Robust self-testing of quantum systems and device-independent uncertainty relations

Quantum mechanics was developed to explain some experimental observations which stood in stark contradiction to the pre-quantum physics, e.g. the photoelectric effect, the black-body radiation or the internal structure of the atom. While it is extremely successful at explaining these microscopic phenomena, some aspects of it severely challenge our classical intuition.

Classically we are used to the idea that objects have properties and that the act of observation simply reveals them to us. For example if I open a letter from my bank to find out that my new secret PIN code is 1234, I will conclude that it must have had exactly the same value even before I opened the envelope. This is precisely what the classical intuition tells me.

In the quantum world, however, measurement is an active process and measurement outcomes only come into existence when we start looking. In other words properties of objects arise as a consequence of the observation. Things become even more unusual when we deal with two (or more) quantum particles in a strongly correlated state. Then, performing a measurement on one of them immediately affects the state of the other, even if they are separated by astronomical distances. This is precisely Einstein's "spooky-action-at-a-distance", which led him to the conclusion that the theory of quantum mechanics must be in some sense incomplete.

After decades of theoretical and experimental efforts we now believe that quantum mechanics is the correct theory (at least in certain regimes). Einstein's "spooky-action-at-a-distance" became more acceptable, when we realised that although indeed there is an influence that travels faster than the speed of light, it does not carry any information. On the other hand, it gives rise to correlations stronger than what classical physics allows, a phenomenon known as Bell nonlocality.

This is obviously an exciting discovery, as it allows us to set up experiments which falsify classical physics. While the first such experiments were performed in 1980s, it is only last year (2015) that a few groups around the world managed to perform Bell tests in a "loophole-free" manner, i.e. in a way that eliminates all possible doubts.

As if the possibility of falsifying classical physics was not exciting enough, stronger-than-classical correlations allow us to say even more. If we assume that the world is governed by quantum mechanics, which at the moment is the only reasonable candidate, then observing certain extreme correlations allows us to essentially deduce what happens at the microscopic level. This phenomenon, which allows a purely classical user to investigate an inherently quantum device, goes under the name of self-testing of quantum systems. On top of providing an intimate link between the macroscopic experimental statistics and the microscopic, quantum world, it has direct practical applications: it paves the way to device-independent quantum information processing, which allows a classical user to harness the power of quantum devices, even if the inner workings are not completely known. In fact, we could even allow the adversary to fabricate the devices and our security will not be compromised. This means that when quantum technologies reach commercial maturity, they will have a huge impact on security and privacy, which are crucial for further development of our increasingly connected society.

The goal of this proposal is to develop new and reliable self-testing procedures, which will allow classical users to characterise complex quantum devices. In particular, we are interested in methods which remain correct under realistic conditions, i.e. in the presence of noise or signal loss, which is a necessary feature for any practical applications. We will do it by extending a recently proposed method, which reduces the self-testing task to a purely mathematical problem of operator inequalities. In the second part of the proposal, we will look at randomness generated by such untrusted devices. This is precisely what is known as device-independent uncertainty relations, which can then be used to analyse security of device-independent quantum cryptographic protocols.