Optimal covariant quantum networks

Giulio Chiribella, Giacomo Mauro D'Ariano, Paolo Perinotti

QUIT *Group, Dipartimento di Fisica "A. Volta", via Bassi 6, 27100 Pavia, Italy*

Abstract. A sequential network of quantum operations is efficiently described by its *quantum comb* [1], a non-negative operator with suitable normalization constraints. Here we analyze the case of networks enjoying symmetry with respect to the action of a given group of physical transformations, introducing the notion of covariant combs and testers, and proving the basic structure theorems for these objects. As an application, we discuss the optimal alignment of reference frames (without pre-established common references) with multiple rounds of quantum communication, showing that *i)* allowing an arbitrary amount of classical communication does not improve the alignment, and *ii)* a single round of quantum communication is sufficient.

A quantum comb [1] describes a quantum network with N open slots in which an ordered sequence of variable quantum devices can be inserted, thus programming the quantum operation of the resulting circuit. Mathematically, a comb implements an *admissible supermap* [2, 3], that transforms an input network of N quantum operations into an output quantum operation. Having at disposal a suitable formalism opens the possibility of optimizing the architecture of quantum circuits for a large number of computational, cryptographic, and game-theoretical tasks, such as discrimination of single-party strategies, cloning of quantum transformations, and storing of quantum algorithms into quantum memories [1, 4, 5, 6]. For example, quantum combs allow one to find the optimal networks for the estimation of an unknown group transformation with N uses at disposal, a problem that has been solved in the past only in the particular case of phase estimation [7]. Using combs and supermaps one can prove in full generality that a parallel disposition of the N black boxes is sufficient to achieve the optimal estimation of the unknown group element [5], thus reducing the problem to the optimal parallel estimation of group transformations already solved in Ref. [8].

In this paper we summarize the main concepts and methods developed so far in the optimization of quantum networks, with focus on the case of networks with symmetry properties, and we present an original result on multi-round protocols for reference frame alignment.

1. BASIC NOTIONS OF QUANTUM CIRCUITS ARCHITECTURE

1.1. Quantum N-combs

Consider a sequential network of N quantum operations (QOs) with memory, as in Fig. 1. Due to the presence of internal memories, there can be other networks that are indistinguishable from it in all experiments that involve only the incoming and outgoing quantum systems. The quantum comb is the equivalence class of all networks having

the same input/output relations, irrespectively of what happens inside. The equivalence
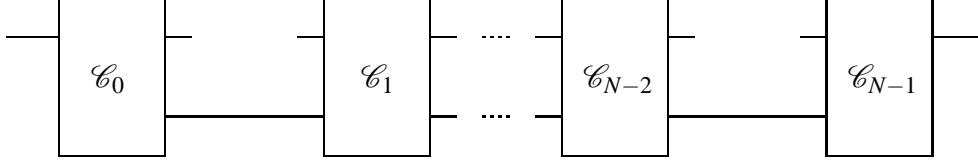
FIGURE 1. N-comb: sequential network of N quantum operations with memory. The network contains input and output systems (free wires in the diagram), as well as internal memories (wires connecting the boxes).

class is in one-to-one correspondence with the Choi operator of the network, which can be computed as the *link product* [1] of the Choi operators of the QOs $(\mathscr{C}_i)_{i=0}^{N-1}$. Here we adopt the convention that the input (output) spaces for the QO $\mathscr{C}_j$ are indicated as $\mathscr{H}_{2j}$ ($\mathscr{H}_{2j+1}$). Accordingly, the Choi operator of the network is a non-negative operator $R^{(N)} \in \mathsf{Lin}\left(\bigotimes_{j=0}^{2N-1} \mathscr{H}_j\right)$. The quantum comb can be then identified with such a Choi operator. For networks of channels (trace-preserving QOs) one has the recursive normalization condition

$$\mathrm{Tr}_{2k-1}[R^{(k)}] = I_{2k-2} \otimes R^{(k-1)} \qquad k = 1,\dots,N \tag{1}$$

where $R^{(k)} \in \mathsf{Lin}\left(\bigotimes_{j=0}^{2k-1} \mathscr{H}_j\right)$, and $R^{(0)} = 1$. Eq. (1) is the translation in terms of Choi operators of the fact that the N-partite channel $\mathscr{R}^{(N)} = \mathscr{C}_{N-1} \circ \mathscr{C}_{N-2} \circ \cdots \circ \mathscr{C}_0$, sending states on the even Hilbert spaces $\mathsf{St}(\bigotimes_{k=0}^{N-1} \mathscr{H}_{2k})$ to states on the odd ones $\mathsf{St}(\bigotimes_{k=0}^{N-1} \mathscr{H}_{2k+1})$, is a deterministic *causal automaton* [9, 10], namely a channel where the reduced dynamics of an input state at step k depends only on input states at steps $k' \leq k$, and not at steps $k' > k$. With different motivations from supermaps and causal automata, Eq. (1) also appeared in the work by Gutoski and Watrous toward a general formulation of quantum games [4].

We call $\mathsf{DetComb}\left(\bigotimes_{j=0}^{2N-1} \mathscr{H}_j\right)$ the set of non-negative operators satisfying Eq.(1), and $\mathsf{ProbComb}\left(\bigotimes_{j=0}^{2N-1} \mathscr{H}_j\right)$ the set

$$\mathsf{ProbComb}\left(\bigotimes_{j=0}^{2N-1} \mathscr{H}_j\right) = \left\{ R^{(N)} \geq 0 \mid \exists S^{(N)} \in \mathsf{DetComb}\left(\bigotimes_{j=0}^{2N-1} \mathscr{H}_j\right) : R^{(N)} \leq S^{(N)} \right\}. \tag{2}$$

It is possible to prove that any operator $R^{(N)} \in \mathsf{DetComb}\left(\bigotimes_{j=0}^{2N-1} \mathscr{H}_j\right)$ is the Choi operator of some sequential network of N channels, or, equivalently, of some causal channel $\mathscr{R}^{(N)}$ [9, 3]. The minimal Stinespring dilation of the channel in terms of the Choi operator is given by [11]

$$\mathscr{R}^{(N)}(\rho) = \mathrm{Tr}_A[V\rho V^\dagger] \qquad V = \left(I_{odd} \otimes \sqrt{R^{(N)\tau}}\right)(|I_{odd}\rangle\rangle \otimes I_{even}), \tag{3}$$
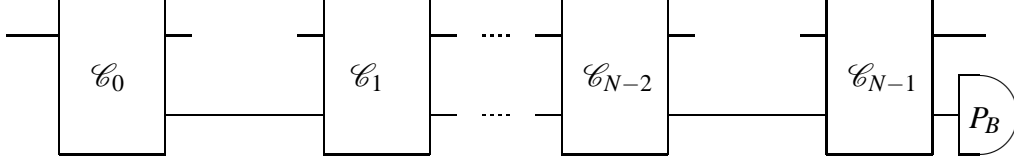
FIGURE 2. *N*-instrument: sequence of *N* channels followed with postselection on the last ancilla.

where $\mathscr{H}_{odd} = \bigotimes_{k=0}^{N-1} \mathscr{H}_{2k+1}$, $\mathscr{H}_{even} = \bigotimes_{k=0}^{N-1} \mathscr{H}_{2k}$, τ denotes transposition w.r.t. a fixed orthonormal basis, $\mathscr{H}_A = \mathsf{Supp}\left(R^{(N)\tau}\right)$ is the minimal ancilla space, $|I_{odd}\rangle\rangle$ is the unnormalized maximally entangled state on $\mathscr{H}_{odd}^{\otimes 2}$, and V is an isometry from $\mathscr{H}_{even}$ to $\mathscr{H}_{odd} \otimes \mathscr{H}_A$.

1.2. Quantum *N*-instruments

Let Ω be a measurable space and $\sigma(\Omega)$ be its σ-algebra of events. A quantum *N*-instrument $R^{(N)}$ on $\bigotimes_{j=0}^{2N-1} \mathscr{H}_j$ is an operator-valued measure that associates to any event $B \in \sigma(\Omega)$ an *N*-comb $R_B^{(N)} \in \mathsf{ProbComb}\left(\bigotimes_{j=0}^{2N-1} \mathscr{H}_j\right)$, and satisfies the normalization

$$R_\Omega^{(N)} \in \mathsf{DetComb}\left(\bigotimes_{j=0}^{2N-1} \mathscr{H}_j\right) . \qquad (4)$$

Theorem 1 (Dilation of *N*-instruments) *For any N-instrument $R^{(N)}$ on $\bigotimes_{j=0}^{2N-1} \mathscr{H}_j$ there exist a deterministic N-comb $S^{(N)} \in \mathsf{DetComb}\left(\bigotimes_{j=0}^{2N-1} \mathscr{H}_j'\right)$ with $\mathscr{H}_j' = \mathscr{H}_j$ for $j = 0, \ldots, 2N-2$, and $\mathscr{H}_{2N-1}' = \mathscr{H}_{2N-1} \otimes \mathscr{H}_A$, and a POVM P on the ancilla $\mathscr{H}_A$ such that*

$$R_B^{(N)} = \mathrm{Tr}_A\left[S^{(N)} \left(I_0 \otimes \cdots \otimes I_{2N-1} \otimes P_B^\tau\right)\right] \qquad \forall B \in \sigma(\Omega) , \qquad (5)$$

τ denoting transposition w.r.t. a fixed orthonormal basis.

The meaning of the theorem is that a quantum *N*-instrument can be always achieved by a network of *N* channels with postselection induced by the measurement on an ancilla exiting from the *N*-th channel, as in Fig. 2.

Proof. Diagonalize $R_\Omega^{(N)}$ as $R_\Omega^{(N)} = \sum_{i=1}^r \lambda_i |\phi_i\rangle\langle\phi_i|$, and take $\mathscr{H}_A = \mathsf{Supp}\left(R_\Omega^{(N)\tau}\right) = \mathsf{Span}\{|\phi_i^*\rangle \mid i = 1, \ldots, r\}$, $|\phi_i^*\rangle := \sum_n \langle n|\phi_i\rangle^* |n\rangle$. Consider the purification $S^{(N)} = |R_\Omega^{(N)\frac{1}{2}}\rangle\rangle\langle\langle R_\Omega^{(N)\frac{1}{2}}|$ where $|R_\Omega^{(N)\frac{1}{2}}\rangle\rangle = \sum_i \sqrt{\lambda_i} |\phi_i\rangle |\phi_i^*\rangle \in \left(\bigotimes_{j=0}^{2N-1} \mathscr{H}_j\right) \otimes \mathscr{H}_A$. By con-

struction, $S^{(N)}$ is a deterministic comb in $\mathsf{DetComb}\left(\bigotimes_{j=0}^{2N-1}\mathscr{H}_j'\right)$. Now define the POVM P by $P_B = \left[R_\Omega^{(N)}\right]^{-\frac{1}{2}} R_B^{(N)} \left[R_\Omega^{(N)}\right]^{-\frac{1}{2}}$, where $\left[R_\Omega^{(N)}\right]^{-\frac{1}{2}}$ is the inverse of $R_\Omega^{(N)\frac{1}{2}}$ on its support. It is immediate to check that for any event $B \in \sigma(\Omega)$ we have $R_B^{(N)} = \mathrm{Tr}_A[S^{(N)}\,(I_0 \otimes \cdots \otimes I_{2N-1} \otimes P_B^\tau)]$. ∎

This theorem is similar in spirit to Ozawa's dilation theorem for quantum instruments [12]. The important difference here that P is a POVM on a finite-dimensional ancilla space, rather than a von Neumann measurement in infinite dimension.

1.3. Quantum N-testers

An N-tester $T^{(N)}$ is an $(N+1)$-instrument where the first and last Hilbert spaces, $\mathscr{H}_0$ and $\mathscr{H}_{2N+1}$, respectively, are one-dimensional. Accordingly, we can shift back by one unit the numeration of Hilbert spaces, so that, if $B \in \sigma(\Omega)$ is an event, then $T_B^{(N)}$ is an operator on $\bigotimes_{j=0}^{2N-1}\mathscr{H}_j$. With this shifting, the normalization of the tester is given by

$$
\begin{aligned}
&T_\Omega^{(N)} = I_{2N-1} \otimes \Xi^{(N-1)} \\
&\mathrm{Tr}_{2k-2}[\Xi^{(k)}] = I_{2k-3} \otimes \Xi^{(k-1)} \qquad k = 2,\ldots,N \\
&\mathrm{Tr}_0[\Xi^{(1)}] = 1\ ,
\end{aligned}
\tag{6}
$$

with $\Xi^{(k)} \in \mathsf{Lin}\left(\bigotimes_{j=0}^{2k-2}\mathscr{H}_j\right)$.

A tester represents a quantum network starting with a state preparation and finishing with a measurement on the ancilla. When such a network is connected to a network of N quantum operations as in Fig. 3, the only outputs are measurement outcomes.
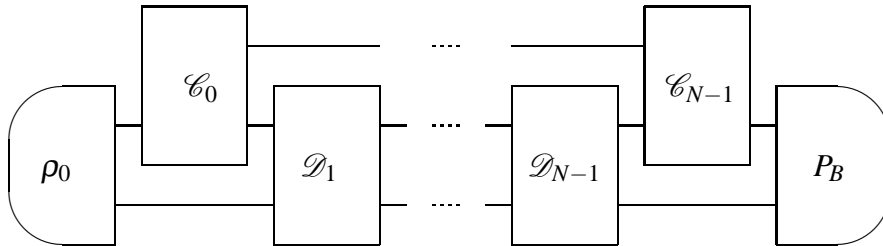
FIGURE 3. Testing a network of N quantum operations $(\mathscr{C}_i)_{i=0}^{N-1}$. The N-tester consists in the preparation of an input state ρ_0, followed by channels $\{\mathscr{D}_1,\ldots,\mathscr{D}_{N-1}\}$, and a final measurement P_B.

Precisely, if the comb of the measured network is $R^{(N)} \in \mathsf{ProbComb}\left(\bigotimes_{j=0}^{2N-1}\mathscr{H}_j\right)$, then the probabilities of any event are given by the generalized Born rule [1, 13]

$$
p(B|R^{(N)}) = \mathrm{Tr}[T_B^{(N)\tau} R^{(N)}] \qquad \forall B \in \sigma(\Omega)\ .
\tag{7}
$$

For deterministic combs $R^{(N)} \in \mathsf{DetComb}\left(\otimes_{j=0}^{2N-1} \mathscr{H}_j\right)$ the probabilities sum up to one:

$$p(\Omega|R^{(N)}) = \mathrm{Tr}[T_\Omega^{(N)\tau} R^{(N)}] = 1 .\tag{8}$$

Clearly, since $T^{(N)\tau}$ is also a tester, the Born rule can be written in the familiar way without the transpose. However, here we preferred to write probabilities in terms of the combs $R^{(N)}$ and $T_B^{(N)}$ of the measured and measuring networks, respectively. In fact, the Born rule is nothing but a particular case of link product [1], and the transpose appears as the signature of the interlinking of the two networks.

Proposition 1 (Decomposition of N-testers [5]) *Let $T^{(N)}$ be a quantum N-tester on $\otimes_{j=0}^{2N-1} \mathscr{H}_j$, and consider the ancilla space $\mathscr{H}_A = \mathsf{Supp}\left(T_\Omega^{(N)\tau}\right)$. Let $\mathscr{S}$ be the linear supermap from $\mathsf{ProbComb}\left(\otimes_{j=0}^{2N-1} \mathscr{H}_j\right)$ to $\mathsf{St}(\mathscr{H}_A)$ given by*

$$\mathscr{S}(R^{(N)}) = \left[T_\Omega^{(N)\tau}\right]^{\frac{1}{2}} R^{(N)} \left[T_\Omega^{(N)\tau}\right]^{\frac{1}{2}}\tag{9}$$

and P be the POVM on $\mathscr{H}_A$ defined by

$$P_B = \left[T_\Omega^{(N)}\right]^{-\frac{1}{2}} T_B^{(N)} \left[T_\Omega^{(N)}\right]^{-\frac{1}{2}} .\tag{10}$$

The supermap $\mathscr{S}$ transforms deterministic combs into normalized states of the ancilla. The probabilities of events are given by

$$p(B|R^{(N)}) = \mathrm{Tr}[T_B^{(N)\tau} R^{(N)}] = \mathrm{Tr}[P_B^\tau \mathscr{S}(R^{(N)})] .\tag{11}$$

This proposition reduces any measurement on an input quantum network to a measurement on a suitable state, which is obtained by linear transformation of the input comb. As we will see in the following, this simple result has very strong consequences in quantum estimation.

Proof. If $R^{(N)}$ is in $\mathsf{DetComb}\left(\otimes_{j=0}^{2N-1} \mathscr{H}_j\right)$, then $\mathrm{Tr}[\mathscr{S}(R^{(N)})] = \mathrm{Tr}[T_\Omega^{(N)\tau} R^{(N)}] = 1$, having used Eq. (8). Eq. (11) is an obvious consequence of the definitions of $\mathscr{S}$ and P. ∎

Proposition 1 reduces the discrimination of two networks to the discrimination of two states. This allows us to define an operational notion of distance between networks [5], whose meaning is directly related to minimum error discrimination:

$$\left\|R^{(N)} - R^{(N)'}\right\|_{op} = \max_{T_\Omega^{(N)}} \left\|\left[T_\Omega^{(N)\tau}\right]^{\frac{1}{2}} \left(R^{(N)} - R^{(N)'}\right) \left[T_\Omega^{(N)\tau}\right]^{\frac{1}{2}}\right\|_1 ,\tag{12}$$

with $\|A\|_1 = \mathrm{Tr}|A|$. Remarkably, the above norm can be strictly greater than the diamond (cb) norm of the difference $\mathscr{R}^{(N)} - \mathscr{R}^{(N)'}$ of the two multipartite channels [5]. This means that a scheme such as in Fig. 3 can achieve a strictly better discrimination than a parallel scheme where a multipartite entangled state is fed in the unknown channel and a multipartite measurement is performed on the output.

2. COVARIANT QUANTUM NETWORKS

2.1. Covariant N-combs

Let $\mathbf{G}$ be a group, acting on the Hilbert space $(\mathcal{H}_j)_{j=0}^{2N-1}$ via the a unitary representation $\{U_{g,j} \mid g \in \mathbf{G}\}$. Denote by $\mathcal{U}_{g,j}$ the map $\mathcal{U}_{g,j}(\rho) = U_{g,j}\rho U_{g,j}^\dagger$. Suppose that the causal channel $\mathscr{R}^{(N)}$ from $\mathsf{St}(\otimes_{k=0}^{N-1}\mathcal{H}_{2k})$ to $\mathsf{St}(\otimes_{k=0}^{N-1}\mathcal{H}_{2k+1})$ is *covariant*, namely

$$\mathscr{R}^{(N)} \circ \left(\bigotimes_{k=0}^{N-1} \mathcal{U}_{g,2k} \right) (\rho) = \left(\bigotimes_{k=0}^{N-1} \mathcal{U}_{g,2k+1} \right) \circ \mathscr{R}^{(N)}(\rho) \, . \tag{13}$$

Then the corresponding comb, which we call *covariant* either, satisfies the commutation property

$$\left[R^{(N)}, \bigotimes_{k=0}^{N-1} (U_{g,2k+1} \otimes U_{g,2k}^*) \right] = 0 \qquad \forall g \in \mathbf{G} \, . \tag{14}$$

For covariant combs, the minimal dilation of the memory channel $\mathscr{R}^{(N)}$ given by Eq. (3) satisfies the commutation relation

$$\left[\left(\bigotimes_{k=0}^{N-1} U_{g,2k+1} \right) \otimes U_{g,A} \right] V = V \left(\bigotimes_{k=0}^{N-1} U_{g,2k} \right) \, , \tag{15}$$

where $U_{g,A}$ is the compression of $\left(\otimes_{k=0}^{N-1}(U_{g,2k+1}^* \otimes U_{g,2k}) \right)$ to the invariant subspace $\mathcal{H}_A = \mathsf{Supp}\left(R^{(N)\tau} \right)$.

2.2. Covariant N-instruments and testers

Suppose that the group $\mathbf{G}$ acts on the outcome space Ω. For $B \in \sigma(\Omega)$, denote by $gB := \{g\omega \mid \omega \in B\}$. A covariant N-instrument $R^{(N)}$ is defined by the property

$$R_{gB}^{(N)} = \left(\bigotimes_{k=0}^{N-1} (\mathcal{U}_{g,2k+1} \otimes \mathcal{U}_{g,2k}^*) \right) \left(R_B^{(N)} \right) \, . \tag{16}$$

A covariant tester is simply a covariant N-instrument with one-dimensional $\mathcal{H}_0$ and $\mathcal{H}_{2N-1}$ and with all remaining labels shifted back by unit. We now suppose that $\mathbf{G}$ is compact and Ω is transitive, i.e. for any pair $\omega_1, \omega_2 \in \Omega$ there always exists a group element $g \in \mathbf{G}$ such that $\omega_2 = g\omega_1$.

Theorem 2 (Structure of covariant N-instruments/testers) *Let $\mathbf{G}$ be compact and Ω be transitive, with normalized Haar measure $\mathrm{d}\omega$. Let $\omega_0 \in \Omega$ be a point of Ω, and let $\mathbf{G}_0 = \{g \in \mathbf{G} \mid g\omega_0 = \omega_0\}$ be the stabilizer of ω_0. Let $\sigma : \Omega \to \mathbf{G}$ be a measurable section,*

such that $\omega = \sigma_\omega \omega_0$. If $R^{(N)}$ is a covariant instrument, then there exists a non-negative operator $D_0^{(N)}$ such that

$$R_B^{(N)} = \int_B d\omega \, D_\omega^{(N)}$$

$$D_\omega^{(N)} = \left(\bigotimes_{k=0}^{N-1} (U_{\sigma_\omega, 2k+1} \otimes U_{\sigma_\omega, 2k}^*) \right) D_0^{(N)} \left(\bigotimes_{k=0}^{N-1} (U_{\sigma_\omega, 2k+1} \otimes U_{\sigma_\omega, 2k}^*) \right)^\dagger \qquad (17)$$

$$\left[D_0^{(N)}, \bigotimes_{k=0}^{N-1} (U_{g_0, 2k+1} \otimes U_{g_0, 2k}^*) \right] = 0 \qquad \forall g_0 \in \mathbf{G}_0 \, .$$

Proof. Simple generalization of the standard proof for covariant POVMs [14].

For a covariant N-instrument/tester, Eq. (16) implies the commutation

$$\left[R_\Omega^{(N)}, \bigotimes_{k=0}^{N-1} (U_{g, 2k+1} \otimes U_{g, 2k}^*) \right] = 0 \qquad \forall g \in \mathbf{G} \, . \qquad (18)$$

This implies additional group structure in the results of Theorem 1 and Proposition 1. In particular, for covariant testers, the map $\mathscr{S} : \mathsf{ProbComb}\left(\bigotimes_{j=0}^{2N-1} \mathscr{H}_j \right) \to \mathsf{St}(\mathscr{H}_A)$ is a *covariant supermap*:

$$\mathscr{S} \circ \left(\bigotimes_{k=0}^{N-1} (\mathscr{U}_{g, 2k+1}^* \otimes \mathscr{U}_{g, 2k}) \right) \left(R^{(N)} \right) = U_{g,A} \, \mathscr{S}(R^{(N)}) \, U_{g,A}^\dagger \, , \qquad (19)$$

where $U_{g,A}$ is the compression of $\bigotimes_{k=0}^{N-1} \left(U_{g, 2k+1}^* \otimes U_{g, 2k} \right)$ to the invariant subspace $\mathscr{H}_A = \mathsf{Supp}\left(T_\Omega^{(N)\tau} \right) \subseteq \bigotimes_{j=0}^{2N-1} \mathscr{H}_j$.

3. OPTIMAL COVARIANT ESTIMATION OF QUANTUM NETWORKS

Let $\left\{ R_\omega^{(N)} \in \mathsf{DetComb}\left(\bigotimes_{j=0}^{2N-1} \mathscr{H}_j \right) \mid \omega \in \Omega \right\}$ be a family of quantum networks parametrized by ω. We now want to find the optimal tester to estimate the parameter ω. For simplicity, we consider here the special case in which $\Omega \equiv \mathbf{G}$, for some compact group $\mathbf{G}$, and $R_g^{(N)}$ has the form

$$R_g^{(N)} = \left(\bigotimes_{k=0}^{N-1} (U_{g, 2k+1} \otimes U_{g, 2k}^*) \right) R_0^{(N)} \left(\bigotimes_{k=0}^{N-1} (U_{g, 2k+1} \otimes U_{g, 2k}^*) \right)^\dagger \qquad (20)$$

Let $c(\hat{g}, g)$ be a cost function, penalizing the differences between the estimated parameter $\hat{g}$ and the true one g. Suppose that $c(\hat{g}, g)$ is left-invariant, namely $c(h\hat{g}, hg) =$

$c(\hat{g}, g) \ \forall h \in \mathbf{G}$. The optimal estimation is then given by the tester $T^{(N)}$ that minimizes the average cost

$$\langle c \rangle = \int_\mathbf{G} \mathrm{d} g \ \int_\mathbf{G} c(\hat{g}, g) \ \mathrm{Tr}[T_{\mathrm{d}\hat{g}}^{(N)\tau} R_g^{(N)}] \ , \tag{21}$$

where $\mathrm{d} g$ is the normalized Haar measure, and $\int_\mathbf{G} f(\hat{g}) \ \mathrm{Tr}\left[T_{\mathrm{d}\hat{g}}^{(N)\tau} R^{(N)}\right]$ denotes integration of f against the scalar measure $\mu_B = \mathrm{Tr}[T_B^{(N)\tau} R^{(N)}]$. An alternative notion of optimality is the minimization of the worst-case cost

$$c_{wc} = \max_{g \in \mathbf{G}} \left(\int_\mathbf{G} c(\hat{g}, g) \ \mathrm{Tr}[T_{\mathrm{d}\hat{g}}^{(N)\tau} R_g^{(N)}] \right) \ . \tag{22}$$

However, it it easy to prove that in the covariant setting it is sufficient to consider covariant testers, for which the average and worst-case cost coincide:

Theorem 3 *There exists a covariant tester $T_B^{(N)} = \int_B \mathrm{d} g \ D_g^{(N)}$, with density*

$$D_g^{(N)} = \left(\bigotimes_{k=0}^{N-1} (U_{g,2k+1}^* \otimes U_{g,2k}) \right) D_0^{(N)} \left(\bigotimes_{k=0}^{N-1} (U_{g,2k+1}^* \otimes U_{g,2k}) \right)^\dagger \tag{23}$$

that is optimal both for the average and worst-case cost.

Proof. The standard averaging argument [14]: if $T^{(N)}$ is an optimal tester, then the tester $\overline{T^{(N)}}$ defined by $\overline{T_B^{(N)}} = \int_\mathbf{G} \mathrm{d} h \bigotimes_{k=0}^{N-1} (\mathscr{U}_{h,2k+1}^* \otimes \mathscr{U}_{h,2k}) \left(T_{h^{-1}B}^{(N)} \right)$ is covariant and has the same average and worst-case cost as $T^{(N)}$. Moreover, for any covariant tester, the average and worst-case cost coincide. ∎

4. APPLICATIONS

4.1. Optimal estimation of group transformations with N copies

Suppose we have at disposal N uses of a black box performing the unknown group transformation U_g, and that we want to find the optimal network for estimating g. In this case the parametric family of networks is $R_g^{(N)} = (|U_g\rangle\rangle\langle\langle U_g|)^{\otimes N}$, where $|U_g\rangle\rangle := (U_g \otimes I)|I\rangle\rangle$, $|I\rangle\rangle = \sum_{i=1}^d |i\rangle|i\rangle$. Using Proposition 1 and Eq. (19), the optimal estimation on these networks is reduced to the optimal estimation on the ancilla states $\rho_g = \mathscr{S}\left(R_g^{(N)}\right) = U_{g,A}\mathscr{S}\left(R_0^{(N)}\right) U_{g,A}^\dagger$, with $R_0^{(N)} = (|I\rangle\rangle\langle\langle I|)^{\otimes N}$. Since the ancilla space is an invariant subspace of $\bigotimes_{j=0}^{2N-1} \mathscr{H}_j$ and the representation $U_{g,A}$ is a sub-representation of $\bigotimes_{k=0}(U_{g,2k+1} \otimes I_{2k})$, it is clear that the minimum cost in the estimation is lower bounded by the minimum cost achievable in a parallel scheme, where the unitary $U_g^{\otimes N} \otimes I_{ref}$ is applied to a multipartite entangled state in $\mathsf{St}(\bigotimes_{k=1}^N \mathscr{H}_k \otimes \mathscr{H}_{ref})$, with $\mathscr{H}_{ref}$ suitable reference space. In this way the optimal estimation is reduced to the optimal parallel estimation of Ref. [8].

4.2. Optimal alignment of reference frames with multi-round protocols

Two distant parties Alice and Bob, who lack a shared reference frame, can try to establish one by sending suitable physical systems, such as clocks and gyroscopes for time and orientation references, respectively. In the quantum scenario, the role of elementary clocks and gyroscopes is played by spin $1/2$ particles, and it has been shown that the optimal protocol using N particles in a single round of quantum communication from Alice to Bob has a r.m.s. error scaling to zero as $1/N$ (with suitable constants) for both for clock synchronization [15] and Cartesian axes alignment [16]. However, the optimal protocol for establishing reference frames with many rounds of quantum communication and arbitrary amount of classical communication has been not analyzed yet. In principle, an adaptive strategy might improve the alignment, if not by changing the scaling with N, at least by improving the constant. With the formalism of covariant combs and testers, however, it is rather straightforward to prove that this is not the case.

Let us consider the general case in which the mismatch between Alice's and Bob's reference frames is represented by an unknown element g of some group of physical transformations $\mathbf{G}$. The unitary (projective) representation in the Hilbert spaces of quantum systems yields the passive transformation of states due to the change from Alice's to Bob's viewpoint: a single-particle state that is $|\psi^{(A)}\rangle$ is Alice's reference frame becomes $|\psi^{(B)}\rangle = U_g|\psi^{(A)}\rangle$ in Bob's one, a single-particle operator $O^{(A)}$ becomes $O^{(B)} = U_g O^{(A)} U_g^\dagger$, and a single-particle operation $\mathscr{C}^{(A)}$ becomes $\mathscr{C}^{(B)} = \mathscr{U}_g \mathscr{C}^{(A)} \mathscr{U}_g^\dagger$. Consider a protocol with $2r$ rounds of quantum communication (r rounds from Alice to Bob and r from Bob to Alice) with q_i quantum particles exchanged per round. We also allow an unbounded amount of classical communication, represented by the exchange of $\mathbf{G}$-invariant systems prepared in classical (diagonal) states. The goal of the protocol is to give the best possible estimate $\hat{g}$ of the mismatch g. Notice that, since Alice and Bob are not restricted in sending classical data, we can imagine without loss of generality that the estimate $\hat{g}$ is produced by Bob (if it were produced by Alice, she could always transmit this classical information to Bob). The protocol is then represented by the interlinking of two networks of quantum operations: *i)* Alice's network is a deterministic r-comb $R^{(r,A)} \in \mathsf{DetComb}\left(\mathscr{H}_{A\to B} \otimes \mathscr{H}_{B\to A} \otimes \mathscr{H}_C\right)$, where $\mathscr{H}_{A\to B}$ ($\mathscr{H}_{B\to A}$) is the Hilbert space of all particles sent from Alice to Bob (from Bob to Alice), and $\mathscr{H}_C$ is the Hilbert space of the invariant systems used for classical communication, and *ii)* Bob's network is an r-tester $T_{d\hat{g}}^{(r,B)}$ on the same Hilbert spaces. When switching to Bob's reference frame, all Alice's operations are conjugated by unitaries, and her comb becomes

$$R_g^{(r,B)} = \left(U_g^{\otimes N_{A\to B}} \otimes U_g^{*\otimes N_{B\to A}} \otimes I_C\right) R^{(r,A)} \left(U_g^{\otimes N_{A\to B}} \otimes U_g^{*\otimes N_{B\to A}} \otimes I_C\right). \qquad (24)$$

where $N_{A\to B}$ ($N_{B\to A}$) is the number of particles traveling from Alice to Bob (from Bob to Alice). Notice that we have the identity I_C on the classical systems, since classical communication (strings of bits) is invariant under changes of reference frame. Therefore, for any left-invariant cost function $c(\hat{g}, g)$ we are in the case of covariant network estimation treated before. The estimation of g from the networks $R_g^{(r,B)}$ is then reduced to the estimation of g from the states $\rho_g = \mathscr{S}(R_g^{(r,B)}) = U_{g,A}\rho_0 U_{g,A}^\dagger$, where $U_{g,A}$ is a

sub-representation of $U_g^{\otimes N_{A\to B}} \otimes U_g^{*\otimes N_{B\to A}} \otimes I_C$. For $\mathbf{G} = U(1)$ and $\mathbf{G} = \mathbb{SU}(2)$ U_g and U_g^* are equivalent representations (up to global phases), hence this is exactly the same estimation that can be achieved by sending $N_{A\to B} + N_{B\to A}$ particles in a single round. Even for groups for which U_g and U_g^* are not equivalent (such as $\mathbb{SU}(d)$), one can achieve the same estimation precision in a single round by sending $N_{A\to B}$ particles and $N_{B\to A}$ charge-conjugate particles from Alice to Bob. This proves that anyway there is no advantage in using more than one round of quantum communication, and that classical communication is completely useless.

REFERENCES

1. G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. **101**, 060401 (2008).
2. G. Chiribella, G. M. D'Ariano, and P. Perinotti, Europhys. Lett. **83**, 30004 (2008).
3. G. Chiribella, G. M. D'Ariano, and P. Perinotti, in preparation.
4. G. Gutoski and J. Watrous, in *Proc. of the 39th Annual ACM Symposium on Theory of Computation*, 565 (2007).
5. G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. **101**, 180501 (2008).
6. G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. **101**, 180504 (2008).
7. W. van Dam, G. M. D'Ariano, A. Ekert, C. Macchiavello, M. Mosca, Phys. Rev. Lett. **98**, 090501 (2007).
8. G. Chiribella, G. M. D'Ariano, and M. F. Sacchi, Phys. Rev. A **72**, 042338 (2005).
9. D. Kretschmann and R. F. Werner, Phys. Rev. A. **72**, 062323 (2005).
10. T. Eggeling, D. Schlingemann and R. F. Werner, Europhys. Lett. **57**, 782-788 (2002).
11. G. Chiribella, P. Perinotti, and G. M. D'Ariano, arXiv:0810.3211.
12. M. Ozawa, J. Math. Phys. **25** (1984), 79.
13. M. Ziman, Phys. Rev. A **77**, 062112 (2008).
14. A. S. Holevo *Probabilistic and Statistical Aspects of Quantum Theory*, North-Holland, Amsterdam, 1982.
15. V. Bužek, R. Derka, and S. Massar, Phys. Rev. Lett. **82**, 2207 (1999).
16. G. Chiribella, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, Phys. Rev. Lett. **93**, 180503 (2004).