

Entanglement distillation from Greenberger-Horne-Zeilinger shares

Péter Vrana¹ and Matthias Christandl²

¹Department of Geometry, Budapest University of Technology and
Economics, Egrý József u. 1., 1111 Budapest, Hungary

²Department of Mathematical Sciences, University of Copenhagen,
Universitetsparken 5, 2100 Copenhagen, Denmark

March 31, 2016

Abstract

We study the problem of converting a product of Greenberger-Horne-Zeilinger (GHZ) states shared by subsets of several parties in an arbitrary way into GHZ states shared by every party. Our result is that if SLOCC transformations are allowed, then the best asymptotic rate is the minimum of bipartite log-ranks of the initial state. This generalizes a result by Strassen on the asymptotic subrank of the matrix multiplication tensor.

1 Introduction

It has been realized recently (see e.g. [1, 2]) that certain problems in algebraic complexity theory can be interpreted as questions regarding asymptotic entanglement transformations by stochastic local operations and classical communication (SLOCC). Most prominently, the asymptotic rate at which GHZ states can be converted to triples of Einstein-Podolsky-Rosen (EPR) pairs, shared between parties AB, BC and AC, is the same as the exponent of matrix multiplication ω , i.e. the infimum of real numbers τ such that $n \times n$ matrices can be multiplied using $O(n^\tau)$ arithmetic operations [1]. This particular problem is still open, the best bounds currently being $2 \leq \omega \leq 2.3728639$ [3], but there are several similar problems where the exact value is known. Interestingly, these include the reverse transformation. To state this precisely, we first introduce some notation.

Definition 1. Let V_1, \dots, V_k and W_1, \dots, W_k be vector spaces and $\psi \in V_1 \otimes \dots \otimes V_k$, $\phi \in W_1 \otimes \dots \otimes W_k$. We say that ψ can be transformed into ϕ via SLOCC ($\psi \xrightarrow{\text{SLOCC}} \phi$) if there exist linear transformations $A_i : V_i \rightarrow W_i$ such that $(A_1 \otimes \dots \otimes A_k)\psi = \phi$.

The asymptotic SLOCC conversion rate from ψ to ϕ is

$$\omega(\psi, \phi) = \lim_{n \rightarrow \infty} \frac{1}{n} \inf \left\{ m \in \mathbb{N} \mid \psi^{\otimes m} \xrightarrow{\text{SLOCC}} \phi^{\otimes n} \right\}. \quad (1)$$

It is clear that the definition is not sensitive to multiplication by scalars, so for simplicity, we will work with unnormalized states.

Let MaMu denote the triple of EPR pairs, i.e.

$$\text{MaMu} = \text{EPR}_{AB} \otimes \text{EPR}_{BC} \otimes \text{EPR}_{AC} \quad (2)$$

and let $\text{GHZ} = |000\rangle + |111\rangle$. Then [4, Theorem 6.6]

$$\omega(\text{MaMu}, \text{GHZ}) = \frac{1}{2} \quad (3)$$

We review the main ingredients of the proof. The first one is a relaxation of SLOCC convertibility:

Definition 2. *Given tensors $\psi \in V_1 \otimes \dots \otimes V_k$, $\phi \in W_1 \otimes \dots \otimes W_k$, we say that ψ degenerates to ϕ if there exist linear transformations $A_i(\epsilon) : V_i \rightarrow W_i$ depending on ϵ and ϵ^{-1} polynomially (i.e. the matrix element functions are polynomials) such that $(A_1(\epsilon) \otimes \dots \otimes A_k(\epsilon))\psi = \phi + O(\epsilon)$ as $\epsilon \rightarrow 0$. This fact will be denoted by $\psi \xrightarrow{\text{SLOCC}} \phi$.*

The key result relating degeneration to asymptotic SLOCC transformations is that $\psi \xrightarrow{\text{SLOCC}} \phi$ implies $\omega(\psi, \phi) \leq 1$ (see [5, 6] or [2] for a proof using the same notations as here). As an example, $\text{GHZ} \xrightarrow{\text{SLOCC}} W$ leads to a simple proof of $\omega(\text{GHZ}, W) = 1$, even though GHZ cannot be converted to W via SLOCC in a one-shot setting.

Next, $\text{MaMu}^{\otimes n}$ is the same as

$$\sum_{i_1, i_2, i_3=1}^N |i_1 i_2\rangle |i_2 i_3\rangle |i_3 i_1\rangle \quad (4)$$

with $N = 2^n$ up to relabelling the local basis states. For some $g \in \mathbb{N}$, we choose the local linear transformations in the following way [4]:

$$\begin{aligned} A_1(\epsilon) |i_1 i_2\rangle &= \epsilon^{i_1^2 + 2i_1 i_2} |i_1 i_2\rangle \\ A_2(\epsilon) |i_2 i_3\rangle &= \epsilon^{i_2^2 + 2i_2(i_3 - g)} |i_2 i_3\rangle \\ A_3(\epsilon) |i_3 i_1\rangle &= \epsilon^{(i_3 - g)^2 + 2(i_3 - g)i_1} |i_3 i_1\rangle. \end{aligned} \quad (5)$$

Applying the product to a term $|i_1 i_2\rangle |i_2 i_3\rangle |i_3 i_1\rangle$ multiplies it by $\epsilon^{(i_1 + i_2 + i_3 - g)^2}$, therefore we have

$$\sum_{i_1, i_2, i_3=1}^N |i_1 i_2\rangle |i_2 i_3\rangle |i_3 i_1\rangle \xrightarrow{\text{SLOCC}} \sum_{\substack{1 \leq i_1, i_2, i_3 \leq N \\ i_1 + i_2 + i_3 = g}} |i_1 i_2\rangle |i_2 i_3\rangle |i_3 i_1\rangle. \quad (6)$$

Up to relabelling, the resulting state is a GHZ state. To see this, it is enough to note that every local basis element appears at most once, since any two of i_1 , i_2 and i_3 determines the third one uniquely.

To complete the proof, one only needs to choose g as a function of N in such a way that the number of terms grows as quadratically. This can be ensured by choosing $g = N$.

One possible generalization of the matrix multiplication state to $k > 3$ parties can be obtained by replacing the EPR pairs by arbitrary collections of GHZ states shared by subsets of the parties. The pattern can be conveniently encoded in a hypergraph on $\{1, \dots, k\}$ with multiple edges allowed. For example, the matrix multiplication state corresponds to the complete graph K_3 . The statement of our main result involves the concept of edge-connectivity. For the readers' convenience, we recall the definition here.

Definition 3. A hypergraph H is connected if for any pair of vertices x and y there is a sequence $(x = v_0, e_1, v_1, e_2, v_2, \dots, e_n, v_n = y)$ such that the e_i are hyperedges, v_i are vertices and e_i is incident to v_{i-1} and v_i for $i = 1, \dots, n$.

A hypergraph is l -edge-connected if it remains connected after removing any subset of strictly less than l edges. The edge-connectivity $\lambda(H)$ of a hypergraph H is the largest l such that H is l -edge-connected.

Now we are ready to state our main result.

Theorem 1. Let the state corresponding to the hypergraph H be GHZ^H . Then

$$\omega(\text{GHZ}^H, \text{GHZ}) = \frac{1}{\lambda(H)} \quad (7)$$

Note that the right hand side is easily seen to be a lower bound. This follows from the fact that 1) the bipartite rank across any bipartition cannot be increased asymptotically, 2) the bipartite log-rank of GHZ^H across the bipartition $S-\bar{S}$ (where \bar{S} denotes the complement) is the number of hyperedges having a nonvanishing intersection with both S and \bar{S} , 3) the minimum of these ranks is therefore $\lambda(H)$, and 4) the rank of GHZ over any bipartition is 2.

2 Proof of main result

By a hypergraph we mean a triple (V, E, I) where V and E are sets and $I \subseteq V \times E$. Elements of V are called vertices, E is the set of edges, and $v \in V$ is said to be incident with $e \in E$ if $(v, e) \in I$. The sum of two hypergraphs $H_1 = (V, E_1, I_1)$ and $H_2 = (V, E_2, I_2)$ on a common vertex set V is defined as $H_1 + H_2 = (V, E_1 \sqcup E_2, I_1 \sqcup I_2)$, where \sqcup stands for disjoint union and $I_1 \sqcup I_2$ is thought of as a subset of $V \times (E_1 \sqcup E_2)$ in the obvious way. Any hypergraph can be uniquely written as the sum of hypergraphs having one edge each.

If $V = [k] = \{1, 2, \dots, k\}$ for some positive integer k , we define the states GHZ_r^H by requiring $\text{GHZ}_r^{H_1+H_2} = \text{GHZ}_r^{H_1} \otimes \text{GHZ}_r^{H_2}$ and that for the hypergraph H_S which consists of a single edge $S \subseteq [k]$, the state $\text{GHZ}_r^{H_S}$ is an r -level GHZ state shared among the parties in S , i.e.

$$\text{GHZ}_r^{H_S} = |00\dots 0\rangle_{\bar{S}} \otimes (|11\dots 1\rangle_S + |22\dots 2\rangle_S + \dots + |rr\dots r\rangle_S) \quad (8)$$

These states are well-defined only up to SLOCC equivalence, but this is sufficient for our purposes. We will make use of the fact that

$$\omega(\text{GHZ}_a^H, \text{GHZ}_b^H) = \frac{\log b}{\log a} \quad (9)$$

for any hypergraph H having at least one edge of size at least 2. If $|E| = 1$ and the only edge is incident with every vertex, we will also write GHZ_r instead of GHZ_r^H .

Similarly to eq. (4), the states GHZ^H may be written as a multiple sum. For simplicity, we identify the edge set with $[l]$ for some $l \in \mathbb{N}$. To each edge $e \in E$ we introduce a summation index i_e , and for each $j \in [k]$ we let E_j be the set of edges incident with the vertex j . Then we can write

$$\text{GHZ}_n^H = \sum_{i_1, \dots, i_l=0}^{n-1} |(i_e)_{e \in E_1}\rangle_1 |(i_e)_{e \in E_2}\rangle_2 \cdots |(i_e)_{e \in E_k}\rangle_k \quad (10)$$

Without loss of generality we will assume that there are no empty edges.

Following the idea in Strassen's proof, but more generally, we wish to consider several linear equalities involving the indices, and apply local ϵ -dependent diagonal operations in such a way that the leading order contains precisely the terms satisfying the equalities. Such a system of equations can be written as

$$c_1 i_1 + c_2 i_2 + \cdots + c_l i_l = g \quad (11)$$

where $c_1, \dots, c_l, g \in \mathbb{Z}^d$, $d \geq 1$. Subtracting g from both sides and taking the inner product with itself results in

$$0 = \langle g, g \rangle + \sum_{e \in E} (\langle c_e, c_e \rangle i_e^2 - \langle c_e, g \rangle i_e) + \sum_{e, f \in E} \langle c_e, c_f \rangle i_e i_f \quad (12)$$

We need to distribute the terms among the vertices in such a way that an index i_e can only appear at vertices incident with e . This is always possible for the first term and the following sum, while the condition for the double sum is that $\langle c_e, c_f \rangle = 0$ whenever there is no vertex incident to both e and f . In other words, $c: E \rightarrow \mathbb{Z}^d$ is an orthogonal representation of the line graph $L(H)$ of H . Given such a c , we can choose local ϵ -dependent operators $A_1(\epsilon), \dots, A_k(\epsilon)$ in such a way that

$$\begin{aligned} & (A_1(\epsilon) \otimes \cdots \otimes A_k(\epsilon)) |(i_e)_{e \in E_1}\rangle_1 |(i_e)_{e \in E_2}\rangle_2 \cdots |(i_e)_{e \in E_k}\rangle_k \\ &= \epsilon^{\langle c_1 i_1 + \cdots + c_l i_l - g, c_1 i_1 + \cdots + c_l i_l - g \rangle} |(i_e)_{e \in E_1}\rangle_1 |(i_e)_{e \in E_2}\rangle_2 \cdots |(i_e)_{e \in E_k}\rangle_k, \end{aligned} \quad (13)$$

which shows that

$$\text{GHZ}_n^H \xrightarrow{\text{SLOCC}} \sum_{\substack{0 \leq i_1, \dots, i_l \leq n-1 \\ c_1 i_1 + \cdots + c_l i_l = g}} |(i_e)_{e \in E_1}\rangle_1 |(i_e)_{e \in E_2}\rangle_2 \cdots |(i_e)_{e \in E_k}\rangle_k \quad (14)$$

Next we want to ensure that the resulting state is a GHZ state. This happens precisely if the values of the indices at any one vertex determine the remaining ones uniquely. After fixing the indices at a vertex, $c_1 i_1 + \cdots + c_l i_l = g$ becomes a system of linear equations in the remaining indices, therefore the condition is that the vectors corresponding to edges not incident with any one vertex are linearly independent. It follows that the dimension d must be at least $|E| - \min_j |E_j|$, and therefore a sufficient condition is that any d vectors are linearly independent. Orthogonal representations of $L(H)$ with this property are said to be in general position. [7]

We now show that after fixing the coefficients in this way, the right hand side g can be chosen such that the number of solutions is large.

Theorem 2. Let $H = ([k], E, I)$ be a hypergraph and suppose that $c : E \rightarrow \mathbb{Z}^d$ is a general-position orthogonal representation of its line graph. Then

$$\omega(\text{GHZ}_2^H, \text{GHZ}_2) \leq \frac{1}{|E| - d}. \quad (15)$$

Proof. Let C be the maximum of 1-norms of the vectors $\{c_e\}_{e \in E}$, and choose G uniformly at random from the cube $[-Cn, Cn - 1]^d \cap \mathbb{Z}^d$. Let $X_{(i_1, \dots, i_l)}$ be the indicator random variable of the event that (i_1, \dots, i_l) is a solution of the (random) system of equations $c_1 i_1 + \dots + c_l i_l = G$. The number of solutions is

$$N = \sum_{i_1, \dots, i_l=0}^{n-1} X_{(i_1, \dots, i_l)}. \quad (16)$$

Since

$$\mathbb{E} X_{(i_1, \dots, i_l)} = \Pr(X_{(i_1, \dots, i_l)} = 1) = \Pr(c_1 i_1 + \dots + c_l i_l = G) = (2Cn)^{-d}, \quad (17)$$

the expected number of solutions is

$$\mathbb{E} N = n^l (2Cn)^{-d} = (2C)^{-d} n^{l-d} \quad (18)$$

Therefore there is at least one vector g such that $c_1 i_1 + \dots + c_l i_l = g$ has at least $M := \lceil (2C)^{-d} n^{l-d} \rceil$ solutions. This implies that

$$\begin{aligned} \omega(\text{GHZ}_2^H, \text{GHZ}_2) &\leq \omega(\text{GHZ}_2^H, \text{GHZ}_n^H) \omega(\text{GHZ}_n^H, \text{GHZ}_M^H) \omega(\text{GHZ}_M^H, \text{GHZ}_2) \\ &\leq \frac{\log n}{\log \lceil (2C)^{-d} n^{l-d} \rceil} \rightarrow \frac{1}{l-d} = \frac{1}{|E| - d} \end{aligned} \quad (19)$$

as $n \rightarrow \infty$. □

It follows that the best bound is obtained if d is as small as possible. The following result completes the proof of Theorem 1 by showing that the optimal value is $d = |E| - \lambda(H)$.

Theorem 3. Let $H = ([k], E, I)$ be a hypergraph. Then its line graph has a general-position orthogonal representation $c : E \rightarrow \mathbb{Z}^{|E| - \lambda(H)}$.

Proof. It is enough to see that there is an orthogonal representation $c : E \rightarrow \mathbb{Q}^{|E| - \lambda(H)}$, since after multiplying each vector by the least common denominator of its entries, it becomes one in $\mathbb{Z}^{|E| - \lambda(H)}$.

Since H is $\lambda(H)$ -edge-connected, its line graph is $\lambda(H)$ -vertex-connected. A result by Lovász, Saks and Schrijver [7, 8] states that any $(n - d)$ -vertex-connected graph with n vertices admits a general-position orthogonal representation in \mathbb{R}^d . Their proof relies in an essential way on using real numbers, and it does not seem to be possible to directly adapt the idea to our case. However, it is possible to deduce the existence of a general-position orthogonal representation in \mathbb{Q}^d as follows.

Let $G = (V, E)$ be an $(n - d)$ -vertex-connected graph with n vertices, and let $V = \{v_1, v_2, \dots, v_n\}$ be an ordering of the vertices. We construct a map $\mathcal{O}_G : (\mathbb{R}^d)^V \rightarrow (\mathbb{R}^d)^V$ recursively as follows. If $f : V \rightarrow \mathbb{R}^d$ is any function, then

$(\mathcal{O}_G f)(v_1) = f(v_1)$. If $i > 1$, we let $A_i = \{v_j | j < i \text{ and } \{v_i, v_j\} \notin E\}$. Let P_i denote the orthogonal projection onto the subspace spanned by $\{(\mathcal{O}_G f)(v) | v \in A_i\}$. Then we set $(\mathcal{O}_G f)(v_i) = (I - P_i)f(v_i)$.

It is clear from the definition that $\mathcal{O}_G f$ is an orthogonal representation for any f , and that if f is an orthogonal representation, then $\mathcal{O}_G f = f$.

Let us find a more explicit form of the projections P_i . Let us write $A_i = \{v_{j_1}, v_{j_2}, \dots, v_{j_r}\}$ with $j_1 < j_2 < \dots < j_r$. To find P_i , we first orthogonalize the vectors $(\mathcal{O}_G f)(v_{j_m})$, i.e. let $g_1 = (\mathcal{O}_G f)(v_{j_1})$ and

$$g_k = (\mathcal{O}_G f)(v_{j_k}) - \sum_{m=1}^{k-1} \frac{\langle g_m, (\mathcal{O}_G f)(v_{j_k}) \rangle}{\langle g_m, g_m \rangle} g_m \quad (20)$$

for $k = 2, \dots, r$. Here and in the following sum we exclude the terms with $g_m = 0$. Then the projection can be written as

$$P_i x = \sum_{m=1}^r \frac{\langle g_m, x \rangle}{\langle g_m, g_m \rangle} g_m. \quad (21)$$

From this form we can see that if $f : V \rightarrow \mathbb{Q}^d$ then P_i maps \mathbb{Q}^d into itself, therefore $\mathcal{O}_G f : V \rightarrow \mathbb{Q}^d$ as well.

If $f : V \rightarrow \mathbb{R}^d$ is a function such that none of the denominators in the above expression of P_i is 0, then $\mathcal{O}_G f$ is clearly continuous at f . This holds in particular if f is a general-position orthogonal representation, because in this case $\mathcal{O}_G f = f$, and the families $(f(v))_{v \in A_i}$ are linearly independent since $|A_i| \leq d$.

Now pick any general-position orthogonal representation $f : V \rightarrow \mathbb{R}^d$. By continuity at f and using that being in general position is an open condition, there is an open neighbourhood U of f such that $f' \in U$ implies that $\mathcal{O}_G f'$ is also a general-position orthogonal representation. Since $U \neq \emptyset$ is open, there is a function $c_0 : V \rightarrow \mathbb{Q}^d$ in U , therefore $c := \mathcal{O}_G c_0$ has the desired properties. \square

3 Discussion

Theorem 1 has a number of interesting special cases. Suppose first that the hypergraph H is a graph consisting of a single path going through every vertex. Then clearly $\lambda(H) = 1$, i.e. asymptotically one GHZ state per copy can be extracted via SLOCC. Of course, this can be easily proved without our result, since by teleportation the transformation can be performed on a single copy exactly via LOCC. On the other hand, if we add a single new edge joining the two endpoints, the graph becomes a cycle, which is 2-edge-connected, therefore asymptotically *two* GHZ states per copy can be obtained. We do not know if the same can be accomplished via LOCC with asymptotically vanishing error.

For the next example, let K_k^l denote the complete l -uniform hypergraph on $[k]$, i.e. the multiplicity of every l -element subset in K_k^l is one and there are no other edges. Then it is not difficult to see that a minimum cut is obtained by removing every edge incident with a distinguished vertex, therefore

$$\omega(\text{GHZ}_2^{K_k^l}, \text{GHZ}_2) = \frac{1}{\binom{k-1}{l-1}}. \quad (22)$$

This special case with $l = 2$ as well as the result for cycle graphs have recently found applications in complexity theory. In particular, ref. [9] shows that our results imply new protocols and bounds in nondeterministic multiparty quantum communication complexity.

Now let H be an arbitrary hypergraph and suppose that instead of GHZ states, the parties wish to distill EPR pairs shared between a specified pair AB . Suppose that the minimum cut separating A from B consists of t edges. By Menger’s theorem for hypergraphs, there exist t edge-disjoint paths P_1, \dots, P_t between A and B in H . Using Theorem 1 for the subhypergraph P_i , $\text{GHZ}_2^{P_i}$ can be transformed to a GHZ state on the subset of vertices incident with at least one edge in P_i , which in turn can be converted to an EPR-pair between A and B . This proves that $\omega(\text{GHZ}_2^H, \text{EPR}_{AB}) = 1/t$. This transformation also has an asymptotic LOCC counterpart with the same rate, under the name localizable entanglement [10].

Finally, let us mention that our result can be easily extended to products of GHZ-type states with possibly different number of levels. In this case, the minimum bipartite log-rank gives the asymptotic rate at which GHZ states can be obtained. Equivalently, H may be replaced with a hypergraph with weighted edges, where the weight corresponding to an r -level GHZ state is $\log r$. In this case $\lambda(H)$ on the right hand side of eq. (7) should be interpreted as the minimum cut weight.

4 Acknowledgement

We thank Jeroen Zuiddam for helpful discussions. MC acknowledges financial support from the European Research Council (ERC Grant Agreement no 337603), the Danish Council for Independent Research (Sapere Aude) and the Swiss National Science Foundation (project no PP00P2_150734). Part of this work was done while the authors were with ETH Zurich.

References

- [1] E. Chitambar, R. Duan, Y. Shi, “Tripartite Entanglement Transformations and Tensor Rank”, *Phys. Rev. Lett.* 101, 140502 (2008)
- [2] P. Vrana and M. Christandl, “Asymptotic entanglement transformation between W and GHZ states,” *Journal of Mathematical Physics*, vol. 56, no. 2, p. 022204, 2015.
- [3] F. Le Gall, “Powers of tensors and fast matrix multiplication”. In *Proceedings of the 39th international symposium on symbolic and algebraic computation*, pages 296–303. ACM, 2014.
- [4] V. Strassen, “Relative bilinear complexity and matrix multiplication”, *Journal für die reine und angewandte Mathematik* (1987) Vol. 375-376, 406-443
- [5] D. Bini, G. Lotti, F. Romani, “Approximate solutions for the bilinear form computational problem”, *SIAM J. Comput.*, 9(4), 692–697
- [6] V. Strassen, “Degeneration and complexity of bilinear maps: Some asymptotic spectra”, *J. Reine Angew. Math.* 413 (1991), pp. 127–180

- [7] L. Lovász, M. Saks, A. Schrijver, “Orthogonal representations and connectivity of graphs”, *Linear Alg. Appl.* **114/115** (1989), 439–454
- [8] L. Lovász, M. Saks, A. Schrijver, “A Correction: Orthogonal representations and connectivity of graphs”, *Linear Alg. Appl.* **313** (2000), 101–105
- [9] H. Buhrman, M. Christandl, and J. Zuiddam, *Multipartite quantum communication complexity: the cyclic equality game and iterated matrix multiplication*, arXiv:1603.03757
- [10] J. A. Smolin, F. Verstraete, and A. Winter, “Entanglement of assistance and multipartite state distillation,” *Physical Review A*, vol. 72, no. 5, p. 052317, 2005.