

Information-Theoretic Hiding in Quantum Marginal Fibers

Exact Repetition Fibers, One-Shot Hiding, and Leakage Bounds

Jaroslav Hrubý

Group of Cryptology, Union of Czech Mathematicians and Physicists (GCUCMP)

Prague, Czech Republic

Corresponding author: hruby.jar@centrum.cz

12 September 2026

Abstract

We study information-theoretic hiding when an adversary has unrestricted quantum processing but physical access to only one region from a declared family of subsystems. Perfectly hidden classical codewords lie in one fiber of the corresponding marginal map. We organize trace-distance diameter, orthogonal zero-error packing, and exact coherent *subspace* hiding on this fixed-marginal set, distinguishing equality of basis-state marginals from the cross-term conditions of quantum error correction.

For $n \geq 3$ sites of local dimension q , we characterize the entire mixed-state fiber of repetition states with prescribed, possibly nonuniform, probabilities p :

$$\mathcal{F}_p = \{VCV^\dagger : C \succeq 0, \text{Tr } C = 1, C_{jj} = p_j\}, \quad V|j\rangle = |j\rangle^{\otimes n}.$$

Writing $r = |\text{supp } p|$ and $a = \max_j p_j$, its affine dimension is $r^2 - r$, its exact coherent hiding dimension is one, and its trace-distance diameter is $\sqrt{1 - \max\{0, 2a - 1\}^2}$. Its orthogonal packing number is at most $\lfloor 1/a \rfloor$, with at least two orthogonal states exactly when $a \leq 1/2$. For uniform p , the equal-amplitude Fourier-phase family attains the exact packing number q , giving $C_{\text{cl}} = \log_2 q$ and $C_{\text{coh}} = 0$. A connectivity criterion identifies which covering families of proper marginals already force the same complete fiber.

These results provide explicit fiber geometry and simultaneous one-shot evaluations; they do not assert a new GHZ nonuniqueness phenomenon or a new no-cloning obstruction. We give binary and finite-alphabet leakage bounds, and an observable-algebra formulation with an exact criterion for autonomous accessible dynamics. In the latter, uniform vanishing of the first-order leakage coefficient already implies exact invariance, unlike vanishing for one selected hidden direction.

Keywords: quantum cryptography; quantum marginal problem; information-theoretic secrecy; quantum secret sharing; private subspaces; trace distance; observable algebras.

1 Introduction

Information-theoretic secrecy can be defined by physical access rather than computational power. A sender encodes a classical message into a multipartite quantum state, while an adversary can act arbitrarily on one region from a prescribed access family $\mathcal{A}$. Perfect secrecy requires the adversary's reduced state to be message-independent. This model is closely related to quantum secret sharing, private quantum coding, and masking [11, 12, 19, 13]. It differs from LOCC-style data hiding, which restricts the measurement class on a larger accessible physical system [14, 15].

The underlying compatibility sets and their convex geometry are established objects in the quantum marginal problem [3, 4, 5, 6]. In particular, Walck and Lyons explicitly used the preimage of the map of all $(n - 1)$ -body reduced density matrices and studied competitors that may be pure or mixed [9]; their earlier result treated pure competitors [8]. Ocko et al. connected nonunique reduced-density-matrix preimages and locally indistinguishable subspaces to quantum error-correcting codes [10]. We use this literature as a starting point, not as a phenomenon newly introduced here.

Let

$$\mathcal{M}_{\mathcal{A}}(\rho) = (\rho_A)_{A \in \mathcal{A}}, \quad \mathcal{F}_m = \{\rho \in \mathcal{D}(\mathcal{H}) : \rho_A = m_A \text{ for every } A \in \mathcal{A}\}. \quad (1)$$

The term *marginal fiber* means this preimage. Distinct states in one fiber can be perfectly distinguishable globally while being indistinguishable on every individually allowed region. Our purpose is to organize several operational questions inside the same fiber and to evaluate a repetition family explicitly.

The cryptographic motivation was presented in preliminary, non-proceedings form in the author's EUROCRYPT 2026 Rump Session contribution [1].

Threat-model convention. The family $\mathcal{A}$ describes the adversary's *complete* access in one execution. If regions can collude or be accessed sequentially with retained quantum memory, that combined access must also be modeled. Equality of separate marginals does not imply security for their union. Auxiliary systems introduced by the adversary are initially independent of the message; any correlated side information must be incorporated explicitly into the accessible system. The results do not establish security against unspecified coalitions, active attacks on state distribution, or arbitrary global LOCC measurements.

1.1 Principal results

Geometry and one-shot quantities. We decompose the kernel of $\mathcal{M}_{\mathcal{A}}$ by tensor support and bound the number $N_{\perp}(\mathcal{F}_m)$ of pairwise orthogonally supported states using support and affine dimensions. The logarithm

$$C_{\text{cl}}(\mathcal{F}_m) = \log_2 N_{\perp}(\mathcal{F}_m) \quad (2)$$

is a one-shot zero-error classical hiding quantity. Exact coherent subspace hiding instead requires $\mathcal{D}(\mathcal{C}) \subseteq \mathcal{F}_m$ for a code subspace $\mathcal{C}$, including all superpositions and mixtures. Its maximum dimension K_{coh} obeys $K_{\text{coh}} \leq N_{\perp}$. We use $C_{\text{coh}} = \log_2 K_{\text{coh}}$ only when $K_{\text{coh}} \geq 1$.

Complete repetition fibers and nonuniform data. For $n \geq 3$, fixing all $(n - 1)$ -party marginals of repetition states with probabilities p gives

$$\mathcal{F}_p = V\{C \in \mathcal{D}(\mathbb{C}^q) : \text{diag } C = p\}V^{\dagger}. \quad (3)$$

For $r = |\text{supp } p|$ and $a = \max_j p_j$ we prove

$$\dim \text{aff } \mathcal{F}_p = r^2 - r, \quad D(\mathcal{F}_p) = \sqrt{1 - \max\{0, 2a - 1\}^2}, \quad K_{\text{coh}}(\mathcal{F}_p) = 1. \quad (4)$$

Moreover, $N_{\perp} \leq \lfloor 1/a \rfloor$ and $N_{\perp} \geq 2$ exactly when $a \leq 1/2$. Uniform probabilities give the exact evaluation

$$D = 1, \quad N_{\perp} = q, \quad C_{\text{cl}} = \log_2 q, \quad K_{\text{coh}} = 1, \quad C_{\text{coh}} = 0. \quad (5)$$

A graph-connectivity criterion characterizes when a covering family of proper marginals already yields (3). The results for nonuniform p include boundary cases with zero probabilities; we do not claim an exact formula for $N_{\perp}$ for every nonuniform p .

Leakage and dynamics. Pairwise local trace-norm separation at most ε gives the exact binary upper bound $1/2 + \varepsilon/4$ and a Holevo upper bound obtained from Audenaert’s entropy-continuity inequality. We also formulate access through a finite-dimensional observable algebra and characterize when microscopic unitary evolution induces an automorphism of its full accessible state space. The general coarse-graining principle is established [21, 22]; here it separates static secrecy from subsequent dynamical leakage.

1.2 Scope and contribution

The contribution is an explicit complete-fiber calculation with simultaneous operational evaluations and extensions to nonuniform data and connected access families. The equal-amplitude classical-coherent separation is *not* presented as a previously unknown quantum-coding phenomenon: quantum secret sharing and no-cloning already preclude a nontrivial pure subspace code hidden from every $(n - 1)$ -party region [11, 12]. The cross-term criterion, Helstrom formula, volumetric estimate, and general algebraic reducibility principle are supporting standard ingredients.

The paper is restricted to finite-dimensional quantum information. It makes no derivation of spacetime, supersymmetric microphysics, or gravitational dynamics. Nor does $K_{\text{coh}} = 1$ rule out every possible quantum encoding: private subsystems, reversible mixed-state encodings, and key-assisted protocols are different tasks [11, 19]. No categorical historical-priority claim is made for the explicit evaluations or their elementary ingredients.

2 Preliminaries

2.1 Multipartite systems and accessible regions

Let

$$\mathcal{H} = \bigotimes_{i=1}^n \mathcal{H}_i, \quad \dim \mathcal{H}_i = d_i < \infty. \quad (6)$$

For $A \subseteq [n] = \{1, \dots, n\}$ write $A^c = [n] \setminus A$ and $\mathcal{H}_A = \bigotimes_{i \in A} \mathcal{H}_i$. The reduced state is $\rho_A = \text{Tr}_{A^c} \rho$. We take $\mathcal{H}_\emptyset = \mathbb{C}$ and allow $\emptyset$ as a region when convenient. The access family $\mathcal{A} \subseteq 2^{[n]}$ is nonempty and need not be downward closed.

Definition 2.1 (Marginal map). The marginal map is

$$\mathcal{M}_\mathcal{A} : \mathcal{D}(\mathcal{H}) \longrightarrow \prod_{A \in \mathcal{A}} \mathcal{D}(\mathcal{H}_A), \quad \rho \longmapsto (\rho_A)_{A \in \mathcal{A}}. \quad (7)$$

A tuple $m = (m_A)_{A \in \mathcal{A}}$ is *compatible* if it lies in its image.

Definition 2.2 (Marginal fiber). For compatible m , set

$$\mathcal{F}_m = \mathcal{M}_\mathcal{A}^{-1}(m) = \{\rho \in \mathcal{D}(\mathcal{H}) : \rho_A = m_A \ \forall A \in \mathcal{A}\}. \quad (8)$$

2.2 Cryptographic access model

A classical variable X is encoded as $x \mapsto \rho_x \in \mathcal{D}(\mathcal{H})$. For a selected $A \in \mathcal{A}$, the adversary may append message-independent ancillas, apply arbitrary completely positive trace-preserving (CPTP) maps on the available registers, and perform arbitrary positive-operator-valued measurements (POVMs). The adversary has no access to A^c .

Definition 2.3 (Perfect subsystem secrecy). The encoding is perfectly secret against $\mathcal{A}$ if for each $A \in \mathcal{A}$ there is a state m_A such that

$$\rho_{x,A} = m_A \quad \text{for all messages } x. \quad (9)$$

Proposition 2.4 (Fiber characterization of perfect secrecy). *An encoding is perfectly secret against $\mathcal{A}$ if and only if all codewords lie in one marginal fiber. Every allowed local strategy then has message-independent outcome statistics.*

Proof. The defining condition is precisely $\mathcal{M}_{\mathcal{A}}(\rho_x) = m$ for every x . A local CPTP map, including independent ancillary preparation, acts on the same input state for every message. Its output and the statistics of every subsequent POVM therefore also coincide. $\square$

The receiver is allowed access to the full system. Thus the quantities below concern global recovery with perfect secrecy from each allowed region, not a complete key-distribution or authentication protocol.

2.3 Trace distance and discrimination

We use

$$T(\rho, \sigma) = \frac{1}{2} \|\rho - \sigma\|_1. \quad (10)$$

Trace distance lies in $[0, 1]$ and is contractive under CPTP maps [2]. In particular, $T(\rho_A, \sigma_A) \leq T(\rho, \sigma)$. For two equiprobable states the Helstrom formula is [16, 2]

$$P_{\text{succ}}(\rho, \sigma) = \frac{1}{2} + \frac{1}{4} \|\rho - \sigma\|_1. \quad (11)$$

All logarithms and entropies below are in base two. For pure states, direct diagonalization in their two-dimensional span gives

$$T(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = \sqrt{1 - |\langle\psi|\phi\rangle|^2}. \quad (12)$$

3 Marginal Fibers as Convex Spectrahedra

3.1 Affine-kernel structure

Extend the marginal map linearly to Hermitian operators and define

$$\mathcal{K}_{\mathcal{A}} = \{X \in \text{Herm}(\mathcal{H}) : \text{Tr}_{A^c} X = 0 \text{ for every } A \in \mathcal{A}\}. \quad (13)$$

Every $X \in \mathcal{K}_{\mathcal{A}}$ is traceless because $\mathcal{A}$ is nonempty.

Proposition 3.1 (Affine-kernel representation). *For any $\rho_0 \in \mathcal{F}_m$,*

$$\mathcal{F}_m = (\rho_0 + \mathcal{K}_{\mathcal{A}}) \cap \mathcal{D}(\mathcal{H}). \quad (14)$$

The fiber is compact, convex, and a spectrahedron in the ambient affine space $\rho_0 + \mathcal{K}_{\mathcal{A}}$.

Proof. The states ρ and ρ_0 have the same accessible marginals exactly when $\rho - \rho_0 \in \mathcal{K}_{\mathcal{A}}$. The remaining condition is positivity; normalization is already fixed. The state space is compact and convex, the affine constraint is closed, and positivity is a linear matrix inequality. $\square$

3.2 Exact decomposition of hidden operator directions

For each site,

$$\text{Herm}(\mathcal{H}_i) = \mathbb{R}I_i \oplus \text{Herm}_0(\mathcal{H}_i), \quad \dim_{\mathbb{R}} \text{Herm}_0(\mathcal{H}_i) = d_i^2 - 1, \quad (15)$$

where Herm_0 denotes the traceless part. Define the real tensor-support sector

$$\mathcal{V}_S = \bigotimes_{i \in S} \text{Herm}_0(\mathcal{H}_i) \otimes \bigotimes_{i \notin S} \mathbb{R}I_i \quad (S \subseteq [n]). \quad (16)$$

The direct sum $\text{Herm}(\mathcal{H}) = \bigoplus_{S \subseteq [n]} \mathcal{V}_S$ is orthogonal in the Hilbert–Schmidt inner product.

Theorem 3.2 (Support decomposition of the marginal kernel).

$$\mathcal{K}_{\mathcal{A}} = \bigoplus_{\substack{\emptyset \neq S \subseteq [n] \\ S \not\subseteq A \ \forall A \in \mathcal{A}}} \mathcal{V}_S, \quad \dim \mathcal{K}_{\mathcal{A}} = \sum_{\substack{\emptyset \neq S \subseteq [n] \\ S \not\subseteq A \ \forall A \in \mathcal{A}}} \prod_{i \in S} (d_i^2 - 1). \quad (17)$$

Proof. If $S \not\subseteq A$, at least one traceless tensor factor is traced out, so $\text{Tr}_{A^c} X_S = 0$ for $X_S \in \mathcal{V}_S$. If $S \subseteq A$, partial trace removes only identity factors and maps the sector injectively, up to a nonzero scalar, to the corresponding sector on A . For fixed A , the images for different $S \subseteq A$ remain orthogonal, so they cannot cancel. The identity sector is always visible. This proves the decomposition and its dimension formula. $\square$

Corollary 3.3 (Full-rank fiber dimension). *If $\mathcal{F}_m$ contains a positive-definite state, then*

$$\dim \text{aff } \mathcal{F}_m = \dim \mathcal{K}_{\mathcal{A}}. \quad (18)$$

Proof. For $\rho_0 > 0$, every sufficiently small perturbation in the finite-dimensional space $\mathcal{K}_{\mathcal{A}}$ remains positive. Consequently the affine hull in (14) is the entire ambient affine space. $\square$

Corollary 3.4 (Exact k -local access structure). *Suppose $d_i = q$ and $1 \leq k \leq n$. For the exact family*

$$\mathcal{A}_k = \{A \subseteq [n] : 1 \leq |A| \leq k\}, \quad (19)$$

a fiber containing a full-rank state has

$$\dim \text{aff } \mathcal{F}_m = \sum_{s=k+1}^n \binom{n}{s} (q^2 - 1)^s. \quad (20)$$

For $k = n$ the sum is zero and every fiber is a singleton. More generally, if every $(n-1)$ -party region is accessible but $[n] \notin \mathcal{A}$, then

$$\mathcal{K}_{\mathcal{A}} = \mathcal{V}_{[n]}, \quad \dim \mathcal{K}_{\mathcal{A}} = (q^2 - 1)^n. \quad (21)$$

Proof. For $\mathcal{A}_k$, a nonempty S is contained in some accessible region exactly when $|S| \leq k$. Apply Theorem 3.2. In the last claim every proper support is visible and the full support is invisible. $\square$

Remark 3.5 (Zero-access convention). With $\mathcal{A}_0 = \{\emptyset\}$, the kernel is the traceless Hermitian space and has dimension $q^{2n} - 1$. This is different from an empty index family, which we do not use.

Remark 3.6. The hidden linear sectors depend only on $\mathcal{A}$. Positivity can reduce the actual affine dimension drastically when the prescribed data have low rank; the repetition example illustrates this distinction.

4 Support Constraints and the Geometry of a Fiber

4.1 The support-compatible subspace

For each m_A let P_A project onto its support, and set

$$\mathcal{S}_m = \bigcap_{A \in \mathcal{A}} (\text{supp}(m_A) \otimes \mathcal{H}_{A^c}). \quad (22)$$

Lemma 4.1 (Support restriction). *Every $\rho \in \mathcal{F}_m$ satisfies $\text{supp}(\rho) \subseteq \mathcal{S}_m$.*

Proof. Put $Q_A = I_A - P_A$. Positivity gives

$$0 = \text{Tr}(Q_A m_A) = \text{Tr}[(Q_A \otimes I) \rho] = \|(Q_A \otimes I) \rho^{1/2}\|_2^2. \quad (23)$$

Thus the range of $\rho^{1/2}$, and hence the support of ρ , is contained in $\text{supp}(m_A) \otimes \mathcal{H}_{A^c}$. Intersect over A . $\square$

4.2 Extreme points and diameter

Definition 4.2 (Global fiber diameter).

$$D(\mathcal{F}_m) = \max_{\rho, \sigma \in \mathcal{F}_m} T(\rho, \sigma). \quad (24)$$

Compactness ensures that the maximum exists.

Proposition 4.3 (Diameter is attained on extreme points).

$$D(\mathcal{F}_m) = \max_{\rho, \sigma \in \text{Ext}(\mathcal{F}_m)} T(\rho, \sigma). \quad (25)$$

Proof. Take a maximizing pair. In finite dimension each member of a compact convex set is a finite convex combination of extreme points. Writing $\rho = \sum_j p_j \rho_j$, convexity of trace distance gives

$$D = T(\rho, \sigma) \leq \sum_j p_j T(\rho_j, \sigma) \leq D.$$

An extreme ρ_j therefore also attains D . Repeat for the second argument. This proves existence of an extreme maximizing pair without assuming that the set of extreme points is closed. $\square$

Theorem 4.4 (Perfect global distinguishability). *The following are equivalent: $D(\mathcal{F}_m) = 1$; the fiber contains two states with orthogonal supports; and two states in the fiber can be perfectly distinguished in one global measurement.*

Proof. For density operators, trace distance one is equivalent to orthogonal supports, and orthogonal supports are equivalent to perfect discrimination [2]. Within one fiber, all accessible marginal statistics coincide by definition. $\square$

5 Orthogonal Packing and Perfect Classical Hiding

Definition 5.1 (Orthogonality number). $N_\perp(\mathcal{F}_m)$ is the largest number of states in $\mathcal{F}_m$ whose supports are pairwise orthogonal.

The number is finite and at least one. The maximum exists because the nonempty set of attainable integer sizes is bounded by $\dim \mathcal{H}$.

Definition 5.2 (One-shot zero-error classical hiding quantity).

$$C_{\text{cl}}(\mathcal{F}_m) = \log_2 N_\perp(\mathcal{F}_m). \quad (26)$$

An alphabet encoded into orthogonally supported states is recovered perfectly by a global support measurement, while every allowed region has the same density operator for every message. The word “capacity” for C_{cl} refers only to this one-shot zero-error task, not a regularized communication capacity.

Theorem 5.3 (Geometric upper bounds on orthogonal packing). *For $k = \dim \text{aff } \mathcal{F}_m$ and $s = \dim \mathcal{S}_m$,*

$$N_\perp(\mathcal{F}_m) \leq \min\{s, k + 1\}, \quad C_{\text{cl}}(\mathcal{F}_m) \leq \log_2 \min\{s, k + 1\}. \quad (27)$$

Proof. By Lemma 4.1, the pairwise orthogonal nonzero supports are subspaces of an s -dimensional space, giving $N \leq s$. They are also affinely independent. Indeed, if $\sum_i c_i \rho_i = 0$, tracing against the support projector of ρ_j gives $c_j = 0$. Their convex hull is therefore an $(N - 1)$ -simplex inside a k -dimensional affine space, so $N \leq k + 1$. $\square$

Corollary 5.4. $D(\mathcal{F}_m) = 1$ if and only if $N_\perp(\mathcal{F}_m) \geq 2$.

6 Exact Coherent Hiding and the Classical–Coherent Gap

A finite classical alphabet and an entire coherent code subspace impose different requirements. Here “coherent hiding” always means the exact *subspace* task defined below.

Definition 6.1 (Exact coherent hiding subspace and dimension). A nonzero subspace $\mathcal{C} \subseteq \mathcal{H}$ hides coherently in $\mathcal{F}_m$ if

$$\mathcal{D}(\mathcal{C}) \subseteq \mathcal{F}_m. \quad (28)$$

Define

$$K_{\text{coh}}(\mathcal{F}_m) = \max(\{\dim \mathcal{C} : \mathcal{C} \neq \{0\}, \mathcal{D}(\mathcal{C}) \subseteq \mathcal{F}_m\} \cup \{0\}). \quad (29)$$

For $K_{\text{coh}} \geq 1$, set $C_{\text{coh}} = \log_2 K_{\text{coh}}$; for $K_{\text{coh}} = 0$ leave C_{coh} undefined.

Thus $K_{\text{coh}} = 0$ exactly when the fiber contains no pure state. A one-dimensional subspace hides no variable logical quantum state and has $C_{\text{coh}} = 0$. This invariant is not an asymptotic quantum-channel capacity and does not optimize over all mixed-state encoders or private subsystems.

Theorem 6.2 (Cross-term criterion). *Let $\{|i_L\rangle\}_{i=1}^K$ be an orthonormal basis of $\mathcal{C}$. Then $\mathcal{D}(\mathcal{C}) \subseteq \mathcal{F}_m$ if and only if*

$$\text{Tr}_{A^c} |i_L\rangle\langle j_L| = \delta_{ij} m_A \quad (A \in \mathcal{A}, 1 \leq i, j \leq K). \quad (30)$$

Proof. If (30) holds, any supported density matrix $\tau = \sum_{ij} \tau_{ij} |i_L\rangle\langle j_L|$ has marginal $\sum_i \tau_{ii} m_A = m_A$. Conversely, the basis projectors have marginal m_A . For $i \neq j$ put $X = \text{Tr}_{A^c} |i_L\rangle\langle j_L|$. The states $(|i_L\rangle + e^{i\theta} |j_L\rangle)/\sqrt{2}$ give $e^{-i\theta} X + e^{i\theta} X^\dagger = 0$. At $\theta = 0$ and $\pi/2$ this yields respectively $X + X^\dagger = 0$ and $X - X^\dagger = 0$. Hence $X = 0$. $\square$

Remark 6.3. This is the standard erasure-correction/private-subspace condition expressed inside a fixed fiber [18, 11, 12, 19]. Ocko et al. likewise use scalar compression of local observables to describe subspaces with indistinguishable reductions [10]. Equality only on a selected basis omits the off-diagonal conditions and protects a classical alphabet, not arbitrary superpositions.

Theorem 6.4 (Coherent dimension is bounded by orthogonal packing). *For every fiber, $K_{\text{coh}} \leq N_\perp$. When $K_{\text{coh}} \geq 1$, one also has $C_{\text{coh}} \leq C_{\text{cl}}$.*

Proof. An orthonormal basis of a K -dimensional coherent hiding subspace gives K orthogonal pure states in the fiber. The case $K_{\text{coh}} = 0$ is immediate. $\square$

Proposition 6.5 (Standard no-cloning obstruction). *If $A, B \in \mathcal{A}$ have disjoint complements, then $K_{\text{coh}}(\mathcal{F}_m) \leq 1$ for every compatible fiber. In particular this holds if $\mathcal{A}$ contains all $(n-1)$ -party regions and $n \geq 2$.*

Proof. For an isometric code, (30) for A implies exact recovery from A^c . To see the implication directly, diagonalize $m_A = \sum_a \lambda_a |a\rangle\langle a|$ on its support and write

$$|i_L\rangle = \sum_a \sqrt{\lambda_a} |a\rangle_A |v_{ia}\rangle_{A^c}.$$

Equation (30) gives $\langle v_{jb} | v_{ia} \rangle = \delta_{ij} \delta_{ab}$. An isometry on their span sends $|v_{ia}\rangle$ to $|i\rangle|a\rangle$; discarding the second register recovers the logical state. The same holds for B^c . If A^c and B^c are disjoint, both recovery channels can be applied simultaneously. For any pure logical input each output is that same pure state, so the joint output is its tensor square. This would clone arbitrary states in a space of dimension at least two, which is impossible [11, 12]. Distinct single-site complements establish the last assertion. $\square$

This proposition isolates the established structural reason for the coherent obstruction in the repetition example. It is not a new no-cloning theorem, and does not apply as stated to a general mixed-state secret-sharing encoding.

7 Exact Repetition/GHZ Marginal Fibers

7.1 The equal-amplitude Fourier-phase family

Let $q \geq 2$, $n \geq 3$, and $\mathcal{H} = (\mathbb{C}^q)^{\otimes n}$. Define

$$V : \mathbb{C}^q \longrightarrow \mathcal{H}, \quad V|j\rangle = |j\rangle^{\otimes n} \quad (0 \leq j < q). \quad (31)$$

Writing $\omega = e^{2\pi i/q}$, the orthonormal Fourier vectors and their images are

$$|\phi_r\rangle = \frac{1}{\sqrt{q}} \sum_{j=0}^{q-1} \omega^{rj} |j\rangle, \quad |\Psi_r\rangle = V|\phi_r\rangle \quad (0 \leq r < q). \quad (32)$$

Tracing out any nonempty complement annihilates every off-diagonal term $|j\rangle^{\otimes n} \langle \ell|^{\otimes n}$ with $j \neq \ell$. Thus every nonempty proper region has marginal

$$m_A = \frac{1}{q} \sum_{j=0}^{q-1} |j^{\otimes |A|} \rangle \langle j^{\otimes |A|}|. \quad (33)$$

The empty-region marginal, when used, is the scalar one. In Sections 7.1–7.4 the access family is exactly

$$\mathcal{A}^{(n-1)} = \{A \subseteq [n] : |A| = n - 1\}. \quad (34)$$

Fixing these marginals also fixes every smaller proper marginal; the full region is excluded. The superscript notation distinguishes this exact-size family from the family $\mathcal{A}_k$ of all regions of size at most k in Section 3.

7.2 Complete characterization of the uniform fiber

Comparison with earlier work. Walck–Lyons [9] already explicitly consider the preimage of the complete $(n-1)$ -body marginal map and competitors that may be mixed. For qubits, GHZ nonuniqueness among arbitrary states is therefore prior work, not a new consequence of the word “fiber.” Their 2008 result concerns pure competitors [8]. The calculation below parameterizes the entire equal-amplitude q -level mixed-state fiber and supports simultaneous evaluations of its one-shot quantities. It does not assert a classification of all locally undetermined qudit states. The link between nonunique preimages and quantum codes also predates this calculation [10].

Lemma 7.1 (Intersection of lifted repetition supports). *For $A_k = [n] \setminus \{k\}$, let $\tilde{\mathcal{S}}_k$ be the lift to $\mathcal{H}$ of $\text{span}\{|j\rangle^{\otimes (n-1)} : 0 \leq j < q\}$ on A_k . Then*

$$\bigcap_{k=1}^n \tilde{\mathcal{S}}_k = \mathcal{R} := \text{span}\{|j\rangle^{\otimes n} : 0 \leq j < q\}. \quad (35)$$

Proof. The lifted support projectors are diagonal in the computational basis. Their intersection is spanned by strings whose symbols outside each position k are all equal. For two positions $r \neq s$, choose $k \notin \{r, s\}$, possible because $n \geq 3$. The constraint for A_k implies $x_r = x_s$. All symbols are therefore equal, and the converse is immediate. $\square$

Theorem 7.2 (Complete equal-amplitude repetition fiber). *For the marginal data (33) and access family (34),*

$$\mathcal{F}_m = \{VCV^\dagger : C \in \mathcal{D}(\mathbb{C}^q), C_{jj} = 1/q \text{ for every } j\}. \quad (36)$$

This fiber has affine dimension $q^2 - q$.

Proof. Lemma 4.1 and Lemma 7.1 put every compatible state in $\mathcal{R} = V\mathbb{C}^q$. Hence it has a unique representation $VCV^\dagger$ with $C \in \mathcal{D}(\mathbb{C}^q)$. Tracing out any site gives

$$\mathrm{Tr}_k(VCV^\dagger) = \sum_j C_{jj} |j^{\otimes(n-1)}\rangle\langle j^{\otimes(n-1)}|, \quad (37)$$

because $\langle \ell | j \rangle = \delta_{j\ell}$ on the removed factor. The prescribed marginal is equivalent to $C_{jj} = 1/q$. Conversely these diagonal constraints give all required marginals. A Hermitian $q \times q$ matrix has q^2 real parameters; fixing its q diagonal entries leaves $q^2 - q$. Since I/q is positive definite on $\mathbb{C}^q$, the positivity constraint does not further reduce this affine dimension. $\square$

Example 7.3 (Qubit GHZ disk). For $q = 2$ the fiber is

$$\rho_z = V \begin{pmatrix} 1/2 & z \\ \bar{z} & 1/2 \end{pmatrix} V^\dagger, \quad |z| \leq 1/2. \quad (38)$$

It is a two-dimensional disk. At $z = e^{i\theta}/2$, the state is the projector onto $(|0\rangle^{\otimes n} + e^{-i\theta}|1\rangle^{\otimes n})/\sqrt{2}$. Antipodal boundary points are orthogonal. This is an explicit coordinate description of the known qubit GHZ preimage, not a claim of a new qubit nonuniqueness phenomenon.

7.3 Exact one-shot quantities in the uniform case

Theorem 7.4 (Uniform repetition evaluation). *For the fiber in Theorem 7.2,*

$$D = 1, \quad N_\perp = q, \quad C_{\mathrm{cl}} = \log_2 q, \quad K_{\mathrm{coh}} = 1, \quad C_{\mathrm{coh}} = 0. \quad (39)$$

Proof. The q Fourier-phase states are orthonormal and in the fiber, so $D = 1$ and $N_\perp \geq q$. All states are supported on the q -dimensional space $\mathcal{R}$, giving $N_\perp \leq q$.

For a direct fiber-specific proof of the coherent claim, identify $\mathcal{R}$ with $\mathbb{C}^q$. If every unit vector of a K -dimensional subspace L has coordinate probabilities $1/q$, then polarization gives, with P_L its projector,

$$P_L |j\rangle\langle j| P_L = \frac{1}{q} P_L \quad \text{for each } j. \quad (40)$$

The left side has rank at most one, whereas the right side has rank K . Thus $K \leq 1$, and a Fourier vector attains one. This agrees with the more general no-cloning obstruction of Proposition 6.5. $\square$

Remark 7.5 (Equal basis marginals do not define a quantum code). The Fourier-phase states form a perfectly hidden classical alphabet, but their span contains the repetition-basis states with nonuniform proper marginals. The off-diagonal conditions of Theorem 6.2 fail. This distinction is consistent with known masking and secret-sharing restrictions [13, 11]; the contribution here is the explicit whole-fiber description and simultaneous evaluation, not the existence of a classical-quantum distinction.

7.4 Nonuniform repetition fibers and their exact diameter

Let $p = (p_0, \dots, p_{q-1})$ be any probability vector, $J = \{j : p_j > 0\}$, $r = |J|$, and $a = \max_j p_j$. Prescribe

$$m_A(p) = \sum_j p_j |j^{\otimes|A|}\rangle\langle j^{\otimes|A|}| \quad (A \in \mathcal{A}^{(n-1)}). \quad (41)$$

These are the proper marginals of $\sum_j \sqrt{p_j} e^{i\theta_j} |j\rangle^{\otimes n}$. They need not have equal amplitudes.

Theorem 7.6 (Complete nonuniform repetition fiber). *For (41),*

$$\mathcal{F}_p = \{VCV^\dagger : C \in \mathcal{D}(\mathbb{C}^q), \text{ diag } C = p\}, \quad \dim \text{aff } \mathcal{F}_p = r^2 - r, \quad K_{\mathrm{coh}}(\mathcal{F}_p) = 1. \quad (42)$$

Proof. The same support intersection argument as in Lemma 7.1, now with labels restricted to J , gives $\text{supp } \rho \subseteq \text{span}\{|j\rangle^{\otimes n} : j \in J\}$. Equation (37) then proves the characterization. Conversely, for a positive semidefinite C with $C_{jj} = p_j$, the inequality $|C_{j\ell}|^2 \leq C_{jj}C_{\ell\ell}$ makes every row and column outside J zero. On the r -dimensional active space, the fixed diagonal imposes r independent real constraints, and $\text{diag}(p|_J)$ is positive definite. The affine dimension is therefore $r^2 - r$, including $r = 1$.

Every phase vector with moduli $\sqrt{p_j}$ gives a pure state in the fiber. For any coherent subspace L and any $j \in J$, polarization gives $P_L|j\rangle\langle j|P_L = p_j P_L$. Since $p_j > 0$, the rank argument in (40) implies $\dim L \leq 1$. Hence $K_{\text{coh}} = 1$. $\square$

Lemma 7.7 (Minimum resultant of prescribed lengths). *For nonnegative p_j summing to one,*

$$\min_{\theta_0, \dots, \theta_{q-1}} \left| \sum_j p_j e^{i\theta_j} \right| = \max\{0, 2a - 1\}, \quad a = \max_j p_j. \quad (43)$$

Proof. For arbitrary lengths with total S and largest length b , the attainable resultant magnitudes form the interval $[\max\{0, 2b - S\}, S]$. Here is an elementary induction. For one length the assertion is immediate. If the previous resultant ranges over $[L, S]$ and a new length c is added, then for fixed old magnitude u the new magnitudes range over $[|u - c|, u + c]$. As u and the relative angle vary continuously over a connected set, the complete range is an interval. Its maximum is $S + c$ and its minimum is the distance from c to $[L, S]$, namely $\max\{0, L - c, c - S\}$. Substituting $L = \max\{0, 2b - S\}$ yields $\max\{0, 2\max\{b, c\} - (S + c)\}$, as required. Apply the assertion with total length one. $\square$

Theorem 7.8 (Exact nonuniform diameter and packing threshold). *For the fiber in Theorem 7.6,*

$$D(\mathcal{F}_p) = \sqrt{1 - \max\{0, 2a - 1\}^2} = \begin{cases} 1, & a \leq 1/2, \\ 2\sqrt{a(1-a)}, & a > 1/2. \end{cases} \quad (44)$$

Moreover,

$$N_{\perp}(\mathcal{F}_p) \leq \left\lfloor \frac{1}{a} \right\rfloor, \quad N_{\perp}(\mathcal{F}_p) \geq 2 \iff a \leq 1/2. \quad (45)$$

In particular $N_{\perp} = 1$ for $a > 1/2$, and $N_{\perp} = 2$ for $1/3 < a \leq 1/2$.

Proof. The isometry V preserves trace distance and support orthogonality, so work with density matrices C, D of diagonal p . If $a \leq 1/2$, Lemma 7.7 produces two orthogonal pure vectors with coordinate moduli $\sqrt{p_j}$; their projectors have the required diagonal and distance one.

Suppose $1/2 < a < 1$ and choose j_* with $p_{j_*} = a$. Choose purifications of C, D on a common sufficiently large ancillary space. The ancillary vector conditional on j_* has norm $\sqrt{a}$ for each purification. An ancillary unitary on one purification can align the corresponding normalized vectors, without changing its reduced state. Thus the purifications can be written

$$|\psi\rangle = \sqrt{a}|j_*\rangle|u\rangle + \sqrt{1-a}|\xi\rangle, \quad |\phi\rangle = \sqrt{a}|j_*\rangle|u\rangle + \sqrt{1-a}|\zeta\rangle,$$

where ξ, ζ are normalized and orthogonal to $|j_*\rangle \otimes \mathcal{H}_{\text{anc}}$. Therefore

$$|\langle\psi|\phi\rangle| = |a + (1-a)\langle\xi|\zeta\rangle| \geq 2a - 1.$$

Contractivity under the ancillary partial trace and (12) give $T(C, D) \leq 2\sqrt{a(1-a)}$. The pure vectors

$$|u\rangle_p = \sum_j \sqrt{p_j}|j\rangle, \quad |v\rangle_p = \sqrt{a}|j_*\rangle - \sum_{j \neq j_*} \sqrt{p_j}|j\rangle$$

attain equality. For $a = 1$ the fiber is a singleton, so the formula still holds.

For the packing bound, let $C_1, \dots, C_N$ have pairwise orthogonal supports with projectors $P_1, \dots, P_N$. A density matrix is bounded above by its support projector. Hence

$$Np_j = \sum_{i=1}^N \langle j | C_i | j \rangle \leq \sum_{i=1}^N \langle j | P_i | j \rangle \leq 1.$$

Take a maximizing j to get $N \leq 1/a$. The equivalence in (45) follows either from the diameter formula and Theorem 4.4, or directly from the packing bound and the polygon construction. The two stated exact ranges follow immediately. $\square$

For uniform p , the packing bound is attained by the Fourier family. For other p with $a \leq 1/3$, (45) is only an upper bound unless a matching construction is given. In particular, the condition $Np_j \leq 1$ has not been proved here sufficient for an arbitrary N -state packing.

7.5 Which proper marginals force the repetition fiber?

Let $\mathcal{A}$ now be any family of nonempty proper subsets of $[n]$ with $\bigcup_{A \in \mathcal{A}} A = [n]$, and prescribe $m_A(p)$ from (41). Define the co-occurrence graph $G_{\mathcal{A}}$ on $[n]$: two different sites are adjacent when some $A \in \mathcal{A}$ contains both. Let its connected components be $B_1, \dots, B_c$.

Proposition 7.9 (Connectivity criterion). *The support-compatible space (22) is*

$$\mathcal{S}_{m(p)} = \text{span} \left\{ \bigotimes_{\ell=1}^c |j_\ell\rangle^{\otimes |B_\ell|} : j_\ell \in J \right\}, \quad \dim \mathcal{S}_{m(p)} = r^c, \quad (46)$$

where tensor factors are placed at the corresponding sites. If $G_{\mathcal{A}}$ is connected, the complete fiber is exactly (42). If $r \geq 2$, connectivity is also necessary for that equality.

Proof. All lifted support projectors are computational-basis diagonal. Membership forces each site to have a label in J , since the family covers $[n]$, and it forces equality on each region and therefore across each graph component. Conversely, strings constant on every component satisfy every support constraint. This proves (46).

For a connected graph the support is $V\mathbb{C}^J$. Every region is nonempty and proper, so its partial trace on $VCV^\dagger$ retains exactly the diagonal coefficients C_{jj} on distinct repetition strings. Thus any one prescribed region fixes these coefficients to p_j , proving the complete-fiber claim.

If $c \geq 2$ and $r \geq 2$, the state

$$\rho_{\text{comp}} = \bigotimes_{\ell=1}^c \left(\sum_{j \in J} p_j |j|^{\otimes |B_\ell|} \langle j|^{\otimes |B_\ell|} \right) \quad (47)$$

has every prescribed marginal: each region lies in one component. But it has positive weight on strings with distinct labels on different components, so it is not supported on the global repetition space. The fiber is then strictly larger than (42). $\square$

In particular, for $n \geq 3$ it suffices to fix the two-body marginals along any spanning tree. When $r = 1$, any covering family already forces the unique repetition-basis state, irrespective of connectivity. The covering and proper-region hypotheses matter: an unobserved site has unconstrained support, and including the full system fixes the entire state. For $n = 2$, singleton marginals do not force repetition support; for example, I/q^2 has uniform singleton marginals but is not supported on the q -dimensional repetition subspace.

8 Finite-Resolution Packing Geometry

Definition 8.1 (δ -packing number). For $0 < \delta \leq 1$, let $P_\delta(\mathcal{F}_m)$ be the largest cardinality of a set in the fiber whose distinct members satisfy $T(\rho_i, \rho_j) \geq \delta$. Define the logarithmic pairwise packing quantity

$$C_\delta(\mathcal{F}_m) = \log_2 P_\delta(\mathcal{F}_m). \quad (48)$$

Compactness makes every positive-separation packing finite. At $\delta = 1$, $P_1 = N_\perp$. For $\delta < 1$, pairwise separation does not by itself guarantee a single POVM that decodes all messages with a specified error probability. We therefore do not interpret C_δ as an unqualified communication capacity.

Theorem 8.2 (Dimension-based metric-entropy bound). *Let $k = \dim \text{aff } \mathcal{F}_m$ and $D = D(\mathcal{F}_m)$. For $0 < \delta \leq D$,*

$$P_\delta(\mathcal{F}_m) \leq \left(1 + \frac{2D}{\delta}\right)^k, \quad C_\delta(\mathcal{F}_m) \leq k \log_2 \left(1 + \frac{2D}{\delta}\right). \quad (49)$$

For $\delta > D$, the packing number is one, including the singleton case $D = 0$.

Proof. Restrict the norm $X \mapsto \|X\|_1/2$ to the k -dimensional translation space of the affine hull. Fix $\rho_0 \in \mathcal{F}_m$. All packing centers lie in its radius- D ball. The open radius- $\delta/2$ balls around them are disjoint and contained in the radius- $(D + \delta/2)$ ball about ρ_0 . Lebesgue volume in this normed space scales as the k th power of the radius. Thus $N(\delta/2)^k \leq (D + \delta/2)^k$. If $\delta > D$, no two distinct points can satisfy the separation condition. $\square$

Remark 8.3. This is the standard finite-dimensional volumetric packing argument, specialized to a marginal fiber. It is not a new general metric-entropy estimate. At zero error, the support and affine-simplex bounds of Theorem 5.3 can be much stronger.

9 Approximate Marginal Fibers

Definition 9.1 (Centered approximate fiber). For compatible m and $u \geq 0$, set

$$\mathcal{F}_m^{(u)} = \{\rho \in \mathcal{D}(\mathcal{H}) : \max_{A \in \mathcal{A}} \|\rho_A - m_A\|_1 \leq u\}. \quad (50)$$

Definition 9.2 (Pairwise local indistinguishability). A set $\mathcal{E} \subseteq \mathcal{D}(\mathcal{H})$ is pairwise ε -locally indistinguishable on $\mathcal{A}$ if

$$\max_{A \in \mathcal{A}} \|\rho_A - \sigma_A\|_1 \leq \varepsilon \quad \text{for all } \rho, \sigma \in \mathcal{E}. \quad (51)$$

A centered radius- u fiber is pairwise $2u$ -locally indistinguishable (and trace-norm differences never exceed two). These are different conventions: the centered radius is not automatically the pairwise separation parameter.

9.1 Continuity of the global diameter

Define

$$D_u(m) = \max_{\rho, \sigma \in \mathcal{F}_m^{(u)}} T(\rho, \sigma). \quad (52)$$

Proposition 9.3 (Zero-noise limit). *The map $u \mapsto D_u(m)$ is nondecreasing, $D_u(m) \geq D_0(m)$, and*

$$\lim_{u \downarrow 0} D_u(m) = D_0(m). \quad (53)$$

Proof. The approximate fibers are nested, so the right limit $L = \inf_{u>0} D_u(m)$ exists and is at least $D_0(m)$. Choose $u_j \downarrow 0$ and maximizing pairs (ρ_j, σ_j) . Compactness gives a convergent subsequence with limit (ρ_*, σ_*) . By continuity of partial trace and the norm, both limiting states satisfy the exact marginal constraints. The scalar sequence $D_{u_j}(m)$ already converges to L by monotonicity, so its subsequence does also. Continuity of trace distance yields $L = T(\rho_*, \sigma_*) \leq D_0(m)$, proving equality. $\square$

This is a qualitative zero-noise limit, not a uniform quantitative modulus over all compatible marginal data.

10 Sharp Binary Leakage Versus Global Distinguishability

Let ρ, σ be equiprobable codewords with $\|\rho_A - \sigma_A\|_1 \leq \varepsilon$ for every $A \in \mathcal{A}$, where $0 \leq \varepsilon \leq 2$. Define

$$P_{\text{succ}}^{\mathcal{A}}(\rho, \sigma) = \max_{A \in \mathcal{A}} P_{\text{succ}}(\rho_A, \sigma_A). \quad (54)$$

Theorem 10.1 (Binary leakage bound).

$$P_{\text{succ}}^{\mathcal{A}}(\rho, \sigma) \leq \frac{1}{2} + \frac{\varepsilon}{4}, \quad (55)$$

$$P_{\text{succ}}^{\text{glob}}(\rho, \sigma) = \frac{1}{2} + \frac{1}{4} \|\rho - \sigma\|_1, \quad (56)$$

$$P_{\text{succ}}^{\text{glob}} - P_{\text{succ}}^{\mathcal{A}} \geq \max \left\{ 0, \frac{\|\rho - \sigma\|_1 - \varepsilon}{4} \right\}. \quad (57)$$

Proof. Apply the Helstrom formula (11) to each allowed marginal and to the full state. Subtraction gives the displayed difference bound. Contractivity ensures the difference is also nonnegative. $\square$

Remark 10.2 (Sharpness). The coefficient $1/4$ is exactly the Helstrom coefficient, not a new discrimination inequality. The local bound is attained whenever the maximum actual local trace-norm separation is ε . Orthogonal Fourier-phase repetition states have local separation zero and global separation two.

10.1 A normalized hiding gap

For distinct states define

$$\Gamma_{\mathcal{A}}(\rho, \sigma) = T(\rho, \sigma) - \max_{A \in \mathcal{A}} T(\rho_A, \sigma_A). \quad (58)$$

Contractivity gives $\Gamma_{\mathcal{A}} \geq 0$. On an exact fiber this equals $T(\rho, \sigma)$, with maximum one for orthogonal pairs. As in the other operational quantities, this comparison concerns the specified access model only.

11 Multi-Message Leakage Bounds

For a finite message distribution $(p_x)_x$ and codewords ρ_x , set

$$\bar{\rho}_A = \sum_x p_x \rho_{x,A}, \quad \chi_A(X) = S(\bar{\rho}_A) - \sum_x p_x S(\rho_{x,A}). \quad (59)$$

The accessible information obeys $I_{\text{acc}}(X : A) \leq \chi_A(X)$ [2]. Define $f_1(t) = 0$, and for $d \geq 2$, $0 \leq t \leq 1$ set

$$f_d(t) = \begin{cases} t \log_2(d-1) + h_2(t), & 0 \leq t \leq 1 - 1/d, \\ \log_2 d, & 1 - 1/d \leq t \leq 1, \end{cases} \quad (60)$$

where $h_2(t) = -t \log_2 t - (1-t) \log_2(1-t)$, with $0 \log_2 0 = 0$. Audenaert's inequality [17] gives

$$|S(\rho) - S(\sigma)| \leq T \log_2(d-1) + h_2(T), \quad T = T(\rho, \sigma). \quad (61)$$

Its right side is not monotone over all of $[0, 1]$. The envelope (60) is monotone and satisfies

$$T(\rho, \sigma) \leq t \implies |S(\rho) - S(\sigma)| \leq f_d(t). \quad (62)$$

Theorem 11.1 (Holevo leakage of an approximately hidden ensemble). *For a fixed A , suppose*

$$\|\rho_{x,A} - \rho_{y,A}\|_1 \leq \varepsilon \quad \text{for all } x, y, \quad 0 \leq \varepsilon \leq 2. \quad (63)$$

Then, writing $d_A = \dim \mathcal{H}_A$,

$$I_{\text{acc}}(X : A) \leq \chi_A(X) \leq \sum_x p_x f_{d_A}((1-p_x)\varepsilon/2) \leq f_{d_A}(\varepsilon/2). \quad (64)$$

The right side can also be intersected with the bounds $H(X)$ and $\log_2 d_A$.

Proof. Convexity of the trace norm, with the $y = x$ term zero, gives

$$\|\rho_{x,A} - \bar{\rho}_A\|_1 \leq \sum_{y \neq x} p_y \|\rho_{x,A} - \rho_{y,A}\|_1 \leq (1-p_x)\varepsilon. \quad (65)$$

Apply (62) to each pair $(\rho_{x,A}, \bar{\rho}_A)$ and use

$$\chi_A(X) \leq \sum_x p_x |S(\bar{\rho}_A) - S(\rho_{x,A})|.$$

Monotonicity of f_{d_A} proves the last inequality. The bounds $\chi_A \leq H(X)$ and $\chi_A \leq \log_2 d_A$ are the standard ensemble entropy bounds [2]. $\square$

Remark 11.2 (Tightness and a classical–quantum trace-distance bound). Audenaert's two-state entropy-continuity inequality is sharp, but the ensemble estimate above is not claimed generally tight: convexity and absolute entropy differences can lose information. Keeping $1-p_x$ gives a distribution-sensitive refinement of the simpler bound $f_{d_A}(\varepsilon/2)$.

There is also a direct statement about the joint classical–quantum state $\omega_{XA} = \sum_x p_x |x\rangle\langle x| \otimes \rho_{x,A}$. Block diagonality and (65) give

$$T(\omega_{XA}, \omega_X \otimes \bar{\rho}_A) = \sum_x p_x T(\rho_{x,A}, \bar{\rho}_A) \leq \frac{\varepsilon}{2} \left(1 - \sum_x p_x^2\right). \quad (66)$$

This bound is stable under processing of the displayed registers. It does not add security against unmodeled correlated side information or accumulated access.

Definition 11.3 (Leakage of the declared access structure).

$$I_{\text{leak}}^A(X) = \max_{A \in \mathcal{A}} I_{\text{acc}}(X : A). \quad (67)$$

Corollary 11.4 (Access-structure Holevo bound). *Set $\varepsilon_A = \max_{x,y} \|\rho_{x,A} - \rho_{y,A}\|_1$. Then*

$$I_{\text{leak}}^A(X) \leq \max_{A \in \mathcal{A}} \min\{H(X), \log_2 d_A, f_{d_A}(\varepsilon_A/2)\}. \quad (68)$$

Proof. Apply Theorem 11.1 separately to each region. $\square$

Corollary 11.5 (Exact fiber secrecy). *If every codeword is in one exact marginal fiber, then $I_{\text{acc}}(X : A) = 0$ for every $A \in \mathcal{A}$ and $I_{\text{leak}}^A(X) = 0$.*

Proof. All ε_A vanish and $f_d(0) = 0$. $\square$

12 Observable-Algebra Access and Dynamical Projectability

Subsystem access is not the only way to specify available observables. Let $\mathcal{B} \subseteq M_d(\mathbb{C})$ be a unital $*$ -subalgebra and let

$$\mathbf{E}_{\mathcal{B}} : M_d(\mathbb{C}) \longrightarrow \mathcal{B} \quad (69)$$

be its trace-preserving Hilbert–Schmidt conditional expectation. This is the orthogonal projection onto $\mathcal{B}$ and is completely positive, unital, and trace preserving [22]. The trace is the ordinary ambient matrix trace throughout; no normalization is silently changed.

Definition 12.1 (Algebraic access equivalence and fiber). For density operators ρ, σ write

$$\rho \sim_{\mathcal{B}} \sigma \iff \text{Tr}[(\rho - \sigma)B] = 0 \text{ for every } B \in \mathcal{B}. \quad (70)$$

Equivalently, $\mathbf{E}_{\mathcal{B}}(\rho) = \mathbf{E}_{\mathcal{B}}(\sigma)$. For compatible ω , define

$$\mathcal{F}_{\omega}^{\mathcal{B}} = \{\rho \in \mathcal{D}(\mathbb{C}^d) : \mathbf{E}_{\mathcal{B}}(\rho) = \omega\}. \quad (71)$$

For $\mathcal{B} = M_{d_A}(\mathbb{C}) \otimes I_{A^c}$ the conditional expectation is

$$\mathbf{E}_{\mathcal{B}}(X) = \text{Tr}_{A^c}(X) \otimes \frac{I_{A^c}}{d_{A^c}}, \quad d_{A^c} = \dim \mathcal{H}_{A^c}. \quad (72)$$

Thus a *single-region* marginal fiber is an algebraic fiber. For several alternative regions, the marginal fiber is an intersection of such fibers. Replacing their algebras by the algebra they generate generally changes the threat model: single-site algebras together generate the full matrix algebra, although equality of single-site marginals need not determine the global state. The generated algebra models combined access, not merely a choice of one region.

Proposition 12.2 (Perfect secrecy for algebraic access). *An encoding is perfectly secret when every allowed POVM has effects in $\mathcal{B}$ if and only if its codewords lie in one algebraic fiber.*

Proof. Equality of restrictions makes $\text{Tr}(\rho_x M_y)$ independent of x for all allowed effects. Conversely every Hermitian $B \in \mathcal{B}$ is an affine rescaling of an effect in $\mathcal{B}$, so equality of all effect probabilities implies equality of all expectation values and hence of the restrictions. Any allowed preprocessing must preserve this total measurement algebra in the Heisenberg picture. $\square$

Let $H = H^\dagger$, $U_t = e^{-itH/\hbar}$, and define

$$\Phi_t(\rho) = U_t \rho U_t^\dagger, \quad \alpha_t(B) = U_t^\dagger B U_t. \quad (73)$$

Lemma 12.3 (Physical realization of hidden Hermitian directions). *If $\delta = \delta^\dagger$ and $\mathbf{E}_{\mathcal{B}}(\delta) = 0$, then $\text{Tr} \delta = 0$. If $\delta \neq 0$ and $0 < s < 1/(d\|\delta\|_\infty)$, the states*

$$\rho_{\pm} = I/d \pm s\delta \quad (74)$$

are positive definite, satisfy $\mathbf{E}_{\mathcal{B}}(\rho_+) = \mathbf{E}_{\mathcal{B}}(\rho_-) = I/d$, and obey $\rho_+ - \rho_- = 2s\delta$.

Proof. Trace preservation gives $\text{Tr} \delta = 0$. The strict operator-norm bound ensures positivity, and the remaining claims follow by linearity and unitality of $\mathbf{E}_{\mathcal{B}}$. $\square$

Theorem 12.4 (Exact autonomous accessible dynamics). *For a finite-dimensional unital $*$ -subalgebra $\mathcal{B}$, the following are equivalent:*

- (i) *For every $t \in \mathbb{R}$ there is a well-defined map Ψ_t on $\mathbf{E}_{\mathcal{B}}(\mathcal{D}(\mathbb{C}^d))$ satisfying $\mathbf{E}_{\mathcal{B}} \circ \Phi_t = \Psi_t \circ \mathbf{E}_{\mathcal{B}}$.*
- (ii) *For every $t \in \mathbb{R}$, $\rho \sim_{\mathcal{B}} \sigma$ implies $\Phi_t(\rho) \sim_{\mathcal{B}} \Phi_t(\sigma)$.*

(iii) $\alpha_t(\mathcal{B}) = \mathcal{B}$ for every $t \in \mathbb{R}$.

(iv) $\delta_H(\mathcal{B}) \subseteq \mathcal{B}$, where $\delta_H(B) = i[H, B]/\hbar$.

When these conditions hold,

$$\mathbf{E}_{\mathcal{B}}\Phi_t = \Phi_t\mathbf{E}_{\mathcal{B}}, \quad \Psi_t(\omega) = U_t\omega U_t^\dagger \quad (\omega \in \mathcal{B}). \quad (75)$$

In particular Ψ_t extends to a trace-preserving $*$ -automorphism of $\mathcal{B}$, and is completely positive with inverse Ψ_{-t} .

Proof. Conditions (i) and (ii) express the same representative-independence. For (ii) $\Rightarrow$ (iii), fix t , a Hermitian $B \in \mathcal{B}$, and a Hermitian $\delta \in \ker \mathbf{E}_{\mathcal{B}}$. By Lemma 12.3, any nonzero such δ is a scalar multiple of a difference of states in one fiber. Condition (ii) gives

$$\mathrm{Tr}[\delta\alpha_t(B)] = 0.$$

Since $\mathbf{E}_{\mathcal{B}}$ is the Hilbert–Schmidt projection, the orthogonal complement of its Hermitian kernel is the Hermitian part of $\mathcal{B}$. Thus $\alpha_t(B) \in \mathcal{B}$, and complex linearity extends this to all $B \in \mathcal{B}$. Applying the same argument at $-t$ gives equality.

Conversely, (iii) gives

$$\mathrm{Tr}[(\Phi_t(\rho) - \Phi_t(\sigma))B] = \mathrm{Tr}[(\rho - \sigma)\alpha_t(B)] = 0$$

whenever the initial restrictions coincide. Hence (ii) holds. Differentiating (iii) at zero gives (iv). Conversely, the exponential of the finite-dimensional invariant linear subspace in (iv) preserves $\mathcal{B}$ for both signs of t , giving (iii).

Finally Φ_t is a Hilbert–Schmidt unitary preserving $\mathcal{B}$. It therefore also preserves its orthogonal complement and commutes with the orthogonal projection $\mathbf{E}_{\mathcal{B}}$. This proves (75); conjugation restricted to an invariant algebra is a trace-preserving $*$ -automorphism, proving the final claims. $\square$

The general reducibility question belongs to established coarse-graining theory [21]. The theorem concerns autonomous evolution of the *complete state on the algebra*, not an arbitrary smaller collection of expectation values. For unitary microscopic dynamics and exact algebra invariance, the induced evolution is reversible, not a generic dissipative channel.

Definition 12.5 (Finite-time leakage defect). For $T > 0$ define

$$\varepsilon_T(\mathcal{B}) = \sup_{\substack{\rho, \sigma \in \mathcal{D}(\mathbb{C}^d) \\ \mathbf{E}_{\mathcal{B}}(\rho) = \mathbf{E}_{\mathcal{B}}(\sigma)}} \sup_{0 \leq t \leq T} \frac{1}{2} \|\mathbf{E}_{\mathcal{B}}(\Phi_t(\rho) - \Phi_t(\sigma))\|_1. \quad (76)$$

The maximum is attained by compactness and lies in $[0, 1]$. It vanishes precisely when the restriction is representative-independent throughout the indicated interval.

Let the Schrödinger generator and hidden real subspace be

$$\mathcal{L}(X) = -\frac{i}{\hbar}[H, X], \quad \mathcal{K}_{\mathcal{B}} = \{\delta = \delta^\dagger : \mathbf{E}_{\mathcal{B}}(\delta) = 0\}. \quad (77)$$

The trace-zero condition is automatic. For each integer $r \geq 1$ set

$$\eta_r(\mathcal{B}) = \sup_{\substack{\delta \in \mathcal{K}_{\mathcal{B}} \\ \|\delta\|_1 \leq 1}} \|\mathbf{E}_{\mathcal{B}}\mathcal{L}^r(\delta)\|_1. \quad (78)$$

This definition also gives zero if $\mathcal{K}_{\mathcal{B}} = \{0\}$. Since $\mathcal{L}$ preserves Hermiticity and $\mathbf{E}_{\mathcal{B}}$ contracts the trace norm on Hermitian operators, $\eta_r \leq \|\mathcal{L}\|_{1 \rightarrow 1}^r$. Expansion of the exponential yields

$$\|\mathbf{E}_{\mathcal{B}} e^{t\mathcal{L}} \delta\|_1 \leq \|\delta\|_1 \sum_{r=1}^{\infty} \frac{|t|^r}{r!} \eta_r(\mathcal{B}) \quad (\delta \in \mathcal{K}_{\mathcal{B}}). \quad (79)$$

The zeroth term vanishes, and the series converges at every finite time. Consequently,

$$\varepsilon_T(\mathcal{B}) \leq \min \left\{ 1, \sum_{r=1}^{\infty} \frac{T^r}{r!} \eta_r(\mathcal{B}) \right\}. \quad (80)$$

There is no missing factor of two: for $\delta = \rho - \sigma$, the prefactor $1/2$ in (76) cancels the upper bound $\|\delta\|_1 \leq 2$.

Proposition 12.6 (Uniform first-order vanishing is an exact closure test). *The condition $\eta_1(\mathcal{B}) = 0$ is equivalent to the conditions of Theorem 12.4. In this case every η_r and every ε_T vanish. Conversely, $\varepsilon_T = 0$ for any $T > 0$ implies $\eta_1 = 0$.*

Proof. If $\eta_1 = 0$, then $\mathbf{E}_{\mathcal{B}} \mathcal{L} \delta = 0$ for every hidden Hermitian δ . For Hermitian $B \in \mathcal{B}$, Hilbert–Schmidt adjointness gives

$$0 = \text{Tr}[B \mathcal{L} \delta] = \text{Tr}[\delta \delta_H(B)].$$

Orthogonality to the entire hidden space implies $\delta_H(B) \in \mathcal{B}$. This is condition (iv) of Theorem 12.4. Conversely, invariance of the algebra and its orthogonal complement implies $\mathbf{E}_{\mathcal{B}} \mathcal{L} \delta = 0$ on the hidden space. Commutation with the flow then gives all higher-order and finite-time assertions. Finally, if $\varepsilon_T = 0$, Lemma 12.3 implies $\mathbf{E}_{\mathcal{B}} \Phi_t \delta = 0$ for every hidden δ and $0 \leq t \leq T$. Differentiating at zero yields $\mathbf{E}_{\mathcal{B}} \mathcal{L} \delta = 0$ and hence $\eta_1 = 0$. $\square$

Example 12.7 (A single vanishing first derivative does not suffice). Take $d = 2$, $\mathcal{B} = \text{span}\{I, Z\}$ with Pauli matrices X, Y, Z , $H = \hbar(X + Z)/2$, and $\delta = X$. Then

$$\mathbf{E}_{\mathcal{B}} \delta = 0, \quad \mathcal{L} X = Y, \quad \mathbf{E}_{\mathcal{B}} \mathcal{L} X = 0, \quad \mathcal{L}^2 X = Z - X, \quad \mathbf{E}_{\mathcal{B}} \mathcal{L}^2 X = Z \neq 0. \quad (81)$$

This direction leaks only at higher order. However, $\eta_1 \neq 0$, since $\mathbf{E}_{\mathcal{B}} \mathcal{L} Y = Z$. Thus a *direction-specific* first-order check can miss leakage, whereas the *uniform* zero coefficient cannot. When $\eta_1 > 0$, its value alone is not a complete formula for the finite-time defect; higher-order bounds such as (80) remain useful.

13 Relation to Established Frameworks and Priority

Fixed marginals and their geometry. Parthasarathy and Rudolph studied extremal states with prescribed marginals [3, 4]; compatibility and spectral aspects belong to the broader quantum marginal problem [5, 6]. Compact convex fixed-marginal sets, their affine-kernel descriptions, and the word “preimage” are not new objects.

GHZ nonuniqueness and quantum codes. Linden, Popescu, and Wootters showed that almost every pure three-qubit state is determined by its two-party reductions [7]. Walck–Lyons established the exceptional GHZ role among pure qubit states, first with pure competitors and then with arbitrary pure-or-mixed competitors [8, 9]. Their preimage formulation and the existence of mixed GHZ competitors directly precede the present work. Ocko et al. connect nonunique marginal preimages, locally indistinguishable degenerate subspaces, and quantum error correction [10]. Our repetition calculation is not a replacement for these classifications or constructions.

Secret sharing, private subspaces, and masking. The cross-term criterion is an erasure-correction condition of Knill–Laflamme type [18] and is central to quantum secret sharing and private codes [11, 12, 19]. The no-cloning argument already forbids a nontrivial pure code hidden from all $(n - 1)$ -party regions. Thus $K_{\text{coh}} = 1$ in a repetition fiber containing pure states is structurally expected. The no-masking theorem [13] is related context, not the sole theorem used to justify a general multipartite obstruction. Private subsystems and mixed-state schemes are not exhausted by our subspace invariant.

Data hiding and observable algebras. LOCC data hiding [14, 15] restricts joint measurements rather than denying physical access to a complement. The models require explicit comparison, not interchangeable terminology. Observable-algebra reductions and dynamical reducibility are established [21, 22]. Section 12 specializes these ideas and distinguishes a uniform first-order closure test from a check along one perturbation.

13.1 Precise contribution statement

The mathematical content emphasized here is the complete q -level repetition mixed-state fiber, including nonuniform probabilities and zero entries; its exact trace-distance diameter and coherent-subspace dimension; a nonuniform orthogonal-packing bound with an exact two-state threshold; the exact uniform packing; and the connectivity characterization for covering families of proper regions. These are proved explicitly in Section 7. The surrounding diameter, packing, leakage, and algebraic framework provides their one-shot interpretation.

We make no claim that classical and coherent hiding were previously conflated in the literature, that GHZ marginal nonuniqueness is new, or that the no-cloning obstruction is new. Neither failure to locate an identical combined formulation nor a different choice of terminology establishes historical priority. The extent of overlap of the explicit quantitative refinements with the broader literature remains a matter for specialist assessment.

14 Open Problems

Beyond repetition fibers, exact evaluation of $D(\mathcal{F}_m)$ and $N_{\perp}(\mathcal{F}_m)$ remains of interest. Even within the nonuniform family, the upper bound $\lfloor 1/\max_j p_j \rfloor$ does not here determine all higher packing numbers. It is useful to characterize when this bound is attained, without assuming that coordinatewise necessary conditions suffice.

Other questions include approximate coherent-subspace hiding with an explicit reference system; operational decoding guarantees beyond pairwise metric packing; semidefinite or symmetry-reduced bounds on packing; and quantitative estimates of dynamical leakage for local Hamiltonians. Any claim about propagation in extended local systems should be compared with Lieb–Robinson theory [20], rather than inferred from the finite-dimensional power-series bound alone. Mixed-state private encodings require a separate invariant and should not be treated as solved by K_{coh} .

15 Conclusion

A specified access family determines a marginal map, and its fibers are exactly the classes of states indistinguishable under that access. Orthogonal packing describes perfectly recoverable classical alphabets; coherent subspace hiding imposes the stronger requirement that an entire density-operator state space remain in one fiber. The cross-term conditions connect this distinction to established erasure-correction and secret-sharing theory.

For repetition data, the complete compatible mixed-state fiber is a fixed-diagonal density-matrix spectrahedron. With $r = |\text{supp } p|$ and $a = \max_j p_j$, we obtained

$$\dim \text{aff } \mathcal{F}_p = r^2 - r, \quad D(\mathcal{F}_p) = \sqrt{1 - \max\{0, 2a - 1\}^2}, \quad N_\perp(\mathcal{F}_p) \leq \lfloor 1/a \rfloor, \quad K_{\text{coh}} = 1. \quad (82)$$

The uniform case attains $N_\perp = q$ and hence $C_{\text{cl}} = \log_2 q$, while $C_{\text{coh}} = 0$. A connected co-occurrence graph of covering proper regions already forces this same complete fiber, so all $(n - 1)$ -party marginals are sufficient but not necessary.

Approximate secrecy is controlled by the Helstrom formula, a monotone entropy-continuity envelope, and the classical–quantum trace-distance estimate (66). Algebraic access gives a precise dynamical closure criterion. Uniform vanishing of the first-order leakage coefficient is already an exact invariance test, whereas a first-order test on only one direction is not. These conclusions are finite-dimensional cryptographic and quantum-informational statements, not assertions about emergent microscopic or gravitational models.

Preparation note. Generative-AI assistance was used during revision for exposition, candidate proof development, reference checking, and preparation of executable consistency tests. Such assistance is not independent peer review.

References

- [1] J. Hrubý, “Secrecy Without Computation: Geometry as a Cryptographic Primitive,” Rump Session presentation, EUROCRYPT 2026, Rome, Italy (2026).
- [2] J. Watrous, *The Theory of Quantum Information*. Cambridge University Press (2018). DOI: 10.1017/9781316848142.
- [3] K. R. Parthasarathy, “Extremal quantum states in coupled systems,” *Ann. Inst. H. Poincaré Probab. Statist.* **41**, 257–268 (2005). DOI: 10.1016/j.anihpb.2003.10.009.
- [4] O. Rudolph, “On extremal quantum states of composite systems with fixed marginals,” *J. Math. Phys.* **45**, 4035–4041 (2004). DOI: 10.1063/1.1776642.
- [5] P. Butterley, A. Sudbery, and J. Szulc, “Compatibility of subsystem states,” *Found. Phys.* **36**, 83–101 (2006). DOI: 10.1007/s10701-005-9006-z. arXiv:quant-ph/0407227.
- [6] A. A. Klyachko, “Quantum marginal problem and N -representability,” *J. Phys.: Conf. Ser.* **36**, 72–86 (2006).
- [7] N. Linden, S. Popescu, and W. K. Wootters, “Almost every pure state of three qubits is completely determined by its two-particle reduced density matrices,” *Phys. Rev. Lett.* **89**, 207901 (2002). DOI: 10.1103/PhysRevLett.89.207901.
- [8] S. N. Walck and D. W. Lyons, “Only n -qubit Greenberger–Horne–Zeilinger states are undetermined by their reduced density matrices,” *Phys. Rev. Lett.* **100**, 050501 (2008). DOI: 10.1103/PhysRevLett.100.050501.
- [9] S. N. Walck and D. W. Lyons, “Only n -qubit Greenberger–Horne–Zeilinger states contain n -partite information,” *Phys. Rev. A* **79**, 032326 (2009). DOI: 10.1103/PhysRevA.79.032326. Preprint arXiv:0808.0859 appeared under the title “The Parts Determine the Whole except for n -Qubit Greenberger–Horne–Zeilinger States.”

- [10] S. A. Ocko, X. Chen, B. Zeng, B. Yoshida, Z. Ji, M. B. Ruskai, and I. L. Chuang, “Quantum codes give counterexamples to the unique preimage conjecture of the N -representability problem,” *Phys. Rev. Lett.* **106**, 110501 (2011). DOI: 10.1103/PhysRevLett.106.110501. arXiv:1010.2717.
- [11] R. Cleve, D. Gottesman, and H.-K. Lo, “How to share a quantum secret,” *Phys. Rev. Lett.* **83**, 648–651 (1999). DOI: 10.1103/PhysRevLett.83.648.
- [12] D. Gottesman, “Theory of quantum secret sharing,” *Phys. Rev. A* **61**, 042311 (2000). DOI: 10.1103/PhysRevA.61.042311.
- [13] K. Modi, A. K. Pati, A. Sen(De), and U. Sen, “Masking quantum information is impossible,” *Phys. Rev. Lett.* **120**, 230501 (2018). DOI: 10.1103/PhysRevLett.120.230501.
- [14] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, “Hiding bits in Bell states,” *Phys. Rev. Lett.* **86**, 5807–5810 (2001). DOI: 10.1103/PhysRevLett.86.5807.
- [15] T. Eggeling and R. F. Werner, “Hiding classical data in multipartite quantum states,” *Phys. Rev. Lett.* **89**, 097905 (2002). DOI: 10.1103/PhysRevLett.89.097905.
- [16] C. W. Helstrom, “Quantum detection and estimation theory,” *J. Stat. Phys.* **1**, 231–252 (1969). DOI: 10.1007/BF01007479.
- [17] K. M. R. Audenaert, “A sharp continuity estimate for the von Neumann entropy,” *J. Phys. A: Math. Theor.* **40**, 8127–8136 (2007). DOI: 10.1088/1751-8113/40/28/S18.
- [18] E. Knill and R. Laflamme, “Theory of quantum error-correcting codes,” *Phys. Rev. A* **55**, 900–911 (1997). DOI: 10.1103/PhysRevA.55.900. arXiv:quant-ph/9604034.
- [19] T. Jochym-O’Connor, D. W. Kribs, R. Laflamme, and S. Plosker, “Quantum subsystems: Exploring the complementarity of quantum privacy and error correction,” *Phys. Rev. A* **90**, 032305 (2014). DOI: 10.1103/PhysRevA.90.032305.
- [20] S. Bravyi, M. B. Hastings, and F. Verstraete, “Lieb–Robinson bounds and the generation of correlations and topological quantum order,” *Phys. Rev. Lett.* **97**, 050401 (2006). DOI: 10.1103/PhysRevLett.97.050401.
- [21] O. Kabernik, “Quantum coarse graining, symmetries, and reducibility of dynamics,” *Phys. Rev. A* **97**, 052130 (2018). DOI: 10.1103/PhysRevA.97.052130.
- [22] O. Kabernik, J. Pollack, and A. Singh, “Quantum state reduction: Generalized bipartitions from algebras of observables,” *Phys. Rev. A* **101**, 032303 (2020). DOI: 10.1103/PhysRevA.101.032303.