Subadditivity of the minimum output entropy and superactivation of the classical capacity of quantum multiple access channels

Ł. Czekaj\textsuperscript{1,2}

\textsuperscript{1}Faculty of Applied Physics and Mathematics, Gdansk University of Technology, 80-952 Gdansk, Poland
\textsuperscript{2}National Quantum Information Center of Gdansk, 81-824 Sopot, Poland
lczekaj@mf.pg.gda.pl

We study subadditivity of the minimum output entropy ($H_{\text{min}}$) of quantum multiple access channels (MACs). We provide an example of violation of the additivity theorem for $H_{\text{min}}$ known in classical information theory. Our result is based on a fundamental property of MACs i.e. independence of each sender. The channels used in the example can be constructed explicitly. On the basis of subadditivity of $H_{\text{min}}$ we also provide an example of extremal superadditivity (super activation) of the classical capacity region of MACs.

PACS numbers: 03.67.Hk, 89.70.Kn

Using quantum resources like quantum entanglement \textsuperscript{1} in quantum information theory \textsuperscript{2} leads to a new class of effects, known as quantum activation, which are impossible in classical information theory \textsuperscript{2}. Some examples of quantum activation are: (i) superadditivity of the classical capacity $C$ in the fundamental case of 1-to-1 quantum channels \textsuperscript{7} where transmission of entangled states leads to capacities larger than using product states, (ii) nonlocality effect for classical capacity region $R$ of quantum multiple access channels \textsuperscript{4,5} where entanglement used by first sender increases maximal rate of an other ($R_2$) without increasing the maximal total rate $R_1 + R_2$. The effect can be quite strong as shown in \textsuperscript{6}, (iii) superactivation, i.e. extremal superadditivity, of the quantum capacity $Q$ for 1-to-1 channels where two quantum channels with 0 quantum capacities working together allow for transmission of qubits \textsuperscript{8}.

This paper addresses subadditivity of the minimum output entropy $H_{\text{min}}$ and quantum activation of the classical capacity region $R$ of the entanglement breaking \textsuperscript{24} multiple access channels (MACs) and it continues the research started in Ref. \textsuperscript{4}. Effect of the subadditivity of $H_{\text{min}}$ is manifested when transmission of entangled states produces lower entropy than transmission of any product states. The question of subadditivity of $H_{\text{min}}$ of quantum 1-to-1 channels appears to have been first considered in print in Ref. \textsuperscript{9}. In Ret. \textsuperscript{17} the equivalence between additivity of $H_{\text{min}}$ and classical capacity $C$ was stated. Finally, an example of subadditivity of $H_{\text{min}}$ for quantum 1-to-1 channels was first provided in Ref. \textsuperscript{7}, and explored further in \textsuperscript{20}. Hastings’ channels seems to be very hard to explicitly construct since this task requires a search through the set of unitary matrices. Here we study the subadditivity of $H_{\text{min}}$ in the realm of MACs. The setup we present is intrinsically MAC and cannot be reduced to the setup of 1-to-1 channels, i.e. to the case studied by Hastings. The advantage of our approach is the existence of effective algorithms allowing the explicit construction of the channels we present.

The superadditivity of $C$ in entanglement breaking MACs suggests qualitative differences between bipartite and multipartite communication since it cannot occur for entanglement breaking 1-to-1 channels. It was first pointed out in Ref. \textsuperscript{6}. Superadditivity was shown for the entanglement breaking MACs cooperating with an identity channel (which is not entanglement breaking). Here we move one step further and show that the very strong superadditivity takes place also if we use only entanglement breaking MACs.

The paper is organized as follows: first we provide definitions and theorems used in the main part of the paper. We stress on the explanation of the idea of a randomness extractor which is of paramount importance to further considerations. Then we present the main results, i.e. subadditivity of $H_{\text{min}}$ and superactivation of the classical capacity of the MACs.

BACKGROUND

A quantum channel $\Gamma$ is a linear, completely positive and trace preserving map from density matrices to density matrices $\rho \rightarrow \Gamma(\rho)$ \textsuperscript{2} and it models transmission of quantum states in the presence of noise. An entanglement breaking channel is a quantum channel which cannot be used to create entanglement between
parts participating in communication [24]. It can be presented in the form of a measurement followed by a state preparation. In quantum multiple access channels there are at least two senders transmitting to one receiver. Each sender sends his state independently of the other, i.e. their inputs are uncorrelated. For the case of two senders, a MAC acts as a map:

\[ \rho_1 \otimes \rho_2 \mapsto \Gamma(\rho_1 \otimes \rho_2) \]  

(1)

where state \( \rho_1 \) (\( \rho_2 \)) is sent by the sender \( S_1 \) (\( S_2 \)).

We will denote as \( \Gamma_A \otimes \Gamma_B \) a parallel setup of channels \( \Gamma_A, \Gamma_B \). It means that each sender has access to one input of the channel \( \Gamma_A \) and one input of the channel \( \Gamma_B \). They can transmit any states through their inputs where the first part of transmitted states goes through \( \Gamma_A \) and the second through \( \Gamma_B \). Channels are used synchronously and the receiver has access to the outputs of both channels.

A quantum channel can be used for transmission of classical information [22] or quantum information [21]. In the transmission of classical information, senders encode classical messages \{1\}, \{j\} into code states transmitted through the channel \( i \mapsto \rho_{1(i)} \), \( j \mapsto \rho_{2(j)} \). Senders and receiver know the ensemble of code states (i.e. the set of code states and the probabilities the states are transmitted with) \{\rho_{1(i)}, \rho_{2(j)}\} but one sender does not know which state is transmitted by the other sender at a given time. The receiver performs measurement on the output state and based on its result tries to infer which message \((i, j)\) was transmitted.

The amount of classical information which can be reliably transmitted through the MAC is given by the pair of rates \((R_1, R_2)\). The set of all achievable rates form the Holevo like classical capacity region \( \mathcal{R}(\Gamma) \). For a given ensemble of code states one can define the state \( \rho = \sum_{i,j} \rho_{1(i)} \otimes \rho_{2(j)} \) where \{\rho_{1(i)}, \rho_{2(j)}\} are projectors on the standard basis of the Hilbert space of the input controlled by \( S_1 \) (\( S_2 \)). The capacity region \( \mathcal{R}(\Gamma) \) is obtained as a convex closure of all rates \((R_1, R_2)\) such that there exists \( \rho \) for which the set of inequalities is fulfilled:

\[ R_1 \leq I(S_1 : R|S_2) \]  

(2)

\[ R_2 \leq I(S_2 : R|S_1) \]  

(3)

\[ R_T = R_1 + R_2 \leq I(S_1, S_2 : R) \]  

(4)

where \( I(S_1, S_2 : R) = H(\rho_{S1}) + H(\rho_{S2}) - H(\rho_R) \) and \( I(S_1 : R|S_1) = \sum_j p_j I(S_1 : R|S_2 = j) \). \( H(\rho) = -\text{tr} [\rho \log \rho] \) is the von Neuman entropy. \( R_T \) denotes the total rate and is defined as \( R_T = \sum_i R_i \). We shall denote "single shot" formula \( \mathcal{R}^{(1)}(\Gamma) = \mathcal{R}(\Gamma) \) and \( \mathcal{R}^{(m)}(\Gamma) = \frac{1}{m} \mathcal{R}(\Gamma^{\otimes m}) \) for the situation where code states can be \( n \)-particle entangled states. The interesting case is that of the regularized capacity region \( \mathcal{R}(\Gamma) = \lim_{n \to \infty} \frac{1}{n} \mathcal{R}(\Gamma^{\otimes n}) \), which expresses the upper bound for the capacity region which can be achieved due to quantum entanglement.

For a MAC \( \Gamma \) with \( n \) senders we define the minimum output entropy \( H_{\text{min}}(\Gamma) \) as:

\[ H_{\text{min}}(\Gamma) = \min_{\rho_1, \ldots, \rho_n} H(\Gamma(\rho_1 \otimes \ldots \otimes \rho_n)) \]  

(5)

where \( \rho_i \) belongs to the input space of the sender \( S_i \). Minimization runs over all states from the input space of each sender. Due to the concavity of \( H(\rho) \), it is sufficient to minimize only over pure states.

In the classical setup senders transmit only product states from orthogonal bases of the input spaces of \( \Gamma_A \) and \( \Gamma_B \). By the properties of the von Neuman entropy, we can state for MACs the additivity theorem:

\[ H_{\text{min}}(\Gamma_A) + H_{\text{min}}(\Gamma_B) = H_{\text{min}}(\Gamma_A \otimes \Gamma_B) \]  

(6)

Existence of entangled states in the input space of the \( \Gamma_A \otimes \Gamma_B \) extends the set we minimize \( H_{\text{min}} \) over and makes the additivity theorem invalid in the quantum setup. Subadditivity of \( H_{\text{min}} \) occurs if transmission of entanglement state through \( \Gamma_A \otimes \Gamma_B \) produce lower entropy than the sum of \( H_{\text{min}} \) of each channel working separately.

The additivity theorem for MACs can be stated analogically:

\[ \mathcal{R}(\Gamma_A) + \mathcal{R}(\Gamma_B) = \mathcal{R}(\Gamma_A \otimes \Gamma_B) \]  

(7)

Here we use the geometrical sum of the sets in Euclidean space. In the parallel setup of quantum MACs we can use entangled states as code words. Superadditivity of the classical capacity regions \( \mathcal{R} \) takes place if there exists a protocol using entangled code states with classical capacity region \( \mathcal{R}_{\text{ent}}(\Gamma_A \otimes \Gamma_B) \) such that for each protocol using only product code states with \( \mathcal{R}_{\text{prod}}(\Gamma_A \otimes \Gamma_B) = \mathcal{R}(\Gamma_A) + \mathcal{R}(\Gamma_B) \) occurs \( \mathcal{R}_{\text{prod}} \subseteq \mathcal{R}_{\text{ent}} \). Superactivation describes the situation when \( \mathcal{R}_{\text{ent}} \) is huge in comparison with \( \mathcal{R}_{\text{prod}} \).

In what follows, we shall use generalized Bell states [14] in the form:

\[ |\psi_{\alpha, \beta}\rangle = \frac{1}{\sqrt{D}} \sum_{l=0}^{D-1} \exp \left( \frac{2\pi i}{D} \alpha l \right) |l\rangle |l + \beta\rangle \]  

(8)

\( \alpha, \beta \in \{0, D - 1\} \) are indices. The states belong to the space \( \mathbb{C}^D \otimes \mathbb{C}^D \). For the state \( |\mu\rangle = \sum_i \mu_i |i\rangle \) where \{\( |i\rangle \)\} is the standard basis, we will write \( |\mu^*\rangle = \sum_i \mu_i^\ast |i\rangle \) and \( D = 2^d \).

For two random variables \( X, Y \) with equal support the statistical distance is defined as:

\[ \text{dist}(X, Y) = \frac{1}{2} \sum_{e \in \text{supp}(X)} |p_x(e) - p_y(e)| \]  

(9)

We denote by \( F_m \) a \( m \)-bit random variable with a flat distribution over its support.
Proposition 1 For a binary random variable $X$ if $\text{dist}(X, F_2) = \epsilon$ then $1 - H(X) = (2/\ln 2)\epsilon^2 + O(\epsilon^4)$ and for $\epsilon \in (0, 0.5)$ we have $1 - H(X) \leq 4\epsilon^2$.

Proof: This follows directly from a Taylor series expansion.

A classical multiple source randomness extractor is a function which distills entropy from independent "weak random sources" into random variables with almost flat distribution. We put the word "classical" to distinguish from situation where randomness is obtained on the basis of quantum effects.

Usability of a random source in a randomness extraction process is characterized by the min-entropy $H_{\infty}$ defined as:

$$H_{\infty}(X) = \min_{x \in \text{supp}(X)} - \log p(x) \quad (10)$$

Definition 1 Multiple source randomness extractor [11]: A function $f_{\text{ext}} : \{0, 1\}^{n \times k} \rightarrow \{0, 1\}^m$ which satisfies:

$$\text{dist}(f_{\text{ext}}(X_1, \ldots, X_i), F_m) \leq \epsilon \quad (11)$$

for every independent $n$-bit source $X_1, \ldots, X_i$ with $H_{\infty}(X_i) \geq k$ is called an $l$-source extractor with $k$-min-entropy requirement, $n$-bit input, $m$-bit output and $\epsilon$-statistical distance.

Theorem 1 Extractor existence [11]: Let $m < k < n$ be integers and let $\epsilon > 0$. If $k > \log n + 2m + 2\log(1/\epsilon) + 1$ holds then there exists a 2-source extractor $f_{\text{opt}} : \{0, 1\}^{n \times 2} \rightarrow \{0, 1\}^m$ with $k$-entropy requirement and distance $\epsilon$. The extractor can be computed in time proportional to $25n^22^n$.

SUBADDITIVITY OF $H_{\min}$

Here we provide two families of MACs $\{\Gamma_A^\delta\}$ and $\{\Gamma_B^\delta\}$ indexed by $\delta$ which exhibit subadditivity of $H_{\min}$ for $\delta < 1/2$.

The channels $\Gamma_A^\delta, \Gamma_B^\delta$ consist of 4 independent $d$-qubit inputs $X_1^A, \ldots, X_4^A$ ($X_1^B, \ldots, X_4^B$) and 1-qubit output $Y^A$ ($Y^B$). The inputs $X_i^A$ and $X_i^B$ are controlled by the sender $S_i$. The size of the inputs depend on $\delta$ as follows: $d = \lceil 2\log(1/\delta) + 12 \rceil$. Both channels are based on the same scheme (see FIG. 1) so we will describe the channel $\Gamma_A$ and point out where the channels differ. In the first step, the channel perform measurements $M_l$ and $M_{ll}$. $M_l$ is a joint measurement on inputs $X_1, X_2$ and $M_{ll}$ is a joint measurement on inputs $X_3, X_4$. In the channel $\Gamma_A$, measurements $M_l$ and $M_{ll}$ are performed in the basis $\{|\Psi_{a,b}\rangle\}$ while in the channel $\Gamma_B$ in the basis $\{|\Psi_{a,b}^*\rangle\}$. The result of the measurement $M_l$ ($M_{ll}$) is denoted by $m_l$ ($m_{ll}$). $m_l$ and $m_{ll}$ provide the $2d$-bits inputs to the randomness extractor $f_{\text{opt}}$, which produces a 1 bit output. Existence of the extractor $f_{\text{opt}}$ with proper features will be proven later. Depending on the value of $f_{\text{opt}}(m_l, m_{ll})$, the channel produces the output state $|0\rangle$ or $|1\rangle$.

We will show that for any $\delta > 0$, $H_{\min}(\Gamma_A^\delta)$ and $H_{\min}(\Gamma_B^\delta)$ cannot be lower than $1 - \delta$. On the other hand we will show that if each sender transmits $|\Psi_{0,0}\rangle$, the output entropy of the $\Gamma_A^\delta \otimes \Gamma_B^\delta$ is equal to 1. Since this is the upper bound for $H_{\min}(\Gamma_A^\delta \otimes \Gamma_B^\delta)$ we will prove that for $\delta < 1/2$, $H_{\min}(\Gamma_A^\delta) + H_{\min}(\Gamma_B^\delta) > H_{\min}(\Gamma_A^\delta \otimes \Gamma_B^\delta)$.

We start by proving that $H_{\min}(\Gamma_A^\delta) = H_{\min}(\Gamma_B^\delta) \geq 1 - \delta$ but first we give a proposition which will be useful in what follows.

Proposition 2 For the random variables associated with the outputs of the measurements performed by the channels $\Gamma_A^\delta$ and $\Gamma_B^\delta$, the following holds: $H_{\infty}(M_A^A) = H_{\infty}(M_{ll}^A) = H_{\infty}(M_{ll}^B) = H_{\infty}(M_A^B) = d$. Here $d$ denotes the input size of the channels.

Proof: We will only prove that $H_{\infty}(M_A^A) = d$.
since the other cases can be proved analogously. Let the projector measurement $M^A_I$ be performed on the product state $|\mu\rangle \otimes |\nu\rangle$, where $|\mu\rangle = \sum_{j=0}^{D-1} \mu_j |j\rangle$, $|\nu\rangle = \sum_{k=0}^{D-1} \nu_k |k\rangle$ are $d$-qubit states pertaining to senders $S_1$ and $S_2$ respectively. We will show that the probability $p(\alpha, \beta) = (|\langle \psi_{m,n}|\mu\rangle|\nu\rangle)^2$ of getting the pair $(\alpha, \beta)$ as the result of measurement satisfies $p(\alpha, \beta) \leq 1$. $H_{\infty}(M^A_I) \geq d$ is simple consequence of this fact.

Observe that:

$$p(\alpha, \beta) = \langle \psi_{\alpha,\beta} |\mu\rangle |\nu\rangle$$  \hspace{1cm} (12)

$$= \frac{1}{\sqrt{D}} \sum_{l=0}^{D-1} \exp \left( \frac{2\pi i}{D} \alpha l \right) |l + \beta\rangle$$  \hspace{1cm} (13)

$$= \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} \mu_j |j\rangle \sum_{k=0}^{D-1} \nu_k |k\rangle$$  \hspace{1cm} (14)

$$= \frac{1}{\sqrt{D}} \sum_{j=0, k=0, l=0}^{D-1} \exp \left( \frac{2\pi i}{D} \alpha l \right) \mu_j \nu_k |l + \beta\rangle$$  \hspace{1cm} (15)

$$= \frac{1}{\sqrt{D}} \sum_{l=0}^{D-1} \exp \left( \frac{2\pi i}{D} \alpha l \right) \mu_l \nu_{l+\beta}$$  \hspace{1cm} (16)

$$= \frac{1}{\sqrt{D}} \langle \mu^* |U^A_{\beta} |\nu\rangle$$  \hspace{1cm} (17)

where $U^A_{\beta} = \sum_{l=0}^{D-1} |l + \beta\rangle \langle l| \exp \left( \frac{2\pi i}{D} \alpha l \right)$ is an unitary. Finally by the property of the scalar product we have $p(\alpha, \beta) = \frac{1}{\sqrt{D}} \langle \mu^* |U^A_{\beta} |\nu\rangle^2 \leq 1$. □

Taking into account proposition 2 and noting that $d/2 > \log d$ is true for $d > 4$, we obtain that $d = \lfloor 2 \log 1/\delta + 12 \rfloor$ fulfills the requirements of Thm. 1 with $\epsilon = \sqrt{\delta}/2$. Since $f_{\text{opt}}$ exists and has statistical distance $\epsilon$, by proposition 1 for each channel we have $H_{\text{min}} \geq 1 - \epsilon$.

Now consider output entropy of the $\Gamma^A_A \otimes \Gamma^B_B$ if all senders transmit $|\psi_{0,0}\rangle$. The first part of the $2d$-qubit state is transmitted through the channel $\Gamma^A_A$ and the second through $\Gamma^B_B$ (see FIG. 2). We will show that in this case the output entropy of the $\Gamma^A_A \otimes \Gamma^B_B$ cannot exceed 1.

The randomness extractor $f_{\text{opt}}$ is a deterministic function of the outcome of the measurements $M_I, M_{II}$. Its output controls which of the pure states $|0\rangle, |1\rangle$ will be the output of the channel. If the results of measurements $M^A_I$ and $M^B_I$ ($M^A_{II}$ and $M^B_{II}$) are identical, then so will the outputs of the channels too. Let us focus on the measurements $M^A_I$ and $M^B_I$. We will show that $p(m^A_I, m^B_I) = p(\alpha, \beta_A, \alpha, \beta_B) \propto \delta_{\alpha_A, \beta_A} \delta_{\beta_A, \beta_B}$.

where Eq. (20) is obtained in the same way as Eq. (17). This result can be viewed as generalized entanglement swapping [14–16]. Entanglement between uses of channels $\Gamma^A_A$ and $\Gamma^B_B$ is swapped by the measurement $M^A_I$ into entanglement between the inputs of the channel $\Gamma^B_B$ belonging to senders $S_1$ and $S_2$. The argument presented is also valid for the measurements $M^A_{II}$ and $M^B_{II}$.

As we have shown, in the case of entangled state transmission, the outputs of $f_{\text{ext}}$ for channels $\Gamma^A_A$ and $\Gamma^B_B$ are equal. Since the output of the channel $\Gamma^A_A \otimes \Gamma^B_B$ can be written in the form $p(00)|00\rangle + (1 - p)|11\rangle \langle 11|$ for which the entropy is upper bounded by 1.

**SUPERACTIVATION OF $R$**

We now turn to on the superactivation of the classical capacity regions of the channels $\Gamma^A_A, \Gamma^B_B$. Namely we will show that if the senders can transmit only product states, classical capacity region $R_{\text{prod}} = \mathcal{R}^{(1)}(\Gamma^A_A) + \mathcal{R}^{(1)}(\Gamma^B_B)$ is bounded by the inequalities $R_S = \sum_{i \in S} R_i \leq 2\delta$ for any subset of senders $S$. We compare this with a protocol using entangled states. $R_{\text{ent}} = \mathcal{R}^{(1)}(\tilde{\Gamma}^A_A \otimes \tilde{\Gamma}^B_B)$ achieved in this case is given by inequality $R_1 + R_2 + R_3 + R_4 \leq 1$.

Let us present the channel $\tilde{\Gamma}^A_A$ (see FIG. 3). It is a 4-to-1 channel. Input of each sender consists $d$-qubits.
line and 1-bit line. The channel acts as:

\[
\tilde{\Gamma}^{(d)}(\rho_1 \otimes e_1^{(1)} \otimes \cdots \otimes \rho_4 \otimes e_4^{(l)}) = \text{CNOT}_1 \circ \cdots \circ \text{CNOT}_l(\Gamma_A^{(d)}(\rho_1 \otimes \cdots \otimes \rho_4))
\]

where \( \rho \) is transmitted through qubit inputs and \( e^{(.)} \) through bit inputs. \( \text{CNOT}_0(\rho) = \rho \) and \( \text{CNOT}_1(\rho) = X \rho X^T \). In the same way we construct \( \tilde{\Gamma}_B^{(d)} \).

Note that \( R_S \leq I(X_S : Y|X_{SC}) \leq H_{max} - H_{min} \) where \( H_{max} \) is the maximal entropy of an output of a channel. By the dimensionality of the output of the channels \( \Gamma_A^{(d)} \) and \( \Gamma_B^{(d)} \), we have in both cases \( H_{max} \leq 1 \). Taking into account results from the previous section we have that \( H_{min} \geq 1 - \delta \) that leads to \( R_S(\Gamma_A^{(d)}) \leq \delta, R_S(\Gamma_B^{(d)}) \leq \delta \) and \( R_S(\Gamma_A^{(d)}) + R_S(\Gamma_B^{(d)}) \leq 2\delta \).

Now consider use of entangled states for communication. In this protocol each sender transmits the state \( \Psi_{0,0} \) through the quantum lines, the label 0 through the classical lines of the channel \( \tilde{\Gamma}_A \) and with equal probability labels 0 or 1 through the classical lines of the channel \( \tilde{\Gamma}_B \). As noted above, outputs of the channels \( \Gamma_A^{(d)} \) and \( \Gamma_A^{(0)} \) are identical. Perform the CNOT operation controlled by the output of \( \tilde{\Gamma}_A \) on the output of \( \tilde{\Gamma}_B \). The result of CNOT pertaining to the channel \( \tilde{\Gamma}_B \) and the classical input lines of this channel can be viewed as the output and input of the well known in the classical information theory binary XOR channel. Its capacity region is given by the \( R_1 + R_2 + R_3 + R_4 \leq 1 \, [23] \).

CONCLUSIONS

We have shown that very strong subadditivity of the minimum output entropy \( H_{min} \) and superadditivity of the capacity region \( R^{(1)} \) occurs in the domain of entanglement breaking quantum multiple access channels. The effect is based on the fundamental properties of MAC i.e. independence of the senders.

Randomness extractors which extract from one randomness source requires additional random seed. That makes them useless for our purposes. The requirement of at least two randomness sources determines the number of senders in the example we presented.

We have shown that superadditivity effect for \( R_T \) occurs for "single shot" capacity regions \( R^{(1)} \) of two different channels. As it was shown in [4] the superadditivity of the regularized classical capacity regions \( R^{(\infty)} \) of two different MACs occurs in realm of single user rates \( R_i \), however the superadditivity of the regularized classical capacity \( C^{(\infty)} \) of 1-to-1 channels and superadditivity of \( R_T \) of \( R^{(\infty)} \) of MACs still remains an open questions.