Existence of Universal Entangler

Jianxin Chen,1 Runyao Duan,1 Zhengfeng Ji,1 Mingsheng Ying,1 and Jun Yu2

1 State Key Laboratory of Intelligent Technology and Systems,
Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China
2 Department of Mathematics, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong
(Dated: June 2, 2014)

A gate is called an entangler if it transforms some (pure) product states to entangled states. A universal entangler is a gate which transforms all product states to entangled states. In practice, a universal entangler is a very powerful device for generating entanglements, and thus provides important physical resources for accomplishing many tasks in quantum computing and quantum information. This Letter demonstrates that a universal entangler always exists except for a degenerate case. Nevertheless, the problem how to find a universal entangler remains open.

PACS numbers: 02.20.-a, 02.20.Uw, 03.65.Ud, 03.67.Lx

Introduction. It is a common sense in the quantum computation and quantum information community that entanglement is an extremely important kind of physical resources. How to generate this kind of resources therefore becomes an important problem. One possibility one may naturally conceive is to generate entanglement from product states which can be prepared separately. If a gate can transform some product states to entangled states, then we call it an entangler. For some given product states, it is not difficult to find an entangler that maps them to entangled states. Here we consider a more challenging problem: Does there exist some entangler that can transform all product states to entangled states. We call such an entangler a universal entangler [3, 17]. One may even wonder at the existence of universal entanglers.

Formally, the problem of existence of universal entanglers in bipartite systems can be stated as follows:

Problem 1. Suppose Alice and Bob have two quantum systems with state spaces $H^A$ and $H^B$ respectively. Whether there exists a unitary operator $U$ acting on $H^A \otimes H^B$ such that $U(|\phi\rangle \otimes |\psi\rangle)$ is always entangled for any $|\phi\rangle \in H^A$ and $|\psi\rangle \in H^B$?

The purpose of this letter is to present a complete solution to the above problem. We have our main theorem as follows:

Theorem 1. Given a bipartite quantum system $H^A \otimes H^B$, where $H^A$ and $H^B$ are Hilbert space with dimension $m$ and $n$ respectively, then there exists a unitary operator $U$ which maps every product state of this system to an entangled bipartite state if and only if $\min(m, n) \geq 3$ and $(m, n) \neq (3, 3)$.

There are many literatures and different approaches which are potentially relevant to the topic of entanglers. Besides universal entangler, Zhang et al. discussed perfect entanglers which are defined as the unitary operations that can generate maximal entangled states from some initially separable states [16, 13, 20]. Bužek et al. [9] considered the entangler that entangles a qubit in unknown state with a qubit in a reference, also they proved the nonexistence of universal entangler for qubits, which answers a special case of our problem. Furthermore, nonexistence of universal entangler in $2 \otimes n$ bipartite system can be derived straightforwardly from Parthasarathy’s recent work on the maximal dimension of completely entangled subspace [14], which is tightly connected to the extendible product bases introduced by Bennett et al. [6, 7, 10].

But the proof of the above theorem requires some mathematical results from basic algebraic geometry. We will first review some basic notions in algebraic geometry in the next section. To make a clear presentation, Theorem 1 is divided into two parts, namely Theorems 2 and 3 below, and detailed proofs of them are given. Finally, a brief conclusion is drawn and some open problems are proposed.

Preliminaries. For the convenience of the reader, we recall some basic definitions in algebraic geometry [3, 11].

The $n \times n$ general linear group and the $n \times n$ unitary group are denoted by $GL(n, \mathbb{C})$ and $U(n)$, respectively.

An affine $n$-space, denoted by $A^n$, is the set of all $n$-tuples of complex numbers. An element of $A^n$ is called a point, and if point $P = (a_1, a_2, \ldots, a_n)$ with $a_i \in \mathbb{C}$, then the $a_i$‘s are called the coordinates of $P$.

The polynomial ring in $n$ variables, denoted by $\mathbb{C}[x_1, x_2, \ldots, x_n]$, is the set of polynomials in $n$ variables with coefficients in a ring.

A subset $Y$ of $A^n$ is an algebraic set if it is the common zeros of a finite set of polynomials $f_1, f_2, \ldots, f_r$ with $f_i \in \mathbb{C}[x_1, x_2, \ldots, x_n]$ for $1 \leq i \leq r$, which is also denoted by $Z(f_1, f_2, \ldots, f_r)$.

It is not hard to check that the union of a finite number of algebraic sets is an algebraic set, and the intersection of any family of algebraic sets is again an algebraic set. Thus by taking the open subsets to be the complements of algebraic sets, we can define a topology, called the Zariski topology on $A^n$. 


A nonempty subset $Y$ of a topological space $X$ is called irreducible if it cannot be expressed as the union $Y = Y_1 \cup Y_2$ of two proper closed subsets $Y_1, Y_2$. The empty set is not considered to be irreducible.

Let $X, Y$ be two topological spaces, then we have two useful facts:

**Fact 1.** If $X$ is irreducible and $F : X \to Y$ be a continuous function, then $F(X)$ with induced topology is also irreducible.

**Fact 2.** Let $Y \subset X$ be a subset, if $X$ is irreducible and $Y$ is open, then $Y$ is irreducible; if $X$ is irreducible and dense in $X$, then $X$ is irreducible.

An affine algebraic variety is an irreducible closed subset of some $\mathbb{A}^n$, with respect to the induced topology.

We define projective $n$-space, denoted by $\mathbb{P}^n$, to be the set of equivalence classes of $(n+1)$-tuples $(a_0, \ldots, a_n)$ of complex numbers, not all zero, under the equivalence relation given by $(a_0, \ldots, a_n) \sim (\lambda a_0, \ldots, \lambda a_n)$ for all $\lambda \in \mathbb{C}$, $\lambda \neq 0$.

A notion of algebraic variety may also be introduced in projective spaces, called projective algebraic variety: a subset $Y$ of $\mathbb{P}^n$ is an algebraic set if it is the common zeros of a finite set of homogeneous polynomials $f_1, f_2, \ldots, f_r$ with $f_i \in \mathbb{C}[x_0, x_1, \ldots, x_n]$ for $1 \leq i \leq r$. We call open subsets of irreducible projective varieties as quasi-projective varieties.

We will mainly use the following two varieties:

**Example 1.** $\mathbb{A}^1$ is irreducible, because its only proper closed subsets are finite, yet it is itself infinite. This fact is somewhat trivial. If $T$ is an algebraic subset of $\mathbb{A}^1$, then we should say, there is a finite set $F$ of polynomials over $\mathbb{C}$, such that $T = Z(F)$. For all $f \in \mathbb{C}[x]$, if $\deg(f) = 0$ or $f$ is a constant function, then $T$ should be the degenerate subset of $\mathbb{C}$, i.e., empty set $\emptyset$ or $\mathbb{C}$. Otherwise, we can choose a $f \in \mathbb{C}[x]$, such that $f$ is not a constant function, and $\deg(f)$ is no less than 1. From the fundamental theorem of algebra, we know the number of its roots is at most its degree, so its solution set should be a finite set. Thus, a subset of the solution set must be finite too, and we proved that $T$ is a finite subset of $\mathbb{C}$.

**Example 2.** The Segre embedding is defined as the map:

$$\sigma : \mathbb{P}^{n-1} \times \mathbb{P}^{m-1} \to \mathbb{P}^{mn-1}$$

taking a pair of points $([x], [y]) \in \mathbb{P}^{n-1} \times \mathbb{P}^{m-1}$ to their product

$$\sigma : ([x_0 : x_1 : \cdots : x_{m-1}], [y_0 : y_1 : \cdots : y_{n-1}]) \mapsto [x_0 y_0 : x_0 y_1 : \cdots : x_{m-1} y_{n-1}]$$

Here, $\mathbb{P}^{m-1}$ and $\mathbb{P}^{n-1}$ are projective vector spaces over some arbitrary field, $[x_0 : x_1 : \cdots : x_{n-1}]$ is the homogeneous coordinates of $x$, and similarly for $y$. The image of the map is a variety, called Segre variety, written as $\Sigma_{m-1,n-1}$.

What concerns us is that Segre variety represents the set of product states $\mathbb{H}_n \otimes \mathbb{H}_m$, where $\mathbb{H}_n$ and $\mathbb{H}_m$ are Hilbert spaces with dimension $n$ and $m$ respectively, if $\min(m, n) \leq 2$ or $(m, n) = (3, 3)$. The following theorem gives a negative answer for this case:

**Theorem 2.** Given a bipartite quantum system $\mathcal{H}_{\mathbb{H}_n} \otimes \mathcal{H}_{\mathbb{H}_m}$, where $\mathcal{H}_n$ and $\mathcal{H}_m$ are Hilbert spaces with dimension $n$ and $m$ respectively, if $\min(m, n) \leq 2$ or $(m, n) = (3, 3)$, then $\forall \Phi \in U(mn)$, we have $\Phi(Z) \cap Z \neq \emptyset$.

In other words, universal entangler does not exist.

To prove the above theorem, we need the following:

**Lemma 1.** [Projective Dimension Theorem] Let $Y, Z$ be varieties of dimensions $r, s$ in $\mathbb{P}^n$. Then every irreducible component of $Y \cap Z$ has dimension $\geq r + s - n$. Furthermore, if $r + s - n \geq 0$, then $Y \cap Z$ is nonempty.

For the proof of Lemma 1 see [11], chapter I, theorem 7.2. Then we can easily prove Theorem 2.

**Proof.** For any $\Phi \in U(mn)$, $\dim(Z) = m - 1 + n - 1 = m + n - 2$. Then we have $\dim(\Phi(Z)) + \dim(Z) - \dim(Y) = 2 \dim(Z) - \dim(Y) = 2(m + n - 2) - (mn - 1) = 1 - (m - 2)(n - 2) \geq 0$. So we have $\Phi(Z) \cap Z \neq \emptyset$ according to Lemma 1.

We now turn to consider the general case where $\min(m, n) \geq 3$ and $(m, n) \neq (3, 3)$.

The following lemmas are needed in the proof of our main theorem.
Lemma 2. $U(k)$ is Zariski dense in $GL(k, \mathbb{C})$

Proof. For the case $k = 1$, the only Zariski closed subsets of $G = GL(1, \mathbb{C}) = \mathbb{C} \setminus \{0\}$ are $\emptyset$, $G$ and non-empty finite subsets of $G$. This follows immediately from Example 1. Since $GL(1, \mathbb{C})$ is an open subset of affine line $\mathbb{C}$, its closed subsets are intersections of closed subsets of $\mathbb{C}$ and $\mathbb{C} \setminus \{0\}$. Now we see that $U(1)$ is infinite, thus $U(1) = G$.

In general, $H(k) = \{ \text{diagonal}(z_1, z_2, \cdots, z_k) : z_1, z_2, \cdots, z_k \in \mathbb{C} \setminus \{0\} \}$ is the fibre product of $k$ copies of $\mathbb{C} \setminus \{0\}$ [11]. Then $H(k) \cap U(k) = \{ \text{diagonal}(z_1, z_2, \cdots, z_k) : |z_1| = |z_2| = \cdots = |z_k| = 1 \} \cong U(1)^k$.

By the results of the case $k = 1$, we also have $H(k) \cap U(k) = H(k) \supseteq A(k) = \{ \text{diagonal}(z_1, z_2, \cdots, z_k) : z_1 > 0, z_2 > 0, \cdots, z_k > 0 \}$.

Now for any $B \in U(k)$, $L_B : X \to B \cdot X$ and $R_B : X \to X \cdot B$ are two isomorphisms of $G$, and $L_B(U(k)) = U(k) = R_B(U(k))$. Thus $L_B(U(k)) = U(k) = R_B(U(k))$.

Since $A(k) \subseteq H(k) \cap U(k) \subseteq U(k)$, we have $U(k)A(k) U(k) \subseteq U(k)$.

By singular value decomposition for $GL(k, \mathbb{C})$, we get $U(k)A(k)U(k) = GL(k, \mathbb{C}) \subseteq U(k)$. Thus $U(k) = GL(k, \mathbb{C})$.

The following lemma [12] establishes a connection between the dimensions of domain and codomain of a variety morphism. A morphism $\Phi : Z_1 \to Z_2$ is called a dominant morphism if $\Phi(Z_1)$ is dense in $Z_2$.

Lemma 3.

1. $Z_1$ and $Z_2$ are both irreducible varieties over $\mathbb{C}$, and $\phi : Z_1 \to Z_2$ is a dominant morphism, then $\dim(Z_2) \leq \dim(Z_1)$.

2. $Z_1$ and $Z_2$ are both varieties over $\mathbb{C}$, and $\phi : Z_1 \to Z_2$ is a morphism, $r = \max \{ \dim(\phi^{-1}(z)) : z \in Z_2 \}$, then $\dim(Z_1) \leq r + \dim(Z_2)$.

3. If $V = \cup_{i=1}^s V_i$ is a finite open covering, and $\forall i, V_i$ is irreducible, $\forall i, j, V_i \cap V_j \neq \emptyset$, then $V$ is irreducible.

Let $X = \{ \Phi : \Phi \in GL(mn, \mathbb{C}), \Phi(Z) \cap Z \neq \emptyset \}$. We are able to give an upper bound on the dimension of the closure of $X$ with respect to the Zariski topology.

Lemma 4. $\dim(\overline{X}) \leq m^2n^2 - (m - 2)(n - 2) + 1$, where $\overline{X}$ is the Zariski closure of $X$.

Proof. We have a morphism $F : G \times Y \to Y$ which is just the left action of $G$ on $Y$, defined by $F(g, [w]) = [g \cdot w]$ where $G = GL(k, \mathbb{C})$, $Y = \mathbb{P}^{mn-1}$, $k = mn$.

Let $y_0 = (1,0,\cdots,0)^T$ be a column vector with $k$ entries. For any given $y_1, y_2 \in Y$, we choose $g_1, g_2 \in GL(k, \mathbb{C})$, such that $[g_1 \cdot y_0] = [y_1]$ and $[g_2 \cdot y_0] = [y_2]$. Then we have

$$[g \cdot y_1] = [y_2]$$

$$\iff [gg_1 \cdot y_0] = [g_2 \cdot y_0]$$

$$\iff [g_2^{-1} gg_1 \cdot y_0] = [y_0]$$

From above observations, $F$ has the following property: for any $y_1, y_2 \in Y$, $F^{-1}(y_2) \cap \{ G \times \{ y_1 \} \} \cong \{ (z_1, g, g') : z_1 \in \mathbb{C} \setminus \{0\}, g' \in GL(k-1, \mathbb{C}), \alpha \in \mathbb{C}^{k-1} \text{ is a row vector} \}$. Hence $\dim(F^{-1}(y_2) \cap G \times \{ y_1 \}) = m^2n^2 - (mn - 1)$.

Let $P_1, P_2$ be projections of $G \times Y$ to $G, Y$ respectively. Now we only look at $G \times Z \subseteq G \times Y$, to get $F : G \times Z \to Y$. Then we have a characterization of $X : Z = P_1 F^{-1}(Z)$. In fact,

$$g \in X$$

$$\iff g(Z) \cap Z \neq \emptyset$$

$$\iff \exists z_1, z_2 \in Z, s.t. g(z_1) = z_2$$

$$\iff \exists z_1, z_2 \in Z, s.t. (g_1, z_1) = F^{-1}(z_2)$$

$$\iff \exists z_2 \in Z, s.t. g \in P_1 F^{-1}(z)$$

$$\iff g \in P_1 F^{-1}(Z)$$

Let $\overline{X} \subseteq G$ be the Zariski closure of $X$ in $G$, then $P_1 : F^{-1}(Z) \to \overline{X}$ is a dominant morphism.

Furthermore, consider $\Psi : F^{-1}(Z) \to Z \times Z$ given by $\Psi([g, z]) = ([z], [g \cdot z])$

For all $z_1, z_2 \in Z$, we have $\Psi^{-1}(z_1, z_2) = (g_2 T g_1^{-1}, z_1)$, where $T = \{ (z_0, 0) : z_0 \in \mathbb{C} \setminus \{0\}, g' \in GL(k-1, \mathbb{C}), \alpha \in \mathbb{C}^{k-1} \text{ is a row vector} \}$, and $g_1, g_2 \in GL(k, \mathbb{C})$, s.t. $g_1(y_0) = z_1$, $g_2(y_0) = z_2$. $\Psi$ is a dominant morphism since $G$ acts transitively on $\mathbb{P}^{mn-1}$. Then we obtain

$$\dim(F^{-1}(Z)) \leq \dim(T) + \dim(Z \times Z)$$

$$= m^2n^2 - mn + 1 + 2 \cdot \dim(Z)$$

It is required in Lemma 3.1 that varieties $Z_1$ and $Z_2$ are irreducible, but we haven’t proved $F^{-1}(Z)$ is irreducible. Actually, this condition can be weakened: Lemma 3.1 is still true for the more general case that $Z_1$ and $Z_2$ are closed subsets of irreducible varieties [11]. Thus, we can fill out the gap and apply this lemma. Indeed, the irreducibility of $F^{-1}(Z)$ and $\overline{X}$ really holds, but the proof is not easy (see [1] for a brief proof). From Lemma 3.1, we have

$$\dim(\overline{X}) \leq \dim(F^{-1}(Z))$$

$$\leq (m^2n^2 - (mn - 1)) + 2 \cdot \dim(Z)$$

$$= m^2n^2 - (mn - 1) + 2(m + n - 2)$$

$$= m^2n^2 - (m - 2)(n - 2) + 1$$

□
With the above lemmas, we can now derive the main result:

**Theorem 3.** Given a bipartite quantum system $\mathcal{H}_m \otimes \mathcal{H}_n$, where $\mathcal{H}_m$ and $\mathcal{H}_n$ are Hilbert spaces with dimensions $m$ and $n$ respectively, if $(m,n) > 2$ and $(m,n) \neq (3,3)$, then there exists an unitary operator $\Phi \in U(mn)$, s.t.

$$\Phi(Z) \cap Z = \emptyset$$

That is, $\Phi$ is a universal entangler.

**Proof.** If $U(mn) \subset X$, then it follows that $GL(mn, \mathbb{C}) = U(mn) \subset X$ from Lemma 2. And in this assumption, we also have $\dim(X) \leq m^2n^2 - (m-2)(n-2) + 1 < m^2n^2 = \dim(GL(mn, \mathbb{C}))$ from Lemma 3.2. It's a contradiction. So $U(mn) \not\subset X$, i.e. a unitary operator $\Phi \in U(mn)$ with $\Phi(Z) \cap Z = \emptyset$ exists. \hfill \qed

**Conclusion.** In summary, it is shown that a universal entangler of bipartite system exists except for the cases of $1 \otimes n$, $2 \otimes n$, $m \otimes 1$, $m \otimes 2$ and $3 \otimes 3$. So we have completely determined when a universal entangler exists. It seems that the method employed in this Letter can be extended to the multipartite case. This extension will lead us to explore the geometric structure of entangled states and other related objects. Furthermore, we can consider some more practical questions: (1) How to construct such a universal entangler for 3 $\otimes$ 4 bipartite system explicitly? (2) Given a universal entangler, what is the minimum entanglement it guarantees to output with respect to the definition of entanglement measure for pure states? (3) Furthermore, what is the optimal universal entangler which maximized the minimally possible entanglement the entangler outputs. Intuitively, for a bipartite system of sufficiently large dimensions, a randomly chosen unitary operator seems to be a universal entangler with high probability. Nevertheless, we failed to give a proof of this conjecture.

**Acknowledgements.** We are thankful to the colleagues in the Quantum Computation and Information Research Group of Tsinghua University for helpful discussions. And one of us (J.-X. Chen) enjoyed delightful discussions with W. Huang, L. Xiao, Z. Q. Zhang and Q. Lin. Jun Yu thank Professor X.-J. Tan and Q.-C. Tian who ask him to study Hartshorne `s book. This work was partly supported by the Natural Science Foundation of China(Grant Nos.60621062 and 60503001) and the Hi-Tech Research and Development Program of China(863 project)(Grant No.2006AA01Z102).

1. Electronic address: dry@tsinghua.edu.cn
2. Electronic address: jzhengfeng98@mails.thu.edu.cn
3. Electronic address: yingmsh@tsinghua.edu.cn
4. Electronic address: majunyu@ust.hk

[1] Here, we will present a short proof of the irreducibility of $F^{-1}(Z)$. \forall i, j: 0 \leq i \leq m-1, 0 \leq j \leq n-1, let $P_{m,i} = \{[x_0, x_1, \cdots, x_{m-1}]| x_i \neq 0 \}$, and $F_{n,j} = \{[y_0, y_1, \cdots, y_{n-1}]| y_j \neq 0 \}$. Let $Z_{i,j} = \sigma(P_{m,i} \times P_{n,j})$, we will have $Z = \cup_i Z_{i,j}$, and for $\forall i, j$, $Z_{i,j} \supseteq F_{m,i} \times P_{n,j} \supseteq A_t^{m-1} \times A_n^{n-2}$, and each $Z_{i,j}$ is open in $Z$. \forall i, j, we can construct a morphism $T_{i,j}: Z_{i,j} \rightarrow GL(mn, \mathbb{C})$ s.t. $Y \in Z_{i,j}$, $(T_{i,j}(y))(y) = y$. Then $\forall i, j, i, j, (g, y) \in \Psi^{-1}(Z_{i,j} \times Z_{i,j}) \iff g \cdot y \in Z_{i,j}$ and $Y \in Z_{i,j}$ \iff $(g \cdot T_{i,j}(y))(y) = T_{i,j}(y)(y)$ for some $y \in Z_{i,j}$, $Y \in Z_{i,j} \iff g \cdot (T_{i,j}(Z_{i,j}))^{-1} \cdot (Y \in Z_{i,j})$. Thus we have $F^{-1}(Z)_{i,j, i, j} = \{(g, y) \in \Psi^{-1}(Z_{i,j} \times Z_{i,j}) \}$ is irreducible since it’s the image of a morphism $Z_{i,j} \times H \times Z_{i,j} \rightarrow F^{-1}(Z)$. Each $F^{-1}(Z)_{i,j, i, j}$ is also open in $F^{-1}(Z)$, then the irreducibility follows from lemma 3.3.

[2] In fact, we proved $\Psi : F^{-1}(Z) \rightarrow Z \times Z$ is an algebraic fibre bundle thus $dim(F^{-1}(Z)) = m^2n^2 - mn + 1 + 2 \cdot dim(Z)$. We also conjecture that $\dim(X) = dim(F^{-1}(Z)) \times X = X$.


