Opinions Libres
le blog d'Olivier Ezratty

Is there a Moore's law for quantum computing?

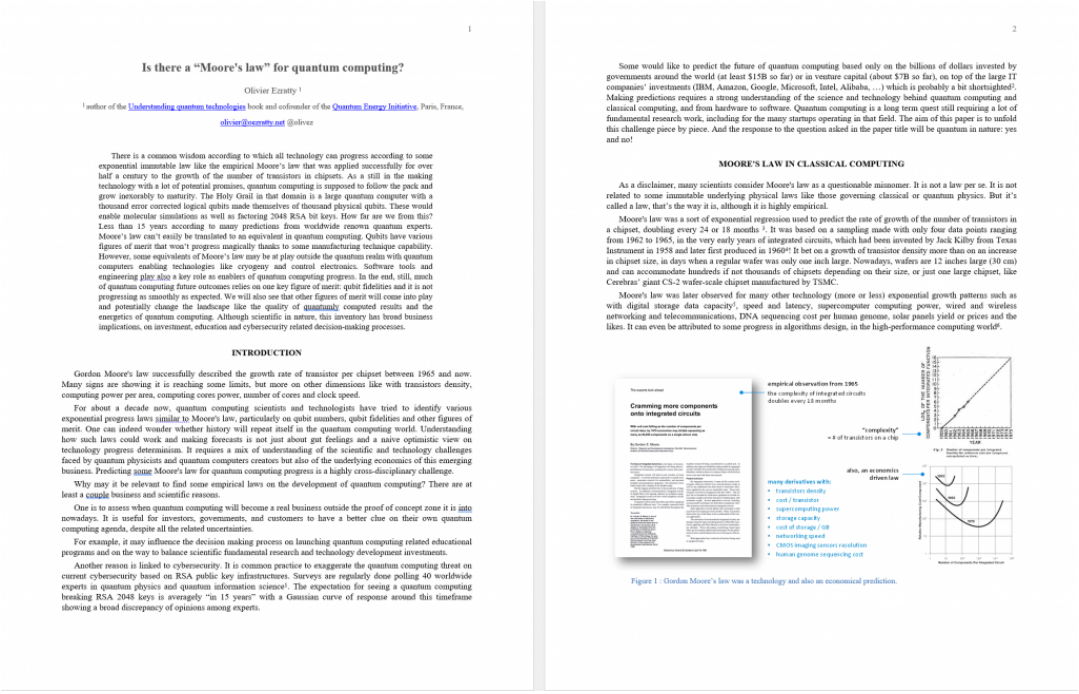
I'm continuing a series of broad review papers on quantum computing after **Disentangling quantum emulation and quantum simulation** that I published in January 2023.

In this new essay, I try to answer a very commonplace question or wisdom: will Moore's law be also applicable for quantum computing. The answer is: yes and no! And in quantum computing, there's an ongoing challenge to assemble both quality qubits and a large number of these qubits. And there's so much entanglement between various figures of merits and quantum+classical technologies plus such a zoo of different types of qubits that a simplistic exponential regression like Moore's law is hard to make. On top of that, Moore's law was rapidly applicable for chipsets that were of practical use and contributed to the birth and rapid expansion of the personal computer market, then to the Internet and the smartphone and all things connected from supercomputers, cloud data-centers down to the tiniest connected objects. Here, with quantum computers, we have not passed the threshold of real utility and the economical drive that did fuel Moore's law is not yet at play.

Here's the abstract from the paper:

"*There is a common wisdom according to which many technologies can progress according to some exponential law like the empirical Moore's law that was validated for over half a century with the growth of transistors number in chipsets. As a still in the making technology with a lot of potential promises, quantum computing is supposed to follow the pack and grow inexorably to maturity. The Holy Grail in that domain is a large quantum computer with thousands of errors corrected logical qubits made themselves of thousands, if not more, of physical qubits. These would enable molecular simulations as well as factoring 2048 RSA bit keys among other use cases taken from the intractable classical computing problems book. How far are we from this? Less than 15 years according to many predictions. We will see in this paper that Moore's empirical law cannot easily be translated to an equivalent in quantum computing. Qubits have various figures of merit that won't progress magically thanks to some new manufacturing technique capacity. However, some equivalents of Moore's law may be at play inside and outside the quantum realm like with quantum computers enabling technologies, cryogeny and control electronics. Algorithms, software tools and engineering also play a key role as enablers of quantum computing progress. While much of quantum computing future outcomes depends on qubit fidelities, it is progressing rather slowly, particularly at scale. We will finally see that other figures of merit will come into play and potentially change the landscape like the quality of computed results and the energetics of quantum computing. Although scientific and technological in nature, this inventory has broad business implications, on investment, education and cybersecurity related decision-making processes.*".

You can **download it here** or on **arXiv**.



Is there a “Moore's law” for quantum computing?

Olivier Ezratty [1]

[1] author of the Understanding quantum technologies book and cofounder of the Quantum Energy Initiative, Paris, France, olivier@oezratty.net @olivez

There is a common wisdom according to which all technology can progress according to some exponential immutable law like the empirical Moore's law that was applied successfully for over half a century to the growth of the number of transistors in chipsets. As a still in the making technology with a lot of potential promises, quantum computing is supposed to follow the pack and grow inexorably to maturity. The Holy Grail in that domain is a large quantum computer with a thousand error corrected logical qubits made themselves of thousand physical qubits. These would enable molecular simulations as well as factoring 2048 RSA bit keys. How far are we from this? Less than 15 years according to many predictions from worldwide renown quantum experts. Moore's law can't easily be translated to an equivalent in quantum computing. Qubits have various figures of merit that won't progress magically thanks to some manufacturing technique capability. However, some equivalents of Moore's law may be at play outside the quantum realm with quantum computers enabling technologies like cryogeny and control electronics. Software tools and engineering play also a key role as enablers of quantum computing progress. In the end, still, much of quantum computing future outcomes relies on one key figure of merit: qubit fidelities and it is not progressing as smoothly as expected. We will also see that other figures of merit will come into play and potentially change the landscape like the quality of quantumly computed results and the energetics of quantum computing. Although scientific in nature, this inventory has broad business implications, on investment, education and cybersecurity related decision-making processes.

INTRODUCTION

Gordon Moore's law successfully described the growth rate of transistor per chipset between 1965 and now. Many signs are showing it is reaching some limits, but more on other dimensions like with transistors density, computing power per area, computing cores power, number of cores and clock speed.

For about a decade now, quantum computing scientists and technologists have tried to identify various exponential progress laws similar to Moore's law, particularly on qubit numbers, qubit fidelities and other figures of merit. One can indeed wonder whether history will repeat itself in the quantum computing world. Understanding how such laws could work and making forecasts is not just about gut feelings and a naive optimistic view on technology progress determinism. It requires a mix of understanding of the scientific and technology challenges faced by quantum physicists and quantum computers creators but also of the underlying economics of this emerging business. Predicting some Moore's law for quantum computing progress is a highly cross-disciplinary challenge.

Why may it be relevant to find some empirical laws on the development of quantum computing? There are at least a couple business and scientific reasons.

One is to assess when quantum computing will become a real business outside the proof of concept zone it is into nowadays. It is useful for investors, governments, and customers to have a better clue on their own quantum computing agenda, despite all the related uncertainties.

For example, it may influence the decision making process on launching quantum computing related educational programs and on the way to balance scientific fundamental research and technology development investments.

Another reason is linked to cybersecurity. It is common practice to exaggerate the quantum computing threat on current cybersecurity based on RSA public key infrastructures. Surveys are regularly done polling 40 worldwide experts in quantum physics and quantum information science[1]. The expectation for seeing a quantum computing breaking RSA 2048 keys is averagely “in 15 years” with a Gaussian curve of response around this timeframe showing a broad discrepancy of opinions among experts.

Some would like to predict the future of quantum computing based only on the billions of dollars invested by governments around the world (at least $15B so far) or in venture capital (about $7B so far), on top of the large IT companies' investments (IBM, Amazon, Google, Microsoft, Intel, Alibaba, …) which is probably a bit shortsighted[2]. Making predictions requires a strong understanding of the science and technology behind quantum computing and classical computing, and from hardware to software. Quantum computing is a long term quest still requiring a lot of fundamental research work, including for the many startups operating in that field. The aim of this paper is to unfold this challenge piece by piece. And the response to the question asked in the paper title will be quantum in nature: yes and no!

MOORE'S LAW IN CLASSICAL COMPUTING

As a disclaimer, many scientists consider Moore's law as a questionable misnomer. It is not a law per se. It is not related to some immutable underlying physical laws like those governing classical or quantum physics. But it's called a law, that's the way it is, although it is highly empirical.

Moore's law was a sort of exponential regression used to predict the rate of growth of the number of transistors in a chipset, doubling every 24 or 18 months [3]. It was based on a sampling made with only four data points ranging from 1962 to 1965, in the very early years of integrated circuits, which had been invented by Jack Kilby from Texas Instrument in 1958 and later first produced in 1960[4]. It bet on a growth of transistor density more than on an increase in chipset size, in days when a regular wafer was only one inch large. Nowadays, wafers are 12 inches large (30 cm) and can accommodate hundreds if not thousands of chipsets depending on their size, or just one large chipset, like Cerebras' giant CS-2 wafer-scale chipset manufactured by TSMC.

Moore's law was later observed for many other technology (more or less) exponential growth patterns such as with digital storage data capacity[5], speed and latency, supercomputer computing power, wired and wireless networking and telecommunications, DNA sequencing cost per human genome, solar panels yield or prices and the likes. It can even be attributed to some progress in algorithms design, in the high-performance computing world[6].

Figure 1 : Gordon Moore's law was a technology and also an economical prediction.

Thanks a lot to Michel Kurek (Multiverse), Jean Senellart (Quandela), Marco Fellous-Asiani (Centre of New Technologies University of Warsaw), Reja Yehia (ICFO), Vincent Elfving (Pasqal) and Vivien Londe (Microsoft) who provided me feedback on the paper and to the many others I bothered when preparing it!

Feedback welcome as usual ? !

Cet article a été publié le 29 mars 2023 et édité en PDF le 29 mars 2023.