Quantum Broadcast Channels

and

Cryptographic Applications for Separable States

Rainer Wilmink

Dissertation zur Erlangung des Doktorgrades,

vorgelegt der Fakultät für Mathematik,
Universität Bielefeld

Bielefeld, 01.06.2003

Gedruckt auf alterungsbeständigem Papier ISO 9706

Abstract

Quantum information-theoretic models of secret source-sharing are developed using a general LOCC scheme, i.e. a protocol involving only local operations and classical communication. This is in order to generate a common random key from a shared quantum state at two terminals without allowing an eavesdropper to obtain information about this key. Coding theorems for special separable states are obtained, and bounds to secret key capacity are also derived for more general quantum source states and other models later. In order to prove results for secret source-sharing schemes with a quantum source state also shared with a wiretapper, multi-user systems are studied and the capacity region for the degraded quantum broadcast channel is started to be determined. Using the results of the foregoing chapters, a sufficient bound on the error rate for unconditional security of the BB84 quantum key distribution protocol is proved.

Acknowledgements

This work originated from an attempt to learn more about both quantum mechanics and information theory at the same time. Great problems arise in the combination of both fields which contribute to some parts of the thesis.

Thanks are due to Prof. Rudolf Ahlswede, who became my Doktorvater. In 1989, at the beginning of the Sonderforschungsbereich 343 (University of Bielefeld), he already formulated an agenda to develop a theory of quantum information, especially by involving the (at that time already well developed) classical theory of channels with many senders and receivers and with correlated sources. Following this program, the dissertations of Peter Löber on information and of Andreas Winter on the quantum multiple access channels appeared. Here we continue with the quantum broadcast channels.

Further thanks are due to Andreas Winter for teaching me quantum information theory, and to Ning Cai for reviewing my thesis. Finally, I would like to thank Marina Kyureghyan and Stefan Grünewald for working alongside me, and for being at my disposal for non-mathematical questions.

Contents

1 Introduction

In the present thesis, problems of quantum information theory are discussed, mainly in the context of coding problems for secret key capacity and broadcast channels. Thus we follow a line of research initiated by Shannon [33] in 1948, where informational-operational meaning was lent to terms such as entropy, information, capacity and building on models of stochastic nature. This is directly in common with quantum theory, generally understood to be a stochastic theory (starting with Born in 1926 [11], modern textbook account e.g. by Peres [30]). A stochastic theory however of a novel type: it was soon understood that the statistical predictions of quantum theory cannot be described in classical stochastic theories (compare the early discussion of Einstein et al. [18] and Bell [8]) resulting in the necessity of a noncommutative probability theory.

These observations led physicists during the 1960s to speculate about the role of quantum probabilism in information theory: cf. the works of Gordon [20], Levitin [26] and Forney [19]. Holevo [23],[24] however is to be credited with founding an appropriate mathematical theory one decade later and proving the (in our days well known) Holevo bound on quantum channel capacities. This bound has already started reflecting the difference from "classical information", which was given a qualitative distinction in the no-cloning theorem of Wootters and Zurek [46], stating that quantum states cannot be duplicated, whereas classical data obviously can. This has had a great impact on models for quantum broadcast channels.

For the cryptography branch, Bennett and Brassard [9] introduced in 1984 their famous BB84 quantum key distribution protocol, which was considered to be unconditionally secure, i.e. the key resulting from this protocol is independent of other parameters, especially of computational power. Finally, in 1994, two significantly novel observations were made: the quantum algorithm of Shor [34] for factoring integers, proving the power of quantum information processing, and by Schuhmacher [31] the successful interpretation of von Neumann entropy as the asymptotic source coding rate for quantum information. Both works continue to exert a great influence on the newly founded quantum information theory research groups, starting with the proof of the coding theorem complementing the Holevo bound (Hausladen et al. [21], Holevo [25], Schuhmacher and Westmoreland [32]), up to multi-user quantum information theory (e.g. the coding theorem for the quantum multiple access channel[44]). In the field of quantum cryptography, an important result was also established: Mayers [28] proved in 1998 the security of the BB84 quantum key distribution theorem, which has not been totally understood for a long time by the research community. Later Shor and Preskill (2000) [35] presented an easier proof, using recently discovered quantum error-correcting codes and privacy amplification at the same

time. In this context it is interesting to see that the research on privacy amplification for quantum protocols led to new results in classical information theory [38].

In this thesis we start modelling a new general local communication scheme (LOCC) for secret sharing in a quantum setting, i.e. two terminals can measure their parts of a commonly shared quantum state and exchange classical messages publicly in order to establish a common secret key unknown to an adversary third terminal, who can listen to the public messages, with high probability. Beside general lower bounds coding theorems are proved in the special cases that the shared quantum state is classically correlated or has an orthogonal structure. In chapter III we extend this model, such that the adversary terminal may also be correlated to the commonly shared state, and a more sophisticated proof for a lower bound to the secret key capacity is given.

In order to state the proofs in chapter III, we had to take totally new research steps in quantum broadcast channel theory, where until now only research on the fundamental No-Cloning theorem had been done. After proving achievable rate points for the asymmetric broadcast channel, we state a coding theorem for the degraded quantum broadcast channel. Here the new problems to be solved arose from the quantum character of the involved channels underlying the above mentioned No-Cloning theorem.

Finally we establish a new proof for the sufficient bound on the error rate for unconditional security of the BB84 quantum key distribution protocol, using new results from the foregoing chapters.

Chapter I

Quantum Cryptography With Separable States I

1 Introduction

In this chapter we will start with definitions of quantum information theory, in order to derive upper and lower bounds for the secret key capacity of a quantum source shared between two users. In the case of a semi-classical quantum source, we will elaborate a coding theorem which will be extended in chapter III, where a wiretapper is also allowed to be correlated with the quantum source.

2 Basic Definitions and Theorems

A $\mathbb{C}^*$-*algebra* with unit is a complex Banach space $\mathfrak{U}$ which is also a $\mathbb{C}$-algebra with unit $\mathbb{1}$ and a $\mathbb{C}$-antilinear involution $*$, such that

$$\|AB\| \leq \|A\|\|B\| \text{ and } \|A^*\|^2 = \|A\|^2 = \|AA^*\|.$$

Quantum systems will be modelled by these algebras, quantum subsystems consequently by $*-$subalgebras. We will assume that all algebras are finite. It is known that in this case those algebras are isomorphic to a direct sum of $\mathfrak{L}(\mathcal{H}_i)$. This includes as extremal cases the algebras $\mathfrak{L}(\mathcal{H})$, and the commutative algebras $\mathbb{C}\mathcal{X}$ over a finite set $\mathcal{X}$. In particular we have on every such algebra a well defined and unique *trace functional*, denoted Tr , that assigns trace one to all minimal positive idempotents. A *state* on a $\mathbb{C}^*$-algebra $\mathfrak{U}$ is a positive $\mathbb{C}$-linear functional ρ with $\rho(\mathbb{1}) = 1$. Positivity here means that its values on the positive cone are nonnegative. Clearly the states form a convex set $\mathfrak{S}(\mathfrak{A})$ whose extreme points are called *pure states*, all others are *mixed*. One can easily see that every state ρ can be represented uniquely in the form $\rho(X) = \text{Tr}\,(\hat{\rho}X)$ for

a positive, selfadjoint element $\hat{\rho}$ of $\mathfrak{U}$ with trace one (such elements are called *density operators*). In the sequel we will make no distinction between ρ and its density operator $\hat{\rho}$.

2.1 Quantum Operations and Observables

A $\mathbb{C}$-linear map $\phi : \mathfrak{U}_2 \to \mathfrak{U}_1$ is called *quantum operation*, if it is completely positive (i.e. positive, so that positive elements have positive images, and also the $\rho \otimes \mathbb{1}_n$ are positive with $\mathbb{1}_n$ being the identity of the $n \times n$-matrices) and unit preserving. There is a 1-1 correspondence with their adjoints ϕ_* by the trace form, mapping states to states, and being completely positive and trace preserving.

Let $\mathbb{F}$ be a $\sigma-$ algebra on some set Ω, $\mathfrak{X}$ a $\mathbb{C}^*-$ algebra. A map $X : \mathbb{F} \to \mathfrak{X}$ is called a *positive operator valued measure* (POVM), or an observable, with values in $\mathfrak{X}$ (or on $\mathfrak{X}$), if:

1) $X(\emptyset) = 0, X(\Omega) = \mathbb{1}$

2) $E \subset F$ implies $X(E) \leq X(F)$

3) If $(E_n)_n$ is a countable family of pairwise disjoint sets in $\mathcal{F}$ then $X(\cup_n E_n) = \sum_n X(E_n)$ in the weak topology.

If the values of the observable are projection operators, and Ω is the real line one speaks of a *spectral measure* or a *von Neumann observable*. An observable X, together with a state ρ, yields a probability measure P^X on Ω via $P^X(E) = \mathrm{Tr}\,(\rho X(E))$. In this way we may view X as a random variable with values in $\mathfrak{X}$, its distribution we denote P_X (note that P_X may not be isomorphic to P^X : if X takes the same value on disjoint events, which means that X introduces randomness by itself). From now on, all observables will be *countable*, i.e. w.l.o.g. they are defined on a countable Ω with $\sigma-$ algebra. This means that we may view an observable X as a resolution of $\mathbb{1}$ into a countable sum $\mathbb{1} = \sum_{j \in \Sigma} X_j$ of positive operators X_j.

Two observables X, Y are said to be *compatible*, if they have values in the same algebra and $XY = YX$ elementwise, i.e. for all $E \in \mathbb{F}_X, F \in \mathbb{F}_Y : X(E)Y(F) = Y(F)X(E)$. If $\mathfrak{U}_1, \mathfrak{U}_2$ are subalgebras of $\mathfrak{U}$, they are *compatible* if they also commute elementwise.

2.2 von Neumann Entropy

The von Neumann entropy of a state ρ (introduced by von Neumann [39]) is defined as $H(\rho) = -\mathrm{Tr}\,(\rho \log \rho)$, which reduces to the usual Shannon entropy for a commutative algebra, because in this case a quantum state is equivalent to a probability distribution. Further, we introduce the *I-divergence* $D(\rho \| \sigma) = \mathrm{Tr}\,(\rho(\log \rho - \log \sigma))$ for states ρ, σ

with $\mathrm{supp}(\rho) \leq \mathrm{supp}(\sigma)$, otherwise $D(\rho\|\sigma) = \infty$. (This useful functional was first defined by Umegaki [36]).

Let X, Y, Z be compatible observables on a $\mathbb{C}^*-$ algebra $\mathfrak{U}$ and ρ a fixed state on $\mathfrak{U}$. In the previous subsection, these are then random variables with a joint distribution, and one defines entropy $H(X)$, conditional entropy $H(X|Y)$, mutual information $I(X \wedge Y)$, and conditional mutual information $I(X \wedge Y|Z)$ for these observables as the respective quantities for them interpreted as random variables. Since this depends on the underlying state ρ we will often add this state as an index, i.e. $H_\rho(X) = H(X)$, etc.

Now let $\mathfrak{X}, \mathfrak{X}_1, \mathfrak{X}_2, \mathfrak{Y}$ be compatible *-subalgebras of the $\mathbb{C}^*$-algebra $\mathfrak{U}$, i.e. they commute elementwise. With the completely positive inclusion map $i : \mathfrak{X} \to \mathfrak{U}$ and its adjoint $i_* : \mathfrak{U}_* \to \mathfrak{X}_*$, we define

$$H(\mathfrak{X}) = H_\rho(\mathfrak{X}) \triangleq H(i_*\rho)$$

(where the von Neumann entropy appears on the right hand side). Now conditional entropy, mutual information, and conditional mutual information are defined by reducing them to entropy quantities:

$$\begin{aligned} H(\mathfrak{X}|\mathfrak{Y}) &\triangleq H(\mathfrak{X}\mathfrak{Y}) - H(\mathfrak{Y}) \\ I(\mathfrak{X}_1 \wedge \mathfrak{X}_2) &\triangleq H(\mathfrak{X}_1) + H(\mathfrak{X}_2) - H(\mathfrak{X}_1\mathfrak{X}_2) \\ I(\mathfrak{X}_1 \wedge \mathfrak{X}_2|\mathfrak{Y}) &\triangleq H(\mathfrak{X}_1|\mathfrak{Y}) + H(\mathfrak{X}_2|\mathfrak{Y}) - H(\mathfrak{X}_1\mathfrak{X}_2|\mathfrak{Y}) \end{aligned}$$

We may now form hybrid expressions involving observables and subalgebras at the same time: let $i : \mathfrak{X} \to \mathfrak{U}$, $j : \mathfrak{Y} \to \mathfrak{U}$ be $*-$ subalgebra inclusions, and X, Y observables on $\mathfrak{U}$, all compatible. Then we can for example define

$$H(\mathfrak{X}|Y) = H(iY) - H(Y),$$

which can be evaluated by

$$H(\mathfrak{X}|Y) = \sum_j \mathrm{Tr}\ (\rho Y_j) H_{\rho_j}(\mathfrak{X}), \text{ with } \rho_j = \frac{1}{\mathrm{Tr}\ (\rho Y_j)} \sqrt{Y_j}\rho\sqrt{Y_j}.$$

A further possible formula is given by

$$I(\mathfrak{X} \wedge \mathfrak{Y}) = H(i) + H(Y) - H(iY).$$

Define for a (measureable) map $\rho_* : \mathcal{X} \to \mathfrak{S}(\mathfrak{Y})$ and a probability distribution P on $\mathcal{X}$

$$I(P; \rho_*) \triangleq I_\gamma(\mathbb{C}\mathcal{X} \wedge \mathfrak{Y})$$

with the channel state $\gamma = \sum_{x\in\mathcal{X}} P(x)[x] \otimes \rho_*(x)$. It is easy to verify that

$$I(P; \rho_*) = H(P\rho_*) - H(\rho_*|P),$$

where $P\rho_* = \mathrm{Tr}_{\mathbb{C}\mathcal{X}}\gamma = \sum_{x\in\mathcal{X}} P(x)\rho_*(x)$ and $H(\rho_*|P) = \sum_{x\in\mathcal{X}} P(x)H(\rho_*(x))$.

In the rest of this thesis, we will always use compatible *-subalgebras of some $\mathbb{C}^* -$ algebra $\mathfrak{U}$, if not otherwise noted. For the language of observables and further definitions and proofs regarding the entropy used in this thesis, we mainly refer to Winter [41].

2.3 Quantum Entropy Inequalities

For the following facts, we refer to Ohya & Petz [29] and Wehrl [40].

Theorem 2.1 (Dilation) *Let* $\phi : \mathfrak{U} \to \mathfrak{L}(\mathcal{H})$ *be a linear map of* $\mathbb{C}^*$*-algebras. Then* ϕ *is completely positive if and only if there exists a representation* $\alpha : \mathfrak{U} \to \mathfrak{L}(\mathcal{K})$, *with Hilbert space* $\mathcal{K}$ *and a bounded linear map* $V : \mathcal{H} \to \mathcal{K}$ *such that*

$$\forall A \in \mathfrak{U} : \ \phi(A) = V^* \alpha(A) V.$$

The well known Kraus representation $\phi(A) = \sum_i B_i^* A B_i$ with $\mathfrak{U} = \mathfrak{L}(\mathcal{U})$ and linear maps $B_i : \mathfrak{L}(\mathcal{H}) \to \mathfrak{L}(\mathcal{U})$, where $\sum_i B_i^* B_i = \mathbb{1}_{\mathcal{H}}$, is a useful corollary.

Theorem 2.2 (Klein inequality) *For positive operators* ρ, σ

$$D(\rho \| \sigma) \geq \frac{1}{2} \mathrm{Tr}\ (\rho - \sigma)^2 + \mathrm{Tr}\ (\rho - \sigma).$$

Further if ρ, σ *are states then* $D(\rho \| \sigma) \geq 0$ *and* $D(\rho \| \sigma) = 0$ *if and only if* $\rho = \sigma$.

Theorem 2.3 (Monotonicity) *Let* ρ, σ *be states on a* $C^* - algebra$ $\mathfrak{U}$, *and* ϕ_* *a trace preserving, completely positive linear map from states on* $\mathfrak{U}$ *to states on* $\mathfrak{B}$. *Then*

$$D(\phi_* \rho \| \phi_* \sigma) \leq D(\rho \| \sigma).$$

Theorem 2.4 ((Strong) Subadditivity) *For compatible* $*-$ *subalgebras* $\mathfrak{U}_1, \mathfrak{U}_2, \mathfrak{U}_3$ *one has:*

$$H(\mathfrak{U}_1 \mathfrak{U}_2) \leq H(\mathfrak{U}_1) + H(\mathfrak{U}_2) \qquad \textit{(Subadditivitiy) and}$$

$$H(\mathfrak{U}_1 \mathfrak{U}_2 \mathfrak{U}_3) + H(\mathfrak{U}_2) \leq H(\mathfrak{U}_1 \mathfrak{U}_2) + H(\mathfrak{U}_2 \mathfrak{U}_3) \qquad \textit{(Strong Subadditivity).}$$

A proof of the strong subadditivity was first done by Lieb & Ruskai. The first inequality can be proved by setting $\mathfrak{U}_2 = \mathbb{C}$.

Theorem 2.5 (Data Processing Lemma) *Let* $\mathfrak{U}_1, \mathfrak{U}_2, \mathfrak{U}_1', \mathfrak{U}_2'$ *be compatible subalgebras of* $\mathfrak{U}$ *and* $\phi_i : \mathfrak{U}_i \to \mathfrak{U}$, $\psi_i : \mathfrak{U}_i' \to \mathfrak{U}_i$ *for* $i \in \{1, 2\}$ *quantum operations. Then we obtain the most general form of a data processing inequality*

$$I(\phi_1 \circ \psi_1 \wedge \phi_2 \circ \psi_2) \leq I(\phi_1 \wedge \phi_2).$$

This is still true in the case that we condition over commutative subalgebras.

Proof: Consider the following diagram

$$\begin{array}{ccccc} \mathfrak{U}_1' & \xrightarrow{\phi_1} & \mathfrak{U}_1 & \xrightarrow{\psi_1} & \mathfrak{U} \\ \downarrow & & \downarrow & & \| \\ \mathfrak{U}_1' \otimes \mathfrak{U}_2' & \xrightarrow{\phi_1 \otimes \phi_2} & \mathfrak{U}_1 \otimes \mathfrak{U}_2 & \xrightarrow{\psi = \psi_1 \psi_2} & \mathfrak{U} \\ \uparrow & & \uparrow & & \| \\ \mathfrak{U}_2' & \xrightarrow{\phi_2} & \mathfrak{U}_2 & \xrightarrow{\psi_2} & \mathfrak{U} \end{array}$$

and apply the Lindblad-Uhlmann monotonicity theorem 2.3 twice, with $\phi_*(\rho)$ and the map $(\psi_1 \otimes \psi_2)_*$. The rest follows from the strong subadditivity theorem 2.4.

■

Define $h(x) \triangleq -x \log x - (1-x)\log(1-x)$.

Theorem 2.6 (Quantum FANO-inequality) *Let $\mathfrak{X}$ be a commutative *-subalgebra compatible with $\mathfrak{Y}$, and X the uniquely determined maximal observable on $\mathfrak{X}$. Then for any observable Y with values in $\mathfrak{Y}$ the probability that "$X \neq Y$", i.e. $p_e = 1 - \sum_j \mathrm{Tr}\,(\rho X_j Y_j)$, satisfies*

$$H(\mathfrak{X}|\mathfrak{Y}) \leq h(p_e) + p_e \log(\mathrm{Tr}\ supp(\rho|_{\mathfrak{X}}) - 1)$$

Proof: This can be easily reduced to the classical FANO-inequality.

2.4 Discrete Memoryless Quantum Channel

A *(discrete memoryless) quantum channel* (q-DMC) is a completely positive, trace preserving mapping ϕ_* from the states on a C^*- algebra $\mathfrak{U}$ into the states on $\mathfrak{L}(\mathcal{H})$, where $d = \dim \mathcal{H}$ is assumed to be finite. A nonstationary q-DMC is a sequence $(\phi_{n*})_{n\in\mathbb{N}}$ of q-DMC's, with a global Hilbert space $\mathcal{H}$. An $n-$ block code is a pair (f, D), where f is a mapping from a finite set $\mathcal{M}$ into $\mathfrak{S}(\mathfrak{U}_1) \times \cdots \times \mathfrak{S}(\mathfrak{U}_n)$, and D is an observable on $\mathfrak{L}(\mathcal{H})^{\otimes n}$ indexed by $\mathcal{M}' \subset \mathcal{M}$. We call (f, D) an $(n, \lambda)-$ code, if the maximum error probability

$$e(f, D) = \max\{1 - \mathrm{Tr}\,(\phi_*^{\otimes n}(f(m))D_m) : m \in \mathcal{M}\}$$

is less or equal λ.

Theorem 2.7 *Let $(\mathfrak{W}_1, \mathfrak{W}_2, \dots)$ be a nonstationary q-DMC, and $C(\mathcal{W}_i) = \sup_{P \text{ p.d. on } \mathfrak{W}} I(P; \mathfrak{W}_i)$. Then for every $\lambda \in (0,1)$*

$$\left\| \frac{1}{n} \log N(n,\lambda) - \frac{1}{n} \sum_{i=1}^{n} C(\mathfrak{W}_i) \right\| \overset{n\to\infty}{\to} 0,$$

where $N(n,\lambda)$ denotes the maximal size of $\mathcal{M}$.

This theorem was independently proved in 1997 by Holevo [25] and Schumacher & Westmoreland [32]. For a more elegant proof, see Winter [42].

3 Typical Sequences

Definition 3.1 (Variance Typical Sequences) *Let P be a probability distribution on the set $\mathcal{X}$, with $|\mathcal{X}| < \infty, \delta > 0$. Define $N(x|x^n) = |\{i : x_i = x\}|$. Then we call the set*

$$\mathcal{T}^n_{V,P,\delta} = \{x^n \in \mathcal{X}^n : \forall x \in \mathcal{X} | N(x|x^n) - nP(x)| \leq \delta\sqrt{n}\sqrt{P(x)(1-P(x))}\}$$

the set of variance-typical sequences with constant δ (cf. Wolfowitz [45]).

The empirical distribution P_{x^n} on $\mathcal{X}$ is called *type* of $\mathcal{X}^n$, defined by $P_{x^n}(x) = \frac{1}{n}N(x|x^n)$. The following set of all types for a given block length n over $\mathcal{X}$ denoted as $\mathcal{P}(n, \mathcal{X})$ is upper bounded by $(n+1)^{|\mathcal{X}|}$, known as type counting. Note that $\mathcal{T}^n_P \triangleq \mathcal{T}^n_{V,P,0}$ is the set of sequences of the same type P. Defining $K \triangleq 2(\log e/e)$ we get

Lemma 3.2 [45] *For every probability distribution on $\mathcal{X}$ and $\delta > 0$*

$$P^{\otimes n}(\mathcal{T}^n_{V,P,\delta}) \geq 1 - \frac{|\mathcal{X}|}{\delta^2}$$

$$|\mathcal{T}_{V,P,\delta}| \leq \exp\{nH(P) + K|\mathcal{X}|\delta\sqrt{n}\}.$$

Proof: $\mathcal{T}^n_{V,P,\delta}$ is the intersection of $|\mathcal{X}|$ events, namely for each $x \in \mathcal{X}$ it is the mean of the independent Bernoulli variables X_i with value 1 iff $x_i = x$ has a deviation from its expectation $P(x)$ at most $\alpha\sqrt{P(x)(1-P(X))}/\sqrt{n}$. According to Chebyshev's inequality each of these has probability at least $1 - 1/\delta^2$. The second inequality is a known fact from type counting (cf. Wolfowitz [45]).

■

Further, let $P_{\mathcal{X}|\mathcal{U}}$ be a stochastic matrix (giving a classical channel $U : \mathcal{U} \to \mathcal{X}$). The set of sequences $x^n \in \mathcal{X}^n$ is called $P_{\mathcal{X}|\mathcal{U}}$-variance-typical under the condition $u^n \in \mathcal{U}^n$ with constant δ :

$$\mathcal{T}_{V,P_{\mathcal{X}|\mathcal{U}},\delta}(u^n) \triangleq \{x^n \in \mathcal{X}^n : \forall u \in \mathcal{U}, x \in \mathcal{X} :$$
$$|N(u,x|u^n,x^n) - N(u|u^n)P_{\mathcal{X}|\mathcal{U}}(x|u)| \leq \delta\sqrt{N(u|u^n)P_{\mathcal{X}|\mathcal{U}}(x|u)(1-P_{\mathcal{X}|\mathcal{U}}(x|u))}\},$$

where $N(u,x|u^n,x^n) \triangleq |\{i \in \{1,\ldots,n\} : u_i = u \text{ and } x_i = x\}|$.

Lemma 3.3 *For every stochastic matrix* $P_{\mathcal{X}|\mathcal{U}}$ *on* $\mathcal{X},\mathcal{U}$, u^n *of type* $P_{\mathcal{U}}$ *and* $\delta > 0$

$$\begin{aligned} P_{\mathcal{X}|\mathcal{U}}^{\otimes n}(\mathcal{T}^n_{V,P_{\mathcal{X}|\mathcal{U}}}(u^n)|u^n) &\geq 1 - \frac{|\mathcal{U}||\mathcal{X}|}{\delta^2}, \\ |\mathcal{T}^n_{V,P_{\mathcal{X}|\mathcal{U}},\delta}(u^n)| &\leq \exp\{nH(P_{\mathcal{X}|\mathcal{U}}|P_{\mathcal{U}}) + K'(2|\mathcal{X}| + \delta)|\mathcal{U}||\mathcal{X}|\sqrt{n}\} \end{aligned}$$

for some $K' > 0$ *independent of* $|\mathcal{X}|, |\mathcal{U}|, \delta, n$.

Proof: For each $u \in \mathcal{U}$ the mean of the independent Bernoulli variables X_i with distribution $P_{X_i} = P_{\mathcal{X}|\mathcal{U}}(\cdot|u_i)$ has a deviation from its expectation $N(u|u^n)P_{\mathcal{X}|\mathcal{U}}(x|u)$ and variance $N(u|u^n)P_{\mathcal{X}|\mathcal{U}}(x|u)(1-P_{\mathcal{X}|\mathcal{U}}(x|u))$. The rest again follows from Chebyshev's inequality.

■

Definition 3.4 (η-shadow of B) B *is said to be an* η*-shadow of a state* ρ*, if* $0 \leq B \leq 1$ *and* $\mathrm{Tr}\ \rho B \geq \eta$.

Lemma 3.5 [42] (Shadow Bound Lemma) *Let* $0 \leq \Pi \leq 1$ *and let* ρ *be a state such that for some* $\lambda, \mu_1, \mu_2 > 0$

$$\mathrm{Tr}\ \rho\Pi \geq 1 - \lambda \tag{3.1}$$

$$\mu_1\Pi \leq \sqrt{\Pi}\rho\sqrt{\Pi} \leq \mu_2\Pi. \tag{3.2}$$

Then

$$\frac{1-\lambda}{\mu_2} \leq \mathrm{Tr}\ \Pi \leq \frac{1}{\mu_1}. \tag{3.3}$$

If further B *is an* η*-shadow of* ρ, *one has*

$$\mathrm{Tr}\ B \geq \frac{\eta - \gamma}{\mu_2},$$

where $\gamma = \lambda$ *if* ρ *and* Π *commute and* $\gamma = \sqrt{8\lambda}$ *otherwise.*

Proof: Equation (3.3) can be archived by taking traces in (3.2) and using (3.1), noting that $\mathrm{Tr}\ \rho\Pi \leq 1$. For the $\eta-$ shadow B observe that

$$\begin{aligned} \mu_2 \mathrm{Tr}\ B &\geq \mathrm{Tr}\ \mu_2\Pi B \geq \mathrm{Tr}\ \sqrt{\Pi}\rho\sqrt{\Pi}B \\ &= \mathrm{Tr}\ (\rho B) - \mathrm{Tr}\ ((\rho - \sqrt{\Pi}\rho\sqrt{\Pi})B \geq \eta - ||\rho - \sqrt{\Pi}\rho\sqrt{\Pi}||_1. \end{aligned}$$

If ρ and Π commute, we can bound the trace norm by λ , otherwise $\sqrt{8\lambda}$ can be archived by lemma 3.6.

■

Lemma 3.6 [[44], Lemma 9] **(Gentle Operator Lemma)** *Let* ρ *be a state, and* X *a positive operator with* $X \leq \mathbb{1}$ *and* $1 - \mathrm{Tr}\,(\rho X) \leq \lambda \leq 1$. *Then*

$$\|\rho - \sqrt{X}\rho\sqrt{X}\|_1 \leq \sqrt{8\lambda}.$$

Lemma 3.7 (Gentle Double Operator Lemma) *Let* ρ *be a state, and* X, $Y \leq \mathbb{1}$ *positive operators such that* $1 - \mathrm{Tr}\,(\rho X) \leq \lambda_1 \leq 1$, $1 - \mathrm{Tr}\,(\rho Y) \leq \lambda_2 \leq 1$. *Then*

$$\|\rho - \sqrt{Y}\sqrt{X}\rho\sqrt{X}\sqrt{Y}\| \leq \sqrt{8\lambda_1} + \sqrt{8\lambda_2}.$$

Proof: Let $\bar{\rho} \triangleq \rho - \sqrt{X}\rho\sqrt{X}$ and observe that $\|\bar{\rho}\|_1 \leq \sqrt{8\lambda_1}$ by lemma 3.6. Furthermore

$$\begin{aligned}\|\rho - \sqrt{Y}\sqrt{X}\rho\sqrt{X}\sqrt{Y}\|_1 &= \|\rho - \sqrt{Y}(\rho - \bar{\rho})\sqrt{Y}\|_1 \\ &\leq \|\rho - \sqrt{Y}\rho\sqrt{Y}\|_1 + \|\sqrt{Y}\bar{\rho}\sqrt{Y}\|_1 \\ &\leq \sqrt{8\lambda_2} + \|\bar{\rho}\|_1\|Y\|_\infty \leq \sqrt{8\lambda_2} + \sqrt{8\lambda_1},\end{aligned}$$

where we used the triangle and Hölder inequality and lemma 3.6 again.

■

Let $\mathcal{H}$ be a finite dimensional Hilbert space of dimension d and $\mathfrak{X} \triangleq \mathfrak{L}(\mathcal{X})$, with $\mathcal{X}$ a finite set.

Now we construct variance-typical projectors $\Pi^n_{V,\rho,\delta}$ using typical sequences: for a diagonalization $\rho = \sum_i q_i\pi_i$ let $s_i = \sqrt{q_i(1-q_i)}$ and

$$\mathcal{T}^n_{V,\rho,\delta} = \{(i_1, \ldots, i_n) : \forall i : |N(i|i^n) - nq_i| \leq s_i\delta\sqrt{n}\},$$

and define

$$\Pi^n_{V,\rho,\delta} = \sum_{(i_1,\ldots,i_n)\in\mathcal{T}^n_{V,\rho,\delta}} \pi_{i_1} \otimes \cdots \otimes \pi_{i_n}.$$

Lemma 3.8 [[43], Lemma 3] *For every state* ρ *on* $\mathcal{H}$ *and* $n > 0$

$$\mathrm{Tr}\;\rho^{\otimes n}\Pi^n_{V,\rho,\delta} \geq 1 - \frac{d}{\delta^2}$$

$$\Pi^n_{V,\rho,\delta}\exp\{-nH(\rho) - Kd\delta\sqrt{n}\} \leq \Pi^n_{V,\rho,\delta}\rho^{\otimes n}\Pi^n_{V,\rho,\delta} \leq \Pi^n_{V,\rho,\delta}\exp\{-nH(\rho) + Kd\delta\sqrt{n}\}$$

$$\mathrm{Tr}\;\Pi^n_{V,\rho,\delta} \leq \exp\{nH(\rho) + Kd\delta\sqrt{n}\}.$$

Every η*-shadow* B *of* ρ^n *satisfies*

$$\mathrm{Tr}\;B \geq \left(\eta - \frac{d}{\delta^2}\right)\exp\{nH(\rho) - Kd\delta\sqrt{n}\}.$$

Proof: The first estimate is the Chebyshev inequality: the trace is the probability of a set of variance-typical sequences of eigenvectors of the ρ_i in the product of the measures given by the eigenvalue lists. The second estimate was proved by Winter [43] lemma 3 and the shadow bound estimate follows from the shadow bound lemma 3.5.

■

Now fix a diagonalization $\rho_x = \sum_j q_{j|x}\pi_{xj}$ (where $q_{j|x}$ becomes a stochastic matrix by definition of ρ). Then define the *conditional variance-typical projector of* ρ *given* x^n *with constant* δ to be

$$\Pi_{V,\rho,\delta^n}(x^n) \triangleq \bigotimes_{x\in\mathcal{X}} \Pi^{I_x}_{V,\rho_x,\delta}$$

where $I_x \triangleq \{i \in \{1,\ldots,n\} : x_i = x\}$. With the convention $\rho_{x^n} \triangleq \rho_{x_1} \otimes \cdots \otimes \rho_{x_n}$ we now have

Lemma 3.9 [[43], Lemma 5] (Conditional typical projector) *For all* $x^n \in \mathcal{X}^n$ *of type* $P_{\mathcal{X}}$

$$\begin{aligned} \text{Tr } (\rho_{x^n}\Pi^n_{V,\rho,\delta}(x^n)) &\geq 1 - \frac{d|\mathcal{X}|}{\delta^2} \\ \text{Tr } \Pi^n_{V,\rho,\delta}(x^n) &\leq \exp\{nH(\rho|P_{\mathcal{X}}) + Kd\sqrt{|\mathcal{X}|}\delta\sqrt{n}\} \\ \text{Tr } \Pi^n_{V,\rho,\delta}(x^n) &\geq \left(1 - \frac{d|\mathcal{X}|}{\delta^2}\right)\exp\{nH(\rho|P_{\mathcal{X}}) - Kd\sqrt{|\mathcal{X}|}\delta\sqrt{n}\} \end{aligned}$$

Every η*-shadow* B *of* ρ_{x^n} *satisfies*

$$\text{Tr } B \leq \left(\eta - \frac{d|\mathcal{X}|}{\delta^2}\right)\exp\{nH(\rho|P_{\mathcal{X}}) - Kd\sqrt{|\mathcal{X}|}\delta\sqrt{n}\}.$$

Proof: The first estimate follows simply by applying lemma 3.8 $|\mathcal{X}|$ times. The second formula is by piecing together the corresponding formulas from lemma 3.8, using $\sum_{x\in\mathcal{X}}\sqrt{P(x)} \leq \sqrt{|\mathcal{X}|}$. The rest follows immediately from lemma 3.5.

■

Definition 3.10 (Constant typical sequences) *The set of constant typical sequences is defined by*

$$\mathcal{T}_{C,P,\delta} = \{x^n \in \mathcal{X}^n : |N(x|x^n) - nP(x)| \leq \delta\sqrt{n} \text{ for all } x \in \mathcal{X}\}.$$

For $\delta = 0$ *we again get the type class* $\mathcal{T}^n_P \triangleq \mathcal{T}_{C,P,0}$ *consisting of sequences of the same type.*

Lemma 3.11 *Let P be a probability distributions and α such that $0 < \alpha \leq \frac{1}{2}$. Then for all $\beta \triangleq -\alpha \log \frac{\alpha}{|\mathcal{X}|}$*

$$\lim_{n\to\infty} P^{\otimes n}(\{\mathcal{T}^n_{C,Q} : \ Q \text{ a p.d. such that } |H(Q) - H(P)| < \beta \text{ with } ||P - Q||_1 \leq \alpha) = 1$$

Proof: Using the Pinsker inequality $D(P||Q) \geq \frac{1}{2\ln 2}||P-Q||_1^2$ and $|H(P) - H(Q)| \leq \beta$ (which is valid since $||P-Q||_1 \leq \alpha \leq \frac{1}{2}$) we get $D(P||Q) \leq \frac{\alpha^2}{2\ln 2}$, if $|H(P)-H(Q)| \geq \beta$. Hence,

$$\begin{aligned}
\sum_{Q\in\mathcal{P}(n,\mathcal{X}):|H(Q)-H(P)|\geq\beta} P^n(\mathcal{T}^n_{C,Q}) &\leq (n+1)^{|\mathcal{X}|}\max_{Q:|H(Q)-H(P)|\geq\beta} \exp\{-nD(Q||P)\} \\
&= (n+1)^{|\mathcal{X}|} \exp\{-n \min_{Q:|H(Q)-H(P)|\geq\beta} D(Q||P)\} \\
&\leq (n+1)^{|\mathcal{X}|} \exp\{-n\frac{\alpha^2}{2\ln 2}\} \stackrel{n\to\infty}{\longrightarrow} 0.
\end{aligned}$$

■

4 The Secret Sharing Source Model

Definition 4.1 (Multiple Quantum Sources)

i) *A* **(discrete memoryless) multiple (s-fold) quantum source (q-DMMS)** *is a tuple $(\mathfrak{X}_1, \ldots, \mathfrak{X}_s, \Pi, P)$ of finite C^*- algebras $\mathfrak{X}_i$, a finite set Π of pure states on $\mathfrak{X} = \mathfrak{X}_1 \otimes \cdots \otimes \mathfrak{X}_s$ and a probability distribution P on Π.*

ii) *The* **average state** *of the source is the state $P\Pi$ of $\mathfrak{X}$. Its marginal, restricted to $\mathfrak{X}^{\otimes I} = \otimes_{i\in I}\mathfrak{X}_\mathrm{i}$, is denoted $P\Pi|_I$.*

iii) *If all states $\pi \in \Pi$ are product states with respect to $\mathfrak{X}_1, \ldots, \mathfrak{X}_s$:*

$$\pi = \pi_1 \otimes \cdots \otimes \pi_s, \ \pi_i \in \mathfrak{S}(\mathfrak{X}_i),$$

the source is denoted **classically correlated**. *Then we obtain for each $J \in \{1, \ldots, n\}$ a multiple source $((\mathfrak{X}_j|j \in J), \Pi|_J, P)$ by restricting the $\pi \in \Pi$ to $\mathfrak{X}^{\otimes J}$, i.e. replacing π by $\pi|J$. W.l.o.g. $\Pi = \Pi_1 \times \cdots \times \Pi_s$.*

Definition 4.2 (Secret Sharing Source Model) *We are given a q-DMMS $(\mathfrak{X}, \mathfrak{Y}, \Pi, P)$ with two component sources. Terminal $\mathcal{X}$ ($\mathcal{Y}$) can use arbitrary quantum operations on source outputs $\mathfrak{X}^{\otimes n} = \mathfrak{X}_1 \otimes \cdots \otimes \mathfrak{X}_n$ (resp. $\mathfrak{Y}^{\otimes n} = \mathfrak{Y}_1 \otimes \cdots \otimes \mathfrak{Y}_n$).*

Further, a noiseless public quantum channel of unlimited capacity is available for communication between $\mathcal{X}$ and $\mathcal{Y}$ enabling them to send commutative subalgebras (i.e. they can send classical information only).

If the two terminals communicate, they can exchange messages or codewords over the public channel. Codewords generated by Terminal $\mathcal{X}$ are denoted by $\mathfrak{M}_i \triangleq \mathbb{C}\mathcal{M}_i$, and by Terminal $\mathcal{Y}$ by $\mathfrak{N}_i \triangleq \mathbb{C}\mathcal{N}_i$ for instances $i = 1, \ldots, k$.

For written abbreviation, we define $\mathfrak{M}_{[k]} \triangleq \mathfrak{M}_1 \otimes \cdots \mathfrak{M}_k$ for $k \in \mathbb{N}$. Note that $\mathfrak{M}_i$ and $\mathfrak{N}_i$ are commutative algebras generated by finite sets $\mathcal{M}_i$ and $\mathcal{N}_i$.

Definition 4.3 (Secret Sharing Strategy)

init) *In the beginning* $\rho^{\otimes n}$ *is a quantum state on* $\mathfrak{X}^{\otimes n} \otimes \mathfrak{Y}^{\otimes n}$. *Let* $\mathfrak{R}_i, \mathfrak{L}_i$ *be finite dimensional subalgebras of* $\mathfrak{U}$, *furthermore let* $\mathfrak{M}_i = \mathbb{C}\mathcal{M}_i$, $\mathfrak{N}_i = \mathbb{C}\mathcal{N}_i$ *commutative subalgebras of* $\mathfrak{U}$ *for* $i \in \{1, \cdots, k\}$.

1st step) *Terminal* $\mathcal{X}$ *uses a completely positive map*

$$\phi_1 : \mathfrak{X}^{\otimes n} \to \mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_1 \otimes \mathfrak{M}_1$$

and sends $\mathfrak{M}_1$ *to* $\mathcal{Y}$. *Terminal* $\mathcal{Y}$ *uses the completely positive map*

$$\psi_1 : \mathfrak{Y}^{\otimes n} \to \mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_1 \otimes \mathfrak{N}_1$$

and sends $\mathfrak{N}_1$ *to* $\mathcal{X}$, *i.e. on the common state* $\rho^{\otimes n}$ *the action* $\rho^{\otimes n} \stackrel{\phi_1 \otimes \psi_1}{\longrightarrow} \rho_1$ *takes place giving a state on* $\mathfrak{X}^{\otimes n} \otimes \mathfrak{Y}^{\otimes n} \otimes \mathfrak{R}_1 \otimes \mathfrak{L}_1 \otimes \mathfrak{N}_1 \otimes \mathfrak{M}_1$ *such that*

$$\rho_1 = \sum_{i,j,k,l} p_1(i,j,k,l) \rho_1^{\mathcal{X}} \otimes \rho_1^{\mathcal{Y}} \otimes R_i \otimes L_j \otimes [k] \otimes [l].$$

i-th step: *Terminal* $\mathcal{X}$ *uses the following completely positive map*

$$\phi_i : \mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_{[i-1]} \otimes \mathfrak{N}_{[i-1]} \to \mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_{[i]} \otimes \mathfrak{N}_{[i-1]} \otimes \mathfrak{M}_i$$

and sends $\mathfrak{M}_i$ *to* $\mathcal{Y}$. *Terminal* $\mathcal{Y}$ *uses the analogous completely positive map*

$$\psi_i : \mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_{[i-1]} \otimes \mathfrak{M}_{[i-1]} \to \mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_{[i]} \otimes \mathfrak{M}_{[i-1]} \otimes \mathfrak{N}_i.$$

I.e. together they perform the action $\rho_{i-1} \stackrel{\phi_i \otimes \psi_i}{\longrightarrow} \rho_i$ *such that (after trivial reordering)* ρ_i *is a state on* $\mathfrak{X}^{\otimes n} \otimes \mathfrak{Y}^{\otimes n} \otimes \mathfrak{R}_{[i]} \otimes \mathfrak{L}_{[i]} \otimes \mathfrak{N}_{[i]} \otimes \mathfrak{M}_{[i]}$

k-th step: *After the last communication terminal* $\mathcal{X}$ *measures their states using a POVM on* $\mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_{[k]} \otimes \mathfrak{N}_{[k]}$ *which is indexed by* $\{1, \ldots, M\}$ *giving a probability distribution* K. *Bob also uses a POVM on* $\mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_{[k]} \otimes \mathfrak{M}_{[k]}$ *with the same indexing, resulting in a probability distribution* L.

Observe that $\mathcal{X}$ uses mathematically a quantum operation $K : \mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_{[k]} \otimes \mathfrak{N}_{[k]} \to \mathfrak{K}$ in the last step, where $\mathfrak{K}$ is a commutative *-subalgebra of dimension M. The same holds analogously for $\mathcal{Y}$.

Remark 4.4 *Note that this Secret Sharing Strategy is a general LOCC (Local Operations, Classical Communication) scheme. Each terminal can apply an arbitrary quantum operation, where we think of* $\mathfrak{R}, \mathfrak{L}$ *as being "full quantum registers" for storage of quantum information (or, more precisely, states) for later computation, and* $\mathfrak{M}, \mathfrak{N}$ *being "classical registers" storing classical data (e.g. from measurements) for communication.*

If ρ is a separable state, i.e. the entanglement of formation is 0, then from the previous remark no entanglement can be achieved between the two terminals $\mathcal{X}$ and $\mathcal{Y}$ by this scheme. More precisely, the entanglement of formation can not change by this strategy for a given start state ρ.

Let $f : \mathcal{A} \to \mathcal{B}$ be a function between finite sets and A a POVM indexed by elements in $\mathcal{A}$. In the direct part of the following proofs, we will only use quantum operations of the following form:

$$\begin{aligned} \Phi : \mathfrak{X}^{\otimes n} &\to \mathfrak{X}^{\otimes n} \otimes \mathfrak{R} \otimes \mathfrak{M} \\ \rho &\to \sqrt{A_i}\rho\sqrt{A_i} \otimes [i] \otimes [f(i)] \end{aligned} \tag{4.1}$$

Remark 4.5 *Since* A *is a POVM the map (4.1) is clearly completely positive according to theorem 2.1. Further observe that we deal only with commutative *-subalgebras* $\mathfrak{R}, \mathfrak{L}$.

Definition 4.6 *A number* R *will be called an achievable secret key rate for the Secret Sharing Source Model if for every* $\epsilon > 0$ *and sufficiently large* n *there exists a Secret Sharing Strategy such that* K *and* L *satisfy*

$$\Pr\{K \neq L\} < \epsilon \tag{4.2}$$

$$\frac{1}{n} I(\mathfrak{M}_{[k]}, \mathfrak{N}_{[k]} \wedge K) < \epsilon \tag{4.3}$$

$$\frac{1}{n} H(K) > R - \epsilon \tag{4.4}$$

$$\frac{1}{n} \log |\mathcal{K}| < \frac{1}{n} H(K) + \epsilon \tag{4.5}$$

The maximal achievable secret key rate is denoted by the **secret key capacity** C_S.

Here (4.2) assures that the two terminals have indeed generated a common key (with a small probability of error). With (4.3) we have a secrecy constraint: No information about the key has been given away by communication over the public channel. The last inequality assures that the distribution of the key is nearly uniform in an entropy sense, i.e. we have a "good" key for encryption.

Without loss of generality, let $\mathcal{K} = \{1, \ldots, M\}$ and $m \in \{1, \ldots, M\}$ a message, which should be transmitted securely form terminal $\mathcal{X}$ to terminal $\mathcal{Y}$. $\mathcal{X}$ sends the ciphertext $c = m + K \mod M$ to $\mathcal{Y}$, who can decode c with small probability of error. We will show that the wiretapper, who has full access to the public channel, gets no information concerning m :

Lemma 4.7 (Secure Transmission) *For a random variable* m *with values in* $\{1,\ldots,M\}$ *and independent of* $(\mathfrak{M}_{[k]},\mathfrak{N}_{[k]},K)$,

$$\frac{1}{n}I(\mathfrak{M}_{[k]},\mathfrak{N}_{[k]},m\oplus K\wedge m)\leq 2\epsilon,$$

if (4.3), (4.5) are valid and $\oplus$ *defines calculation* $\bmod M$.

Proof: First note that $\mathfrak{M}$, $\mathfrak{N}$ are commutative subalgebras.

$$\begin{aligned}
I(\mathfrak{M}_{[k]},\mathfrak{N}_{[k]},(m\oplus K)\wedge m) &\overset{(i)}{=} I(m\oplus K\wedge m|\mathfrak{M}_{[k]},\mathfrak{N}_{[k]})\\
&= H(m\oplus K|\mathfrak{M}_{[k]},\mathfrak{N}_{[k]})-H(m\oplus K|m,\mathfrak{M}_{[k]},\mathfrak{N}_{[k]})\\
&\leq \log N-H(K|m,\mathfrak{M}_{[k]},\mathfrak{N}_{[k]})\\
&\overset{Eq.(4.5)}{\leq} H(K)+n\epsilon-H(K|m,\mathfrak{M}_{[k]},\mathfrak{N}_{[k]})\\
&= I(K\wedge m,\mathfrak{M}_{[k]},\mathfrak{N}_{[k]})+n\epsilon\\
&\overset{Eq.(4.3)}{\leq} 2n\epsilon
\end{aligned}$$

Since m is independent of the state on $(\mathfrak{M}_{[k]},\mathfrak{N}_{[k]})$, (i) is correct.

■

Definition 4.8 (Source States) *Let* $(\mathfrak{X},\mathfrak{Y},\Pi,P)$ *be a q-DMMS with* $\mathfrak{X}=\mathfrak{L}(\mathcal{H}_{\mathcal{X}})$ *and* $\mathfrak{Y}=\mathfrak{L}(\mathcal{H}_{\mathcal{Y}})$ $*-$*subalgebras over finite dimensional Hilbert spaces.*

i) The Secret Sharing Source Model is called **fully quantum**, *if* Π *is a set of arbitrary quantum states.*

ii) The Secret Sharing Source Model is denoted **separable**, *if* Π *is a set of separable quantum states, i.e. the average state* $P\Pi$ *is given by* $\hat{\rho}=\sum_i p_i\hat{\sigma}_i\otimes\hat{\tau}_i$.

iii) The Secret Sharing Source Model is called **semi-classical**, *if beside ii) there is also an orthogonal basis* $|i\rangle$ *of* $\mathcal{H}_{\mathcal{X}}$ *such that* $\sigma_i=|i\rangle\langle i|$. *Thus,* $\mathfrak{X}$ *can be modelled by* $\mathbb{C}\mathcal{X}$.

Now we define recursively a special orthogonal class of states, denoted oc-type states, representing the special orthogonal-channel character :

iv) ρ *is called a* **oc-type state** *if the following is true:*

1) $\hat{\rho}=\sum_i p_i|i\rangle\langle i|\otimes\hat{\tau}_i$ *or*

2) If the states $\hat{\rho}_1, \ldots, \hat{\rho}_l$ *are oc-type states and* $\lambda_i \geq 0,\ 1 \leq i \leq l,\ \sum_{i=1}^{l} \lambda_i = 1$ *such that*

$$\text{for all } i,j \in \{1,\ldots,l\} \text{ and all } \mathfrak{Z} \in \{\mathfrak{X},\mathfrak{Y}\} : \mathrm{Tr}_{\mathfrak{Z}}\hat{\rho}_i \perp \mathrm{Tr}_{\mathfrak{Z}}\hat{\rho}_j$$

then $\hat{\rho} = \sum_{i=1}^{l} \lambda_i \hat{\rho}_i$ *is also an oc-type state.*
Observe that the semi-classical states are involved in the oc-type states. The Secret Sharing Source Model is denoted **oc-type** *if the average state* $P\Pi = \hat{\rho}$.

5 Secret Key Capacity Theorem for Semi-Classical States

Theorem 5.1 (Main Theorem) *The secret key-capacity* C_S *for the semi-classical Secret Sharing Source Model equals the quantum mutual information and is attainable by using a single forward transmission, i.e.*

$$C_{S,semi-classical,\rightarrow} = I(\mathfrak{X} \wedge \mathfrak{Y}).$$

Before we prove this theorem, we need the following lemma due to Ahlswede and Körner (see [4]):

Lemma 5.2 (Code Partition Lemma) *Consider the q-DMC* $W : \mathcal{X} \rightarrow \mathfrak{S}(\mathfrak{Y})$, P *a probability distribution on* $\mathcal{X}, \lambda, \delta, \eta \geq 0$. *Then for* $n \geq n_0(|\mathcal{X}|, dim\ \mathcal{H}, \lambda, \delta, \eta)$ *there exists* $N \leq \exp\{n(H(P) - I(P;W) + 3\delta)\}$ *many* $(n,\lambda)-$ *codes with pairwise disjoint "large" codebooks* $\mathcal{C}_i$: $M \triangleq |\mathcal{C}_i| \geq \exp\{n(I(P;W) - 2\delta)\}$ *such that* $P^n(\bigcup_{i=1}^{N} \mathcal{C}_i) \geq \eta$. *This is also true for the constant type sequences with same type.*

Proof: Choose $\alpha > 0$ such that $P^{\otimes n}(\mathcal{T}^n_{V,P,\alpha}) \geq 1 - \eta/2$ and n large enough such that for every $\mathcal{A} \subset \mathcal{T}^n_{V,P,\alpha}$ with $P^{\otimes n}(\mathcal{A}) \geq \eta/2$ there is a (n,λ)-code with codebook $\mathcal{C} \subset \mathcal{A}$ and $|\mathcal{C}| \geq \exp(n(I(P;W) - 2\delta))$ from theorem 2.7. Choosing such a codebook $\mathcal{C}_1 \subset \mathcal{A}_\infty = \mathcal{T}^n_{V,P,\alpha}$ and inductively $\mathcal{C}_i \subset \mathcal{C}_{i-1} \subset \mathcal{A}_i = \mathcal{A}_{i-1} \backslash \mathcal{C}_{i-1}$ until $P^{\otimes n}(\mathcal{A}_i) < \eta/2$, we have from lemma 3.2 $|\mathcal{T}^n_{V,P,\alpha}| \leq \exp\{n(H(P) + \delta)\}$ for large n. So we get

$$N \exp\{n(I(P;W) - 2\delta)\} \leq \sum_{i=1}^{N} |\mathcal{C}_i| \leq |\mathcal{T}^n_{V,P,\alpha}|.$$

Next we will show that there exists a subcode with constant type property and all codewords in the codebooks of the same type. This is easily seen by type counting but we will give a more precise proof here:

Fix $i \in \{1, \ldots, N\}$ and define for $\beta > 0$

$$\bar{C}_i(\beta) \triangleq C_i \cap \mathcal{T}^n_{C,P,\beta}.$$

Now for sufficiently large n we have $P^{\otimes n}(\bar{C}_i(\beta)) \geq \frac{\eta}{4}$. According to the pigeonhole principle, there exists a constant type Q with $|H(P) - H(Q)| \leq \beta$ and $P^{\otimes n}(C_i \cap \mathcal{T}^n_Q) \geq \frac{\eta}{4} \cdot P^{\otimes n}(\mathcal{T}^n_Q)$. Since all the sequences in $\mathcal{T}^n_Q$ are of the same type, they are equiprobable, and we get

$$\begin{aligned} |C_i \cap \mathcal{T}^n_Q| &\geq \frac{\eta}{4}|\mathcal{T}^n_Q| \geq \frac{\eta}{4(n+1)^{|\mathcal{X}|}} \exp\{nH(Q)\} \\ &\geq \frac{\eta}{4} \frac{1}{(n+1)^{|\mathcal{X}|}} \exp\{n(H(P) - \beta)\}. \end{aligned}$$

This applies to all $\beta \geq 0$, and especially to $\beta = H(\mathfrak{X}|\mathfrak{Y}) + 3\delta - \log \frac{\eta}{4(n+1)^{|\mathcal{X}|}}$, where n can be made sufficiently large to ensure the positivity restriction. Now

$$|C_i \cap \mathcal{T}^n_Q| \geq \exp\{n(I(P;W)) - 3\delta\}.$$

giving a new codebook $\mathcal{C}'_i \triangleq \mathcal{C}_i \cap \mathcal{T}^n_Q$. This method will be used several times, denoted by type counting.

■

Now we will prove the achievability in the semi-classical case.

Proof of theorem 5.1: (cf. [2], Proposition I) The idea can be divided into two parts:

- At first terminal $\mathcal{X}$ transmits a code of $\mathfrak{X}^{\otimes n}$ of rate $\approx H(\mathfrak{X}|\mathfrak{Y})$, determining a codebook $\mathcal{C}_i$.
- $\mathcal{Y}$ can then decode with small probability of error, since he can measure $\mathfrak{Y}$, given the codebook $\mathcal{C}_i$.

Since $\rho = \sum_x |x\rangle\langle x| \otimes W_x$ we can establish a q-DMC $W : \mathcal{X} \to \mathfrak{Y}_*$ with same type, and each of size

$$M = \lceil \exp\{n(I(P;W) - 3\delta\} \rceil. \tag{5.1}$$

from lemma 5.2. For this (n, ϵ) -codes (g_i, D_i) we use the identity mapping as an encoding, so the message sets are coincident with the codeword sets.

Let $\{E_{i_j}\}_{i,j}, 1 \leq i \leq N, 1 \leq j \leq M$ be orthogonal projection measurements acting on $\mathfrak{X}^{\otimes n}$ for the i-th codebook $\mathcal{C}_i$ regarding the j-th codeword $x^n_{i,j}$ randomly chosen in $\mathcal{C}_i$ and $\{D_{i_j}\}_{i,j}, 1 \leq i \leq N, 1 \leq j \leq M$ the decoding measurements of the i-th codebook $\mathcal{C}_i$ regarding the j-th codeword $W_{x^n_{i,j}}$, respectively.

Extending the encoding measurement to a POVM E, by adjoining an encoding error $E_0 = \mathbb{1} - \sum_{i=1}^{N}\sum_{j=1}^{M} E_{i_j}$, we further define a "codebook distinguishing" POVM $\bar{E}$ by $\bar{E}_i \triangleq \sum_{j=1}^{M} E_{i_j}$ with encoding error $\bar{E}_0$. Notice that the POVM E is a refinement of $\bar{E}$.

In the first step, terminal $\mathcal{X}$ uses the quantum operation

$$\phi_1 : \rho_{\mathcal{X}} \to \sum_{i=0}^{N} \sqrt{\bar{E}_i}\rho_{\mathcal{X}}\sqrt{\bar{E}_i} \otimes [i] \otimes [i] \; + \; \sqrt{\bar{E}_0}\rho_{\mathcal{X}}\sqrt{\bar{E}_0} \otimes [0] \otimes [0],$$

i.e. the encoding POVM $\bar{E}$ produces a random variable described by $\mathfrak{M}_1$ without making a real measurement. A short calculation shows that $\mathfrak{M}_1 = [i]$ if $x^n \in \mathcal{C}_i$ was the source input for terminal $\mathcal{X}$. Now terminal $\mathcal{X}$ sends $\mathfrak{M}_1$ to $\mathcal{Y}$. Terminal $\mathcal{Y}$ does nothing in the first step (i.e. he applies the quantum operation $\psi_1 : \rho_{\mathcal{Y}} \to \rho_{\mathcal{Y}} \otimes \mathbb{1} \otimes \mathbb{1}$.)

In the end-round terminal $\mathcal{X}$ uses the POVM K on $\mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_{[1]} \otimes \mathfrak{N}_{[1]}$ given by $K_j = \sum_{i=1}^{N} E_{i_j} \otimes [i] \otimes \mathbb{1}$ and $K_0 = \mathbb{1} \otimes [0] \otimes \mathbb{1}$, giving an error.

Now terminal $\mathcal{Y}$ uses the decoding POVM D defined by $D_j \triangleq \sum_{i=1}^{N} D_{i_j} \otimes i$ for $j = 1, \ldots M$ and $D_0 \triangleq \mathbb{1} - \sum_{j=1}^{M} D_j$ as the decoding error. Observe that $\sum_{j=0}^{M} D_j = \mathbb{1} \otimes \mathbb{1}$, fulfilling the POVM property.

Applying this POVM on $\mathfrak{Y}^{\otimes n} \otimes \mathfrak{M}_1$ terminal $\mathcal{Y}$ gets $L = j$ if $\mathfrak{M}_1 = [i]$ and codebook $\mathcal{C}_i$ was used for encoding. Otherwise 0 was measured and we set L to a random value in $\{1, \ldots, M\}$ independent of $\rho^{\otimes n}$ in $\mathfrak{X}^{\otimes n}, \mathfrak{Y}^{\otimes n}$.

Since for the q-DMC W we have (n, ϵ)-codes, we get

$$\Pr(L \neq K | \mathfrak{M}_1 = [i]) = 1 - \sum_{j=1}^{M} \mathrm{Tr}\ (\rho^{\otimes n} E_{i_j} \otimes D_{i_j}) \leq \epsilon, \qquad i = 1, \ldots, N.$$

Observing that $\Pr(\mathfrak{M}_1 = [0]) = \Pr(\mathcal{X}^n \setminus \bigcup_{i=1}^{N} \mathcal{C}_i) \leq \eta$ we get

$$\begin{aligned} \Pr(L \neq K) &= \sum_{i=1}^{N} \Pr(\mathfrak{M}_1 = [i]) \Pr(L \neq K | \mathfrak{M}_1 = [i]) + \Pr(\mathfrak{M}_1 = [0]) \Pr(L \neq K | \mathfrak{M}_1 = [0]) \\ &\leq \epsilon \sum_{i=1}^{N} \Pr(\mathfrak{M}_1 = [i]) + \Pr(\mathfrak{M}_1 = [0]) \leq \epsilon + \eta. \end{aligned}$$

Since each $\mathcal{C}_i$, $1 \leq i \leq N$, consists of sequences of the same type, i.e. for all $x^n \in \mathcal{C}_i$: $\frac{1}{n} N(x|x^n) = P_i$ and $P^n(x^n) = \Pi_{x \in \mathcal{X}} P(x)^{N(x|x^n)} = \Pi_{x \in \mathcal{X}} P(x)^{nP_i}$ for all $x \in \mathcal{X}$, we get for $1 \leq i \leq N$:

$$\begin{aligned}\Pr(K=j|\mathfrak{M}_1=[i]) &= \frac{\Pr(K=j,\ \mathfrak{M}_1=[i])}{\Pr(\mathfrak{M}_1=[i])}\\ &= \frac{\mathrm{Tr}\ \rho^{\otimes n}(E_{i_j}\otimes \mathbb{1})}{\mathrm{Tr}\ \rho^{\otimes n}(\bar{E}_i\otimes \mathbb{1})}\\ &= \frac{P^{\otimes n}(x^n_{i,j})}{\sum_{x^n\in\mathcal{C}_i} P^{\otimes n}(x^n)}\\ &= \frac{\Pi_{x\in\mathcal{X}}P(x)^{nP_i}}{\sum_{x^n\in\mathcal{C}_i}\Pi_{x\in\mathcal{X}}P(x)^{nP_i}} = \frac{1}{M},\end{aligned}$$

where $x^n_{i,j}\in\mathcal{C}_i$ is the j-th codeword in the codebook $\mathcal{C}_i$.

For $\mathfrak{M}_1=[0]$ (encoding error) terminal $\mathcal{X}$ and $\mathcal{Y}$ set K randomly in $\{1,\dots M\}$, achieving a uniform distribution on $\{1,\cdots,M\}$ (see definition 4.5). Checking definition 4.4 now gives

$$\frac{1}{n}H(K)=\frac{1}{n}I(K\wedge\mathfrak{M}_1)+H(K|\mathfrak{M}_1)=\frac{1}{n}\log M,$$

since $I(K\wedge\mathfrak{M}_1)=0$. Immediately we get

$$\frac{1}{n}H(K)\geq I(P;W)-3\delta$$

by (5.1) achieving the secret key-rate $I(P;W)=I(\mathfrak{X}\wedge\mathfrak{Y})$. Definition 4.3 can also be granted since the quantum subsystems $\mathfrak{M}_1$ and $\mathfrak{N}_1$ are independent of K. The converse follows from the general upper bound theorem 5.3.

■

The following theorem will provide a general upper bound to $\frac{1}{n}H(K)$, implying a converse to theorem 5.1 and theorem 6.2.

Theorem 5.3 (General Upper Bound) *Let $\mathfrak{X}^{\otimes n},\mathfrak{Y}^{\otimes n},\mathfrak{R}_i,\mathfrak{L}_i,\mathfrak{N}_i,\mathfrak{M}_i,\mathfrak{K},\mathfrak{L}$ be compatible *-subalgebras of the $\mathbb{C}^*$-algebra $\mathfrak{U}$ given by the Secret Sharing Strategy and ρ_u a appropriate fixed overall state on $\mathfrak{U}$. Let $\rho^{\otimes n}_{\mathcal{X}}=i_x\rho_u$, $\rho^{\otimes n}_{\mathcal{Y}}=i_y\rho_u$, i.e. $\rho^{\otimes n}=\rho^{\otimes n}_{\mathcal{X}}\otimes\rho^{\otimes n}_{\mathcal{Y}}=i_x\rho\otimes i_y\rho$, where i_x and i_y are the inclusion maps of $\mathfrak{X}^{\otimes n}$ in $\mathfrak{U}$ and $\mathfrak{Y}^{\otimes n}$ in $\mathfrak{U}$, respectively. Further let $K:\mathfrak{X}^{\otimes n}\otimes\mathfrak{R}_{[i]}\otimes\mathfrak{N}_{[i]}$, $L:\mathfrak{Y}^{\otimes n}\otimes\mathfrak{L}_{[i]}\otimes\mathfrak{M}_{[i]}$ be the observables defined by the Secret Sharing Strategy. Then for every $\epsilon>0$ and arbitrary separable Secret Sharing Model state ρ*

$$\frac{1}{n}H(K)\leq I_\rho(\mathfrak{X}\wedge\mathfrak{Y})$$

$$
\begin{array}{ccccc}
\mathfrak{X}^{\otimes n} & \xrightarrow{i_x} & \mathfrak{U} & \xleftarrow{i_y} & \mathfrak{Y}^{\otimes n} \\
\downarrow \phi_1 & \searrow \varphi & \uparrow \mu & \swarrow \hat{\varphi} & \downarrow \psi_1 \\
\mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_1 \otimes \mathfrak{M}_1 & & \mathfrak{X}^{\otimes n} \otimes \mathfrak{Y}^{\otimes n} & & \mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_1 \otimes \mathfrak{N}_1 \\
\vdots & & & & \vdots \\
\mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_{[i-1]} \otimes \mathfrak{N}_{[i-1]} & & & & \mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_{[i-1]} \otimes \mathfrak{M}_{[i-1]} \\
\downarrow \phi_i & & & & \downarrow \psi_i \\
\mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_{[i]} \otimes \mathfrak{N}_{[i-1]} \otimes \mathfrak{M}_i & & & & \mathfrak{Y}^{\otimes n}_{[i]} \otimes \mathfrak{L}_{[i]} \otimes \mathfrak{M}_{[i-1]} \otimes \mathfrak{N}_i \\
\vdots & & & & \vdots \\
\downarrow K & & & & \downarrow L \\
\mathfrak{K} & & & & \mathfrak{L}
\end{array}
$$

This scheme will help to understand the dynamics in the Secret Sharing Strategy used by the proofs for the general upper bound.

Proof: With $\rho_0 \triangleq \rho^{\otimes n}$ we get the following inequality chain, using the notation of the above diagram:

$$
\begin{aligned}
I_{\rho_0}(\mathfrak{X}^{\otimes n} \wedge \mathfrak{Y}^{\otimes n}) + n\epsilon \quad &= \quad D(\mu_*(\rho_0)||\varphi\mu_*(\rho_0) \otimes \hat{\varphi}\mu_*(\rho_0)) + n\epsilon \\
&\overset{\text{Th. 2.3}}{\geq} \quad D_{\rho_1}((\phi_1 \otimes \mathbb{1})_*\mu_*(\rho_0)||\phi_1\varphi\mu(\rho_0) \otimes \hat{\varphi}\mu_*(\rho_0)) + n\epsilon \\
&\overset{\text{Th. 2.3}}{\geq} \quad D_{\rho_1}((\mathbb{1} \otimes \psi_1)_*(\phi_1 \otimes \mathbb{1})_*\mu_*(\rho_0)||\phi_1\varphi\mu(\rho_0) \otimes \psi_1\hat{\varphi}\mu_*(\rho_0)) + n\epsilon \\
&= \quad I_{\rho_1}(\mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_1 \otimes \mathfrak{M}_1 \wedge \mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_1 \otimes \mathfrak{N}_1) + n\epsilon \\
&\geq \quad I_{\rho_1}(\mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_1 \wedge \mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_1 \otimes \mathfrak{N}_1|\mathfrak{M}_1) + n\epsilon \\
&\geq \quad I_{\rho_1}(\mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_1 \wedge \mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_1|\mathfrak{M}_1, \mathfrak{N}_1) + n\epsilon \\
&\geq \quad I_{\rho_1}(\mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_1 \otimes \mathfrak{N}_1 \wedge \mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_1 \otimes \mathfrak{M}_1|\mathfrak{M}_1, \mathfrak{N}_1) + n\epsilon \\
&\overset{\text{Lem. 5.5}}{\geq} \quad I_{\rho_k}(\mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_{[k]} \otimes \mathfrak{N}_{[k]} \wedge \mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_{[k]} \otimes \mathfrak{M}_{[k]}|\mathfrak{M}_{[k]}, \mathfrak{N}_{[k]}) + n\epsilon \\
&\overset{\text{Lem. 2.5}}{\geq} \quad I_{\rho_k}(K \wedge L|\mathfrak{M}_{[k]}, \mathfrak{N}_{[k]}) + n\epsilon \qquad (5.2) \\
&\overset{\text{Eq. (4.3)}}{\geq} \quad I_{\rho_k}(K,\ \mathfrak{M}_{[k]}, \mathfrak{L}_{[k]} \wedge L) \\
&\geq \quad I_{\rho_k}(K \wedge L) \qquad (5.3)
\end{aligned}
$$

Since with i.i.d sources $I_{\rho^{\otimes n}}(\mathfrak{X}^{\otimes n} \wedge \mathfrak{Y}^{\otimes n}) = nI_\rho(\mathfrak{X} \wedge \mathfrak{Y})$ and $H(K) = H_{\rho_k}(K)$, we obtain the result using the FANO-inequality theorem 2.6 and definition 4.2:

$$\begin{aligned}
\frac{1}{n}H_{\rho_k}(K) &= \frac{1}{n}I_{\rho_k}(K \wedge L) + \frac{1}{n}H_{\rho_k}(K|L) \\
&\overset{Eq.(5.3)}{\leq} I_\rho(\mathfrak{X} \wedge \mathfrak{Y}) + \epsilon + \frac{1}{n}H_{\rho_k}(K|L) \\
&\overset{\text{Fano ineq. 2.6}}{\leq} I_\rho(\mathfrak{X} \wedge \mathfrak{Y}) + \epsilon + h(\epsilon)/n + \epsilon \log(|\mathcal{K}| - 1)/n.
\end{aligned}$$

Observe that the two rightmost terms tend to zero for n sufficiently large.

■

Remark 5.4 *We conjecture that the upper bound derived here is also true in the full quantum Secret Sharing Source Model.*

We still have to prove the following recursion lemma used in the previous proof dealing with the recursive structure of the Source Sharing Model protocol.

Lemma 5.5 *With the assumptions of theorem 5.3, the following recursive expression for the Secret Sharing Strategy is valid for arbitrary separable states ρ_1 :*

$$I_{\rho_1}(\mathfrak{X}^{\otimes n}\mathfrak{R}_1\mathfrak{N}_1 \wedge \mathfrak{Y}^{\otimes n}\mathfrak{L}_1\mathfrak{M}_1|\mathfrak{M}_1, \mathfrak{N}_1) \geq I_{\rho_k}(\mathfrak{X}^{\otimes n}\mathfrak{R}_{[k]}\mathfrak{N}_{[k]} \wedge \mathfrak{Y}^{\otimes n}\mathfrak{L}_{[k]}\mathfrak{M}_{[k]}|\mathfrak{M}_{[k]}, \mathfrak{N}_{[k]})$$

Proof: We state the proof by induction starting with k=2:

$$\begin{aligned}
& I_{\rho_1}(\mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_1 \otimes \mathfrak{N}_1 \wedge \mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_1 \otimes \mathfrak{M}_1|\mathfrak{M}_1, \mathfrak{N}_1) \\
\overset{\text{Lem. 2.5}}{\geq} & I_{\rho_2}(\mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_2 \otimes \mathfrak{N}_1 \otimes \mathfrak{M}_2 \wedge \mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_2 \otimes \mathfrak{M}_1 \otimes \mathfrak{N}_2|\mathfrak{M}_1, \mathfrak{N}_1) \\
\overset{(i)}{\geq} & I_{\rho_2}(\mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_{[2]} \otimes \mathfrak{N}_1 \wedge \mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_{[2]} \otimes \mathfrak{M}_1 \otimes \mathfrak{N}_2|\mathfrak{M}_1, \mathfrak{N}_1, \mathfrak{M}_2) \\
\overset{(ii)}{\geq} & I_{\rho_2}(\mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_{[2]} \otimes \mathfrak{N}_1 \otimes \mathfrak{N}_2 \wedge \mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_{[2]} \otimes \mathfrak{M}_1 \otimes \mathfrak{M}_2|\mathfrak{M}_1, \mathfrak{N}_1, \mathfrak{M}_2, \mathfrak{N}_2) \\
\overset{\text{Definition}}{=} & I_{\rho_2}(\mathfrak{X}^{\otimes n} \otimes \mathfrak{R}_{[2]} \otimes \mathfrak{N}_{[2]} \wedge \mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_{[2]} \otimes \mathfrak{M}_{[2]}|\mathfrak{M}_{[2]}, \mathfrak{N}_{[2]})
\end{aligned}$$

Here (i),(ii) are simple exchange rules considering the commutativity of $\mathfrak{M}_{[k]}, \mathfrak{N}_{[k]}$.

Now for $k-1 \to k$ we obtain:

$$
\begin{aligned}
& I_{\rho_{k-1}}(\mathfrak{X}^{\otimes n}\otimes\mathfrak{R}_{[k-1]}\otimes\mathfrak{N}_{[k-1]}\wedge\mathfrak{Y}^{\otimes n}\otimes\mathfrak{L}_{[k-1]}\otimes\mathfrak{M}_{[k-1]}|\mathfrak{M}_{[k-1]},\mathfrak{N}_{[k-1]}) \\
\overset{(i)}{\geq}\ & I_{\rho_k}(\mathfrak{X}^{\otimes n}\otimes\mathfrak{R}_{[k]}\otimes\mathfrak{N}_{[k-1]}\otimes\mathfrak{M}_k\wedge\mathfrak{Y}^{\otimes n}\otimes\mathfrak{L}_{[k]}\otimes\mathfrak{M}_{[k-1]}\otimes\mathfrak{N}_k|\mathfrak{M}_{[k-1]},\mathfrak{N}_{[k-1]}) \\
\overset{(ii)}{\geq}\ & I_{\rho_k}(\mathfrak{X}^{\otimes n}\otimes\mathfrak{R}_{[k]}\otimes\mathfrak{N}_{[k-1]}\wedge\mathfrak{Y}^{\otimes n}\otimes\mathfrak{L}_{[k]}\otimes\mathfrak{M}_{[k-1]}\otimes\mathfrak{N}_k|\mathfrak{M}_{[k-1]},\mathfrak{N}_{[k-1]},\mathfrak{M}_k) \\
\overset{(iii)}{\geq}\ & I_{\rho_k}(\mathfrak{X}^{\otimes n}\otimes\mathfrak{R}_{[k]}\otimes\mathfrak{N}_{[k-1]}\wedge\mathfrak{Y}^{\otimes n}\otimes\mathfrak{L}_{[k]}\otimes\mathfrak{M}_{[k-1]}|\mathfrak{M}_{[k-1]},\mathfrak{N}_{[k-1]},\mathfrak{M}_k,\mathfrak{N}_k) \\
\overset{(iv)}{\geq}\ & I_{\rho_k}(\mathfrak{X}^{\otimes n}\otimes\mathfrak{R}_{[k]}\otimes\mathfrak{N}_{[k-1]}\otimes\mathfrak{N}_k\wedge\mathfrak{Y}^{\otimes n}\otimes\mathfrak{L}_{[k]}\otimes\mathfrak{M}_{[k-1]}\otimes\mathfrak{M}_k|\mathfrak{M}_{[k-1]},\mathfrak{N}_{[k-1]},\mathfrak{M}_k,\mathfrak{N}_k) \\
\overset{(v)}{=}\ & I_{\rho_k}(\mathfrak{X}^{\otimes n}\otimes\mathfrak{R}_{[k]}\otimes\mathfrak{N}_{[k]}\wedge\mathfrak{Y}^{\otimes n}\otimes\mathfrak{L}_{[k]}\otimes\mathfrak{M}_{[k]}|\mathfrak{M}_{[k]},\mathfrak{N}_{[k]})
\end{aligned}
$$

Here, (i) is given by the data processing lemma 2.5, (ii)-(iv) by simple exchange rules, observing that $\mathfrak{M}_{[k]},\mathfrak{N}_{[k]}$ are commutative *-subalgebras and (v) by definition of $\mathfrak{M}_{[k]},\mathfrak{N}_{[k]}$. Now we can reduce the inequality inductively, in order to get the result.

■

6 Secret Key Capacity for oc-type States

Definition 6.1 *The* **Recursion Deepness** *of an oc-type state is the maximal number of rounds used to build the state by the recursive definition 4.8, starting from a standard semi-classical state.*

Notice that, for example, the state $\rho=\sum_i|i\rangle\langle i|\otimes W_i$ has Recursion Deepness 1 by definition. Let $\mathfrak{X}=\mathfrak{L}(\mathcal{H}_\mathcal{X}),\mathfrak{Y}=\mathfrak{L}(\mathcal{H}_\mathcal{Y})$.
With $\mathcal{I}\triangleq\{1,\ldots,|\mathcal{I}|\},\mathcal{J}\triangleq\{1,\ldots,|\mathcal{J}|\}$ finite sets we define

$$\hat{\rho}\triangleq\sum_{i\in I}p_i\sum_{j\in J}q_{j_i}e_{j_i}\otimes|j_i\rangle\langle j_i|\text{ on }\mathfrak{X}_*\otimes\mathfrak{Y}_*$$

with $p_i,q_{j_i}\geq 0$ for all $i\in\mathcal{I},\sum_{i\in\mathcal{I}}p_i=\sum_{j\in\mathcal{J}}q_{j_i}=1$, e_{j_i} states in $\mathfrak{X}_*$ and the following properties

$$
\begin{aligned}
&i)\quad \text{for all } i\in\mathcal{I},\ j\in\mathcal{J}:\ |j_i\rangle\perp|k_i\rangle \text{ for all } k\in\mathcal{J}\backslash\{j\}\\
&ii)\quad \text{for all } j,k\in\mathcal{J}:\ e_{j_i}\perp e_{k_l} \text{ for all } l\in\mathcal{I}\backslash\{i\}
\end{aligned}
$$

Notice that the e_{j_i} are defined on $\mathfrak{X}_*$, and $|j_i\rangle\langle j_i|$ are pure states in $\mathfrak{Y}_*$. Using the definition it is easy to see that ρ is of Recursive Deepness 2 and it is not difficult to prove that all other oc-type states of the same Recursive Deepness are isomorph to ρ with respect to degeneration, i.e the size of $\mathcal{I}$ and $\mathcal{J}$. (I.e. for another oc-type state τ there exists a completely positive map $c:\mathfrak{X}\otimes\mathfrak{Y}\to\mathfrak{X}\otimes\mathfrak{Y}$ which maps $\hat{\rho}$ to $\hat{\tau}$ and the inverse c.p. map, respectively.)

Theorem 6.2 (oc-type Secret Sharing Capacity) *For oc-type states of Recursive Deepness 2, the secret key capacity is given by* $C_{S,2-oc-type} = I(\mathfrak{X} \wedge \mathfrak{Y})$. *One forward and backward public communication is sufficient.*

Proof: From the foregoing it is sufficient to prove that $C_{S,2-oc-type} = I_\rho(\mathfrak{X} \wedge \mathfrak{Y})$. To shorten the notation, we define for all $i \in \mathcal{I}, j \in \mathcal{J}$

$$\begin{aligned} \rho^X &\triangleq \text{Tr }_{\mathfrak{Y}}\rho \text{ and } \rho^Y \triangleq \text{Tr }_{\mathfrak{X}}\rho \\ \rho_{j_i} &\triangleq e_{j_i} \otimes |j_i\rangle\langle j_i| \\ \rho_i &\triangleq \sum_{j\in J} q_{j_i}\rho_{j_i} \\ \rho_i^X &\triangleq \text{Tr }_{\mathfrak{Y}}\rho_i = \sum_{j\in\mathcal{J}} q_{j_i}e_{j_i} \text{ and } \rho_i^Y \triangleq \text{Tr }_{\mathfrak{X}}\rho_i \\ \rho_{i^n} &\triangleq \rho_{i_1} \otimes \cdots \otimes \rho_{i_n}. \end{aligned} \tag{6.1}$$

Since $\rho_k^X \perp \rho_l^X$ for $k, l \in \mathcal{I}, k \neq l$ there exists a projective measurement $\bar{A}$ where $\bar{A}_i$ is the projection onto ρ_i^X for all $i \in I$ such that $\rho_i = \frac{1}{\text{Tr }\rho A_i \otimes \mathbb{1}}\sqrt{A_i \otimes \mathbb{1}}\rho\sqrt{A_i \otimes \mathbb{1}}$, which can distinguish all states ρ_i^X. Without loss of generality, let us assume that this gives a POVM A on $\mathfrak{X}$ (otherwise define an error $A_0 \triangleq \mathbb{1} - \sum_{i\in\mathcal{I}} A_i$) which we extend to an POVM A^n on $\mathfrak{X}^{\otimes n}$.

Now terminal $\mathcal{X}$ starts with a pre-encoding quantum operation

$$\Phi_1 : \sigma \to \sum_{i^n\in\mathcal{I}^n} \sqrt{A_{i^n}^n}\sigma\sqrt{A_{i^n}^n} \otimes [i^n] \otimes [i^n].$$

where $\mathfrak{M}_1 \triangleq (\mathbb{C}\mathcal{I})^{\otimes n}$. Notice that we can now apply theorem 5.1 for the state $\bar{\rho} = \sum_{i\in I} p_i[i] \otimes \rho_i^Y$ on $(\mathbb{C}\mathcal{I})_* \otimes (\mathfrak{Y})_*$, achieving the secret key capacity $I(\mathfrak{I} \wedge \mathfrak{Y})$, with $\mathfrak{I} \triangleq \mathbb{C}\mathcal{I}$.

Since all information concerning the secret key K can be stored in the quantum system, we can wait w.l.o.g. for the end measurement ("step k") and use the stored quantum state for a backward-transmission of $\mathcal{Y}$ to $\mathcal{X}$. Observe that lemma 3.6 assures us that the state on $\mathfrak{X}^{\otimes n} \otimes \mathfrak{Y}^{\otimes n} \otimes \mathfrak{M}_1$ is not disturbed very much: Let D_* be the decoding observable defined in the proof of theorem 5.1. For all $i^n \in \mathcal{C}_j, 1 \leq k \leq N$ we have $1 - \text{Tr }\bar{\rho}_{i^n}^Y \otimes [k]D_{i^n}^k \leq \epsilon$. Hence we use a gentle measurement argument (i.e an extension of lemma 3.6, cf. [44]) to obtain

$$\|\bar{\rho}_{i^n}^Y \otimes [k] - D_*(\bar{\rho}_{i^n}^Y \otimes [k])\|_1 \leq \sqrt{8\epsilon} + \epsilon. \tag{6.2}$$

Now fix $i \in \mathcal{I}$. Terminal $\mathcal{Y}$ can use the state $\rho_i = \sum_{j\in\mathcal{J}} q_{j_i}e_{j_i} \otimes |j_i\rangle\langle j_i|$ to set up a backward q-DMC $W_i : j \to \rho_i^X$ since $\text{Tr }_{\mathfrak{X}}(e_{k_i} \otimes |k_i\rangle\langle k_i|) \perp \text{Tr }_{\mathfrak{X}}(e_{l_i} \otimes |l_i\rangle\langle l_i|)$ for all

$k, l \in \mathcal{J}, k \neq l$. Again using theorem 5.1 and (6.2) we can achieve a secret key capacity $I_{\rho_i}(\mathfrak{X} \wedge \mathfrak{Y}|\mathfrak{I} = [i])$. It is easy to see how to set up one completely positive map in order to use only one step/public transmission for all evaluations of $i \in \mathcal{I}$. Hence we achieve the secret key capacity

$$I(\mathfrak{X}\mathfrak{I} \wedge \mathfrak{Y}) = I(\mathfrak{I} \wedge \mathfrak{Y}) + I(\mathfrak{X} \wedge \mathfrak{Y}|\mathfrak{I})$$

using a forward and a backward transmission given ρ. Further with (6.1)

$$\begin{aligned}
H(\text{Tr }_{\mathfrak{X}}\rho_i) &= H(\rho_i^Y) = H(q_{j_i}) && (6.3)\\
H(\text{Tr }_{\mathfrak{Y}}\rho_{ji}) &= H(e_{j_i}) = H(e_{j_i} \otimes |j_i\rangle\langle j_i|), \text{ since } H(|j_i\rangle\langle j_i|) = 0 && (6.4)\\
H(\rho^X) &= H(p_i) + \sum_{i\in I} p_i H(\rho_i^X) = H(p_i) + \sum_{i\in I} p_i H(q_{j_i}) && (6.5)\\
&= H(p_i) + \sum_{i\in I} p_i H(q_{j_i}) && (6.6)
\end{aligned}$$

we get

$$\begin{aligned}
I(\mathfrak{X}\mathfrak{I} \wedge \mathfrak{Y}) &= H(\text{Tr }_{\mathfrak{X}}\rho) - \sum_{i\ inI} p_i H(\text{Tr }_{\mathfrak{X}}\rho_i) + \sum_{i\in I} p_i \left[H(\text{Tr }_{\mathfrak{Y}}\rho_i) - \sum_{j\in J} q_{j_i} H(\text{Tr }_{\mathfrak{Y}}\rho_{j_i}) \right]\\
&\overset{(6.3)}{=} H(\rho^Y) - \sum_{i\in I, j\in J} p_i q_{j_i} H(\text{Tr }_{\mathfrak{Y}}\rho_{j_i})\\
&\overset{(6.4)}{=} H(\rho^Y) - \sum_{i\in I, j\in J} p_i q_{j_i} H(e_{j_i} \otimes |j_i\rangle\langle j_i|)\\
&= H(\rho^Y) - [H(p_i q_{j_i}) + \sum_{i\in I, j\in J} p_i q_{j_i} H(e_{j_i}) \otimes |j_i\rangle\langle j_i|)] + H(p_i q_{j_i})\\
&\overset{(6.6)}{=} H(\rho^Y) - H(\rho) + H(\rho^X)\\
&= H(\mathfrak{Y}) - H(\mathfrak{X}\mathfrak{Y}) + H(\mathfrak{X}) = I(\mathfrak{X} \wedge \mathfrak{Y}).
\end{aligned}$$

Since we used theorem 5.1 twice, the definitions (4.2)-(4.5) can be checked in the same way as in the proof of the corresponding theorem giving some weaker bounds by (6.2), e.g. $\Pr(K \neq L) \leq 2\epsilon + \sqrt{8\epsilon} + 2\eta$ if (n, ϵ)-codes were used in both communication directions, and the probability of the codeword sets given by the Code Partition Lemma 5.2 were greater than or equal to η. For the converse theorem 5.3 is still true.

■

Corollary 6.3 *For oc-type states of Recursion Deepness $m \in \mathbb{N}$ we get the secret key capacity $C_{S,m-oc-type} = I(\mathfrak{X} \wedge \mathfrak{Y})$, achievable with 2m communication rounds ("steps" in the Secret Sharing Source Model)). For general oc-type states, we get the same capacity perhaps applying an infinite number of communication rounds.*

Proof The proof is clear already from the 2-oc-type states, using the same recursive structure.

■

7 General Bounds for Secret Key Capacity

In the semi-classical Secret Sharing Source Model we were able to achieve a Coding Theorem using only a single public-forward-transmission. For backward communication the upper bound can not be achieved in all cases, as we shall now show.

Let $\rho^Y = \mathrm{Tr}_{\mathfrak{X}}\rho = \sum_x p_x W_x$ be the average state seen by terminal $\mathcal{Y}$ given by the source output $\{p_x, W_x\}$, with non-commuting states W_x. W.l.o.g Terminal $\mathcal{Y}$ has to use a pre-encoding measurement A given by a POVM $(A_1, \cdots, A_l)$ on $\mathfrak{Y}$ in the first step (in order to distinguish the states) (Otherwise we can wait till the end-round, where a measurement has to be applied in order to get a classical key). Maximizing over the involved measurement, with fixed ensemble, yields the accessible information at fixed ensemble $I_{acc}(p \wedge W)$, which is a stronger version of the usual presented measurement independent Holevo bound. It was shown in [23] that the accessible information reaches the Holevo bound $H(\rho^Y) - \sum_i p_x H(W_x) = H_\rho(\mathfrak{Y}) - H(\mathfrak{Y}|\mathfrak{X})$ if and only if all the states that compose the ensemble commute, being strictly less otherwise. Furthermore, this difference remains even asymptotically when one considers measurements on many independent states emitted by the source, because (see [22])

$$I_{acc}(p^n \wedge W^{\otimes n}) = nI_{acc}(p \wedge W).$$

Hence the inequality (5.2) in the proof of the general upper bound in theorem 5.3 becomes a strict inequality, i.e. there exists a constant $K > 0$ only depending on the fixed ensemble $\{p_x, W_x\}$ such that

$$I_{\rho^{\otimes n}}(\mathfrak{X}^{\otimes n} \wedge \mathfrak{Y}^{\otimes n}) \geq I_{\rho_k}(K \wedge L|\mathfrak{M}_{[k]}, \mathfrak{N}_{[k]}) - nK. \tag{7.1}$$

Thus

$$\frac{1}{n}H(K) \leq I_\rho(\mathfrak{X} \wedge \mathfrak{Y}) - K + \epsilon$$

for sufficiently large n.

Theorem 7.1 *The secret key capacity $C_{S,semi-classical,\leftarrow}$ using only one backward transmission is strictly less than $I(\mathfrak{X} \wedge \mathfrak{Y})$ if the fixed ensemble states of ρ^Y do not commute.*

Now let the source state ρ be arbitrary separable. If terminal $\mathcal{X}$ uses a maximal pre-encoding measurement A given by a POVM $(A_1, \ldots, A_l)$ on $\mathfrak{X}$ in the first step (i.e.

$\Phi_1 : \rho \to \sum_{i=1}^{l} \sqrt{A_i}\rho\sqrt{A_i} \otimes [i] \otimes [0])$ we obtain a new semi-classical Secret Sharing Source Model with the following properties:

$$\lambda_i \triangleq \Pr(i) = \text{Tr } (\rho(A_i \otimes \mathbb{1}))$$

$$\rho_i \triangleq \frac{1}{\lambda_i}\sqrt{A_i \otimes \mathbb{1}}\rho\sqrt{A_i \otimes \mathbb{1}}$$

Now with $W_i \triangleq \text{Tr }_{\mathfrak{X}}\rho_i$ we get a new semi-classical state $\bar{\rho} \triangleq \sum_{i=1}^{l} \lambda_i[i] \otimes W_i$.

Theorem 7.2 *The secret key capacity $C_{S,arbitrary}$ for the Secret Sharing Source Model with arbitrary separable states ρ is lower bounded by*

$$H\left(\sum_{i=1}^{l} \lambda_i W_i\right) - \sum_{i=1}^{l} \lambda_i H(W_i) + \sum_{i=1}^{l} C_{S,arbitrary}(\rho_i),$$

where $C_{S,arbitrary}(\rho_i)$ denotes the secret key capacity for the not used states. As an upper bound we still have $I(\mathfrak{X} \wedge \mathfrak{Y})$ from lemma 5.3.

Since we can apply the theorem recursively on the states ρ_i we could even derive a better bound, but it is still unknown how a possible maximizing pre-encoding measurement A is given. Further questions are: is it better to extract as much secrecy in one step using one good pre-encoding A, or is it better to use several recursive pre-encodings A^1, $A^2, \ldots$ in an adaptive way? This may depend very much on the source state itself (cf. orthogonal channel state model). It is not known, however, how many rounds terminals $\mathcal{X}$ and $\mathcal{Y}$ have to take. We conjecture that there exist source states which need an infinite number of communication rounds.

8 Open Problems

1) Try to extend theorem 5.1 to the full separable case. We conjecture that the capacity for non-oc-type states is strictly less than $I(\mathfrak{X} \wedge \mathfrak{Y})$.

2) Analyse the full quantum Secret Sharing Model and state bounds.

3) We used only quantum operations to describe and analyse the Secret Sharing Source Model. Extend this also to other cryptographic problems like BB84 ([9], for an approach see chapter IV).

Chapter II

Quantum Broadcast Channels

1 Introduction

There are many problems regarding quantum broadcast channels, unknown to classical broadcast channels. One problem already appears when we think of the easiest known broadcast channel, the copy-machine. Since it is not possible by linearity to copy an unknown, non-orthogonal state [46], there exists no quantum operation ϕ such that $\phi(\rho) = \rho \otimes \rho$. Recently, great steps have been made in cloning a tensor product of an unknown state, i.e. finding a quantum operation ϕ such that $\phi(\rho^{\otimes n}) = \rho^{\otimes n} \otimes \rho^{\otimes n}$ with high fidelity, but we will restrict ourselves to orthogonal input states. With this, the input state of a broadcast channel can be copied and then also sent physically to two different receivers (mathematically described by two quantum operations acting on the classical input).

Already, in the classical case, the rate region for broadcast channels is only known for special cases, e.g. the degraded broadcast channel. This special channel network problem was raised in 1972 by Cover [14], and he conjectured a result where the direct part of the coding theorem was proven by Bergmans [10] one year later. The corresponding strong converse was established by Ahlswede, Gacs and Körner [5] in 1976.

In this chapter, we will first prove a main lemma concerning two q-DMC's, on which the proof of special rate points for the quantum asymmetric broadcast channel and the achievable rate region of the quantum degraded broadcast channel relies. Further, we will give an upper bound for the rate region of the quantum degraded broadcast channel, provided one of the receivers also has a classical channel. Finally, we finish with a code stuffing lemma (using ideas mainly established by Ahlswede [4] in the classical case) which will be needed in chapter III.

The proofs of this chapter are mainly motivated by the book of Ciszar and Körner [15] where these theorems were partly proved for the classical case.

2 Definitions

For the further chapters, let $\mathcal{X},\mathcal{U}$ be finite sets with probability distributions $P_{\mathcal{X}}, P_{\mathcal{U}}$ and conditional probability $P_{\mathcal{X}|\mathcal{U}}$, $\mathfrak{Y},\mathfrak{Z}$ $*-$ subalgebras. Define two q-DMC W,V by completely positive maps

$$W_* : \mathcal{X} \to \mathfrak{Y}_*$$
$$V_* : \mathcal{X} \to \mathfrak{Z}_*$$

which can be generalized uniquely by linearity to

$$W_* : (\mathbb{C}\mathcal{X})_* \to \mathfrak{Y}_*$$
$$V_* : (\mathbb{C}\mathcal{X})_* \to \mathfrak{Z}_*.$$

From now on, we will often suppress $*$ for convenience, if the situation is clear. Let n be a positive integer, and consider sequences $x^n = x_1 \cdots x_n \in \mathcal{X}^n$. Then the channel output of x^n is given by $W_{x^n} \triangleq W_{x_1} \otimes \cdots \otimes W_{x_n}$ where $W_x \triangleq W(x)$. Further, let $\mathfrak{X} \triangleq \mathbb{C}\mathcal{X}$, $\mathfrak{U} \triangleq \mathbb{C}\mathcal{U}$.

This gives us an a priori overall channel state

$$\rho^{\otimes n} = \sum_{x^n \in \mathcal{X}^n} P_{\mathcal{X}}(x^n)[x^n] \otimes W_{x^n} \otimes V_{x^n}$$

on $\mathfrak{X}^{\otimes n} \otimes \mathfrak{Y}^{\otimes n} \otimes \mathfrak{Z}^{\otimes n}$.

Definition 2.1 *A* **quantum broadcast channel (q-BC)** *is a quadruple* $(P_{\mathcal{X}}, \mathcal{X}, W, V)$ *given by two q-DMC's*

$$W : \mathcal{X} \to \mathfrak{Y}$$
$$V : \mathcal{X} \to \mathfrak{Z}$$

where $\mathfrak{X},\mathfrak{Y},\mathfrak{Z}$ *are compatible *-subalgebras,* $\mathfrak{X} = \mathbb{C}\mathcal{X}$ *a commutative *-subalgebra,* $\mathcal{X}$ *a finite set with a priori probability distribution* $P_{\mathcal{X}}$ *, and an a priori state on* $\mathfrak{X} \otimes \mathfrak{Y} \otimes \mathfrak{Z}$ *:*

$$\rho = \sum_x P_{\mathcal{X}}(x)[x] \otimes W_x \otimes V_x. \tag{2.1}$$

Let $\mathcal{M}_1, \mathcal{M}_0, \mathcal{M}_2$ be the message sets of the encoder, where $\mathcal{M}_1$ should be sent from input 1 to $\mathcal{Y}$, $\mathcal{M}_2$ by input 2 to $\mathcal{Z}$, respectively, and $\mathcal{M}_0$ should be decodeable by both.

Definition 2.2 (Broadcast Condition) *Let* $(P_{\mathcal{X}}, \mathcal{X}, W, V)$ *be a quantum broadcast-channel. Let* $\mathfrak{U} = \mathbb{C}\mathcal{U}$ *be a commutative helper *-subalgebra with a probability distribution* $P_{\mathcal{U}}$ *and a fixed a priori conditional distribution* $P_{\mathcal{X}|\mathcal{U}}$ *(simulating a classical channel* $U : \mathcal{U} \to \mathcal{X}$*), defining a mapping*

$$\hat{W} : \mathcal{U} \to \mathfrak{Y}, \qquad \hat{V} : \mathcal{U} \to \mathfrak{Z}$$

defined by $\hat{W}_u \triangleq \sum_{x\in\mathcal{X}} P_{\mathcal{X}|\mathcal{U}}(x|u)W_x$ *and* $\hat{V}_u$ *in the analogous way. Thus*

$$\begin{aligned}\hat{W}_{u^n} &= \sum_{x^n\in\mathcal{X}^n} P_{\mathcal{X}|\mathcal{U}}(x_1|u_1)W_{x_1}\otimes\cdots\otimes P_{\mathcal{X}|\mathcal{U}}(x_n|u_n)W_{x_n}\\ &= \sum_{x^n\in\mathcal{X}^n} P^n_{\mathcal{X}|\mathcal{U}}(x^n|u^n)W_{x^n}.\end{aligned}$$

If further on $\mathfrak{U}\otimes\mathfrak{X}\otimes\mathfrak{Y}\otimes\mathfrak{Z}$ *an a priori channel state* ρ *with* $I(\mathfrak{U}\wedge\mathfrak{Y}\mathfrak{Z}|\mathfrak{X}) = 0$ *and*

$$\begin{aligned}\mathrm{Tr}_{\mathfrak{U}\mathfrak{Z}}\rho &= \sum_{x\in\mathcal{X}} P_{\mathcal{X}}(x)[x]\otimes W_x\\ \mathrm{Tr}_{\mathfrak{U}\mathfrak{Y}}\rho &= \sum_{x\in\mathcal{X}} P_{\mathcal{X}}(x)[x]\otimes V_x\\ \mathrm{Tr}_{\mathfrak{X}\mathfrak{Z}}\rho &= \sum_{u\in\mathcal{U}} P_{\mathcal{U}}(u)[u]\otimes W_u\\ \mathrm{Tr}_{\mathfrak{X}\mathfrak{Y}}\rho &= \sum_{u\in\mathcal{U}} P_{\mathcal{U}}(u)[u]\otimes V_u\end{aligned}$$

exists, then the **broadcast condition** *is fulfilled. If further* $I(\mathfrak{X}\wedge\mathfrak{Z}|\mathfrak{Y}) = 0$ *the* **strong broadcast condition** *is valid.*

Note that this definition is equivalent to the desired Markov-conditions in the classical case.

Lemma 2.3 (Main Lemma) *For every* $\epsilon, \delta_u, \eta \in (0,1)$ *, every quantum broadcast channel* $(P_{\mathcal{X}}, \mathcal{X}, W, V)$ *satisfying the broadcast condition with* $(\mathcal{U}, P_{\mathcal{X}|\mathcal{U}}, P_{\mathcal{U}})$ *, for every typical sequence* $u^n \in \mathcal{T}^n_{P_{\mathcal{U}},\delta_u}$ *and set* $\mathcal{A} \in \mathcal{X}^n$ *satisfying*

$$P^n_{\mathcal{X}|\mathcal{U}}(\mathcal{A}|u^n) \geq \eta$$

there exists a constant $K'(|\mathcal{X}|, |\mathcal{U}|, \dim\mathfrak{Y}, \dim\mathfrak{Z}, \delta_u, \epsilon)$ *, and* $(n,\epsilon)-$ *codes* (f, D^Y) *and* (f, D^Z) *for the q-DMC* $W : \mathcal{X} \to \mathfrak{Y}$ *(resp.* $V : \mathcal{X} \to \mathfrak{Z}$*) having the same encoder* $f : \mathcal{M} \to \mathcal{A}$ *such that*

$$\frac{1}{n}\log|\mathcal{M}| \geq \min[I(\mathfrak{X}\wedge\mathfrak{Y}|\mathfrak{U}), I(\mathfrak{X}\wedge\mathfrak{Z}|\mathfrak{U})] - K'/\sqrt{n}$$

and

$$\forall m\in\mathcal{M} \qquad f(m)\in\mathcal{A},\ \textit{and}\ [\mathrm{Tr}\ D^Y_m \leq \mathrm{Tr}\ \Pi^n_{V,W,\delta_w}(f(m))\ \textit{or}\ \mathrm{Tr}\ D^Z_m \leq \mathrm{Tr}\ \Pi^n_{V,V,\delta_v}(f(m))]$$

Proof: Let $\mathcal{A}' = \mathcal{A} \cap \mathcal{T}^n_{P_{\mathcal{X}|\mathcal{U}}, \sqrt{2|\mathcal{X}||\mathcal{U}|/\eta}}(u^n)$ (thus $P^n_{\mathcal{X}|\mathcal{U}}(\mathcal{A}'|u^n) \geq \frac{\eta}{2}$ for $u^n \in \mathcal{T}^{\otimes n}_{P_{\mathcal{U}},\delta_u}$ and $\mathcal{A}' \subset \mathcal{T}^{\otimes n}_{P_{\mathcal{X}},\delta_x}$ with $\delta_x \triangleq \delta_x(\delta_u, |\mathcal{X}|, |\mathcal{U}|, \eta) > 0$.) and (n,ϵ)-codes (f, D^Y), (f, D^Z) for the two q-DMC with codewords $f(m) \in \mathcal{A}$ for all $m \in \mathcal{M}$ such that

$$\text{Tr } D_m \leq \Pi^n_{V,W,\delta_w}(f(m)) \text{ or Tr } D^Z_m \leq \text{Tr } \Pi^n_{V,V,\delta_v}(f(m))$$

with $\delta_w \triangleq \sqrt{2|\mathcal{X}| \dim \mathfrak{Y}/\epsilon}$, $\delta_v \triangleq \sqrt{2|\mathcal{X}| \dim \mathfrak{Z}/\epsilon}$. Define

$$B \triangleq \sum_{m\in\mathcal{M}} D_m, \qquad C \triangleq \sum_{m\in\mathcal{M}} E_m.$$

Let $\gamma = \min\{1-\epsilon, \epsilon^2/32\}$. We claim that

$$\text{for all } x^n \in \mathcal{A} : \text{Tr } W_{x^n} B \geq \gamma \text{ or Tr } V_{x^n} C \geq \gamma. \tag{2.2}$$

This is clear, if x^n is a codeword, and true else. Otherwise we could extend our code with the word x^n and decoding observable

$$D^Y_{x^n} = \sqrt{\mathbb{1}_{\mathfrak{Y}} - B}\Pi^n_{V,W,\delta_1}(x^n)\sqrt{\mathbb{1}_{\mathfrak{Y}} - B} \text{ or } D^Z_{x^n} = \sqrt{\mathbb{1}_{\mathfrak{Z}} - C}\Pi^n_{V,V,\delta_2}(x^n)\sqrt{\mathbb{1}_{\mathfrak{Z}} - C}.$$

Assume the first inequality (the latter goes in the same way).
Note that $B + D^Y_{x^n} \leq \mathbb{1}$. Apply Lemma 3.6 to the assumption Tr $W_{x^n}(\mathbb{1} - B) \geq 1 - \frac{\epsilon^2}{32}$:

$$||W_{x^n} - \sqrt{1_{\mathfrak{Y}} - B} W_{x^n} \sqrt{\mathbb{1}_{\mathfrak{Y}} - B}||_1 \leq \sqrt{8\gamma} \leq \frac{\epsilon}{2}.$$

Thus

$$\begin{aligned} \text{Tr } (W_{x^n} D^Y_{x^n}) &= \text{Tr } (W_{x^n}\sqrt{\mathbb{1}_{\mathfrak{Y}} - B}\Pi^n_{V,W,\delta_w}\sqrt{\mathbb{1}_{\mathfrak{Y}} - B}) \\ &= \text{Tr } (W_{x^n}\Pi^n_{V,W_{x^n},\delta_W}) - ||(W_{x^n} - \sqrt{1_{\mathfrak{Y}} - B} W_{x^n}\sqrt{1_{\mathfrak{Y}} - B})\Pi^n_{V,W,\delta_w}(x_n)||_1 \\ &\geq (1 - \frac{\epsilon}{2}) - \frac{\epsilon}{2} = 1 - \epsilon \end{aligned}$$

Let $\mathcal{A}_1$ resp. $\mathcal{A}_2$ be the set of those $x^n \in \mathcal{A}'$ for which the first resp. second inequality or (2.2) applies. We have

$$P^n_{\mathcal{X}|\mathcal{U}}(\mathcal{A}_1|u^n) \geq \frac{1}{2}\eta \text{ or } P^n_{\mathcal{X}|\mathcal{U}}(\mathcal{A}_2|u^n) \geq \frac{1}{2}\eta.$$

In the first case Tr $W_{u^n} B \geq \frac{1}{2}\eta\gamma$ for $u^n \in \mathcal{T}_{V,P_{\mathcal{U}},\delta_u}$. Hence

$$\text{Tr } (P_{\mathcal{U}} W_u)^{\otimes n} B \geq \frac{1}{2}\eta\gamma(1 - \frac{|U|}{\delta_u^2}) \triangleq \tau. \tag{2.3}$$

Thus $(P_{\mathcal{U}}W_u)^{\otimes n}$ is in the τ-shadow of B, and by lemma 3.8 we get

$$\begin{aligned}\text{Tr } B &\geq (\tau - \frac{\dim \mathfrak{Y}}{\delta_0^2}) \exp\{nH(P_{\mathcal{U}}W_u) - Kd\delta_w\sqrt{n}\} \\ &\geq (\tau - \frac{\dim \mathfrak{Y}}{\delta_0^2}) \exp\{nH(W_u|P_{\mathcal{U}}) - Kd\delta_w\sqrt{n}\}.\end{aligned}$$

Choosing $\delta_0 \triangleq \sqrt{2\dim \mathfrak{Y}}/\tau$ and observing by lemma 3.9 that

$$\text{Tr } B \leq \sum_{m\in\mathcal{M}} D_m^Y \leq |\mathcal{M}| \exp\{nH(W_x|P_{\mathcal{X}}) + (K \dim \mathfrak{Y}\sqrt{|\mathcal{X}|}\delta_w + K|\mathcal{X}|\delta_x \log \dim \mathfrak{Y})\sqrt{n})$$

the proof is complete.

■

Remark 2.4 *Observe from the proof of lemma 2.3 that the decoder for channel code W (resp. V) may be chosen as a von Neumann observable (i.e. all its operators are mutually orthogonal projectors). This is because if the code (f, D^Y) is of this type, then $B \triangleq \sum_{m\in\mathcal{M}} D_m$ is a projector, and this means that we may use the projector $D'_{x^n} \triangleq \text{supp}D_{x^n}$ instead of the constructed $D_{x^n} \leq \mathbb{1} - B$: this is still bounded by $\mathbb{1} - B$, only decreases the error probability, and obeys the size condition:*

$$\text{Tr supp}D_{x^n} = \dim \text{im}D_{x^n} \leq \dim \text{im}\Pi^n_{V,W,\delta}(x^n) = \text{Tr } \Pi^n_{V,W,\delta}(x^n).$$

The same applies analogously to the second channel V and its decoding observable D^Z.

Corollary 2.5 *For $\epsilon, \eta \in (0,1)$ and for every set $\mathcal{A} \in \mathcal{X}^n$ satisfying $P^n_{\mathcal{X}}(\mathcal{A}) \geq \eta$ there exist $K > 0$ and (n,ϵ)-codes for the q-DMC's $W : \mathcal{X} \to \mathfrak{Y}$ and $V : \mathcal{X} \to \mathfrak{Z}$ having the same encoder $f : \mathcal{M} \to \mathcal{A}$ and rate*

$$\frac{1}{n}\log|\mathcal{M}| \geq \min[I(\mathfrak{X} \wedge \mathfrak{Y}), I(\mathfrak{X} \wedge \mathfrak{Z})] - K/\sqrt{n}$$

for $n \geq n_0(|\mathcal{X}|, \dim \mathfrak{Y}, \dim \mathfrak{Z}, \epsilon, \eta, K)$.

3 Quantum Asymmetric Broadcast Channel

A quantum asymmetric broadcast channel (q-ABC) is a quantum broadcast channel where either of the inputs 1 and 2 is idle, i.e. messages from the message set $\mathcal{M}_1$ and $\mathcal{M}_0$ are to be encoded, and then decoded, by two receivers, where the first decoder is able to

decode the messages of the message set $\mathcal{M}_1$ and $\mathcal{M}_0$, whereas the other decoder may only decode the message set $\mathcal{M}_0$:

$$\begin{array}{ccc} [1] & & [0] \\ & \searrow & \downarrow \\ & & [X] \\ & \swarrow & \downarrow \\ [10] & & [0] \end{array}$$

Definition 3.1 *A n-block code for the q-ABC is a triple* (f, D^Y, D^Z) *with the encoder* $f : \mathcal{M}_0 \times \mathcal{M}_1 \to \mathcal{X}^n$ *and a POVM* D^Y *on* $\mathfrak{Y}^{\otimes n}$ *indexed by* $\mathcal{M}_0' \times \mathcal{M}_1' \subset \mathcal{M}_0 \times \mathcal{M}_1$ *(resp. a POVM* D^Z *on* $\mathfrak{Z}^{\otimes n}$ *indexed by* $\mathcal{M}_0'' \subset \mathcal{M}_0$*) .*

Definition 3.2 *The probability of (maximal) error is defined by*

$$e_{10} = \max_{(m_0,m_1)\in\mathcal{M}_0\times\mathcal{M}_1}\{1 - \mathrm{Tr}\ W_{f(m_0,m_1)}D^Y_{m_0,m_1}\}$$

$$e_0 = \max_{(m_0,m_1)\in\mathcal{M}_0\times\mathcal{M}_1}\{1 - \mathrm{Tr}\ V_{f(m_0,m_1)}D^Z_{m_0}\}$$

(f, D^Y, D^Z) *is denoted a* (n, ϵ)*-code, if* $e_{10}(f, D^Y),\ e_0(f, DZ) \leq \epsilon$.

Remark 3.3 *Let* $x^n = (x_1, \ldots, x_n) \in \mathcal{X}^n$. *Then the encoding will be done by* $W_{x^n} = W_{x_1} \otimes \cdots \otimes W_{x_n}$ *defining a product state. There may be better rates possible by encoding in superpositions and using entanglement, but this is a still unexplored area of quantum information theory already for the common quantum-DMC in the general case.*

Definition 3.4 *A rate tuple* (R_{10}, R_0) *is defined by* $R_{10} = \frac{1}{n}\log|\mathcal{M}_0||\mathcal{M}_1|$, $R_1 = \frac{1}{n}\log|\mathcal{M}_0|$.

Theorem 3.5 (Quantum Asymmetric Broadcast Channel) *For the quantum asymmetric broadcast channel which fulfills the broadcast condition, the rate point*

$$R_{10} = I(\mathfrak{X} \wedge \mathfrak{Y}|\mathfrak{U}),\ R_0 = I(\mathfrak{U} \wedge \mathfrak{Z}) \tag{3.1}$$

and

$$R_{10} + R_0 \leq I(\mathfrak{X} \wedge \mathfrak{Y}) \tag{3.2}$$

is achievable regarding an average channel state ρ.

Proof: Note that from (3.1) and (3.2), we obtain

$$I(\mathfrak{U} \wedge \mathfrak{Z}) \leq I(\mathfrak{U} \wedge \mathfrak{Y}), \tag{3.3}$$

otherwise

$$\begin{aligned} R_{10}+R_0 &= I(\mathfrak{X}\wedge\mathfrak{Y}|\mathfrak{U})+I(\mathfrak{U}\wedge\mathfrak{Z}) \\ &> I(\mathfrak{X}\wedge\mathfrak{Y}|\mathfrak{U})+I(\mathfrak{U}\wedge\mathfrak{Y}) \\ &= I(\mathfrak{X}\mathfrak{U}\wedge\mathfrak{Y}) \\ &\geq I(\mathfrak{X}\wedge\mathfrak{Y}), \end{aligned}$$

which is in conflict with (3.2). Fix some $K>0, \epsilon\in(0,1/2\sqrt{2})$. Let $\hat{W}:\mathcal{U}\to\mathfrak{Y}$ and $\hat{V}:\mathcal{U}\to\mathfrak{Z}$ be two q-DMC. By (3.3) and corollary 2.5 to every $n\geq n_1(|\mathcal{U}|,\dim\mathfrak{Y},\dim\mathfrak{Z}),\epsilon,\mathfrak{K}$ there exist (n,ϵ)-codes $(\hat{f},\hat{D}^Y)$ resp. $(\hat{f},\hat{D}^Z)$ for the q-DMC $\hat{W}$ and $\hat{V}$ with a common encoder of rate

$$\frac{1}{n}\log|\mathcal{M}_{\hat{f}}|\geq I(\mathfrak{U}\wedge\mathfrak{Z})-K/\sqrt{n}.$$

For every $m\in\mathcal{M}_{\hat{f}}$ we have, by definition, the inequalities

$$\text{Tr }\hat{W}_{\hat{f}(m)}\hat{D}^Y_m=\sum_{x^n\mathcal{X}^n}P^n_{\mathcal{X}|\mathcal{U}}(x^n|\hat{f}(m))\text{Tr }W_{x^n}\hat{D}^Y_m\geq 1-\epsilon \tag{3.4}$$

$$\text{Tr }\hat{V}_{\hat{f}(m)}\hat{D}^Z_m=\sum_{x^n\mathcal{X}^n}P^n_{\mathcal{X}|\mathcal{U}}(x^n|\hat{f}(m))\text{Tr }V_{x^n}\hat{D}^Z_m\geq 1-\epsilon \tag{3.5}$$

Let $\mathcal{A}(m)$ be the largest subset of $\mathcal{X}^n$ such that

$$\text{Tr }W_{x^n}\hat{D}^Y_m\geq 1-2\epsilon \text{ and Tr } V_{x^n}\hat{D}^Z_m\geq 1-2\epsilon \quad \text{for every } x^n\in\mathcal{A}(m). \tag{3.6}$$

W.l.o.g the sets $\mathcal{A}(m)$ are disjoint (otherwise use remark 2.4 changing the decoding observables to achieve this, noting that $\epsilon<1/2\sqrt{2}$). With $\mathcal{A}(m)^C$ being the complement of $\mathcal{A}(m)$, we get for every $m\in M_{\hat{f}}$:

$$\begin{aligned} P^n_{\mathcal{X}|\mathcal{U}}(\mathcal{A}(m)|\hat{f}(m)) &\geq \sum_{x^n\in\mathcal{A}(m)}P^n_{\mathcal{X}|\mathcal{U}}(x^n|\hat{f}(m))\text{Tr }W_{x^n}\hat{D}^Y_m \\ &= \text{Tr }\hat{W}_{\hat{f}(m)}\hat{D}_m-\sum_{x^n\in\mathcal{A}(m)^C}P^n_{\mathcal{X}|\mathcal{U}}(x^n|\hat{f}(m))\text{Tr }W_{x^n}\hat{D}^Y_m \\ &\overset{Eq.\ (3.4)}{\geq} 1-\epsilon-\sum_{x^n\in\mathcal{A}^C(m)}P^n_{\mathcal{X}|\mathcal{U}}(x^n|\hat{f}(m))\text{Tr }W_{x^n}\hat{D}^Y_m \\ &\geq 1-\epsilon-(1-2\epsilon)(1-P^n_{\mathcal{X}|\mathcal{U}}(\mathcal{A}(m)|\hat{f}(m))), \end{aligned}$$

so by easy calculus:

$$P^n_{\mathcal{X}|\mathcal{U}}(\mathcal{A}(m)|\hat{f}(m))\geq\frac{1}{2}.$$

Using Lemma 2.3, to every $m \in \mathcal{M}_{\hat{f}}$ we can construct an (n, ϵ)-code $(f_m, D^{Y,m})$ for the q-DMC W with the codewords in $\mathcal{A}(m)$, each code having the same message set $\mathcal{M}_1$, where

$$\frac{1}{n} \log |\mathcal{M}_1| \geq I(\mathfrak{X} \wedge \mathfrak{Y}|\mathfrak{U}) - K/\sqrt{n}$$

Define now the encoding mapping $f : \mathcal{M}_1 \times \mathcal{M}_0 \to \mathcal{X}^n$ as $f(m_1, m_0) \triangleq f_{m_0}(m_1)$ for every $m_1 \in \mathcal{M}_1$, $m_0 \in \mathcal{M}_0 \triangleq \mathcal{M}_{\hat{f}}$. The decoding observable for $\mathfrak{Z}$ is defined as follows:

$$D^Z := \hat{D}^Z$$

For the decoding observable on $\mathfrak{Y}$, we have to solve to following problem: How can $\mathcal{Y}$ decode the message (m_1, m_0)?

To be brief, we define $W_{m_1}^{m_0} \triangleq W_{f(m_1,m_0)} = W_{f_{m_0}(m_1)}$ and suppress Y in $D^{Y,m}$ and $\hat{D}^Y$, i.e. $\hat{D}_b \triangleq \hat{D}_b^Y$. Now observe that we can define two quantum decoding operations

$$\begin{aligned} \Delta^{m_0} : \mathfrak{Y}^{\otimes n} &\to \mathfrak{M}_0 \otimes \mathfrak{Y}^{\otimes n} \\ \rho &\to \sum_{b \in \mathcal{M}_0} [b] \otimes \sqrt{\hat{D}_b} \rho \sqrt{\hat{D}_b} \end{aligned}$$

where

$$\forall m_0 \in \mathcal{M}_0 : \qquad \text{Tr } W_{m_1}^{m_0} \hat{D}_{m_0} \geq 1 - 2\epsilon \qquad \forall m_1 \in \mathcal{M}_1 \tag{3.7}$$

by (3.6). Since for fixed $m_0 \in \mathcal{M}_0$ we have further

$$\text{Tr } W_{m_1}^{m_0} D_{m_1}^{m_0} \geq 1 - \epsilon \tag{3.8}$$

by lemma 2.3. We define for given $m_0 \in \mathcal{M}_0$ and for all $m_1 \in \mathcal{M}_1$

$$\begin{aligned} \Delta^{m_1} : \mathfrak{M}_0 \otimes \mathfrak{Y}^{\otimes n} &\to \mathfrak{M}_1 \otimes \mathfrak{M}_0 \otimes \mathfrak{Y}^{\otimes n} \\ \rho &\to \sum_{c \in \mathcal{M}_1} [c] \otimes \sqrt{D_c} \rho \sqrt{D_c} \end{aligned}$$

where D_{m_1} is a POVM element defined by $D_{m_1} = \sum_{d \in \mathcal{M}_0} [d] \otimes D_{m_1}^d$. That this D is a POVM can easily be checked, since $\sum_{m_1 \in \mathcal{M}_1} D_{m_1} \leq \mathbb{1}$. Further observe that

$$\sqrt{D_{m_1}} = \sqrt{\sum_{m_0 \in \mathcal{M}_0} [m_0] \otimes D_{m_1}^{m_0}} = \sum_{m_0 \in \mathcal{M}_0} [m_0] \otimes \sqrt{D_{m_1}^{m_0}},$$

since we get a block structure in the full matrix algebra.

Now fix $m_0 \in \mathcal{M}_0, m_1 \in \mathcal{M}_1$ and assume that $f(m_1, m_0)$ was sent, i.e. $W_{m_1}^{m_0}$ was received. Then we get with $\bar{\mathcal{M}}_i := \mathcal{M}_i \backslash \{m_i\},\ i = 0, 1$ and $W_m \triangleq m_1 \otimes m_0 \otimes W_{m_1}^{m_0}$

$$
\begin{aligned}
& \left\| [m_1] \otimes [m_0] \otimes W_{m_1}^{m_0} - \Delta^{m_1}\Delta^{m_0}(W_{m_1}^{m_0}) \right\| && (3.9)\\
= & \left\| W_m - \Delta^{m_1}\left(\sum_{b\in\mathcal{M}_0} [b] \otimes \sqrt{\hat{D}_b} W_{m_1}^{m_0} \sqrt{\hat{D}_b} \right) \right\| \\
= & \left\| W_m - \sum_{c\in\mathcal{M}_1} [c] \otimes \sqrt{D_c} \left(\sum_{[b]\in\mathcal{M}_0} [b] \otimes \sqrt{\hat{D}_b} W_{m_1}^{m_0} \sqrt{\hat{D}_b} \right) \sqrt{D_c} \right\| \\
= & \left\| W_m - \sum_{c\in\mathcal{M}_1} [c] \otimes \left(\sum_{e\in\mathcal{M}_0} [e] \otimes \sqrt{D_c^e} \right) \left(\sum_{b\in\mathcal{M}_0} [b] \otimes \sqrt{\hat{D}_b} W_{m_1}^{m_0} \sqrt{\hat{D}_b} \right) \left(\sum_{f\in\mathcal{M}_0} [f] \otimes \sqrt{D_c^f} \right) \right\| \\
= & \left\| [m_1] \otimes [m_0] \otimes W_{m_1}^{m_0} - \sum_{c\in\mathcal{M}_1,\ b\in\mathcal{M}_0} [c] \otimes [b] \otimes \sqrt{D_c^b} \sqrt{\hat{D}_b} W_{m_1}^{m_0} \sqrt{\hat{D}_b} \sqrt{D_c^b} \right\| && (3.10)\\
\leq & \left\| [m_1] \otimes [m_0] \otimes W_{m_1}^{m_0} - [m_1] \otimes [m_0] \otimes \sqrt{D_{m_1}^{m_0}} \sqrt{\hat{D}_{m_0}} W_{m_1}^{m_0} \sqrt{\hat{D}_{m_0}} \sqrt{D_{m_1}^{m_0}} \right\| && (3.11)\\
& + \sum_{c\in\bar{\mathcal{M}}_1, b\in\bar{\mathcal{M}}_0} \left\| [c] \otimes [b] \otimes \sqrt{D_c^b} \sqrt{\hat{D}_b} W_{m_1}^{m_0} \sqrt{\hat{D}_b} \sqrt{D_c^b} \right\| && (3.12)\\
& + \sum_{b\in\bar{\mathcal{M}}_0} \left\| [m_1] \otimes [b] \otimes \sqrt{D_{m_1}^b} \sqrt{\hat{D}_b} W_{m_1}^{m_0} \sqrt{\hat{D}_b} \sqrt{D_{m_1}^b} \right\| && (3.13)\\
& + \sum_{c\in\bar{\mathcal{M}}_1} \left\| [c] \otimes [m_0] \otimes \sqrt{D_c^{m_0}} \sqrt{\hat{D}_{m_0}} W_{m_1}^{m_0} \sqrt{\hat{D}_{m_0}} \sqrt{D_c^{m_0}} \right\|, && (3.14)\\
& && (3.15)
\end{aligned}
$$

where the last triangle inequality gives 4 terms:

Term 1: [Equation (3.11)] By lemma I.3.7 we can immediately bound (3.11) by $(\sqrt{8}+4)\sqrt{\epsilon} \leq \sqrt{47\epsilon}$.

Term 2: [Equation (3.12)] Since $(\mathbb{1} - D_{m_1}^b) \leq \mathbb{1}$ for all $b \in \mathcal{M}_0$, we get

$$
\begin{aligned}
\sum_{c\in\bar{\mathcal{M}}_1, b\in\bar{\mathcal{M}}_0} \left\| \sqrt{D_c^b} \sqrt{\hat{D}_b} W_{m_1}^{m_0} \sqrt{\hat{D}_b} \sqrt{D_c^b} \right\| &= \sum_{b\in\bar{\mathcal{M}}_0} \mathrm{Tr}\ \sqrt{\hat{D}_b} W_{m_1}^{m_0} \sqrt{\hat{D}_b} \sum_{c\in\bar{\mathcal{M}}_1} D_c^b \\
&= \sum_{b\in\bar{\mathcal{M}}_0} \mathrm{Tr}\ \sqrt{\hat{D}_b} W_{m_1}^{m_0} \sqrt{\hat{D}_b} (\mathbb{1} - D_{m_1}^b) \\
&\leq \sum_{b\in\bar{\mathcal{M}}_0} \mathrm{Tr}\ W_{m_1}^{m_0} \hat{D}_b \leq 1 - \mathrm{Tr}\ W_{m_1}^{m_0} \hat{D}_{m_0} \\
&\leq 2\epsilon
\end{aligned}
$$

Term 3: [Equation (3.13)] Since $D_b, \sqrt{D^b_{m_1}} \leq \mathbb{1}$ using the Hölderlin inequality we have

$$\begin{aligned}\sum_{b\in\bar{\mathcal{M}}_0} \|\sqrt{D^b_{m_1}}\sqrt{\hat{D}_b}W^{m_0}_{m_1}\sqrt{\hat{D}_b}\sqrt{D^b_{m_1}}\| &\leq \sum_{b\in\bar{\mathcal{M}}_0} \|\sqrt{D^b_{m_1}}\|_\infty \|\sqrt{\hat{D}_b}W^{m_0}_{m_1}\sqrt{\hat{D}_b}\|_1 \|\sqrt{D^b_{m_1}}\|_\infty \\ &\leq \sum_{b\in\bar{\mathcal{M}}_0} \text{Tr } W^{m_0}_{m_1}\hat{D}_b \leq 1 - \text{Tr } W^{m_0}_{m_1}\hat{D}_{m_0} \\ &\leq 2\epsilon.\end{aligned}$$

Term 4: [Equation (3.14)] Using a similar technique as in the latter case, we get

$$\begin{aligned}\sum_{c\in\bar{\mathcal{M}}_1} \|\sqrt{D^{m_0}_c}\sqrt{\hat{D}_{m_0}}W^{m_0}_{m_1}\sqrt{\hat{D}_{m_0}}\sqrt{D^{m_0}_c}\|_1, &\leq \sum_{c\in\bar{\mathcal{M}}_1} \|\sqrt{\hat{D}_{m_0}}\|_\infty \|W^{m_0}_{m_1}\sqrt{\hat{D}_{m_0}}D^{m_0}_c\|_1, \\ &\leq \sum_{c\in\bar{\mathcal{M}}_1} \|\sqrt{\hat{D}_{m_0}}\|_\infty \|D^{m_0}_c W^{m_0}_{m_1}\|_1, \\ &\leq 1 - \text{Tr } W^{m_0}_{m_1}D^{m_0}_{m_1} \leq \epsilon.\end{aligned}$$

So we can finally bound (3.9) by $\epsilon' \triangleq 5\epsilon + \sqrt{47\epsilon}$. Using the partial trace operation $\text{Tr}_{\mathfrak{y}}$, we get

$$\|[m_1]\otimes[m_0] - \text{Tr}_{\mathfrak{y}}\Delta^{m_1}\Delta^{m_0}(W^{m_0}_{m_1})\|_1 \leq \epsilon', \tag{3.16}$$

so we have shown that there exists a decoding POVM indexed by $\mathcal{M}_1 \times \mathcal{M}_0$ with a maximal error ϵ' :

$$D^Y_{(m_1,m_0)*} \triangleq \text{Tr}_{\mathfrak{y}_*} \circ \Delta^{m_1}_* \circ \Delta^{m_0}_*$$

■

Remark 3.6 *Using Lemma 4.2 of [15] it is possible to show that the rate points given above are also valid if we assume an average error for the two channels. This is not true in every multi user case (cf. the multiple access channel).*

4 Degraded Broadcast Channel

Definition 4.1 *A quantum broadcast channel* $(P_{\mathcal{X}}, \mathcal{X}, W, V)$ *is called* **degraded** *if there exists a quantum operation*

$$\phi : \mathfrak{Y} \to \mathfrak{Z}$$

such that for all $x \in \mathcal{X}$

$$\phi(W_x) = V_x.$$

Observe that for $x^n \in \mathcal{X}^n$ we get $\phi^{\otimes n}(W_{x^n}) = V_{x^n}$.

An n-block code for the quantum degraded broadcast channel is a collection (f, D^Y, D^Z) of maps $f : \mathcal{M}_1 \otimes \mathcal{M}_2 \to \mathfrak{X}^{\otimes n}$ and decoding observables

$$D^Y \subset \mathfrak{Y}^{\otimes n} \qquad D^Z \subset \mathfrak{Z}^{\otimes n}$$

index by $\mathcal{M}_1$ (resp. $\mathcal{M}_2$), i.e.

$$D^Y = \{D^Y_m \in \mathfrak{Y} : m \in \mathcal{M}_1\}$$

$$D^Z = \{D^Z_m \in \mathfrak{Z} : m \in \mathcal{M}_2\}$$

such that $D^Y_m, D^Z_m \geq 0$, $\sum_m D^Y_m \leq \mathbb{1}$, $\sum_m D^Z_m \leq \mathbb{1}$

There are two average error probabilities of the code, the probability that the receiver $\mathcal{Y}$ (resp. $\mathcal{Z}$) guesses incorrectly any one of the sent words, taken over the uniform distribution on the message set:

$$\bar{e}_1(f, D^Y) = 1 - \frac{1}{|\mathcal{M}_1||\mathcal{M}_2|} \sum_{(m_1,m_2)\in\mathcal{M}_1\times\mathcal{M}_2} \mathrm{Tr}\,(W^n_{f(m_1,m_2)} D^Y_{m_1}),$$

and $\bar{e}_2(f, D^Z)$ analogously.

Definition 4.2 *(f, D^Y, D^Z) is an $(n, \bar{\epsilon})$ -code if the error probabilities $\bar{e}_1(f, D^Y)$, $\bar{e}_2(f, D^Z)$ do not exceed $\bar{\epsilon}$. The rates of the code are the $R_i \triangleq \frac{1}{n}\log|\mathcal{M}_i|$, $i = 1, 2$.*

Definition 4.3 *(R_1, R_2) is achievable, if for any $\bar{\epsilon}, \delta > 0$ there exists for any large enough n an (n, ϵ) -code with i-th rate at least $R_i - \delta$.*

Theorem 4.4 (Quantum Degraded Broadcast Channel) *Let $\mathfrak{U}$ be an auxiliary commutative subalgebra with $\dim|\mathfrak{U}| \leq \min\{\dim|\mathfrak{X}| + 2, \dim|\mathfrak{Y}|\dim|\mathfrak{Z}|\}$ and fixed a priori probability distribution $P_{\mathcal{U}}$ on $\mathcal{U}$. Let R_1, R_2 be nonnegative real numbers, satisfying for some a priori distribution $P_{\mathcal{U}}$ and conditional probability distribution $P_{\mathcal{X}|\mathcal{U}}$ on $\mathcal{X}$ and $\mathcal{U}$ the constraints*

$$\begin{aligned} R_1 &\leq I(\mathfrak{X} \wedge \mathfrak{Y}|\mathfrak{U}), \\ R_2 &\leq I(\mathfrak{U} \wedge \mathfrak{Z}), \\ R_1 + R_2 &\leq I(\mathfrak{X} \wedge \mathfrak{Y}) \end{aligned}$$

and fulfilling the strong broadcast condition. Then the rate $(R_1,\ R_2)$ is achievable.

Before we can prove this theorem we shall prove the following lemma concerning quantum degraded channels:

Lemma 4.5 *Let* $(P_{\mathcal{X}}, \mathcal{X}, W, V)$ *be a quantum degraded broadcast channel. Then for every n-length block-code* (f, D^Z) *for the q-DMC* V *there exists a block code* (f, D^Y) *for* W *with the same encoder such that* $\bar{e}(W, f, D^Y) \leq \bar{e}(V, f, D^Z)$.

Proof: Let the codeword set be given by $\mathcal{C}$ and define the decoding observable $D^Y = (D_{c^n})_{c^n \in \mathcal{C}}$ such that

$$0 \leq \sum_{c^n \in \mathcal{C}} [D^Y_{c^n} - \phi_*^{\otimes n}(D^Z_{c^n})] \leq \mathbb{1} \text{ and } \sum_{c^n \in \mathcal{C}} D^Y_{c^n} \leq \mathbb{1} \tag{4.1}$$

where $\phi_* : \mathfrak{Z} \to \mathfrak{Y}$ is the adjoint to the channel ϕ which connects $\mathfrak{Y}$ and $\mathfrak{Z}$ (e.g. set $D^Y_{c^n} \triangleq \phi_*^{\otimes n}(D^Z_{c^n})$ and observe that $\sum_{c^n \in \mathcal{C}} D^Y_{c^n} = \sum_{c^n \in \mathcal{C}} \phi_*^{\otimes n}(D^Z_{c^n}) \leq \phi_*^{\otimes n}(\mathbb{1}) = \mathbb{1}$.) W.l.o.g. this will give the decoding POVM D^Y (otherwise extend this with an error observable).

Since $\phi_*^{\otimes n}(D^Z_{c^n}) \geq 0$, $W_{c^n} \geq 0$ for all $c^n \in \mathcal{C}$ we get from equation (4.1)

$$\sum_{c^n \in \mathcal{C}} W_{c^n} D^Y_{c^n} \geq \sum_{c^n \in \mathcal{C}} W_{c^n} \phi_*^{\otimes n}(D^Z_{c^n}).$$

Hence, the result follows immediately:

$$\begin{aligned}
\bar{e}(W, f, D^Y) &= 1 - \frac{1}{|\mathcal{C}|} \sum_{c^n \in \mathcal{C}} \text{Tr } W_{c^n} D^Y_{c^n} \\
&\leq 1 - \frac{1}{|\mathcal{C}|} \sum_{c^n \in \mathcal{C}} \text{Tr } W_{c^n} \phi_*^{\otimes n}(D^Z_{c^n}) \\
&= 1 - \frac{1}{|\mathcal{C}|} \sum_{c^n \in \mathcal{C}} \text{Tr } \phi^{\otimes n}(W_{c^n}) D^Z_{c^n} \\
&= 1 - \frac{1}{|\mathcal{C}|} \sum_{c^n \in \mathcal{C}} \text{Tr } V_{c^n} D^Z_{c^n} = \bar{e}(V, f, D^Z)
\end{aligned}$$

■

Proof of theorem 4.4: Fix some $K > 0, \epsilon \in (0, 1/2\sqrt{2})$. Let $\hat{W} : \mathcal{U} \to \mathfrak{Y}$ and $\hat{V} : \mathcal{U} \to \mathfrak{Z}$ be two q-DMC. From theorem I.2.7 to every $n \geq n_1(|\mathcal{U}|, \dim \mathfrak{Z}), \epsilon, \mathfrak{K}$ there exist $(n, \hat{\epsilon})$ -codes $(\hat{f}, \hat{D}^Z)$ for the q-DMC V with encoder of rate

$$\frac{1}{n} \log |\mathcal{M}_{\hat{f}}| \geq I(\mathfrak{U} \wedge \mathfrak{Z}) - K/\sqrt{n}.$$

and average error rate $\hat{\epsilon}$.

Further, according to lemma 4.5 there exists for every $(n,\hat{\epsilon})$-code $(\hat{f},D^Z)$ a n-block code $(\hat{f},D^Y)$ with the same encoder $\hat{f}$ and $\bar{e}(\hat{W},\hat{f},D^Y)\leq\bar{e}(\hat{V},\hat{f},D^Z)\triangleq\bar{\epsilon}$. For every $m\in\mathcal{M}_{\hat{f}}$ we have, by definition, the inequalities

$$1-\frac{1}{|\mathcal{M}_{\hat{f}}|}\sum_{m\in\mathcal{M}_{\hat{f}}}\text{Tr }\hat{W}_{\hat{f}(m)}\hat{D}^Y_m=1-\frac{1}{|\mathcal{M}_{\hat{f}}|}\sum_{m\in\mathcal{M}_{\hat{f}}}\sum_{x^n\mathcal{X}^n}P^n_{\mathcal{X}|\mathcal{U}}(x^n|\hat{f}(m))\text{Tr }W_{x^n}\hat{D}^Y_m\leq\bar{\epsilon},\quad(4.2)$$

$$1-\frac{1}{|\mathcal{M}_{\hat{f}}|}\sum_{m\in\mathcal{M}_{\hat{f}}}\text{Tr }\hat{V}_{\hat{f}(m)}\hat{D}^Z_m=1-\frac{1}{|\mathcal{M}_{\hat{f}}|}\sum_{m\in\mathcal{M}_{\hat{f}}}\sum_{x^n\mathcal{X}^n}P^n_{\mathcal{X}|\mathcal{U}}(x^n|\hat{f}(m))\text{Tr }V_{x^n}\hat{D}^Z_m\leq\bar{\epsilon}.\quad(4.3)$$

Let $\mathcal{A}(m)$ be the largest subset of $\mathcal{X}^n$ such that

$$\text{Tr }W_{x^n}\hat{D}^Y_m\geq 1-2\bar{\epsilon}\text{ and Tr }V_{x^n}\hat{D}^Z_m\geq 1-2\bar{\epsilon}\quad\text{for every }x^n\in\mathcal{A}(m).\qquad(4.4)$$

Using the same argument as in the proof of theorem 3.5 the sets $\mathcal{A}(m)$ are disjoint. Hence,

$$\sum_{m\in\mathcal{M}_{\hat{f}}}P^n_{\mathcal{X}|\mathcal{U}}(\mathcal{A}(m)|\hat{f}(m))\geq\frac{1}{2}|\mathcal{M}_{\hat{f}}|.$$

Throwing away half of the codewords, and reducing the rate slightly, we can still get

$$P^n_{\mathcal{X}|\mathcal{U}}(\mathcal{A}(m)|\hat{f}(m))\geq\frac{1}{2}$$

for every $m\in\mathcal{M}'_{\hat{f}}\subset\mathcal{M}_{\hat{f}}$. Using Lemma 2.3, to every $m\in\mathcal{M}'_{\hat{f}}$ we can construct an (n,ϵ)-code $(f_m,D^{Y,m})$ for the q-DMC W with the codewords in $\mathcal{A}(m)$, each code having the same message set $\mathcal{M}_1$, where

$$\frac{1}{n}\log|\mathcal{M}_1|\geq I(\mathfrak{X}\wedge\mathfrak{Y}|\mathfrak{U})-K'/\sqrt{n}$$

and the average error is $\bar{\epsilon}$. Define now the encoding mapping $f:\mathcal{M}_1\times\mathcal{M}_0\to\mathcal{X}^n$ as $f(m_1,m_0)\triangleq f_{m_0}(m_1)$ for every $m_1\in\mathcal{M}_1$, $m_0\in\mathcal{M}_0\triangleq\mathcal{M}_{\hat{f}}$. The decoding observable for $\mathfrak{Z}$ is defined as follows:

$$D^Z:=\hat{D}^Z$$

For the decoding observable on $\mathfrak{Y}$ we observe from the proof of theorem 3.5, that there exists a decoding POVM $D^Y_{m_1*}$ such that

$$\frac{1}{|\mathcal{M}_1||\mathcal{M}_2|}\sum_{m_1\in\mathcal{M}_1,m_2\in\mathcal{M}_2}\left\|[m_1]\otimes[m_2]-D^Y_{m_1*}(W_{f(m_1,m_2)})\right\|_1\leq 5\bar{\epsilon}+\sqrt{47\bar{\epsilon}}\triangleq\bar{\epsilon}'.$$

Observe that equation (3.9) in the averaged version is still valid with all the terms.

■

Theorem 4.6 (Converse to Degraded Broadcast Channel I) *The capacity region of the quantum degraded broadcast channel with a classical receiver $\mathcal{Y}$ is contained in the closure of the set of all nonnegative (R_1, R_2) satisfying*

$$\begin{aligned} R_1 &\leq \sum_u q_u I_{\gamma_u}(\mathfrak{X} \wedge \mathfrak{Y}|\mathfrak{U}) \\ R_2 &\leq \sum_u q_u I_{\gamma_u}(\mathfrak{U} \wedge \mathfrak{Z}) \\ R_1 + R_2 &\leq \sum q_u I_{\gamma_u}(\mathfrak{X} \wedge \mathfrak{Y}) \end{aligned}$$

for some channel states γ_u and $q_u \geq 0, \sum_u q_u = 1$.

Proof: Observe that $\mathfrak{Y}$ is a commutative *-subalgebra since $\mathcal{Y}$ is a classical receiver. Supposing that (R_1, R_2) is an achievable rate pair, consider a sequence of n-length block codes (f_n, D, E) achieving (R_1, R_2). Let $\mathfrak{M}_1 = \mathbb{C}\mathcal{M}_1$ and $\mathfrak{M}_2 = \mathbb{C}\mathcal{M}_2$ be independent and uniformly distributed *-subalgebras over the corresponding message sets, i.e. the underlying state on $\mathfrak{M}_1 \otimes \mathfrak{M}_2$ is given by $\sum_{m_1 \in \mathcal{M}_1, m_2 \in \mathcal{M}_2} \frac{1}{|\mathcal{M}_1||\mathcal{M}_2|}[m_1] \otimes [m_2]$, and let $f_* : \mathfrak{M}_1 \otimes \mathfrak{M}_2 \to \mathfrak{X}^{\otimes n}$. Further, observe by the q-DMC's W and ϕ

$$V : \mathfrak{X}^{\otimes n} \xrightarrow{W^{\otimes n}} \mathfrak{Y}^{\otimes n} \xrightarrow{\Phi^{\otimes n}} \mathfrak{Z}^{\otimes n}.$$

We have

$$R_2 - \delta \leq \frac{1}{n} H(\mathfrak{M}_2) = \frac{1}{n} I(\mathfrak{M}_2 \wedge \mathfrak{Z}^{\otimes n}) + \frac{1}{n} H(\mathfrak{M}_2|\mathfrak{Z}^{\otimes n})$$

and

$$\begin{aligned} R_1 - \delta &\leq \frac{1}{n} H(\mathfrak{M}_1|\mathfrak{M}_2) = \frac{1}{n} I(\mathfrak{M}_1 \wedge \mathfrak{Y}^{\otimes n}|\mathfrak{M}_2) + \frac{1}{n} H(\mathfrak{M}_1|\mathfrak{Y}^{\otimes n}\mathfrak{M}_2) \\ &\leq \frac{1}{n} I(\mathfrak{X}^{\otimes n} \wedge \mathfrak{Y}^{\otimes n}|\mathfrak{M}_2) + \frac{1}{n} H(\mathfrak{M}_1|\mathfrak{Y}^{\otimes n}). \end{aligned}$$

By Fano's Inequality (theorem I.2.6) the right most term is converging to zero. Further

$$\begin{aligned} I(\mathfrak{M}_2 \wedge \mathfrak{Z}^{\otimes n}) &= H(\mathfrak{Z}^{\otimes n}) - H(\mathfrak{Z}^{\otimes n}|\mathfrak{M}_2) \\ &\overset{\text{Th. } I.2.4}{\leq} \sum_{i=1}^n H(\mathfrak{Z}_i) - H(\mathfrak{Z}^{\otimes n}|\mathfrak{M}_2) \\ &\overset{\text{Definition}}{=} \sum_{i=1}^n H(\mathfrak{Z}_i) - \sum_{i=1}^n H(\mathfrak{Z}_i|\mathfrak{M}_2\mathfrak{Z}^{\otimes(i-1)}) \\ &\leq \sum_{i=1}^n [H(\mathfrak{Z}_i) - H(\mathfrak{Z}_i|\mathfrak{M}_2\mathfrak{Z}^{\otimes(i-1)}\mathfrak{Z}^{\otimes(i-1)})]. \end{aligned}$$

Here for every fixed value $m_2 \in \mathcal{M}_2$ on $\mathfrak{M}_2$ the output $V_{f(\cdot\ ,m_2),i} \in \mathfrak{Z}_i$ of the q-DMC Φ is conditionally independent of the previous outputs $V^{i-1}_{f(\cdot\ ,m_2)} \in \mathfrak{Z}^{i-1}$, if $W^{i-1}_{f(\cdot\ ,m_2)} \in \mathfrak{Y}^{\otimes(i-1)}$ and the value of $\mathfrak{M}_2$ are given (Note that we only use block-encoding without entanglement at the encoder!) . Thus we have

$$H(\mathfrak{Z}_i|\mathfrak{M}_2\mathfrak{Z}^{\otimes(i-1)}\mathfrak{Y}^{\otimes(i-1)}) = H(\mathfrak{Z}_i|\mathfrak{M}_2\mathfrak{Y}^{\otimes(i-1)}),$$

whence

$$I(\mathfrak{M}_2 \wedge \mathfrak{Z}^{\otimes n}) \leq \sum_{i=1}^{n} I(\mathfrak{M}_2\mathfrak{Y}^{\otimes(i-1)} \wedge \mathfrak{Z}_i). \tag{4.5}$$

Further

$$\begin{aligned} I(\mathfrak{X}^{\otimes n} \wedge \mathfrak{Y}^{\otimes n}|\mathfrak{M}_2) &= H(\mathfrak{Y}^{\otimes n}|\mathfrak{M}_2) - H(\mathfrak{Y}^{\otimes n}|\mathfrak{M}_2\mathfrak{X}^{\otimes n}) \\ &= \sum_{i=1}^{n}[H(\mathfrak{Y}_i|\mathfrak{M}_2\mathfrak{Y}^{\otimes(i-1)}) - H(\mathfrak{Y}_i|\mathfrak{M}_2\mathfrak{X}_i\mathfrak{Y}^{\otimes(i-1)})] \\ &= \sum_{i=1}^{n} I(\mathfrak{X}_i \wedge \mathfrak{Y}_i|\mathfrak{M}_2\mathfrak{Y}^{\otimes(i-1)}). \end{aligned} \tag{4.6}$$

Defining $\mathfrak{U}_i \triangleq \mathfrak{M}_2\mathfrak{Y}^{\otimes(i-1)}$ we can bound (4.6)

$$\frac{1}{n} I_\gamma(\mathfrak{X}^{\otimes n} \wedge \mathfrak{Y}^{\otimes n}|\mathfrak{M}_2) \leq \frac{1}{n}\sum_{i=1}^{n} I_\gamma(\mathfrak{X}_i \wedge \mathfrak{Y}_i|\mathfrak{U}_i) \leq \sum_u q_u I_{\gamma_u}(\mathfrak{X} \wedge \mathfrak{Y}|\mathfrak{U})$$

and (4.5) becomes

$$\frac{1}{n} I_\gamma(\mathfrak{M}_2 \wedge \mathfrak{Z}^{\otimes n}) \leq \frac{1}{n}\sum_{i=1}^{n} I_\gamma(\mathfrak{M}_2 \wedge \mathfrak{Z}_i) \leq \sum_u q_u I_{\gamma_u}(U \wedge \mathfrak{Z})$$

where we denote γ as the average state on $\mathfrak{M}_2(\mathfrak{U}\mathfrak{X}\mathfrak{Y}\mathfrak{Z})^{\otimes n}$, and γ_u the u-th tensor-copy of the channel state.

■

If the receiver $\mathcal{Y}$ is not classical, we have the following conjecture:

Conjecture 4.7 (Converse to Degraded Broadcast Channel II) *The capacity region of the quantum degraded broadcast channel is contained in the closure of the set all nonnegative* (R_1, R_2) *satisfying*

$$\begin{aligned} R_1 &\leq \sum_u q_u I_{\gamma_u}(\mathfrak{X} \wedge \mathfrak{Y}|\mathfrak{U}) \\ R_2 &\leq \sum_u q_u I_{\gamma_u}(\mathfrak{U} \wedge \mathfrak{Z}) \\ R_1 + R_2 &\leq \sum q_u I_{\gamma_u}(\mathfrak{X} \wedge \mathfrak{Y}) \end{aligned}$$

for some channel states γ_u *and* $q_u \geq 0, \sum_u q_u = 1$.

5 Code Stuffing Lemma

Lemma 5.1 (Code Stuffing Lemma I) *For every* $\tau, \eta, \delta_u > 0, \epsilon \in (0,1)$ *and* $n \geq n_0(\mathcal{X}, \dim \mathfrak{Y}, \dim \mathfrak{Z}, \tau, \eta, \epsilon)$, *to every quadruple of *-subalgebras* $(\mathfrak{X}, \mathfrak{U}, \mathfrak{Y}, \mathfrak{Z})$ *with channel state* ρ_u *satisfying the broadcast-constraint and*

$$I(\mathfrak{X} \wedge \mathfrak{Y}|\mathfrak{U}) \geq I(\mathfrak{X} \wedge \mathfrak{Z}|\mathfrak{U}),$$

to every set $\mathcal{A} \in \mathcal{X}^n$ *and sequence* $u^n \in \mathcal{T}^n_{V,P_U,\delta_u}$ *with* $P^n_{\mathcal{X}|\mathcal{U}}(\mathcal{A}|u^n) \geq \eta$ *there exists a subset* $\tilde{\mathcal{A}}$ *of* $\mathcal{A}$ *such that*

1) *all* $x^n \in \tilde{\mathcal{A}}$ *have the same type;*

2) $\tilde{\mathcal{A}}$ *is the codeword set of an* (n,ϵ)*-code for the q-DMC* W *;*

3) $\tilde{\mathcal{A}}$ *is the disjoint union of sets* $\tilde{\mathcal{A}}^{(m)}, m = 1, \ldots, M$ *where*

$$\begin{aligned} \left| \frac{1}{n} \log |\tilde{\mathcal{A}}^{(m)}| - I(\mathfrak{X} \wedge \mathfrak{Z}|\mathfrak{U}) \right| &\leq \tau, \\ \left| \frac{1}{n} \log M - (I(\mathfrak{X} \wedge \mathfrak{Y}|\mathfrak{U}) - I(\mathfrak{X} \wedge \mathfrak{Z}|\mathfrak{U})) \right| &\leq \tau \end{aligned}$$

and $\tilde{\mathcal{A}}^{(m)}$ *is the codeword set of an* (n,ϵ)*-code for the q-DMC* V.

Proof: We extend an idea of Ahlswede's reported in [6] by applying the maximal code construction of lemma 2.3 in two cycles. In this proof, consider only such codes for which the encoder is the identity mapping on the codeword set. In such cases the code will be defined by the codeword set and the decoder POVMs. Write $\tau' \triangleq \frac{\tau}{4}$ and suppose that $\epsilon \leq \frac{1}{2\sqrt{2}}$. In lemma 2.3, there exist (n,ϵ)-codes with common codeword set $\bar{\mathcal{A}} \in \mathcal{A}$ for the q-DMC's W and V such that

$$\left| \frac{1}{n} \log |\bar{\mathcal{A}}| - I(\mathfrak{X} \wedge \mathfrak{Z}|\mathfrak{U}) \right| \leq 2\tau' \tag{5.1}$$

and the corresponding decoding projectors $D^Y_{x^n}, D^Z_{x^n}$ satisfy

$$\text{Tr } D^Y_{x^n} \leq \text{Tr } \Pi^n_{V,W,\delta}(x^n) \text{ and Tr } D^Z_{x^n} \leq \text{Tr } \Pi^n_{V,V,\delta}(x^n) \text{ for all } x^n \in \bar{\mathcal{A}},$$

if n is large enough for some $\delta > 0$. For any such code write

$$\bar{B} \triangleq \sum_{x^n \in \bar{\mathcal{A}}} D^Y_{x^n}, \qquad \bar{C} \triangleq \sum_{x^n \in \bar{\mathcal{A}}} D^Z_{x^n}.$$

Considering a family of such pairs of codes, with disjoint codeword set $\mathcal{A}^{(m)}, m = 1\ldots,\hat{M}-1$, such that the corresponding decoding projectors $\bar{B}$, denoted by $B^{(m)}$, $m = 1,\ldots\hat{M}-1$, also commute pairwise.

Observe from remark 2.4 that the decoder for the channel code W may be chosen as a von Neumann observable (i.e. all its operators are mutually orthogonal projectors).

Now, we claim that for large enough n such a family exists with

$$\frac{1}{n}\log\hat{M} \geq I(\mathfrak{X}\wedge\mathfrak{Y}|\mathfrak{U}) - I(\mathfrak{X}\wedge\mathfrak{Z}|\mathfrak{U}) - 4\tau'. \tag{5.2}$$

In fact, consider a maximal family of code pairs as above. This means that if a pair of (n,ϵ)-codes with common codeword set $\bar{\mathcal{A}}\in\mathcal{A}$ satisfies (5.2), further $\hat{\mathcal{A}}$ is disjoint from $\bigcup_{m<\hat{M}}\mathcal{A}^{(m)}$ and $\bar{B}$ is orthogonal to $\sum_{m<\hat{M}}B^{(m)}$, then it cannot meet (5.1).

Let the (possibly empty) set $\mathcal{A}^{(\hat{M})}$ be such an $\bar{\mathcal{A}}$ which is not properly contained in any set with the same properties; let $B^{(\hat{M})}$ and $C^{(\hat{M})}$ be the corresponding set $\bar{B}$ resp. $\bar{C}$. Then

$$\frac{1}{n}\log|\mathcal{A}^{(\hat{M})}| < I(\mathfrak{X}\wedge\mathfrak{Z}|\mathfrak{U}) - 2\tau'. \tag{5.3}$$

Further, setting

$$B \triangleq \sum_{m=1}^{\hat{M}} B^{(m)},$$

it follows that with $\gamma = \min\{1-\epsilon, \epsilon/32\}$

$$\text{Tr } W_{x^n}B \geq \gamma \text{ or } \text{Tr } V_{x^n}C^{(\hat{M})} \geq \gamma \tag{5.4}$$

for every $x^n \in \mathcal{A}\setminus\bigcup_{m=1}^{\hat{M}}\mathcal{A}^{(m)}$. By definition we already have $\text{Tr } W_{x^n}B \geq 1-\gamma$ for all $x^n\in\bigcup_{m=1}^{\hat{M}}\mathcal{A}^{(m)}$ and with $\gamma\leq 1/2\sqrt{2}$ (5.4) is true for every $x^n\in\mathcal{A}$.

Denoting $\mathcal{A}_1$ resp. $\mathcal{A}_2$ the set of those $x^n\in\mathcal{A}$ for which the first resp. second inequality of (5.4) holds, the assumption $P^n_{\mathcal{X}|\mathcal{U}}(\mathcal{A}|u^n)\geq\eta$ gives

$$P^n_{\mathcal{X}|\mathcal{U}}(\mathcal{A}_1|u^n) \geq \frac{\eta}{2} \text{ or } P^n_{\mathcal{X}|\mathcal{U}}(\mathcal{A}_2|u^n) \geq \frac{\eta}{2}.$$

As in the proof of (2.3), it follows for $n\geq n_2$ that

$$\frac{1}{n}\log\left|\bigcup_{m=1}^{\hat{M}}\mathcal{A}^{(m)}\right| \geq I(\mathfrak{X}\wedge\mathfrak{Y}|\mathfrak{U}) - 2\tau' \text{ or } \frac{1}{n}\log|\mathcal{A}^{(\hat{M})}| \geq I(\mathfrak{X}\wedge\mathfrak{Z}|\mathfrak{U}) - 2\tau'.$$

But the second possibility is ruled out by (5.3). Thus, with (5.1) and (5.3) we obtain (5.2). The commutativity of the (codebook) decoding projectors $B^{(m)}$ means exactly

that the union of the sets $\mathcal{A}^{(m)}$ is the codeword set of an (n, ϵ)-code for the q-DMC W.

Further, by type counting, for every $m < \hat{M}$ there is a type P_m such that

$$\left| \frac{1}{n} \log |\mathcal{A}^{(m)} \cap \mathcal{T}_{P_m}| - I(\mathfrak{X} \wedge \mathfrak{Z}|\mathfrak{U}) \right| \leq 3\tau'$$

if $n \geq n_3$. For an exact calculation see also the proof of theorem I.5.1. Denote $\tilde{\mathcal{A}}^{(m)} \triangleq \mathcal{A}^{(m)} \cap \mathcal{T}_{P_m}$. Similarly, denote for every type P by $M(P)$ the set of those indices m for which $P_m = P$. Then, again with type counting, there exists a type $\tilde{P}$ such that

$$\frac{1}{n} \log |M(\tilde{P})| \geq I(\mathfrak{X} \wedge \mathfrak{Y}|\mathfrak{U}) - I(\mathfrak{X} \wedge \mathfrak{Z}|\mathfrak{U}) - \tau'$$

if $n \geq n_4$. Restricting the original codes to the codeword sets $\tilde{\mathcal{A}}^{(m)}, m \in \mathcal{M}(\tilde{P})$, the result follows.

■

Chapter III

Quantum Cryptography with Separable States and Wiretapper

In chapter I we derived a coding theorem for semi-classical and oc-type states where a wiretapper was allowed to listen to the public channel. In this chapter we will use results of the quantum multi-user communication theory in chapter II in order to prove the existence of a Secret Sharing Strategy with positive rate even if the wiretapper $\mathcal{Z}$ is (semi-classically) correlated with the quantum source state of $\mathcal{X}$ and $\mathcal{Y}$.

Again, we will extend results of [2] to the quantum case, i.e. we will especially construct so called wiretap-channel-codes.

1 Code Stuffing

In order to prove the main results, we will first prove a slight variation of the Code Stuffing Lemma II.5.1:

Lemma 1.1 (Code Stuffing Lemma II) *Given compatible *-subalgebras $\mathfrak{U}, \mathfrak{X}, \mathfrak{Y}, \mathfrak{Z}$ such that the broadcast condition is fulfilled, $\mathfrak{Z}$ commutative and*

$$I(\mathfrak{X} \wedge \mathfrak{Y}|\mathfrak{U}) - I(\mathfrak{X} \wedge \mathfrak{Z}|\mathfrak{U}) \triangleq H \geq 0,$$

and arbitrary small $\eta > 0, \epsilon > 0, \tau > 0$, for sufficiently large n every set $\mathcal{A} \in \mathcal{X}^n$ with $P_{\mathcal{X}}^{\otimes n}(\mathcal{A}) \geq \eta$ contains a subset $\bar{\mathcal{A}}$ with the following properties:

i) $\bar{\mathcal{A}}$ consists of sequences of the same type, and it is codeword set of an (n, ϵ)-code for the q-DMC $W : \mathfrak{X} \to \mathfrak{Y}$ with channel state $\rho_V = \sum_{x^n \in \mathcal{X}^n} [x^n] \otimes W_{x^n}$.

ii) $\bar{\mathcal{A}}$ is the union of $M = \exp\{n(H - \epsilon)\}$ mutually disjoint sets $\bar{\mathcal{A}}^{(m)}$ of size $|\bar{\mathcal{A}}^{(m)}| = |\exp\{n(I(\mathfrak{X} \wedge \mathfrak{Z}|\mathfrak{U}) - \epsilon)\}$, $m = 1, \ldots, M$.

iii) If $\mathfrak{X}^{\hat{\otimes} n}$ denotes a $*$-subalgebra of $\mathfrak{X}^{\otimes n}$ such that a measurement on $\hat{\mathfrak{X}}^{\otimes n}$ gives a uniform distribution on $\hat{\mathcal{A}}$ and $\hat{\mathfrak{Z}}^{\otimes n}$ denotes the corresponding output of the q-DMC $V : \mathfrak{X} \to \mathfrak{Z}$, then for a POVM $\hat{K}$ with values

$$\hat{K} = m \text{ if } \hat{\mathfrak{X}}^{\otimes n} \in \tilde{\mathcal{A}}^{(m)}, \qquad 1 \leq m \leq M,$$

we have

$$I(\hat{K} \wedge \hat{\mathfrak{Z}}^{\otimes n}) < \tau n. \tag{1.1}$$

Proof: In lemma II.5.1 we already proved that if $\mathcal{A} \in \mathcal{X}^n$ satisfies $P_{\mathcal{X}|\mathcal{U}}(\mathcal{A}|u^n) > \eta$ for some $u^n \in \mathcal{T}_{P_{\mathcal{U}},\delta}$, then $\mathcal{A}$ contains a subset $\tilde{\mathcal{A}}$ with the properties 1), 2) and further, $\tilde{A}^{(m)}$ is the codeword set of an (n, ϵ)-code for the DMC V. Now we can copy the proof of [2], Lemma A, where $I(\hat{K} \wedge \hat{\mathfrak{Z}}^{\otimes n})$ can be upper-bounded using classical information theory (note that $\mathfrak{X}$ and $\mathfrak{Z}$ are commutative algebras), explicitly bounding the three terms of $I(\hat{K} \wedge \hat{\mathfrak{Z}}^{\otimes n})$:

$$\begin{aligned} I(\hat{K} \wedge \hat{\mathfrak{Z}}^{\otimes n}) &= H(\hat{\mathfrak{Z}}^{\otimes n}) \\ &\quad -H(\hat{\mathfrak{Z}}^{\otimes n}|\hat{\mathfrak{X}}^{\otimes n}) \\ &\quad -I(\hat{\mathfrak{X}}^{\otimes n} \wedge \hat{\mathfrak{Z}}^{\otimes n}|\hat{K}) \\ &\leq 1 + n(H(\hat{\mathfrak{Z}}|\mathfrak{U}) + \epsilon) + \epsilon n \log \dim \mathfrak{Z} \\ &\quad +n((H(\hat{\mathfrak{X}}) + \epsilon) \\ &\quad +(1-\epsilon)nI(\mathfrak{X} \wedge \mathfrak{Z}|\mathfrak{U}) - \epsilon) - 1 \\ &\leq \tau n \end{aligned}$$

provided ϵ/τ is sufficiently small by classical methods of Csiszar and Körner [16].

■

2 Source-Type Model with Wiretapper

We are again given a q-DMMS with a three-component source $(\mathfrak{X}, \mathfrak{Y}, \mathfrak{Z}, \Pi, P)$. Terminal $\mathcal{X}$ can apply quantum operations on $\mathfrak{X}^{\otimes n}$, (resp. terminal $\mathcal{Y}$ on $\mathfrak{Y}^{\otimes n}$ and terminal $\mathcal{Z}$ on $\mathfrak{Z}^{\otimes n}$).

The Secret Sharing Strategy is the same as in chapter I, except that besides listening to the public communication between terminal $\mathcal{X}$ and $\mathcal{Y}$, terminal $\mathcal{Z}$ can also apply a POVM onto its part of the common state (output $\mathfrak{Z}^{\otimes n}$). We will again prove the lower bounds by restricting the quantum operations to the standard form (cf. (I.4.1)).

We have to modify definition I.4.6 for our model by replacing (I.4.3) by

$$\frac{1}{n} I(\mathfrak{M}_{[k]}, \mathfrak{N}_{[k]}, \mathfrak{Z}^{\otimes n} \wedge K) < \epsilon. \tag{2.1}$$

Definition 2.1

1) The Source-Type Model with Wiretapper is called **fully quantum**, *if the average state* ρ *is arbitrary.*

2) The Source-Type Model with Wiretapper is called **separable**, *if the average state is given by* $\rho = \sum_{i=1}^{l} P(i)\sigma_i \otimes W_i \otimes V_i$, *i.e. separable by itself.*

3) The Source-Type Model with Wiretapper is called **1-semi-classical**, *if besides 2)* $\mathfrak{X} = \mathbb{C}\mathcal{X}$ *and* **2-semi-classical** *if, further,* $\mathfrak{Z} = \mathbb{C}\mathcal{Z}$.

We will restrict ourselves to the 2-semi-classical case, i.e. a multiple source $(\mathbb{C}\mathcal{X}, \mathfrak{Y}, \mathbb{C}\mathcal{Z}, \{[x]\otimes \pi \otimes [z]\}, P(x,\pi,z))$. Cai and Yeung [12] also recently solved the analogous quantum wiretap-channel problem in the 1-semi-classical case, so there might be a possible improvement here.

Theorem 2.2 *For the Secret Sharing Source Model with Wiretapper, the forward key-capacity for the 2-semi-classical source is lower bounded by*

$$\max_{P_U, P_{\mathcal{X}|\mathcal{U}}} I(\mathfrak{X} \wedge \mathfrak{Y}|\mathfrak{U}) - I(\mathfrak{X} \wedge \mathfrak{Z}|\mathfrak{U}),$$

for a commutative, finite helper subalgebra $\mathfrak{U} = \mathbb{C}\mathcal{U}$ *such that the broadcast condition definition II.2.2 is fulfilled.*

Proof: If suffices to show that for any $(\mathcal{U}, P_{\mathcal{X},\mathcal{U}})$ fulfilling the broadcast condition

$$H \triangleq I(\mathfrak{X} \wedge \mathfrak{Y}|\mathfrak{U}) - I(\mathfrak{X} \wedge \mathfrak{Z}|\mathfrak{U})$$

is a forward-achievable key rate.

The proof follows the same lines as the proof of theorem I.5.1, but now $\mathcal{X}^n$ will be partitioned into sets C_i of more complex structure. Let $P^n_{\mathcal{Z}|\mathcal{X}}$ be the distribution of the classical DMC $V : \mathcal{X} \to \mathcal{Z}$ and assume $H > 0$. W.l.o.g. we apply lemma 1.1 to consecutively selected mutually disjoint sets $\mathcal{C}_i \subset \mathcal{X}^n$ such as $\tilde{\mathcal{A}}$ in that lemma (following the idea of the Code Partition Lemma 5.2). Then, if this process can not be continued after having picked $\mathcal{C}_N$, we obtain

$$P^n_{\mathcal{X}}(\bigcup_{i=1}^{N} \mathcal{C}_i) > 1 - \eta. \tag{2.2}$$

By definition, each $\mathcal{C}_i$ consists of sequences of the same type and is the codeword set of an $(n, \epsilon')-$ code for the q-DMC $W : \mathcal{X} \to \mathfrak{Y}$ (which can be extended uniquely by linearity to $W : \mathfrak{X} \to \mathfrak{Y}$.) Further, $\mathcal{C}_i$ is the disjoint union of $M = \lceil \exp\{nH - n\epsilon\} \rceil$ subsets $\mathcal{C}_{i,m}$ of equal size, such that the following holds: If a maximal measurement $\hat{X}^n$

on a subalgebra $\hat{\mathfrak{X}}^{\otimes n}$ of $\mathfrak{X}^{\otimes n}$ gives a uniform distribution on $\mathcal{C}_i$ and the support of the channel output of $\hat{\mathfrak{X}}^{\otimes n}$ is given by $\hat{\mathfrak{Z}}^{\otimes n}$ such that the classical channel distribution of the channel $V : \hat{\mathcal{X}} \to \hat{\mathcal{Z}}$ is $P_{\hat{\mathcal{Z}}^n|\hat{\mathcal{X}}^n} = P^n_{\hat{\mathcal{Z}}|\hat{\mathcal{X}}}$ then, defining a POVM $\hat{K}$ setting $\hat{K} = m$ if a maximal measurement on the average state $\rho^{\otimes n}$ restricted to $\hat{\mathfrak{X}}^{\otimes n}$ determines an element $x^n \in \mathcal{C}_{i,m}$, we have $I(\hat{\mathfrak{Z}}^{\otimes n} \wedge \hat{K}) < \tau n$.

Let E_{i_m}, $1 \leq i \leq N, 1 \leq m \leq M$ be the orthogonal encoding measurement projecting $\rho^{\otimes n}|_{\mathfrak{X}^{\otimes n}}$ to the m-th sub-code of the i-th codebook $\mathcal{C}_{i,m}$. Extending this to a POVM E in the normal way (extend an error POVM element E_0) we further define the codebook separating POVM $\hat{E}$ by $\hat{E}_i = \sum_{m=1}^{M} E_{i_m}$ and $\hat{E}_0 = E_0$.

Now, let terminal $\mathcal{X}$ apply the quantum operation

$$\Phi : \rho_{\mathcal{X}} \to \sum_{i=0}^{N} \sqrt{\hat{E}_i}\rho_{\mathcal{X}}\sqrt{\hat{E}_i} \otimes [i] \otimes [i]$$

and sending $\mathfrak{M}_1$ to terminal $\mathcal{Y}$, who again does nothing in the first step. Further $\mathcal{X}$ uses the POVM K' defined by

$$K'_m \triangleq \begin{cases} \sum_{i=1}^{N} E_{i_m} \otimes [i] \otimes \mathbb{1}, & \text{if } 1 \leq m \leq M, \\ \mathbb{1} - \sum_{j=1}^{M} K_j, & \text{if } m = 0. \end{cases}$$

Let D_i be the decoding POVM of the channel $W : \mathcal{X} \to \mathfrak{Y}$ related to the codebook $\mathcal{C}_i$, i.e D_{i_j} is the decoding element concerning the $j-th$ element of the i-th codebook. Then define a further decoding mesurement $\hat{D}_i$ to the codebook $\mathcal{C}_i$ by $\hat{D}_{i_m} = \sum_{x_{i_j} \in \mathcal{C}_{i,m}} D_{i_j}$ and extend this to an overall decoding POVM L' on $\mathfrak{Y}^{\otimes n} \otimes \mathfrak{L}_1 \otimes \mathfrak{M}_1$ given by

$$L'_m \triangleq \begin{cases} \sum_{i=1}^{N} \hat{D}_{i,m} \otimes \mathbb{1} \otimes [i], & \text{if } 1 \leq m \leq M, \\ \mathbb{1} - \sum_{j=1}^{M} L_j, & \text{if } m = 0. \end{cases}$$

If $\mathcal{X}$ measures $K' = [0]$ an error occurred and w.l.o.g. we can extend the measurement K' to a quantum operation K, such that K becomes uniformly distributed over $\{1, \ldots, M\}$ independent of the source if $K' = [0]$. The same is valid for $\mathcal{Y}$ measuring $L' = [0]$ (which denotes an encoding or decoding error) extending this to a POVM L in the same way. Now, since there is only a single forward transmission $\mathfrak{M}_1$, (2.1) reduces to

$$\frac{1}{n} I(\mathfrak{M}_1, \mathfrak{Z}^{\otimes n} \wedge K) < \epsilon \tag{2.3}$$

We want to check the definition I.4.6 with (2.3) in the case of (I.4.3) (for more details see also the proof of of theorem I.5.1)

1) Equation (I.4.2): Clearly

$$\frac{1}{n}\Pr(K \neq L) \leq \eta + \epsilon' \leq \epsilon$$

with $\epsilon \triangleq \eta + \epsilon'$ by (2.2) and the fact that we used (n, ϵ')-codes for the encoding.

2) Equation (I.4.5): Since $\mathcal{C}_i$ consists of sequences of the same type, and each $C_{i,m}$ has the same size, we get for $1 \leq i \leq N$:

$$\Pr(K = [m] | \mathfrak{M}_1 = [i]) = \frac{\operatorname{Tr} \rho^{\otimes n}(E_{i_m} \otimes \mathbb{1}_{\mathfrak{Y}^{\otimes n}} \otimes \mathbb{1}_{\mathfrak{Z}^{\otimes n}})}{\operatorname{Tr} \rho^{\otimes n}(E_i \otimes \mathbb{1}_{\mathfrak{Y}^{\otimes n}} \otimes \mathbb{1}_{\mathfrak{Z}^{\otimes n}})} = \frac{1}{M}$$

For $\mathfrak{M}_1 = [0]$ we already have this by definition. Thus K is uniformly distributed on $\{1, \cdots, M\}$ and it is independent of $\mathfrak{M}_1$. Hence,

$$\frac{1}{n} \log |\mathcal{K}| < \frac{1}{n} H(K) + \epsilon'$$

is trivially fulfilled.

3) Equation (I.4.4): Since $M = \lceil \exp\{nH - n\epsilon'\} \rceil$ we easily get from 2)

$$\frac{1}{n} H(K) > \frac{1}{n} \log M - \epsilon' \geq H - \epsilon'$$

for sufficiently large n.

4) Equation (2.3): Now, observing that only commutative subalgebras are involved, we obtain

$$\begin{aligned} I(\mathfrak{M}_1, \mathfrak{Z}^{\otimes n} \wedge K) &\overset{(i)}{=} I(\mathfrak{Z}^{\otimes n} \wedge K | \mathfrak{M}_1) \\ &\overset{(ii)}{=} \sum_{i=1}^{N} P_{\mathcal{X}}^n(\mathcal{C}_i) I(\mathfrak{Z}^{\otimes n} \wedge K | \mathfrak{M}_1 = [i]) \\ &\overset{(iii)}{=} I(\hat{\mathfrak{Z}}^{\otimes n} \wedge \hat{K}) < \tau n. \end{aligned}$$

Here (i) follows by the independence of K and $\mathfrak{M}_1$, and (ii) holds because of the definition of the POVM K $I(\mathfrak{Z}^{\otimes n} \wedge K | \mathfrak{M}_i = [0]) = 0$. Since $\mathcal{C}_i$ consists of sequences of the same type, we get $\Pr(\mathfrak{X}^{\otimes n} = [x^n] | \mathfrak{M}_1 = [i]) = 1/|\mathcal{C}_i|$, given the state $\Phi(\rho_{\mathcal{X}}^{\otimes n})$. It follows that

$$\Pr(\mathfrak{Z}^{\otimes n} = [z^n], K = [m] | \mathfrak{M}_1 \neq [0]) = \Pr(\hat{\mathfrak{Z}}^{\otimes n} = [z^n], \hat{K} = [m]),$$

thus (iii) is valid and the result follows with τ in the role of ϵ by (1.1).

■

Corollary 2.3 *If there exists a maximal measurement Y such that with the uniquely defined maximal measurement X and Z $I(X \wedge Y) > I(X \wedge Z)$, a secret key can be achieved with positive rate.*

3 Open Problems

1) Try to prove the converse to theorem 2.2 using the construction of Ahlswede and Ciszar [2] and properties of the quantum mutual information.

2) Use the result of Cai and Yeung [12] to extend the theorem to the 1-semi-classical case (maybe giving other bounds).

Chapter IV

Quantum Cryptography With Entangled States

1 Quantum Key Distribution Protocol

Quantum key distribution (QKD) is a provably secure secret sharing protocol by which private key bits can be created between two terminals $\mathcal{X}$ and $\mathcal{Y}$ using a public channel. The key bits can then be used to implement a classical private key cryptosystem, to enable both terminals to communicate securely. The only requirement for the QKD protocol is that qubits can be communicated over the public channel, with an error rate lower than a certain threshold. In this chapter we shall present an easy approximation of this bound for the BB84 QKD protocol introduced 1984 by Bennett and Brassard [9].

A large number of proofs for the security of various quantum key distribution protocols, under different circumstances, have been presented. Of particular note is a complete (and complicated) proof of the security of QKD with BB84 given by Mayers [28] in 1998. A simpler proof, which uses EPR states and requires perfect quantum computation, was given by Lo and Chau [27] one year later. An even simpler (and nice) proof of Shor and Preskill [35] in 2000 reduces a perfect EPR protocol to a simplified Lo/Chau-protocol, and then further to the BB84 protocol, using error-correcting codes (producing privacy amplification and error-correction at the same time). For an overview of this reduction-proof see also the recent textbook account of [13].

Let $|0\rangle, |1\rangle$ be an orthogonal qubit basis, denoted as $X-$basis , and define $|+\rangle \triangleq (|0\rangle + |1\rangle)/\sqrt{2}$, $|-\rangle \triangleq (|0\rangle - |1\rangle)/\sqrt{2}$, which gives the corresponding $Z-$basis.

Let terminals $\mathcal{X}$ and $\mathcal{Y}$ try to calculate a common secret key, which should be unknown to a third terminal $\mathcal{Z}$, as in the last two chapters. In order to achieve this we will use

The BB84 QKD protocol [9]

1: Terminal $\mathcal{X}$ chooses $(4+\delta)n$ random data bits.

2: Terminal $\mathcal{X}$ chooses a random $(4+\delta)n$-bit string b. It encodes each data bit as $\{|0\rangle, |1\rangle\}$ if the corresponding bit of b is 0 or $\{|+\rangle, |-\rangle\}$ if b is 1.

3: Terminal $\mathcal{X}$ sends the resulting state to terminal $\mathcal{Y}$.

4: Terminal $\mathcal{Y}$ receives the $(4+\delta)n$ qubits, announces this fact, and measures each qubit in the X or Z basis using the corresponding observables σ_x (resp. σ_z) at random.

5: Terminal $\mathcal{X}$ announces b.

6: Terminal $\mathcal{X}$ and $\mathcal{Y}$ discard any bits where terminal $\mathcal{Y}$ measured a different basis than that which terminal $\mathcal{X}$ prepared. With high probability, there are at least $2n$ bits left (if not, abort the protocol). They keep $2n$ bits.

7: Terminal $\mathcal{X}$ selects a subset of n bits that will serve as a check on terminal $\mathcal{Z}$'s interference, and tells terminal $\mathcal{Y}$ which bits it selected.

8: Terminal $\mathcal{X}$ and $\mathcal{Y}$ announce and compare the values of the n check bits. If more than an accepted number disagree, they abort the protocol.

9: Terminal $\mathcal{X}$ and $\mathcal{Y}$ perform information reconciliation and privacy amplification on the remaining n bit-string k to obtain m shared key bits.

Definition 1.1 *Let p_e be the probability of error for the quantum qubit channel from $\mathcal{X}$ to $\mathcal{Y}$, under the constraint, that $\mathcal{X}$ and $\mathcal{Y}$ choose the same measurement basis, i.e.*

$$p_e \triangleq \frac{N_w}{N_r + N_w},$$

where N_w denotes the number of wrong bits even when the same measurement basis was chosen, and $N_r = 2n - N_w$ is the number of right decoded bits.

Let $(P, \mathfrak{X} \otimes \Pi)$ consist of a probability distribution P on a finite set of states $[i] \otimes \rho_i$ on $\mathbb{C}\mathcal{X} \otimes \mathfrak{L}(\mathcal{H})$ in $\mathfrak{X} \otimes \Pi$ with commutative $\mathfrak{X}$. By the Holevo bound [23] we know that

$$I_\rho(X \wedge Y) \leq I_\rho(X \wedge \mathfrak{Y}),$$

with $\rho = \sum_i P_i [i] \otimes \rho_i$, X the uniquely defined maximal measurement on $\mathfrak{X}$ and Y an arbitrary measurement on $\mathfrak{Y}$. This can easily be extended to the form

$$I_\rho(X \wedge Y_1) + I_\rho(X \wedge Y_2) + \cdots \leq J_\rho(X, Y_1, Y_2, \dots)$$

for observables Y_1, $Y_2, \dots$ giving a nontrivial upper bound J. This is known as an information-exclusion principle in the literature. Observe that a non-ideal measurement

$\tilde{Y}$ of an observable Y cannot give more information than a measurement of A itself, thus $I_\rho(X \wedge \tilde{Y}_1) + I_\rho(X \wedge \tilde{Y}_2) + \cdots \leq J_\rho(X, Y_1, Y_2, \ldots, \mathfrak{Y})$.

Now let D^Y and D^Z be two observables in an $N-$ dimensional Hilbert space $\mathcal{H}$ with eigenstates $|d_j^Y\rangle$, $|d_j^Z\rangle$, $1 \leq j \leq N$ and define

$$d = \max_{i,j} |\langle d_i^Y || d_j^Z \rangle|$$

giving the maximal possible overlap of eigenstates of D^Y and D^Z. For non-degenerate D^Y, D^Z we immediately get

$$H_\rho(D^Y), H_\rho(D^Z) \leq \log N. \tag{1.1}$$

while

$$-2 \log d \leq H_\rho(D^Y) + H_\rho(D^Z) \tag{1.2}$$

was derived by [37]. Observe further that (1.1) is tight for $\rho_* = \frac{1}{N} \mathbb{1}_\mathcal{H}$.

Now we get (suppressing the state ρ)

$$\begin{aligned} I(X \wedge D^Y) + I(X \wedge D^Z) &= [H(D^Y) + H(D^Z)] - [\sum_i P_i H_{\rho_i}(D^Y) + \sum_i P_i H_{\rho_i}(D^Z)] \\ &\leq 2 \log N + 2 \log d \leq 2 \log Nd. \end{aligned} \tag{1.3}$$

Further note that this inequality is also valid for degenerated D^Y and D^Z, since each observable can be regarded as corresponding to a non-ideal measurement of a non-degenerated observable.

Definition 1.2 *Two non-degenerated observables are called complementary, if the distribution of one is uniform for any eigenstate of the other, and vice versa.*

Remark 1.3 *The maximum* $\log N$ *of (1.3) can only be achieved by using complementary measurements* D^Y, D^Z.

2 Sufficient Bound on the Error Rate for Unconditional Security

Theorem 2.1 *If* $h(p_e) \leq \frac{1}{2}$, *terminal* $\mathcal{X}$ *and* $\mathcal{Y}$ *can distribute a secret key using the BB84 protocol and privacy amplification/error correction.*

Proof: Assume that $\mathcal{X}$ has sent $(4+\delta)n$ qubits and n qubits were measured by $\mathcal{Y}$ in the correct basis, eliminating the check bits. We assume further that $\mathcal{Z}$ knows the position of these bits in the $(4+\delta)n$ -qubit stream (since this was publicly announced).

Hence we can reduce the observation to ρ_{key} in a finite Hilbert space of dimension $N = 2^n$, where ρ_{key} is the a priori state of the system after throwing away the check bits from ρ_{sb}, where ρ_{sb} denotes the state ρ restricted to the case that $\mathcal{X}$ and $\mathcal{Y}$ chose the same measurement basis.

W.l.o.g. let $\rho_{key} = \sum_{k^n \in \{0,1\}^n} |k^n\rangle \otimes W_{k^n}$, i.e. $\mathcal{X}$ has encoded the full key in the X-basis. and $\mathcal{Y}$ has used the product observable $D^Y = (\sigma_{x^n})_{x^n \in \mathcal{X}^n}$ for his measurement with $\sigma_{x^n} \triangleq \sigma_{x_1} \otimes \cdots \otimes \sigma_{x_n}$.

From (1.3) we have

$$I_{\rho_{key}}(X \wedge \sigma_{x^n}) + I_{\rho_{key}}(X \wedge Z) \leq 2 \log N d. \tag{2.1}$$

Using remark 1.3 the (maximal) upper bound $\log N$ can be achieved by using the complementary measurement to σ_{x^n} : $D^Z = (\sigma_{z^n})_{z^n \in \mathcal{Z}^n}$. Thus $d = 2^{-n/2}$ and (2.1) becomes

$$\frac{1}{n} I_{\rho_{key}}(X \wedge \sigma_{x^n}) + \frac{1}{n} I_{\rho_{key}}(X \wedge \sigma_{z^n}) \leq 1. \tag{2.2}$$

From corollary III.2.3 we deduce for the case that a secret key is achievable with positive rate

$$I_{\rho_{key}}(X \wedge \sigma_{x^n}) > \frac{n}{2}.$$

Since $\frac{1}{n} I_{\rho_{key}}(X \wedge \sigma_{x^n}) = h(p_e)$, the result follows.

■

Thus for $p_e \geq 0.11$ there might be a protocol, such that terminal $\mathcal{Z}$ can gain information $I_{\rho_{sb}}(X \wedge Z) > 0$ using a special measurement Z. Hence $\mathcal{Z}$ may gain information over the key. This bound was already shown by Shor and Preskill [34] using another proof. For $p_e \geq 0.15$ there are special known protocols such that $\mathcal{Z}$ gains information about the key distributed between $\mathcal{X}$ and $\mathcal{Y}$.

Chapter V

List of Notations

$\mathcal{A},\ \mathcal{B}, \ldots$	Finite sets
$\mathfrak{X}, \mathfrak{Y}, \ldots$	$\mathbb{C}^*-$algebras/*-subalgebras
$\mathcal{H}$	Finite Hilbert space
ρ	State (as $\mathbb{C}$-linear functional or density operator)
$\hat{\rho}$	Density operator
$\mathfrak{S}(\mathfrak{X})$	Convex set of states in $\mathfrak{X}$
$\phi : \mathfrak{X} \to \mathfrak{Y}$	Quantum operation/completely positive map
$M : \mathfrak{X} \to \mathfrak{Y}$	Positive operator valued measure with values in an commutative $\mathfrak{Y}$
W_{x^n}	A tensor product of states $W_{x_1} \otimes \cdots \otimes W_{x_n}$
$\mathfrak{X} \otimes \mathfrak{Y}$	Tensor product of subalgebras $\mathfrak{X}$ and $\mathfrak{Y}$
Tr	Trace function
$H(\rho)$	von Neumann entropy of the state ρ
$H(\mathfrak{X}),\ H_\rho(\mathfrak{X})$	von Neumann entropy of a state ρ reduced to the $*-$ (sub)algebra $\mathfrak{X}$
$H(X),\ H_\rho(X)$	von Neuman entropy of a state ρ with respect to the observable X (giving a probability distribution)
$I(\mathfrak{X} \wedge \mathfrak{Y}),\ I_\rho(\mathfrak{X} \wedge \mathfrak{Y})$	I-divergence over $*-$ (sub)algebras $\mathfrak{X}, \mathfrak{Y}$ with respect to an underlying state ρ
$I(X \wedge Y),\ I_\rho(X \wedge Y)$	I-divergence with respect to the observables X, Y with respect to an underlying state ρ

Bibliography

[1] Ahlswede, R., An elementary proof of the strong converse theorem for the multiple-access channel, J. Combin. Inform. System Sci., Vol. 7, No. 3, pp. 216-230, 1982.

[2] Ahlswede, R., and Csiszar, I., Common randomness in information theory and cryptography - part I: Secret sharing, IEEE Trans. Inform. Theory, Vol. 39, No. 4, pp. 1121-1132, 1993.

[3] Ahlswede, R., and Csiszar, I., Common randomness in information theory and cryptograpy - part II: CR Capacity, IEEE Trans. Inform. Theory, Vol. 44, No. 1, 1998, pp. 225-240, 1998.

[4] Ahlswede, R., and Körner, On common information and related characteristics of correlated information sources, presented at the 7th Prague Conf. on Inf. Th., Stat. Dec. Fct's and Rand. Proc., 1974, included in [15].

[5] Ahlswede, R., Gacs, P., and Körner, J., Bounds on conditional probabilities with applications in multi-user communication, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete, Vol. 34, No. 2, pp. 157-177, 1976.

[6] Ahlswede, R., and Körner, Source coding with side information and a converse for degraded broadcast channels, IEEE Trans. Inf. Theory, Vol. IT-21, pp. 629-637, 1975.

[7] Arveson, W., *An invitation to C^* -algebras*, New York, Heidelberg, 1976.

[8] Bell, J., On the Einstein-Podolsky-Rosen paradox., Physics, Vol. 1, No. 3, pp. 195-200, 1964.

[9] Bennett, C.H., and Brassard, G., Quantum cryptography: Public key distribution and coin tossing, Proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, New York, pp. 175-179, 1984.

[10] Bergmans, P.P., Random coding theorems for broadcast channels with degraded components, IEEE Inform. Trans., Vol. 19, No. 2, pp. 197-207, 1973.

[11] Born, M., Zur Quantenmechanik der Stossvorgänge, Zeitschrift für Physik, Vol. 37, pp. 863-867, 1926.

[12] Cai, N., and Yeung, R.W., Quantum privacy and quantum wiretap channels, to be published, 2002.

[13] Chuang, I.L., and Nielsen, M.A. *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.

[14] Cover, T.M., Broadcast channels, IEEE Inform. Trans., Vol. 18, pp. 2-14, 1972.

[15] Csiszar, I., and Körner, J., *Information theory: Coding theorems for discrete memoryless channels*, New York, Academic Press, 1981.

[16] Csiszar, I., and Körner, J., Broadcast channels with confidential messages, IEEE Trans. Inform. Theory, Vol. 24, No. 3, pp. 339-348, 1978.

[17] Dueck, G., The strong converse to the coding theorem for the multiple-access channel, J. Combin. Inform. System Sci., Vol. 6, No. 3, pp. 187-196, 1981.

[18] Einstein, A., Podolsky, B., and Rosen, N., Can quantum-mechanical description of physical reality be considered complete?, Physical Review, Vol. 47, pp. 777-780, 1935.

[19] Forney, G.D., unpublished Master thesis, MIT, Boston, 1963.

[20] Gordon, J.P., Noise at optical frequencies: information theory, Proc. Int. School Phys. "Enrico Fermi" (P.A. Miles, ed.), Academic Press, New York, pp. 156-181, 1964.

[21] Hausladen, P., Josza, R, Schuhmacher, B., Westmoreland, M, and Wootters, W.K., Classical information capacity of a quantum channel, Phys. Rev. A, Vol. 54, No. 3, pp. 1869-1876, 1997.

[22] Holevo, A. S., Information-theoretical aspects of quantum measurement, Prob. Inf. Transm., Vol. 9, No. 2, pp. 110-118, 1973.

[23] Holevo, A. S., Bounds for the quantity of information transmitted by a quantum channel, Prob. Inf. Transm., Vol. 9, No. 3, pp. 177-183, 1973.

[24] Holevo, A.S., Capacity of a quantum communication channel, Probl. Inf. Transm., Vol. 15, No. 4, pp. 247-253, 1979.

[25] Holevo, A. S., The capacity of the quantum channel with general signal states, IEEE Trans. Inform. Theory, Vol. 44, No. 1, pp. 269-273, 1998.

[26] Levitin, L. B., On quantum measure of information, Proc. IV All-Union Conference on Information Transmission and Coding Theory, Tashkent, pp. 111-115, 1969.

[27] Lo, H., and Chau, H.F., Unconditional security of quantum key distibution over arbitrary long distances, Science, Vol. 283, pp. 2050-2056, 1999.

[28] Mayers, D., Unconditional security in quantum crypthography, arXive e-print quant-ph/9802025, 1998.

[29] Ohya, M., and Petz, D., *Quantum entropy and its use*, Springer, Berin, 1993.

[30] Peres, A., *Quantum theory: Concepts and methods*, Kluwer, Dordrecht, 1995.

[31] Schumacher, B., Quantum coding, Physical Review A, Vol. 51, No. 4, pp. 2738-2747, 1995.

[32] Schumacher, B., and Westmoreland, M.D., Sending classical information via noisy quantum channels, Phys. Rev. A, Vol. 56, No. 1, pp. 131-138, 1997.

[33] Shannon, C.E., A mathematical theory of communication, Bell System Technical Journal, Vol. 27, pp. 379-423, 1948.

[34] Shor, P., Algorithms for quantum computation: Discrete logarithm and factoring, In Proc. 35th Ann. Symp. Foundations of Computer Sience (S. Goldwasser, ed.), IEEE Press, Santa Fe, pp. 124-134, 1994, or Polynomial-time algoithms for prime factorization and discrete logarithms on a quantum computer, SIAM J., Computing, Vol. 26, No. 5, pp. 1484-1509, 1997.

[35] Shor, P., and Preskill, J., Simple proof of security of the BB84 quantum key distibution protocol, Phys. Rev. Lett., Vol.85, pp. 441-444, 2000.

[36] Umegaki, H., Conditional expectations in an operator algebra, IV (entropy and information), Kodai Math. Sem. Rep., Vol. 14, pp. 59-85, 1962.

[37] Maassen, H., and Uffink, J.B.M., Generalized entropic uncertainty relations, Phys. Rev. Lett., Vol. 60, pp. 1103-1106, 1988.

[38] Maurer, U., Unconditionally secure key agreement and the intrinsic conditional information, IEEE Trans. Inform. Theory, Vol. 45, No. 2, pp. 499-514, 1999.

[39] von Neumann, J., Thermodynamik quantenmechanischer Gesamtheiten, Nachr. der Gesellschaft der Wiss. Gött., pp. 273-291, 1927.

[40] Wehrl, A., General properties of entropy, Review Mordern Physics, Vol. 50, No. 2, pp. 221-260, 1978.

[41] Winter, A., Languages of quantum information theory, Preprint E98-009, Sonderforschungsbereich 343 "Diskrete Strukturen in der Mathematik", Universität Bielefeld, 1998, or arXive e-print quant-ph/9807008.

[42] Winter, A., Coding Theorems of Quantum Information Theory, Dissertation Uni Bielefeld, arXive e-print quant-ph/9907077, 1999.

[43] Winter, A., Coding theorem and strong converse for quantum channels, IEEE Trans. Inform. Theorey, Vol. 45, No. 7, p. 2481-2485, 1999.

[44] Winter, A., The capacity of the quantum multiple-access channel, IEEE Trans. Inform. Theory, Vol. 47, No. 7, pp. 3059-3065, 2001.

[45] Wolfowitz, J., *Coding theorems of information theory*, Springer, Berlin, second edition, 1964.

[46] Wootters, W.K., and Zurek, W.H., A single quantum cannot be cloned, Nature, Vol. 299, pp. 802-803, 1982.