Quantum Comparison

Erika Andersson[1] * Anthony Chefles[2] † Igor Jex[3] ‡ Stephen M. Barnett[1] §

[1] *Department of Physics, University of Strathclyde, Glasgow G4 0NG, UK*
[2] *Department of Physical Sciences, University of Hertfordshire, Hatfield AL10 9AB, Hertfordshire, UK*
[3] *Department of Physics, FNSPE, Czech Technical University Prague, Břehová 7, 115 19 Praha, Czech Republic*

Abstract. We investigate how to determine, with minimal resources and maximal reliability, whether the states of two or more quantum systems, or whether two or more given unitary transformations, are identical or not. We treat error-free (unambiguous) comparison, as well as minimum-error and minimum-cost comparison strategies. We show that it is possible to realise comparison strategies using only linear networks and particle detectors. This is of great significance for practical applications of quantum comparison.

Keywords: Quantum information, linear optical networks, measurement theory

In this contribution, we investigate how to compare the states of two or more quantum systems [1, 2], as well as how to compare two or more unitary transformations acting on quantum systems [3]. With minimal resources and maximal reliability, we want to determine whether the states, or the unitary transformations, are identical or different. We treat both unambiguous, that is, error-free comparison, and comparison strategies where errors in the results are allowed. Error-free here means that we aim to obtain answers which are guaranteed to be correct as often as possible. When errors are allowed, we show how to construct optimal comparison strategies, minimising either the error probability or the cost of making an error.

When comparing classical systems, a straightforward way to proceed is to measure a number of observables of each system individually, and then compare the measurement results. To compare the states of quantum systems is less straightforward, since the results of quantum measurements are of statistical nature. In addition, the measurement usually introduces a nonnegligible disturbance of the measured state. In quantum mechanics, simultaneous measurements of non-commuting observables are restricted. If only a single copy of each quantum system is available, we cannot measure all observables of the systems precisely, and thus cannot compare the states of quantum systems in the same way as classical systems. Based on measurements of the individual quantum systems, it is in general only possible to make statistical predictions of their similarities and differences. If an ensemble of identically prepared systems is available for each of the compared quantum states, the result will be more reliable.

It is, however, possible to obtain reliable information about whether the states of two or more quantum systems are identical or not, even when only a single copy of each state is available. We can understand this by thinking about two quantum systems, prepared in unknown pure states. If the individual pure quantum states are the same, the overall state will always be symmetric. Therefore, if their state is found to be not symmetric, in this case antisymmetric, we can infer with certainty that the individual states of the systems must have been different. If we find the state of the systems in the symmetric subspace, the individual states may have been either identical or different.

When comparing the states of N quantum systems, prepared in unknown pure states, we can also obtain information about how many of these could have had identical states. The symmetric subspace will correspond to no certain information, exactly as for two quantum systems. In addition to this, there will be a number of other subspaces, invariant under permutations and unitary transformations on the individual systems, depending on the number of particles and their internal dimensions. These subspaces are connected with more detailed knowledge about differences among the quantum systems. As an example, when comparing the states of four qubit systems, there are two non-symmetric subspaces, which are connected with at most three of the qubit states being identical, and with at most two of the qubit states being identical. As before, if the overall state of the four qubits is found in the totally symmetric subspace, the states may or may not have been identical.

A definite answer that the states of the quantum systems are not identical is always possible to obtain, as described above, whereas a definite answer that they are identical will not always be possible to obtain. It is found that, if a definite answer that the states are identical is to be possible, the states have to be members of a known set of states, where at least one of the states is linearly independent of the other states.

It is also possible to allow for errors in the answer, making the error as small as possible. Different errors may also have different costs attached to them, and in this case, one is led to consider minimum-cost comparison strategies. Comparing the states of the quantum systems is now equivalent to distinguishing between two density matrices, ρ_S for when the states are all identical, and ρ_D for when they are not all identical. The problem of distinguishing between two density matrices with minimum error or minimum cost was solved already by Helstrom in his pioneering work [4]. The method can be employed in any comparison situation. Using prior information about the states, if this is available, one has to form the density matrices ρ_S and ρ_D. The Helstrom minimum-error mea-

* erika@phys.strath.ac.uk
† anthony.chefles@herts.ac.uk
‡ igor.jex@fjfi.cvut.cz
§ steve@phys.strath.ac.uk

surement can then be understood as a measurement in the eigenbasis of the operator $p_S\rho_S - p_D\rho_D$, where p_S and p_D are the prior probabilities for the states to be identical or different. The minimum-cost measurement is a modification of the minimum-error measurement, depending on the costs for the errors.

An optimal quantum state comparison strategy is usually a collective measurement, in an entangled basis, on the involved quantum systems. Nevertheless, it is possible to realise error-free quantum state comparison, albeit with less than ideal efficiency, using only linear elements and particle detectors, for example with a linear optical network. The realisation utilises a symmetric multiport, and certain click patterns at the outputs would indicate a difference in the internal states of the photons. Also minimum-error comparison may, at least in some cases, be realised in this way. This is of great significance for practical applications of quantum state comparison, including quantum digital signatures [5] and quantum fingerprinting [6].

We also investigate how to compare unitary transformations acting on quantum states, with only a single application of each transformation. It is reasonable to assume that any comparison strategy would involve the action of the transformations to be compared upon some test state, followed by a generalised measurement of the test state. To be more specific, we have to construct a network where each transform occurs only once, feed a test quantum state through the network, and then measure the output state.

Different realisations for comparing unitary transformations are derived and compared with respect to their efficiency. With a linear interferometric setup, it is possible to compare arbitrarily many unitary transforms using only one test particle, such as a photon. Using a symmetric multiport, the test particle is split in as many paths as there are transforms to compare, and the transforms are applied, one in each of the paths. The paths are then recombined, and depending on in which output port the test particle exits, we can infer if the unitary transforms were different. Another strategy makes use of an entangled test state. An efficient entangled test state is a totally antisymmetric state, such as a two-particle singlet state. This state is invariant if the same unitary transformation is applied to each individual particle. Therefore, we can infer that the unitary transformations were different, if the test state is found not to be in the antisymmetric state afterwards. For one run of the comparison strategy, this strategy is more efficient than using a non-entangled test state, thus demonstrating the benefit of entanglement. On the other hand, the linear setup has the advantage of being easier to realise experimentally, which is important for potential applications.

We have investigated how to compare the states of quantum systems, and also how to compare unitary transformations to each other. Quantum comparison may be used in quantum information applications, and from this point of view it is interesting to note that a linear setup often may be used for the realisation of quantum comparison.

References

[1] S. M. Barnett, A. Chefles, and I. Jex. Comparison of two unknown pure quantum states. *Phys. Lett. A* **307**, 189, 2003.

[2] I. Jex, E. Andersson, and A. Chefles. Comparing the states of many quantum systems. *LANL e-print* quant-ph/0305120, 2003.

[3] E. Andersson, I. Jex, and S. M. Barnett. Comparison of unitary transforms. *J. Phys. A: Math. Gen.* **36**, 1, 2003.

[4] C. W. Helstrom, *Quantum Detection and Estimation Theory*, Academic Press, New York, 1976.

[5] D. Gottesman and I. Chuang. Quantum Digital Signarures. *LANL e-print* quant-ph/0105032, 2001.

[6] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.* **87**, 167902, 2001.