Ann. Henri Poincaré 2 (2001) 1 – 26

1424-0637/01/010001-26 \$ 1.50+0.20/0

Annales Henri Poincaré

The Rate of Optimal Purification Procedures

M. Keyl, R. F. Werner

Abstract. Purification is a process in which decoherence is partially reversed by using several input systems which have been subject to the same noise. The purity of the outputs generally increases with the number of input systems, and decreases with the number of required output systems. We construct the optimal quantum operations for this task, and discuss their asymptotic behaviour as the number of inputs goes to infinity. The rate at which output systems may be generated depends crucially on the type of purity requirement. If one tests the purity of the output systems one at a time, the rate is infinite : this fidelity may be made to approach 1, while at the same time the number of outputs goes to infinity arbitrarily fast. On the other hand, if one also requires the correlations between outputs to decrease, the rate is zero: if fidelity with the pure product state is to go to 1, the number of outputs per input goes to zero. However, if only a fidelity close to 1 is required, the optimal purifier achieves a positive rate, which we compute.

1 Introduction

A central problem of quantum information processing is to ensure that devices which have been designed to perform certain tasks still work well in the presence of decoherence, i.e., under the combined influences of inaccurate specifications, interaction with further degrees of freedom, and thermal noise. Decoherence typically has the effect of producing mixed states out of pure states, so it is natural to ask whether the effects of decoherence can be partially undone, by processes turning mixed states into purer ones. As in the classical case this is impossible for operations working on single systems. However, if many (say N) systems are available, all of which were originally prepared in the same unknown pure state σ, and subsequently exposed to the same (known) decohering process R_*, then an analysis of the combined state may well allow the reconstruction of the original pure state. The quality of this reconstruction will increase with N. In fact, it should approach perfection as $N \to \infty$: in this limit one can determine the decohered state $R_*\sigma$ to an arbitrary accuracy by statistical measurements. The question is only, whether the knowledge of the full density matrix $R_*\sigma$ admits the reconstruction of σ, i.e., whether the linear operator R_* is invertible. Generically, and for sufficiently small decoherence, this is the case. However, the operator R_*^{-1} is usually not positive, i.e., it takes some density matrices into operators with negative eigenvalues. Therefore, it does not correspond to a physically realizable apparatus. But it does describe a computation we can perform to reconstruct σ from the measured (or estimated) density matrix $\rho = R_*\sigma$.

How well can this reversal of decoherence be done when the number N of inputs is given, and finite? The answer depends critically on the way the purification task is set up, and what "figure of merit" we try to optimize. In general, the resulting variational problems may be very hard to solve. However, in the specific model situation chosen in this paper, the solution is fairly straightforward: we take qubit systems, and assume that decoherence is described by a depolarizing channel of the form

$$R_* \sigma = \lambda \sigma + (1 - \lambda) \frac{\mathbb{1}}{2}. \tag{1}$$

The purifier will be a device T taking a state of N qubits, and turning out some number M of qubits, where M may be either fixed or itself a random quantity. In the latter case T is given mathematically by a family T_M of completely positive maps, where T_M takes a density matrix of N qubit systems, and produces a positive operator on the M qubit space, which is not necessarily normalized to unity: the normalization constant $w_M = \mathrm{tr}(T_M(\rho))$ is interpreted as the probability of getting exactly M outputs from the input state ρ. Thus $\sum_M w_M = 1$.

Our aim is to design T to get outputs as close as possible to the uncorrupted input state σ, and also as many of them as possible. This is reminiscent of cloning problems [1, 2]. However, in cloning problems the aim is to get many copies of the input state to T, which in our case is the mixed state $R_* \sigma$, rather than the pure state σ. In both cases there is clearly a trade-off between the quality of the outputs and their number, which is why there are several different ways to state the problem. In the sequel we will briefly describe the variants of the purification problem, together with the results, which will be shown later in the paper.

1. *Maximal fidelity, failure to produce any output admissible.* The best fidelity of outputs is clearly achieved, when the weakest possible demands are made on the number of outputs. In this case we do not even insist on an output every time the device is run, but only on some non-zero probability for getting an output. The best achievable fidelity of these outputs goes to 1 as $N \to \infty$, but not substantially faster than with the following stronger requirement on output numbers.

2. *$M = 1$ fixed, number M never increased at expense of output purity.* This is the approach taken by [3]. At least one output qubit is required, and the figure of merit is based on the fidelity of this one qubit. As it turns out the optimal device for this problem can just as well produce more outputs of the same optimal fidelity, with a certain rate. However, this rate is not part of the optimization criterion.

3. *M fixed, purity measured by one-particle restrictions.* For fixed M, N, this problem is rather similar to 2. However, with the additional parameter M we can discuss better the trade-off between rate and quality of outputs. Suppose we fix some dependence of the number of outputs $M(N)$ on the number of

inputs. Do the states still approach σ as $N \to \infty$? Clearly, if $M(N)$ increases slowly, e.g., at the rate given by the optimal device from 2, this will be the case. What may seem surprising at first, however, is that *no matter* how fast $M(N) \to \infty$, the state of each output qubit still approaches the uncorrupted pure state. In this sense, optimal purification works with an *infinite rate*.

4. *M fixed, purity measured by fidelity with respect to $\sigma^{\otimes N}$.* The infinite rate depends critically on what we use as the quality criterion for outputs. Apart from the fidelity of the restrictions of the output state to single qubits used in 3 we could also look at the fidelity of the outputs with respect to the M particle pure state $\sigma^{\otimes M}$, thereby taking into account also the correlations between different outputs. For fixed M, the difference between these two fidelity measures does not seem so great, because one can be estimated in terms of the other. However, the estimates are M-dependent (see below), and hence for problems involving a limit $M \to \infty$ the fidelity with respect to the combined state may (and does) turn out to be a much tighter criterion. In fact, no process with finite rate M/N achieves fidelity$\to 1$, and in this sense even optimal purification works with *zero rate*, in sharp contrast to 3 above. On the other hand, for any finite fidelity requirement, there is an output rate for an optimized process, which is computed below.

These results will be stated in precise terms in the following Section 2, together with the notation needed for that purpose, and graphs of the optimal fidelities and rates. The proofs follow in the subsequent sections. Technically they hinge on the decomposition theory of tensor product representations of SU(2), and this background is provided in Section 3. The reason for representation theory to enter in such a crucial way is isolated in Section 3.1, where it is shown that the optimal devices can be taken to be SU(2)-covariant (do not single out a basis in the qubit space). The two basic purifiers, called the "natural purifier" (optimal for question 2 above), and the "optimal purifier" (optimal for question 3 above) are defined in Section 4, and their fidelities are computed. The proof of the optimality claims is given in Section 5. Finally, in Section 6, we determine the asymptotic behaviour for the optimal purifier, and the output rates.

2 Figures of Merit and Main Results

In this section we will state the optimization problems for purifiers mathematically. A device (not necessarily a purification procedure) taking N qubit systems as input and producing M output qubits is described mathematically by a trace preserving, completely positive linear map ("cp-map")

$$T_* : \mathcal{B}_*(\mathcal{H}^{\otimes N}) \to \mathcal{B}_*(\mathcal{H}^{\otimes M}),$$

which takes input density matrices to output density matrices. Equivalently, we may work in the Heisenberg picture, using the dual T of T_*, the *unital* (i.e. $T(\mathbb{1}) =$

$\mathbb{1}$) cp-map

$$T : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}^{\otimes N}),$$

which is related to T_* by $\mathrm{tr}\big(T(X)\rho\big) = \mathrm{tr}\big(XT_*(\rho)\big)$. Here $\mathcal{H} = \mathbb{C}^2$ is the one qubit Hilbert space, $\mathcal{B}(\,\cdot\,)$ is the space of all (bounded) operators on the corresponding Hilbert space and $\mathcal{B}_*(\,\cdot\,)$ denotes the space of trace class operators. Since $\dim \mathcal{H} = 2 < \infty$, the spaces $\mathcal{B}_*(\mathcal{H})$ and $\mathcal{B}(\mathcal{H})$ are just the 2×2-matrices, but it is nevertheless helpful to keep track of the distinction between spaces of observables and spaces of states.

"Good purifiers" should make $T_*((R_*\sigma)^{\otimes N})$ very close to $\sigma^{\otimes M}$. A simple figure of merit is the fidelity of the output with respect to the desired state in the worst case, i.e.,

$$\mathcal{F}_{\mathrm{all}}(T) = \inf_{\sigma} \mathrm{tr}\left(\sigma^{\otimes M} T_*\big((R_*\sigma)^{\otimes N}\big)\right), \tag{2}$$

where the infimum is over all one-particle pure states σ. Similarly, we could pick any one of the outputs, say the one with number i, $1 \leq i \leq M$, and test its fidelity. The worst case then gives the fidelity

$$\mathcal{F}_{\mathrm{one}}(T) = \inf_{i} \; \inf_{\sigma} \mathrm{tr}\left(\sigma^{(i)} T_*\big((R_*\sigma)^{\otimes N}\big)\right), \tag{3}$$

where $\sigma^{(i)} = \mathbb{1} \otimes \cdots \otimes \sigma \otimes \cdots \otimes \mathbb{1}$ denotes the tensor products with $(M-1)$ factors "$\mathbb{1}$" and one factor σ at the i^{th} position. We seek to maximize these numbers by judicious choice of T. Let us denote the optimal values by

$$\mathcal{F}_{\sharp}^{\max}(N, M) = \sup_{T} \; \mathcal{F}_{\sharp}(T), \tag{4}$$

where $\sharp$="all" or $\sharp$="one", and the supremum is over all unital cp-maps T with the specified number of inputs and outputs.

For devices with *variable numbers of outputs* all these quantities become random variables, as well. Typically, one will seek to optimize the mean fidelity. It is then natural not to take the infimum in Equation (3), but the mean. The case where no output is produced at all, is interpreted here as one output qubit in the completely mixed state. The resulting *mean fidelity* [3] can be thought of as the fidelity $\mathcal{F}_{\mathrm{one}}(\widetilde{T})$ of a modified device $\widetilde{T}$, which uses T, followed by a random selection of one of the outputs. Therefore, the problem of maximizing mean fidelity is exactly the same as maximizing $\mathcal{F}_{\mathrm{one}}(T)$ for devices with fixed output number $M = 1$, with optimal value $\mathcal{F}_{\sharp}^{\max}(N, M)$.

Rather than looking at the mean of the fidelity distribution of a device with variable number of outputs we could also look at its maximum. This corresponds to the problem in item 1 of the previous section. More precisely, one should omit the "worst case" infimum with respect to i in this case, and allow the device to either pick one of its outputs, or to declare failure. This leads to a device with only the two output numbers 0 and 1, and the functional to be optimized is the fidelity of the "1"-output. We will denote the optimum for this problem by $\mathcal{F}^{\max}_{\sharp}(N,0)$, with a slight abuse of notation expressing that this is the case with no demands on output numbers at all.

It is clear that $\mathcal{F}^{\max}_{\sharp}(N,M)$ is a decreasing function of M, and that therefore the limit

$$\mathcal{F}^{\max}_{\sharp}(N,\infty) = \lim_{M\to\infty} \mathcal{F}^{\max}_{\sharp}(N,M) \tag{5}$$

exists. For $\sharp$=all, this limit is zero. However, for $\sharp$=one, it is an interesting quantity, which even goes to 1 as $N \to \infty$.

The results for the quantities $\mathcal{F}^{\max}_{\text{one}}(N,0)$, $\mathcal{F}^{\max}_{\text{one}}(N,1)$, and $\mathcal{F}^{\max}_{\text{one}}(N,\infty)$ are shown in Figure 1. Of course, all these quantities also depend on the parameter describing the noise, which we have suppressed for notational convenience. It is fixed in the following graphs as $\lambda = 0.5$ (resp. $\beta = 0.549$, see Section 3). It is clear that $\mathcal{F}^{\max}_{\sharp}(N,M) \to 1$ for any N and M, as the noise level goes to zero ($\lambda \to 1$).

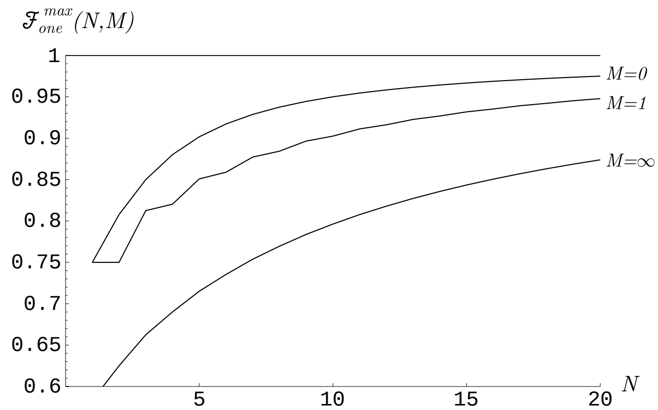

Figure 1: The three basic fidelities for the one-particle figure of merit: top: $\mathcal{F}^{\max}_{\text{one}}(N,0)$, middle: $\mathcal{F}^{\max}_{\text{one}}(N,1)$, bottom: $\mathcal{F}^{\max}_{\text{one}}(N,\infty)$

The leading asymptotic behaviour (as $N \to \infty$) is of the form

$$\mathcal{F}^{\max}_{\text{one}}(N,M) \propto 1 - \frac{c_M}{2N} + \cdots \tag{6}$$

$$c_0 = (1-\lambda)/\lambda \tag{7}$$

$$c_1 = (1-\lambda)/\lambda^2 \tag{8}$$

$$c_\infty = (\lambda+1)/\lambda^2. \tag{9}$$

From these asymptotic results, a simple estimate for the all-particle fidelity criteria can be obtained: By Equation (41), $1 - \mathcal{F}_{\text{all}}(T) \leq M(1 - \mathcal{F}_{\text{one}}(T))$, where

M is the number of outputs. Hence, for sufficiently small rate M/N one achieves good fidelity, even for the all-particle test criterion: $1 - \mathcal{F}_{\text{all}}^{\max}(N, M) \leq M(1 - \mathcal{F}_{\text{one}}^{\max}(N, M)) \leq M(1 - \mathcal{F}_{\text{one}}^{\max}(N, \infty)) \approx \frac{M}{2N} c_\infty$. Of course, the second estimate is rather crude, and a refined version will be given in Section 6. The argument does show, however, that one may expect optimal all-particle fidelity to become a function of the output rate. This function will be computed in Section 6.3: for every $\mu > 0$, we find the limit

$$\Phi(\mu) = \lim_{\substack{N\to\infty \\ M/N\to\mu}} \mathcal{F}_{\text{all}}^{\max}(N, M) = \begin{cases} \dfrac{2\lambda^2}{2\lambda^2 + \mu(1-\lambda)} & \text{if } \mu \leq \lambda \\ \dfrac{2\lambda^2}{\mu(1+\lambda)} & \text{if } \mu \geq \lambda. \end{cases} \tag{10}$$

The function Φ is continuous and satisfies $\Phi(0) = 1$ and $\Phi(\infty) = 0$, so at small rates purification is near perfect, but becomes arbitrarily bad at too high rates. In Figure 2 Φ is plotted with the noise parameter λ going in steps of 0.1 from 0 to 1. The dotted line describes the performance of the natural purifier (see Section 4.1), which operates with rate $\mu = \lambda$.

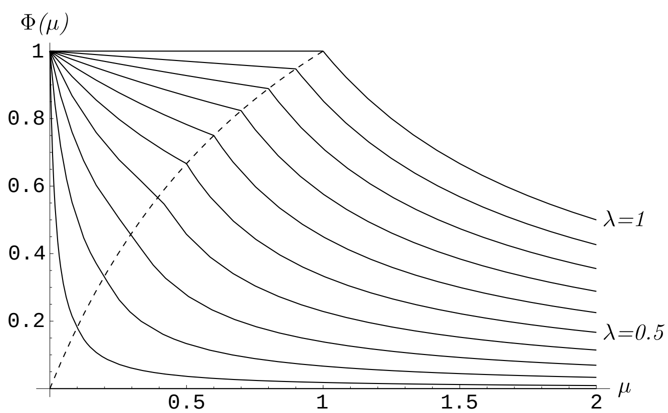

Figure 2: Asymptotic fidelity $\Phi(\mu)$ for the all-particle figure of merit (10). Curve parameter: $\lambda = .1, .2, ..., 1$; dotted line: natural purifier

3 Decomposition theory

Many arguments in this paper are based on group theory, in particular the decomposition of tensor products of irreducible representations of SU(2). In this section we will summarize the relevant results which are needed throughout the paper.

3.1 Reduction to fully symmetric case

There are two reason why group theory is useful for us. First of all the depolarizing channel R producing the noise is "covariant" which means that it does not prefer any particular polarization direction (basis in the underlying Hilbert space $\mathcal{H} = \mathbb{C}^2$), and second we are looking at a "universal" purification problem, i.e. the purification devices T we are looking for should work well on an arbitrary unknown input state σ. Therefore, it is natural to look at those T which are covariant as well: T should work in exactly the same way on any input. Carrying this idea further it should also be impossible to single out any one of the input and output channels. Mathematically, these "natural conditions" are stated as follows:

Definition 3.1. *A unital, cp-map $T : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}^{\otimes N})$ is called* fully symmetric *if it is* $\mathrm{U}(2)$ *covariant, i.e.*

$$T(U^{\otimes M} A U^{*\otimes M}) = U^{\otimes N} T(A) U^{*\otimes N} \quad \forall A \in \mathcal{B}(\mathcal{H}^{\otimes M})\ \forall U \in \mathrm{U}(2)$$

and permutation invariant, i.e.

$$T(\eta A \eta^*) = T(A) \quad \forall \eta \in \mathrm{S}_M\ \ \forall A \in \mathcal{B}(\mathcal{H}^{\otimes M})$$

and

$$\tau T(A) \tau^* = T(A) \quad \forall \tau \in \mathrm{S}_N\ \ \forall A \in \mathcal{B}(\mathcal{H}^{\otimes N}).$$

Here $\eta \in \mathrm{S}_M$, $\tau \in \mathrm{S}_N$ denote permutations of M respectively N elements and at the same time the corresponding unitaries on $\mathcal{B}(\mathcal{H}^{\otimes M})$ and $\mathcal{B}(\mathcal{H}^{\otimes N})$, i.e. $\eta(\psi_1 \otimes \cdots \otimes \psi_M) = \psi_{\eta(1)} \otimes \cdots \otimes \psi_{\eta(M)}$.

We could have made this condition part of our definition of a purifier, and restricted the discussion to fully symmetric operations from the outset. However, we have chosen to take the heuristic arguments at the beginning of this section more seriously: the kind of "universality" described there is already embodied in the figures of merit of Section 2, so it becomes a mathematical question whether optimal purifiers are indeed fully symmetric or else symmetry is broken, and a non-symmetric purifier can outperform all symmetric ones.

We now argue that the *optimal* devices (with respect to $\mathcal{F}_{\mathrm{one}}$ and $\mathcal{F}_{\mathrm{all}}$) may be indeed assumed to be fully symmetric. To make this precise, note that $\mathcal{F}_{\mathrm{all}}(T)$ and $\mathcal{F}_{\mathrm{one}}(T)$ are infima over expressions which are linear in T, and hence concave functionals. Therefore, averaging over many T's with the same figure of merit produces a T at least as good. Clearly, for all permutations $\eta \in \mathrm{S}_M$, $\tau \in \mathrm{S}_N$ and $U \in \mathrm{U}(2)$, the purifier $T'(X) = \tau U^{\otimes N} T(\eta U^{*\otimes M} X U^{\otimes M} \eta^*) U^{*\otimes N} \tau^*$ has the same figure of merit as T. By averaging over these parameters (with respect to the appropriate Haar measures) we thus find a purifier, which is at least as good as T and, in addition, fully symmetric. Similar arguments apply for purifiers with variable numbers of outputs (although one has to be more careful in defining figures of merit). Therefore, we will restrict our discussion to fully symmetric purifiers from now on.

3.2 Decomposition of tensor products

The reduction to fully symmetric purifiers allows the application of techniques from group theory (especially representation theory of SU(2)) which simplifies our problems significantly. Consider in particular the $N-$fold tensor product

$$\mathrm{SU}(2) \ni U \mapsto \pi_{1/2}(U)^{\otimes N} = U^{\otimes N} \in \mathcal{B}(\mathcal{H}^{\otimes N}),$$

of the spin-1/2, or the "defining" representation $\mathrm{SU}(2) \ni U \mapsto \pi_{1/2}(U) = U \in \mathcal{B}(\mathcal{H})$. It decomposes into a direct sum of irreducible subrepresentations

$$\pi_{1/2}(U)^{\otimes N} = U^{\otimes N} = \bigoplus_{s \in I[N]} \pi_s(U) \otimes \mathbb{1} \tag{11}$$

with

$$\pi_s(U) \otimes \mathbb{1} \in \mathcal{B}(\mathcal{H}_s \otimes \mathcal{K}_{N,s}) \text{ and } \mathcal{H}^{\otimes N} = \bigoplus_{s \in I[N]} \mathcal{H}_s \otimes \mathcal{K}_{N,s}$$

and

$$I[N] = \begin{cases} \{0, 1, \dots, \frac{N}{2}\} & N \text{ even} \\ \{\frac{1}{2}, \frac{3}{2} \dots, \frac{N}{2}\} & N \text{ odd} \end{cases}$$

Here π_s denotes the spin-s irreducible representation of SU(2), $\mathcal{H}_s$ its $2s+1$-dimensional representation space, which we will identify in the following with the symmetric tensor-product $\mathcal{H}_+^{\otimes 2s}$, i.e. the $2s$–qubits Bose subspace, and $\mathcal{K}_{N,s}$ denotes a multiplicity space, which carries an appropriate representation of the symmetric group S_N.

3.3 Decomposition of states

Consider now a general qubit density matrix ρ, which in its eigenbasis can be written as ($\beta \geq 0$)

$$\begin{aligned} \rho(\beta) &= \frac{1}{2\cosh(\beta)} \exp\left(2\beta \frac{\sigma_3}{2}\right) = \frac{1}{e^{\beta} + e^{-\beta}} \begin{pmatrix} e^{\beta} & 0 \\ 0 & e^{-\beta} \end{pmatrix} \\ &= \tanh(\beta) |\psi\rangle\langle\psi| + (1 - \tanh(\beta)) \frac{1}{2} \mathbb{1}, \quad \psi = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{aligned} \tag{12}$$

The parametrization of ρ in terms of the "pseudo-temperature" β is chosen here, because it is, as we will see soon, very useful for calculations. The relation to the form of $\rho = R_* \sigma$ initially given in Equation (1) is obviously

$$\lambda = \tanh(\beta).$$

The N–fold tensor product $\rho^{\otimes N}$ can be expressed as

$$\rho(\beta)^{\otimes N} = (2\cosh(\beta))^{-N} \exp(2\beta L_3)$$

where

$$\mathcal{B}(\mathcal{H}^{\otimes N}) \ni L_3 = \frac{1}{2}\Big(\sigma_3 \otimes \mathbb{1}^{\otimes(N-1)} + \cdots + \mathbb{1}^{\otimes(N-1)} \otimes \sigma_3\Big). \tag{13}$$

denotes the 3–component of angular momentum in the representation $\pi_{1/2}^{\otimes N}$. In other words, the density matrices are just analytic continuations of group unitaries, or "SU(2)-rotations by an imaginary angle $2i\beta$". This reduces the decomposition of $\rho(\beta)^{\otimes N}$ to the decomposition (11) of the tensor product representation. Of course, analytically continued group elements are not normalized as density operators. Extracting appropriate normalization factors the decomposition becomes

$$\rho(\beta)^{\otimes N} = \bigoplus_{s \in I[N]} w_N(s)\rho_s(\beta) \otimes \frac{\mathbb{1}}{\dim \mathcal{K}_{N,s}},$$

with

$$w_N(s) = \frac{\sinh\big((2s+1)\beta\big)}{\sinh(\beta)(2\cosh(\beta))^N} \dim \mathcal{K}_{N,s}, \tag{14}$$

and

$$\rho_s(\beta) = \frac{\sinh(\beta)}{\sinh\big((2s+1)\beta\big)} \exp(2\beta L_3^{(s)}).$$

Here $L_3^{(s)}$ denotes again the 3–component of angular momentum, now in the representation π_s.

The $\rho_s(\beta)$ are normalized, i.e. $\operatorname{tr} \rho_s(\beta) = 1$. Hence $\sum_s w_N(s) = 1$ and $0 \leq w_N(s) \leq 1$ due to the normalization of $\rho(\beta)^{\otimes N}$. Together with the fact that the multiplicities $\dim \mathcal{K}_{N,s}$ are independent of β we can extract from Equation (14) a generating functional for $\dim \mathcal{K}_{N,s}$:

$$\begin{aligned} 2\sinh(\beta)(2\cosh(\beta))^N &= 2 \sum_{s \in I[N]} \sinh\big((2s+1)\beta\big) \dim \mathcal{K}_{N,s} \\ = \big(e^{\beta} - e^{-\beta}\big)\big(e^{\beta} + e^{-\beta}\big)^N &= \sum_{s \in I[N]} \Big(e^{(2s+1)\beta} - e^{-(2s+1)\beta}\Big) \dim \mathcal{K}_{N,s}, \end{aligned}$$

obtaining

$$\dim \mathcal{K}_{N,s} = \frac{2s+1}{N/2+s+1} \binom{N}{N/2-s}$$

provided $N/2 - s$ is integer, and zero otherwise. The same result can be derived using representation theory of the symmetric group; see [4], where the more general case $\dim \mathcal{H} = d \in \mathbb{N}$ is studied.

3.4 Decomposition of operations and optimal cloning

Let us come back now to fully symmetric cp-maps $T : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}^{\otimes N})$. Using the results of Subsection 3.2 it is easy to see that T can be decomposed into a direct sum

$$T(A) = \bigoplus_{s \in I[N]} T_s(A) \otimes \mathbb{1} \tag{15}$$

where the $T_s : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}_s)$ are unital cp-maps which are again fully symmetric (using an obvious modification of Definition 3.1). Identifying, as in Subsection 3.2, the representation space $\mathcal{H}_s$ with the $2s$–fold symmetric tensor product $\mathcal{H}_+^{\otimes 2s}$, leads to the significantly simpler problem of decomposing fully symmetric, unital cp-maps $Q : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$, which is already solved in [2]. Hence we will state only the corresponding results here. In particular we have the following theorem:

Theorem 3.1. *Consider again the 3-components of angular momentum L_3 and $L_3^{(s)}$ in the representations $\pi_{1/2}^{\otimes M}$ respectively π_s (cf. Subsection 3.3).*

1. *For each fully symmetric cp-map $Q : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}_+^{\otimes 2s})$ there is a constant $\omega(Q) \in \mathbb{R}^+$ with $Q(L_3) = \omega(Q) L_3^{(s)}$.*

2. *For each $2s \in \mathbb{N}_0$ there is exactly one fully symmetric $\hat{Q}_{2s}$ with*

$$\omega(\hat{Q}_{2s}) = \max_Q \omega(Q) = \begin{cases} \dfrac{M}{2s} & \text{for } 2s \geq M \\ \dfrac{M+2}{2s+2} & \text{for } 2s < M, \end{cases} \tag{16}$$

   where the maximum is taken over the set of all fully symmetric cp-maps $Q : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}_+^{\otimes 2s})$.

3. *If $M > 2s$ holds $\hat{Q}_{2s}$ is given in terms of its pre-dual $\hat{Q}_{2s*} : \mathcal{B}_*(\mathcal{H}_+^{\otimes 2s}) \to \mathcal{B}_*(\mathcal{H}^{\otimes M})$ by*

$$\hat{Q}_{2s*}(\theta) = \frac{2s+1}{M+1} S_M(\theta \otimes \mathbb{1}^{\otimes(M-2s)}) S_M \tag{17}$$

   where S_M is the projector from $\mathcal{H}^{\otimes M}$ onto the Bose subspace $\mathcal{H}_+^{\otimes M}$.

4. *For $M \leq 2s$ the map $\hat{Q}_{2s}$ is given by*

$$\hat{Q}_{2s}(A) = S_{2s}(A \otimes \mathbb{1}^{\otimes(2s-M)}) S_{2s},$$

   or in terms of its predual

$$\hat{Q}_{2s*}(\theta) = \operatorname{tr}_{2s-M} \theta, \tag{18}$$

   where tr_{2s-M} denotes the partial trace over the first $2s - M$ tensor factors.

Note that the family of cp-maps $\hat{Q}_{2s}$ defined in Equation (17) respectively (18) plays a very special role not only mathematically: $\hat{Q}_{2s}$ describes the optimal way to *increase* (17) or *dercrease* (18) the number of qubits. More precisely $\hat{Q}_{2s*}$ maps a finite number $2s$ of qubits in the same unknown pure state σ to the best possible approximation $Q_{2s*}(\sigma^{\otimes 2s})$ of the product state $\sigma^{\otimes M}$. The quality of $Q_{2s*}(\sigma^{\otimes 2s})$ is measured here by the fidelities

$$\mathcal{G}_{\text{all}}(Q) := \inf_{\sigma} \operatorname{tr}\left(\sigma^{\otimes M} Q_*\left(\sigma^{\otimes 2s}\right)\right)$$

or

$$\mathcal{G}_{\text{one}}(Q) := \inf_{i} \ \inf_{\sigma} \operatorname{tr}\left(\sigma^{(i)} Q_*\left(\sigma^{\otimes 2s}\right)\right).$$

If $2s \geq M$ holds (item 4) we simply have to discard $2s - M$ qubits to get exactly $\hat{Q}_{2s*}(\sigma^{\otimes 2s}) = \sigma^{\otimes M}$. If the number of qubits should be increased, i.e. $M > 2s$ holds (item 3), the target state $\sigma^{\otimes M}$ can not be reached. In this case $\hat{Q}_{2s}$ is the *optimal quantum cloning device* described in [1, 2].

4 Natural and optimal purifiers

In this section we will introduce a particular class of purification maps which arise very naturally from the group theoretical discussion of the last section and which maximize, as we will see in Section 5, the fidelities $\mathcal{F}_{\text{all}}$ and $\mathcal{F}_{\text{one}}$.

4.1 The definitions

As a first step let us reinterpret the decomposition of $\rho(\beta)^{\otimes N}$ discussed in Subsection 3.3 in terms of the of cp-map

$$\bigoplus_{s \in I[N]} \mathcal{B}(\mathcal{H}_+^{\otimes 2s}) \ni \bigoplus_{s \in I[N]} A_s =: A \mapsto T^{\text{nat}}(A) := \bigoplus_{s \in I[N]} T_s^{\text{nat}}(A_s) :=$$
$$:= \bigoplus_{s \in I[N]} A_s \otimes \mathbb{1} \in \bigoplus_{s \in I[N]} \mathcal{B}(\mathcal{H}_s \otimes \mathcal{K}_{N,s}) = \mathcal{B}(\mathcal{H}^{\otimes N}). \quad (19)$$

Its predual maps the density matrix $\rho(\beta)^{\otimes N}$ to $\bigoplus_{s \in I[N]} w_N(s)\rho_s(\beta)$. The latter should be interpreted as a (normal) state on the von Neumann algebra $\bigoplus_{s \in I[N]} \mathcal{B}(\mathcal{H}_+^{\otimes 2s})$. Hence T^{nat} is an *instrument* which produces with probability $w_N(s)$ the $2s$–qubit state $\rho_s(\beta)$ from the input state $\rho(\beta)^{\otimes N}$. This implies in particular that the number of output systems of T^{nat} is not a fixed parameter but an observable. We will see soon that the fidelities of the output states $\rho_s(\beta)$ are bigger than those of the input state $\rho(\beta)^{\otimes N}$ provided $s > 0$ holds. Hence we will call T^{nat} the *natural purifier*.

The most obvious way to construct a device which produces always the same number of output systems is the composition of T^{nat} with the cloning operation

$$\mathcal{B}(\mathcal{H}^{\otimes M}) \ni A \mapsto \hat{Q}(A) = \bigoplus_{s \in I[N]} \hat{Q}_{2s}(A) \in \bigoplus_{s \in I[N]} \mathcal{B}(\mathcal{H}_+^{\otimes 2s}).$$

Here the $\hat{Q}_{2s}$ are the operations introduced in Theorem 3.1. Combining T^{nat} with $\hat{Q}$ we get an operation

$$\mathcal{B}(\mathcal{H}^{\otimes M}) \ni A \mapsto T^{\mathrm{opt}}(A) := (T^{\mathrm{nat}}\hat{Q})(A) \in \mathcal{B}(\mathcal{H}^{\otimes N}) \tag{20}$$

which produces, as stated, a fixed number M of output systems from N input qubits. Physically we can interpret $T^{\mathrm{opt}}(A)$ in the following way: First we apply the natural purifier to the input state $\rho(\beta)^{\otimes N}$ and we get $2s$ output systems in the common state $\rho_s(\beta)$. If $2s \geq M$ we throw away $M - 2s$ qubits and end up with a number of M. If $2s < M$ we have to invoke the $2s \to M$ optimal cloner to reach the required number of M output systems. Although this cloning process is wasteful we will see soon that the fidelities $\mathcal{F}_{\#}(T^{\mathrm{opt}})$ of the output state produced by T^{opt} are even the best fidelities we can get for any $N \to M$ purifier. Hence we will call T^{opt} therefore the *optimal purifier.*

4.2 The one qubit fidelity

Now we will calculate the one qubit fidelity $\mathcal{F}_{\mathrm{one}}$. Due to covariance of the depolarizing channel R the expressions under the infima defining $\mathcal{F}_{\mathrm{one}}(T)$ (and $\mathcal{F}_{\mathrm{all}}(T)$) in Equation (2) and (3) depend for any fully symmetric purifier not on σ and i. I.e. we get with $R_*\sigma = \rho(\beta)$:

$$\mathcal{F}_{\mathrm{all}}(T) = \mathrm{tr}\left[\sigma^{\otimes M} T_*\big(\rho(\beta)^{\otimes N}\big)\right] \text{ and } \mathcal{F}_{\mathrm{one}}(T) = \mathrm{tr}\left[\sigma^{(1)} T_*\big(\rho(\beta)^{\otimes N}\big)\right] \tag{21}$$

with $\sigma = |\psi\rangle\langle\psi|$. In the case of $\mathcal{F}_{\mathrm{one}}$ the situation is further simplified by the introduction of the *black cow parameter* (cf. [1]) $\gamma(\theta)$ which is defined for each density matrix θ on $\mathcal{H}^{\otimes M}$ by

$$\gamma(\theta) = \frac{1}{M}\,\mathrm{tr}(2L_3\theta).$$

To derive the relation of γ to $\mathcal{F}_{\mathrm{one}}$ note that full symmetry of T implies equivalently to (21)

$$\mathcal{F}_{\mathrm{one}}(T) = \mathrm{tr}\left[\left(\frac{1}{M}\sum_{j=1}^{M}\sigma^{(j)}\right) T_*\big(\rho(\beta)^{\otimes N}\big)\right].$$

Since $\sigma = (\mathbb{1} + \sigma_3)/2$ holds with the Pauli matrix σ_3 we get together with the definition of L_3 in Equation (13)

$$\mathcal{F}_{\mathrm{one}}(T) = \frac{1}{2}\Big[1 + \gamma\big[T_*(\rho(\beta)^{\otimes N})\big]\Big]. \tag{22}$$

In other words it is sufficient to calculate $\gamma\big[T_*(\rho(\beta)^{\otimes N})\big]$ (which is simpler because SU(2) representation theory is more directly applicable) instead of $\mathcal{F}_{\rm one}(T)$.

Another advantage of γ is its close relation to the parameter $\lambda = \tanh(\beta)$ defining the operation R_* in Equation (1). In fact we have

$$\gamma(\rho(\beta)^{\otimes N}) = \frac{1}{N}\operatorname{tr}\big(2L_3\rho(\beta)^{\otimes N}\big) = \frac{1}{N}N\operatorname{tr}\big(\sigma_3\rho(\beta)\big) = \tanh(\beta) = \lambda.$$

In other words the one particle restrictions of the output state $T\big(\rho(\beta)^{\otimes N}\big)$ are given by

$$\gamma\big[T(\rho(\beta)^{\otimes N})\big]\sigma + \big[1 - \gamma[T(\rho(\beta)^{\otimes N})]\big]\frac{\mathbb{1}}{2}.$$

This implies that $\gamma\big[T(\rho(\beta)^{\otimes N})\big] > \lambda$ should hold if T is really a purifier.

Let us consider now the natural purifier $T^{\rm nat}$. Since the number of output qubits is not constant in this case we have to consider for each $s \in I[N]$ the quantity $\mathcal{F}_{\rm one}(T^{\rm nat}_s)$ (see Equation (19) for the definition of the $T^{\rm nat}_s$) instead of one fixed parameter $\mathcal{F}_{\rm one}(T^{\rm nat})$ (in other words: The fidelity of $T^{\rm nat}$ is, as the number of output qubits, not a constant but an observable). According to the discussion above we get

$$\begin{aligned}\gamma\big(\rho_s(\beta)\big) &= \frac{1}{2s}\operatorname{tr}\Big(2L_3^{(s)}\rho_s(\beta)\Big) = \frac{1}{2s}\frac{\operatorname{tr}\big(2L_3^{(s)}\exp(2\beta L_3^{(s)})\big)}{\operatorname{tr}\big(\exp(2\beta L_3^{(s)})\big)} \\ &= \frac{1}{2s}\frac{d}{d\beta}\ln\operatorname{tr}\big(\exp(2\beta L_3^{(s)})\big) = \frac{1}{2s}\frac{d}{d\beta}\big(\ln\sinh\big((2s+1)\beta\big) - \ln\sinh\beta\big) \\ &= \frac{2s+1}{2s}\coth\big((2s+1)\beta\big) - \frac{1}{2s}\coth\beta \end{aligned} \tag{23}$$

and hence

$$\begin{aligned}\mathcal{F}_{\rm one}(T^{\rm nat}_s) &= \frac{1}{2}\Big[1 + \gamma\big(\rho_s(\beta)^{\otimes N}\big)\Big] \\ &= \frac{1}{2}\left[1 + \frac{2s+1}{2s}\coth\big((2s+1)\beta\big) - \frac{1}{2s}\coth\beta\right].\end{aligned}$$

If $s = 1/2$ we have $\gamma\big(\rho_s(\beta)\big) = \tanh(\beta) = \lambda$ hence the (perturbed) input state $\rho(\beta)$ is reproduced. Taking the derivative with respect to s shows in addition that $\gamma\big(\rho_s(\beta)\big)$ is strictly increasing in s. Hence $T^{\rm nat}$ really purifies (according to the remark above) and the best result we get if s is maximal. In the limit $s \to 0$ we find $\gamma\big(\rho_s(\beta)\big) = 0$ which is reasonable because $T^{\rm nat}$ does not produce any output at all in this case ($\dim\mathcal{H}_s = 1$ for $s = 0$).

Let us apply these results to the optimal purifier. According to the definition of $T^{\rm opt}$ and $T^{\rm nat}$ in Equations (20) and (19) the decomposition of $T^{\rm opt}$ given in (15) has the form

$$T^{\rm opt}(A) = T^{\rm nat}(\hat{Q}(A)) = \sum_{s\in I[N]}\hat{Q}_{2s}(A)\otimes\mathbb{1} = \sum_{s\in I[N]}T^{\rm opt}_s(A)\otimes\mathbb{1}, \tag{24}$$

hence $T_s^{\rm opt}(A) = \hat{Q}_{2s}(A)$. Together with (22) we get

$$\begin{aligned}\mathcal{F}_{\rm one}(T^{\rm opt}) &= \frac{1}{2}\left[1 + \sum_{s\in I[N]} w_N(s)\gamma\big[T^{\rm opt}_{s*}(\rho_s(\beta))\big]\right] \\ &= \frac{1}{2}\left[1 + \sum_{s\in I[N]} w_N(s)\gamma\big[\hat{Q}_{2s*}(\rho_s(\beta))\big]\right] \\ &=: \sum_{s\in I[N]} w_N(s) f_{\rm one}(M,\beta,s),\end{aligned} \tag{25}$$

where we have introduced the abbreviation

$$f_{\rm one}(M,\beta,s) := \frac{1}{2}\left[1 + \gamma\big[\hat{Q}_{2s}(\rho_s(\beta))\big]\right].$$

Together with Theorem 3.1 this implies:

$$\begin{aligned}2f_{\rm one}(M,\beta,s) - 1 = \gamma\big[\hat{Q}_{2s*}(\rho_s(\beta))\big] &= \frac{1}{M}\,{\rm tr}\big[2\hat{Q}_{2s}(L_3)\rho_s(\beta)\big] \\ &= \frac{\omega(\hat{Q}_{2s})}{M}\,{\rm tr}[2L_3^{(s)}\rho_s(\beta)] = \frac{\omega(\hat{Q}_{2s})2s}{M}\gamma[\rho_s(\beta)].\end{aligned}$$

Inserting the values of $\omega(\hat{Q}_{2s})$ and $\gamma[\rho_s(\beta)]$ from Equations (16) and (23) we get

$$\begin{aligned}&2f_{\rm one}(M,\beta,s) - 1 = \\ &\quad = \begin{cases} \dfrac{2s+1}{2s}\coth\big((2s+1)\beta\big) - \dfrac{1}{2s}\coth\beta & \text{for } 2s > M \\ \dfrac{1}{2s+2}\dfrac{M+2}{M}\Big((2s+1)\coth\big((2s+1)\beta\big) - \coth\beta\Big) & \text{for } 2s \leq M. \end{cases}\end{aligned} \tag{26}$$

Hence we have proved the following proposition.

Proposition 4.1. *The one–qubit fidelity $\mathcal{F}_{\rm one}(T^{\rm opt})$ of the optimal purifier is given by*

$$\mathcal{F}_{\rm one}(T^{\rm opt}) = \sum_{s\in I[N]} w_N(s) f_{\rm one}(M,\beta,s) \tag{27}$$

with $f_{\rm one}(M,\beta,s)$ from Equation (26).

Note in particular that in the case $M = 1$ the one–qubit fidelity coincides with the expectation value of the fidelity of $T^{\rm nat}$ in the state $T^{\rm nat}_*(\rho(\beta)^{\otimes N})$ – the *mean fidelity*. Hence we can reinterpret the natural purifier as a device which produces exactly one output system (cf. [3]).

4.3 The all qubit fidelity

As in the one–qubit case the all–qubit fidelity of T^{nat} is an observable rather than a fixed parameter. Hence we have to calculate $\mathcal{F}_{\mathrm{all}}(T_s^{\mathrm{nat}})$ for each fixed s. Applying again Equation (21) we get

$$\begin{aligned}\mathcal{F}_{\mathrm{all}}(T_s^{\mathrm{nat}}) &= \mathrm{tr}\big(\sigma^{\otimes 2s}\rho_s(\beta)\big) = \frac{\sinh(\beta)}{\sinh\big((2s+1)\beta\big)}e^{2\beta s}\\ &= \frac{e^{(2s+1)\beta}-e^{(2s-1)\beta}}{e^{(2s+1)\beta}-e^{(2s+1)\beta}} = \frac{1-e^{-2\beta}}{1-e^{-(4s+2)\beta}}.\end{aligned}$$

Using the decomposition of T^{opt} given in Equation (24) we get for the optimal purifier something similar as in the last subsection:

$$\begin{aligned}\mathcal{F}_{\mathrm{all}}(T^{\mathrm{opt}}) &= \sum_{s\in I[N]} w_N(s)\,\mathrm{tr}\left[\sigma^{\otimes M}T_{s*}^{\mathrm{opt}}\big(\rho_s(\beta)\big)\right] \qquad (28)\\ &= \sum_{s\in I[N]} w_N(s)\,\mathrm{tr}\left[\sigma^{\otimes M}\hat{Q}_{2s*}\big(\rho_s(\beta)\big)\right].\end{aligned}$$

However the calculation of

$$f_{\mathrm{all}}(M,\beta,s) := \mathrm{tr}\left[\sigma^{\otimes M}\hat{Q}_{2s*}\big(\rho_s(\beta)\big)\right]$$

is now more difficult, since the knowledge of $\hat{Q}_{2s}(L_3) = \omega(\hat{Q}_{2s})L_3^s$ is not sufficient in this case. Hence we have to use the explicit form of $\hat{Q}_{2s}$ in Equation (17) and (18). For $2s < M$ this leads to

$$\begin{aligned}f_{\mathrm{all}}(M,\beta,s) &= \frac{2s+1}{M+1}\,\langle\psi^{\otimes M}, S_M(\rho_s\otimes\mathbb{1}^{\otimes(M-2s)})S_M\psi^{\otimes M}\rangle\\ &= \frac{2s+1}{M+1}\,\langle\psi^{\otimes M}, (\rho_s\otimes\mathbb{1}^{\otimes(M-2s)})\psi^{\otimes M}\rangle = \frac{2s+1}{M+1}\,\langle\psi^{\otimes 2s}, \rho_s\psi^{\otimes 2s}\rangle\\ &= \frac{2s+1}{M+1}\,\frac{1-e^{-2\beta}}{1-e^{-(4s+2)\beta}}.\end{aligned}$$

For $M \leq 2s$ we have to calculate

$$\begin{aligned}f_{\mathrm{all}}(s,M,\beta) &= \mathrm{tr}\left[\sigma^{\otimes M}\hat{Q}_{2s*}\big(\rho_s(\beta)\big)\right] = \mathrm{tr}\left[\hat{Q}_{2s}(\sigma^{\otimes M})\rho_s(\beta)\right]\\ &= \mathrm{tr}\left[\rho_s(\beta)\Big(S_M[(|\psi^{\otimes M}\rangle\langle\psi^{\otimes M}|)\otimes\mathbb{1}^{\otimes(2s-M)}]S_M\Big)\right] \qquad (29)\end{aligned}$$

We will compute the operator $\hat{Q}_{2s}(\sigma^{\otimes M})$ in occupation number representation. By definition, the basis vector "$|n\rangle$" of the occupation number basis is the normalized version of $S_M\Psi$, where Ψ is a tensor product of n factors ψ and $(M-n)$ factors

ϕ, where $\phi = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$ denotes obviously the second basis vector. The normalization factor is easily computed to be

$$S_M(\psi^{\otimes n} \otimes \phi^{\otimes(M-n)}) = \binom{M}{n}^{-1/2} |n\rangle. \tag{30}$$

We can now expand the "$\mathbb{1}$" in Equation (29) in product basis, and apply (30), to find

$$S_M[(|\psi^{\otimes M}\rangle\langle\phi^{\otimes M}|) \otimes \mathbb{1}^{\otimes(2s-M)}]S_M = \sum_K \binom{2s-M}{K-M}\binom{2s}{K}^{-1} |K\rangle\,\langle K|.$$

Now L_3 is diagonal in this basis, with eigenvalues $m_K = (K-s)$, $K = 0, \dots, (2s)$. With $\rho_s(\beta)$ from (12) we get

$$f_{\mathrm{all}}(M,\beta,s) = \frac{1-e^{-2\beta}}{1-e^{-(4s+2)\beta}} \sum_K \binom{2s-M}{K-M}\binom{2s}{K}^{-1} e^{2\beta(K-s)} \quad \text{for } M \leq 2s.$$

Together with

$$\binom{2s-M}{K-M}\binom{2s}{K}^{-1} = \frac{(2s-M)!}{(K-M)!(2s-K)!}\,\frac{K!(2s-K)!}{(2s)!} = \binom{2s}{M}^{-1}\binom{K}{M}$$

we get

$$f_{\mathrm{all}}(M,\beta,s) = \frac{1-e^{-2\beta}}{1-e^{-(4s+2)\beta}}\binom{2s}{M}^{-1} \sum_K \binom{K}{M} e^{2\beta(K-s)}.$$

Summarizing these calculations we get the following proposition:

Proposition 4.2. *The all–qubit fidelity $\mathcal{F}_{\mathrm{all}}(T^{\mathrm{opt}})$ of the optimal purifier is given by*

$$\mathcal{F}_{\mathrm{all}}(T^{\mathrm{opt}}) = \sum_{s \in I[N]} w_N(s) f_{\mathrm{one}}(M,\beta,s) \tag{31}$$

where $f_{\mathrm{all}}(M,\beta,s)$ is given by

$$f_{\mathrm{all}}(M,\beta,s) = \begin{cases} \dfrac{2s+1}{M+1}\,\dfrac{1-e^{-2\beta}}{1-e^{-(4s+2)\beta}} & M \leq 2s \\[2ex] \dfrac{1-e^{-2\beta}}{1-e^{-(4s+2)\beta}}\dbinom{2s}{M}^{-1} \displaystyle\sum_K \dbinom{K}{M} e^{2\beta(K-s)} & M > 2s. \end{cases} \tag{32}$$

5 Solution of the optimization problems

Now we are going to prove the following theorem:

Theorem 5.1. *The purifier T^{opt} maximizes the fidelities $\mathcal{F}_{\text{one}}(T)$ and $\mathcal{F}_{\text{all}}(T)$. Hence the optimal fidelities $\mathcal{F}_{\text{one}}^{\max}(N,M)$ and $\mathcal{F}_{\text{all}}^{\max}(N,M)$ defined in Section 2 are given by Equation (27) and (31).*

Proof. Note first that the funtionals $\mathcal{F}_{\text{one}}$ and $\mathcal{F}_{\text{all}}$ are, as infima over continuous functions, upper semicontinuous. Together with the compactness of the set of admissible T this implies that the suprema $\mathcal{F}_{\#}^{\max}(N,M)$ from Equation (4) are attained. In other words: optimal purifier T with $\mathcal{F}_{\#}(T) = \mathcal{F}_{\#}^{\max}(N,M)$ exist, and we can assume without loss of generality that they are fully symmetric (according to the discussion in Section 3.1). Hence we can apply Equation (21) and the decomposition (15) to get in analogy to (25) and (28)

$$\mathcal{F}_{\text{one}}(T) = \frac{1}{2}\left[1 + \sum_{s \in I[N]} w_N(s)\gamma\big[T_{s*}(\rho_s(\beta))\big]\right]$$

and

$$\mathcal{F}_{\text{all}}(T) = \sum_{s\in I[N]} w_N(s)\,\mathrm{tr}\left[\sigma^{\otimes M} T_{s*}\big(\rho_s(\beta)\big)\right]. \tag{33}$$

The last two Equations show that we have to optimize each component T_s of the purifier T independently. In the one qubit case this is very easy, because we can use Theorem 3.1 to get $T_s(L_3) = \omega(T_s)L_3^{(s)}$ and $\gamma\big[T_{s*}(\rho_s(\beta))\big] = \omega(T_s)\,\mathrm{tr}\big(L_3^{(s)}\rho_s(\beta)\big)$. Hence maximizing $\gamma\big[T_{s*}(\rho_s(\beta))\big]$ is equivalent to maximizing $\omega(T_s)$. But we have according to Theorem 3.1

$$\max_T \omega(T_s) = \omega(\hat{Q}_{2s}) = \begin{cases} \dfrac{M}{2s} & \text{for } 2s \geq M \\ \dfrac{M+2}{2(s+1)} & \text{for } 2s < M, \end{cases}$$

which shows that $\mathcal{F}_{\text{one}}^{\max}(N,M) = \mathcal{F}_{\text{one}}(T^{\text{opt}})$ holds as stated.

For the many qubit–test version the proof is slightly more difficult. However as in the $\mathcal{F}_{one}$-case we can solve the optimization problem for each summand in Equation (33) separately. First of all this means that we can assume without loss of generality that T_{s*} takes its values in $\mathcal{B}(\mathcal{H}_+^{\otimes M})$ because the functional

$$f_s(T_s) := \mathrm{tr}\left(\sigma^{\otimes M} T_{s*}\big(\rho_s(\beta)\big)\right) \tag{34}$$

which we have to maximize, depends only on this part of the operation. Full symmetry implies in addition that $T_{s*}(\rho_s(\beta))$ is diagonal in occupation number basis (see Equation (30)), because $T_{s*}(\rho_s(\beta))$ commutes with each $\pi_{s'}(U)$ ($s' = M/2$, $U \in \mathrm{U}(2)$) if $\pi_s(U)$ commutes with $\rho_s(\beta)$.

If $M > 2s$ this means we have $T_{s*}(\rho_s(\beta)) = \kappa_* \sigma^{\otimes M} + r_*$ where r_* is a positive operator with $\sigma^{\otimes M} r_* = r_* \sigma^{\otimes M} = 0$. Inserting this into (34) we see that $f_s(T_s) = \kappa_*$. Hence we have to maximize κ_*. The first step is an upper bound which we get from the fact that $\mathrm{tr}\big(\sigma^{\otimes M}\rho_s(\beta)\big)\mathbb{1} - \rho_s(\beta)$ is a positive operator. Since $T_{s*}(\mathbb{1}) = (2s+1)/(M+1)\mathbb{1}$ (another consequence of full symmetry) we have

$$0 \leq T\Big(\mathrm{tr}\big(\sigma^{\otimes 2s}\rho_s(\beta)\big)\mathbb{1} - \rho_s(\beta)\Big) = \frac{2s+1}{M+1}\,\mathrm{tr}\big(\sigma^{\otimes M}\rho_s(\beta)\big)\mathbb{1} - \kappa\sigma^{\otimes M} - r_*.$$

Multiplying this Equation with $\sigma^{\otimes M}$ and taking the trace we get

$$\kappa_* \leq \frac{2s+1}{M+1}\,\mathrm{tr}\big(\sigma^{\otimes M}\rho_s(\beta)\big). \tag{35}$$

However calculating $f_s(T_s^{\mathrm{opt}})$ we see that this upper bound is achieved, in other words T_s^{opt} maximizes f_s.

If $M \leq 2s$ holds we have to use slightly different arguments because the estimate (35) is to weak in this case. However we can consider in Equation (34) the dual T_s instead of T_{s*} and use then similar arguments. In fact for each covariant T_s the quantity $T_s(\sigma^{\otimes M})$ is, due to the same reasons as $T_{s*}(\rho_s(\beta))$ diagonal in the occupation number basis and we get $T_s(\sigma^{\otimes M}) = \kappa\sigma^{\otimes 2s} + r$ where r is again a positive operator with $r = \sum_{n=0}^{2s-1} r_n|n\rangle$ ($|n\rangle$ denotes again the occupation number basis) and κ is a positive constant. Since T_s is unital we get from $\mathbb{1} - \sigma^{\otimes M} \geq 0$ the estimate $0 \leq \kappa \leq 1$ in the same way as Equation (35). Calculating $T_s^{\mathrm{opt}}(\sigma^{\otimes M})$ shows again that the upper bound $\kappa = 1$ is indeed achieved, however it is now not clear whether maximizing κ is equivalent to maximizing $f_s(T_s)$.

Hence let us show first that $\kappa = 1$ is *necessary* for $f_s(T_s)$ to be maximal. This follows basically from the fact that T_s is, up to a multiplicative constant, trace preserving. In fact we have

$$\mathrm{tr}\big(T_s(\sigma^{\otimes M})\big) = \mathrm{tr}\big(T_s(\sigma^{\otimes M})\mathbb{1}\big) = \mathrm{tr}\big(\sigma^{\otimes M}T_{s*}(\mathbb{1})\big) = \frac{2s+1}{M+1}.$$

This means especially that $\kappa + \mathrm{tr}(r) = (2s+1)/(M+1)$ holds, i.e. decreasing κ by $0 < \epsilon < 1$ is equivalent to increasing $\mathrm{tr}(r)$ by the same ϵ. Taking into account that $\rho_s(\beta) = \sum_{n=0}^{2s} h_n|n\rangle$ holds with $h_n = \exp\big(2\beta(n-s)\big)$, we see that reducing κ by ϵ reduces $f_s(T_s)$ at least by

$$\epsilon\Big(\mathrm{tr}\big(\sigma^{\otimes 2s}\rho_s(\beta)\big) - \mathrm{tr}\big(|2s-1\rangle\rho_s(\beta)\big)\Big) = \epsilon\big(e^{2\beta s} - e^{(2s-1)\beta}\big) > 0.$$

Therefore $\kappa = 1$ is necessary.

The last question we have to answer, is how the rest term r has to be chosen, for $f_s(T_s)$ to be maximal. To this end let us consider the slightly modified fidelity $\tilde{f}_s(T_s) = \mathrm{tr}\big(T_s(\sigma^{\otimes M})\sigma^{\otimes 2s}\big)$ (which is in fact related to optimal cloning; see [1] and Section 3.4). It is in contrast to $f_s(T_s)$ maximized *iff* $\kappa = 1$. However the operation which maximizes $\tilde{f}(T_s)$ is obviously the optimal $M \to 2s$ cloner (up to normalization) which is according to [2] unique. This implies that $\kappa = 1$ fixes T_s already. Together with the facts that $\kappa = 1$ is necessary for $f_s(T_s)$ to be maximal and $\kappa = 1$ is realized for T_s^{opt} we conclude that $\max f_s(T_s) = f_s(T_s^{\mathrm{opt}})$ holds, which proves the assertion. □

6 Asymptotic behaviour

Now we want to analyze the rate with which nearly perfect purified qubits can be produced in the limit $N \to \infty$. To this end we have to compute the asymptotic behaviour of various expectations involving s. It turns out that it is much better not to do work with the explicit expressions of these expectations, as sums over expressions with many binomial coefficients, but to go back to the definition, and use general properties of expectations of $\rho^{\otimes N}$. This has the added advantage of being easily generalized to Hilbert space dimensions $d > 2$, so we expect the method to be useful in its own right. We collect the basic statements in the following subsection, applying them to the concrete expressions in subsequent ones.

6.1 Convergence of weights to a point measure

In the classical case the general theory alluded to above is nothing but the theory of asymptotic distributions for independent identically distributed random variables (Laws of large numbers of various sorts). In the quantum case this theory has been developed in the context of the statistical mechanics of general mean-field systems [5]. Of this theory we need only the simplest aspects (convergence to a point measure), and not the more advanced "Large Deviation" parts, in which it is shown how the probability of deviations from the limit decrease exponentially fast.

Consider operators of the form $A_N = (1/N)\sum_{i=1}^{N} a^{(i)}$, where $a^{(i)}$ denotes the copies of a fixed operator on $\mathcal{H}$, acting in the i^{th} tensor factor of $\mathcal{H}^{\otimes N}$. It is clear that the expectations $\mathrm{tr}(\rho^{\otimes N} A_N) = \mathrm{tr}(\rho a)$ are independent of N. Now consider products of a finite number of such operators and expand the expectation into the average over all terms of the form $\mathrm{tr}(\rho^{\otimes N} a^{(i)} b^{(j)} c^{(k)} \cdots)$. It is easy to see that for large N the majority of these terms will be such that all indices $i, j, k, \ldots$ are different, and for such terms the above expression is equal to $\mathrm{tr}(\rho a)\,\mathrm{tr}(\rho b)\,\mathrm{tr}(\rho c) \cdots$. So this will be the limit of the expectation of the product $A_N B_N C_N \cdots$ as $N \to \infty$ (for precise combinatorial estimates, see [5]). Of course, this allows us to compute the asymptotic expectations for arbitrary polynomials, and by taking suitable limits of arbitrary continuous functions of Hermitian operators. There is an abstract non-commutative functional calculus describing exactly these possibilities (see appendix of [5]). However, for our purposes it is sufficient to say that all combinations of algebraic operations and continuous functions of a Hermitian variable (evaluated in the usual spectral functional calculus) are in this class.

For the case at hand, note that the angular momentum operators L_k as in Equation (13) are of the form NA_N therefore, for any sequence of functions f_N of three non-commuting arguments (this means that in writing out f_N we have to keep track of operator ordering), which converges to a limit function, f_∞, we get

$$\lim_{N\to\infty} \operatorname{tr}\left(\rho^{\otimes N} f_N\left(\tfrac{L_1}{N}, \tfrac{L_2}{N}, \tfrac{L_3}{N}\right)\right) = f_\infty\left(\operatorname{tr}(\rho\frac{\sigma_1}{2}), \operatorname{tr}(\rho\frac{\sigma_2}{2}), \operatorname{tr}(\rho\frac{\sigma_3}{2})\right). \tag{36}$$

Note that the function f_∞ is just evaluated on numbers (operators on a one-dimensional space) so all operator ordering problems disappear in the limit. This is the huge simplification which makes mean-field theory so accessible. The limit formula will be applied to functions of "$2s$", the number of outputs from the natural purifier, which can itself be written as a function of this sort. It is, of course, constant on each summand of the decomposition (11), so it is a function of the Casimir operator $\vec{L}^2 = s(s+1)$:

$$\begin{aligned}\frac{2s}{N} = g_N\left(\tfrac{L_1}{N}, \tfrac{L_2}{N}, \tfrac{L_3}{N}\right) &= \sqrt{4(\vec{L}/N)^2 + N^{-2}} - 1/N \\ g_\infty(x_1, x_2, x_3) &= \lim_{N\to\infty} \sqrt{4(\vec{x})^2 + N^{-2}} - 1/N = 2|\vec{x}| \\ g_\infty\left(\operatorname{tr}(\rho\frac{\sigma_1}{2}), \operatorname{tr}(\rho\frac{\sigma_2}{2}), \operatorname{tr}(\rho\frac{\sigma_3}{2})\right) &= g_\infty(0,0,\lambda/2) = \lambda = \tanh\beta, \end{aligned}\tag{37}$$

when $\rho = \rho(\beta)$ is given by eq.(12). Functions of g then also lie in the relevant functional calculus, so we get the following statement, taylored to our need in the following subsections. In it we have already encorporated further, straightforward approximation arguments, using uniformly convergent sequences of continuous functions to establish upper and lower bounds separately.

Lemma 6.1. *Let $f_N : (0,1) \to \mathbb{R}$, $N \in \mathbb{N}$ be a uniformly bounded sequence of continuous functions, converging uniformly on a neighborhood of $\lambda = \operatorname{tr}(\rho(\beta)\sigma_3)$ to a continuous function f_∞, and let $w_N(s)$ denote the weights in Equation (14). Then*

$$\lim_{N\to\infty} \sum_{s\in I[N]} w_N(s) f_N(2s/N) = f_\infty(\lambda). \tag{38}$$

In the language of measure theory this is saying that the probability measures $\sum_s w_N(s)\delta(x - 2s/N)dx$ on the interval $[0,1]$ converge to the point measure $\delta(x - \lambda)dx$. Graphically, this is shown in Figure 3

6.2 The one particle test

Let us analyze first the behaviour of the optimal one–qubit fidelity $\mathcal{F}^{\max}_{\text{one}}(N,M)$ in the limit $M \to \infty$. Obviously only the $M > 2s$ case of $f_{\text{one}}(M,\beta,s)$ is relevant in this situation and we get, together with Equation (27), the expression

$$\mathcal{F}^{max}_{one}(N,\infty) = \sum_{s\in I[N]} w_N(s) \frac{1}{2}\left[1 + \frac{1}{2s+2}\Big((2s+1)\coth\big((2s+1)\beta\big) - \coth\beta\Big)\right],$$

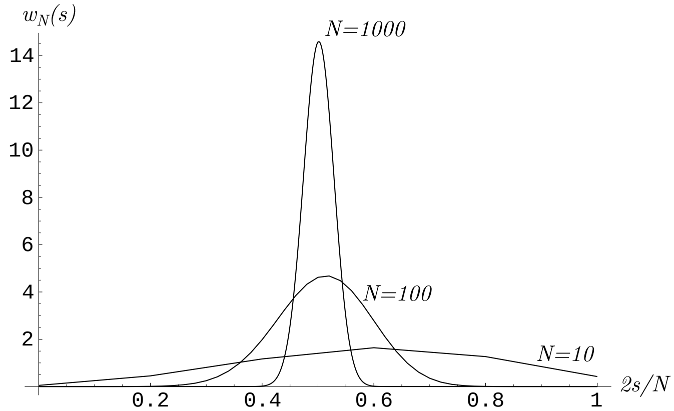

Figure 3: Convergence of $w_N(s)$ to a point measure ($\lambda = .5$, $N = 10, 100, 1000$). Discrete points joined, and rescaled for total area 1

which obviously takes its values between 0 and 1. To take the limit $N \to \infty$ we can write

$$\lim_{N\to\infty} \mathcal{F}_{\text{one}}^{\max}(N,\infty) = \lim_{N\to\infty} \sum_{s\in I[N]} w_N(s) f_{N,\infty}(\frac{2s}{N})$$

with

$$f_{N,\infty}(x) = \frac{1}{2}\left[1 + \frac{1}{Nx+2}\Big((Nx+1)\coth\big((Nx+1)\beta\big) - \coth\beta\Big)\right].$$

The functions $f_{N,\infty}$ are continuous, bounded and converge on each interval $(\epsilon, 1)$ with $0 < \epsilon < 1$ uniformly to $f_{\infty,\infty} \equiv 1$. Hence the assumptions of Lemma 6.1 are fulfilled and we get

$$\lim_{N\to\infty} \mathcal{F}_{\text{one}}^{\max}(N,\infty) = f_{\infty,\infty}(\lambda) = 1$$

as already stated in Section 2. This means that we can produce arbitrarily good purified qubits at infinite rate if we have enough input systems.

To analyze how fast the quantity $\mathcal{F}_{\text{one}}^{\max}(N,\infty)$ approaches 1 as $N \to \infty$ let us consider the limit

$$\lim_{N\to\infty} N(1 - \mathcal{F}_{\text{one}}^{\max}(N,\infty)) = \sum_{s\in I[N]} w_N(s) \tilde{f}_{N,\infty}(\frac{2s}{N}) \equiv \frac{c_\infty}{2} \tag{39}$$

with $\tilde{f}_{N,\infty} = N(1 - f_{N,\infty})$. The existence of this limit is equivalent to the asymptotic formula

$$\mathcal{F}_{\text{one}}^{\max}(N,\infty) = 1 - \frac{c_\infty}{2N} + \mathbf{o}\left(\frac{1}{N}\right),$$

where, as usual, $\mathbf{o}\left(\frac{1}{N}\right)$ stands for terms going to zero faster than $\frac{1}{N}$. Lemma 6.1 leads to $c_\infty/2 = \tilde{f}_{\infty,\infty}(\lambda)$ with $\tilde{f}_{\infty,\infty} = \lim_{N\to\infty} \tilde{f}_{N,\infty}$ uniformly on $(\epsilon, 1)$. To calculate $\tilde{f}_{\infty,\infty}$ note that

$$\tilde{f}_{N,\infty}(x) = \frac{N}{Nx+2} + \frac{N\coth\beta}{Nx+2} + \text{ Rest}$$

holds, where "Rest" is a term which vanishes exponentially fast as $N \to \infty$. Hence with $\coth\beta = 1/\lambda$ we get

$$c_\infty = 2\tilde{f}_{\infty,\infty}(\lambda) = \frac{1+\lambda}{\lambda^2}$$

The asymptotic behaviour of $\mathcal{F}^{\max}_{\text{one}}(N,1)$ can be analyzed in the same way. The only difference is that we have to consider now the $1 = M \leq 2s$ branch of Equation (26). In analogy to Equation (39) we have to look at

$$\lim_{N\to\infty} N(1 - \mathcal{F}^{\max}_{\text{one}}(N,1)) = \sum_{s\in I[N]} w_N(s)\tilde{f}_{N,1}(\frac{2s}{N}) = \frac{c_1}{2}$$

with $\tilde{f}_{N,1} = N(1 - f_{N,1})$ and

$$f_{N,1}(x) = \frac{1}{2}\left[1 - \frac{1}{Nx}\left[(Nx+1)\coth\big((Nx+1)\beta\big) - \coth\beta\right]\right].$$

For $\tilde{f}_{\infty,1}$ we get

$$\tilde{f}_{\infty,1}(x) = \frac{1}{2}(\frac{-1}{x} + \frac{1}{x\lambda}). \tag{40}$$

Using again Lemma 6.1 leads to

$$c_1 = 2\tilde{f}_{\infty,1}(\lambda) = \frac{1-\lambda}{\lambda^2}.$$

Finally let us consider $\mathcal{F}^{\max}_{\text{one}}(N,0)$. Here the situation is easier than in the other cases because $\mathcal{F}^{\max}_{\text{one}}(N,0)$ equals the fidelity of the best possible output of the natural purifier, i.e.

$$\mathcal{F}^{\max}_{\text{one}}(N,0) = \frac{1}{2}\left[1 - \frac{1}{N}\left[(N+1)\coth\big((N+1)\beta\big) - \coth\beta\right]\right] = f_{N,1}(1).$$

Hence we only need the asymptotic behaviour of $f_{N,1}(x)$ at $x = 1$. Using Equation (40) we get

$$\mathcal{F}^{\max}_{\text{one}}(N,0) = 1 - \frac{1-\lambda}{\lambda}\frac{1}{2N} + \cdots .$$

This concludes the proof of Equations (6) to (9).

6.3 The many particle test

Consider now the many–qubit fidelity $\mathcal{F}_{\rm all}$. Although, like $\mathcal{F}_{\rm one}$, it lies between zero and one, and would attain the value 1 precisely for a (non-existent) ideal purifier, both quantities behave quite differently, when we use them to compare states in systems of varying size. We are looking here at the two kinds of fidelities for an M-particle output state ρ_M with respect to a one-particle pure state given by the vector ψ, namely

$$\begin{aligned} F_{\rm all} &= \langle \psi^{\otimes M}, \rho_M \psi^{\otimes M}\rangle = \operatorname{tr}\rho_M \Big(|\psi^{\otimes M}\rangle\langle\psi^{\otimes M}| \Big) \quad \text{, and} \\ F_i &= \langle \psi, \rho_M^{(i)} \psi\rangle = \operatorname{tr}\rho_M \Big(\mathbb{1} \otimes \cdots (|\psi\rangle\langle\psi|)_i \otimes \mathbb{1} \Big) \quad , \end{aligned}$$

where $\rho_M^{(i)}$ denotes the restriction of ρ_M to the $i^{\rm th}$ tensor factor. Let $p_{\rm all}$ and p_i denote the projections whose ρ_M-expectations appear on the right hand side of these Equations. These projections commute, and $p_{\rm all}$ is the intersection (in the commuting case: the product) of the p_i in the lattice of projections. This corresponds to the union of the respective complements, i.e.,

$$\mathbb{1} - p_i \le \mathbb{1} - p_{\rm all} \le \sum_i (\mathbb{1} - p_i) \quad .$$

Taking expectations with respect to ρ_M, we find that $\sup_i(1-F_i) \le (1-F_{\rm all}) \le \sum_i (1-F_i) \le M \sup_i(1-F_i)$. For the two figures of merit introduced in Section 1 this implies

$$(1 - \mathcal{F}_{\rm one}(T)) \le (1 - \mathcal{F}_{\rm all}(T)) \le M(1 - \mathcal{F}_{\rm one}(T)) \quad , \tag{41}$$

for every purifying device T. Hence, for fixed N the two figures of merit are equivalent to within a factor . But the upper bound becomes meaningless in the limit $M \to \infty$, so it is not clear at all whether we can bring the fidelity $\mathcal{F}_{\rm all}(T)$ close to one for an increasing number of outputs.

As a consequence of this analysis it is necessary to perform the limit $N, M \to \infty$ more carefully as in the one qubit case. We will consider therefore the limits $N \to \infty$ and $M \to \infty$ simultaneously, while the quotient M/N approaches a constant μ, i.e. we will calculate the function $\Phi(\mu)$ defined in Equation (10). The first step in this context is the following lemma, which allows us to handle the $\binom{2s}{M}^{-1} \sum_K \binom{K}{M} e^{2\beta(K-s)}$ term in Equation (32).

Lemma 6.2. *For integers $M \le K$ and $z \in \mathbb{C}$, define*

$$\Phi(K, M, z) = \binom{K}{M}^{-1} \sum_{R=M}^{K} \binom{R}{M} z^{K-R}.$$

Then, for $|z| < 1$, and $c \ge 1$:

$$\lim_{\substack{M,K\to\infty \\ M/K\to c}} \Phi(K, M, z) = \frac{1}{1 - (1-c)z}.$$

Proof. We substitute $R \mapsto (K - R)$ in the sum, and get

$$\Phi(K, M, z) = \sum_{R=0}^{\infty} c(K, M, R) z^R,$$

where coefficients with $M + R > K$ are defined to be zero. We can write the non-zero coefficients as

$$\begin{aligned} c(K, M, R) &= \binom{K}{M}^{-1} \binom{K-R}{M} = \frac{(K-M)!(K-R)!}{K!(K-R-M)!} \\ &= \frac{(K-M)}{K} \frac{(K-M-1)}{(K-1)} \cdots \frac{(K-M-R+1)}{(K-R+1)} \\ &= \prod_{S=0}^{R-1} \left(1 - \frac{M}{K-S}\right). \end{aligned}$$

Since $0 \leq c(K, M, R) \leq 1$, for all K, M, R, the series for different values of M, K are all dominated by the geometric series, and we can go to the limit termwise, for every R separately. In this limit we have $M/(K - S) \to c$ for every S, and hence $c(K, M, R) \to (1 - c)^R$. The limit series is again geometric, with quotient $(1 - c)z$ and we get the result. □

To calculate now $\Phi(\mu)$ recall that the weights $w_N(s)$ approach a point measure in $2s/N =: x$ concentrated at $\lambda = \mathrm{tr}(\rho(\beta)\sigma_3)$. This means that in Equation (31) only the term with $2s = \lambda N$ survives the limit. Hence if $\mu \geq \lambda$ we get $M \geq \lambda N = 2s$. Using Equation (32) and Lemma 6.1 we get in this case

$$\Phi(\mu) = \frac{\lambda}{\mu}(1 - e^{-2\beta}).$$

We see that $\Phi(\mu) \to 0$ for $\mu \to \infty$ and $\Phi(\mu) \to 1 - \exp(-2\beta)$ for $\mu \to \lambda$.

If $0 < \mu < \lambda$ we get $M < \lambda N = 2s$, which means we have to choose Equation (32) for $f_{\mathrm{all}}(M, \beta, s)$. With Lemma 6.2 and Lemma 6.1 we get

$$\Phi(\mu) = \frac{1 - e^{-2\beta}}{1 - (1 - \mu/\lambda)e^{-2\beta}}$$

which approaches 1 if $\mu \to 0$ and $1 - \exp(-2\beta)$ if $\mu \to \lambda$. Writing this in terms of $\lambda = \tanh \beta$, we obtain Equation (10).

6.4 Estimating the many particle fidelity in terms of one particle

In Section 2 we motivated the observation that the the best all-particle fidelity is a function of the rate (and not identically equal to 1) by estimating the all-particle fidelity in terms of the one-particle fidelity. Since the latter quantity tends to be more easily computable it is of some interest for further investigations, how good that estimate actually is. The estimate mentioned in the text before Equation (10) amounts to

$$\Phi(\mu) \geq 1 - \frac{\mu}{2} c_\infty = 1 - \frac{\mu(\lambda + 1)}{2\lambda}. \tag{42}$$

However, the same basic estimate via Equation (41) gives even more information:

$$\begin{aligned} \Phi(\mu) &\geq 1 - \lim_{\substack{N\to\infty \\ M/N\to\mu}} M(1 - \mathcal{F}_{\text{one}}^{\max}(N, M)) \\ &\geq 1 - \mu \lim_{N\to\infty} \sum_{s\in I[N]} w_N(s)\ N(1 - f_{\text{one}}(\mu N, \beta, s)) \\ &= \begin{cases} 1 - \dfrac{\mu(1-\lambda)}{2\lambda^2} & \text{if } \mu \leq \lambda \\ 2 - \dfrac{\mu(1+\lambda)}{2\lambda^2} & \text{if } \mu \geq \lambda, \end{cases} \end{aligned} \tag{43}$$

where the evaluation of the limit was carried out with the same technique based on Lemma 6.1 used in the previous sections. Figure 4 displays the lower bounds (42) and (43) together with the exact result (10).

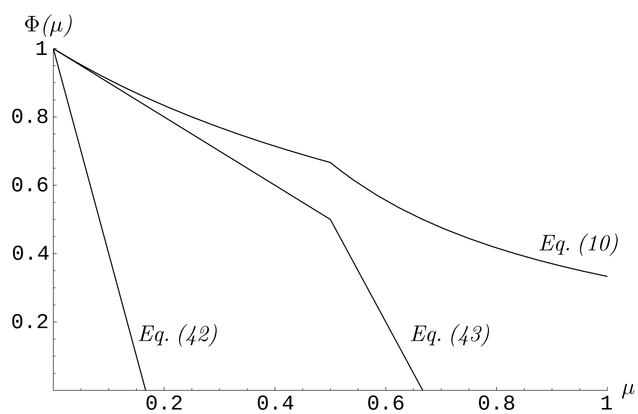

Figure 4: The lower bounds (42) and (43) together with the exact result (10) for the all-particle test fidelity as a function of the rate ($\lambda = .5$)

It is apparent that these bounds are rather weak, and in fact completely trivial for large rates. Hence all-particle fidelities contain new and independent information about purification processes, which is not already contained in their one-particle counterparts.

Acknowledgements

We acknowledge several rounds of email discussions with Ignacio Cirac, which helped to clarify the precise relation between this work and [3].

References

[1] R.F. Werner, Optimal cloning of pure states, *Phys.Rev.* **A58**, 980–1003 (1998).

[2] M. Keyl and R.F. Werner, Optimal cloning of pure states, testing single clones, *J. Math. Phys.* **40**, 3283–3299 (1999).

[3] J.I. Cirac, A.K. Ekert and C. Macchiavello, Optimal purification of single qubits, *Phys. Rev. Lett.* **82**, 4344–4347 (1999).

[4] B. Simon, Representations of finite and compact groups, American Mathematical Society, Providence (1996).

[5] G.A. Raggio and R.F. Werner, Quantum statistical mechanics of general mean field systems, *Helv. Phys. Acta* **62**, 980–1003 (1989).

M. Keyl and R. F. Werner
Institut für Mathematische Physik
TU Braunschweig
Mendelssohnstr. 3
D-38106 Braunschweig, Germany
e-mail: m.keyl@tu-bs.de
e-mail: R.Werner@tu-bs.de

Communicated by Vincent Rivasseau
submitted 24/01/00, accepted 25/09/00