Multiparty distributed compression of quantum information

David Avis
avis@cs.mcgill.ca

Patrick Hayden
patrick@cs.mcgill.ca

Ivan Savov
ivan.savov@mcgill.ca

***Abstract*—We study a protocol in which many parties use quantum communication to transfer a shared state to a receiver without communicating with each other. This protocol is a multiparty version of the fully quantum Slepian-Wolf protocol for two senders and arises through the repeated application of the two-sender protocol. We describe bounds on the achievable rate region for the distributed compression problem. The inner bound arises by expressing the achievable rate region for our protocol in terms of its vertices and extreme rays and, equivalently, in terms of facet inequalities. We also prove an outer bound on all possible rates for distributed compression based on multiparty squashed entanglement.**

I. Introduction

Many of the protocols of information theory deal with multiple senders or multiple receivers. As a whole, however, *network information theory*, the field which studies general multiparty communication scenarios, is not yet fully developed even for classical systems [1]. Quantum network information theory, which deals with quantum multipartite communication, is also under active development [2], [3], [4] and, thanks to the no-cloning properties of quantum information, sometimes admits simple solutions [2]. On the other hand, a full understanding of quantum network theory will require a precise characterization of multiparty entanglement, a task which is far from completed [5], [6], [7]. Nevertheless, we can hope that in the future we will have a rigorous and complete theory of multiparty information in the spirit of the resource framework for two-party protocols [8], [9].

One step towards the development of multiparty information theory would be to generalize the compression protocols [10], [11] to situations where the information is "distributed" to many spatially separated parties. This is the multiparty distributed compression problem, where multiple parties use quantum communication to faithfully transfer their shares of a quantum state to a common receiver. The two-sender classical version of this problem was solved by Slepian and Wolf [12] while the quantum version was studied in [13], [14], [15]. In this paper, we build a protocol for multiparty distributed compression based on the fully quantum Slepian-Wolf protocol [15] and prove both inner and outer bounds on the achievable rate region. We relate our findings to previous results in information theory and discuss some possible applications.

We will denote quantum systems as A, B and the corresponding Hilbert spaces $\mathcal{H}^A, \mathcal{H}^B$ with respective dimensions d_A, d_B. We denote pure states of the system A by a *ket* $|\varphi\rangle^A$ and the corresponding density matrices as $\varphi^A = |\varphi\rangle\langle\varphi|^A$. We denote by $H(A)_\rho = -\mathrm{Tr}\left(\rho^A \log \rho^A\right)$ the von Neumann entropy of the state ρ^A. For a bipartite state σ^{AB} we define the conditional entropy $H(A|B)_\sigma = H(AB)_\sigma - H(B)_\sigma$ and the mutual information $I(A;B)_\sigma = H(A)_\sigma + H(B)_\sigma - H(AB)_\sigma$. The fidelity is defined to be $F(\sigma,\rho) = \mathrm{Tr}\left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2$. Throughout this paper, logarithms are taken base two unless otherwise specified.

II. Multiparty Distributed Compression

Distributed compression of classical information involves many parties collaboratively encoding their sources $X_1, X_2, \ldots, X_m$ and sending the information to a common receiver [16]. In the quantum setting, the parties are given a quantum state $\psi^{A_1A_2\cdots A_m} \in \mathcal{H}^{A_1A_2\cdots A_m}$ and are asked to individually compress their shares of the state and transfer them to the receiver Charlie, while sending as few qubits as possible [13]. No communication between the senders is allowed and, unlike [14], in this paper there is no classical communication between the senders and the receiver.

For our analysis, we work in the setting where the input consists of n copies of a state: $|\psi\rangle^{A_1A_2\cdots A_mR} = (|\varphi\rangle^{A_1A_2\cdots A_mR})^{\otimes n}$, where the A_i's denote the m different senders and R denotes the reference system, which does not participate in the protocol. Note that we use A_i to denote both the individual system associated with state φ as well the n-copy version associated with ψ; the meaning should be clear from the context.

The objective of the distributed compression task is for the participants to transfer their R-entanglement to a third party Charlie as illustrated in Figure 1. Note that any other type of correlation the A systems could have with an external subsystem is automatically preserved if entanglement is [17].

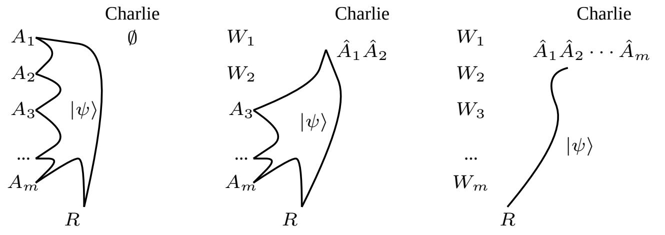

Fig. 1. Pictorial representation of the quantum correlations between the systems at three stages of the protocol. Originally the state $|\psi\rangle$ is shared between $A_1A_2\cdots A_m$ and R. The middle picture shows the protocol in progress. Finally, all systems are received by Charlie and $|\psi\rangle$ is now shared between Charlie's systems $\widehat{A}_1\widehat{A}_2\cdots\widehat{A}_m$ and R.

An equivalent way of thinking about quantum distributed compression is to say that the participants are attempting to decouple their systems from the reference R by sending quantum information to Charlie. Indeed, assume that originally R is the purification of $A_1 A_2 \cdots A_m$, and call W_1 through W_m the systems left behind at the end of the protocol with the holders of the original A_1 through A_m. If there are no correlations between $W_1 W_2 \cdots W_m$ and R, then the purification of R must have been transferred to Charlie's laboratory.

To perform the distributed compression task, each of the senders independently encodes her share before sending part of it to Charlie. The encoding operations are modeled by quantum operations, that is, completely positive trace-preserving (CPTP) maps E_i with outputs C_i of dimension 2^{nQ_i}. Once Charlie receives the systems that were sent to him, he will apply a decoding CPTP map D with output system $\widehat{A} = \widehat{A}_1 \widehat{A}_2 \ldots \widehat{A}_m$ isomorphic to the original $A = A_1 A_2 \ldots A_m$.

Definition 2.1 (The rate region): We say that a rate tuple $\vec{Q} \equiv (Q_1, Q_2, \ldots, Q_m)$ is achievable if for all $\epsilon > 0$ there exists $N(\epsilon)$ such that for all $n \geq N(\epsilon)$ there exist n-dependent maps $(E_1, E_2, \ldots, E_m, D)$ with domains and ranges as in the previous paragraph for which the fidelity between the original state, $|\psi\rangle^{A^n R^n} = \left(|\varphi\rangle^{A_1 A_2 \cdots A_m R}\right)^{\otimes n}$, and the final state, $\sigma^{\widehat{A}_1 \widehat{A}_2 \ldots \widehat{A}_m R} = \sigma^{\widehat{A}^n R^n}$, satisfies

$$F\left(|\psi\rangle^{A^n R^n},\ \sigma^{\widehat{A}^n R^n}\right) \geq 1 - \epsilon. \tag{1}$$

We call the closure of the set of achievable rates the rate region.

III. Protocols

In this section we introduce the fully quantum Slepian-Wolf (FQSW) protocol [15], which describes a procedure for simultaneous quantum state transfer and entanglement distillation. The two-party protocol is then used as a building block for a multiparty distributed compression protocol.

A. The FQSW protocol

Consider a setup where the state $|\psi\rangle^{ABR} = \left(|\varphi\rangle^{ABR}\right)^{\otimes n}$ is shared between Alice, Bob and a reference system R. The FQSW protocol describes a procedure for Alice to transfer her R-entanglement to Bob while at the same time generating ebits with him. Alice can accomplish this by encoding and sending part of her system, denoted A_1, to Bob. The state after the protocol can be written as $|\Phi\rangle^{A_2 \widetilde{B}} (|\varphi\rangle^{R\widehat{B}})^{\otimes n}$, where the systems $\widetilde{B}$ and $\widehat{B}$ are held in Bob's lab while A_2 remains with Alice. The state $|\Phi\rangle^{A_2 \widetilde{B}}$ is a maximally entangled state shared between Alice and Bob, a handy side-product which can be used to build more advanced protocols [18], [19]. Figure 2 illustrates the entanglement structure before and after the protocol.

The protocol consists of the following steps:

1) Alice performs Schumacher compression on her system A to obtain the output system A^S.
2) Next, she splits her system into two parts: $A_1 A_2 = A^S$ with $d_{A_1} = 2^{nQ_A}$ and
$$Q_A > \frac{1}{2} I(A;R)_\varphi. \tag{2}$$

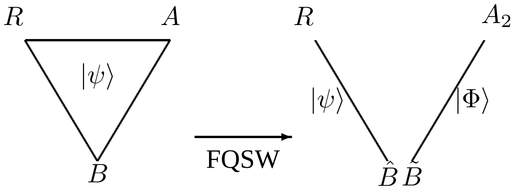

Fig. 2. Diagram representing the ABR correlations before and after the FQSW protocol. Alice manages to decouple completely from the reference R. The $\widehat{B}$ system is isomorphic to AB.

3) Alice then applies a random unitary U_A to A^S, and sends the system A_1 to Bob.
4) Bob, in turn, performs a decoding operation $V_B^{A_1 B \to \widehat{B}\widetilde{B}}$ which splits his system into a $\widehat{B}$ part purifying R and a $\widetilde{B}$ part which is fully entangled with Alice.

In other words, in the limit of many copies of the state, the FQSW protocol will succeed if the rate at which Alice sends qubits to Bob is

$$Q_A = \frac{1}{2} I(A;R)_\varphi + \delta. \tag{3}$$

for any $\delta > 0$.

B. The multiparty FQSW protocol

The FQSW protocol provides a natural approach to the two sender case of the multiparty distributed compression problem illustrated in Figure 1: if the first sender transfers her entire state to Charlie, then FQSW is sufficient to complete the compression task. Like the two-party FQSW protocol, the multiparty FQSW protocol demands that each sender individually Schumacher compress her system and apply a random unitary operation. The only additional ingredient is an agreed upon permutation of the participants. The temporal order in which the participants will perform their encoding is of no importance. However, the permutation determines how much information each participant is to send to Charlie.

For each permutation π of the participants, the protocol demands that Alice-i sends to Charlie a system C_i of dimension 2^{nQ_i} where

$$Q_i > \frac{1}{2} I(A_i; A_{\mathcal{K}_i} R)_\varphi, \tag{4}$$

where $\mathcal{K}_i = \{\pi(j) : j > \pi^{-1}(i)\}$ is the set of participants who come after i in the permutation. Charlie applies a decoding operation D consisting of the composition of the decoding maps $D_{\pi(m)} \circ \cdots \circ D_{\pi(2)} \circ D_{\pi(1)}$ defined by the individual FQSW steps in order to recover $\sigma^{\widehat{A}_1 \widehat{A}_2 \ldots \widehat{A}_m}$ nearly identical to the original $\psi^{A_1 A_2 \cdots A_m}$ and purifying R.

IV. Statement of Results

This subsection contains our two main theorems about multiparty distributed compression. In Theorem 4.1 we give the formula for the set of achievable rates using the multiparty FQSW protocol (sufficient conditions). Then, in Theorem 4.2 we specify another set of inequalities for the rates $(Q_1, \ldots, Q_m)$ which must be hold for any distributed compression protocol (necessary conditions).

Theorem 4.1: Let $|\varphi\rangle^{A_1 A_2 \cdots A_m R}$ be a pure state. If the inequality

$$\sum_{k\in\mathcal{K}} Q_k \geq \frac{1}{2}\left[\sum_{k\in\mathcal{K}} H(A_k)_\varphi + H(R)_\varphi - H(RA_{\mathcal{K}})_\varphi\right] \quad (5)$$

holds for all $\mathcal{K} \subseteq \{1, 2, \ldots, m\}$, then the rate tuple $\vec{Q} \equiv (Q_1, \cdots, Q_m)$ is achievable for distributed compression of the A_i systems.

Because Theorem 4.1 expresses a set of sufficient conditions for the protocol to succeed, we say that these rates are contained in the rate region. In the m-dimensional space of rate tuples $\vec{Q} \in \mathbb{R}^m$, the inequalities (5) define a convex polyhedron [20] whose facets are given by the corresponding hyperplanes, as illustrated in Figure 3. More specifically, the rate region is a supermodular polyhedron [21] with properties that will aid us in the proof of Theorem 4.1.

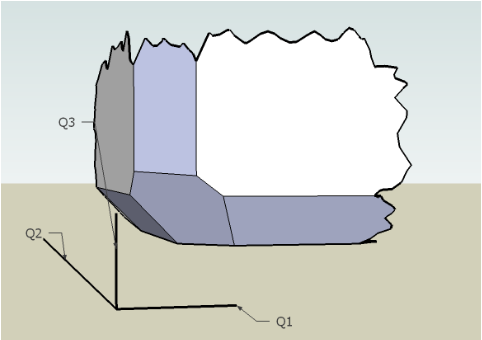

Fig. 3. The rate region for the multiparty FQSW protocol for three senders.

In order to characterize the rate region further we also derive an outer bound which all rate tuples must satisfy.

Theorem 4.2: Let $|\varphi\rangle^{A_1 A_2 \cdots A_m R}$ be a pure state input to a distributed compression protocol which achieves the rate tuple $(Q_1, \ldots, Q_m)$, then it must be true that

$$\sum_{k\in\mathcal{K}} Q_k \geq \frac{1}{2}\left[\sum_{k\in\mathcal{K}} H(A_k)_\varphi + H(R)_\varphi - H(RA_{\mathcal{K}})_\varphi\right] - E_{\text{sq}}(A_{k_1}; A_{k_2}; \ldots; A_{k_{|\mathcal{K}|}})_\varphi, \quad (6)$$

for all $\mathcal{K} \subseteq \{1, 2, \ldots, m\}$, where E_{sq} is the multiparty squashed entanglement.

The multiparty squashed entanglement [22], [4] is a measure of multipartite entanglement which generalizes the bipartite squashed entanglement of [23]. It is defined analogously to the bipartite version.

Definition 4.1 (Multiparty squashed entanglement): Consider the state $\rho^{X_1 X_2 \ldots X_m}$ shared by m parties. We define the multiparty squashed entanglement in the following manner:

$$E_{\text{sq}}(X_1; \ldots; X_m)_\rho := \frac{1}{2}\inf_E \left[\sum_{i=1}^{m} H(X_i|E)_{\tilde{\rho}} - H(X_1 \cdots X_m|E)_{\tilde{\rho}}\right] \quad (7)$$

where the infimum is taken over all states $\tilde{\rho}^{X_1 X_2 \ldots X_m E}$ such that $\text{Tr}_E\left(\tilde{\rho}^{X_1 X_2 \ldots X_m E}\right) = \rho^{X_1 X_2 \ldots X_m}$. (We say $\tilde{\rho}$ is an *extension* of ρ.)

The dimension of the extension system E is a priori unbounded, which unfortunately makes calculations of the squashed entanglement very difficult except for simple systems.

The motivation behind this definition is that we can include a copy of all classical correlations inside the extension E and thereby eliminate them from the multiparty information by conditioning. Since it is impossible to copy quantum information, we know that taking the infimum over all possible extensions E we will be left with purely quantum correlations. It is shown in [22], [4] that E_{sq} is continuous, monotonic under local operations and classical communication, convex and subadditive — a desirable and rare combination of properties in the multiparty case.

Notice that Theorems 4.1 and 4.2 both provide bounds of the same form and only differ by the presence of the E_{sq} term. The rate region is squeezed somewhere between these two bounds as illustrated in Figure 4.

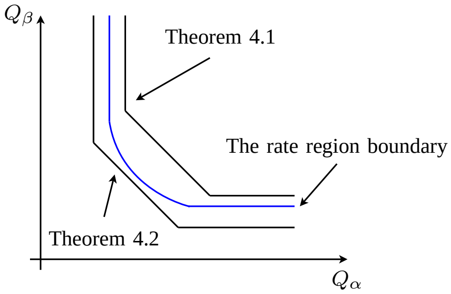

Fig. 4. A two dimensional diagram showing the inner bound from Theorem 4.1 and the outer bound from Theorem 4.2. The boundary of the rate region must lie somewhere in between.

For states which have zero squashed entanglement, like separable states for example, the inner and outer bounds on the rate region coincide so that in those cases our protocol is an optimal solution to the multiparty distributed compression problem.

V. Proof of the Achievable Rates

In this section we'll explain how to achieve the rates advertised in Theorem 4.1. Additional details and the proof of Theorem 4.2 can be found in [4].

The multiparty fully quantum Slepian-Wolf protocol can be constructed directly [24] or through the repeated application of the two-party FQSW protocol [15], [4]. We choose the latter approach here in order to illustrate the power of the FQSW protocol as a building block for more complex protocols. To complete the proof of Theorem 4.1 we will have to "stitch together" the entire rate region from different achievable points using some concepts from the theory of polyhedra [20]. The multiparty rate region has a complicated but highly structured geometry so it is important that we use the right language to describe it.

For every permutation $\pi \in S_m$ of the m senders, there is a different rate tuple $\vec{q}_\pi = (Q_1, Q_2, \ldots, Q_m)_\pi \in \mathbb{R}^m$ which is achievable in the limit of many copies of the state. By time-sharing we can achieve any rate that lies in the *convex hull* of these points. We will show that the rate region for an input state $|\varphi\rangle^{A_1\cdots A_mR}$ can equivalently be described by the set of inequalities from Theorem 4.1, that is

$$\sum_{k\in\mathcal{K}} Q_k \geq C_{\mathcal{K}}, \tag{8}$$

where $\mathcal{K} \subseteq \{1,\ldots,m\}$ ranges over all subsets of participants and $C_{\mathcal{K}} := \frac{1}{2}\big[\sum_{k\in\mathcal{K}} H(A_k)_\varphi + H(R)_\varphi - H(RA_{\mathcal{K}})_\varphi\big]$. The proof of Theorem 4.1 proceeds in two steps. First we show the set of rate tuples $\{\vec{q}_\pi\}$ is contained in the rate region and then we prove that the set of inequalities (8) is an equivalent description of the rates obtained by time sharing and resource wasting of the rates $\{\vec{q}_\pi\}$.

Consider the m-dimensional space of rate tuples $(Q_1,\cdots,Q_m) \in \mathbb{R}^m$. We begin by a formal definition of a corner point $\vec{q}_\pi$.

Definition 5.1 (Corner point): Let $\pi \in S_m$ be a permutations of the senders in the protocol. The corresponding rate tuple $q_\pi = (Q_1, Q_2, \ldots, Q_m)$ is a corner point if

$$Q_{\pi(k)} = \frac{1}{2} I(A_{\pi(k)}; A_{\pi(k+1)}\cdots A_{\pi(m)}R) \tag{9}$$

where the set $A_{\pi(k+1)}\cdots A_{\pi(m)}$ denotes all the systems which come after k in the permutation π.

We define $\mathcal{Q} := \{\vec{q}_\pi : \pi \in S_m\}$, the set of all corner points. Clearly $|\mathcal{Q}| \leq m!$, but since some permutations might lead to the same rate tuple, the inequality may be strict.

Lemma 5.2: The set of corner points, $\mathcal{Q} = \{\vec{q}_\pi : \pi \in S_m\}$, is contained in the rate region.

Proof sketch for Lemma 5.2: We know from the FQSW inequality (3) that in order for Alice to decouple from the some reference system R, she needs to send quantum information at a rate of $Q > \frac{1}{2}I(A;R)$. In each step of the multiparty FQSW protocol, we are facing a similar situation but instead we are trying to decouple from the reference R as well as all the remaining participants. The participants which have merged their shares of the state earlier provide side information at the decoder, which was the role of the B system in the FQSW protocol.

Thus, for a given permutation π, we should be able to successfully transfer the state if each Alice-i sends at a rate $Q_i > \frac{1}{2}I(A_i; A_{\mathcal{K}_i}R)_\varphi + \delta$ for any $\delta > 0$ and $\mathcal{K}_i = \{\pi(j) : j > \pi^{-1}(i)\}$ and the receiver applies the decoding map D consisting of the composition of the decoding maps $D_{\pi(m)} \circ \cdots \circ D_{\pi(2)} \circ D_{\pi(1)}$ defined by the individual FQSW steps. More precisely, Charlie should be able to recover a state $\sigma^{\widehat{A}_1\widehat{A}_2\cdots\widehat{A}_m}$ which will be such that the fidelity between $|\psi\rangle^{A^nR^n}$ and $\sigma^{\hat{A}^nR^n}$ is high. The proof follows because we can make the δs arbitrarily small, so the rate tuple $(Q_1,\cdots,Q_m)_\pi$, with

$$Q_{\pi(k)} = \frac{1}{2} I(A_{\pi(k)}; A_{\pi(k+1)}\cdots A_{\pi(m)}R) \tag{10}$$

must be contained in the rate region. This argument holds for all permutations $\pi \in S_m$, leading to the conclusion that the full set $\mathcal{Q}$ is contained in the rate region. ■

Each one of the corner points $\vec{q}_\pi$ can also be described by an equivalent set of equations involving sums of the rates.

$$\sum_{m-l+1\leq k\leq m} Q_{\pi(k)} = C_{\pi[m-l+1,m]} \tag{11}$$

for all l such that $1 \leq l \leq m$, where

$$C_{\pi[m-l+1,m]} = \frac{1}{2}\left[\sum_{m-l<k\leq m} H(A_{\pi(k)}) + H(R) - H(A_{\pi[m-l+1,m]}R)\right]$$

and $A_{\pi[m-l+1,m]} := A_{\pi(m-l+1)}A_{\pi(m-l+2)}\cdots A_{\pi(m)}$ denotes the last l participants according to the permutation π.

So far, we have shown that the set of corner points $\mathcal{Q}$ is contained in the rate region of the multiparty fully quantum Slepian-Wolf protocol. The convex hull of a set of points $\mathcal{Q}$ is defined to be $conv(\mathcal{Q}) := \{\vec{x} \in \mathbb{R}^m :\ \vec{x} = \sum \lambda_i \vec{q}_i,\ \vec{q}_i \in \mathcal{Q},\ \lambda_i \geq 0,\ \sum \lambda_i = 1\}$. Because of the possibility of time-sharing between the different corner points, the entire convex hull $conv(\mathcal{Q})$ must be achievable. Furthermore, by simply allowing any one of the senders to waste resources, we know that if a rate tuple $\vec{q}$ is achievable, then so is $\vec{q} + \vec{w}$ for any vector $\vec{w}$ with nonnegative coefficients. More formally, we say that any $\vec{q} + cone(\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_m)$ is also inside the rate region, where $\{\vec{e}_i\}$ is the standard basis for $\mathbb{R}^m$ and $cone(\vec{e}_1,\cdots,\vec{e}_m) := \{\vec{x} \in \mathbb{R}^m : \vec{x} = \sum \lambda_i \vec{e}_i, \lambda_i \geq 0\}$. Thus, we have demonstrated that the set of rates

$$P_{\mathcal{V}} := conv(\mathcal{Q}) + cone(\vec{e}_1,\cdots,\vec{e}_m) \tag{12}$$

is achievable. By the Minkowski-Weyl Theorem [20, p.30], we know that $P_{\mathcal{V}}$ can also be written as the intersection of a finite number of half-spaces. To complete the proof of Theorem 4.1, we will in fact show that $P_{\mathcal{V}}$ has an equivalent description as

$$P_{\mathcal{H}} := \left\{ \vec{Q} \in \mathbb{R}^m : \sum_{k\in\mathcal{K}} Q_k \geq C_{\mathcal{K}}, \forall\mathcal{K} \subseteq \{1,\ldots,m\} \right\}, \tag{13}$$

where the constants $C_{\mathcal{K}}$ are as defined in equation (8).

Preliminaries Before we begin the equivalence proof in earnest, we make two useful observations which will be instrumental to our subsequent argument.

Lemma 5.3 (Superadditivity): Let $\mathcal{K}, \mathcal{L} \subseteq \{1,2,\ldots,m\}$ be any two subsets of the senders. Then

$$C_{\mathcal{K}\cup\mathcal{L}} + C_{\mathcal{K}\cap\mathcal{L}} \ \geq\ C_{\mathcal{K}} + C_{\mathcal{L}}. \tag{14}$$

As a consequence of this lemma, we can derive an equivalence property for the saturated inequalities.

Corollary 5.4: Suppose that the following two equations hold for a given point of $P_{\mathcal{H}}$:

$$\sum_{k\in\mathcal{K}} Q_k = C_{\mathcal{K}} \qquad \text{and} \qquad \sum_{k\in\mathcal{L}} Q_k = C_{\mathcal{L}}. \tag{15}$$

Then the following equations must also be true:

$$\sum_{k\in\mathcal{K}\cup\mathcal{L}} Q_k = C_{\mathcal{K}\cup\mathcal{L}} \qquad \text{and} \qquad \sum_{k\in\mathcal{K}\cap\mathcal{L}} Q_k = C_{\mathcal{K}\cap\mathcal{L}}. \tag{16}$$

An important consequence of Lemma 5.3 is that it implies that the polyhedron $P_{\mathcal{H}}$ is of a very special type, known as a supermodular polyhedron or contra-polymatroid. The fact that $conv(Q) = P_{\mathcal{H}}$ was proved by Edmonds [21], whose ingenious proof makes use of linear programming duality. Below we give an elementary proof that does not use duality.

A *vertex* is a zero-dimensional face of a polyhedron. A point $\bar{Q} = (\bar{Q}_1, \bar{Q}_2, \ldots, \bar{Q}_m) \in P_{\mathcal{H}} \subset \mathbb{R}^m$ is a vertex of $P_{\mathcal{H}}$ if and only if it is the unique solution of a set of linearly independent equations

$$\sum_{k \in \mathcal{L}_i} Q_k = C_{\mathcal{L}_i}, \qquad 1 \leq i \leq m \tag{17}$$

for some subsets $\mathcal{L}_i \subseteq \{1, 2, \ldots, m\}$. In the remainder of the proof we require only a specific consequence of linear independence, which we state in the following lemma.

Lemma 5.5 (No co-occurrence): Let $\mathcal{L}_i \subseteq \{1, 2, \ldots, m\}$ be a collection of m sets such that the system (17) has a unique solution. Then there is no pair of elements j, k such that $j \in \mathcal{L}_i$ if and only if $k \in \mathcal{L}_i$ for all i.

Proof: If there was such a pair j and k, then the corresponding columns of the left hand side of (17) would be linearly dependent. ■

Armed with the above tools, we will now show that there is a one-to-one correspondence between the corner points $\mathcal{Q}$ and the vertices of the $\mathcal{H}$-polyhedron $P_{\mathcal{H}}$. We will then show that the vectors that generate the cone part of the $\mathcal{H}$-polyhedron correspond to the resource wasting vectors $\{\vec{e}_i\}$.

Step 1: $\mathcal{Q} \subseteq vertices(P_{\mathcal{H}})$ We know from equation (11) that every point $\vec{q}_\pi \in \mathcal{Q}$ satisfies the m equations

$$\sum_{m-i+1 \leq k \leq m} Q_{\pi(k)} = C_{\pi[m-i+1,m]}, \qquad 1 \leq i \leq m. \tag{18}$$

The equations (18) are very similar in form to the inequalities in (13) that are used to define $P_{\mathcal{H}}$. Because the left hand side is triangular, the equations have the unique solution:

$$Q_{\pi(m)} = C_{\pi(m)} \qquad Q_{\pi(i)} = C_{\pi[i,m]} - C_{\pi[i+1,m]}, \tag{19}$$

where $1 \leq i \leq m-1$. We need to show that this solution satisfies all the inequalities used to define $P_{\mathcal{H}}$ in (13). We proceed by induction on $|\mathcal{K}|$. The case $|\mathcal{K}| = 1$ follows from (19) and the superadditivity property (14). For $|\mathcal{K}| \geq 2$ we can write $\mathcal{K} = \{\pi(i)\} \cup \mathcal{K}'$ for some $\mathcal{K}' \subseteq \{\pi(i+1), \pi(i+2), \ldots, \pi(m)\}$. Then

$$\begin{aligned} \sum_{k \in \mathcal{K}} Q_k &= Q_{\pi(i)} + \sum_{k \in \mathcal{K}'} Q_k \\ &\geq C_{\pi[i,m]} - C_{\pi[i+1,m]} + \sum_{k \in \mathcal{K}'} Q_k \\ &\geq C_{\pi[i,m]} - C_{\pi[i+1,m]} + C_{\mathcal{K}'} \qquad \text{(induction)} \\ &\geq C_{\mathcal{K}} \end{aligned}$$

where we again used superadditivity to get the last inequality.

Step 2: $vertices(P_{\mathcal{H}}) \subseteq \mathcal{Q}$ In order to prove the opposite inclusion, we will show that every vertex of $P_{\mathcal{H}}$ is of the form of equation (11). More specifically, we want to prove the following proposition.

Proposition 5.6 (Existence of a maximal chain): Every vertex of $P_{\mathcal{H}}$, that is, the intersection of m linearly independent hyperplanes

$$\sum_{k \in \mathcal{L}_i} Q_k = C_{\mathcal{L}_i}, \qquad 1 \leq i \leq m, \tag{20}$$

defined by the family of sets $\{\mathcal{L}_i; 1 \leq i \leq m\}$ can be described by an equivalent set of equations

$$\sum_{k \in \mathcal{K}_i} Q_k = C_{\mathcal{K}_i}, \qquad 1 \leq i \leq m, \tag{21}$$

for some family of sets distinct $\mathcal{K}_i \subseteq \{1, 2, \ldots, m\}$ that form a *maximal chain* in the sense of

$$\emptyset = \mathcal{K}_0 \subset \mathcal{K}_1 \subset \mathcal{K}_2 \subset \cdots \subset \mathcal{K}_m = \{1, 2, \ldots, m\}. \tag{22}$$

Since there exists a permutation π such that $\forall i$, $\pi[m-i+1, m] = \mathcal{K}_i$ this implies that all the vertices of $P_{\mathcal{H}}$ are in $\mathcal{Q}$. The main tool we have have at our disposal in order to prove this proposition is Corollary 5.4, which we will use extensively.

Proof of Proposition 5.6: Let $\{\mathcal{L}_i\}_{i=1}^m$ be the subsets of $\{1, 2, \ldots, m\}$ for which the inequalities are saturated and define $\mathcal{L}_i^{\mathcal{S}} := \mathcal{L}_i \cap \mathcal{S}$, the intersection of $\mathcal{L}_i$ with some set $\mathcal{S} \subseteq \{1, 2, \ldots, m\}$.

Construct the directed graph $G = (V, E)$, where:

- $V = \{1, 2, \ldots, m\}$, i.e. the vertices are the numbers from 1 to m;
- $E = \{(j, k) \; : \; (\forall i) \; j \in \mathcal{L}_i \implies k \in \mathcal{L}_i \}$, i.e. there is an edge from vertex j to vertex k if whenever vertex j occurs in the given subsets, then so does vertex k.

Now G has to be acyclic by Lemma 5.5, so it has a topological sorted order. Let us call this order ν. Let $\mathcal{K}_0 = \emptyset$ and let

$$\mathcal{K}_l = \{\nu_{m-l+1}, \ldots, \nu_m\} \tag{23}$$

for $l \in \{1, \ldots, m\}$. The sets $\mathcal{K}_l$, which consist of the last l vertices according to the ordering ν, form a maximal chain $\mathcal{K}_0 \subset \mathcal{K}_1 \subset \cdots \subset \mathcal{K}_{m-1} \subset \mathcal{K}_m$ by construction.

We claim that all the sets $\mathcal{K}_l$ can be constructed from the sets $\{\mathcal{L}_i\}$ by using unions and intersections as dictated by Corollary 5.4. The statement is true for $\mathcal{K}_m = \{1, 2, \ldots, m\}$ because every variable must appear in some constraint equation, giving $\mathcal{K}_m = \cup_i \mathcal{L}_i$. The statement is also true for $\mathcal{K}_{m-1} = \{\nu_2, ..., \nu_m\}$ since the vertex ν_1 has no in-edges in G by the definition of a topological sort, which means that

$$\mathcal{K}_{m-1} = \bigcup_{\nu_1 \notin \mathcal{L}_i^{\mathcal{K}_m}} \mathcal{L}_i^{\mathcal{K}_m}. \tag{24}$$

For the induction statement, let $l \in \{m-1, \ldots, 2, 1\}$ and assume that $\mathcal{K}_l = \bigcup_i \mathcal{L}_i^{\mathcal{K}_l}$. Since the vertex ν_{m-l} has no in-edges in the induced subgraph generated by the vertices $\mathcal{K}_l$ by the definition of the topological sort, $\mathcal{K}_{l-1}$ can be obtained from the union of all the sets not containing ν_{m-l}:

$$\mathcal{K}_{l-1} = \bigcup_{\nu_{m-l} \notin \mathcal{L}_i^{\mathcal{K}_l}} \mathcal{L}_i^{\mathcal{K}_l}. \tag{25}$$

In more detail, we claim that for all $\omega \neq \nu_{m-l} \in \mathcal{K}_{l-1}$ there exists i such that $\nu_{m-l} \notin \mathcal{L}_i^{\mathcal{K}_l}$ and $\omega \in \mathcal{L}_i^{\mathcal{K}_l}$. If it were not true, that would imply the existence of $\omega \neq \nu_{m-l} \in \mathcal{K}_{l-1}$ such that for all i, $\nu_{m-l} \in \mathcal{L}_i^{\mathcal{K}_l}$ or $\omega \notin \mathcal{L}_i^{\mathcal{K}_l}$. This last condition implies that whenever $\omega \in \mathcal{L}_i^{\mathcal{K}_l}$ it is also true that $\nu_{m-l} \in \mathcal{L}_i^{K_l}$, which corresponds to an edge (ω, ν_{n-l}) in the induced subgraph. ■

We have shown that every vertex can be written in precisely the same form as equation (11) and is therefore a point in $\mathcal{Q}$. This proves $vertices(P_{\mathcal{H}}) \subseteq \mathcal{Q}$, which together with the result of Step 1, implies $vertices(P_{\mathcal{H}}) = \mathcal{Q}$.

Step 3: Cone Part The generating vectors of the cone part of $P_{\mathcal{H}}$ are all vectors that satisfy the homogeneous versions of the halfspace inequalities (13), which in our case are

$$\sum_{k \in \mathcal{K}} Q_k \geq 0, \qquad \mathcal{K} \subseteq \{1, \ldots, m\}. \tag{26}$$

These inequalities are satisfied if and only if $Q_k \geq 0$ for all k. The cone part of $P_{\mathcal{H}}$, therefore, is given by $cone(\vec{e}_1, \ldots, \vec{e}_m)$.

This completes our demonstration that $P_{\mathcal{V}}$ is the $\mathcal{V}$-polyhedron description of the $\mathcal{H}$-polyhedron $P_{\mathcal{H}}$ and by extension the proof of Theorem 4.1.

VI. Discussion

We have shown how to build protocols for multiparty distributed compression out of the two-party fully quantum Slepian-Wolf protocol. The resulting achievable rates generalize those found in [15] for the two-party case and, for the most part, the arguments required are direct generalizations of those required for two parties. The most interesting divergence is to be found in section V, where we characterize the multiparty rates that can be achieved starting from sequential applications of the two-party protocol. The proof we obtained uses a sufficient level of mathematical abstraction so as to apply to other problems in information theory involving multiparty rate regions proved in terms of achievable points but expressed instead in terms of facet inequalities like for example, the rate regions for the classical multiparty Slepian-Wolf problem [16] and the multiparty state merging protocol [14].

Multiparty compression joins entanglement distillation, entanglement-assisted communication, channel simulation, communication over quantum broadcast channels, state redistribution [19] and many other protocols in the list of protocols that can be built out of the simpler nearly-universal two-party FQSW protocol.

Multiparty FQSW can then itself be used as a building block for other multiparty protocols. For example, when classical communication between the senders and the receiver is free, combining multiparty FQSW with teleportation reproduces the multiparty state merging protocol of [14]. Running the protocol backwards in time yields an optimal reverse Shannon theorem for broadcast channels [3].

The multiparty fully quantum Slepian-Wolf protocol is an optimal solution to the distributed compression problem for separable states, i.e. states of the form

$$\varphi^{X_1 \cdots X_m} = \sum_i p_i \varphi_i^{X_1} \otimes \varphi_i^{X_2} \otimes \cdots \otimes \varphi_i^{X_m},$$

because $E_{\text{sq}} = 0$ for such states. For general states, we have provided an outer bound on the set of achievable rates based on the multiparty squashed entanglement.

We are thus left with some compelling open problems. The most obvious is, of course, to close the gap between our inner and outer bounds on distributed compression. While that may prove to be difficult, some interesting related questions may be easier. For example, can the gap between the rate region we have presented here and the true distributed compression region be characterized by an entanglement measure? That is, while we have used the multiparty squashed entanglement as a correction term, could it be that the true correction term is an entanglement monotone?

Acknowledgments

We would like to thank L. Chindelevitch, F. Dupuis, M. Horodecki, J. Oppenheim and A. Winter for helpful comments on the subjects of distributed compression and squashed entanglement. The authors gratefully acknowledge funding from the Alfred P. Sloan Foundation, the Canada Research Chairs program, CIFAR, FQRNT, MITACS, NSERC and QuantumWorks.

References

[1] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, 1991.

[2] D. Leung, J. Oppenheim, and A. Winter, "Quantum network communication – the butterfly and beyond," 2006, arXiv:quant-ph/0608223.

[3] P. Hayden and F. Dupuis, "An optimal reverse shannon theorem for quantum broadcast channels," 2007, in preparation.

[4] D. Avis, P. Hayden, and I. Savov, "Multiparty distributed compression and squashed entanglement," 2007, arXiv:0707.2792.

[5] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland, "Reversibility of local transformations of multiparticle entanglement," *Quant. Inf. Proc.*, vol. 4, no. 3, pp. 241–250, 2005, arXiv:quant-ph/9912039.

[6] V. Coffman, J. Kundu, and W. K. Wootters, "Distributed entanglement," *Phys. Rev. A*, vol. 61, p. 052306, 2000, arXiv:quant-ph/9907047.

[7] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, "Exact and asymptotic measures of multipartite pure-state entanglement," *Phys. Rev. A*, vol. 63, no. 1, p. 012307, Dec 2000, arXiv:quant-ph/9908073.

[8] I. Devetak, A. W. Harrow, and A. Winter, "A family of quantum protocols," *Phys. Rev. Lett.*, vol. 93, p. 230504, 2004, arXiv:quant-ph/0308044.

[9] I. Devetak, A. W. Harrow, and A. Winter, "A resource framework for quantum shannon theory," 2005, arXiv:quant-ph/0512015.

[10] C. E. Shannon, "A mathematical theory of communication," *Bell Sys. Tech. Journal*, vol. 27, pp. 379–423,623–656, 1948.

[11] B. Schumacher, "Quantum coding," *Phys. Rev. A*, vol. 51, pp. 2738–2747, 1995, doi:10.1103/PhysRevA.51.2738.

[12] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, 1973. [Online]. Available: http://web.mit.edu/6.962/www/www_fall_2001/kusuma/slepwolf.pdf

[13] C. Ahn, A. Doherty, P. Hayden, and A. Winter, "On the distributed compression of quantum information," *IEEE Trans. Inf. Theory*, vol. 52, p. 4349, 2006, arXiv:quant-ph/0403042.

[14] M. Horodecki, J. Oppenheim, and A. Winter, "Quantum state merging and negative information," 2005, arXiv:quant-ph/0512247.

[15] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, "The mother of all protocols: Restructuring quantum information's family tree," 2006, arXiv:quant-ph/0606225.

[16] T. Cover, "A proof of the data compression theorem of Slepian and Wolf for ergodic sources," *IEEE Trans. Inf. Theory*, vol. 21, no. 2, pp. 226–228, 1975.

[17] B. Schumacher, “Sending entanglement through noisy quantum channels,” *Phys. Rev. A*, vol. 54, pp. 2614–2628, 1996, arXiv:quant-ph/9604023.

[18] F. Dupuis and P. Hayden, “A father protocol for quantum broadcast channels,” 2006, arXiv:quant-ph/0612155.

[19] I. Devetak and J. Yard, “The operational meaning of quantum conditional information,” 2006, arXiv:quant-ph/0612050.

[20] G. M. Ziegler, *Lectures on polytopes*. New York: Springer-Verlag, 1995.

[21] J. Edmonds, “Submodular functions, matroids, and certain polyhedra,” *Proc. Calgary Int. Conf. Combinatorial Structures and Algorithms*, pp. 69–87, June 1969, (Reprinted in *LNCS* 2570:11–26, 2003).

[22] D. Yang, K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, “Squashed entanglement for multipartite states and entanglement measures based on the mixed convex roof,” 2007, arXiv:0704.2236.

[23] M. Christandl and A. Winter, “Squashed entanglement - an additive entanglement measure,” *J. Math. Phys.*, vol. 45, p. 829, 2004, arXiv:quant-ph/0308088.

[24] P. Hayden and A. Winter, “Achievable rates for multiparty distributed compression,” 2006, unpublished.