Universal entanglement embezzlement with inverse-quadratic logarithmic infidelity

Dev D. Goyal

27 October 2026; revised 1 November 2026

Abstract

Entanglement embezzlement extracts an approximate target state while returning a shared catalyst approximately unchanged. The harmonic family of van Dam and Hayden [1] gives root fidelity $1 - O(1/\log n)$ in local dimension n, and Leung and Wang [2] leave open whether a universal family can achieve the faster rate $1 - O(1/(\log n)^2)$ known for target-dependent constructions. We construct one family of catalysts that works for every finite target Schmidt probability vector. For each integer $L \geq 1$, the catalyst has local dimension $n_L = 2^{4L}$, and a basis permutation on each party gives global root fidelity at least $1 - 125m/L^2$ for every target vector on m entries. Thus the root infidelity is at most $2000m/(\log_2 n_L)^2$. The catalyst depends on neither the target nor m. Its Schmidt amplitudes combine the harmonic profile with a tent function of the dyadic rank. A finite interval coupling bounds the squared amplitude error, and a doubly stochastic completion then gives a local permutation with the required error. This construction addresses the general-family rate question of Leung and Wang. The dependence on m and the leading constant are not claimed to be optimal. A companion Lean formalization proves the coefficient bound and its interpretation on finite complex Hilbert spaces with separate local basis permutations; the change from an arbitrary bipartite basis to Schmidt form is not formalized.

1 Problem, conventions, and statement

An embezzling catalyst is an entangled resource from which two parties can approximately extract a desired entangled state while returning the resource approximately unchanged. The approximation here is global: it compares the entire output with the tensor product of the original catalyst and the target. The operations use no communication. Catalysis in quantum information theory more broadly is reviewed in [11].

The quantity used is *root fidelity*, $F(\psi, \phi) = |\langle \psi, \phi \rangle|$ for unit pure states. This convention is essential. It differs from the squared fidelity $|\langle \psi, \phi \rangle|^2$ and from trace distance between reduced states. The harmonic family of van Dam and Hayden gives a universal root-fidelity estimate of order $1 - O(1/\log n)$ for a fixed target [1]. A target-dependent construction with the faster rate $1 - O(1/(\log n)^2)$ was already known; Leung and Wang explicitly distinguish it from a universal family and leave the universal rate question open in their Section 6 [2, 3].

For $1 \leq i \leq n_L = 2^{4L}$, define

$$r(i) = \lfloor \log_2 i \rfloor, \qquad b_L(i) = \min\{r(i),\, 4L - r(i)\}, \tag{1}$$

$$a_L(i) = \frac{b_L(i)}{\sqrt{i}}, \qquad Z_L = \sum_{i=1}^{n_L} \frac{b_L(i)^2}{i}, \qquad c_L(i) = \frac{a_L(i)}{\sqrt{Z_L}}. \tag{2}$$

The catalyst is

$$|C_L\rangle = \sum_{i=1}^{n_L} c_L(i) |i\rangle_A |i\rangle_B.$$

The number n_L denotes the local dimension, or a Schmidt-rank upper bound. The coefficients at the two endpoints vanish. The coefficients are not assumed to be in decreasing order; the argument

allows arbitrary basis permutations. This is a nonregular family in the terminology of [2], because the unnormalized envelope depends on L.

Theorem 1 (Universal quantitative embezzlement)**.** *Let $L \geq 1$, let J be a nonempty finite set with $|J| = m$, choose $j_0 \in J$, and let $p_j \geq 0$ satisfy $\sum_{j\in J} p_j = 1$. Put*

$$|\phi_p\rangle = \sum_{j\in J} \sqrt{p_j}|j\rangle_A|j\rangle_B.$$

There is a permutation σ of $J \times \{1, \ldots, n_L\}$ such that the corresponding separate local basis permutations satisfy

$$|\langle (P_\sigma \otimes P_\sigma)(|j_0 j_0\rangle \otimes |C_L\rangle),\ |\phi_p\rangle \otimes |C_L\rangle\rangle| \geq 1 - \frac{125m}{L^2} = 1 - \frac{2000m}{(\log_2 n_L)^2}. \tag{3}$$

Both states in the comparison have norm one. The family $|C_L\rangle$ depends on neither J nor p.

The register ordering in (3) places the target index before the catalyst index on each party. The theorem is stated for arbitrary Schmidt probability vectors, including zeros. This is the finite coefficient formulation used in the embezzlement literature. The formal operational theorem uses complex-linear isometric equivalences on these finite Hilbert spaces. It proves that the bipartite map is the product of the two local basis permutations.

For each fixed m and every $\varepsilon > 0$, the bound holds with $F \geq 1 - \varepsilon$ for all sufficiently large L, uniformly over p. The finite bound and this quantified consequence are formalized. No efficiency claim is made for preparing the state or implementing a permutation in a local gate model.

The contribution is a target-independent catalyst family with an explicit inverse-quadratic logarithmic bound, obtained from a tent envelope of the dyadic rank, a finite interval coupling and Birkhoff rounding. The harmonic profile and the rounding principle are known; Section 7 compares the construction with earlier ones and states its limits. The finite bound, its logarithmic form, the uniform threshold and the operational statement with separate local basis permutations are proved in Lean 4 (Section 6).

2 Dyadic estimates

The envelope has three required properties. Write $T_K(i) = \min\{\lfloor \log_2 i \rfloor, (K - \lfloor \log_2 i \rfloor)_+\}$ for every positive integer i, where $x_+ = \max\{x, 0\}$. On $1 \leq i \leq 2^K$, the positive-part operation is redundant. Lean uses natural-number subtraction, which implements this truncation.

Lemma 2 (Envelope bounds)**.** *For positive integers $k \leq i \leq 2^K$, if $i \leq 2^D k$, then*

$$|T_K(i) - T_K(k)| \leq D.$$

If $k \geq 1$ and $2^K \leq 2^D k$, then $T_K(k) \leq D$. Also $0 \leq T_K(k) \leq k$.

Proof. Put $r_k = \lfloor \log_2 k \rfloor$. Since $k < 2^{r_k+1}$, the first scaling inequality gives $i < 2^{D+r_k+1}$, hence $\lfloor \log_2 i \rfloor \leq D + r_k$. Monotonicity gives the reverse ordering of the two logarithms. The map $r \mapsto \min\{r, K - r\}$ is 1-Lipschitz on $[0, K]$, which proves the first assertion. Applying the same logarithmic inequality to $2^K \leq 2^D k$ gives $K \leq D + r_k$, so $(K - r_k)_+ \leq D$, proving the tail assertion. Finally $T_K(k) \leq \lfloor \log_2 k \rfloor \leq k$. □

Lemma 3 (Normalization and harmonic mass)**.** *For $L \geq 1$,*

$$Z_L \geq L^3 > 0, \qquad H_{n_L} := \sum_{i=1}^{n_L} \frac{1}{i} \leq 4L + 1 \leq 5L.$$

Proof. Each dyadic shell $2^r \leq i < 2^{r+1}$ has 2^r terms. Its harmonic mass is between $1/2$ and 1. The $2L$ shells with $L \leq r < 3L$ have $b_L(i) \geq L$. Their contribution to Z_L is therefore at least $2L \cdot L^2/2 = L^3$. The $4L$ shells between 1 and $n_L - 1$, together with the last term $1/n_L$, give $H_{n_L} \leq 4L + 1$. □

3 A finite coupling and its local error

Fix L and abbreviate $n = n_L$, $a_i = a_L(i)$, $b_i = b_L(i)$, and $Z = Z_L$. For $1 \le i, k \le n$ and $j \in J$, define the nonnegative weight

$$W_{i,(j,k)} = \mathrm{length}([p_j(i-1), p_j i] \cap [k-1, k]). \tag{4}$$

Only lengths of intervals are involved. The Lean definition uses the algebraic clipping function

$$s(x,y) = \max\{0, \min\{1, x-y\}\}, \qquad W_{i,(j,k)} = s(p_j i, k-1) - s(p_j(i-1), k-1).$$

Thus neither integration nor an approximation by a continuum is used in the proof.

Lemma 4 (Mass and support)**.** *The weights satisfy*

$$\sum_{j,k} W_{i,(j,k)} = 1, \qquad q_{jk} := \sum_i W_{i,(j,k)} = s(p_j n, k-1) \in [0,1].$$

If $W_{i,(j,k)} > 0$, then $p_j > 0$, $k \le i$, $|k - p_j i| \le 1$, and

$$i \le (1 + 1/p_j)k.$$

If $q_{jk} < 1$, then $p_j n < k$.

Proof. Since $0 \le p_j \le 1$, the interval $[p_j(i-1), p_j i]$ lies in $[0, n]$. Summing its intersections with the unit intervals gives p_j; summing over j gives the row mass one. Summing over i instead joins the intervals into $[0, p_j n]$, giving the stated column mass.

A positive intersection implies $k - 1 < p_j i$ and $p_j(i-1) < k$. These imply $k \le i$ by integrality, and $-p_j < k - p_j i < 1$, giving the distance bound. They also give $i < k/p_j + 1 \le (1 + 1/p_j)k$. A zero probability has zero interval length and cannot occur in this case. Finally, a column is full whenever $p_j n \ge k$, which proves the last statement. □

Lemma 5 (Square-root scaling error)**.** *Let $I, K > 0$, $p \ge 0$, $0 \le w \le K$, and $|K - pI| \le 1$. Then*

$$\left| \frac{w}{\sqrt{I}} - \frac{\sqrt{p}\, w}{\sqrt{K}} \right| \le \frac{1}{\sqrt{I}}.$$

Consequently, if $|u - w| \le D$, then

$$\left(\frac{u}{\sqrt{I}} - \frac{\sqrt{p}\, w}{\sqrt{K}} \right)^2 \le \frac{(D+1)^2}{I}. \tag{5}$$

Proof. The difference-of-squares identity gives

$$|\sqrt{K} - \sqrt{p}\sqrt{I}|\, \sqrt{K} \le |\sqrt{K} - \sqrt{p}\sqrt{I}|\, (\sqrt{K} + \sqrt{p}\sqrt{I}) = |K - pI| \le 1.$$

Since $w \le K$, division by $\sqrt{I}\sqrt{K}$ gives the first inequality. For the second, insert $w/\sqrt{I}$ between the two terms and use the triangle inequality, obtaining an absolute-value bound $(D+1)/\sqrt{I}$. The hypothesis itself implies $D \ge 0$, so squaring is legitimate. □

For every j with $p_j > 0$, choose an integer $D_j \ge 0$ such that

$$1 + 1/p_j \le 2^{D_j}. \tag{6}$$

For $p_j = 0$, set $D_j = 0$. Lemmas 2–5 show that a positive coupling entry satisfies

$$(a_i - \sqrt{p_j} a_k)^2 \le \frac{(D_j + 1)^2}{i}. \tag{7}$$

Indeed, the two tent values differ by at most D_j, and the smaller-rank tent value is at most k. The probability-zero case contributes no active weight. If $q_{jk} < 1$ and $p_j > 0$, then $n < k/p_j \le 2^{D_j} k$, so the tail part of Lemma 2 gives $b_k \le D_j$. Therefore

$$(\sqrt{p_j} a_k)^2 \le \frac{p_j D_j^2}{k} \quad (q_{jk} < 1). \tag{8}$$

For $p_j = 0$, both sides vanish.

4 From the coupling to a permutation

Assume first that $m \geq 2$. Index both full vectors by $J \times \{1, \ldots, n\}$ and put

$$A_{(j,i)} = \begin{cases} a_i & j = j_0, \\ 0 & j \neq j_0, \end{cases} \qquad B_{(j,k)} = \sqrt{p_j} a_k.$$

They have the same squared norm Z. The n designated input rows of a square matrix are filled with W. Fill each of the remaining $n(m-1)$ rows at column (j,k) with

$$\frac{1 - q_{jk}}{n(m-1)}.$$

The result is a doubly stochastic matrix M: the total column deficit is $nm - n$, and each column deficit is filled exactly. Its averaged squared error is

$$\begin{aligned} E_M &= \sum_{i,j,k} W_{i,(j,k)} (a_i - \sqrt{p_j} a_k)^2 + \sum_{j,k} (1 - q_{jk}) p_j a_k^2 && (9) \\ &\leq H_n \sum_j p_j (D_j + 1)^2 + H_n \sum_j p_j D_j^2 && (10) \\ &\leq 2 H_n \sum_j p_j (D_j + 1)^2. && (11) \end{aligned}$$

In the first sum, the sum over k of a branch's row weights is p_j. In the second, full columns contribute zero and every deficit is at most one, so (8) applies.

Birkhoff's theorem writes M as a convex combination of permutation matrices. Since squared-error cost is linear in M, some permutation σ satisfies

$$\sum_r (A_r - B_{\sigma(r)})^2 \leq E_M. \tag{12}$$

This rounding principle is known; in the embezzlement setting, the doubly stochastic fidelity optimization is explicit in Lasecki's thesis [5]. The companion formalization uses Mathlib's proved Birkhoff theorem and proves the required cost consequence.

For any two real vectors of squared norm Z,

$$\sum_r (A_r - B_{\sigma(r)})^2 = 2Z - 2 \sum_r A_r B_{\sigma(r)}.$$

Combining this identity with (11)–(12) gives the normalized overlap bound

$$\sum_r \frac{A_r B_{\sigma(r)}}{Z} \geq 1 - \frac{H_n}{Z} \sum_j p_j (D_j + 1)^2. \tag{13}$$

The same permutation on both local indices maps the input diagonal bipartite state to a diagonal state whose inner product with the target equals this overlap. Taking its absolute value can only increase the lower bound. When $m = 1$, the target coefficient is one and the identity permutation gives exact overlap one, so no completion with a zero denominator is needed.

5 A uniform bound over all target probabilities

Lemma 6 (Uniform dyadic shifts)**.** *For every $0 < p \leq 1$, there is a natural number D such that*

$$1 + 1/p \leq 2^D, \qquad p(D+1)^2 \leq 25.$$

Proof. Set $K = \lceil 1/\sqrt{p} \rceil$ and $D = K + 2$. Then $1/p \le K^2$. For every natural number K, $K^2 + 1 \le 2^{K+2}$: check $K = 0, 1, 2$, and for $K \ge 2$ use $(K+1)^2 + 1 \le 2(K^2+1)$ to propagate the inequality. Thus the first assertion holds. Also $K < 1/\sqrt{p} + 1$ and $\sqrt{p} \le 1$, so

$$\sqrt{p}(D+1) = \sqrt{p}(K+3) \le 1 + 4\sqrt{p} \le 5.$$

Squaring proves the second assertion. □

Apply this lemma to positive probabilities and use $D_j = 0$ for zero probabilities. Then

$$\sum_j p_j (D_j + 1)^2 \le 25m.$$

Lemma 3 gives $H_n/Z \le 5/L^2$. Substituting these two bounds into (13) proves Theorem 1. Since $\log_2(2^{4L}) = 4L$, its logarithmic form follows exactly, not merely asymptotically.

6 Formal verification and reproduction

The companion project pins Lean 4.19.0 and the Mathlib commit

`c44e0c8ee63ca166450922a373c7409c5d26b00b`.

Its main exported declarations are:

- `Embezzlement.catalyst_normalized`: the stated coefficients have squared norm one.
- `Embezzlement.universal_tent_overlap`: the finite universal overlap bound, including a one-element target index set and zero target probabilities.
- `Embezzlement.universal_tent_local_unitary`: the same result for explicit unit vectors in complex Euclidean space and separate local basis permutations.
- `Embezzlement.universal_tent_logarithmic_fidelity`: the exact logarithmic-dimension bound.
- `Embezzlement.universal_tent_epsilon_threshold`: a threshold uniform over all target probability vectors on a fixed finite index set.

The formalization uses the proved Birkhoff theorem from Mathlib. The README identifies the pinned sources and gives the commands to rebuild the results and to check their axiom dependencies with `Audit.lean`.

The operational model uses a finite complex Hilbert space in the displayed Schmidt basis. It includes norm preservation and the two separate local maps. A change from an arbitrary bipartite basis to Schmidt form is not part of this formalization.

7 Relation to previous results and limits

The construction gives a target-independent catalyst with global root infidelity $O((\log n)^{-2})$. The bound is uniform over target probability vectors of a fixed finite dimension. Leung and Wang ask whether a regular or general universal family can achieve this rate [2]. Here the coefficient envelope depends on L, so the result concerns the general-family question.

The harmonic family of van Dam and Hayden gives the inverse-logarithmic root-fidelity guarantee [1]. Their statement about reduced-state trace distance uses a different error measure. It does not exclude an improved global root-infidelity bound. The earlier sine-weight construction achieves the quadratic rate for a chosen target [3]. Leung and Wang show that this construction need not embezzle other two-qubit targets with vanishing error [2]. In the present construction, the catalyst is independent of the target. The amplitudes also retain the factor $1/\sqrt{i}$ within each dyadic block.

Zanoni, Theurer, and Gour characterize universal embezzling families under local operations and classical communication [4]. Their results include regular families and concern qualitative convergence. The present theorem gives an explicit finite bound using local basis permutations. George and Chitambar study finite conversion fidelities and target-dependent optimization [6]. Multipartite, Gaussian, and hydrodynamic constructions address further settings [7, 8, 9]. Logarithmic-scale smoothing also occurs in correlated state preparation. Song uses raised-cosine labels for a resource that depends on a finite family of targets [10]. The theorem here requires one catalyst family and compares the output with the returned catalyst tensored with the target.

The constant $125m$ is a sufficient bound. The argument does not optimize that constant or its dependence on m. The proved dimension sequence is $n_L = 16^L$. The formal statement does not separately cover each intervening integer dimension. The guarantee concerns one approximate extraction and the entire output state. It does not give exact catalyst return or an unlimited sequence of extractions. The local permutation depends on the target, although the catalyst does not. State preparation and the number of local gates are separate questions.

8 Research process and AI disclosure

This work is fully autonomous agentic research. As recorded for this result, the initial research and proofs were generated autonomously by GPT 6 with Pro Reasoning in ChatGPT, and GPT 6 Astra in Codex autonomously produced the formalizations and corrections. The author checked the proofs to the best of their mathematical abilities; this check is not expert validation or peer review. The editorial revision of 1 November 2026 was made with Opus 5.5 by Anthropic used with Claude Code; it changed the presentation only, not the mathematics or the formalization.

Dev D. Goyal is responsible for publication. The work has not been externally peer reviewed. Section 6 states the formal scope, and Section 7 the limits of the result.

References

[1] W. van Dam and P. Hayden, *Universal entanglement transformations without communication*, Physical Review A **67**, 060302(R) (2003). arXiv:quant-ph/0201041.

[2] D. Leung and B. Wang, *Characteristics of universal embezzling families*, Physical Review A **90**, 042331 (2014). arXiv:1311.6842v2. Especially Sections 5–6.

[3] D. Leung, B. Toner, and J. Watrous, *Coherent state exchange in multi-prover quantum interactive proof systems*, Chicago Journal of Theoretical Computer Science, Article 11 (2013). doi:10.4086/cjtcs.2013.011.

[4] E. Zanoni, T. Theurer, and G. Gour, *Complete characterization of entanglement embezzlement*, Quantum **8**, 1368 (2024). arXiv:2303.17749v3.

[5] D. Lasecki, *Noisy embezzlement of entanglement and applications to entanglement dilution*, Master of Mathematics thesis, University of Waterloo (2019), Section 2.7. Institutional repository.

[6] I. George and E. Chitambar, *Reexamination of quantum state transformations with zero communication*, Physical Review A **109**, 062418 (2024). Preprint: *Revisiting pure state transformations with zero communication*, arXiv:2301.04735.

[7] L. van Luijk, A. Stottmeister, and H. Wilming, *Multipartite embezzlement of entanglement*, Quantum **9**, 1818 (2025). arXiv:2409.07646v3.

[8] A. Kera, L. van Luijk, A. Stottmeister, and H. Wilming, *Gaussian fermionic embezzlement of entanglement*, arXiv:2509.15749v2 (2026 revision).

[9] S.-X. Zhang, S. Liu, and Y.-Q. Chen, *Entanglement embezzlement from diffusive hydrodynamics*, arXiv:2609.26362v1 (2026).

[10] Z. Song, *Parallel repetition for entangled games with gap exponent three*, ECCC TR26-199 (2026), Section 4.1. ECCC report.

[11] P. Lipka-Bartosik, H. Wilming, and N. H. Y. Ng, *Catalysis in quantum information theory*, Reviews of Modern Physics **96**, 025005 (2024). arXiv:2306.00798v2.