International Publishing. 1, 2, 4, 5, 6, 7, 11, 15, 18, 21, 56, 62, 70, 74, 76

[CMP22] Andrea Coladangelo, Christian Majenz, and Alexander Poremba. Quantum copy-protection of compute-and-compare programs in the quantum random oracle model, 2022. 1, 7, 19

[Col23] Andrea Coladangelo. Quantum trapdoor functions from classical one-way functions. Cryptology ePrint Archive, Paper 2023/282, 2023. 4, 11

[CP24] Joseph Carolan and Alexander Poremba. Quantum one-wayness of the single-round sponge with invertible permutations. In *Advances in Cryptology – CRYPTO 2024: 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2024, Proceedings, Part VI*, page 218–252, Berlin, Heidelberg, 2024. Springer-Verlag. 19

[CPZ24] Joseph Carolan, Alexander Poremba, and Mark Zhandry. (quantum) indifferentiability and pre-computation, 2024. 19

[CV22] Eric Culf and Thomas Vidick. A monogamy-of-entanglement game for subspace coset states. *Quantum*, 6:791, September 2022. 2, 3, 4, 5, 6, 9, 11, 15, 18, 21, 23, 56, 62, 70, 76

[DBWR14] Frédéric Dupuis, Mario Berta, Jürg Wullschleger, and Renato Renner. One-shot decoupling. *Communications in Mathematical Physics*, 328(1):251–284, May 2014. 10

[EFL+24] Netta Engelhardt, Asmund Folkestad, Adam Levine, Evita Verheijden, and Lisa Yang. Cryptographic censorship, 2024. 3, 15, 18, 23

[EW01] T. Eggeling and R. F. Werner. Separability properties of tripartite states with $u \bigotimes u \bigotimes u$ symmetry. *Phys. Rev. A*, 63:042111, Mar 2001. 10

[GBO23] Dmitry Grinko, Adam Burchardt, and Maris Ozols. Gelfand-tsetlin basis for partially transposed permutations, with applications to quantum information, 2023. 10

[GHZ89] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. *Going Beyond Bell's Theorem*, pages 69–72. Springer Netherlands, Dordrecht, 1989. 1

[GLSV21] Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in miniqcrypt. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II*, volume 12697 of *Lecture Notes in Computer Science*, pages 531–561. Springer, 2021. 20, 22

[GMR23] Vipul Goyal, Giulio Malavolta, and Justin Raizes. Unclonable commitments and proofs. Cryptology ePrint Archive, Paper 2023/1538, 2023. 1, 7, 19, 22

[GO23] Dmitry Grinko and Maris Ozols. Linear programming with unitary-equivariant constraints, 2023. 10

[GZ20] Marios Georgiou and Mark Zhandry. Unclonable decryption keys. Cryptology ePrint Archive, Paper 2020/877, 2020. 1, 7, 19, 22

[Har93] Lucien Hardy. Nonlocality for two particles without inequalities for almost all entangled states. *Phys. Rev. Lett.*, 71:1665–1668, September 1993. 1

[Haw76] S. W. Hawking. Breakdown of predictability in gravitational collapse. *Phys. Rev. D*, 14:2460–2473, November 1976. 5, 15

[HH13] Daniel Harlow and Patrick Hayden. Quantum computation vs. firewalls. *Journal of High Energy Physics*, 2013(6), June 2013. 15, 16, 18

[HP07] Patrick Hayden and John Preskill. Black holes as mirrors: quantum information in random subsystems. *Journal of High Energy Physics*, 2007(09):120, September 2007. 3, 5, 15, 16, 18, 19, 66, 67

[Imp95] R. Impagliazzo. A personal view of average-case complexity. In *Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference*, pages 134–147, 1995. 20, 22

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. Cryptology ePrint Archive, Paper 2018/544, 2018. https://eprint.iacr.org/2018/544. 4, 5, 11, 20, 21, 27, 45

[JNV+21] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP* = RE. *Commun. ACM*, 64(11):131–138, October 2021. 1

[KLVY23] Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. Quantum advantage from any non-local game. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, page 1617–1628, New York, NY, USA, 2023. Association for Computing Machinery. 1

[Kni00] E. Knill. Approximation by quantum circuits. August 2000. 15

[KP23] Isaac H. Kim and John Preskill. Complementarity and the unitarity of the black hole S-matrix. *Journal of High Energy Physics*, 2023(2), February 2023. 3, 15, 18, 23

[KQST23] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. In Barna Saha and Rocco A. Servedio, editors, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*, pages 1589–1602. ACM, 2023. 20, 22

[Kre21] William Kretschmer. Quantum pseudorandomness and classical complexity. In Min-Hsiu Hsieh, editor, *16th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2021, July 5-8, 2021, Virtual Conference*, volume 197 of *LIPIcs*, pages 2:1–2:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. 3, 20, 21, 64

[KT23] Srijita Kundu and Ernest Y. Z. Tan. Device-independent uncloneable encryption, 2023. 1, 19, 20, 24, 75

[Mel24] Antonio Anna Mele. Introduction to Haar Measure Tools in Quantum Information: A Beginner's Tutorial. *Quantum*, 8:1340, May 2024. 63

[Mer90] N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett.*, 65:3373–3376, December 1990. 1

[MH24] Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. Cryptology ePrint Archive, Paper 2024/1652, 2024. 10, 11, 20, 22, 27

[MPSY24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t-designs and pseudorandom unitaries. In *65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024, Chicago, IL, USA, October 27-30, 2024*, pages 485–492. IEEE, 2024. 3, 5, 10, 11, 20, 22, 27

[MVW13] Abel Molina, Thomas Vidick, and John Watrous. Optimal counterfeiting attacks and generalizations for Wiesner's quantum money. In Kazuo Iwama, Yasuhito Kawano, and Mio Murao, editors, *Theory of Quantum Computation, Communication, and Cryptography*, pages 45–64, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. 1

[MY22] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I*, volume 13507 of *Lecture Notes in Computer Science*, pages 269–295. Springer, 2022. 20, 22

[NC16] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information (10th Anniversary edition)*. Cambridge University Press, 2016. 24, 39

[O'D21] Ryan O'Donnell. Analysis of boolean functions. *CoRR*, abs/2105.10386, 2021. 60

[PQS24] Alexander Poremba, Yihui Quek, and Peter Shor. The learning stabilizers with noise problem, 2024. 20

[Pre92] John Preskill. Do black holes destroy information? In *International Symposium on Black holes, Membranes, Wormholes and Superstrings*, January 1992. 5, 15

[Ron19] Marco Roncaglia. On the conservation of information in quantum physics. *Foundations of Physics*, 49:1278–1286, 2019. 1

[RUV12] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games, 2012. 1

[Sat22] Or Sattath. Uncloneable cryptography, 2022. 1, 2

[Sim95] Barry Simon. Representations of finite and compact groups. 1995. 26

[SS25] Michael Schleppy and Emina Soljanin. Winning rates of (n, k) quantum coset monogamy games. *arXiv preprint arXiv:2501.17736*, 2025. 2, 3, 4, 5, 6, 9, 11, 15, 18, 21, 23, 56, 59, 62, 70, 76

[SSS24] Michael Schleppy, Emina Soljanin, and Nicolas Swanson. Optimal strategies for winning certain coset-guessing quantum games. *arXiv preprint arXiv:2410.08160*, 2024. 9, 59

[STU93] Leonard Susskind, Lárus Thorlacius, and John Uglum. The stretched horizon and black hole complementarity. *Phys. Rev. D*, 48:3743–3761, October 1993. 15, 67

['t 85] Gerard 't Hooft. On the quantum structure of a black hole. *Nuclear Physics B*, 256:727–745, 1985. 67

[Ter04] B. M. Terhal. Is entanglement monogamous? *IBM Journal of Research and Development*, 48(1):71–78, 2004. 7

[TFKW13] Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, October 2013. 1, 2, 3, 4, 5, 7, 8, 9, 11, 12, 13, 14, 16, 18, 21, 23, 35, 36, 40, 47, 55, 56, 57, 59, 62, 66, 68, 70, 75, 76

[Web16] Zak Webb. The clifford group forms a unitary 3-design, 2016. 26

[Wer98] R. F. Werner. Optimal cloning of pure states. *Phys. Rev. A*, 58:1827–1832, Sep 1998. 4, 10, 11, 21, 45

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. 1

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, October 1982. 1, 2, 16, 19

[Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 239–268. Springer, 2019. 12, 42

[Zha21a] Mark Zhandry. How to construct quantum random functions. *J. ACM*, 68(5), August 2021. 11

[Zha21b] Mark Zhandry. Quantum lightning never strikes the same state twice. or: Quantum money from cryptographic assumptions. *J. Cryptol.*, 34(1):6, 2021. 22

A Relating Cloning Games to Monogamy-Like Games

In this section, we show that $t \mapsto t+1$ cloning games can be recast as a particular variant of a monogamy of entanglement game, as defined in Section 3.1. We first begin by presenting this argument when $t = 1$, which essentially follows by an argument laid out by Broadbent and Lord [BL20]. The additional structure we impose on the MOE game is as follows:

- The tripartite state $\rho \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}})$ which is shared between Alice, Bob and Charlie is the result of applying a cloning channel $\Phi_{\mathsf{A}' \to \mathsf{BC}}$ to one half of an EPR pair, i.e.,

  $$\rho_{\mathsf{ABC}} = (\mathbb{I}_{\mathsf{A}} \otimes \Phi_{\mathsf{A}' \to \mathsf{BC}})(|\mathsf{EPR}\rangle\langle\mathsf{EPR}|_{\mathsf{AA}'}).$$

  In other words, ρ_{ABC} is the normalized Choi state of some channel $\Phi_{\mathsf{A}' \to \mathsf{BC}}$.

- Alice's measurement $\left\{\mathbf{A}_x^\theta\right\}_{\theta \in \Theta, x \in \mathcal{X}}$ on register A is a projective measurement of the form

  $$\mathbf{A}_x^\theta = \bar{U}_\theta \left|x\right\rangle\!\left\langle x\right| \bar{U}_\theta^\dagger,$$

  for some family of unitary operators $\{U_\theta\}_{\theta \in \Theta}$ acting on $\mathcal{H}_{\mathsf{A}}$.

- (If we are in the oracular setting) Bob and Charlie's measurements can only depend on oracle queries to U_θ and $U_\theta^\dagger$, rather than directly on θ.

We now prove a formal equivalence between the two notions for $t = 1$.

Lemma A.1. *Let $\mathsf{G}_{1 \mapsto 2} = (1, \mathcal{H}_{\mathsf{A}}, \Theta, \mathcal{X}, \{U_\theta\}_{\theta \in \Theta})$ be a $1 \mapsto 2$ cloning game, for some family of unitary operators $\{U_\theta\}_{\theta \in \Theta}$ acting on the Hilbert space $\mathcal{H}_{\mathsf{A}}$. Then, the winning probability of a particular strategy $\mathsf{S} = (\mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}}, \Phi_{\mathsf{A} \to \mathsf{BC}}, \{\mathbf{P}_{1,x}^\theta\}_{\theta \in \Theta, x \in \mathcal{X}}, \{\mathbf{P}_{2,x}^\theta\}_{\theta \in \Theta, x \in \mathcal{X}})$ (possibly in the oracular setting) with*

$$\omega_{\mathsf{S}}(\mathsf{G}_{1 \mapsto 2}) = \mathop{\mathbb{E}}_{\theta \sim \Theta} \mathop{\mathbb{E}}_{x \sim \mathcal{X}} \operatorname{Tr}\left[\left(\mathbf{P}_{1,x}^\theta \otimes \mathbf{P}_{2,x}^\theta\right) \Phi_{\mathsf{A} \to \mathsf{BC}}(U_\theta \left|x\right\rangle\!\left\langle x\right|_{\mathsf{A}} U_\theta^\dagger)\right].$$

is exactly equal to the winning probability

$$\omega_{\tilde{\mathsf{S}}}(\mathsf{G}) = \mathop{\mathbb{E}}_{\theta\sim\Theta} \sum_{x\in\mathcal{X}} \operatorname{Tr}\left[\left(\mathbf{P}^{\theta}_{1,x} \otimes \mathbf{P}^{\theta}_{2,x} \otimes (\bar{U}_\theta \left|x\right\rangle\!\left\langle x\right|_{\mathsf{A}} \bar{U}_\theta^\dagger)\right) \rho_{\mathsf{BCA}}\right].$$

of a quantum strategy $\tilde{\mathsf{S}} = (\mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{C}}, \rho_{\mathsf{BCA}}, \{\mathbf{P}^{\theta}_{1,x}\}_{\theta\in\Theta,x\in\mathcal{X}}, \{\mathbf{P}^{\theta}_{2,x}\}_{\theta\in\Theta,x\in\mathcal{X}})$ *(possibly in the oracular setting) of a monogamy entanglement game* $\mathsf{G} = (\mathcal{H}_{\mathsf{A}}, \Theta, \mathcal{X}, \{\bar{U}_\theta \left|x\right\rangle\!\left\langle x\right| \bar{U}_\theta^\dagger\}_{\theta\in\Theta,x\in\mathcal{X}})$*, where*

$$\rho_{\mathsf{BCA}} = (\Phi_{\mathsf{A}'\to\mathsf{BC}} \otimes \mathbb{I}_{\mathsf{A}}) \left|\mathsf{EPR}\right\rangle\!\left\langle\mathsf{EPR}\right|_{\mathsf{A}'\mathsf{A}}.$$

Here, $\left|\mathsf{EPR}\right\rangle_{\mathsf{AA}'}$ *denotes* $\frac{1}{\sqrt{|\mathcal{X}|}} \sum_{x\in\mathcal{X}} \left|x\right\rangle_{\mathsf{A}} \otimes \left|x\right\rangle_{\mathsf{A}'}$*. (We swap the* A *and* BC *registers in the formulation of the relevant monogamy game for the purposes of syntactic compliance with Corollary 2.2 in our proof.)*

Proof. Recall that Corollary 2.2 implies that, for any projector $\mathbf{P} \in L(\mathcal{H}_{\mathsf{BC}})$,

$$\operatorname{Tr}\left[\mathbf{P}_{\mathsf{BC}} \Phi_{\mathsf{A}'\to\mathsf{BC}}(U_\theta \left|x\right\rangle\!\left\langle x\right|_{\mathsf{A}} U_\theta^\dagger)\right] = \operatorname{Tr}\left[\left(\mathbf{P} \otimes \bar{U}_\theta \left|x\right\rangle\!\left\langle x\right| \bar{U}_\theta^\dagger\right) J(\Phi)\right],$$

where $J(\Phi) \in \mathrm{L}(\mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}} \otimes \mathcal{H}_{\mathsf{A}})$ is the Choi-Jamiołkowski isomorphism of Φ. Therefore:

$$\begin{aligned}
\omega_{\mathsf{S}}(\mathsf{G}_{1\mapsto 2}) &= \mathop{\mathbb{E}}_{\theta\sim\Theta} \mathop{\mathbb{E}}_{x\sim\mathcal{X}} \operatorname{Tr}\left[\left(\mathbf{P}^{\theta}_{1,x} \otimes \mathbf{P}^{\theta}_{2,x}\right) \Phi_{\mathsf{A}\to\mathsf{BC}}(U_\theta \left|x\right\rangle\!\left\langle x\right|_{\mathsf{A}} U_\theta^\dagger)\right] \\
&= \mathop{\mathbb{E}}_{\theta\sim\Theta} \mathop{\mathbb{E}}_{x\sim\mathcal{X}} \operatorname{Tr}\left[\left(\mathbf{P}^{\theta}_{1,x} \otimes \mathbf{P}^{\theta}_{2,x} \otimes (\bar{U}_\theta \left|x\right\rangle\!\left\langle x\right|_{\mathsf{A}} \bar{U}_\theta^\dagger)\right) J(\Phi)\right] \\
&= \mathop{\mathbb{E}}_{\theta\sim\Theta} \sum_{x\sim\mathcal{X}} \operatorname{Tr}\left[\left(\mathbf{P}^{\theta}_{1,x} \otimes \mathbf{P}^{\theta}_{2,x} \otimes (\bar{U}_\theta \left|x\right\rangle\!\left\langle x\right|_{\mathsf{A}} \bar{U}_\theta^\dagger)\right) \rho_{\mathsf{BCA}}\right] = \omega_{\tilde{\mathsf{S}}}(\mathsf{G}),
\end{aligned}$$

where we define $\rho_{\mathsf{BCA}} = (\Phi_{\mathsf{A}'\to\mathsf{BC}} \otimes \mathbb{I}_{\mathsf{A}}) \left|\mathsf{EPR}\right\rangle\!\left\langle\mathsf{EPR}\right|_{\mathsf{A}'\mathsf{A}}$. The final step holds because of the identity $J(\Phi) = |\mathcal{X}| \cdot \rho_{\mathsf{BCA}}$ (see the definitions preceding Lemma 2.1). This proves the claim. □

We can generalize this to arbitrary t as follows:

Lemma A.2. *For any* $t \geq 1$*, let* $\mathsf{G}_{t\mapsto t+1} = (t, \mathcal{H}_{\mathsf{A}^t}, \Theta, \mathcal{X}, \{U_\theta\}_{\theta\in\Theta})$ *be a* $t \mapsto t+1$ *cloning game, for some family of unitary operators* $\{U_\theta\}_{\theta\in\Theta}$ *acting on the Hilbert space* $\mathcal{H}_{\mathsf{A}}$*. Moreover, define the shared state*

$$\rho_{\mathsf{B}_{1:t+1}\mathsf{A}'_{1:t}} := (\Phi_{\mathsf{A}_1\ldots\mathsf{A}_t\to\mathsf{B}_1\ldots\mathsf{B}_{t+1}} \otimes \mathbb{I}_{\mathsf{A}'_{1:t}}) \left(\left|\mathsf{EPR}^n\right\rangle\!\left\langle\mathsf{EPR}^n\right|^{\otimes t}\right).$$

Then, the winning probability of a particular strategy $\mathsf{S} = (\mathcal{H}_{\mathsf{B}^{t+1}}, \Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}, \{\mathbf{P}^{\theta}_{1,x}\}_{\theta\in\Theta,x\in\mathcal{X}}, \ldots, \{\mathbf{P}^{\theta}_{t+1,x}\}_{\theta\in\Theta,x\in\mathcal{X}})$ *(possibly in the oracular setting) with*

$$\omega_{\mathsf{S}}(\mathsf{G}_{t\mapsto t+1}) := \mathop{\mathbb{E}}_{\theta\sim\Theta} \mathop{\mathbb{E}}_{x\sim\mathcal{X}} \operatorname{Tr}\left[\left(\mathbf{P}^{U_\theta, U_\theta^\dagger}_{1,x} \otimes \ldots \otimes \mathbf{P}^{U_\theta, U_\theta^\dagger}_{t+1,x}\right) \Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}\left((U_\theta \left|x\right\rangle\!\left\langle x\right| U_\theta^\dagger)^{\otimes t}_{\mathsf{A}^t}\right)\right].$$

is exactly equal to the quantity

$$|\mathcal{X}|^{t-1} \cdot \mathop{\mathbb{E}}_{\theta\sim\Theta} \sum_{x\in\mathcal{X}} \operatorname{Tr}\left[\left(\bigotimes_{i=1}^{t+1} \mathbf{P}^{\theta}_{i,x} \otimes (\bar{U}_\theta \left|x\right\rangle\!\left\langle x\right|_{\mathsf{A}} \bar{U}_\theta^\dagger)^{\otimes t}\right) \rho_{\mathsf{B}_{1:t+1}\mathsf{A}'_{1:t}}\right].$$

Proof. Let $J(\Phi) \in \mathrm{L}(\mathcal{H}_{\mathsf{B}_{1:t+1}} \otimes \mathcal{H}_{\mathsf{A}'_{1:t}})$ denote the Choi-Jamiołkowski isomorphism of the cloning map $\Phi_{\mathsf{A}_{1:t}\to\mathsf{B}_{1:t+1}}$. Recall that

$$J(\Phi) = |\mathcal{X}|^t \cdot (\Phi_{\mathsf{A}_1\ldots\mathsf{A}_t\to\mathsf{B}_1\ldots\mathsf{B}_{t+1}} \otimes \mathbb{I}_{\mathsf{A}'_{1:t}}) \left(|\mathsf{EPR}^n\rangle\langle\mathsf{EPR}^n|^{\otimes t}\right) = |\mathcal{X}|^t \rho.$$

Now using Lemma 2.1, we have:

$$\begin{aligned}
\omega_{\mathsf{S}}(\mathsf{G}) =& \mathop{\mathbb{E}}_{\theta} \mathop{\mathbb{E}}_{x\sim\mathcal{X}} \mathrm{Tr}\left[\left(\bigotimes_{i=1}^{t+1} \mathbf{P}^{\theta}_{i,x}\right) \Phi_{\mathsf{A}_1\ldots\mathsf{A}_t\to\mathsf{B}_1\ldots\mathsf{B}_{t+1}} \left((U_\theta |x\rangle\langle x| U_\theta^\dagger)^{\otimes t}_{\mathsf{A}_1\ldots\mathsf{A}_t}\right)\right] \\
=& \mathop{\mathbb{E}}_{\theta} \mathop{\mathbb{E}}_{x\sim\mathcal{X}} \mathrm{Tr}\left[\left(\bigotimes_{i=1}^{t+1} \mathbf{P}^{\theta}_{i,x} \otimes \left(\bar{U}_\theta |x\rangle\langle x| \bar{U}_\theta^\dagger\right)^{\otimes t}_{\mathsf{A}'_{1:t}}\right) J(\Phi)_{\mathsf{B}_{1:t+1}\mathsf{A}'_{1:t}}\right] \\
=& |\mathcal{X}|^t \cdot \mathop{\mathbb{E}}_{\theta} \mathop{\mathbb{E}}_{x\sim\mathcal{X}} \mathrm{Tr}\left[\left(\bigotimes_{i=1}^{t+1} \mathbf{P}^{\theta}_{i,x} \otimes \left(\bar{U}_\theta |x\rangle\langle x| \bar{U}_\theta^\dagger\right)^{\otimes t}_{\mathsf{A}'_{1:t}}\right) \rho_{\mathsf{B}_{1:t+1}\mathsf{A}'_{1:t}}\right] \\
=& |\mathcal{X}|^{t-1} \cdot \mathop{\mathbb{E}}_{\theta} \sum_{x\sim\mathcal{X}} \mathrm{Tr}\left[\left(\bigotimes_{i=1}^{t+1} \mathbf{P}^{\theta}_{i,x} \otimes \left(\bar{U}_\theta |x\rangle\langle x| \bar{U}_\theta^\dagger\right)^{\otimes t}_{\mathsf{A}'_{1:t}}\right) \rho_{\mathsf{B}_{1:t+1}\mathsf{A}'_{1:t}}\right].
\end{aligned}$$

□