Exploring Quantum Process Calculi via barbs and contexts

Gabriele Tedeschi

Le tecnologie quantistiche promettono numerosi vantaggi sia in termini di efficienza di calcolo, grazie a computer quantistici collegati in rete, sia in termini di garanzie di sicurezza nella comunicazione. La disponibilità di tecniche per la verifica di sistemi quantistici distribuiti e concorrenti è quindi di grande rilevanza e interesse, data la complessità e il costo dei sistemi impiegati. I risultati controintuitivi della meccanica quantistica mettono però in discussione l'adeguatezza di tecniche preesistenti, e impongono lo sviluppo di nuovi modelli e tecniche formali di cui sia comprovata l'esattezza rispetto alla teoria fisica di base.

Diversi calcoli di processi e semantiche sono stati proposti per modellare e verificare protocolli quantistici quali il teletrasporto e lo scambio di chiavi BB84. Tali proposte sono state raramente confrontate fra loro e comparate alle predizioni della meccanica quantistica, e nessuna di esse si è affermata come standard.

In questo lavoro presentiamo un nuovo calcolo, LqCCS, e analizziamo l'equivalenza di processi sotto la lente delle bisimulazioni basate su contesti. Grazie a un sistema di tipi lineare, LqCCS astrae dalle assunzioni implicite nelle proposte precedenti, permettendo di codificarle e confrontarle su un terreno comune.

Riducendo l'equivalenza fra processi al concetto di indistinguibilità secondo contesti appropriati, dimostriamo che la "bisimilarità probabilistica", usata in molte delle proposte precedenti, non è adeguata al caso quantistico. Il motivo di questa differenza rispetto al caso classico risiede nei limiti alle capacità di osservazione che la meccanica quantistica prescrive, ma che vengono ignorati in tale relazione di equivalenza.

Proponiamo dunque una nuova "bisimilarità quantum", nella quale i limiti osservazionali siano presi in considerazione, estendendoli dall'ambito dei dati quantistici a quello dei processi che li manipolano e comunicano. La tesi propone infine un'analisi preliminare della nuova bisimilarità e alcune sue tecniche dimostrative, mostrando come sia adatta a modellare e verificare casi d'uso reali.