# Characteristics of Universal Embezzling Families

Debbie Leung[*]        Bingjie Wang[†]

6 July, 2014

### Abstract

We derive properties of general universal embezzling families for bipartite embezzlement protocols, where any pure state can be converted to any other without communication, but in the presence of the embezzling family. Using this framework, we exhibit various families inequivalent to that proposed by van Dam and Hayden. We suggest a possible improvement and present detail numerical analysis.

## 1   Introduction

We begin by defining bipartite *quantum state embezzlement* between Alice and Bob. Let $|\varphi\rangle$ and $|\mu\rangle$ be bipartite quantum states; embezzlement of $|\varphi\rangle$ from $|\mu\rangle$ is the transformation $|\mu\rangle \mapsto |\mu\rangle |\varphi\rangle$ using only local operations. Operationally, Alice and Bob share $|\mu\rangle$ and, without further communication, "embezzle" a shared $|\varphi\rangle$.

Pure bipartite entangled states, their interconversions, and their applications in quantum information processing tasks have been well-studied. Axiomatically, entanglement, as a quantum correlation, does not increase without communication, rendering exact embezzlement impossible for a general $|\varphi\rangle$. Surprisingly, van Dam and Hayden [vDH03] showed embezzlement can be approximated, with arbitrary precision, as the dimension of $|\mu\rangle$ grows. Furthermore, arbitrary $|\varphi\rangle$ can be embezzled from the same $|\mu\rangle$. We call such a sequence of states $|\mu(n)\rangle$ a *universal embezzling family*.

Embezzlement has found interesting applications. It enables remote parties to share an arbitrary state on demand without communication (see for example [DSV13]). Furthermore, embezzlement hides the existence or the disappearance of a quantum state from any external observer. Thus embezzlement is used in the noisy channel simulation in the original [BDH+09] and an alternative [BCR11] proof of the quantum reverse Shannon theorem. Finally, in [LTW13], embezzlement motivates a game for which no finite amount of entanglement suffices in an optimal strategy, and provides proofs that some natural classes of quantum operations are not topologically closed.

---

[*]Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada.

[†]University of Cambridge, Cambridge, Cambridgeshire, United Kingdom.

The results in [vDH03] have been extended in several ways. An alternative embezzling family for any number of parties is proposed in [LTW13]. This family also achieves better approximation for a given dimension of $|\mu\rangle$ for non-universal embezzlement (a method attributed to [HS]). Reference [DSV13] provides an embezzlement protocol that is robust against discrepancy between the descriptions of $|\varphi\rangle$ available to Alice and Bob.

There are many unresolved questions concerning embezzlement. In the multiparty setting, the only known universal multiparty embezzlement family is an $\epsilon$-net of the non-universal embezzlement states [LTW13]; perhaps more efficient universal families exist. In the bipartite setting, the family in [vDH03] is not known to be optimal, but it has been elusive to find an optimality proof or a better family. Likewise, there may be a lower dimensional resource state for the robust protocol in [DSV13]. Very few universal embezzling families are known, and finite size effect or the computational complexity of embezzlement is hardly studied.

In this paper, we focus on the bipartite setting. We derive conditions for universal embezzlement, and exhibit a countably infinite number of inequivalent families. We conjecture a universal embezzling family based on our findings, and provide numerical evidence for the improvement in efficiency.

During the preparation of this manuscript, we learned of the result by Dinur, Steurer, and Vidick reported in [DSV13], and another on-going study of embezzlement by Haagerup, Scholz, and Werner [HSW].


## Canonical Form for Embezzlement

Any pure bipartite state has a Schmidt decomposition (see for example [NC00]). Since the parties can perform local unitary operations, without loss of generality, $|\mu\rangle = \sum_{i=1}^{\tilde{n}} \mu_i |i\rangle_{A_1} |i\rangle_{B_1}$ and $|\varphi\rangle = \sum_{j=1}^{m} \varphi_j |j\rangle_{A_2} |j\rangle_{B_2}$ where $\{|i\rangle\}_{i=1}^{\tilde{n}}$, $\{|j\rangle\}_{j=1}^{m}$ are orthonormal bases for Alice's systems $A_1, A_2$, and for Bob's systems $B_1, B_2$. Furthermore, $\mu_i$, $\varphi_i$ can be chosen non-negative and decreasing, with $\sum \mu_i^2 = 1$ and $\sum \varphi_i^2 = 1$ so $|\mu\rangle$ and $|\varphi\rangle$ are normalized. We refer to $\tilde{n}$ as the Schmidt rank and the $\mu_i$s as Schmidt coefficients of $|\mu\rangle$; the same terminology holds for the Schmidt decomposition of any bipartite state.

In this canonical form, there is an exchange symmetry between Alice and Bob. Furthermore, any quantum operation can be implemented as an isometry, $U$, with possibly larger output space. In embezzlement, the actual output state is $U \otimes U |\mu\rangle$.


## Measure of success and optimal strategy

One measure of the precision of the embezzlement protocol is the fidelity. The fidelity between two pure states $|\varphi\rangle$ and $|\psi\rangle$ is given by $F(|\varphi\rangle, |\psi\rangle) = |\langle\varphi|\psi\rangle|$ (see [NC00]). From [VJN00], it follows that the fidelity between the output $U \otimes U |\mu\rangle$ and the target $|\mu\rangle |\varphi\rangle$ is optimized by the isometry $U$ taking $A_1 \mapsto A_1 A_2$ (likewise for Bob) that simply permutes the basis states, such that $|\omega\rangle := U^\dagger \otimes U^\dagger |\mu\rangle |\varphi\rangle$ has decreasing Schmidt coefficients. The optimal fidelity is $\max_U \langle\mu|\langle\varphi| (U \otimes U |\mu\rangle) = \langle\omega| (|\mu\rangle \otimes |1\rangle|1\rangle)$. The state $|\mu\rangle \otimes |1\rangle|1\rangle$ has Schmidt coefficients $\mu_i$ followed by zeros. We denote

it by the equivalent state $|\mu\rangle$ throughout.

In this paper, we only consider embezzlement protocols that involve permutation of the basis states. We often consider "optimal embezzlement" as described above. Given a universal embezzling family, we focus on a subsequence $|\mu(n)\rangle$ indexed by the local dimension $n = \tilde{n}$.

Intuitively, a state $|\mu\rangle$ is useful for universal embezzlement if its Schmidt coefficients $\mu_i's$ has high fidelity with respect to $\{\mu_i \varphi_j\}_{ij}$ for any valid $\{\varphi_j\}$.

### General vs regular embezzling families

The most general embezzling family has the form

$$|\mu(n)\rangle = \sum_{i=1}^{n} \mu(i,n) |i\rangle |i\rangle$$

where for each $n$, $\mu(i,n)$ is decreasing with $i$ and $\sum_{i=1}^{n} \mu(i,n)^2 = 1$. An interesting special case concerns embezzling families whose Schmidt coefficients are generated by decreasing functions of one variable $i$, $f : \mathbb{N} \mapsto \mathbb{R}^+$. They are given by

$$|\mu(f,n)\rangle = \frac{1}{\sqrt{C(f,n)}} \sum_{i=1}^{n} f(i) |i\rangle |i\rangle \ .$$

where $C(f,n) = \sum_{i=1}^{n} f(i)^2$ so $|\mu(f,n)\rangle$ is normalized. We call these universal embezzling families "regular". They are a direct generalization of the universal embezzling family proposed in [vDH03]:

$$|\mu(f_{dh},n)\rangle = \frac{1}{\sqrt{C(f_{dh},n)}} \sum_{i=1}^{n} \frac{1}{\sqrt{i}} |i\rangle |i\rangle$$

where $f_{dh}(x) = 1/\sqrt{x}$.

## 2   Properties of Embezzling Families

In this section, we present necessary conditions and sufficient conditions for a sequence, $|\mu(n)\rangle$, to be a universal embezzling family.

First, for universal embezzlement, it suffices to be able to embezzle any Schmidt rank 2 state. We first introduce a lemma stating that embezzlement of different Schmidt rank $m$ states can be done in superposition. This result is a simple generalization of both embezzlement and coherent state exchange [LTW13].

**Lemma 1.** *Suppose it is possible to embezzle any $|\varphi\rangle$ with Schmidt rank m using $|\mu\rangle$ with fidelity at least F (see Section 1), then the following transformation*

$$\sum_{j=1}^{k} \alpha_j |\mu\rangle |jj\rangle \rightarrow \sum_{j=1}^{k} \alpha_j |\mu\rangle |\varphi_j\rangle$$

3

*can be performed with fidelity at least F without communication, for any $\alpha_j$'s satifying $\sum_{j=1}^{k} |\alpha_j|^2 = 1$ and for each $|\varphi_j\rangle$ of the form*

$$|\varphi_j\rangle = \sum_{l=1}^{m} \varphi_{j,l}|m(j-1)+l\rangle|m(j-1)+l\rangle \ \text{ with } \sum_{l=1}^{m} |\varphi_{j,l}|^2 = 1\,.$$

*Proof.* The given embezzlement property, as specified in Section 1, implies that $\forall j, \exists U_j$ such that $F(U_j \otimes U_j|\mu\rangle|11\rangle, |\mu\rangle \sum_{l=1}^{m} \varphi_{j,l}|ll\rangle) \geq F$. Modifying the input and output bases gives a $\widetilde{U}_j$ such that $F(\widetilde{U}_j \otimes \widetilde{U}_j|\mu\rangle|jj\rangle, |\mu\rangle|\varphi_j\rangle) \geq F$. Further define $\widetilde{U}_j|\xi\rangle|j'\rangle = 0$ for all $|\xi\rangle$ whenever $j' \neq j$. So, $U = \sum_j \widetilde{U}_j$ is an isometry satisfying:

$$\left[\sum_{j'=1}^{k} \alpha_{j'}^* \langle\mu|\langle\varphi_{j'}|\right]\left[U \otimes U \sum_{j=1}^{k} \alpha_j|\mu\rangle|jj\rangle\right] = \left[\sum_{j'=1}^{k} \alpha_{j'}^* \langle\mu|\langle\varphi_{j'}|\right]\left[\sum_{j=1}^{k} \alpha_j \widetilde{U}_j \otimes \widetilde{U}_j|\mu\rangle|jj\rangle\right] \geq F\,.$$

$\square$

We now analyze embezzlement of general states by recursively embezzling Schmidt rank 2 states while reusing the embezzlement state. To do so, we use two facts concerning the *trace distance* between two density matrices $\sigma_{1,2}$ of equal dimension, defined as $T(\sigma_1, \sigma_2) := \frac{1}{2}\|\sigma_1 - \sigma_2\|_1$ where $\|\cdot\|_1$ denotes the Schatten 1-norm. First, for two pure states, $T(|\sigma_1\rangle, |\sigma_2\rangle)^2 + F(|\sigma_1\rangle, |\sigma_2\rangle)^2 = 1$. Second, the trace distance is nonincreasing under any quantum operation and is subadditive. (See [Rus94, FvdG99, NC00] for detail.) In particular, if $F(|\sigma\rangle, U|\sigma_1\rangle) \geq F_1$ and $F(|\sigma_1\rangle, |\sigma_2\rangle) \geq F_2$, then,

$$\sqrt{1 - F(|\sigma\rangle, U|\sigma_2\rangle)^2} = T(|\sigma\rangle, U|\sigma_2\rangle) \leq T(|\sigma\rangle, U|\sigma_1\rangle) + T(|\sigma_1\rangle, |\sigma_2\rangle) \leq \sqrt{1 - F_1^2} + \sqrt{1 - F_2^2}, \quad (1)$$

which bounds the performance of substituting $|\sigma_1\rangle$ by $|\sigma_2\rangle$ in any operation $U$.

**Lemma 2.** *Suppose it is possible to embezzle any Schmidt rank 2 state from $|\mu\rangle$ with fidelity at least F. Then, embezzlement of any Schmidt rank m state $|\varphi\rangle$ can be achieved with fidelity at least $F_m$ where $1 - F_m^2 \leq \lceil\log_2 m\rceil^2(1-F^2)$.*

*Proof.* It suffices to prove the theorem for $m = 2^l$ for $l \in \mathbb{N}$ via induction on $l$. The base case $l = 1$ is given. Assume, for some $k$, for any state $|\phi\rangle$ with Schmidt rank at most $2^k$, there exists an isometry $V$, such that $F_k = F(V \otimes V|\mu\rangle, |\mu\rangle|\phi\rangle)$ satisfies $1 - F_k^2 \leq k^2(1-F^2)$.

It remains to show that any $|\varphi\rangle = \sum_{i=1}^{m} \varphi_i|i\rangle|i\rangle$ with $m = 2^{k+1}$ can be embezzled with the desired fidelity. To do so, let $\alpha_j^2 = \varphi_{2j-1}^2 + \varphi_{2j}^2$ and $|\varphi_j\rangle = \alpha_j^{-1}(\varphi_{2j-1}|2j-1\rangle|2j-1\rangle + \varphi_{2j}|2j\rangle|2j\rangle)$ for $j = 1, 2, 3, \cdots, 2^k$. Apply the induction hypothesis; so $|\phi\rangle = \sum_{j=1}^{m/2} \alpha_j|jj\rangle$ can be embezzled with fidelity at least $F_k$ with some isometry $V$. In addition, from Lemma 1, $|\mu\rangle|\phi\rangle \rightarrow |\mu\rangle(\sum_{j=1}^{m/2} \alpha_j|\varphi_j\rangle) = |\mu\rangle|\varphi\rangle$ can be performed with fidelity at least $F$. Finally, using Eq. (1), we evaluate the fidelity of composing these two steps by taking $|\sigma\rangle = |\mu\rangle|\varphi\rangle$, $|\sigma_1\rangle = |\mu\rangle|\phi\rangle$, and $|\sigma_2\rangle = V \otimes V|\mu\rangle$. This yields $\sqrt{1 - F_{k+1}^2} \leq \sqrt{1-F^2} + \sqrt{1-F_k^2} \leq \sqrt{1-F^2} + \sqrt{k^2(1-F^2)} = (k+1)\sqrt{1-F^2}$. $\square$

*Remark.* Due to Lemma 2, we take $|\varphi\rangle = \alpha|00\rangle + \beta|11\rangle$ unless otherwise stated. In $|\omega\rangle$, the Schmidt coefficients either have the form $\alpha\mu(i,n)$ or $\beta\mu(i,n)$ which we will refer to as $\alpha$ and $\beta$ terms respectively.

Our next observation implies the divergence of the normalization factor $C(f, n)$ for regular embezzling families.

**Lemma 3.** *If $|\mu(n)\rangle$ is a universal embezzling family, then $\mu(1, n) \to 0$ as $n \to \infty$. In particular, for regular universal embezzling families, $C(f, n) \to \infty$ as $n \to \infty$.*

*Proof.* Let $F$ be the fidelity of the embezzlement protocol, minimized over $|\varphi\rangle$. Lower bound $1 - F$ by considering specifically $|\varphi\rangle = (|11\rangle + |22\rangle)/\sqrt{2}$:

$$1 - \mathrm{F}(|\mu(n)\rangle, |\omega\rangle) = 1 - \sum_i \mu_i \omega_i = \frac{1}{2} \sum_{i=1}^{2n} (\mu_i - \omega_i)^2 \geq \frac{1}{2} (\mu_1 - \omega_1)^2 = \frac{1}{2} \left(1 - \frac{1}{\sqrt{2}}\right)^2 \mu_1^2,$$

where we use the shorthard $\mu_i$ for $\mu(i, n)$, $\omega_i$'s are the Schmidt coefficients of $|\omega\rangle$ in decreasing order, and $\omega_1 = \mu_1/\sqrt{2}$. Since $\mu_1 > 0$ (else $|\mu(n)\rangle$ cannot be a valid quantum state), $F \to 1$ implies $\mu(1, n) \to 0$ as $n \to \infty$.

For regular families $|\mu(f, n)\rangle$, $\mu(1, n) = f(1)/\sqrt{C(f, n)}$, so $C(f, n) \to \infty$ as $n \to \infty$. $\square$

Note that $|\mu(f, n)\rangle = |\mu(cf, n)\rangle$ for any constant $c$. Thus, we consider the *order* of a regular universal embezzling family defined as follows: a universal embezzling family has *order* $g$ if and only if $C(f, n) = \Theta(g)$, e.g., $|\mu(f_{dh}, n)\rangle$ has order $\ln n$. Lemma 3 shows that the "misalignment" of the first terms of $|\mu(n)\rangle$ and $|\omega(n)\rangle$ has to be corrected by a divergent order.

The next lemma gives a sufficient condition in terms of the asymptotic behavior of the ratio $\rho(|\varphi\rangle, f, i) := \omega_i/\mu_i$. First, given $|\varphi\rangle = \sum_{j=1}^m \varphi_j |j\rangle|j\rangle$ and $f$, we explain how to make this ratio well-defined for all $i \in \mathbb{N}$. Fix an arbitrary $n$ and let $\mu(i, n) = f(i)/\sqrt{C(f, n)}$ for $i = 1, \cdots, n$. Let $\omega(i, n)$ be the $i$-th largest element in $S_n = \{\mu(i, n)\varphi_j\}$. Define $\rho(|\varphi\rangle, f, i)$ to be $\omega(i, n)/\mu(i, n)$ for $i = 1, \cdots, n$. Note that the $\sqrt{C(f, n)}$ factors cancel out in the ratios. Furthermore, let $n' > n$ and define $\omega(i, n')/\mu(i, n')$ for $i = 1, \cdots, n'$ similarly. The first $n$ ratios coincide with $\omega(i, n)/\mu(i, n)$ because the $n$ largest terms in $S_{n'} = \{\mu(i, n')\varphi_j\}$ are labeled by the same $(i, j)$'s as those in $S_n$.

**Lemma 4.** *Let $f : \mathbb{N} \mapsto \mathbb{R}^+$ be a decreasing function with $C(f, n) \to \infty$. If $\forall |\varphi\rangle$, $\rho(|\varphi\rangle, f, i) \to 1$, then $|\mu(f, n)\rangle$ forms a regular universal embezzling family.*

*Proof.* Since $\rho \to 1$, given any $\varepsilon > 0$, $\exists n_\varepsilon$ such that $(1 - \varepsilon)\mu_i < \omega_i < (1 + \varepsilon)\mu_i$ for all $i > n_\varepsilon$. Thus

$$\mathrm{F}(|\mu(f, n)\rangle, |\omega\rangle) = \sum_{i=1}^n \mu_i \omega_i = \sum_{i=1}^{n_\varepsilon} \mu_i \omega_i + \sum_{i=n_\varepsilon+1}^n \mu_i \omega_i > \sum_{i=n_\varepsilon+1}^n \mu_i \omega_i$$

$$> (1 - \varepsilon) \sum_{i=n_\varepsilon+1}^n \mu_i^2 > (1 - \varepsilon) - \sum_{i=1}^{n_\varepsilon} \mu_i^2 > (1 - \varepsilon) - \frac{C(f, n_\varepsilon)}{C(f, n)}.$$

Since $n_\varepsilon$ does not depend on $n$, and $C(f, n) \to \infty$, $\mathrm{F}(|\mu(f, n)\rangle, |\omega\rangle) \to 1$. Thus, $|\mu(f, n)\rangle$ forms a universal embezzling family. In fact, $1 - F < \varepsilon + C(f, n_\varepsilon)/C(f, n)$. $\square$

We note on the side that Lemma 4 does not have a natural converse. Universal embezzling families may exist with infinitely many but intermittent violations of the condition $\rho(|\varphi\rangle, f, i) \approx 1$.

# 3   Variations on $|\mu(f_{dh}, n)\rangle$

In this section and the next, we focus on regular universal embezzling families. We consider the "simplest" variation from $f_{dh}$, which is $f = g/\sqrt{x}$. This construction can be used in two ways to yield a universal embezzling family.

**Lemma 5.** *Let $h : \mathbb{N} \to \mathbb{R}^+$. If, $C(f, n) \to \infty$, $f = h/\sqrt{x}$ is decreasing, and $h(kx + c)/h(x) \to 1$ as $x \to \infty$ for any constant $k \in \mathbb{N}$, $c \in \mathbb{N} \cup \{0\}$, then, $|\mu(f, n)\rangle$ forms a universal embezzling family.*

*Proof.* First, if $h(kx + c)/h(x) \to 1$ as $x \to \infty$, for any constants $k \in \mathbb{N}$, $c \in \mathbb{N} \cup \{0\}$, then, $h(k_1 x + c_1)/h(k_2 x + c_2) \to 1$ as $x \to \infty$ for any constants $k_1, k_2 \in \mathbb{N}$ and $c_1, c_2 \in \mathbb{N} \cup \{0\}$. This follows from the quotient rule

$$\lim_{x \to \infty} \frac{h(k_1 x + c_1)}{h(k_2 x + c_2)} = \frac{\lim_{x \to \infty} \frac{h(k_1 x + c_1)}{h(x)}}{\lim_{x \to \infty} \frac{h(k_2 x + c_2)}{h(x)}} = 1.$$

Following Lemma 2, consider $|\varphi\rangle = \alpha |11\rangle + \beta |22\rangle$. Let $z = (\alpha/\beta)^2$. Recall that the optimal fidelity is achieved with decreasing Schmidt coefficients $\omega_i$ for $|\omega\rangle$. Here, we consider a particular ordering of Schmidt coefficients, $|\widetilde{\omega}\rangle$, which can be suboptimal. Then, any lower bound on $F(|\mu(f, n)\rangle, |\widetilde{\omega}\rangle)$ also applies to $F(|\mu(f, n)\rangle, |\omega\rangle)$.

First, suppose $z = p/q \in \mathbb{Q}$. Call the $p$ largest $\alpha$-terms (see remark to Lemma 2) the first $\alpha$-block, the next $p$ largest $\alpha$-terms the second $\alpha$-block, and so on. Define the $\beta$-blocks similarly, but with block size $q$ instead. Construct $|\widetilde{\omega}\rangle$ such that the $l$-th block of $p + q$ terms comes from the $l$-th $\alpha$- and $\beta$-blocks. In other words, for $l(p + q) + 1 \le i \le (l + 1)(p + q)$:

$$\widetilde{\omega}_i = \begin{cases} \alpha f(lp + C_1)/C(f, n) \text{ or} \\ \beta f(lq + C_2)/C(f, n) \end{cases}$$

where $1 \le C_1 \le p$ and $1 \le C_2 \le q$. Now consider $\widetilde{\omega}_i/\mu_i$ where $i = l(p + q) + C$ for any $0 \le C \le p + q$. If $\widetilde{\omega}_i$ is an $\alpha$-term, then

$$\frac{\widetilde{\omega}_i}{\mu_i} = \alpha \sqrt{\frac{l(p + q) + C}{lp + C_1}} \cdot \frac{h(lp + C_1)}{h(l(p+q) + C)}.$$

As $i \to \infty$, $l \to \infty$, $h(lp + C_1)/h(l(p+q) + C) \to 1$, so $\widetilde{\omega}_i/\mu_i \to \alpha\sqrt{(p + q)/p} = 1$. If $\widetilde{\omega}_i$ is a $\beta$-term, with a similar argument, $\widetilde{\omega}_i/\mu_i \to \beta\sqrt{(p + q)/q} = 1$. Then, by Lemma 4, $F(|\mu(f, n)\rangle, |\widetilde{\omega}\rangle) \to 1$.

If $z \notin \mathbb{Q}$, the above proof applied to rational approximations of $z$ provides the desired result. More specifically, if $z = (\alpha/\beta)^2 \notin \mathbb{Q}$, $\forall \delta > 0$, $\exists z' = p/q \in \mathbb{Q}$ such that

$$\left(\frac{\alpha}{\beta}\right)^2 - \delta < \frac{p}{q} < \left(\frac{\alpha}{\beta}\right)^2 + \delta. \tag{2}$$

The previous argument shows that $\widetilde{\omega}_i/\mu_i$ tends to either $\alpha\sqrt{(p + q)/p}$ or $\beta\sqrt{(p + q)/q}$. Eliminating $p/q$ in these expression using (2) gives:

$$1 - \frac{\delta\beta^4}{\alpha^2 + \delta\beta^2} < \alpha\sqrt{\frac{p + q}{p}} < 1 + \frac{\delta\beta^4}{\alpha^2 + \delta\beta^2} \quad \text{and} \quad 1 - \delta\beta^2 < \beta\sqrt{\frac{p + q}{q}} < 1 + \delta\beta^2$$

and both quantities tend to 1 as $\delta \to 0$. □

**Lemma 6.** *Let* $g : \mathbb{N} \mapsto \mathbb{R}^+$ *be an increasing function such that* $f = g/\sqrt{x}$ *is decreasing. If, in addition,* $\forall m \in \mathbb{N}, C(f, n/m)/C(f, n) \to 1$ *as* $n \to \infty$, *then* $|\mu(f, n)\rangle$ *forms a universal embezzling family.*

*Proof.* This proof derives heavily from [vDH03].

Claim: $\forall j$, $\omega_j \leq \mu_j$. Let $N(t) = |\{l : \mu_t < \omega_l\}|$. The claim is equivalent to $N(t) < t$ as $\{\omega_l\}$ is decreasing. Since $\omega_l = \varphi_i f(j)/C(f, n)$ for some $i, j$, we let $N_i^t = |\{j : \mu_t < \varphi_i f(j)/C(f, n)\}|$. Now,

$$\mu_t < \varphi_i \frac{f(j)}{C(f, n)} \quad \Leftrightarrow \quad f(t) < \varphi_i f(j) \quad \Leftrightarrow \quad \frac{jg(t)^2}{tg(j)^2} < \varphi_i^2.$$

We can infer that $t \leq j$ since the middle inequality implies $f(j) < f(t)$ and $f$ is decreasing. Then, the last inequality and the monotonicity of $g$ imply that $j < \varphi_i^2 t$, so $N_i^t < \varphi_i^2 t$ and $N(t) = \sum_i N_i^t < t$ (recall the normalization $\sum_i \varphi_i^2 = 1$). Finally,

$$F(|\mu(f, n)\rangle, |\omega\rangle) = \sum_{i=1}^n \mu_i \omega_i \geq \sum_{i=1}^n \omega_i^2 \geq \sum_{j=1}^{\lfloor n/m \rfloor} \sum_{i=1}^m \frac{\varphi_i^2 f(j)^2}{C(f, n)} = \frac{C(f, \lfloor n/m \rfloor)}{C(f, n)} \to 1 \qquad (3)$$

where the last inequality comes from replacing the sum with possibly fewer and smaller terms. □

Lemma 6 states that $f$ can fall off slower than $f = 1/\sqrt{x}$ as long as $C(f, n/m)/C(f, n) \to 1$.

# 4 New classes of regular universal embezzling families

Now we present two sequences of regular universal embezzling families using Lemmas 5 and 6. First, define $\lambda(x) = \ln(x + e)$ and its n-fold composition: $\lambda^0(x) = x$, $\lambda^1(x) = \ln(x + e)$, $\lambda^2(x) = \ln(\ln(x + e) + e)$, and so on.

Now define the $G$ and $H$ functions of class $r$ as:

$$G_r(x) = \frac{1}{\sqrt{x}} \prod_{s=1}^r \sqrt{\lambda^s(x)} \qquad (4)$$

$$H_r(x) = \frac{1}{\sqrt{x}} \prod_{s=1}^r \frac{1}{\sqrt{\lambda^s(x)}} \qquad (5)$$

For every $r$, we will see that $|\mu(G_r, n)\rangle$ and $|\mu(H_r, n)\rangle$ have different orders and are universal embezzling families. Therefore, the number of orders for regular universal embezzling families is infinite.

To estimate $C(H_r, n)$, we use integral approximations:

$$\frac{d}{dx} \lambda^{r+1}(x) = \prod_{s=0}^r \frac{1}{\lambda^s(x) + e} \approx H_r(x)^2 \Rightarrow \sum_{i=1}^n H_r(i)^2 \approx \int_1^n H_r(x)^2 dx \approx \lambda^{r+1}(n)$$

7

Thus, the order of $|\mu(H_r, n)\rangle$ is $\lambda^{r+1}(n) \approx \ln^{r+1}(n)$ for large $n$.

For $C(G_1, n)$, we apply integral approximations and the inequality $G_1(x)^2 \leq (\ln(x-e))/(x-e)$ for $x \geq 5$ to obtain:

$$\int_1^n \frac{\ln(x+e)}{x+e} < \int_1^n \frac{\ln(x+e)}{x} \approx \sum_{i=1}^n G_1(i)^2 \leq \sum_{i=1}^5 G_1(i)^2 + \int_5^n \frac{\ln(x-e)}{x-e}. \tag{6}$$

The integrals are all well approximated by $(\ln n)^2/2$. Thus $C(G_1, n) = \Theta[(\ln n)^2]$. For general $C(G_r, n)$, there is no simple approximation, but we can show that subsequent orders are progressively "higher." First,

$$C(G_{r+1}, n) = \sum_{i=1}^n G_{r+1}(i)^2 = \sum_{i=1}^n \lambda^{r+1}(i)\, G_r(i)^2 \geq \sum_{i=1}^n G_r(i)^2 = C(G_r, n). \tag{7}$$

We show by contradiction that $C(G_{r+1}, n) \neq \Theta[C(G_r, n)]$. If so, there are constants $\kappa, n_0$, such that $\forall n > n_0$, $C(G_{r+1}, n) \leq \kappa C(G_r, n)$. Pick $n_1 > n_0$ so that $\lambda^{r+1}(n_1) \geq 3\kappa$, and $n_2 > n_1$ such that $\sum_{i=1}^{n_1} G_r(i)^2 \leq \sum_{i=n_1+1}^{n_2} G_r(i)^2$. Now,

$$\kappa C(G_r, n_2) \leq 2\kappa \sum_{i=n_1+1}^{n_2} G_r(i)^2 \leq \frac{2}{3} \lambda^{r+1}(n_1) \sum_{i=n_1+1}^{n_2} G_r(i)^2 \leq \frac{2}{3} \sum_{i=n_1+1}^{n_2} G_r(i)^2 \lambda^{r+1}(i)^2 \leq \frac{2}{3} C(G_{r+1}, n_2)$$

a contradiction.

**Embezzling Properties of $|\mu(G_r, n)\rangle$**

First, we sketch that $G_r(x)$ is decreasing. Let $t(x) = \lambda(x)/\sqrt{x}$. Then, $t(x)$ is decreasing because its first derivative has the same sign as $\theta(x) = 2x - (x+e)\ln(x+e)$, and $\forall x > 0$, $\theta(x) < 0$ because its first derivative is negative and $\theta(0) < 0$. Therefore, $\lambda(x+1)/\sqrt{x+1} < \lambda(x)/\sqrt{x}$ and $\lambda(x+1)/\lambda(x) < \sqrt{x+1}/\sqrt{x}$ for $x > 0$. Repeating this result yields: $\lambda^2(x+1)/\lambda^2(x) < \sqrt{\lambda(x+1)}/\sqrt{\lambda(x)} < [(x+1)/x]^{1/4}$, etc. Now:

$$\frac{G_r(x+1)^2}{G_r(x)^2} = \frac{x}{x+1} \prod_{i=1}^r \frac{\lambda^i(x+1)}{\lambda^i(x)} < \frac{x}{x+1} \prod_{i=1}^r \left[\frac{x+1}{x}\right]^{1/2^i} < 1$$

so the positive functions $G_r$ are all decreasing.

Second, $\forall r \geq 1, C(G_r, n)$ diverges (see Eq. (7)).

We can establish that $|\mu(G_1, n)\rangle$ forms a universal embezzling family using Lemma 6, by using the estimate (6) to conclude that

$$\frac{C(G_1, n/m)}{C(G_1, n)} \sim \left(1 - \frac{\ln m}{\ln n}\right)^2.$$

However, the lower bound for fidelity of embezzlement by $|\mu(G_1, n)\rangle$ is no better than that of $|\mu(f_{dh}, n)\rangle$, despite Lemma 4 (recall: $1 - F < \varepsilon + C(f, N_\varepsilon)/C(f, n)$) and the higher order of $G_1$.

For other $G_r$, we will show that Lemma 5 applies. We first show by induction that $\forall s \in \mathbb{N}$, $\lambda^s(kx+c)/\lambda^s(x) \to 1$ for any constants $k, c$

8

For $s = 1$:

$$\frac{\lambda^1(kx+c)}{\lambda^1(x)} = \frac{\ln(x+c/k)+\ln k}{\ln(x)} \to 1. \tag{8}$$

For $s \geq 2$, both $\lambda^{s-1}(kx+c) \to \infty$ and $\lambda^{s-1}(x) \to \infty$. By induction hypothesis, their ratio tends to 1. Thus, the proven base case (8) implies $\lambda^s(kx+c)/\lambda^s(x) = \lambda^1(\lambda^{s-1}(kx+c))/\lambda^1(\lambda^{s-1}(x)) \to 1$.

Then, for any class $r$, by the limit rule for products and the continuity of $\sqrt{\cdot}$ and $1/\cdot$ over the range of interest, both $\prod_{s=1}^{r} \sqrt{\lambda^s(x)}$ and $\prod_{s=1}^{r} 1/\sqrt{\lambda^s(x)}$ satisfy the condition in Lemma 5. Thus, all 3 conditions in Lemma 5 holds for $G_r$ and $|\mu(G_r, n)\rangle$ forms a universal embezzling family.

## Embezzling Properties of $|\mu(H_r, n)\rangle$

$H_r$ is obviously decreasing $\forall r$. We have already shown that $\prod_{s=1}^{r} 1/\sqrt{\lambda^s(x)}$ satisfies the condition in Lemma 5 and $C(H_r, n) \to \infty$ from our estimate of $C(H_r, n)$. Therefore, by Lemma 5, $|\mu(H_r, n)\rangle$ forms a universal embezzling family.

However, $|\mu(f_{dh}, n)\rangle$ performs better when embezzling any entangled state. This follows from Lemma 3 and the fact $C(H_r, n)/C(f_{dh}, n) \to 0$ as $n \to \infty$.

## Entanglement of $|\mu(f_{dh}, n)\rangle$, $|\mu(G_1, n)\rangle$, and $|\mu(H_1, n)\rangle$

Another metric of embezzlement efficiency is the amount of entanglement required in creating $|\mu\rangle$. For the original embezzling family proposed in [vDH03], using integral approximations:

$$\text{Ent}(|\mu(f_{dh}, n)\rangle) = -\sum_{i=1}^{n} \mu_i^2 \log_2(\mu_i^2) \approx -\sum_{i=1}^{n} \frac{1}{i}\frac{1}{\ln n} \log_2 \frac{1}{i}\frac{1}{\ln n} .$$

Simplifying the above and using integral approximations, the leading term of $\text{Ent}(|\mu(f_{dh}, n)\rangle)$ is $(\log_2 n)/2$.

Similarly, we can estimate $\text{Ent}(|\mu(G_1, x)\rangle)$. We use $C(G_1, n) \approx (\ln n)^2/2$ and the approximation $\lambda(x) \approx \ln x$ to conclude that

$$\text{Ent}(|\mu(G_1, n)\rangle) \approx -\sum_{i=1}^{n} \frac{\ln i}{i}\frac{2}{(\ln n)^2} \log_2 \frac{\ln i}{i}\frac{2}{(\ln n)^2} \approx \frac{2}{3}\log_2 n$$

where the last estimate concerns only the lead term and uses integral approximations.

Finally, we use $C(H_1, n) \approx \lambda^2(n) \approx \ln \ln n$ to estimate $\text{Ent}(|\mu(H_1, n)\rangle)$ which is $\approx (\log_2 n)/(\ln \ln n)$.

For a fixed Schmidt rank, $\text{Ent}(|\mu(G_1, n)\rangle)$ and $\text{Ent}(|\mu(f_{dh}, n)\rangle)$ are of the same order. Meanwhile, $\text{Ent}(|\mu(H_1, n)\rangle) \ll \text{Ent}(|\mu(f_{dh}, n)\rangle)$. However, if one fixes the precision, a higher Schmidt rank is needed to embezzle using $H_1$ than $f_{dh}$.

9

# 5   Outperforming $|\mu(f_{dh}, n)\rangle$?!

In the previous sections, we examine regular families that do not have order $\ln n$. There are interesting sequences that are not regular. One such sequence is presented in [LTW13] (due to [HS]):

$$|\mu(n)\rangle = \sqrt{\frac{2}{N+1}} \sum_{k=1}^{N} \sin\left(\frac{k\pi}{N+1}\right) |00\rangle^{\otimes k} |\varphi\rangle^{\otimes N-k+1} \tag{9}$$

where $n = 2^N$. This sequence enables the embezzling of the specific state $|\varphi\rangle$ with fidelity at least $1 - \pi^2/2N^2 = 1 - \pi^2/2(\log_2 n)^2$, a marked improvement over the provable lower bound $1 - O(1/\log_2 n)$ of the fidelity achieved by $|\mu(f_{dh}, n)\rangle$. The sequence in (9) also saturates an upper bound of the fidelity proved in [vDH03]. However, if $|\varphi\rangle = (|11\rangle + |22\rangle)/\sqrt{2}$ and Alice and Bob want to embezzle $|\varphi'\rangle = \alpha |11\rangle + \beta |22\rangle$, the fidelity $\to (\alpha + \beta)/\sqrt{2}$ as $N \to \infty$ which is bounded away from 1 when $|\varphi'\rangle \neq |\varphi\rangle$.

Instead, we propose the following. Let $gh$ be defined, for fixed $n$, and for $x \in \mathbb{N}, 1 \leq x \leq n$ as:

$$gh(x) = \begin{cases} H_1(1) \text{ when } x = 1 \\ H_1(x) \text{ when } C(gh, x-1) \geq \ln(x) \\ G_1(x) \text{ when } C(gh, x-1) < \ln(x). \end{cases}$$

Then define $GH(x)$ for $x \in \mathbb{N}, 1 \leq x \leq n$ as $gh(x)$ with elements in decreasing order (the $n$ dependence is implicit here) and designate $|\mu(n)\rangle = \sum_{i=1}^{n} GH(i) |i\rangle |i\rangle$. Due to the limited dependence on $n$, we can still define $C(GH, n)$ as before, and it differs from $\ln n$ by at most $G_1(n)^2$ or $H_1(n)^2$, but both $G_1(x)$ and $H_1(x) \to 0$ as $x \to \infty$. Therefore, $C(GH, n) \to \ln n$ as $n \to \infty$.

The precise performance of $|\mu(n)\rangle$ as a universal embezzling family is hard to analyse. So, we *numerically* evaluate the optimal fidelity (see Section 1) of embezzling three sample states: $|\varphi_+\rangle = (2 |00\rangle + |11\rangle)/\sqrt{5}$, $|\varphi_*\rangle = (\sqrt{\pi - 1} |00\rangle + |11\rangle)/\sqrt{\pi}$, and $|\varphi_\circ\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, using $|\mu(n)\rangle$ for $n = 2^N$, $N = 3, \cdots, 33$. For comparison, we also perform numerical optimization for the fidelity of embezzlement using $|\mu(f_{dh}, n)\rangle$.

Figure 1 summarizes the result.

All calculations are done in IEEE double-precision. The main source of inaccuracy in the numerical optimization is the accumulation of machine truncation errors in the calculation of $C(GH, n)$. We directly calculate $C(GH, n)$ for $3 \leq N \leq 26$ and approximate $C(GH, n)$ by $\ln n$ for $18 \leq N \leq 33$. The two methods yield optimal fidelities differing by less than $2 \times 10^{-6}$ for $18 \leq N \leq 26$.

A quick inspection of Figure 1 suggests that $|\mu(n)\rangle$ is indeed a universal embezzling family. Furthermore, $|\mu(n)\rangle$ outperforms $|\mu(f_{dh}, n)\rangle$ for the specific cases studied.

We extrapolate the data to try to understand the asymptotic behavior of $|\mu(n)\rangle$. The least square fits to the optimal fidelities to embezzle $|\varphi_+\rangle, |\varphi_*\rangle, |\varphi_\circ\rangle$ using $|\mu(n)\rangle$ are:

$$\begin{aligned} F_+ &= 0.9980 - 0.0759/N - 0.6358/N^2 \\ F_* &= 0.9976 - 0.1395/N - 0.6691/N^2 \\ F_\circ &= 0.9974 - 0.1971/N - 0.6862/N^2. \end{aligned}$$
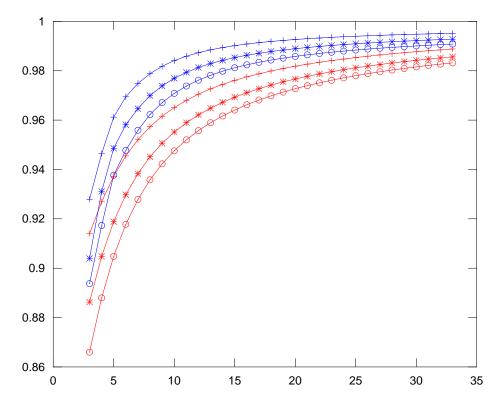
Figure 1: Optimal fidelity of embezzlement as a function of the number of qubits ($N = \log_2 n$) held by each party. The blue and red curves correspond to embezzlement using $|\mu(GH, n)\rangle$ and $|\mu(f_{dh}, n)\rangle$ respectively. Data points marked by $+$, $*$, and $\circ$ correspond to $|\varphi\rangle$ being $|\varphi_+\rangle$, $|\varphi_*\rangle$, and $|\varphi_\circ\rangle$ respectively.

The fitting parameters are insensitive to the method used to generate $C(GH, n)$. When fitting the data for $N_0 \leq N \leq 33$, the fitting parameters are slightly sensitive to $N_0$. We show the fits for $N_0 = 10$, when the constant term is smallest, the magnitude for the coefficients of the $1/N$ and $1/N^2$ terms are smallest and largest respectively. For $N_0$ ranging from 5 to 20, the constant can increase by 0.001, the magnitude of the second coefficients can increase by 0.03, that of the third coefficient can decrease by 0.3. We cannot conclude convincingly whether $F \to 1$ as $N \to \infty$.

The corresponding fits for the embezzling family $|\mu(f_{dh}, n)\rangle$ for $N_0 = 10$ are:

$$
\begin{aligned}
F_+ &= 0.999982 - 0.377165/N + 0.282380/N^2 \\
F_* &= 0.999970 - 0.484107/N + 0.359519/N^2 \\
F_\circ &= 0.999960 - 0.565744/N + 0.418400/N^2
\end{aligned}
$$

When $N_0$ ranges from 5 to 20, the constant can increase by 0.0001, the magnitudes of the second and third coefficients can increase by 0.01 and 0.1.

From the various fits, $|\mu(f_{dh}, n)\rangle$ starts to outperform $|\mu(n)\rangle$ when $N \approx 140 - 160$.

We note on the side that [vDH03] provides lower and upper bounds on the optimal fidelity of embezzlement using $|\mu(f_{dh}, n)\rangle$. We present the actual optimal performance (numerically) for small $N$ that may be of interest elsewhere.

11

# 6 Discussions

We have provided necessary conditions and sufficient conditions for universal embezzling in the bipartite setting. We exhibit an infinite number of inequivalent families, present a family that outperforms that proposed in [vDH03] for small $N$, but the latter *appears* optimal asymptotically based on our numerics. Our work does not resolve whether there is a regular or general universal embezzling family achieving fidelity $1 - O(1/(\log_2 n)^2)$. We hope our results are a step towards answering some of these questions.

# 7 Acknowledgements

# References

[BCR11]  M. Berta, M. Christandl, and R. Renner. The quantum reverse shannon theorem based on one-shot information theory. *Commun. Math. Phys.*, 306:579, 2011.

[BDH+09]  C. Bennett, I. Devetak, A. Harrow, P. Shor, and A. Winter. Quantum reverse shannon theorem. Available as arXiv.org e-Print 0912.5537, 2009.

[DSV13]  I. Dinur, D. Steurer, and T. Vidick. A parallel repetition theorem for entangled projection games. Available as arXiv.org e-Print 1310.4113, 2013.

[FvdG99]  C. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999.

[HS]  A. Harrow and P. Shor. personal communication.

[HSW]  U. Haagerup, V. Scholz, and R. Werner. personal communication.

[LTW13]  D. Leung, B. Toner, and J. Watrous. Coherent state exchange in multi-prover quantum interactive proof systems. *Chicago Journal of Theoretical Computer Science*, (11), August 2013.

[NC00]  M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, U.K., 2000.

[Rus94]  M. B. Ruskai. Beyond strong subadditivity: improved bounds on the contraction of generalized relative entropy. *Rev. Math. Phys.*, 6(5A):1147–1161, 1994.

[vDH03]  Wim van Dam and Patrick Hayden. Universal entanglement transformations without communication. *Phys. Rev. A*, 67:060302, 2003.

[VJN00]  G. Vidal, D. Jonathan, and M. Nielsen. Approximate transformations and robust manipulation of bipartite pure state entanglement. *Physical Review A*, 62:012304, 2000.