Cooperation for the Classical-Quantum Multiple Access Channel

H. Boche, J. Nötzel
Lehrstuhl für Theoretische Informationstechnik, Technische Universität München
Email: {boche, janis.noetzel}@tum.de

Abstract—**We prove coding theorems for two scenarios of cooperating encoders for the multiple access channel with two classical inputs and one quantum output. In the first scenario (ccq-MAC with common message), the two senders each have their private messages, but would also like to transmit common messages. In the second scenario (ccq-MAC with conferencing encoders), each sender has its own set of messages, but they are allowed to use a limited amount of noiseless classical communication amongst each other prior to encoding their messages. This conferencing protocol may depend on each individual message they intend to send. The two scenarios are related to each other not only in spirit - the existence of a capacity-achieving construction scheme for codes for the ccq-MAC with common messages is used for proving the existence of another such scheme for the ccq-MAC with conferencing encoders.**

I. Introduction

The classical multiple access channel (MAC) was introduced by Shannon [11], who also started to analyze it. Later, Ahlswede [1] and Liao [8] proved full coding theorems.

In 1983 Willems published the work [18], introducing the model of a MAC with conferencing encoders and providing a complete coding theorem with a weak converse.

In this model, each of the encoders wants to transmit a set of messages. In contrast to the usual MAC model, they can both gain at least partial knowledge of the other sender's message through *conferencing*: An iterative and noiseless exchange of messages under some given rate constraint. The question then is, how the capacity region of the MAC with conferencing encoders depends on the allowed rates of the conference. Willems [18] reduced the direct part to an application of the coding theorem for the MAC with a common messages that had been solved in [13].

The model fits into a broader range of problems in which partial cooperation between different parties of some communication scenario is allowed and that has attracted a lot of attention recently: see for example [5], [16], [6], [9], [14], [15], [12].

In the present paper we extend the results of Willems to quantum channels. More precisely, we consider two senders, both of which are connected to the receiver by a ccq-MAC, a generalization of the classical setting in which the outputs of the channel are quantum states. Both senders transmit their classical messages to one receiver, who tries to decode them. A full solution of the coding problem for the ccq-MAC without conferencing has been achieved by Winter [20] in 2001. In 2012 Fawzi, Hayden, Savov, Sen and Wilde [7] provided a different proof of the direct part of the coding theorem for the ccq-MAC, enabling the receiver to decode both messages *simultaneously*.

We use this rather recent result together with a coding theorem for cq-channels that was developed by Winter in [19] and has the property that at least partial control on the codewords is given: They all have approximately the same type. Nonetheless, the codes whose existence are guaranteed by the theorem are still randomly chosen. Together, these results enable us to prove the direct part of a coding theorem for the ccq-MAC with conferencing encoders. Like in the classical case, we allow the two senders to exchange messages amongst each other prior to encoding the messages that ought to be sent to the receiver. A very brief formulation of our main result then reads as follows:

Conferencing can enlarge the capacity region of a ccq-MAC.

Of course, much more is proven hereafter. And in the classical setting, much more is also known already: Conferencing can for example stabilize the communication between two senders and one receiver when the communication line between the legal users is being actively manipulated by an evil party in order to prevent the communication. Good codes in such a setting are robust against a large class of clearly specified attacks, making them a good choice for applications in security applications. The impact of conferencing on such systems is strong: a tiny amount of conferencing can already boost the capacity from zero up to the maximally attainable value [15]. The existence of a similar result for the quantum case seem to be a reasonable assumption, and the present paper is a first step into that direction.

II. Notation

All Hilbert spaces are assumed to have finite dimension and are over the field $\mathbb{C}$. The set of linear operators from $\mathcal{H}$ to $\mathcal{H}$ is denoted $\mathcal{B}(\mathcal{H})$. The adjoint of $b \in \mathcal{B}(\mathcal{H})$ is marked by a star and written b^*.

$\mathcal{S}(\mathcal{H})$ is the set of states, i.e. positive semi-definite operators with trace (the trace function on $\mathbb{B}(\mathcal{H})$ is written tr) 1 acting on the Hilbert space $\mathcal{H}$. Pure states are given by projections onto one-dimensional subspaces. A vector $x \in \mathcal{H}$ of unit length spanning such a subspace will therefore be referred to as a state vector, the corresponding state will be written $|x\rangle\langle x|$. For a finite set $\mathbf{X}$ the notation $\mathfrak{P}(\mathbf{X})$ is reserved for the set of probability distributions on $\mathbf{X}$, and $|\mathbf{X}|$ denotes its cardinality.

978-1-4799-5186-4/14/$31.00 ©2014 IEEE

For any $l \in \mathbb{N}$, we define $\mathbf{X}^l := \{(x_1, \ldots, x_l) : x_i \in \mathbf{X}\ \forall i \in \{1, \ldots, l\}\}$, we also write x^l for the elements of $\mathbf{X}^l$. Associated to every such element is a function $N(\cdot|x^l) : \mathbf{X} \to \mathbb{N}$ defined by $N(x|x^l) := |\{i : x_i = x\}|$.
The set of classical-quantum channels (abbreviated here using the term 'cq-channels') with finite input alphabet $\mathbf{Z}$ and output system $\mathcal{K}$ is denoted $CQ(\mathbf{Z}, \mathcal{K})$.
For any natural number N, we define $[N]$ to be the shortcut for the set $\{1, ..., N\}$.
Using the usual operator ordering symbols $\leq$ and $\geq$ on $\mathcal{B}(\mathcal{H})$ and suppressing the dependence on $\mathcal{H}$, the set of positive operator valued measurements (POVMs) with $N \in \mathbb{N}$ different outcomes is written

$$\mathcal{M}_N := \{\mathbf{D} = (D_i)_{i=1}^N : \sum_{i=1}^N D_i \leq \mathbb{1}_{\mathcal{H}},\ D_i \geq 0\ \forall i \in [N]\}.$$

To every $\mathbf{D} \in \mathcal{M}_N(\mathcal{H})$ there corresponds a unique operator defined by $D_0 := \mathbb{1}_{\mathcal{H}} - \sum_{i=1}^N D_i$. Throughout the paper, we will assume that $D_0 = 0$ holds. This is possible in our scenario, since adding the element D_0 to any of the other $D_1, \ldots, D_N$ does not decrease the performance of a given code.
The von Neumann entropy of a state $\rho \in \mathcal{S}(\mathcal{H})$ is given by

$$S(\rho) := -\mathrm{tr}(\rho \log \rho),$$

where $\log(\cdot)$ denotes the base two logarithm which is used throughout the paper.
The Holevo information is for a given channel $\mathcal{W} \in CQ(\mathbf{Z}, \mathcal{H})$ and input probability distribution $p \in \mathfrak{P}(\mathbf{X})$ defined by

$$\chi(p, \mathcal{W}) := S(\overline{\mathcal{W}}) - \sum_{z \in \mathbf{Z}} p(z) S(\mathcal{W}(z)),$$

where $\overline{\mathcal{W}}$ is defined by $\overline{\mathcal{W}} := \sum_{z \in \mathbf{Z}} p(z)\mathcal{W}(z)$. We shall employ a slightly different notation that is closer to the one used in the classical scenario. To the distribution p we can always associate a random variable Z with values in $\mathbf{Z}$ that is distributed according to p. If we label the physical system that is modelled on the Hilbert space $\mathcal{K}$ by Q, we can define

$$I(Z; Q) := \chi(p, \mathcal{W}).$$

It is clear that this is a quantum mutual information - given a bipartite random variable (X, Y), its mutual information $I(X, Y)$ is given by $I(X, Y) := H(X) + H(Y) - H(X, Y)$. If our channel has a bipartite input ($\mathbf{Z} = \mathbf{X} \times \mathbf{Y}$), and (X, Y) is a random variable on $\mathbf{X} \times \mathbf{Y}$ that is distributed according to $\mathbb{P}((X, Y) = (x, y)) = p(y)q(x|y)$ it even makes sense to define the quantity

$$I(X; Q|Y) := \sum_{y \in \mathbf{Y}} p(y)\chi(q(\cdot|y), \mathcal{W}(\cdot \times y)).$$

Whenever necessary, the elements x of some finite set $\mathbf{X}$ will be identified with a set $\{|x\rangle\langle x|\}_{x \in \mathbf{X}} \subset B(C^{|\mathbf{X}|})$ of matrix units that are pairwise orthogonal (with respect to the Hilbert Schmidt inner product).

III. Definitions

In the remainder, $\mathcal{W} \in \mathcal{C}(\mathbf{X} \times \mathbf{Y}, \mathcal{K})$ will denote a classical, classical - quantum multiple access channel (ccq-MAC). The quantum part of the system will also be referred to by the symbol Q and, given a probability distribution on the input system of the channel, the corresponding random variable will be written (X, Y). Further random variables may arise.

Definition 1 (Codes for the ccq-MAC with conferencing encoders)**.** *For given $l \in \mathbb{N}$, an (M_l, N_l, C, D) code $\mathfrak{C}_l$) for the ccq-MAC with encoders conferencing at rates $C \geq 0$ and $D \geq 0$ consists of:*

1) *Two natural numbers M_l and N_l that form the message sets $[M_l]$ and $[N_l]$.*
2) *Positive numbers C, D that give upper bounds on the overall rate of a* conference. *This conference consists of: a natural number $K \in \mathbb{N}$, finite message sets $V_{l,1}, \ldots, V_{l,K}$ and $W_{l,1}, \ldots, W_{l,K}$ ($V_{l,0} = W_{l,0} = \emptyset$ in order to have more compact notation) and conferencing functions*

$$f_{l,i} : [M_l] \times (\times_{j=0}^{i-1} W_{l,j}) \times (\times_{j=0}^{i-1} V_{l,j}) \mapsto V_{l,i}, \quad i \in [K], \qquad g_{l,i} :$$

s.t. $\sum_{k=1}^K \log|V_{l,k}| \leq C$ and $\sum_{k=1}^K \log|W_{l,k}| \leq D$. The outcomes of the conference are stored in the set $U_l := \prod_{i=1}^K W_i \times \prod_{i=1}^K V_i$. If the codewords (n, m) were sent, they are given by arrays that will be written

$$\mathcal{C}_l(m, n) =$$
$$(m, g_1(n), g_2(n, f_1(m)), g_3(n, f_1(m), f_2(m, g_1(n))), \ldots)$$
$$\mathcal{D}_l(m, n) =$$
$$(n, f_1(m), f_2(m, g_1(n)), f_3(m, g_1(n), g_2(n, f_1(m))), \ldots).$$

3) *Two functions f_l and g_l such that f_l takes as inputs the outcomes $\mathcal{C}_l(m, n)$ and g_l the outcomes $\mathcal{D}_l(m, n)$ of the conference and f_l outputs a corresponding codeword in $\mathbf{X}^l$, while g_l gives one in $\mathbf{Y}^l$.*
4) *A POVM $\mathbf{D}^l = \{D_{mn}^l\}_{m,n=1}^{M_l, N_l} \in \mathcal{M}_{M_l \cdot N_l}$ on $\mathcal{K}^{\otimes l}$.*
5) *We can write the average success probability $p_{\mathrm{s}}(\mathfrak{C}_l)$ of the code $\mathfrak{C}_l$ as*

$$\frac{1}{M_l N_l} \sum_{m,n=1}^{M_l, N_l} \mathrm{tr}\{D_{mn}^l \mathcal{W}^{\otimes l}(f_l(\mathcal{C}_l(m, n)), g_l(\mathcal{D}_l(m, n)))\}.$$

Definition 2 (Achievability for the ccq-MAC with conferencing encoders)**.** *A pair (R_M, R_N) of nonnegative real numbers is said to be achievable for the ccq-MAC with encoders conferencing at rates $C \geq 0$ and $D \geq 0$ if there is a sequence $(\mathfrak{C}_l)_{l \in \mathbb{N}}$ of codes as in Definition 1 with conferencing rates C and D such that*

$$\liminf_{l \to \infty} \frac{1}{l} \log M_l \geq R_M, \quad \liminf_{l \to \infty} \frac{1}{l} \log N_l \geq R_N$$
$$\text{and} \quad \liminf_{l \to \infty} p_{\mathrm{s}}(\mathfrak{C}_l) = 1.$$

Definition 3 (Capacity region of the ccq-MAC with conferencing encoders)**.** *The capacity region $C(\mathcal{W}, C, D)$ of the ccq-MAC with encoders conferencing at rates $C \geq 0$ and $D \geq 0$*

is defined to be the closure of the set of all rates that are achievable (for the ccq-MAC, with conferencing at rates C and D).

Definition 4 (Codes for the ccq-MAC with common messages)**.** *For $l \in \mathbb{N}$, a code $\mathfrak{C}_l$ for the ccq-MAC with common messages consists of a triple (K_l, T_l, M_l) of natural numbers, two encoding functions $f_l : [K_l] \times [M_l] \to \mathbf{X}^l$, $g_l : [T_l] \times [M_l] \to \mathbf{Y}^l$, and a POVM $(\Lambda_{k,t,m})_{k,l,m=1}^{K_l,T_l,M_l}$. The success probability of the code is given by*

$$p_s(\mathfrak{C}_l) := \frac{1}{K_l T_l M_l} \sum_{k,t,l=1}^{K_l,T_l,M_l} \mathrm{tr}\{\Lambda_{k,t,l} \mathcal{W}^{\otimes l}(f_l(k,m), g_l(t,m))\}.$$

Definition 5 (Achievability for the ccq-MAC with common messages)**.** *A triple (S_X, S_Y, S_C) of nonnegative real numbers is said to be achievable for the ccq-MAC with a common message if there exists a sequence of $(\mathfrak{C}_l)_{l\in\mathbb{N}}$ of codes as in Definition 4 such that*

$$\liminf_{l\to\infty} \frac{1}{l} \log K_l \geq S_X, \quad \liminf_{l\to\infty} \frac{1}{l} \log T_l \geq S_Y,$$
$$\liminf_{l\to\infty} \frac{1}{l} \log M_l \geq S_C \quad \text{and} \quad \liminf_{l\to\infty} p_s(\mathfrak{C}_l) = 1.$$

Definition 6 (Capacity region of the ccq-MAC with common messages)**.** *The capacity region of the ccq-MAC $\mathcal{W}$ with common message is given by the closure of the set of all rate triples that are achievable (for $\mathcal{W}$, with common message).*

IV. Main Results

Our main results are two complete coding theorems: One for the ccq-MAC with conferencing encoders, the other for the ccq-MAC with a common message. This joint presentation is not just by chance: The direct part of the coding theorem for the model with a joint message serves as a building block for the model with conferencing senders.

We now state our theorems, in the same order as their proofs are given later. The first one is an outer bound on the capacity region of a ccq-MAC with conferencing encoders:

Theorem 1 (Converse of the coding theorem for ccq-MAC with conferencing encoders)**.** *For the ccq-MAC with conferencing encoders, a rate pair (R_X, R_Y) is achievable only if it is contained in the set*

$$\mathfrak{R}_{\mathrm{conf}}(\mathcal{W}, C, D) := \mathrm{cl}(\cup_p \mathfrak{R}_{p,\mathrm{conf}}(\mathcal{W}, C, D)) \tag{1}$$

defined by the sets $\mathfrak{R}_{p,\mathrm{conf}}(\mathcal{W}, C, D)$ of all pairs of real nonnegative numbers (R_N, R_M) satisfying

$$R_M \leq I(X;Q|Y,U) + C \tag{2}$$
$$R_N \leq I(Y;Q|X,U) + D \tag{3}$$
$$R_M + R_N \leq I(X,Y;Q|U) + C + D \tag{4}$$
$$R_M + R_N \leq I(X,Y;Q) \tag{5}$$

where the states used to evaluate the entropic quantities on the right hand sides are defined by

$$\sum_{u,x,y} p(u,x,y) |u\rangle\langle u| \otimes |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \mathcal{W}(x,y) \tag{6}$$

and the distribution $p \in \mathfrak{P}(\mathbf{U} \times \mathbf{X} \times \mathbf{Y})$ can be decomposed such that $p(u,x,y) = q(u)r(x|u)s(y|u)$ for suitable distributions $q \in \mathfrak{P}(\mathbf{U})$, where $s(\cdot|u) \in \mathfrak{P}(\mathbf{X})$ and $r(\cdot|u) \in \mathfrak{P}(\mathbf{Y})$ for every $u \in \mathbf{U}$. Finally, the cardinality of the alphabet $\mathbf{U}$ can be restricted by the cardinality bound $|\mathbf{U}| \leq |\mathcal{X}| \cdot |\mathcal{Y}| + 3$.

Second, we prove the existence of codes that transmit common messages as well as individual messages of two senders over a ccq-MAC with asymptotically vanishing average error probability, at certain rates. This means that we can give an inner bound on the capacity region of that model. The result is used afterwards to obtain a direct coding theorem for the ccq-MAC with conferencing encoders as well.

Theorem 2 (Direct part of coding theorem for the ccq-MAC with a common message)**.** *Every rate triple (R_C, R_X, R_Y) satisfying $(R_C, R_X, R_Y) \in \mathfrak{R}_{\mathrm{comm}}(\mathcal{W})$ is achievable. The convex set $\mathfrak{R}_{\mathrm{comm}}(\mathcal{W})$ is given by*

$$\mathfrak{R}_{\mathrm{comm}}(\mathcal{W}) = \mathrm{cl}(\cup_q \mathfrak{R}_{q,\mathrm{comm}}(\mathcal{W})), \tag{7}$$

where the sets $\mathfrak{R}_{q,\mathrm{comm}}(\mathcal{W})$ are given by all triples (S_C, S_X, S_Y) satisfying below inequalities for a distribution $q \in \mathbf{U} \times \mathbf{X} \times \mathbf{Y}$ having the structure $q(x,y,u) = p(u)r(x|u)s(y|u)$ $\forall (u,x,y) \in \mathbf{U}\times\mathbf{X}\times\mathbf{Y}$ and with the overall cq state being $\sum_{u,x,y} q(u,x,y)|u\rangle\langle u| \otimes |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \mathcal{W}(x,y)$.

$$S_X \leq I(X;Q|Y,U) \tag{8}$$
$$S_Y \leq I(Y;Q|X,U) \tag{9}$$
$$S_X + S_Y \leq I(X,Y;Q|U) \tag{10}$$
$$S_C + S_X + S_Y \leq I(X,Y;Q) \tag{11}$$

As was the case in the classical paper [18] by Willems, the existence of a coding result for the ccq-MAC with private and common messages enables one to prove the direct part of the coding theorem for the ccq-MAC with conferencing encoders, leading to the following result:

Theorem 3 (Direct part of coding theorem for cc-q-MAC with conferencing encoders)**.** *Every rate pair $(R_X, R_Y) \in \mathfrak{R}_{\mathrm{conf}}(\mathcal{W})$ is achievable, thus $C(\mathcal{W}, C, D) = \mathfrak{R}_{\mathrm{conf}}(\mathcal{W}, C, D)$.*

- ► An optimal choice of encoding and decoding is already achieved by one-shot conferencing - Given the message pair (m, n), Alice sends one message to Bob and vice versa, no iterative exchange of messages is necessary!
- ► This is albeit the fact that, combinatorically, the set of general iterative conferencing strategies is much larger than the set of one-shot conferencing strategies.

At last, and in order to have a coherent and self-contained presentation, we also prove the converse theorem for the ccq-MAC with common and private messages. This part, as well as the direct part for the ccq-MAC with conferencing encoders, shows that the two models are in fact closely related from an information theoretic point of view.

Theorem 4 (Converse for the ccq-MAC with common message)**.** *For the ccq-MAC with common message, no rate triple (R_C, R_X, R_Y) outside of $\mathfrak{R}_{\text{comm}}(\mathcal{W})$ is achievable.*

Remark 1. *Above results, put together, establish the region $\mathfrak{R}_{\text{conf}}(\mathcal{W}, C, D)$ as the rate region of the ccq-MAC $\mathcal{W}$with senders conferencing at rates C, D and the region $\mathfrak{R}_{\text{comm}}(\mathcal{W})$ as the rate region for the same model but with a common message instead of conferencing senders.*

V. Sketch of Proof

We now give informal sketches of the proofs of above results. Exact details can be found in the extended version [4] of this paper on the arXiv. *Converse for conferencing encoders.* Let, for $l \in \mathbb{N}$, a code $\mathfrak{C}_l$ for conferencing encoders be given and let $P_{\text{s}}(\mathfrak{C}_l) = 1 - \varepsilon_l$. With some risk of ambiguity in notation, we introduce the following random variables: U_l, whose values are the outcomes of the conference, the values of M_l and M_l are the messages sent by Alice and Bob, and M_l', N_l' are those received by Charlie. The quantum system he operates on is denoted Q_l.
Obviously, the conference together with the encoding functions and their outputs, the MAC and the POVM chosen by Charlie for decoding of the messages can all together be described by a quantum state $\rho_{\mathrm{M}_l\mathrm{N}_l\mathrm{U}_l\mathrm{X}^l\mathrm{Y}^l\mathrm{Q}_l\mathrm{M}_l'\mathrm{N}_l'}$, which shall be abbreviated as ρ in the sequel.
The Holevo bound in combination with strong subadditivity then yields

$$S(\mathrm{M}_l, \mathrm{N}_l | \mathrm{Q}_l, \mathrm{U}_l) \leq \delta_l \tag{12}$$

for some suitably chosen sequence δ_l satisfying $\delta_l \searrow 0$. Since the information in the classical parts of ρ can be copied, after a few steps one derives

$$\log M_l \leq I(\mathrm{M}_l; \mathrm{U}_l|\mathrm{N}_l) + I(\mathrm{M}_l; \mathrm{Q}_l|\mathrm{N}_l, \mathrm{U}_l) + \delta_l \tag{13}$$
$$\log N_l \leq I(\mathrm{M}_l; \mathrm{U}_l|\mathrm{M}_l) + I(\mathrm{M}_l; \mathrm{Q}_l|\mathrm{M}_l; \mathrm{U}_l) + \delta_l \tag{14}$$
$$\log N_l M_l \leq I(\mathrm{M}_l, \mathrm{M}_l; \mathrm{U}_l) + I(\mathrm{M}_l, \mathrm{M}_l; \mathrm{Q}_l|\mathrm{U}_l) + \delta_l. \tag{15}$$

Above estimates are essentially the same as in [18], and at this point the problem clearly splits up into a purely classical part and one that contains the quantum system Q_l. For the classical conditional mutual information terms, the inequalities (11,12,13) in [18] apply. For the other terms, one uses the independence of M_l and M_l given U_l which carries over to an independence of the input variables X_i and Y_i given U_l. With some additional care for the quantum part of the system, and using the converse for the MAC that was proven in [20] for the fourth inequality, this is sufficient to prove

$$\log(M_l) \leq I(\mathrm{M}_l; \mathrm{Q}_l|\mathrm{M}_l, \mathrm{U}_l) \leq \sum_{i=1}^{l} I(\mathrm{X}_i; \mathrm{Q}_i|\mathrm{Y}_i, \mathrm{U}_l) + \delta_l$$
$$\log(N_l) \leq I(\mathrm{M}_l; \mathrm{Q}_l|\mathrm{M}_l, \mathrm{U}_l) \leq \sum_{i=1}^{l} I(\mathrm{Y}_i; \mathrm{Q}_i|\mathrm{X}_i, \mathrm{U}_l) + \delta_l$$
$$\log N_l M_l \leq I(\mathrm{M}_l, \mathrm{M}_l; \mathrm{Q}_l|\mathrm{U}_l) \leq \sum_{i=1}^{l} I(\mathrm{X}_i, \mathrm{Y}_i; \mathrm{Q}_i|U^l) + \delta_l$$
$$\log N_l M_l \leq I(\mathrm{M}_l, \mathrm{M}_l; \mathrm{Q}_l) \leq \sum_{i=1}^{l} I(\mathrm{X}_i, \mathrm{Y}_i; \mathrm{Q}_i) + \delta_l.$$

By regularizing above inequalities using a factor $\frac{1}{l}$ one can, with some extra care, prove that this implies that every achievable rate pair (R_A, R_B) is contained in $\mathfrak{R}_{\text{conf}}(\mathcal{W})$.

Direct part for MAC with conferencing encoders. The proof of the direct part is carried out by resorting back to Theorem 3: Consider the two senders with conferencing capacities C, D attempting to send messages at rates R_M, R_N. Define the numbers $c := \min\{R_M, C\}$ and $d := \min\{R_N, D\}$, and make a disjoint partitioning of the message set $[\lfloor 2^{nR_M} \rfloor] = \cup_{i=1}^{c} M_i$ into subsets all having the same size, and the same for the other sender: $[\lfloor 2^{nR_N} \rfloor] = \cup_{i=1}^{d} N_i$. The senders now send as a conferencing message the index of the partition that their message is chosen from, and the conferencing only uses this one step.
The pairs (i, j) of indices numbering the partitions can then be considered a common message of the two senders, and the code for the ccq-MAC with a common message from Theorem 2 is used. The requirement that all the sets N_i, M_i are of the same size ensures that (i, j) is evenly distributed, and this is true with a small and asymptotically vanishing error.

Direct part for MAC with common message. Take any finite set $\mathbf{U}$. At the heart of this proof is Theorem 10 in [20], which guarantees the existence of a sequence of codes for stationary memoryless classical-quantum channels $\mathcal{T} \in CQ(\mathbf{U}, \mathcal{K})$, with asymptotic rate approximately $\chi(q; \mathcal{T})$ for every $q \in \mathfrak{P}(\mathbf{U})$ and all codewords approximately q-typical.
We then take an arbitrary $q \in \mathfrak{P}(\mathbf{U})$ and conditional probability distributions $\{r(\cdot|u)\}_{u \in \mathbf{U}} \subset \mathfrak{P}(\mathbf{X})$ and $\{s(\cdot|u)\}_{u \in \mathbf{U}} \subset \mathfrak{P}(\mathbf{Y})$ which define a new channel $\mathcal{V} \in CQ(\mathbf{U}, \mathcal{K})$ by

$$\mathcal{V}(u) := \sum_{x \in \mathbf{X}} \sum_{y \in \mathbf{Y}} r(x|u) s(y|u) \mathcal{W}(x, y). \tag{16}$$

Then Theorem 10 in [20] delivers a good code for message transmission over $\mathcal{V}$, and we use it for transmission of the common message. For the transmission of the private messages, we make heavy use of the fact that all codewords for transmission of the common message have basically the same type.
Consider a fixed l and one codeword u^l, and assume for sake

of a short enough argument for the moment, that $\mathbf{U} = \{0,1\}$ and $u = (0,\dots,0,1,\dots,1)$ contains approximately $l \cdot q(0)$ zeros. On the first block of length $l \cdot q(0)$ we use the recent results of [7] to obtain a code for $\mathcal{W}$ with codewords sampled i.i.d. according to $r(\cdot|0)s(\cdot|0)$, and on the second block we do the same but sample according to $r(\cdot|1)s(\cdot|1)$.

This can be done for each of the codewords u at the same time, due to the random structure of the argument. After some amount of careful algebra, this enables one to show the existence of natural numbers K, T, M and a $POVM$ $\{\Delta_{k,t,m}\}_{k,t,m}^{K,T,M}$ on $\mathcal{K}^{\otimes l}$, and encoding functions $f_m, g_m : [K], [L] \to \mathbf{X}^l, \mathbf{Y}^l$ $(m \in [M])$ such that for the corresponding code $\mathfrak{C}_l$ it holds

$$p_{\mathrm{s}}(\mathfrak{C}_l) \geq 1 - \min_{m\in[M_l]} \sum_{u\in\mathbf{U}} \nu(l_u^m) - 6\sqrt{l^{-1/4}} \qquad (17)$$

holds, for large enough $l \in \mathbb{N}$ and some function $\nu : \mathbb{N} \to \mathbb{R}$ satisfying $\lim_{n\to\infty} \nu(n) = 0$ that stems from the results of [7].

Proof of the converse for the MAC with common message. The proof of this result rests on a generalization of Lemma 1 in [13]:

Lemma 1. *Let M, K, L be independent random variables with values in the finite sets $\mathbf{M}, \mathbf{K}, \mathbf{L}$, each distributed evenly on the respective set. Let $\mathcal{V} \in CQ(\mathbf{X}, \mathbf{Y}, \mathcal{K})$ and encoding functions $a : \mathbf{M} \times \mathbf{K} \to \mathbf{X}$, $b : \mathbf{M} \times \mathbf{K} \to \mathbf{Y}$ be given, as well as a POVM $\mathbf{D} \in \mathcal{M}_{|\mathbf{M}\times\mathbf{K}\times\mathbf{L}|}$ on $\mathcal{K}$. Define the distribution $p \in \mathfrak{P}(\mathbf{M}\times\mathbf{K}\times\mathbf{L}\times\mathbf{M}\times\mathbf{K}\times\mathbf{L})$ and the quantitiy p_e through*

$$p(m,k,l,\bar{m},\bar{k},\bar{l}) := \frac{\mathrm{tr}\{\mathcal{V}(a(m,k),b(m,l))D_{\bar{k}\bar{m}\bar{l}}\}}{|\mathbf{M}|\cdot|\mathbf{K}|\cdot|\mathbf{L}|},$$

$$p_e := 1 - \sum_{k,l,m} p(m,k,l,m,k,l).$$

Then for $p_e \leq 1/2$,

$$H(K|(M',K',L'),M,L) \leq p_e \log|\mathbf{K}| + 1,$$
$$H(L|(M',K',L'),M,K) \leq p_e \log|\mathbf{L}| + 1,$$
$$H(K,L|(M',K',L'),M) \leq p_e \log|\mathbf{K}|\cdot|\mathbf{L}| + 1,$$
$$H(M,K,L|M',K',L') \leq p_e \log|\mathbf{K}|\cdot|\mathbf{L}|\cdot|\mathbf{M}| + 1.$$

In a a manner similar to the proof of Theorem 1, this Lemma ultimately enables one to prove the inequalities

$$\log(K_l) \leq \sum_{i=1}^{l} I(\mathrm{X}_i;\mathrm{Q}_i|\mathrm{Y}_i,M^l) + \delta_l \qquad (18)$$

$$\log(L_l) \leq \sum_{i=1}^{l} I(\mathrm{Y}_i;\mathrm{Q}_i|\mathrm{X}_i,M^l) + \delta_l \qquad (19)$$

$$\log(K_l \cdot L_l) \leq \sum_{i=1}^{l} I(\mathrm{X}_i,\mathrm{Y}_i;\mathrm{Q}_i|M^l) + \delta_l \qquad (20)$$

$$\log(K_l \cdot L_l \cdot M_l) \leq \sum_{i=1}^{l} I(\mathrm{X}_i,\mathrm{Y}_i;\mathrm{Q}_i) + \delta_l, \qquad (21)$$

from which it follows that every achievable rate triple is an element of $\mathfrak{R}_{\mathrm{comm}}(\mathcal{W})$.

Acknowledgment

This work was supported by the DFG via grant BO 1734/20-1 (H.B.) and by the BMBF via grant 01BQ1050 (H.B., J.N.).

References

[1] R. Ahlswede, "Multiway communication channels",*Proceedings of 2nd International Symposium on Information Theory, Thakadsor, Armenian SSR, Akademiai Kiado, Budapest*, 2352 (1971)

[2] R. Ahlswede, J. Körner "Source Coding with Side Information and a Converse for Degraded Broadcast Channels", *IEEE Trans. Inf. Theory*, Vol. 21, Iss. 6, 629 - 637 (1975)

[3] R. Ahlswede, "Elimination of Correlation in Random Codes for Arbitrarily Varying Channels", *Z. Wahrscheinlichkeitstheorie verw. Gebiete* 44, 159-175 (1978)

[4] H. Boche, J. Nötzel, "The Classical-Quantum Multiple Access Channel with Conferencing Encoders and with Common Messages ", *arXiv:1310.1970* (2013)

[5] S. Bross, A. Lapidoth, and M. Wigger, "The Gaussian MAC with conferencing encoders", *Proc. IEEE International Symposium on Information Theory (ISIT 2008)*, 2702-2706, (2008)

[6] H. T. Do, T. J. Oechtering, and M. Skoglund, "The Gaussian Z-Interference Channel with Rate-Constrained Conferencing Decoders", *Proc. IEEE International Conference on Communications (ICC), Cape Town, South Africa*, (2010)

[7] O. Fawzi, P. Hayden, I. Savov, P. Sen, M. M. Wilde, "Classical Communication Over a Quantum Interference Channel", *IEEE Trans. Inf. Theory*, Vol 58, Iss. 6, 3670 - 3691 (2012)

[8] H. H.-J. Liao, "Multiple access channels", *Ph.D. dissertation, University of Hawaii, Honolulu, HI*, (1972).

[9] I. Maric, R. Yates, and G. Kramer, "Capacity of Interference Channels With Partial Transmitter Cooperation", *IEEE Trans. Inf. Theory*, Vol. 53, Iss. 10, 3536-3548 (2007)

[10] C. T. K. Ng, I. Maric, A. J. Goldsmith, S. Shamai (Shitz), and R. D. Yates. "Iterative and One-shot Conferencing in Relay Channels", *Proc. IEEE Information Theory Workshop, Punta del Este, Uruguay*, (2006)

[11] C. E. Shannon, "Two-way communication channels", *Proc. 4th Berkeley Symp. Math. Statist. Probability, Berkeley, CA*, Vol. 1, 611-644 (1961)

[12] O. Simeone, D. Gunduz, H. V. Poor, A. J. Goldsmith, and S. Shamai, "Compound Multiple-Access Channels With Partial Cooperation", *IEEE Trans. Inf. Theory*, Vol. 55, Iss. 6, 2425-2441 (2009)

[13] D. Slepian, J. K. Wolf, "A Coding Theorem for Multiple Access Channnels With Correlated Sources", *Bell Syst. Tech. J.*, Vol. 52, No. 7, 1037 - 1076 (1973)

[14] M. Wiese, H. Boche, I. Bjelakovic, V. Jungnickel, "The Compound Multiple Access Channel With Partially Cooperating Encoders", *IEEE Trans. Inf. Theory*, Vol. 57, Iss. 5, 3045-3066 (2011)

[15] M. Wiese, H. Boche. "The Arbitrarily Varying Multiple-Access Channel With Conferencing Encoders" *IEEE Trans. Inf. Theory*, Vol. 59, Iss. 3, 1405-1416 (2013)

[16] M. A. Wigger, "Cooperation on the Multiple-Access Channel", *PhD thesis, ETH Zürich, Switzerland*, (2008)

[17] F. M. J. Willems, "Informationtheoretical Results for the Discrete Memoryless Multiple Access Channel", *PhD thesis, Katholieke Universiteit Leuven, Belgium*, (1982)

[18] F. M. J. Willems, "The Discrete Memoryless Multiple Access Channel with Partially Cooperating Encoders", *IEEE Trans. Inf. Theory*, Vol. 29, No. 3, 441-445 (1983)

[19] A. Winter, "Coding Theorems of Quantum Information Theory", *PhD thesis, Universität Bielefeld, Germany*, (1999)

[20] A. Winter, "The Capacity of the Quantum Multiple Access Channel", *IEEE Trans. Inf. Theory*, Vol. 47, Iss. 7, 3059-3065 (2001)