Programmable projective measurement with linear optics

***Ulysse Chabaud*[1], *Eleni Diamanti*[1], *Damian Markham*[1], *Elham Kashefi*[1,2], *Antoine Joux*[3]**

[1]*Laboratoire d'Informatique de Paris 6, CNRS, Sorbonne Université, 4 place Jussieu, 75005 Paris*
[2]*School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh, EH8 9AB*
[3]*Chaire de Cryptologie de la Fondation SU, Sorbonne Université, Institut de Mathématiques de Jussieu – Paris Rive Gauche, CNRS, INRIA, Université Paris Diderot, Campus Pierre et Marie Curie, 4 place Jussieu, 75005 Paris*

We present a scheme for a programmable projective measurement using M program states, and its implementation in linear optics.

We cast our problem as follows, illustrated in Fig. 1. One has M program registers each prepared in the state $|\psi\rangle$ corresponding to the choice of measurement basis, and an input register prepared in some state $|\phi\rangle$. Our aim is to output a classical bit corresponding to a projective measurement, where 0 represents the outcome $|\psi\rangle$ and 1 represents its complement. In an ideal measurement the result 0 would occur with probability $|\langle\phi|\psi\rangle|^2$. However, this is impossible for finite M [1]. We can thus only ever approximate perfect measurements. In our case we parameterise this approximation by ε, requiring that the result of 0 is returned with probability ε-close to $|\langle\phi|\psi\rangle|^2$. Our scheme achieves this optimally in terms of how ε scales with M, under the condition that if the input is ϕ, the measurement always returns 0. The size of the linear optical circuit we propose to implement this scales as $M \log M$, with $O(M \log M)$ classical side processing.

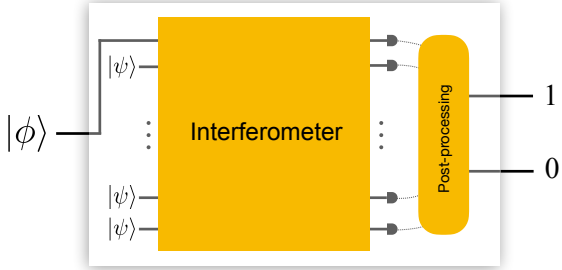

Figure 1: Programmable projective measurement. Given an input $|\phi\rangle$ and M program registers, we apply some transformation, independent of the choice of measurement basis $|\psi\rangle$, and measure the output. The measurement outcomes are then post-processed to retrieve the projective measurement statistics.

Our scheme can be viewed as an extension of the swap test to the instance where one state is supplied many times. From this perspective one can imagine a single quantum optical chip which can be programmed to perform any projective measurement, the input and program states being encoded in single photons.

Our interest is not so much to explore the computational notion of quantum programs or how efficiently to do so, but rather the separation of measurement choice to a quantum state. In the cryptographic setting, remote programming of measurements with non-orthogonal states can be used to test the behaviour of a remote party. This is the essence, for example, behind the delegated blind verified quantum computation in [2]. At a fundamental level these programmable measurements separate as much as possible the choice of measurement basis and the bulk of the physical apparatus carrying out the measurement, which could be interesting in probing foundational questions of quantum measurement, for example in tests of contextuality where macroscopic information about which measurement is being carried out leads to loopholes [3].

References

[1] M. A. Nielsen, and I. L. Chuang, "Programmable quantum gate arrays", Physical Review Letters **79**, 2 (1997).
[2] J. F. Fitzsimons, and E. Kashefi, "Unconditionally verifiable blind quantum computation", Physical Review A **96**, 1 (2017).
[3] A. Winter, "What does an experimental test of quantum contextuality prove or disprove?", Journal of Physics A: Mathematical and Theoretical **47**, 42 (2014).