Quantum algorithms help to effectively detect symmetries and why it is important: a proposal

Jose Hernandez[1], Olga Kosheleva[2], and Vladik Kreinovich[1]
Departments of [1]Computer Science and [2]Teacher Education
University of Texas at El Paso, 500 W. University, El Paso, TX 79968, USA
jlhernandez24@miners.utep.edu, olgak@utep.edu, vladik@utep.edu

What are symmetries and why they are important. One of the main objectives of science and engineering is to predict future events – and to make sure that these future events are beneficial for us. Why are we able to predict future events?

For example, why are we sure that if we drop a pen, it will fall down with an acceleration of 9.81 m/sec^2? Because this experiment was repeated many times, at different locations on Earth, at different orientations, at different moments of time – and the result was always the same. In other words, when we shift in space or in time or rotate, the phenomenon remains the same.

Similarly, why do we believe that Ohm's law will hold in the students' lab? Because this law held in many cases before, so it has been shown that the corresponding phenomena do not change under shifts and rotations. In physics, such transformations – under which the physical phenomena do not change – are known as *symmetries*. Symmetries do not have to be geometric: e.g., if we change the sign of all electric charges, all phenomena remain the same.

So the very possibility to predict future events is based on symmetries. In line with this, many new fundamental physical theories are now proposed not in terms of differential equations – as it was in Newton's time – but by describing the corresponding symmetries, and differential equations follow from these symmetries.

Moreover, for many theories that were originally proposed in the form of differential equations – Maxwell's equations for electrodynamics, Schroedinger's equation for quantum physics, Einstein's General Relativity equations describing space-time, and many others – it is now known that these equations can be uniquely determined by the corresponding symmetries.

It is therefore important to detect symmetries in data. Because of the above, the way to analyze a new phenomenon is to detect the corresponding symmetries.

Such a detection is not easy. With traditional – non-quantum – computers, the only known algorithms for detecting symmetries require time which grows exponentially with data size – and is thus not feasible: since, e.g., for even a small size $n = 500$, already 2^{500} is larger than the lifetime of the Universe.

This is true even in the simplest case, when we have a function f that maps bit sequences into bit sequences, and symmetry means invariance under some shift: for some s, we have $f(x) = f(x \oplus s)$ for all x, where $\oplus$ means component-wise addition modulo 2 (i.e., exclusive or).

Quantum computing can help. In 1994, Daniel Simon provided a quantum algorithm that solves the above simple version of this problem in feasible time. This algorithm has been generalized to other possible symmetries – and it helped Peter Shor come up with a feasible quantum algorithm for breaking the RSA encryption – the main encryption that makes current communications secure.

What we propose. Simon's algorithm originated in quantum computing – and this is what motivated its generalizations. Because of the above-described importance of symmetries in data analysis, we propose to try to generalize it to physical situations beyond quantum computing, situations when we are trying to make sense of the new data.