Number 112 January 2018

ERCIM NEWS

www.ercim.eu

Special theme:

Quantum Computing

Also in this issue:

Research and Innovation:

Computers that negotiate on our behalf

ERCIM News is the magazine of ERCIM. Published quarterly, it reports on joint actions of the ERCIM partners, and aims to reflect the contribution made by ERCIM to the European Community in Information Technology and Applied Mathematics. Through short articles and news items, it provides a forum for the exchange of information between the institutes and also with the wider scientific community. This issue has a circulation of about 6,000 printed copies and is also available online.

ERCIM News is published by ERCIM EEIG
BP 93, F-06902 Sophia Antipolis Cedex, France
Tel: +33 4 9238 5010, E-mail: contact@ercim.eu
Director: Philipp Hoschka, ISSN 0926-4981

Contributions
Contributions should be submitted to the local editor of your country

ERCIM News online edition
http://ercim-news.ercim.eu/

Next issue
October 2017, Special theme: Digital Humanities

Subscription
Subscribe to ERCIM News by sending an email to en-subscriptions@ercim.eu or by filling out the form at the ERCIM News website: http://ercim-news.ercim.eu/

Contents

JOINT ERCIM ACTIONS

SPECIAL THEME

The special theme section "Quantum Computing" has been coordinated by Jop Briët (CWI) and Simon Perdrix (CNRS, LORIA)

RESEARCH AND INNOVATION

This section features news about research activities and innovative developments from European research institutes

EVENTS, IN BRIEF

Reports

Announcements

In Brief

Foreword from the President

ERCIM is a great organisation with a lot of potential. I am proud that I am the third CWI director since ERCIM's foundation in 1989 who has become a President of ERCIM, after Cor Baayen and Gerard van Oortmerssen. I will outline my ideas on ERCIM's strategy below.

The number of ERCIM Members has declined in recent years. I want to focus more on our roots, what we are, and how we started: as an association with a focus on research institutes in the fields of both informatics and mathematics. Of course, leading research universities are also welcome to become ERCIM members, as we have university members now. Our focus will distinguish us from other organisations.

Further, experience has taught us that it is not good to limit the number of members per country to one. This led to artificial consortia that fell apart at some point. The model of one organisation or consortium per country has failed. We can and should have more ERCIM members per country. For instance, not only CWI could be a member in the Netherlands but also TNO. The Board of Directors should see it as a joint effort to recruit new members.

I want to maintain ERCIM's achievements, namely:
- *ERCIM News.* This magazine is widely appreciated and is becoming ever more important.
- *Awards.* In addition to the Cor Baayen Award for the more fundamentally orientated research, we could establish an innovation award, which would be a good supplement and which is in line with the increased importance of valorisation.
- *Programs* such as the ERCIM Alain Bensoussan Fellowship programme and the PhD program we are currently working on to develop young talent.
- *The Working Groups.* I want to revive the former working groups by setting up new working groups on hot topics such as blockchain. This will allow us to really benefit from our mutual collaboration within ERCIM by coordi-

Jos Baeten Elected President of ERCIM AISBL

Jos Baeten (left) and Domenico Laforenza.

The General Assembly of the ERCIM AISBL, held on 24 October in Lisbon, unanimously elected Jos Baeten, general director of Centrum Wiskunde & Informatica (CWI) in the Netherlands as its new President for a period of two years as of January 2018. Jos Baeten succeeds Domenico Laforenza from the Institute for Informatics and Telematics (IIT) of the Italian National Research Council (CNR) who served as President of ERCIM since January 2014.

Jos Baeten has a PhD in mathematics from the University of Minnesota (1985). From 1991 to 2015, he was professor of computer science at the Technische Universiteit Eindhoven (TU/e). In addition, from 2010 to 2012 he was professor of systems engineering at TU/e. As of October 2011, he is the general director of Centrum Wiskunde & Informatica (CWI) in Amsterdam, the national research institute for mathematics and computer science in the Netherlands. Since January 2015, he is part-time professor in theory of computing at the Institute of Logic, Language and Computation of the University of Amsterdam. He is well-known as a researcher in model-based engineering, in particular in process algebra.

Jos Baeten expressed his gratitude to Domenico for his dedication to ERCIM during his four years of presidency. "The festive 25th anniversary celebration of ERCIM at CNR, where Domenico welcomed over a hundred guests from academia, industry and politics, his efforts in approaching ERCIM and Informatics Europe to cooperate, and his remarkably inspiring speeches were highlights during Domenico's presidency", Jos says. Domenico began his activity in ERCIM in 1993, contributing to the creation of the ERCIM Parallel Processing Network (PPN). He has represented CNR on the Board of Directors since 2006 and will continue representing CNR after his presidency.

nating research in those new fields. Working groups have a limited life span, focusing on temporary, topical, short-term research that responds to new and current developments. In terms of collaboration, it's important that researchers, not just directors, will be able to find each other. This is also the idea behind exchanging researchers in our Fellowships and PhD programme. Added value can be found in new research areas.

ERCIM also successfully coordinates EU projects. This task is carried out by the EEIG office, originally conceived as a service for the members. I will strongly encourage the members to make use of it and cooperate through EU funded research projects.

For our leading role in Europe, lobbying is also important. I would like to have more contact with Brussels. We must act together, ERCIM, Informatics Europe, and, for instance, the ACM Europe Council and EIT Digital. The cooperating organisations must become members of advisory bodies in the European Commission, such as the CONNECT Advisory Forum for Research and Innovation in ICT in Horizon 2020. I commit myself to recruiting members and to reinforce contacts with the EC. Together, as an association of organisations, we will endeavour to exert more influence on the policies of the EU. For instance: to be heard at the creation of the European Innovation Council (EIC) and to be involved in the preparations for FP9, the programme that follows H2020. We need to be putting more effort into this area, and I intend to make this my personal mission.

In addition to lobbying, collaboration is also important. For instance, I believe that the annual Informatics Europe meeting should continue to coincide with ERCIM meetings. This requires much consultation and coordination. The other semi-annual meeting of ERCIM should also be for researchers, and not just the directors.

One of ERCIM's unique features is our combination of informatics and mathematics, and these areas are becoming increasingly important for Europe. My personal opinion is that Europe is not doing well: ICT companies are being sold to the US and China, which means that we no longer have control over our data. I think this is an unhealthy trend; citizens must have control over their own data and at least know who has them. We do not necessarily have to own our data but we must be able to control who has or uses them. Together, we need to work to benefit all European citizens. Together, we can conduct research that will bring us the innovations of the future – for the short and the long term. It is vital for the future of Europe that we are actively involved in helping to shape future innovations: that we do not lose the innovation capacity, as we are already losing ground to emerging economies and other world powers. China and the USA are out in front at the moment, and I think Europe must have a leading role, certainly in the field of long-term research for future innovations.

With ERCIM, I hope that we can contribute to this goal.

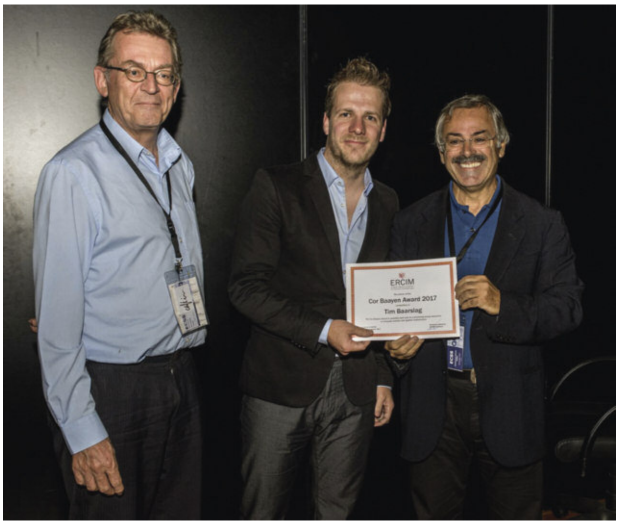
Jos Baeten,
General Director of CWI and President of ERCIM AISBL

Tim Baarslag Winner of the 2017 Cor Baayen Young Researcher Award

Tim Baarslag from CWI was selected as the winner of the 2017 ERCIM Cor Baayen Award, in a very tough competition with 15 finalists. The award committee recognises Tim's skills and the results that he has achieved. His enthusiasm for internationally oriented research cooperation, his talent for recognising the potential use of mathematical tools, and his cooperative skills make him a young researcher of outstanding quality.

Tim has obtained some very impressive scientific results. His PhD dissertation was awarded cum laude, which is conferred to less than 5% of doctoral candidates at the Delft University of Technology. His dissertation won the 2014 Victor Lesser Distinguished Dissertation Runner-up Award in recognition of an exceptional and highly impressive dissertation in the area of autonomous agents and multiagent systems. He was shortlisted for the 2014 Artificial Intelligence Dissertation Award, which recognises the best doctoral dissertations in the general area of artificial intelligence. His dissertation is also published by the Springer Theses "the best of the best" series, which recognises outstanding PhD research by selecting the very best PhD theses from around the world for their scientific excellence and high impact on research.

Tim has made a real scientific impact with his work since embarking on his PhD in 2010. He has already published over 40 articles, in collaboration with 35 researchers from 17 international institutes and five industrial partners. His research is published in the highest ranking publications in his field, including the top journal Artificial Intelligence and top conferences such as IJCAI, ECAI, AAAI and AAMAS. His research on how artificial intelligence can help negotiate better deals for humans was recently featured in Science. His achievements point to great promise for his future work and for others who build on it.



Tim Barslaag (center) receiving the award from the ERCIM president Domenico Laforenza (right) and ERCIM president-elect Jos Baeten.

ERCIM Cor Baayen Award 2017

Winner:
Tim Baarslag (CWI), nominated by Eric Pauwels (CWI)

Honorary mention:
Fabrice Ben Hamouda-Guichoux (IBM Research), nominated by David Pointcheval (Inria)

Finalists:
- Markus Borg (RI.SE SICS), nominated by Jakob Axelsson (RI.SE SICS)
- Frederik Diederichs (Fraunhofer IAO), nominated by Anette Weisbecker Fraunhofer (IAO)
- Hadi Fanaee Tork (University of Oslo), nominated by Alípio Jorge (INESC)
- Eemil Lagerspetz (University of Helsinki), nominated by Tuomo Tuikka (VTT)
- Pierre Lairez (Inria), nominated by Bertrand Braunschweig (Inria)
- Britta Meixner (CWI), nominated by Pablo Cesar (CWI)
- Iason Oikonomidis (ICS-FORTH), nominated by Antonis Argyros (ICS-FORTH)
- Giulio Rossetti (University of Pisa), nominated by Fosca Giannotti (CNR)
- Ville Salo (University of Turku), nominated by Tuomo Tuikka (VTT)
- Anna Ståhl, RI.SE SICS, nominated by Kristina Höök (RI.SE SICS)
- João Tiago Medeiros Paulo (INESC TEC and University of Minho), nominated byJosé Pereira (INESC TEC and University of Minho)
- Vassilis Vassiliades (Inria), nominated by Chris Christodoulou (University of Cyprus)
- Daniel Weber (Fraunhofer IGD), nominated by Arjan Kuijper (Fraunhofer IGD).

Since 2016, Tim Baarslag has been working as a researcher at CWI, where he studies negotiation strategies for smart energy cooperatives. He collaborates closely with key smart grid stakeholders to develop his negotiation results into user-adaptable energy trading technology. His negotiation algorithms support energy trading in a sustainable energy community 'Schoonschip' in Amsterdam as part of the ERA-Net Grid-Friends project. He has recently received a personal 'Veni' grant for young, talented researchers from The Netherlands Organisation for Scientific Research (NWO).

As the lead developer of the negotiation environment "Genius", he contributed to an international platform for research on automated negotiation agents, which is downloaded more than 100 times a week and is used by more than 20 research institutes all over the world, including Harvard University and Massachusetts Institute of Technology (MIT). Additionally, he is part of the organising team of the International Automated Negotiating Agent Competition (ANAC), which has had more than 100 international participants and is held in conjunction with the leading artificial and multi-agent conferences in his field (AAMAS and IJCAI). Not only have his results and the competition provided a state-of-the-art repository of automated negotiators, they also continue to steer the automated negotiation research agenda.

Tim's work provides a unique blend of mathematically optimal results and application-driven research with a strong potential for knowledge utilisation. In collaboration with MIT CSAIL and the University of Southampton, he has developed new mathematical models that enable essential next steps for conducting privacy negotiations feasibly. Furthermore, together with multiple UK partners including The Open University, Tim helps to design Internet of Things solutions that enable negotiable data access for future data marketplaces. His research has influenced the negotiation architecture that will be used to assess and mitigate privacy trade-offs in existing Internet of Things applications and platforms.

Tim was the first to untangle the connection between negotiation performance and opponent learning. In acknowledgement of the originality of this work, he received the Best Paper Award (out of 101 papers) at the 2013 IEEE/WIC/ACM International Conference on Intelligent Agent Technology. Moreover, he was the first to combine a number of theoretical results in search theory, such as optimal stopping and Pandora's Problem, to formulate new and tested negotiation strategies. This resulted in the Best Paper Award (out of 122 papers) for his results on optimal negotiation strategies during the 2015 IEEE/WIC/ACM International Conference on Intelligent Agent Technology. Moreover, a negotiating agent that successfully applied his open source dissertation framework won The 2013 International Automated Negotiating Agents Competition (ANAC).

Tim is also actively engaged in the broader computing community and highly involved with the most eminent researchers within computer science and mathematics. In 2016, he was selected as one of 200 highly talented, preeminent young researchers in mathematics and computer scientists from over 50 countries for the Heidelberg Laureate Forum scholarship. In 2017, he was selected from over 300 applicants as an outstanding early career individual in the field of computing to take part in the ACM Future of Computing Academy and attend the 2017 Turing Award ceremony, in an effort to support and foster the next generation of computing professionals.

See also Tim's article "Computers that Negotiate on Our Behalf" on page 34 in this issue.

Link:
ERCIM Cor Baayen Award:
https://www.ercim.eu/human-capital/cor-baayen-award

ERCIM “Alain Bensoussan” Fellowship Programme

ERCIM offers fellowships for PhD holders from all over the world. Topics cover most disciplines in Computer Science, Information Technology, and Applied Mathematics. Fellowships are of 12 months duration, spent in one ERCIM member institute. Fellowships are proposed according to the needs of the member institutes and the available funding.

Application deadlines for the next rounds: 30 April and 30 September 2018

More information: http://fellowship.ercim.eu/

HORIZON 2020 Project Management

A European project can be a richly rewarding tool for pushing your research or innovation activities to the state-of-the-art and beyond. Through ERCIM, our member institutes have participated in more than 80 projects funded by the European Commission in the ICT domain, by carrying out joint research activities while the ERCIM Office successfully manages the complexity of the project administration, finances and outreach.

The ERCIM Office has recognized expertise in a full range of services, including identification of funding opportunities, recruitment of project partners, proposal writing and project negotiation, contractual and consortium management, communications and systems support, organization of attractive events, from team meetings to large-scale workshops and conferences, support for the dissemination of results.

How does it work in practice?
Contact the ERCIM Office to present your project idea and a panel of experts will review your idea and provide recommendations. If the ERCIM Office expresses its interest to participate, it will assist the project consortium as described above, either as project coordinator or project partner.

Please contact:
Philippe Rohou, ERCIM Project Group Manager
philippe.rohou@ercim.eu

ERCIM Established Working Group on Blockchain Technology

ERCIM established a new Working Group Blockchain Technology to study the potential of this technology for a range of application fields in industry and public administration. First chairperson of the Working Group is Wolfgang Prinz from the Fraunhofer Institute for Applied Information Technology FIT.

Following up on the ERCIM workshop on Blockchain Technology in May 2017 in Paris, ERCIM now established the new Working Group Blockchain Technology. It has become evident that blockchain technology is being investigated in various areas of computer science research. That includes peer-to-peer networks, distributed systems, cryptography, algorithms for consensus building and validation as well as for modeling processes and business models. In addition to these basic technologies, the Working Group will also study applications in relevant fields like Internet-of-Things, supply chains, energy and Smart Grid, the media, the medical field and the financial industry.

“We want to establish blockchain technology as a new field of computer science research in Europe. Our working group will strengthen the young community of European blockchain researchers and foster interdisciplinary cooperation and exchange”, Wolfgang Prinz stated.

The Working Group will also establish a roadmap documenting ongoing research and open research questions in the rapidly moving field of blockchain technology. Another element of its mission is to build a blockchain research community that will be able to successfully initiate and carry out collaborative research projects on a European level.

For its first year the group is planning several meetings and editorial projects in accordance with the objectives of the group. The next major event will be a workshop organized by members of the group, to be held May 8-9, 2018 in Amsterdam, in conjunction with the ERCIM spring meetings.

Researchers from ERCIM member institutions and other organizations are cordially invited to join the new ERCIM working group Blockchain Technology.

Link:
ERCIM Blockchain WG:
https://wiki.ercim.eu/wg/BlockchainTechnology/

Please contact:
For additional information please contact the workgroup chair Wolfgang Prinz
Fraunhofer FIT, Germany
wolfgang.prinz@fit.fraunhofer.de

Introduction to the Special Theme

Quantum Computation and Information

by Jop Briët (CWI) and Simon Perdrix (CNRS, LORIA)

For more than a century now, we've understood that we live in a quantum world. Even though quantum mechanics cannot be ignored during the development of atomic scale components of everyday computers, the computations they perform are governed, like the Turing machine, by the laws of classical Newtonian mechanics. But the most striking and exotic features of quantum mechanics, superposition and entanglement, currently play no part in every-day information processing. This is about to change – and in some specialised applications, already has. In academia, the field of quantum computation has been growing explosively since its inception in the 1980s and the importance of these devices is widely recognised by industry and governments. Big players in the tech industry like IBM and Google frequently announce that they have built yet a larger rudimentary quantum computation device and in 2016 the European Commission launched a one-billion Euro Flagship Initiative on Quantum Technologies.

The development of this technology has both a hardware and a software component, both of which have been the subjects of intense research for the past few decades. On the hardware side, past efforts went into controlling and storing small numbers (5-10) of qubits, the fundamental building blocks for quantum computation. The current state of the art is that this can be done for arrays of about fifty qubits. Although a seemingly modest scale, this is where things become very interesting, because quantum systems of 50-100 qubits cannot be simulated on our current classical computers and so hold the possibility of harnessing a computational power we have not seen before. A more long-term goal (in the order of a few decades) is to scale-up further to millions of qubits. This scale is what the NSA is worried about, because quantum computers of this size could break most modern-day cryptography.

Hardware, however, is not much good without interesting software. Some important research areas on this side of the development include:

- *Quantum simulation*, which includes research on applications of medium-sized quantum computers. Potential application areas include chemistry and materials science.
- *Algorithms and complexity,* which explores what larger-scale quantum computers could do. Think for instance about machine learning, search and optimisation and tackling number-theoretic problems (relevant to cryptography).
- *Cryptography*, important because larger scale quantum computers will break our current cryptosystems, but also hold the key for future cryptosystems.
- *Quantum software framework,* including quantum programming languages, together with formal and logical methods to ease the use of quantum computers and understand the fundamental structures of quantum information processing.
- *Quantum information science in general,* which is to provide the mathematical theory behind quantum information processing and is important for the development of error correction schemes, understanding counterintuitive quantum phenomena and the physical theory behind the hardware.

The articles in this special theme offer a more detailed look into the complexities of some of the above-mentioned aspects of the emerging paradigm shift currently happening in computation. Below you will find lightning-fast introductions to the basic concepts appearing in the articles.

Basic features of quantum computation

Qubits and superpositions

The basic building block for classical computation is the bit, a physical system that can be toggled between one of two possible states, 0 and 1. For quantum computers, this building block is fundamentally different. It is the qubit, short for quantum bit. A qubit is a physical system that can be in a sort of intermediate state given by one of the infinitely many possible superpositions of two basis states. If the two basis states are represented by two-dimensional row vectors (1,0) and (0,1), then a superposition is a complex Euclidean unit vector of the form (x,y) where x and y are complex numbers, referred to as probability amplitudes, whose absolute values squared sum to 1. A measurement of the qubit results in finding it in the first or second state with probability $|x|^2$ or $|y|^2$, respectively. Toggling of quantum states can be done via linear, length-preserving operations, in other words, unitary transformations. A measurement performed after a unitary operation is also referred to as doing a measurement in a different basis. Whereas the state of n classical bits can be represented by an n-bit string, the state of an n-qubit system is in general given by a superposition of 2^n basis states: a complex 2^n-dimensional Euclidean unit vector. The observation that n-qubit states require an exponential number of parameters to be described is what makes simulating quantum-mechanical systems hard to do on classical computers. It is also one of the key features of quantum mechanics that gives quantum computers their power.

Entanglement
Arguably the most striking features of quantum mechanics is entanglement, which manifests itself when two or more quantum systems are measured locally in one of two or more possible bases. As an argument against quantum, it was observed by Einstein, Podolsky and Rosen that compound systems allow superpositions that can result in measurement statistics that defy classical explanation. Celebrated work of Bell later showed that one can actually test this feature experimentally using what is nowadays referred as a Bell test. The most basic example of such a test can be cast as a game involving two players, Alice and Bob, and a referee. The referee picks two bits at random and sends these to Alice and Bob, respectively. Without communicating, and thus without knowing the other's bit value, the players each return a binary answer to the referee. They win the game if the sum of the answers modulo 2 equals the product of the questions. A simple calculation shows that if they players are constrained by the laws of classical physics, then they can win this game with probability at most 3/4. However, by performing local measurements on a two-qubit "EPR pair", the players can produce a probability distribution over their answer pairs with which they win with probability roughly 0,85!

Quantum algorithms
Quantum algorithms consist of a carefully chosen sequence of unitary transformations that are applied one by one to a register of qubits, followed in the end by a measurement to determine an output. A crucial property of unitary transformations is that they can cause cancellations among the probability amplitudes describing the overall state of the register. These cancellations can in turn cause large superpositions to quickly converge into a state that, when measured, with near-certainty gives only a single possible outcome. Two early, but still important, examples demonstrating the power of this phenomenon are Shor's factoring algorithm and Grover's search algorithm. Shor's algorithm factors a given number into its prime-number components exponentially faster than the best-known classical algorithm to date, with dramatic consequences for important cryptographic schemes (see below). Grover's algorithm finds the location of a 1 with good probability in a given n-bit sequence, provided there is one, using a number of basic computational steps given by roughly the square root of n. The best-possible classical algorithm needs roughly n steps in the worst case, however.

Quantum cryptography
Shor's algorithm can break the most important cryptographic schemes we have today, which are based on the assumption that factoring is hard. A fully operational large-scale quantum computer shatters this assumption. This means that alternative cryptography is needed immediately, as some of today's information may need to be kept secret even after quantum computers are built. Multiple lines of research on post-quantum cryptography address this issue. On the one hand, one can try to look for problems that might even be hard for quantum computers, an important motivation for lattice-based cryptography. On the other hand, quantum mechanics itself offers alternatives too, as was pointed out already long before Shor's discovery. Wiesner circa 1970 introduced a quantum money scheme, a proposal where bank notes are unfalsifiable thanks to the presence of qubits on it. This was the first attempt to use quantum mechanics in a cryptographic protocol. More than a decade later, in 1984, Bennett and Brassard introduced the revolutionary quantum key distribution protocol, an unconditionally secure communication protocol relying on the laws of quantum mechanics. In this protocol, Alice wants to share a random key with Bob, to do so she sends random bits encoded into randomly chosen basis among two complementary basis. Complementary basis are subject to the uncertainty principle: if a bit of information is encoded into one of the basis, measuring according to the other one produces an random bit, uncorrelated with the encoded information. Roughly speaking a spy who wants to observe the sent qubits will not only get no information if he does not guess the appropriate basis, but will be detected by Alice and Bob with high probability. The protocol is relatively simple to implement, and has been commercialised. Notice however, the proof that the protocol is actually unconditionally secure took 15 years!

Scalability and error correction
One of the major challenges in the quest for a quantum computer is its scalability. Prototypes of quantum computers already exist but their memory, subject to decoherence, is limit to a few dozen qubits. The scalability of quantum computers is not only a technological challenge, error correcting code are crucial: a large scale robust quantum computer requires that the quality of the quantum device should meet the maximal amount of errors quantum codes can correct.

Please contact:
Jop Briët
CWI, The Netherlands
j.briet@cwi.nl

Simon Perdrix
LORIA, CNRS, Inria Mocqua,
Université de Lorraine, France
simon.perdrix@loria.fr

How Classical Beings Can Test Quantum Devices

by Stacey Jeffery (CWI)

As the race to build the first quantum computer heats up, we can soon expect some lab to claim to have a quantum computer. How will they prove that what they have built is truly a quantum computer?

It is already possible to buy quantum hardware for certain cryptographic tasks, such as random number generation and key distribution. In cryptographic scenarios, being able to test that your devices behave as advertised is clearly of paramount importance.

The first commercial quantum computers are likely to run as shared servers, where clients can pay to have a quantum computation run. This is another scenario where we would like the client, who does not have a quantum computer, to have some guarantee that the correct computation has been performed.

These scenarios are captured by a *verification protocol*, in which a *verifier*, who would like to run some quantum computation, interacts with one or more provers who have a quantum computer. By the end of the protocol, the verifier either "accepts" or "rejects" the output of the computation. The verifier might represent an experimenter testing a quantum system, and the provers a personification of nature, or more precisely, the physical systems being tested. If the provers are "honest" and follow the protocol – that is, they behave as predicted – the verifier should learn the result of the quantum computation. However, if the provers are deviating from the protocol, the verifier should detect this and "reject".

Verifying quantum computations is related to the more fundamental task of experimentally verifying quantum mechanics. A quantum system has an internal state that an observer cannot perceive directly. To learn about this state, a quantum measurement can be performed, giving some incomplete information. If an experimentalist hypothesises that a particular quantum system has a particular state, this can be verified by performing measurements, but this presupposes some trusted quantum measurement device. If one wants to verify the theory of quantum mechanics, one cannot circularly assume that the measurement device behaves as predicted by the theory quantum mechanics.

However, there *are* means of verifying certain aspects of quantum mechanics that do not require the experimenter to have a trusted quantum device, called *Bell tests*. In a Bell test, two provers play a game with a verifier. The verifier asks each prover a question, and they must each return an answer, without communicating during the game. What makes a Bell test special is that they can win the game with higher probability if they share a quantum resource called entanglement than if they are classical. Thus, such a game offers a way to experimentally test quantum mechanics.

Analogous to the situation in testing quantum mechanics, testing a quantum computer can be accomplished in either of two regimes. In the *quantum-verifier regime*, the verifier must have a simple trusted quantum device, like a measurement device. In this regime, several efficient verification protocols are known. However, the requirement that the verifier have a trusted quantum device is a big drawback.

In the *two-prover regime*, analogous to a Bell test, a *classical* verifier interacts with two provers who do not communicate. The first protocol in this regime was a significant breakthrough, providing, for the first time, a method for a classical verifier to verify any quantum

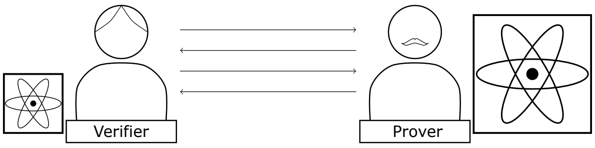


Figure 1: Quantum-verifier Regime. A verifier with a simple quantum device interacts with a prover with a full quantum computer.

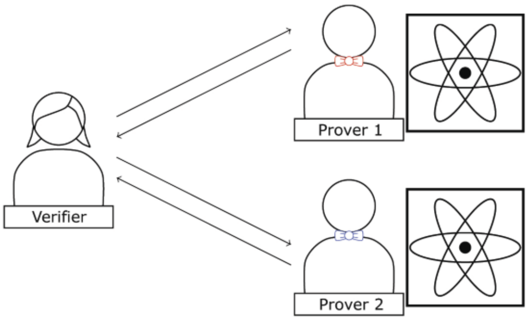


Figure 2: Two-prover Regime. A classical verifier interacts with two quantum provers.

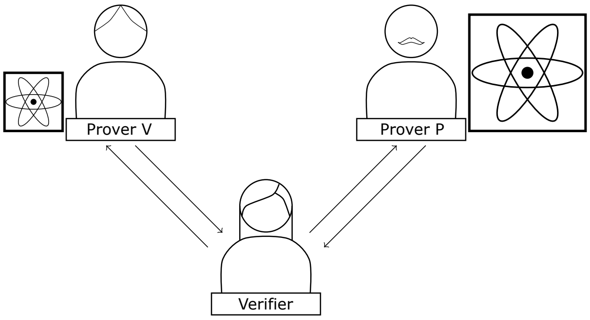


Figure 3: Our new two-prover protocol. The provers play the role of the verifier and prover from Broadbent's Protocol, which is a quantum-verifier protocol.

computation [3]. However, the protocol had the major disadvantage of requiring resources that scale like g^{8192} to verifiably implement a quantum circuit of size g. For comparison, there are an estimated 2^{286} elementary particles in the universe. Subsequent improvements decreased this overhead to g^{2048}, but this is still thoroughly impractical, even for a quantum circuit of size $g = 2$.

In collaboration with researchers from Université Paris Diderot and Caltech, we presented the first *efficient* protocol in the two-prover regime [2]. This protocol requires resources that scale like $O(g \log g)$ to verify a quantum circuit of size g.

We begin with a quantum-verifier protocol due to Broadbent [1]. The provers in our protocol are asked to simulate Broadbent's verifier and prover, respectively. We call our provers Prover V, for verifier, and Prover P, for prover.

By the properties of Broadbent's Protocol, we can use Prover V to *test* Prover P, to make sure he is following the protocol. Then it only remains to ensure that Prover V is, in fact, following the protocol. We develop new Bell tests that are used to make Prover P test Prover V. While the classical verifier may not be powerful enough to keep a quantum prover in check, she can use the two provers to control one another.

In the future, we hope to see experimental realisations of our protocol, which is possible for the first time, due to its efficiency. Its near-optimal efficiency means that verifying a particular quantum computation does not require much more resources than simply implementing that computation.

Links:
CWI's algorithms and complexity group: https://kwz.me/hBD
QuSoft: http://www.qusoft.org/

References:
[1] A. Broadbent: "How to Verify a Quantum Computation" Arxiv preprint arXiv:1509.09180, 2015.
[2] A. Coladangelo, A. Grilo, S. Jeffery, T. Vidick: "Verifier-on-a-Leash: new schemes for verifiable delegated quantum computation, with quasilinear resources" Arxiv preprint arXiv:1708.07359, 2017.
[3] B. W. Reichardt, F. Unger and U. Vazirani: "Classical command of quantum systems" Nature 496, 456-460, 2013.

Please contact:
Stacey Jeffery, CWI and QuSoft,
jeffery@cwi.nl

Keeping Quantum Computers Honest (or Verification of Quantum Computing)

by Alexandru Gheorghiu (University of Edinburgh) and Elham Kashefi (University of Edinburgh, CNRS)

Quantum computers promise to efficiently solve not only problems believed to be intractable for classical computers, but also problems for which verifying the solution is also intractable. How then, can one check whether quantum computers are indeed producing correct results? We propose a protocol to answer this question.

Quantum information theory has radically altered our perspective about quantum mechanics. Initially, research into quantum mechanics was devoted to explaining phenomena as they are observed in nature. But the focus then changed to designing and creating quantum systems for computation, information processing, communication, and cryptography among many other tasks. In particular, what became clear was that quantum interference - "the heart of quantum mechanics", as Richard Feynman described it - can be harnessed for quantum computation. Algorithms running on a hypothetical quantum computer would be able to solve problems by creating an interference pattern of different computational branches. This can lead to an exponential saving in the amount of resources used by a quantum algorithm, when compared to the best known classical algorithms. The most famous example of this is Shor's algorithm for factoring numbers which is exponentially faster than the best known classical factoring algorithms.

But having a device which can solve problems exponentially faster than classical computers raises an interesting question: can a classical computer efficiently verify the results produced by this device? At first, one might be tempted to dismiss this question and say that as long as each component of a quantum computer has been tested and works correctly, there is no need to worry about the validity of the device's results. However, the point of verification is much more profound. Quantum computers would provide one of the most stringent tests of the laws of quantum mechanics. While numerous experiments involving quantum systems have already been performed to a remarkable precision, they all utilized relatively few degrees of freedom. But when many degrees of freedom are involved, and because predicting the outcome of the experiment requires exponential resources, it quickly becomes infeasible to calculate the possible results of the experiment without resorting to lax approximations. Verification of quantum computation would therefore allow for a new test of quantum mechanics, a test in the regime of high complexity.

There is another important reason for verifying quantum computations, having to do with cryptography. The first quantum computers are likely to be servers, to which clients can connect through the Internet. We can already see an instance of this with the recent 5-qubit and 16-qubit devices that IBM has made available to the general public [L1]. When larger devices become available, users will wish to delegate complex computations to them. However, in such a distributed environment, malicious agents might perform

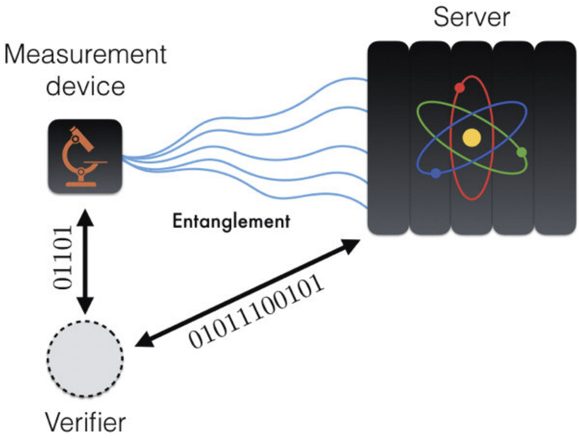


Figure 1: Device-independent verification protocol. The client, or verifier, will instruct both the measurement device and the server to measure entangled qubits. The statistics of these measurements are then checked by the verifier. All communication with the quantum devices is classical.

man-in-the-middle attacks or compromise the remote server. The clients would then need a means to check the validity of the server's responses. In fact, in this setting, users might also wish to keep their data hidden even from the quantum computer itself, as it might involve sensitive or classified information.

So can one verify quantum computations while also maintaining the secrecy of the client's input? The answer is yes. In fact, the client's ability to keep the input hidden is what makes verification possible. This was shown by Fitzsimons and Kashefi when they proposed a verification protocol based on a cryptographic primitive known as Universal Blind Quantum Computation (UBQC) [1,2]. In UBQC, a client that can prepare single qubits has the ability to delegate quantum computations to a server, in such a way that the server is oblivious to the computation being performed. To do verification, the client can then exploit this property by embedding tests in the computation, referred to as traps, which will fail if the server doesn't perform the correct computation. Of course, the problem with this approach is that the client needs to trust that the qubit preparation device works correctly and produces the specified states. But if, prior to the start of the protocol, a malicious agent corrupts the preparation device, the client could later be tricked into accepting incorrect results.

To address this issue, we, together with Dr. Petros Wallden, at the University of Edinburgh, proposed a verification protocol which is device-independent [3]. In other words, the client need not trust any of the quantum devices in the protocol. This is achieved by using a powerful result of Reichardt, Unger and Vazirani, known as rigidity of non-local correlations [4]. Non-local correlations are correlations between responses of non-communicating parties that cannot be reproduced classically, unless the parties are allowed to communicate. Such correlations can be produced, quantum mechanically, through a suitable strategy for measuring certain entangled states. The rigidity result is essentially a converse to this. It states that certain non-local correlations can only be produced by a particular, unique strategy. Observing such correlations between non-communicating devices then implies that the devices are behaving according to this fixed strategy. What is remarkable about this result is that it only requires examining the outputs of the devices, without assuming anything about their inner workings.
The protocol then works as follows: the client has an untrusted device for measuring single qubits and is also communicating classically with the quantum server. By examining the outputs of the two devices, it follows from the rigidity result that the client can check whether the two devices are sharing entanglement and performing measurements as instructed. If so, the client leverages this and uses the entanglement to remotely prepare single qubit states on the server's side. Finally, the client uses the trap-based scheme of Fitzsimons and Kashefi to delegate and verify an arbitrary quantum computation to the server.

Verification is an important milestone on the road to scalable quantum computing technology. As we have seen, verification protocols exist even for the most paranoid users. But even so, questions still remain regarding their optimality, their ability to tolerate noise and imperfections, as well as other issues. Addressing all these questions is a key challenge for both theorists and experimentalists and their resolution will shape the landscape of the emerging Quantum Internet.

Link:
[L1] https://kwz.me/hBv

References:

[1] A. Broadbent, J.F. Fitzsimons, E. Kashefi: "Universal blind quantum computation", in Proc. of FOCS '09, IEEE Computer Society (2009) 517 – 526.
[2] J.F. Fitzsimons, E. Kashefi: "Unconditionally verifiable blind quantum computation", Phys. Rev. A 96 (2017) 012303.
[3] A. Gheorghiu, E. Kashefi, P. Wallden: "Robustness and device independence of verifiable blind quantum computing", New Journal of Physics 17(8) (2015) 083040.
[4] B.W. Reichardt, F. Unger, U. Vazirani: Classical command of quantum systems. Nature 496(7446) (2013) 456.

Please contact:

Elham Kashefi, University of Edinburgh, UK and CNRS, France
ekashefi@inf.ed.ac.uk

Alexandru Gheorghiu
University of Edinburgh, UK
agheorgh@inf.ed.ac.uk

Experimental Requirements for Quantum Computational Supremacy by Boson Sampling

by Alex Neville and Chris Sparrow (University of Bristol)

Boson sampling has emerged as a leading candidate for demonstrating "quantum computational supremacy". We have devised improved classic al algorithms to solve the problem, and shown that photon loss is likely to prevent a near-term demonstration of quantum computational supremacy by boson sampling.

The prospect of harnessing precisely engineered quantum systems to run algorithms which vastly outperform their best classical counterparts has generated a large amount of interest and investment in the field of quantum computing. However, a universal and fault-tolerant quantum computer is unlikely to be built soon. Considering this potentially long wait, recently several new problems have been proposed with the purpose of demonstrating "quantum computational supremacy", which refers to the point at which a quantum machine performs a computational task that is beyond the capability of any classical computer [1], with specialised near-term quantum devices.

One such proposal is the boson sampling problem introduced by Aaronson and Arkhipov [2]. The problem consists of sampling from the output distribution of detection events generated when many single photons are concurrently injected in to a randomly chosen network of linear optical components. A sample value is generated by recording where photons were detected at the end of the linear optical network. The probability for each possible output in the experiment is related to a matrix function known as the permanent, which is in general especially hard to compute. By making the plausible conjecture that the permanent is hard to approximate for Gaussian random matrices, as well as another reasonable conjecture about the distribution of these permanents, Aaronson and Arkhipov were able to show that an efficient classical algorithm for even approximate Boson sampling would lead to the collapse of the polynomial hierarchy of complexity classes to its third level – something considered extremely unlikely in computational complexity theory. The result applying to approximate boson sampling is key, as it allows for the possibility of solving the boson sampling problem with realistic quantum experiments, without the need for quantum error correction. Physically, the complexity of the problem stems from the complex quantum interference of indistinguishable photons; if we make the photons distinguishable (say, by using photons of different colours) then the problem is no longer hard.

Our best new classical boson sampling algorithm [3] is based on Metropolised Independence Sampling (MIS), a Markov chain Monte Carlo procedure similar to the famous Metropolis-Hastings algorithm. We start a list by proposing a sample value from some easy-to-sample distribution, and continue by iteratively proposing new values and either adding this new value to the list or repeating our previous value. Which of these possibilities actually occurs is determined by a carefully crafted acceptance rule which depends on the probabilities of the proposed and current value occurring in both the target distribution and the proposal distribution, and guarantees that the list tends towards a genuine boson sampling sample.

We identified the corresponding distribution for distinguishable particles at the output of the linear optical network as a proposal distribution which provides rapid convergence to the boson sampling distribution. Although the probabilities in this distribution are also given by matrix permanents (albeit different matrices), the distribution can be efficiently sampled. Using this, we found strong numerical evidence that computing just 200 matrix permanents is enough to generate a boson sampling value via MIS for a problem size of up to 30 photons, roughly amounting to a speed-up of 50 orders of magnitude over the best previously suggested classical algorithm at this problem size.

By assuming that 200 matrix permanent computations suffice to produce a good sample for larger photon numbers, we were able to predict the amount of time it would take to solve boson sampling for up to 100 photons if we ran MIS on a powerful supercomputer. Alongside this, we computed the expected time to experimentally perform boson sampling as a function of the probability of a single photon surviving the experiment (i.e., not getting lost from source to detector). We found that it would require more than 50 photons before the classical runtime would exceed a week. To achieve this experimentally would not only require the ability to produce a state of 50 indistinguishable photons at a high rate (the current record-holding boson sampling experiment is with five photons), but also that all photons survive the experiment with a probability greater than 50%. Considering that each photon would require to be injected in to the circuit, pass through over 1000 beamsplitters and be coupled out of the circuit to single photon detectors, this would amount to a significant engineering breakthrough which is unlikely to be realised in the near future.

Our results not only provide a benchmark for quantum supremacy by boson sampling, but also highlight how significant the experimental improvement must be in order to achieve this.

Link:
https://kwz.me/hB1

References:

[1] A. Harrow, A Montanaro: "Quantum computational supremacy", Nature 549 (2017), 203–209.

[2] S. Aaronson, A. Arkhipov: "The computational complexity of linear optics", Theory Comput. 9, 143–252, 2013.

[3] A. Neville, C. Sparrow, et al.: "Classical boson sampling algorithms with superior performance to near-term experiments", Nature Physics 13, 1153–1157 (2017).

Please contact:

Alex Neville, Chris Sparrow
University of Bristol, UK
alex.neville@bristol.ac.uk,
chris.sparrow@bristol.ac.uk

From Classical to Quantum Information – Or: When You Have Less Than No Uncertainty

by Serge Fehr (CWI)

Over the last few years, significant progress has been made in understanding the peculiar behaviour of quantum information. An important step in this direction was taken with the discovery of the quantum Rényi entropy. This understanding will be vital in a possible future quantum information society, where quantum techniques are used to store, communicate, process and protect information.

Information theory is the area of computer science that develops and studies abstract mathematical measures of "information" – or, from a more pessimistic perspective, measures of "uncertainty", which capture the lack of information. It is clear that when you toss a coin there will be uncertainty in the outcome: it can be either "head" or "tail", and you have no clue what it will be. Similarly, there is uncertainty in the face that will show up when you throw a dice. It is even intuitively clear that there is more uncertainty in the latter than in the coin toss. However, such comparisons become less clear for more complicated cases. If we want to compare, say, tossing three coins on the one hand with throwing two dice and taking the sum of the two faces on the other hand, it is not immediately clear in which of the two there is more uncertainty: there are fewer possible outcomes in the former, namely eight, but, on the other hand, the eleven possible outcomes in the latter are biased.

Information theory offers quantitative measures that express precisely how much uncertainty there is. Similarly, it also offers measures of conditional uncertainty given that one holds some "side information". For instance, how much uncertainty is there in the faces of the two dice given that I know the sum of the two? How much uncertainty is there in a message that was communicated over a noisy channel given that I hold the received noisy version? How much uncertainty is there in a digital photo given that I hold a compressed version? How much uncertainty does an eavesdropper have on secret data given that he got to see an encryption? Information theory allows us to answer such questions in a precise manner and to make rigorous predictions about the behaviour of information in all kinds of information processing tasks. As such, information theory had – and still has – a major impact on the development of today's information and communication infrastructure.

What makes information theory very powerful is its independence of how information is physically represented: whether the information is represented by coins that show "head" or "tail", or by the tiny indentations on a DVD, or whether the information is stored on a flash drive or communicated over WiFi, the predictions of information theory hold universally – well, until we hit the realm of quantum mechanics. If, say, we encode information into the polarisation of photos, then information starts to behave very differently. Therefore, a quantum version of information theory is necessary in order to rigorously study the behaviour of information in the quantum realm, and, for instance, to be able to quantify the amount of information an eavesdropper may have on secret data when the data is protected by means of quantum cryptography, or to quantify the amount of error correction needed in order to counter the loss of information in quantum computation caused by decoherence.

From a mathematical perspective, given that quantum mechanics is described by non-commuting mathematical objects, quantum information theory can be understood as a non-commutative extension of its classical commutative counterpart. This insight can serve as a guideline for coming up with quantum versions of classical information measures, but it also shows a typical predicament: a commutative expression can be generalised in various ways into a non-commutative one. For instance, an expression like A^5B^4 can be generalised to A^5B^4 or to B^4A^5 for non-commuting A and B, or to ABABABABA, or to $B^2A^5B^2$, etc. One of the challenging questions is to understand which of the possible generalisations of classical information measures are suitable measures of quantum information and have operational significance.

Building upon new insights and new results [1] that we discovered on the classical notion of Rényi entropy, and in collaboration with several partners, we succeeded in lifting the entire family of Rényi entropies to the quantum setting [2,3]. The Rényi entropies form a continuous spectrum of information measures and cover many important special cases; as such, our extension to the quantum setting offers a whole range of new quantum information measures. We showed that our newly proposed definition satisfies various mathematical properties that one would expect from a good notion of information and which make it convenient to work with the definition. It is due to these that our quantum Rényi entropies have quickly turned into an indispensable tool for studying the behaviour of quantum information in various contexts.

One very odd aspect of quantum information is that uncertainty may become negative: it may be that you have less than no uncertainty in your target of interest. This peculiarity is an artifact of entanglement, which is one of the most bizarre features of quantum mechanics. Entanglement is a form of correlation between quantum information that has no classical counterpart. A sensible explanation of negative uncertainty can be given as follows. By Heisenberg's uncertainty principle, even when given full information in the form of a perfect description of the quantum state of interest, there is still uncertainty in how the state behaves under different measurements. However, if you are given another quantum state that is entangled with the state of interest, then you can actually predict the behaviour of the state of interest under any measurement by means of performing the same measurement on your state. Indeed, by what Einstein referred to as "spooky action at a distance", the measurement on your entangled state will instantaneously affect the other state as to produce the same measurement outcome.

The above aspect nicely illustrates that quantum information theory is much more than a means for understanding the behaviour of information within possible future quantum communication and computation devices: it sheds light on the very foundations of quantum mechanics itself.

References:

[1] S. Fehr, S. Berens: "On the Conditional Rényi Entropy", in IEEE Trans. Inf. Theory 60(11):6801 (2014).

[2] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, M. Tomamichel: "On Quantum Rényi Entropies: A New Generalization and Some Properties", in J. Math. Phys 54:122203 (2013).

[3] M. Wilde, A. Winter, D. Yang: "Strong Converse for the Classical Capacity of Entanglement-Breaking and Hadamard Channels via a Sandwiched Rényi Relative Entropy", in Commun. Math. Phys 331:593 (2014).

Please contact:
Serge Fehr, CWI, The Netherlands
+31 20 592 42 57, serge.fehr@cwi.nl

Preparing Ourselves for the Threats of the Post-Quantum Era

by Thijs Veugen (TNO and CWI), Thomas Attema (TNO), Maran van Heesch (TNO), and Léo Ducas (CWI)

In the post-quantum era, most of the currently used cryptography is no longer secure due to quantum attacks. Cryptographers are working on several new branches of cryptography that are expected to remain secure in the presence of a universal quantum computer. Lattice-based cryptography is currently the most promising of these branches. The new European PROMETHEUS project will develop the most secure design and implementations of lattice-based cryptographic systems. Exploitation of the project results will be stimulated by demonstrating and validating the techniques in industry-relevant environments.

Most current day cryptosystems are based on two computationally hard problems: factoring integers and computing the discrete logarithms in finite groups. Advances in solving these problems (classically) and increased classical computational power form a threat that is relatively easy to diminish by 'simply' increasing the key sizes. A more serious threat was revealed in 1994 already, when Shor [1] had proven that quantum algorithms are able to efficiently solve both these problems. While the requirement for a truly universal quantum computer to execute these attacks has long kept us secure, recent advances in quantum computing once again highlight our dependency on these computational problems. In short, the arrival of a quantum computer will leave commonly used cryptosystems such as RSA, DH and ECDH insecure.

To ensure secure communication in the presence of a universal quantum computer, for many years cryptographers have been working on constructing cryptographic schemes based on other computational problems since many years. Their efforts have led to the following six possible building blocks for cryptographic schemes: hash trees, error-correcting codes, lattices, multivariate equations, supersingular elliptic curve isogenies, and even quantum physics. These cryptographic building blocks fall within the realm of so-called "post-quantum cryptography", the study of cryptographic algorithms that are secure against attacks by a quantum computer.

PROMETHEUS is a new, four-year European H2020 project (starting in January 2018) aiming to provide a secure design and implementation of new and quantum-safe cryptographic systems. The twelve project partners (ENS Lyon, ORANGE SA, CWI Amsterdam, IBM Research, RHU London, RU Bochem, Scytl Barcelona, Thales, TNO, UPC Barcelona, University Rennes, WIS Rehovot) will focus their efforts on lattice-based cryptography. A fundamental property of lattice-based cryptographic schemes is that their security can be reduced to well-studied computational problems, which is not necessarily the case for other post-quantum mechanisms.

An n-dimensional lattice L is a set of integer linear combinations of n independent vectors. The grid displayed in Figure 1 represents a lattice L. An example of a computationally hard lattice problem is the closest vector problem (CVP): given a lattice L and a random point y (not necessarily an ele-

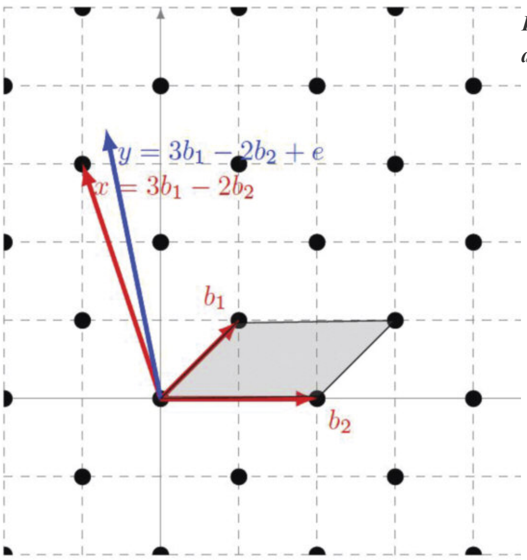


Figure 1: Illustration of a two-dimensional lattice.

ment of the lattice), find the lattice element *x* closest to *y*. For higher dimensional lattices this problem soon becomes very hard to solve. In fact, no (quantum) algorithms have been found yet solving this problem efficiently.

Research in using this and other hard lattice problems for cryptographic purposes began with the publication of the public key encryption scheme by Ajtai and Dwork in 1997 [2]. Improvements to this scheme and new schemes followed, trying to make use of additional structures in specific types of lattices. The first lattice-based cryptographic schemes for public-key encryption, signatures and key-exchange have been proposed, and are considered for standardization [L1]. A recently proposed key-exchange protocol [3] (partly developed at CWI) has successfully been implemented and tested by Google in the Chrome web browser [L2], and was awarded the Facebook Internet Defense prize [L3].

One particular challenge for the transfer from theory to practice lies in the choice of parameters for those schemes: while lattice problems become ‘hard’ with larger dimensions, predicting precisely how hard they are (e.g., it will take 100 years to solve with a cluster of 10,000 GPUs) remains difficult and uncertain. The issue becomes even more delicate when considering quantum algorithms, especially in the light of recent quantum algorithms specialised for “ideal lattices” [4]. This is the main issue for which CWI’s crypto group will provide its expertise.

The PROMETHEUS project recognises that modern day cryptography entails much more than protecting private information over insecure communication channels. With its digital signatures, commitment schemes, and homomorphic properties, lattice-based cryptography offers a wide variety of applications. To enhance the applicability and the adaptation of these techniques, four use-cases will be studied. By means of these use-cases PROMETHEUS aims to cover the entire range from theory to application.

The first use case will focus on constructing an anonymous credential system, which allows a user to prove to a service provider that he owns a certain attribute (e.g., driving licence), while minimising the information given to third parties, then protecting the user’s privacy. In the second use case technology will be developed that allows users to make secure, privacy-friendly contactless transactions, for a long-term use. In the third use case, a long-term secure e-voting system will be developed. Lastly, in the fourth use case, PROMETHEUS will develop quantum-safe homomorphic encryption techniques, and use them to develop a secure cyber threat-intelligence sharing mechanism.

All four use-cases aim for long-term security in the quantum era, requiring the cryptographic building blocks to be quantum safe. Many of these techniques already exist in a quantum vulnerable setting. Introducing long-term security by mitigating quantum threats is the core of our innovation. By covering the entire range from theory to application and building demonstrators, the exploitation of the project results will be stimulated.

Links:

[L1] https://kwz.me/hB2
[L2] https://kwz.me/hB3
[L3] https://kwz.me/hB5

References:

[1] P.W. Shor: “Algorithms for quantum computation: Discrete logarithms and factoring”, in Proc. of SFCS ‘94, 1994.
[2] M. Ajtai, C. Dwork: “A public-key cryptosystem with worst-case/average-case equivalence”, Proc. of the 29th annual ACM symposium on Theory of Computing. ACM, 1997.
[3] E. Alkim, L. Ducas, T. Pöppelmann, P. Schwabe: “Post-quantum Key Exchange-A New Hope”, USENIX Security Symposium, 2016.
[4] R. Cramer, L. Ducas, B. Wesolowski: ‘’Short Stickelberger Class Relations and application to Ideal-SVP’’, IACR, Eurocrypt 2017.

Please contact:

Thijs Veugen, TNO, The Netherlands
+31888667314, thijs.veugen@tno.nl

Quantum Cryptography Beyond Key Distribution

by Georgios M. Nikolopoulos (IESL-FORTH, Greece)

Quantum cryptography is the science of exploiting fundamental effects and principles of quantum physics, in the development of cryptographic protocols that are secure against the most malicious adversaries allowed by the laws of physics, the "quantum adversaries". So far, quantum cryptography has been mainly identified with the development of protocols for the distribution of a secret truly random key between two legitimate users, known as quantum key-distribution (QKD) protocols. Beyond QKD, quantum cryptography remains a largely unexplored area. One of the main ongoing projects at the Quantum Optics and Technology group of IESL-FORTH [L1], is the design and development of cryptographic solutions, which rely on fundamental quantum-optical systems and processes, and offer security against quantum adversaries.

Electronic communications and transactions constitute one of the main pillars of our society. The role of cryptography is to ensure the stability of this pillar, by providing techniques for keeping information secure, for determining whether information has been maliciously altered, and for determining who authored pieces of information. To a large extent, modern public-key cryptography relies on mathematical problems, such as the factorisation of large integers and the discrete logarithm problem, which are considered to be hard to solve on classical computers, in the sense that there are no known efficient classical algorithms for solving these problems for all integers in polynomial time. Given, however, that the non-existence of such algorithms has never been rigorously proved, most of the widely used public-key cryptosystems are susceptible to advances in algorithms or in hardware (computing power). Indeed, Peter Shor has proved that a quantum computer could solve both of the aforementioned mathematical problems efficiently.

Though a fully functional universal quantum computer of the necessary size to break widely used cryptosystems is still far off in the future, there is a necessity for ensuring the security, the integrity and the authenticity of data that is encrypted or digitally signed today, and they have long lifetime. Unfortunately, the currently available QKD systems become inefficient for

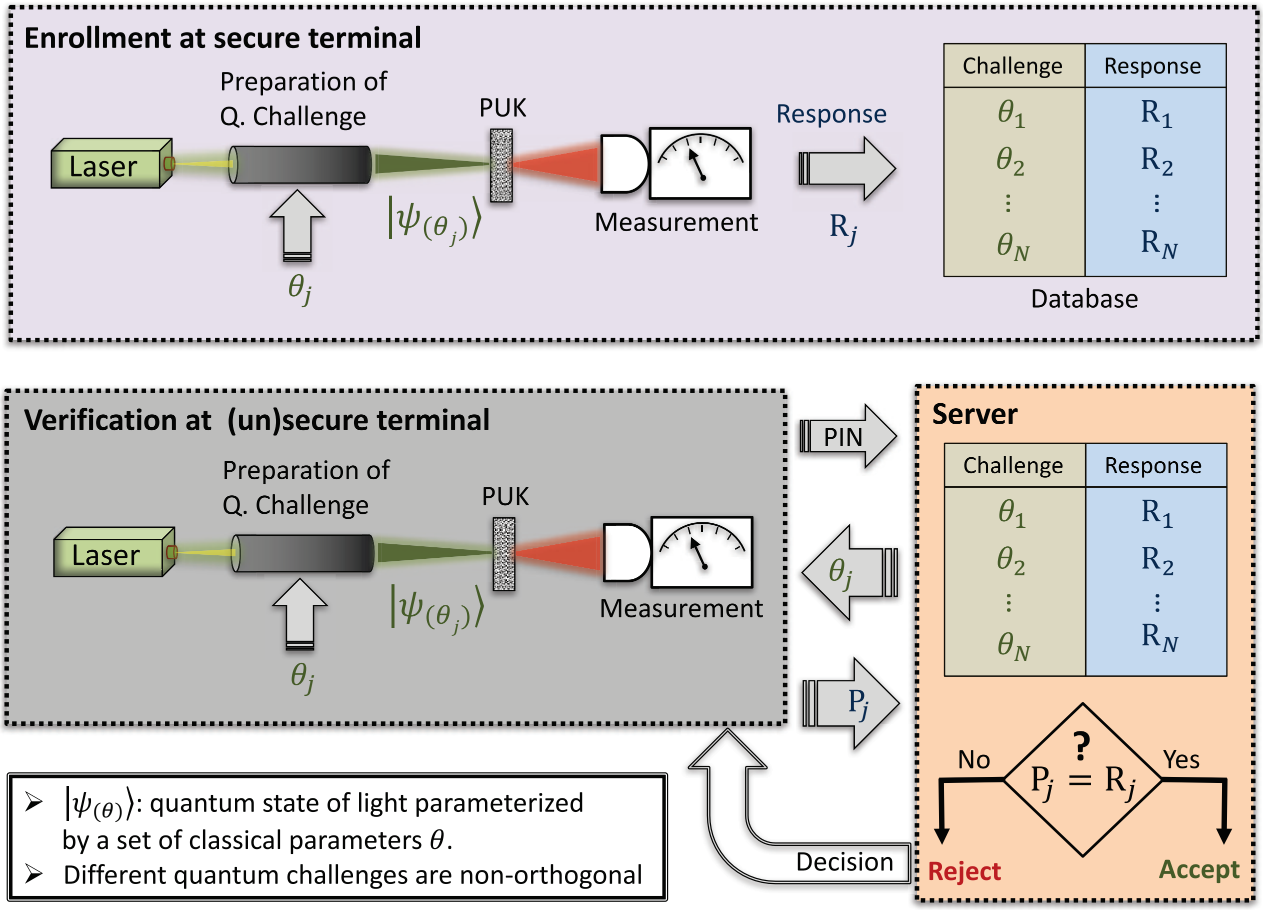

Enrollment at secure terminal
Preparation of Q. Challenge
PUK
Response
Laser
$|\psi_{(\theta_j)}\rangle$
Measurement
R_j
θ_j
Challenge
Response
θ_1
R_1
θ_2
R_2
$\vdots$
$\vdots$
θ_N
R_N
Database
Verification at (un)secure terminal
Preparation of Q. Challenge
PUK
Laser
$|\psi_{(\theta_j)}\rangle$
Measurement
θ_j
PIN
θ_j
P_j
Server
Challenge
Response
θ_1
R_1
θ_2
R_2
$\vdots$
$\vdots$
θ_N
R_N
No
Yes
$P_j \overset{?}{=} R_j$
Reject
Accept
Decision
➢ $|\psi_{(\theta)}\rangle$: quantum state of light parameterized by a set of classical parameters θ.
➢ Different quantum challenges are non-orthogonal

Figure 1: Schematic representation of a quantum-optical EAP, which relies on a challenge-response mechanism. The enrolment stage is performed once by the manufacturer, while the verification stage takes place each time the holder of the PUK has to be authenticated.

large networks (many users), where the establishment of many pairwise secret keys is needed, and the key management remains a major problem. Moreover, QKD alone does not address many other cryptographic tasks and functions, which are of vital importance in everyday life (e.g., authentication, non-repudiation, integrity, etc.).

Cryptographic research in our theoretical group started in 2007, and its emphasis is on the design and the development of quantum cryptographic primitives and protocols, which rely on fundamental quantum-optical systems and processes, and offer security against quantum adversaries [1-3]. Typical quantum-optical systems are single photons, light in various quantum states, atoms, waveguides, and cavities. A description of our activities and related publications can be found at [L1] and [L2].

Entity authentication (identification) is an important cryptographic task, in which one party (the verifier) obtains assurance that the identity of another party (the claimant) is as declared, thereby preventing impersonation. Most of the entity authentication protocols (EAPs) used for everyday tasks (e.g., transactions in automatic teller machines), rely on dynamic challenge-response mechanisms, which combine something that the claimant knows (e.g., a PIN), with something that the claimant possesses (e.g., a smart card). In such mechanisms, after the user types in the correct PIN, the smart card is challenged with random numerical challenges, and the verifier checks if the responses of the card are valid. Conventional EAPs are not totally immune to card-cloning, while they are susceptible to emulation attacks, in which an adversary knows the challenge-response properties of the smart card (e.g., by hacking the database of challenge-response pairs), and his task is to intercept each numerical challenge during the verification stage, and send to the verifier the expected response. Currently, optical physical unclonable keys (PUKs) are considered to be the most promising candidates for the development of highly secure EAPs. Such PUKs are materialised by an optical multiple-scattering disordered medium, and they are considered to be unclonable, in the sense that their cloning requires the exact positioning (on a nanometre scale) of millions of scatterers with the exact size and shape, which is considered to be a formidable challenge not only for current, but for future technologies as well. Typically, a PUK-based EAP relies on a challenge-response mechanism, in which the PUK is interrogated by light pulses with randomly chosen parameters, and acceptance or rejection of the PUK is decided upon whether the recorded responses agree with the expected ones. Although, in general, PUK-based EAPs are more robust against cloning than conventional EAPs, they are still vulnerable to emulation attacks when challenges pertain to classical light, and the verification set-up is not tamper-resistant. To eliminate this vulnerability, in collaboration with E. Diamanti (CNRS, Université Pierre et Marie Curie), we have proposed a novel quantum-optical EAP in which a PUK is interrogated by randomly chosen non-orthogonal coherent quantum states of light (see Figure 1) [1]. The response of the PUK to a quantum state (challenge) is sensitive to the internal disorder of the PUK, which makes our protocol collision resistant, and robust against cloning. Moreover, on-going research shows that the security of our protocol against an emulation attack relies on the laws of quantum physics, which do not allow unambiguous discrimination between non-orthogonal quantum states, while information gain cannot be obtained without disturbing the quantum state under interrogation. The proposed protocol can be implemented with current technology, and its performance under realistic conditions is the subject of future theoretical and experimental work.

Links:
[L1] http://www.quantum-technology.gr/
[L2] http://gate.iesl.forth.gr/~nikolg

References:

[1] G. M. Nikolopoulos, E. Diamanti: "Continuous-variable quantum authentication of physical unclonable keys", Scientific Reports, 2017, 7, p. 46047.
[2] G. M. Nikolopoulos, T. Brougham: "Decision and function problems based on boson sampling", Physical Review A, 2016, 94, p. 012315.
[3] G.M. Nikolopoulos: "Applications of single-qubit rotations in quantum public-key cryptography", Physical Review A, 2008, 77, p. 032348.

Please contact:

Georgios M. Nikolopoulos
IESL-FORTH, Greece
nikolg@iesl.forth.gr

Quantum Lego: Graph States for Quantum Computing and Information Processing

by Damian Markham (LIP6, CNRS - Sorbonne Université)

The massive global investment in quantum technologies promises unprecedented boosts for security, computation, communication and sensing. In this article we explore the use of so-called 'graph states' – a family of multipartite entangled states which act as ubiquitous resources for quantum information, are easily adapted for different tasks and applications, and can be combined in ways that fuses different utilities.

Quantum computing and quantum information in general offer incredible benefits to our information society. Since the original discoveries of better than classical security in quantum key distribution and super-classical computational advantage, the field has exploded with new possibilities for exploiting quantum encoding.

In quantum cryptography we have seen new protocols for coin flipping, quantum money and secure multiparty computation offering functionality and or security that is not possible classically. For certain communication tasks, quantum techniques provide an exponential gap between what is possible quantumly and classically. Even before universal quantum computers are born, sub-universal devices will have a plethora of applications from quantum learning to simulation. In quantum metrology, quantum sensing provides precision in measurements that would simply not be possible without uniquely quantum features.

A remarkable family of multipartite entangled states acts as generic resources for almost all these applications. Graph states are described in one to one correspondence with a simple graph, where vertices represent qubits (a two dimensional quantum system which is the basic quantum information unit) and edges represent a particular entanglement preparation. They are universal resources for quantum computation, act as codes for quantum error correction and are the entangled resource for many communication and cryptographic protocols. Perhaps their most compelling strength is that they can be connected in different ways to allow the utility of one function to be combined with another in a natural way. In this sense, these "graph states" are like quantum Lego – decide what you want to make and put them together in the right way to achieve it. This capacity will be key in taking the best advantage of quantum technologies in future quantum networks. Indeed, typically, more sophisticated applications are built up by combining basic protocols.

The natural connection to graph theory has proven an additional benefit of the graph state approach. It turns out that one can understand many properties of their use for quantum information – how computation flows, where information sits – entirely in terms of the underlying graph properties. This allows many graph theory techniques to be put into play to push more what quantum advantages can be had. Examples include graphical characterisation of where information sits in secret sharing [1] and the application of random graph techniques for finding optimal codes [2].

Another consequence of their ubiquity in quantum information is that there has been a lot of effort to demonstrate them experimentally. Indeed they represent the cutting edge in what entangled states are prepared, with audacious experiments preparing graph states of thousands of qubits. Experiments routinely produce and control graph states of up to 10 qubits in different media in optics, atomics and ions.

There are now several groups across Europe and the world working on exploring graph state quantum information processing. In a series of works with the groups of Mark Tame (Durban, South Africa) and John Rarity (Bristol, UK) we have been pushing the quantum Lego aspect, in particular. In one experiment we demonstrated a graph state protocol, which combined three different protocols to enable verified secret sharing [3]. This flexibility here proved crucial – by combining protocols we get functionality that is better than could be achieved by any single protocol in isolation. But there are many exciting things still to do, and we're still figuring out how graph states can be used, in several directions to push the limits of quantum information. For example, graph states have proven a fertile test space to understand the resources of non-locality and contextuality and their role in many quantum advantages. The graphical notion of flow of information also lends itself to the study of exciting new directions in quantum information where the inherent ambiguity in causal order has been shown to be yet another source of quantum advantage. Recently, we have also seen that graph states are resources for the generation of quantum randomness, an almost generic resource in quantum information and key in our understanding in much of physics.

References:

[1] D. Markham, B. C. Sanders: "Graph states for quantum secret sharing", Physical Review A 78.4 (2008): 042309.

[2] J. Javelle, M. Mehdi, S. Perdrix: "New Protocols and Lower Bounds for Quantum Secret Sharing with Graph States", TQC 12 (2012): 1-12.

[3] B. A. Bell, et al.: "Experimental demonstration of a graph state quantum error-correction code", Nature communications, 5, 2014

Please contact:

Damian Markham
CNRS, LIP6, Sorbonne Université
damian.markham@lip6.fr

Graph Parameters and Physical Correlations: from Shannon to Connes, via Lovász and Tsirelson

by Simone Severini (University College London)

Quantum information theory builds bridges between combinatorics, optimisation, and functional analysis.

Nowadays, it is theoretically predicted with paper and pencil, and experimentally demonstrated in the lab, that the physical state of most multi-object quantum mechanical systems cannot be described by looking only at their individual components, and displays stronger-than-classical correlations. In virtue of this point, manipulating some of the components has a global effect on the whole system, even if the components are spatially separated – something expressed by the currently overused and somehow unwelcoming Einstein's "spooky action at distance". This phenomenon is known as "entanglement".

When talking about entanglement, the average mathematical person tends to naturally refrain from alluding to the halo of mysticism surrounding this term, but to focus on the intricate structure of matrices and operators in composite Hilbert spaces. However, while entanglement may appear as a flat consequence of the tensor product used to combine systems as in wave-mechanics, it also has the status of a legitimate and possibly fundamental physical quantity. In truth, its freshly discovered applications range from information-theoretically secure solutions for distributing cryptographic keys to an assortment of remarkable protocols for transmitting information, including superdense coding and teleportation.

Two-player non-local games on graphs have been shown to be a particularly fruitful arena for rigorous research into the power of entanglement and, more generally, the correlations induced by the axiomatic choices leading to their different physical theories. In the proposed framework, two players, Alice and Bob, receive vertices of some graphs. Their task is to respond to questions without knowing each other's vertices; answers need to satisfy a certain property as a function of the received vertices. Depending on the type of correlations displayed by the physical world of Alice and Bob, this situation suggests a collection of new graph parameters, which are captured by rich mathematical structures, and give an occasion to generalise graph theory ideas to functional analysis. One of these quantities is now called quantum chromatic number and it is known to be loosely upper bounded by the more familiar chromatic number – when, in the non-local game, answers need to be different for adjacent and equal for identical vertices. The quantum chromatic number was the first quantum graph parameter to be studied. Such research direction has eventually ramified into multiple routes. A brief account of the salient points follows.

In 1956, Shannon defined the zero-error capacity of a communication channel as the largest rate at which information can be transmitted over the channel with error probability zero. The notion has contributed to fuel a great amount of research in semidefinite programming and structural graph theory. Berge's perfect graphs were remarkably motivated by the zero-error capacity and the Lovász theta function was introduced as an upper bound. When the parties can share and locally manipulate entangled states, the analogue capacity has also been proved to be bounded by Lovász theta, but to be exponentially larger in various single-shot and asymptotic cases [1, 2]. Given the link between zero-error capacity and the problem of transmitting data over a broadcast channel (e.g., coaxial cable or satellite), this result highlights a prospective quantum advantage exploitable in real-world communications.

In 1976, Connes casually formulated a conjecture about a fundamental approximation property for finite von Neumann algebras – the Connes embedding problem. Over time, many

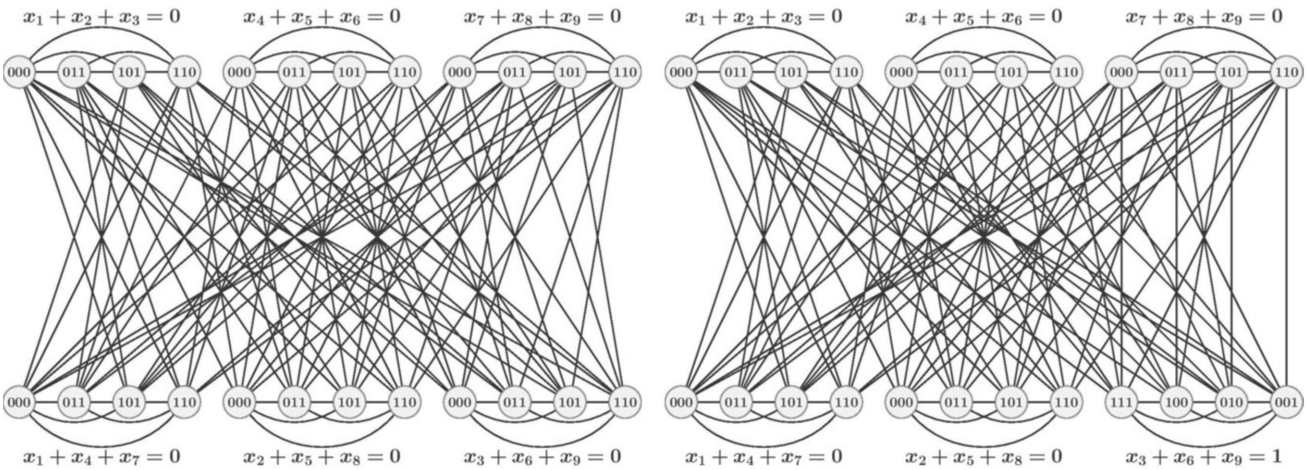


Figure 1: Two graphs on 24 vertices that are quantum isomorphic but not isomorphic. The construction is related to the FGLSS reduction from inapproximability literature, as well as the CFI construction.

Some members of the Quantum Computing, Information, and Algebras of Operators (QCIAO) collective (lecturers of the LMS Research School Combinatorics and Operators in Quantum Information Theory, Belfast September 2016).

unexpected equivalent statements for the conjecture have emerged. A hierarchy beyond the quantum chromatic number has led to a novel reformulation of the Connes conjecture, and generated a fresh effort towards its solution [L1]. The new approach is centred on combinatorial ideas lifted to the realm of operator algebras. Moreover, extending this mathematical landscape, hierarchies of quantum graph parameters associated to correlations can be placed in the framework of (tracial noncommutative) polynomial optimisation [L2]

In 1993, Tsirelson proposed some problems concerned with deciding whether the axiomatic mathematical models of non-relativistic quantum mechanics, where observers have operators acting on a finite dimensional tensor product space, and algebraic quantum field theory, where observers have commuting operators on a (possibly infinite dimensional) single space, produce the same set of correlations. A 2016 breakthrough, based on geometric group theory, settled the “middle” Tsirelson problem, by observing that the set of (tensor-product) quantum correlations is not closed [L3]. Interestingly, a successive alternative proof of this result makes use of quantum graph parameters [L4].

This new technical machinery became further consolidated via a quantum version of graph homomorphism, a familiar but powerful generalisation of graph colouring. This new technical machinery became further consolidated via a quantum version of graph homomorphism, a familiar but powerful generalisation of graph colouring. The new type of homomorphism suggested relaxations of graph isomorphism to settings corresponding to various physical theories. The findings of this line of research are surprising. While fractional isomorphism corresponds to sharing some type of correlations stronger than entanglement – hence, it gets an operational interpretation, – quantum isomorphism is obtained by relaxing the integer programming formulations for standard isomorphism to Hermitian variables [3] (see Figure 1).

The QCIAO Collective is an international collaboration focused on the topics of this article [L5].

Links:

[L1] https://arxiv.org/abs/1503.07207
[L2] https://arxiv.org/abs/1708.09696
[L3] https://arxiv.org/abs/1606.03140
[L4] https://arxiv.org/abs/1709.05032
[L5] http://www.qciao.org/

References:

[1] R. Duan, S. Severini, A. Winter: “Zero-error communication via quantum channels, non-commutative graphs and a quantum Lovasz theta function”, IEEE Trans. Inf. Theory 59(2):1164-1174, 2013.

[2] J. Briët, H. Buhrman, D. Gijswijt: “Violating the Shannon capacity of metric graphs with entanglement”, PNAS 2013 110 (48) 19227-19232.

[3] A. Atserias, et al.: “Quantum and non-signalling graph isomorphisms”, ICALP 2017.

Please contact:

Simone Severini
University College London, UK
+44 (0)20 3108 7093
s.severini@ucl.ac.uk

High-Speed Entanglement Sources for Photonic Quantum Computers

by Fabian Laudenbach, Sophie Zeiger, Bernhard Schrenk and Hannes Hübel (AIT)

Photonic quantum computers promise compact, user-friendly packaging. The building blocks of such an implementation comprise of sources for efficient production of photons with high purity. To increase the clock speed of the computation, such sources need to operate in the GHz range.

Although the current favourites for a scalable quantum computer seem to be super-conducting qubit implementations, a pure photonic-based solution should not be disregarded, since it offers room temperature operation and small footprints. As the standard approach to quantum computing is based on the quantum circuit model, a generalisation of the classical circuit, featuring logical operations such as AND and XOR gates, single-qubit gates (e.g. rotations) and two-qubit gates (e.g. controlled-NOT) are required for universal quantum computing. This quantum circuit model is not very well suited to a photonic implementation, since the photon-photon interaction is negligible and a two-photon gate is hence not feasible.

Computations over the quantum internet

With the near advent of quantum networks, consisting of distribution of single or entangled photons between users, a photonic quantum computer would have another advantage. Unlike matter based quantum computers, which require a photon/matter quantum interface, a cluster-state quantum computer could be directly connected to a global “quantum internet”. Protocols which rely on a quantum link between user and quantum computer exist today. Imagine the scenario, in which quantum computers are still very large and expensive, and clients can only request computation time from a remotely located quantum computer centre which is not necessarily trustworthy. Using the blind quantum computing protocol [1], the client’s inputs, outputs and computation remain perfectly private, even to the operators of the quantum computer centre. In another algorithm, quantum enabled one-time programing, the program itself is encoded onto photons, sent to a classical processing unit and executed. Since the qubits are destroyed during the measurement process, the program will only run once, a much sought-after property for cryptographic application and secure software distribution.

Cluster state computing

A scalable model for photonic quantum computation is the so called one-way or measurement based quantum computer [2]. In this approach, the actual computation proceeds by single qubit measurements only, on a large entangled resource state (cluster state). In a photonic implementation, the cluster state is a set of large numbers of photons, which are entangled to each nearest neighbour. The advantage lies in the fact, that there is no difference between performing a single-qubit or two-qubit gate operation. In both cases, there will be only measurements on single photons, a feat easy to achieve.

The main challenge lies of course in the creation of the entangled cluster state which sounds like a taunting task, especially for large states of several hundreds of qubits. Fortunately, it can be shown that heralded photon sources suffice to build a cluster state of any size. Of course efficiencies have to be increased and losses minimised, but in general, multiplexing a large number of such sources together will produce the necessary entangled state. One key issue is that the photons produced must be indistinguishable, i.e. they must look all the same. Therefore, no correlations in frequency, time or spatial modes are allowed between the photons. The figure of merit for this property is the purity, photons that are completely uncorrelated have a high purity whereas photons which correlate in a degree of freedom show a low purity. Figure 1 illustrates the absence of frequency correlation between two generated single photons.

The GHz entanglement source

The AIT-Austrian Institute of Technology in Vienna successfully developed a source for polarisation-entangled photon pairs which can be operated at a tunable repetition rate of up to 40 GHz to be used in cluster state generation [3]. Our source is based on a Sagnac-interferometer, where a non-linear optical medium is pumped by two pulsed laser beams from two diametrically opposed directions. By virtue of a

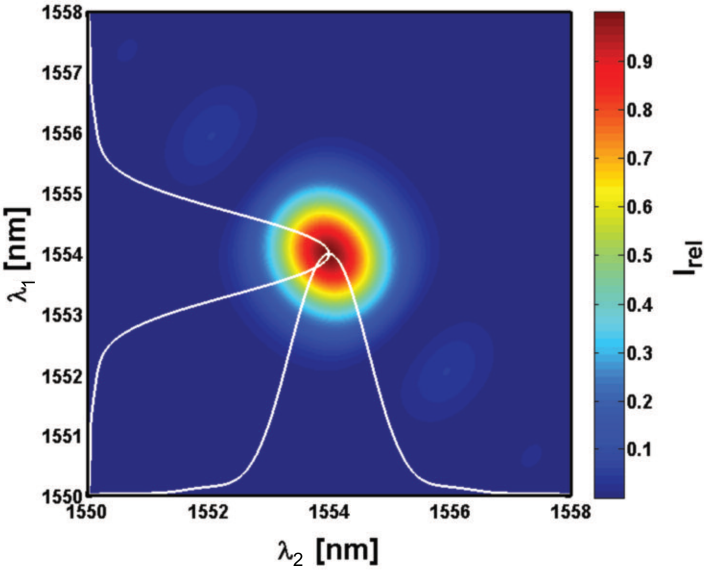


Figure 1: Frequency correlation plot (joint spectral intensity) between the photons of the generated pair. The nearly circular distribution indicates a low degree of correlations; in contrast a more elongated spectral distribution would point to a low purity of the photons.

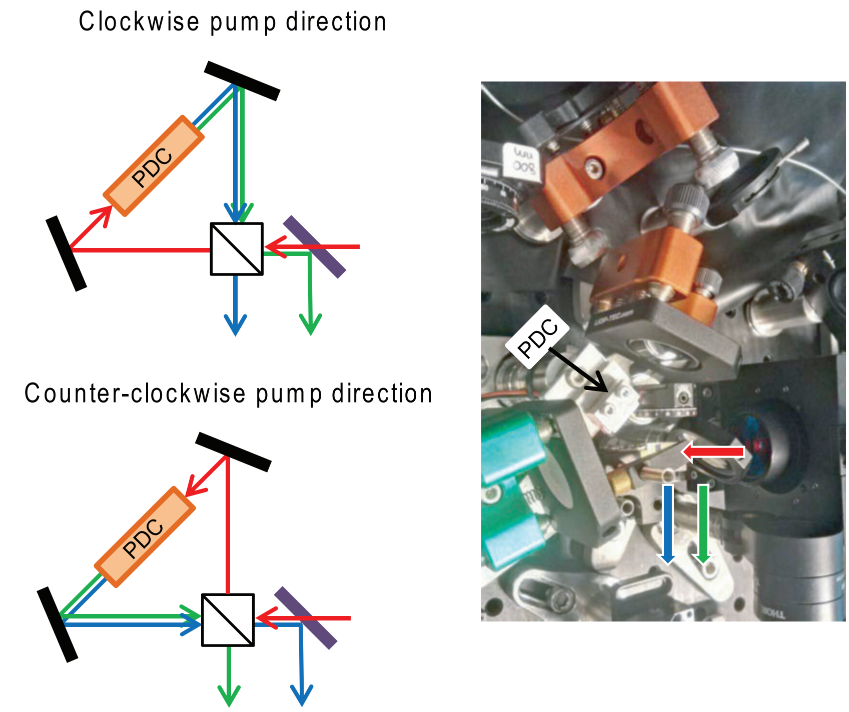


Figure 2: Left: Principle of entanglement generation. Depending on the path of the pump laser (red), the vertical (green) and horizontal (blue) photons are exiting at different ports; Right: Experimental setup of Sagnac interferometer, the red pump beam enters from the right side.

nonlinear process called parametric downconversion (PDC), some of the laser photons would decay within the crystal and give birth to two photons with half the energy each. Entanglement emerges from the lost “which-way information” after recombination of the two paths: There is no possible way to tell which pump beam produced the twin photons; therefore the two possible origins exist at the same time in a quantum superposition, as shown in Figure 2. The photons are generated with high purity and are highly entangled (95%).

Outlook

In the next step, we will simultaneously pump three Sagnac-interferometers (instead of one) in order to generate larger cluster states. Moreover, we will replace our avalanche photo diodes by superconducting nanowire detectors which not only have significantly higher detection efficiency but also operate at a higher time resolution. This will allow us to generate cluster states close to the maximal pulse rate of the laser at 40 GHz. While enlarging the number of photons in the cluster state, we will also strive to reduce the overall size of the experiment using photonic integration techniques.

Acknowledgements

This work was funded by the Austrian Research Promotion Agency (Österreichische Forschungsförderungsgesellschaft, FFG) through the project KVQ (No. 4642983).

Link:
https://www.ait.ac.at/themen/optical-quantum-technologies

References:

[1] S. Barz et al.: “Demonstration of Blind Quantum Computing”, Science 335 (2012), 303

[2] R. Raussendorf and H. J. Briegel: “A One-Way Quantum Compute”, PRL 86 (2001) 5188

[3] F. Laudenbach et al.: “Modelling parametric down-conversion yielding spectrally pure photon pairs”, Opt. Exp. 24 (2016), 2712

Please contact:
Hannes Hübel, Martin Stierle
AIT Austrian Institute of Technology, Austria
hannes.huebel@ait.ac.at,
martin.stierle@ait.ac.at

A Formal Analysis of Quantum Algorithms

by Benoît Valiron (LRI – CentraleSupelec, Univ. Paris Saclay)

Moving from the textual description of an appealing algorithm to an actual implementation reveals hidden difficulties.

Between 2011 and 2013, I had the opportunity to collaborate on the Pan-American project QCS (Quantum Computer Science) devoted to the implementation and analysis of quantum algorithms. Researchers from different areas, ranging from physicists to theoretical computer scientists, were working on this project; I was at the latter end of this spectrum. We were given a set of seven, state-of-the-art quantum algorithms instantiated on some concrete problems, with the task to implement and estimate the resources necessary to effectively run them, in the event of an actual quantum computer. To this end we developed the quantum programming language Quipper [L1].

Quantum algorithms are not usually designed as practical handles but instead as tools to explore complexity boundaries between classical and quantum computation: for a given problem, as the size of the input parameter grows, can we asymptotically go faster with the use of a quantum memory than with purely classical means? It turns out that many interesting problems have this property: many fields ranging from big-data to chemistry and pharmaceutic could benefit from the use of quantum algorithms. The natural question is how to concretely implement these quantum algorithms, estimate the required resources and validate the implementation.

In the realm of classical computation, implementing an algorithm implies the choice of a programming language to code it, a platform to run the resulting program, and a compiler that can turn the code into a program executable on this platform. The realm of quantum computation is currently less developed: several competing platform co-exists, and in 2011, at the beginning of the QCS project, no scalable quantum programming language even existed.

From a programmer's perspective, quantum computation is very close to classical computation. The main difference lies in the use of a special kind of memory with exotic properties: in particular, quantum data is non-duplicable and reading quantum data is a probabilistic operation. The interaction with the quantum memory is done by a sequence of elementary operations that are summarised by what is known as a quantum circuit. A quantum algorithm mainly consists of the construction of such circuits, their execution on the quantum memory, and various classical pre- and post-processing.

This hints at the main required design choice: a quantum programming language is primarily a circuit-description language. However, quantum algorithms are not simply fixed, static quantum circuits. Unlike classical circuitry such as FGPAs, quantum algorithms describe families of quantum circuits: the circuit depends on the size and shape of the input data. A quantum programming language therefore has to account for this parametricity. Quipper has been designed from the ground up with these aspects in mind. Following a successful trend in domain specific languages, Quipper is an embedded language within a host language. The chosen host language is Haskell. This modern, functional language features an expressive type system making it easy to define and enforce the specificities of circuit construction and manipulation. Parametricity is naturally obtained with the use of lists and list combinators. The construction of a circuit is modelled as printing on a particular kind of output channel: generating an elementary instruction corresponds to writing it on the channel. Within Haskell, this kind of side-effect can naturally be encapsulated within a type construct known as monad. This automatically outlaws various ill-defined programs, renders their coding less error-prone while easing debugging.

Quipper has been used to code large algorithms and perform logical resource estimation: for a given set of parameters to the problem, what is the size of circuit generated by the algorithm? The size can be counted in the number of elementary, logical operations and in the size of the required quantum memory footprint. The analysis shows that for naive implementations, these numbers can be quite large, yielding unrealistic circuits. This analysis tends to show that producing usable algorithms requires more than concentrating on complexity analysis. Nowadays, it is possible to do so: with the help of programming languages such as Quipper, a quantum algorithm designer can effectively analyse and tune its algorithm for concrete use-cases.

The advent of modern quantum programming languages clears a path towards the design of quantum compilation stacks and tools for certification of quantum programs. Quipper is currently the backbone of two projects aiming at such goals. The European Itea3 project Quantex spanning across France, Netherlands and Germany gathers Atos/Bull, CEA/Leti, LORIA, LRI, TUDelft, KPN, Siemens and Univ. Tübingen. Quantex aims at developing the programming environment around Quipper and focuses on the compilation towards emulation of quantum computation. The recently started French ANR SoftQPro is centered on a formalisation of Quipper's semantics toward certification, and on the development of a compilation stack based on the graphical calculus ZX, envisioned as a more natural intermediate representation than existing proposals.

Link: [L1] https://kwz.me/hB6

References:

[1] A. S. Green, P. L. Lumsdaine, N. J. Ross et al.: "Quipper: A Scalable Quantum Programming Language", in Proc. of PLDI 2013, ACM SIGPLAN Notices, Vol. 48 Issue 6, pp. 333-342, 2013.

[2] B. Valiron, N. J. Ross, P. Selinger et al.: "Programming the Quantum Future", Communications of the ACM, Vol. 58 No. 8, pp. 52-61, 2015.

[3] A. Scherer, et al.: "Concrete resource analysis of the quantum linear-system algorithm used to compute the electromagnetic scattering cross section of a 2D target", Quantum Information Processing 16:60, 2017.

Please contact:

Benoît Valiron, LRI – CentraleSupelec, Univ. Paris Saclay, France
benoit.valiron@lri.fr

Diagram Transformations Give a New Handle on Quantum Circuits and Foundations

by Aleks Kissinger (Radboud University)

String diagrams provide a powerful tool for uncovering hidden algebraic structure in quantum processes. This structure can be exploited to optimise quantum circuits, derive fault-tolerant computations, and even probe the foundations of physics.

Quantum computers have the ability to reshape the modern world, offering huge computational speed-ups for a wide variety of problems in mathematics, physics, chemistry, and computer science. However, the existing and emerging quantum computational devices face stringent limitations in memory, computational power, and tolerance to noise, making it crucial to develop sophisticated techniques for optimising the software which drives

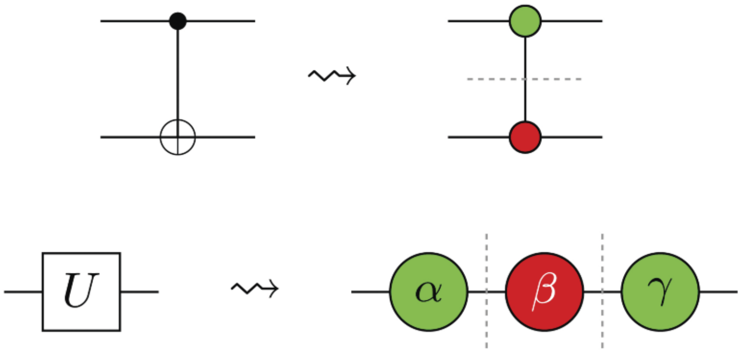


Figure1: Decomposing quantum gates into more primitive pieces called "spiders".

these systems. Quantum circuits have become the de facto "assembly language" for quantum software. They describe computations in terms of a series of primitive operations, called quantum gates, performed on a register of quantum bits (qubits), which is then measured to give a result. While quantum gates are useful as building blocks for computations, they lack a well-understood algebraic structure, making it difficult to understand when two circuits are equivalent (i.e., describe the same computation) or to transform one circuit into another for the sake of optimisation or fault-tolerance.

In 2008, researchers at Oxford University produced a unique solution to this problem: the ZX-calculus. Originally developed as an abstract method for studying the behaviour of complementary observables in quantum mechanics (indeed the 'Z' and 'X' refer to the complementary Pauli observables of the same name), the ZX-calculus quickly showed itself to be a useful practical language for reasoning about quantum circuits, as well as other qubit-based models of computation, such as measurement-based quantum computation. The ZX-calculus works by decomposing quantum gates into even more primitive components, called "spiders" (Figure 1). These basic pieces satisfy a small number of algebraic laws, which in turn yield a great deal of power. For example, the four laws shown in Figure 2 suffice to transform any two equivalent Clifford quantum circuits into the same circuit. Clifford circuits are a well-studied class of circuits which can be simulated efficiently on a classical computer, so it may not be too surprising that the ZX-calculus gives an easy, algebraic handle on circuit equivalence. However, what is surprising is that groups in Oxford and LORIA (a research unit affiliated with ERCIM member Inria) have shown in recent months that an extension to these rules can decide equality for Clifford+T circuits [1] and even a fully universal family of quantum circuits [2]. These families of circuits are capable of producing any quantum computation imaginable (or, in the case of Clifford+T, approximating it to arbitrarily high precision). Thus, a complete algebraic characterisation of equivalence for these circuits is a major breakthrough.

The ZX-calculus—including the extensions proposed by the Oxford and LORIA groups—is based on string diagrams, which can be seen as a sort of generalisation of quantum circuits. They first appeared in the work of Penrose in the 1970s, and since then have been applied to a broad range of applications in physics and computer science, including tensor networks in high-energy physics, signal-flow graphs, electrical and electronic circuits, computational linguistics, and concurrent computation. Earlier this year, Coecke and Kissinger published a textbook which gives a comprehensive introduction to quantum theory, quantum computation, and quantum foundations purely in the language of string diagrams [3].

String diagrams not only provide a unique and intuitive way to introduce the core concepts of quantum theory, but also a dramatically different way of working with quantum mechanical processes. Within the diagrammatic approach to quantum theory (a.k.a. "Categorical Quantum Mechanics", see link [L2]), concepts such as connectivity, composition, and interaction take centre stage, whereas concrete Hilbert-space calculations are secondary. For example, foundational questions around

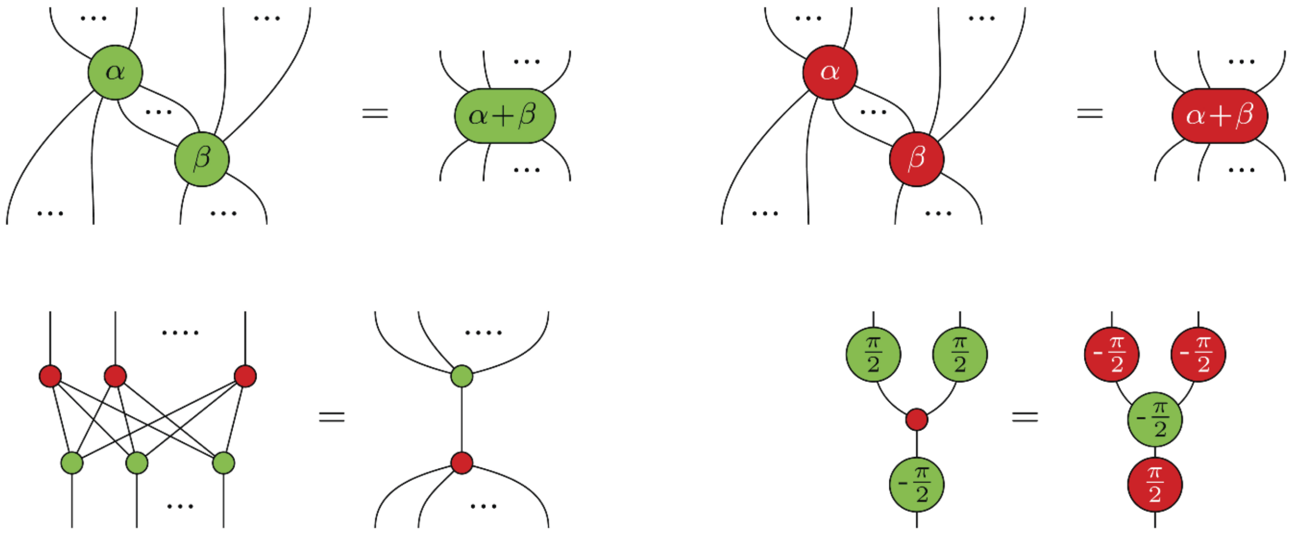
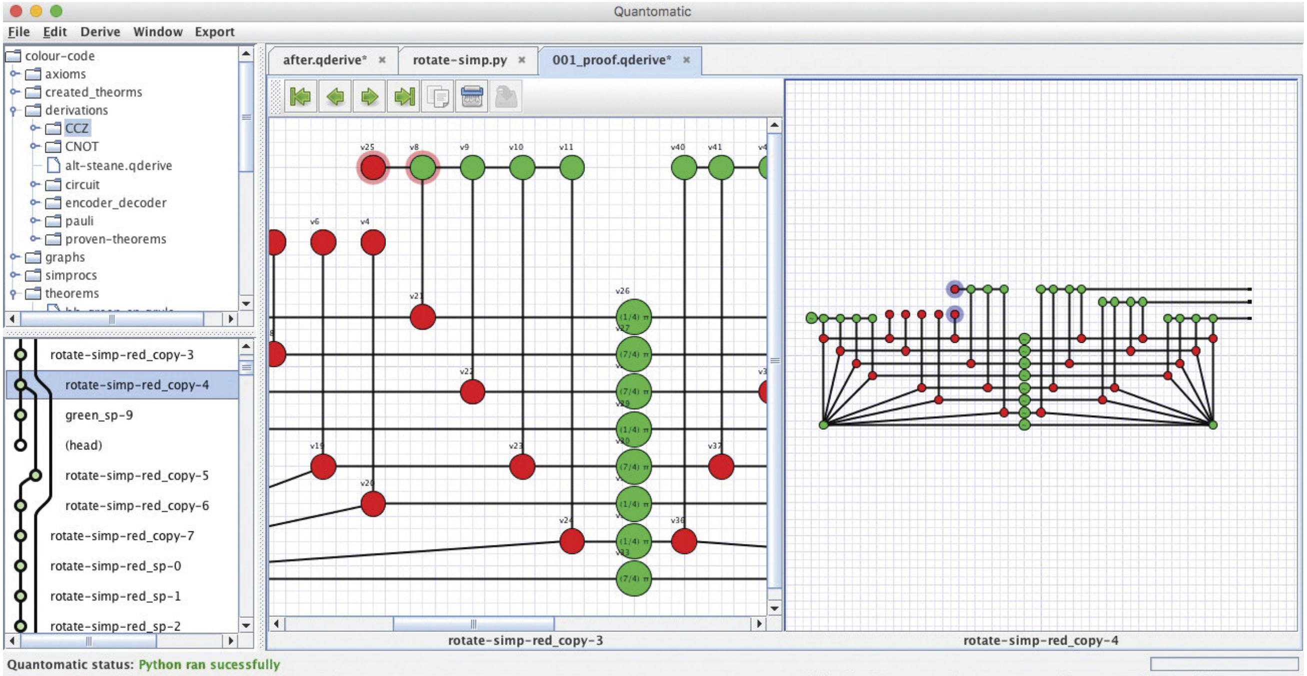


Figure 2: The rules of the ZX-calculus, which suffice to derive all equations that hold between Clifford circuits.



Quantomatic status: Python ran sucessfully

Figure 3: Quantomatic, a proof assistant for diagrammatic reasoning. Here, it is computing a transversal implementation of a CCZ gate within a quantum error correcting code (namely, the [[8,3,2]] colour code; see links [L1] and [L3] for more details).

quantum non-locality and quantum causal structure can be posed in terms of whether a diagram decomposes in a certain way across time and space, and what consequences that decomposition has on our observations.

More pragmatically, quantum algorithms and communication protocols can be proven correct using diagram transformation rules, even in cases involving far too many qubits for concrete calculation. To assist with producing, checking, and sharing these proofs, researchers at Radboud University, University of Strathclyde, and Oxford have developed a tool called Quantomatic (Figure 3). Quantomatic is a “proof assistant for diagrammatic reasoning”. Using a combination of human-guided diagram transformations and automated rewrite strategies (programmable in a Python-based strategy language), it is possible to perform a variety of tasks in Quantomatic, such as optimising small to medium-sized quantum circuits, verifying multi-party communication protocols, and computing encoded logical operations within certain families of quantum error correcting codes.

The teams in Nijmegen, Oxford, LORIA, and Strathclyde, with the help of collaborators at LRI, Durham, and the UK’s NQIT Quantum Hub, are now aiming to produce fully automated techniques for circuit optimisation, scale up to large computations on hundreds of logical qubits (with error correction), and develop new kinds of transformation procedures to work within the constraints of first-generation quantum hardware, such as limited topologies for qubit interactions and distinguished gate- vs. memory-optimised physical qubits.

Links:

[L1] http://quantomatic.github.io
[L2] http://cqm.wikidot.com
[L3] https://kwz.me/hB7

References :

[1] E. Jeandel, S. Perdrix, R. Vilmart: “A Complete Axiomatisation of the ZX-Calculus for Clifford+T Quantum Mechanics”, Preprint, arXiv:1705.11151. 2017.

[2] K. Ng, Q. Wang: “A universal completion of the ZX-calculus”, Preprint, arXiv:1706.09877. 2017.

[3] B. Coecke, A. Kissinger: “Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning”, Cambridge University Press. 2017.

Please contact:

Aleks Kissinger
iCIS Radboud Universiteit, The Netherlands
aleks@cs.ru.nl

Quantum Computers and Their Software Interfaces

by Peter Mueller, Andreas Fuhrer and Stefan Filipp (IBM Research – Zurich)

Scientific groups in industry and academia have made enormous progress in the implementation of first quantum computer prototypes. IBM's quantum experience with five and 16 qubits are already publicly accessible in the cloud. Three "standard" software interfaces are available. Client systems with 20 qubits ready for use and the next-generation IBM Q system is in development with the first working 50 qubit processor.

Quantum computers are expected to solve problems which are intractable to classical information processing. Built on the principles of quantum mechanics, they exploit the complex and fascinating laws of nature at the molecular and atomic level, which usually remain hidden from view. By harnessing this quantum behaviour, quantum computing can run new types of algorithms to process information in extremely large state spaces. These algorithms may one day lead to revolutionary breakthroughs in materials simulation, the optimisation of complex manmade systems, and in machine learning.

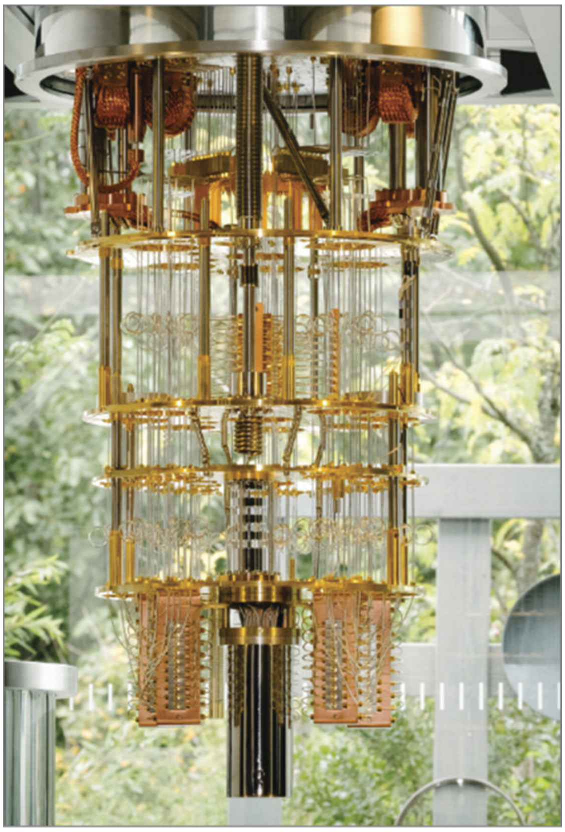


Figure 1: Open cryogenic system for a 50 qubit quantum computing device. The device is hidden inside the shielding tube attached at bottom center. The copper structures to the left and right of the shielding tube contain parametric quantum amplifiers to readout information from the qubits.

Quantum computers are based on qubits, which operate according to two key principles of quantum physics: superposition and entanglement. Superposition means that each qubit can represent both a "1" and a "0" at the same time [1]. It leads to what is called "quantum parallelism", an effect that allows an n-qubit register to store all 2n possible states at the same time. Entanglement means that the state of multiple qubits can be correlated with each other; that is, the state of one qubit (whether it is a "1" or a "0") depends on the state of one or more other qubits and the qubit can no longer be described separately. Using the principle of entanglement creates additional processing capabilities which are not available on classical processors.

IBM's quantum devices are built on superconducting Josephson junction technology which requires cryogenic temperatures as depicted in Figure 1. The quantum bits are anharmonic LC resonators, known as transmon qubits [2], where the non-linear inductor (L) is implemented by a Josephson junction. The left outer device in Figure 2 shows five square shaped qubits (a). The meandering connections (b) are coplanar waveguides (CPW). They are used to couple qubits with each other for information processing and to couple qubits to I/O ports (c) to manipulate, write and read the qubits. All the qubit manipulations and readout processes are controlled by microwave pulses in the range of 4 to 8 GHz.

The "IBM Q experience" provides a platform to explore basic quantum circuits on real quantum devices as shown in Figure 2 (left and middle). Currently, 5-qubit and 16-qubit devices are publicly available to run user programs from the cloud. Alternatively, a cloud-based simulator software which handles up to 20 qubits can be chosen. Examples of the three different programming interfaces are depicted in Figure 3. The graphical user interface is the simplest way to access the real

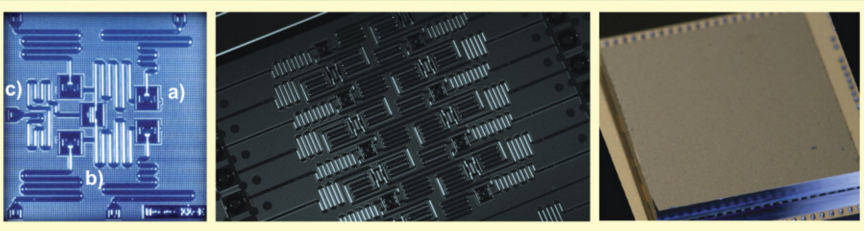
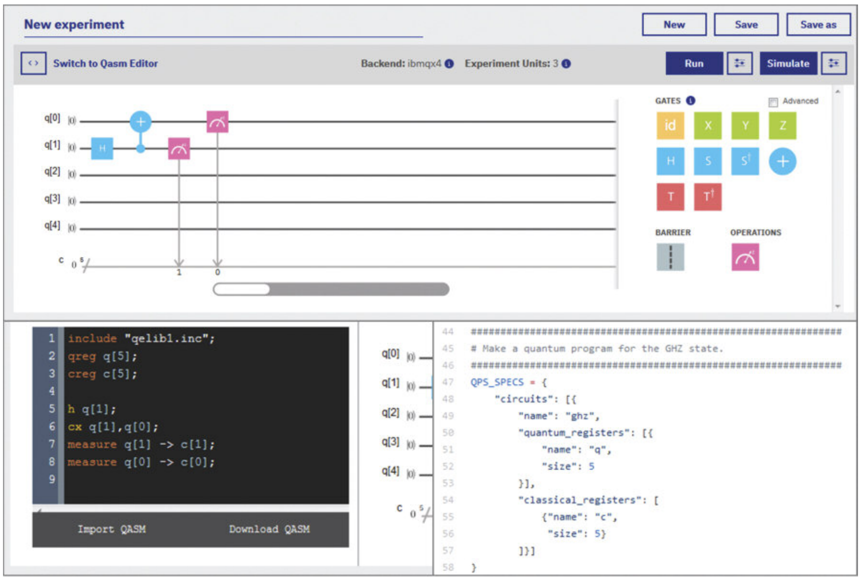


Figure 2: An experimental 5-qubit (left) and 16-qubit (mid) device as used in the publicly available "IBM Q experience" and a package as used for the upcoming 20/50 qubit devices (right). For further details see text.



```
include "qelib1.inc";
qreg q[5];
creg c[5];

h q[1];
cx q[1],q[0];
measure q[1] -> c[1];
measure q[0] -> c[0];
```

```
######################################################################
# Make a quantum program for the GHZ state.
######################################################################
QPS_SPECS = {
    "circuits": [{
        "name": "ghz",
        "quantum_registers": [{
            "name": "q",
            "size": 5
        }],
        "classical_registers": [
            {"name": "c",
             "size": 5}
        ]}]
}
```

Figure 3: The three "IBM Q experience" web interfaces – graphical user interface (top), OpenQASM assembler (bottom left) and the Quantum Information Software Kit (bottom right) – give access to the experimental five and 16 qubit circuits.

quantum hardware using a web browser. OpenQASM [3] is a low level hardware interface which enables compatible software stacks to be built. For more advanced developments, the Quantum Information Software Kit (QISKit) is an open-access programing interface which provides highest functionality for working with both, the real quantum processors and various software based quantum simulators. The open-access interface allows a user-application to integrate the quantum processor as an accelerator, through the cloud.

On the application side, calculations of e.g., the ground state energies of small molecules such as H2, LiH and BeH2 have been reported. Further examples are shown in the links given below. The "IBM Q experience" provides a platform to explore basic quantum circuits on real quantum processors based on superconducting qubits. It has been used by more than 60,000 users and has already generated more than 35 third-party research publications on applications of quantum computing. On the software side, a growing number of developers are using QISKit. To summarise, the time is now to join forces, execute and continue to make key breakthroughs on this revolutionary journey of information technology.

Links:
http://ibm.com/ibmq/
http://www.qiskit.org/
http://math.nist.gov/quantum/zoo/

References:

[1] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information", 10th edt., Cambridge University Press, 2010.
[2] J. Koch et al., "Charge-insensitive qubit design derived from the Cooper pair box", Phys. Rev. A 76, 042319, 2007.
[3] A. W. Cross et al., "Open Quantum Assembly Language", [arXiv:1707.03429], 2017.

Please contact:

Peter Mueller
IBM Research – Zurich, Switzerland
pmu@zurich.ibm.com

Chevalley-Warning Theorem in Quantum Computing

by Gábor Ivanyos and Lajos Rónyai (MTA SZTAKI, Budapest)

Effective versions of some relaxed instances of the Chevalley-Warning Theorem may lead to efficient quantum algorithms for problems of key practical importance such as discrete logarithm or graph isomorphism.

The Theory of Computing Research Group of the Informatics Laboratory at MTA SZTAKI has expertise in algebraic aspects of quantum computing, including quantum algorithms for algebraic and arithmetical problems, as well as application of algebraic methods as ingredients of quantum algorithms. Some of our projects aim at discovering hidden algebraic structures, e.g., symmetries of certain objects. A main example is the so-called "hidden subgroup problem", which includes such prominent special cases as the task of computing discrete logarithms and the question of finding isomorphisms of graphs. The object we are given is a function *f* defined on a large finite group *G* and we are looking for the subgroup *H* consisting of all elements h for which *f(xh)* = *f(x)* for every *x* from *G*. In other words, *H* is the group of elements whose action leaves *f* invariant. (We remark note that in most cases, we further require that *f* is such that *f(x)* = *f(y)* if and only if *y* = *xh* for some *h* from *H*.) Perhaps the simplest and best known example of this is finding periods for functions defined on the integers. One of the greatest successes of quantum algorithms, Shor's method for factoring integers, is based on finding such a period. Computing discrete logarithms in various settings are is also an instance of the hidden subgroup problem over abelian groups.

The graph isomorphism problem can be cast as an instance of the hidden subgroup problem over a noncommutative group *G*. In contrast with the commutative case, for which efficient quantum algorithms are known, the complexity of the noncommutative hidden subgroup problem has remained open even for certain groups that are very close to commutative ones. Among the few positive results in this direction, we mention our polynomial time algorithm, developed in a joint work [1], which finds hidden subgroups in a fairly wide class of groups in which the order of the elements is bounded by a constant. The overall progress is much more modest even in "so-called two-step solvable groups" (these are in a certain sense composed of two commutative groups) in which elements of larger order are present.

With our collaborators we found [2] that the hidden subgroup problem for a subclass of such groups can be further generalised to another class of problems regarding hidden algebraic structure. In this class, the hidden object is a polynomial map between vector spaces over a finite field. Certain hidden subgroup problems can be formulated as hidden polynomial map instances (there is a reduction in the other direction as well, but this results in a bigger hidden subgroup problem). A simple illustrative example of a hidden polynomial map is as follows: let *f(X)* be an unknown univariate polynomial of constant degree. We have access to a quantum oracle which returns $E(Y^2\text{-}f(X))$ for given pairs *(X,Y)*. Here *E* is an unknown injective encoding of the field. The task is to determine *f* (up to constant term). We developed [2,3] a polynomial time quantum algorithm for finding such hidden polynomial maps under the assumption that they have constant degree.

One of the critical ingredients of our quantum algorithm is a classical algorithm that under certain conditions finds a nontrivial solution of a system of polynomial equations of a very special kind, for which the basic and famous Chevalley-Warning theorem of number theory ensures the existence of a nontrivial solution. Our system is obtained from a system of homogeneous linear equations by replacing each variable by its d-th power where d is a fixed positive integer:

$$\begin{array}{rcl} a_{11}x_1^d + \cdots + a_{1n}x_n^d & = & 0 \\ \vdots & \vdots & \vdots \\ a_{m1}x_1^d + \cdots + a_{mn}x_n^d & = & 0. \end{array}$$

The condition that allowed us a method running in polynomial time is that the number of variables, compared to the number of equations and the degree *d*, is sufficiently large. (Here by polynomial time we mean time bounded by a function polynomial in the bit size of the array of the coefficients, which is the number of equations, *m*, times the number of variables, *n*, times the logarithm of the size of the base field). In the quantum setting in which our algorithm is applied, the degree is essentially the degree of the hidden polynomial map and the number of equations is related to the dimension of the underlying spaces, while we are allowed to choose the number of variables. (Note however, that the system is not required to be sparse, the *n* times *m* array of the coefficients can be arbitrary.)

Observe that without any assumption on the number *n* of variables, already over the field consisting of three elements the quadratic case of the problem becomes NP-hard. This can be shown by a modification of the standard reduction of *SAT* to *Subset sum*. (In fact, that case of the problem is just finding a zero-one solution of the corresponding linear system.) On the other hand, from the Chevalley-Warning Theorem it follows that if *n* > *md*, then our system always has a nontrivial solution. Then an interesting question arises: how hard is it to find a nontrivial solution? There is some evidence (such as the above mentioned hardness result) that this question is too difficult when the number of variables is close to the Chevalley-Warning bound *md*. For this reason, we look for an efficient solution for relaxations in which *n* is substantially larger than this bound. First, it is worth noting that by a simple and natural recursive algorithm, it is easy to find a solution in polynomial time, when the number *n* of variables is greater than a function like *d* raised to the *m*-th power. This method is useful when m is constant. What can we say when d is kept constant? For this variant of the problem, we have developed a much more sophisticated algorithm [3]. This result is probably not optimal and an improvement could be a first step toward quantum algorithms for finding hidden polynomial maps of higher degree and toward hidden subgroup algorithms in some more complex groups.

References:

[1] K. Friedl, et al: "Hidden translation and translating coset in quantum computing" SIAM Journal on Computing 43 (2014), pp. 1-24.

[2] T. Decker, et al.: "Polynomial time quantum algorithms for certain bivariate hidden polynomial problems", Quantum Information and Computation 14 (2014), pp. 790-806.

[3] G. Ivanyos, M. Santha: "Solving systems of diagonal polynomial equations over finite fields," Theoretical Computer Science 657 (2017), pp. 73-85.

Please contact:

Gábor Ivanyos and Lajos Rónyai
MTA-SZTAKI, Hungary
gabor.ivanvos@sztaki.hu,
lajos.ronyai@sztaki.hu

Hardware Shortcuts for Robust Quantum Computing

by Alain Sarlette (Inria) and Pierre Rouchon (MINES ParisTech)

Despite an improved understanding of the potential benefits of quantum information processing and the tremendous progress in witnessing detailed quantum effects in recent decades, no experimental team to date has been able to achieve even a few logical qubits with logical single and two qubit gates of tunably high fidelity. This fundamental task at the interface between software and hardware solutions is now addressed with a novel approach in an integrated interdisciplinary effort by physicists and control theorists. The challenge is to protect the fragile and never fully accessible quantum information against various decoherence channels. Furthermore, the gates enacting computational operations on a qubit do not reduce to binary swaps, requiring precise control of operations over a range of values.

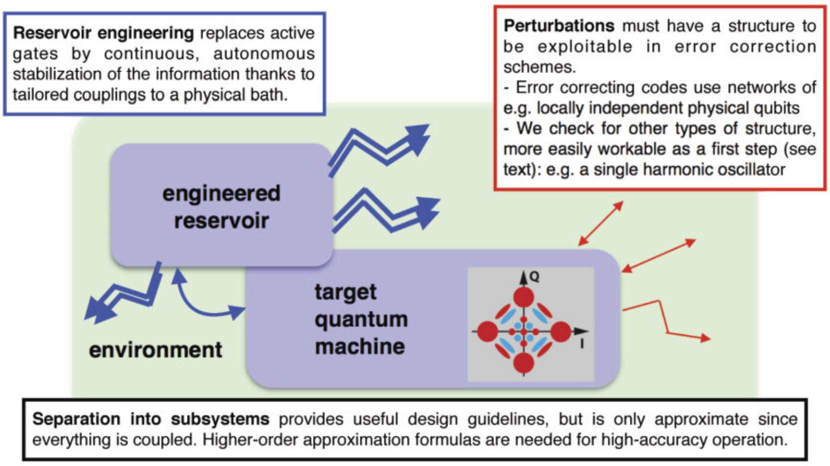
The major issue for building a quantum computer is thus to protect quantum information from errors. The quantum counterpart of error correcting codes provides an algorithmic solution, based on redundant encoding, towards scaling up the precision in this context. However, it first requires technology to reach a threshold at which the hardware achieves the following on its own:

- all operations, in any big system, must already be accurate to a very high precision;
- the remaining errors follow a particular scaling model, e.g., they are all independent in a network of redundant qubits.

Under these conditions, adding more physical degrees of freedom to encode the same quantum information keeps leading to better protection. Otherwise, the fact that new degrees of freedom and additional operations also carry new possibilities for inducing errors or cross-correlations, can degrade the overall performance.

In the QUANTIC lab at Inria Paris [L1], we are pursuing a systems engineering approach to tackle this issue by drawing inspiration from both mathematical control theory and the algorithmic error correction approach (Figure 1).

A first focus of the group is to design a hardware basis where a large Hilbert space for redundant encoding of information comes with just a few specific decoherence channels. Concentrating efforts on rejecting these dominant noise sources allows more tailored and simple stabilising control schemes to be applied to improve the quality of these building blocks towards more complex error correction strategies. Such hardware efficiency is typically achieved when many energy levels are associated to one and the same physical degree of freedom. A prototypical example is the “cat qubit”, where information about a single qubit is redundantly encoded in the infinite-dimensional state space of a harmonic oscillator, in such a way that the dominant errors reduce to the single photon loss channel; and this error is both information-preserving and non-destructively detectable. This overcomes the need for tracking multiple local error syndromes and applying according corrections in a coupled way, as would be the case for a logical qubit encoded on a network of spin-1/2 subsystems. An implementation of this principle in superconducting circuits has recently achieved the first quantum memory improvement thanks to active error correction.


Reservoir engineering replaces active gates by continuous, autonomous stabilization of the information thanks to tailored couplings to a physical bath.

Perturbations must have a structure to be exploitable in error correction schemes.
- Error correcting codes use networks of e.g. locally independent physical qubits
- We check for other types of structure, more easily workable as a first step (see text): e.g. a single harmonic oscillator

Separation into subsystems provides useful design guidelines, but is only approximate since everything is coupled. Higher-order approximation formulas are needed for high-accuracy operation.

Figure 1: General scheme of our quantum error correction approach via “hardware shortcuts”. The target “quantum machine” is first embedded into a high-dimensional system that may have strong decoherence, but only along a few dominating channels (red). Then, a part of the environment is specifically engineered and coupled to it in order to induce a strong information-stabilising dissipation (blue). This entails stabilising the target quantum machine into a target subspace, e.g., “four-legged cats” of a harmonic oscillator mode; and possibly, replacing the measurement of error syndromes and conditional action, by a continuous stabilisation of the error-less codewords. Development of high-order model reduction formulas is needed to go beyond this first-order idea and reach the accuracies enabling scalable quantum information processing.

A second point of attention is the speed of operations. Indeed, quantum operations take place at extremely fast timescales — e.g., tens of nanoseconds in the superconducting circuits favoured by several leading research groups. This leaves little computation time for a digital controller acting on the system. Conversely, it hints at the fact that a smartly designed quantum system could stabilise fast on its own onto a protected subspace, possibly in combination with a few basic control primitives. Such autonomous stabilisation can be approached by a “reservoir engineering” strategy, where conditions are set up for dissipation channels to systematically push the system into a desired direction. This can enact e.g., fast reset of qubits, or error decoding and correction, all in one fast and continuously operating (“pumping”) hardware without any algorithmic gates. Such “reservoir engineering” also plays an important role in effectively isolating quantum subsystems with particularly concentrated error channels, thus in creating the conditions of the previous paragraph.

This brings us to the more mathematical challenges. The design of engineered reservoirs, such as the singling out of a "quantum machine" from its environment, is based on approximations where weak couplings are neglected with respect to dominant effects. These approximations enable tractable systems engineering guidelines to be derived — rather than having to treat a single big quantum bulk, whose properties are one target of the quantum computers themselves. Current designs are based on setting up systems with first dominant local effects. This has to be improved and scaled up to reach the requirements 1. and 2., since every control scheme can only be as precise as its underlying model. We are therefore launching a concrete effort towards high-precision model reduction formulas, together with the superconducting circuit experimentalists to identify typical needs, but with a general scope in mind. Preliminary work already shows the power of higher-order formulas in identifying design opportunities (Figure 1), paving the way to improved "engineered" hardware for robust quantum operation.

Link:
[L1] https://www.inria.fr/en/teams/quantic

References:

[1] M. Mirrahimi, Z.Leghtas et al: "Dynamically protected cat-qubits: a new paradigm for universal quantum computation", New Journal of Physics, 2014.

[2] N. Ofek et al.: "Extending the lifetime of a quantum bit with error correction in superconducting circuits", Nature, 2016.

[3] J. Cohen: "Autonomous quantum error correction with superconducting qubits", PhD thesis, ENS Paris, 2017.

Please contact:

Alain Sarlette, Pierre Rouchon, Inria
alain.sarlette@inria.fr,
pierre.rouchon@mines-paristech.fr
+ 33 1 80 49 43 59

Quantum Gates and Simulations with Strongly Interacting Rydberg Atoms

by David Petrosyan (IESL-FORTH)

In order to develop functional devices for quantum computing and analogue and digital quantum simulations, we need controlable interactions between the physical systems representing quantum bits – qubits. We explore strong, long-range interactions between atoms excited to high-lying Rydberg states to implement quantum logic gates and algorithms and to realise quantum simulators of various spin-lattice models to study few- and many-body quantum dynamics.

Quantum systems with many degrees of freedom, such as those composed of many interacting subsystems or particles, are notoriously hard to simulate on classical computers. This is because the Hilbert space for the quantum states of the composite system is exponentially large in the system size, while quantum correlations, or entanglement, between the constituent subsystems often preclude factorisation of the problem into smaller parts. This has led Richard Feynman to suggest, back in 1981, to simulate quantum physics with quantum computers, or universal quantum simulators [1] composed of many quantum two-level systems, like spin-1/2 particles arranged in a lattice, with appropriately controlled couplings between them. In principle, any many-body Hamiltonian dynamics can be decomposed into small time-steps and finite-range interactions between the qubits. This idea has then developed into a general purpose quantum computer which is suitable not only for digital simulations of physical systems, but also for quantum computations. Quantum algorithms for certain mathematical tasks, such as search of unstructured database (Grover) or integer factorisation (Shor), are polynomially or exponentially more efficient than the best known classical algorithms for the same tasks.

Cold atoms trapped in optical lattices or arrays of microtraps represent a scalable architecture to realise quantum computers as well as analogue and digital quantum simulations of many-body dynamics of various spin lattice models. Neutral atoms in the lower electronic states interact very weakly with each other, but when excited to the Rydberg states, their interaction can be very strong over large distances. Rydberg states are highly excited states with the atomic electron placed on an orbit that is far from the ionic core. Due to weak binding of the electron to the ion, the atoms in the Rydberg states are easily polarisable. The resulting long-range interactions between the Rydberg atoms makes them uniquely suited for realising strongly-interacting many-body systems and for implementing various quantum information processing tasks [2].

The interatomic interactions are controllable by lasers that can excite and de-excite the atoms from the non-interacting ground state to the strongly interacting Rydberg state on demand. This has led to proposals to implement quantum logic gates using the switchable interactions, or interaction-induced excitation blockade, between the atoms representing qubits. There have been several experimental demonstrations of the Rydberg quantum gates, but the fidelity of operations has so far been below the threshold value ~0.9999 for a scalable fault-tolerant quantum computation. We study the performance of quantum algorithms under realistic experimental conditions involving noise and imperfections (see Figure 1). We devise novel schemes for high-fidelity quantum logic gates using blockade and resonant exchange interactions between the Rydberg state atoms. This work is being done in collaboration with the theory group of

Klaus Mølmer at the Aarhus University and the experimental group of Mark Saffman at the University of Wisconsin—Madison, USA.

Arrays of trapped atoms excited on demand to the Rydberg states by lasers can realise various spin-lattice models that can serve for both digital and analogue quantum simulations. In addition to switchable interactions, relaxations and energy dissipation can be introduced in this system in a controlled way. We study the dynamics of few- and many-body quantum systems using such Rydberg quantum simulators. As an example, in Figure 2 we show simulations of quasi-crystals of Rydberg excitation as observed in the experiments with laser driven atoms in optical lattices [3]. We collaborate with the theory group of Michael Fleischhauer at the University of Kaiserslautern, Germany, and part of this work is being done within the EU H2020 FET Proactive project RySQ (Rydberg Quantum Simulations) which involves many leading theory and experimental groups in Europe.

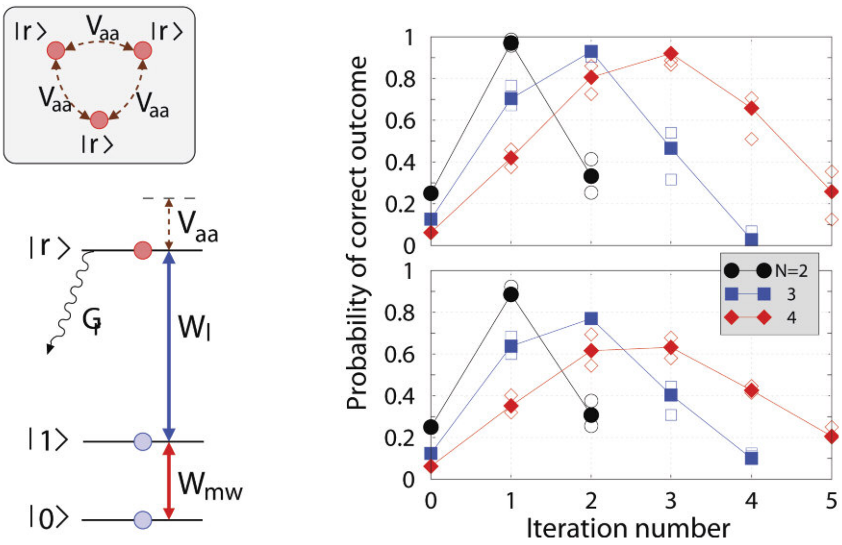


Figure 1: Grover search algorithm with Rydberg blockaded atoms. Left: Level scheme of the register atoms interacting with a microwave field on the qubit transition and with a resonant laser field on the transition to the Rydberg state. Atoms in Rydberg states interact with each other via a strong, long-range potential V_{aa} which suppresses Rydberg excitation of all but one atom at a time. Right: Probabilities of measuring correct outcomes of the Grover search versus number of iterations, for N=2,3,4 digit quantum register, without (top) and with (bottom) decay of the Rydberg state.

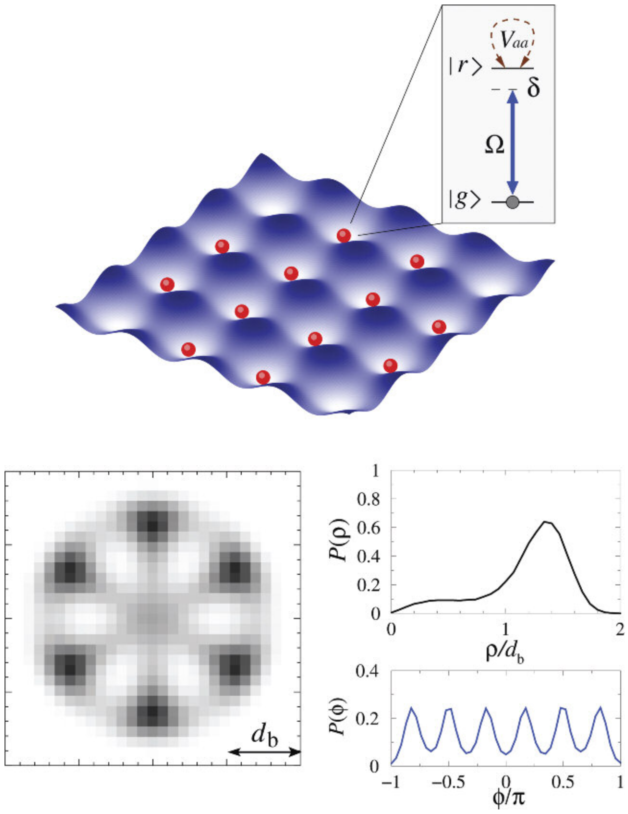


Figure 2: Realising interacting spin lattice models with laser driven atoms. Upper panel illustrates an optical lattice potential for ground state atoms and laser coupling to the strongly interacting Rydberg state. Lower panel shows spatial configuration of six Rydberg excitations, with the axial P(ρ) and angular P(φ) probability distributions, in a 2D disk shaped lattice of 400 atoms driven by a resonant field.

Finally, strong transitions between the Rydberg states of atoms in the microwave frequency range enable their efficient coupling to electrical circuits involving superconducting qubits and resonators. Superconducting qubits can realise fast quantum gates but are less suitable for storage of quantum information. Coupling atoms to solid-state systems permits the realisation of hybrid quantum systems composed of different components with complementary functionalities including quantum information processing, storage and conversion to optical photons for long-distance quantum communication. This is another direction of our research on quantum computation and simulations with Rydberg atoms.

Links:

http://www.quantum-technology.gr/
http://qurope.eu/projects/rysq/

References:

[1] S. Lloyd: "Universal Quantum Simulators", Science, Vol. 273 (5278), pp. 1073-1078, 1996.

[2] M. Saffman, T. G. Walker, and K. Mølmer, "Quantum information with Rydberg atoms", Rev. Mod. Phys. Vol. 82, pp. 2313-2363, 2010.

[3] P. Schauß et al., "Crystallization in Ising quantum magnets", Science Vol. 347 (6229), pp. 1455-1458, 2015.

Please contact:

David Petrosyan
IESL-FORTH, Greece
+30-2810 39 1131
dap@iesl.forth.gr

Control of Quantum Systems by Broken Adiabatic Paths

by Nicolas Augier (École polytechnique), Ugo Boscain (CNRS) and Mario Sigalotti (Inria)

The dynamics of a quantum mechanical system is described by a mathematical object called Hamiltonian. The possible results of an energy measure are known as the "eigenvalues" (or energy levels) of the Hamiltonian. After an energy measure, the system collapses into a particular state called the eigenstate corresponding to the measured energy. Adding corners to adiabatic paths can be used to generate superpositions of eigenstates with simple and regular control laws.

The goal of quantum control is to design external fields (the controls) whose action induces a prescribed transition between two states of a quantum system.

A widely used technique is based on the principle of adiabatic evolution: If the initial condition is an eigenstate of the controlled Hamiltonian (i.e., the Hamiltonian including the external field) and the variation of the external fields is slow, then the state of the system stays close to the instantaneous eigenstate (namely, the eigenstate of the controlled Hamiltonian with frozen time).

Adiabatic evolution works as described when the energy levels of the controlled Hamiltonian satisfy a gap condition, which means that they stay away from one from another and in particular they do not intersect. The theory can be extended to systems presenting eigenvalue intersections. When the intersection of two eigenvalues is transversal and the initial condition corresponds to the lower eigenvalue then, after the intersection, the trajectory adiabatically follows the eigenstate corresponding to the upper eigenvalue.

One is typically interested in adiabatic paths for which the controls start and end at zero. Such controls may be used to induce nontrivial transitions only if there exist paths in the space of controls that are not passing back and forth through the same intersections. This is why such an adiabatic setup makes sense for control purposes only when the controls have more than one degree of freedom.

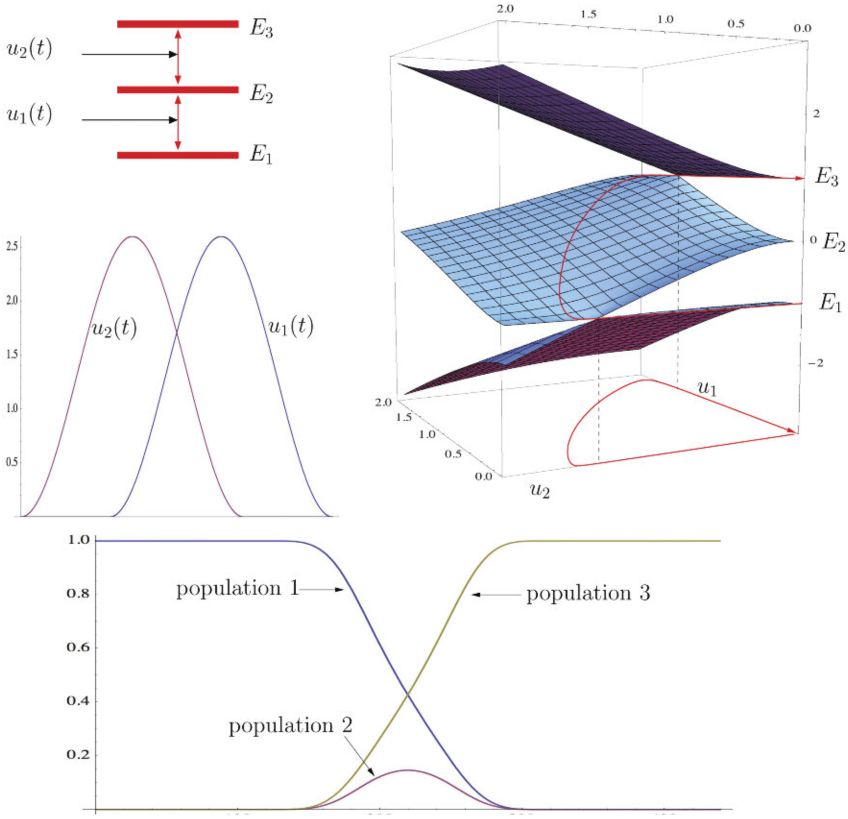


Figure 1: The eigenvalues of a 3-level quantum system driven by 2 controls in the STIRAP configuration.

In the general case one looks at the singular set, i.e., the set of all control values for which the Hamiltonian has degenerate eigenvalues. The applicability of the adiabatic strategy relies on the fact that the singular set does not disconnect the set of available control parameters. Such a disconnection is very rare, however, in the sense that for a generic system the singular set has codimension 3 for complex Hamiltonians and codimension 2 for real ones.

Figure 1 shows the eigenvalues of a 3-level quantum system driven by two controls in the well-known STIRAP configuration. In this case there are two eigenvalue intersections: one between the first and the second levels (on the axis where the first control is zero) and one between the second and the third levels (where the second control vanishes). Notice that the resulting adiabatic strategy follows the famous counter-intuitive pattern, meaning that one first activates the control associated with the transition between the second and the third energy levels and then the one associated with the transition between first and the second ones, with an overlap between the two pulses [1].

The technique explained above provides a simple strategy to induce a transition between any two eigenstates of the free Hamiltonian, under the assumption that all energy levels intersect.

In collaboration with Francesca Chittaro (Toulon University) and Paolo Mason (CNRS, CentraleSupelec) we have developed a technique to create superpositions between eigenstates using broken adiabatic paths [2].

The principle of our approach is that if an adiabatic path reaches a point in the

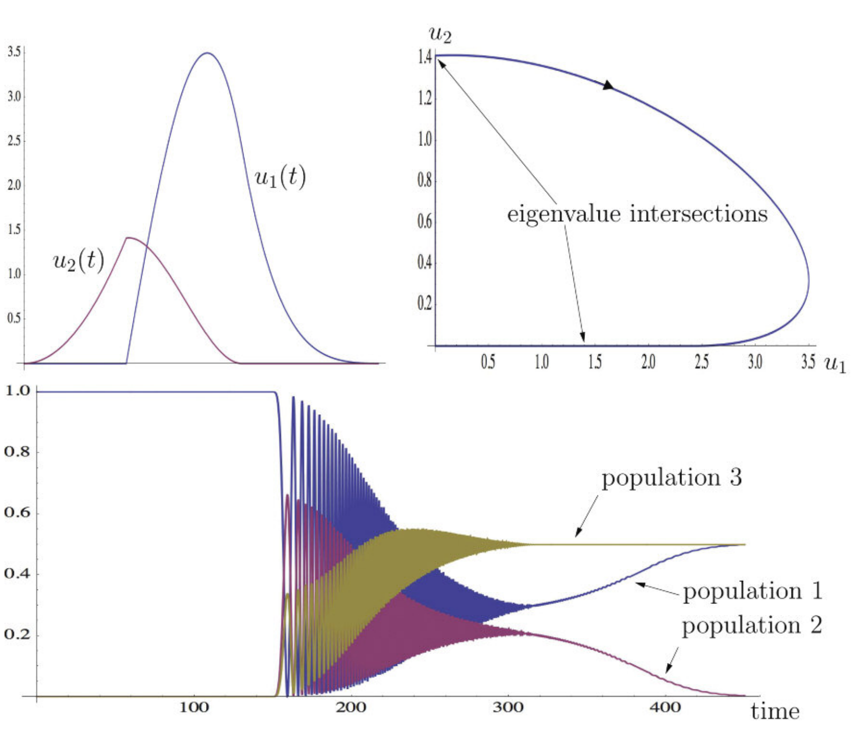


Figure 2: A broken adiabatic path inducing a transition from the first energy level to a superposition of the first and the third energy levels.

singular set and makes there a corner, then the state splits partially on the lower energy level and partially on the upper one. Modulating the entry and exit direction, hence the angle between the two, one can arbitrarily select the occupation of the two energy levels. Such an idea makes it possible, starting from an eigenstate, to reach any superposition of eigenstates whose corresponding eigenvalues intersect [3].

Figure 2, for a 3-level system, shows a broken adiabatic path inducing a transition from the first energy level to a superposition of the first and the third energy levels. Given the desired population levels at the final time, it is possible to compute the angle between the entry and exit direction at the corner in order to induce a transition to a state having such population levels. In the picture, we show for instance a control inducing a transition from an eigenstate corresponding to the first eigenvalue to a superposition with equal weights between the first and the third eigenstates, with no population on the second energy level.

The project is supported by the ERC starting grant GECOMETHODS (2010-2016) and by the French ANR projects GCM (2009-2013). Extensions and algorithmic refinements are under study in the framework of the Inria team CAGE thanks to the support of the French ANR project QUACO (2017-2021).

References:

[1] C.E. Carroll and F.T. Hioe: “Analytic solutions for three-state systems with overlapping pulses”, Phys. Rev. A, vol. 42, pp. 1522-1531, 1990.

[2] U. Boscain et al.: “Adiabatic control of the Schrödinger equation via conical intersections of the eigenvalues”, IEEE Trans. Autom. Control, vol. 57, pp. 1970-1983, Aug. 2012.

[3] U. Boscain et al.: “Approximate controllability, exact controllability, and conical eigenvalue intersections for quantum mechanical systems”, Commun. Math. Phys, vol. 333, pp. 1225-1239, Feb. 2015.

Please contact:

Nicolas Augier, CMAP, École polytechnique, France
nicolas.augier@cmap.polytechnique.fr

Ugo Boscain, CNRS, LJLL, Université Pierre et Marie Curie, France
ugo.boscain@polytechnique.edu

Mario Sigalotti
Inria, LJLL, Université Pierre et Marie Curie, France
mario.sigalotti@inria.fr

The Case for Quantum Software

by Harry Buhrman (CWI and QuSoft) and Floor van de Pavert (QuSoft)

Researchers and industry specialists across Europe have launched a Quantum Software Manifesto. With the Manifesto, the group aims to increase awareness of and support for quantum software research.

Quantum computers, once just the dream of science fiction writers, are rapidly becoming a reality. Already, the first small quantum hardware devices are being put through their paces, with researchers probing for evidence that they really do work in a fundamentally different way, unlocking solutions to problems classical computers could never solve.

Several leading scientists and decision makers, recognising the imminent practical impact of quantum technologies, came together in 2016 to write the Quantum Manifesto [L1] (not to be confused with the Quantum Software Manifesto), calling for an ambitious European quantum technology initiative that would place Europe at the heart of these new developments. After more than 3,400 endorsements from people in scientific, industrial and governmental organisations, the European Commission launched the Flagship Initiative on Quantum Technologies.

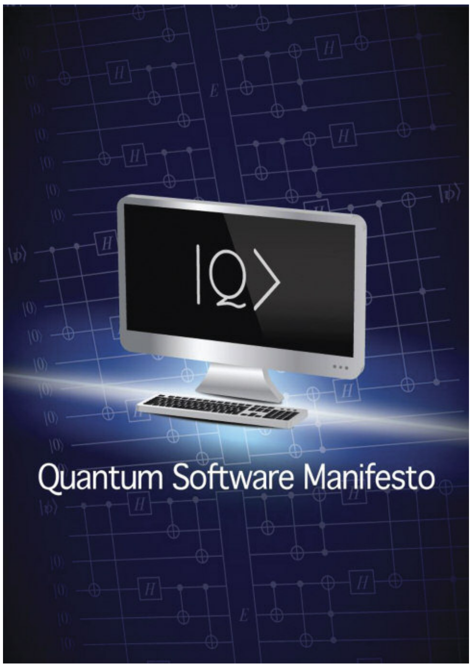
As miraculous as the new quantum hardware may be, though, it can never reach its full potential without great quantum software; this new paradigm will demand new approaches, algorithms and protocols. With this in mind, and spurred by feeling that the Flagship Initiative risks under-representing the crucial role of software and theory, we have developed the Quantum Software Manifesto, which focuses on the status, outlook and specific challenges facing the quantum software field.

It is important to remember, first of all, that quantum computers are no silver bullet: where some problems will see dramatic speedups, others see none at all. Identifying potential applications and designing new quantum algorithms based on new principles will be critical, as will finding ways to achieve a useful quantum advantage on the small, noisy devices that are likely to be available in the short to medium term. We need both foundational, theoretical breakthroughs and practical work on optimising algorithms for real quantum architectures. That, in turn, will demand ever-closer collaboration between software and hardware developers, and between academic and industrial partners.

In particular, developing reliable quantum computers is exceedingly difficult because their basic building blocks, called qubits, are so fragile. Even the tiniest environmental perturbation can destroy their delicate superposition states. Software techniques for quantum error correction and fault-tolerant computation could greatly ease the task of hardware design, helping to pave the way for large, stable quantum systems. New verification and testing protocols based on new theoretical ideas will also be essential to both guarantee than such devices are functioning correctly and guide their design.

Important practical applications include simulating physical and chemical systems, approximate optimisation and machine learning. Classical computers find it notoriously difficult to simulate quantum systems; indeed, this currently takes up about 20% of supercomputer time. In contrast, little could be more natural for a quantum computer, and this will be vital in fields such as quantum chemistry, materials science and high-energy physics. Many exciting experiments are already bringing this idea closer to reality.

Machine learning is another hot topic in the modern world, and a flurry of new developments in this area have been kicked off by the discovery of an exponential quantum speedup for solving particular types of linear equations. This has led to new algorithms for core problems such as data fitting, support vector machines and classification. Indeed, a new quantum recommender can already help users of, say Netflix or Amazon, to find good options exponentially faster. But the real work has still has to begin in finding applications where these techniques can be exploited.



The Quantum Software Manifesto tcalls for increased awareness of the importance and urgency of quantum software research.

Quantum algorithms have the potential to both break current cryptography (via Shor’s algorithm) and provide new and fundamentally more secure cryptosystems, in principle even allowing users to run programs on untrusted systems while keeping their data secret. Practical and commercial technologies have already been developed for quantum key distribution and random number generation, but much work remains to fully develop the potential of quantum cryptography, particularly for large-scale quantum networks.

Quantum networking has already been demonstrated, with entangled states being successfully distributed from satellites to ground stations. As well as allowing truly secure communication, a global quantum internet would enable distributed quantum algorithms to exploit the power of quantum teleportation and error correction to solve distributed tasks that require quantum resources or for which they can make the communication more efficient..

If any of these developments can come to pass, however, we will need more good quantum programmers. Because working with quantum computers is so fundamentally different from classical programming, the pool of people with the necessary knowledge is currently small and new education programs are urgently needed, in both academia and industry. Although some initial steps have been taken, a proposed curriculum is still in its infancy.

We stand at the dawn of the quantum era. It may be imminent, or may take a little while longer to materialise, and we believe it is investment in quantum software and programmers that will make the difference. This will help us to build practical hardware and develop life-changing applications, but none that will be possible without an integrated approach to quantum hardware and software development by industry and academia.

The Quantum Software Manifesto can be downloaded via [L2].

Link:
[L1] https://kwz.me/hBj
[L2] https://kwz.me/hBq

Please contact:
Harry Buhrman,
QuSoft and CWI, The Netherlands
Floor van de Pavert
QuSoft, The Netherlands
+31 (0)20 592 4189
info@qusoft.org

Computers that Negotiate on Our Behalf

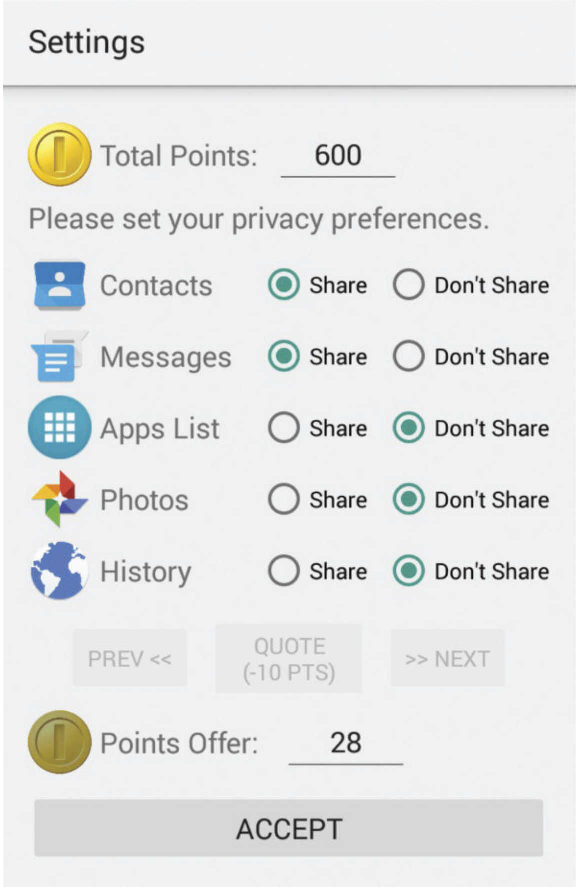
by Tim Baarslag (CWI)

Computers that negotiate on behalf of humans hold great promise for the future and will even become indispensable in emerging application domains such as the smart grid, autonomous driving, and the Internet of Things. An important obstacle is that in many real-life settings, it is impossible to elicit all information necessary to be sensitive to the individual needs and requirements of users. This makes it a lot more challenging for the computer to decide on the right negotiation strategy; however, new methods are being created at CWI that make considerable progress towards solving this problem.

Imagine a system that helps a group of friends decide on a holiday destination based on their individual preferences about cultural activities, costs, and flight duration. After that, the system contacts a number of travel operators to negotiate the best hotel and airline deal and proposes a joint holiday schedule. This is what researchers believe we can one day expect from the research field of automated negotiation: a domain of mathematics and computer science that designs algorithms that can negotiate with people and among computerised systems. As part of the NWO Innovational Research Incentives Scheme Veni and the EU project GridFriends, CWI is developing technology that can help computers get the best deal for users, even when their preferences are not fully specified.

The field of automated negotiation is fueled by a number of benefits that computerised negotiation can offer, including better (win-win) and faster deals, and reduction costs, stress and cognitive effort on the part of users [1]. Autonomous negotiation technology might even play an indispensable role in real-world applications where the human scale is simply too slow and expensive. For instance, with the worldwide deployment of the smart electrical grid and the must for renewable energy sources, flexible devices in our household will soon (re-)negotiate complex energy contracts automatically. Another example is the rise of the Internet of Things (IoT), which will introduce countless smart, interconnected devices that autonomously negotiate the usage of sensitive data and make trade-offs between privacy concerns, price, and convenience. In such settings, the agent can help represent users in complex and constantly ongoing negotiations in an automated manner.

However, one of the key challenges in designing a successful automated negotiator is that in real-life settings, only limited information is available about the user and other parties. Users are often unwilling or unable to fully specify their preferences to a negotiation system; as a consequence, automated negotiators are required to strike deals with very limited available user information. Recently, we investigated such negotiations in two different domains: privacy negotiations and smart grid trading.



Settings

Total Points: 600

Please set your privacy preferences.

Contacts ● Share ○ Don't Share

Messages ● Share ○ Don't Share

Apps List ○ Share ● Don't Share

Photos ○ Share ● Don't Share

History ○ Share ● Don't Share

Points Offer: 28

Figure 1: What if we could negotiate our app permissions?

Together with The University of Southampton and The Massachusetts Institute of Technology, we are working on new interaction mechanisms for achieving mutually beneficial agreements, i.e., negotiation, as a more flexible interaction paradigm for meaningful consent towards data sharing and permission management [3]. The aim is to address the inadequacy of current interaction mechanisms for handling data requests and obtaining consent, such as cookie notices and permission pop-ups, which fail to align consumer choices with their privacy preferences. The hope is to provide users with a more granular and iterative permission model than current take-it-or-leave it approaches. The main catalyst for improvement is a new querying model that can elicit preference information at the right time based on information theoretical models from search theory. The first results from our lab study show that users are able and willing to share significantly more of their personal data when offered the benefits of negotiation, while maintaining the same level of satisfaction with their sharing decisions. Users adopt strategies in which they explore around their desired permission set for a more nuanced negotiation that better aligns with their privacy preferences.

As a second line of research, we explore automated negotiations within the smart electrical grid as part of the Grid-Friends project, which is coordinated by CWI in cooperation with Fraunhofer-ITWM. The Grid-Friends team is currently developing efficient algorithms that can be used for user-adaptable energy management systems within a smart grid cooperative of homeowners. We developed an optimal and tractable decision model based on adaptive utility elicitation [2] that can find the point of diminishing returns for improving the model of user preferences. Our framework provides an extensible basis for interactive negotiation agents and is scheduled to be put in practice in 2018 within a household community in Amsterdam.

Collaborative work is currently being undertaken to extend this research further. We are organising a yearly automated negotiation competition (ANAC) [L1, L2] where uncertain preferences will act as a novel challenge for the negotiation research community. Other future work will include personalised assistants (including for travel), autonomous driving, and making meaningful and dynamic consent workable at the Internet of Things scale.

This work is part of the Veni research programme with project number 639.021.751, which is financed by the Netherlands Organisation for Scientific Research (NWO). This work is supported by a grant from the ESPRC for Meaningful Consent in the Digital Economy project (EP/K039989/1). The research has received funding through the ERA-Net Smart Grids Plus project Grid-Friends, with support from the European Union's Horizon 2020 research and innovation programme.

References:

[1] T. Baarslag, et al.: "Computers That Negotiate on Our Behalf: Major Challenges for Self-sufficient, Self-directed, and Interdependent Negotiating Agents", AAMAS 2017 Workshops Visionary Papers, Lecture Notes in Computer Science. Springer International Publishing, Cham, 2017.

[2] T. Baarslag and M. Kaisers: "The value of information in automated negotiation: A decision model for eliciting user preferences", in Proc. of the 16th Conf. on Autonomous Agents and MultiAgent Systems, AAMAS'17, p. 391-400, Richland, SC, 2017. International Foundation for Autonomous Agents and Multiagent Systems. http://dl.acm.org/citation.cfm?id=3091125.3091185

[3] T. Baarslag, Alper T. Alan, Richard C. Gomer, Ilaria Liccardi, Helia Marreiros, Enrico H. Gerding, and M.C. Schraefel.et al.: "Negotiation as an interaction mechanism for deciding app permissions", in Proc. of the 2016 CHI Conference: Extended Abstracts on Human Factors in Computing Systems, CHI EA'16, p. 2012-2019, New York, NY, USA, 2016. ACM. http://doi.acm.org/10.1145/2851581.2892340

Please contact:

Tim Baarslag, CWI, The Netherlands
+31(0)20 592 4019, T.Baarslag@cwi.nl

Faster Text Similarity Using a Linear-Complexity Relaxed Word Mover's Distance

by Kubilay Atasu, Vasileios Vasileiadis, Michail Vlachos (IBM Research – Zurich)

A significant portion of today's data exists in a textual format: web pages, news articles, financial reports, documents, spreadsheets, etc. Searching across this collected text knowledge requires two essential components: a) A measure to quantify what is considered 'similar', to discover documents relevant to the users' queries, b) A method for executing in real-time the similarity measure across millions of documents.

Researchers in the Information Retrieval (IR) community have proposed various document similarity metrics, either at the word level (cosine similarity, Jaccard similarity) or at the character level (e.g., Levenshtein distance). A major shortcoming of traditional IR approaches is that they identify documents with similar words, so they fail in cases when similar content is expressed in a different wording. Strategies to mitigate these shortcoming capitalize on synonyms or concept ontologies, but maintaining those structures is a non-trivial task.

Artificial Intelligence and Deep Learning have heralded a new era in document similarity by capitalizing on vast amounts of data to resolve issues related to text synonymy and polysemy. A popular approach, called 'word embeddings', is given in [1], which maps words to a new space in which semantically similar words reside in proximity to each other. To learn the embedding (i.e., location) of the words in the new space, those techniques train a neural network using massive amounts of publicly available data, such as Wikipedia. Word embeddings have resolved many of the problems of synonymy.

In the new embedding space, each word is represented as a high-dimensional vector. To discover documents similar to a user's multi-word query, one can use a measure called the 'Word-Mover's Distance', or WMD [2], which essentially tries to find the minimum cost to transform one text to another in the embedding space. An example of this is shown in Figure 1, which can effectively map the sentence "The Queen to tour Canada" to the sentence "Royal visit to Halifax", even though (after "stopword" removal) they have no words in common. WMD has been shown to work very effectively in practice, outperforming both in precision and in recall many traditional IR similarity measures. However, WMD is costly to compute because it solves a minimum cost flow problem, which requires cubic time in the average number of words in a document. The authors in [2] have proposed a lower-bound to the WMD called Relaxed WDM, or RWMD, which in practice, retrieves documents very similar to WMD, but at a much lower cost. However, RWMD still exhibits quadratic execution time complexity and can prove costly when searching across millions of documents.

For searches involving millions of documents, the RWMD execution is inefficient because it may require repetitive computation of the distance across the same pairs of words. Pre-computing the distances across all words in the vocabulary is a possibility, but it is wasteful regarding storage space. To mitigate these shortcomings, we have proposed a linear-complexity RWMD that avoids wasteful and repetitive computations. Given a database of documents, where the documents are stored in a bag-of-words representation, the linear-complexity RWMD computes the distance between a query document and all the database documents in two phases:

- In the first phase, for each word in the vocabulary, the Euclidean distance to the closest word in the query document is computed based on the vector representations of the words. This phase involves a dense matrix-matrix multiplication followed by a column- or row-wise reduction to find the minimum distances. The result is a dense vector Z.
- In the second phase, the collection of database documents is treated as a sparse matrix, which is then multiplied with the dense vector Z. This phase produces the RWMD distances between the query document and all the database documents.

Both phases map very well onto the linear algebra primitives supported by modern GPU (Graphics Processing Unit) devices. In addition, the overall computation can be scaled out by distributing the query documents or the reference documents across several GPUs for parallel execution. Figure 2 depicts the overall approach, which enables the linear-complexity RWMD to achieve high speeds.

The result is that, when computing the similarity of one document with h words against n documents each having on average h words using a vector space of dimension m, the complexity of the brute-force RWMD is $O(nh^2m)$, whereas

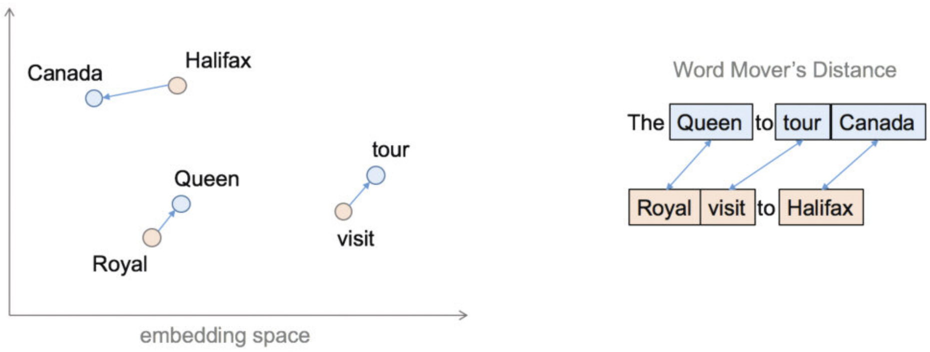
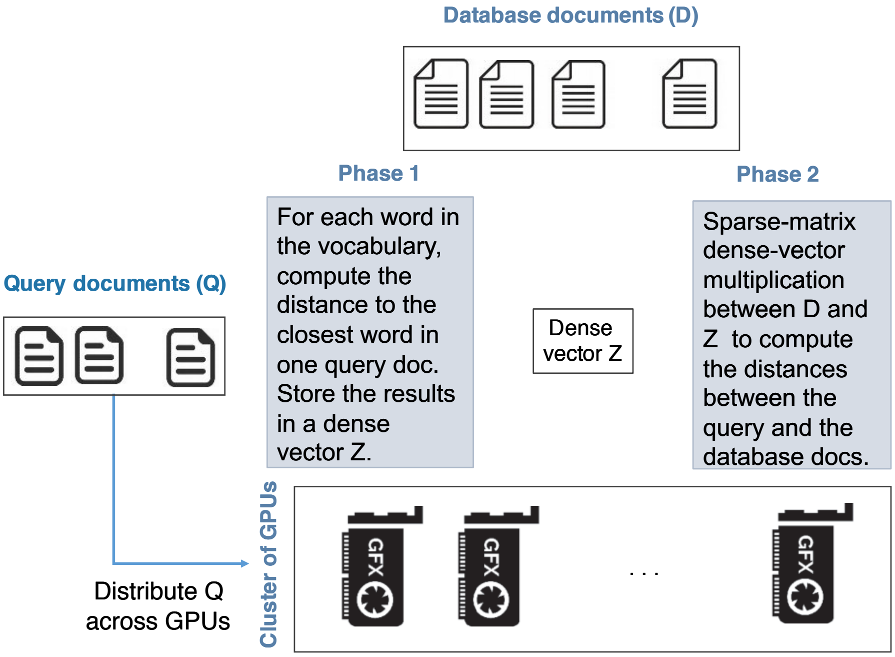


Figure 1: (Left) Mapping of word to a high-dimensional space using word embeddings. (Right) An illustration of the Word Mover's Distance.

Figure 2:
Overview of our approach.


Database documents (D)
Phase 1
Phase 2
For each word in the vocabulary, compute the distance to the closest word in one query doc. Store the results in a dense vector Z.
Dense vector Z
Sparse-matrix dense-vector multiplication between D and Z to compute the distances between the query and the database docs.
Query documents (Q)
Distribute Q across GPUs
Cluster of GPUs
GFX
GFX
. . .
GFX

under our methodology the complexity is $O(nhm)$. The interested reader can find additional technical details about the linear complexity RWMD implementation in [3].

To showcase the performance of the new methodology, we have used very large datasets of news documents. One document is posed as the query and the search retrieves the k-most-similar documents in the database. Such a scenario can be used either for performing duplicate detection (when the distance is below a threshold), or for achieving clustering of similar news events. We conducted our experiments on a cluster of 16 NVIDIA Tesla P100 GPUs on two datasets. Set 1 comprises 1 million documents, with an average number of 108 words per document. Set 2 comprises 2.8 million words, with an average number of 28 words per document. The comparison of the runtime performance between WMD, RWMD, and our solution is given in Figure 3, which shows that the proposed linear-complexity RWMD can be more than 70 times faster than the original RWMD and more than 16,000 times faster than the Word Mover's Distance.

The results suggest that we could use the high-quality matches of the RWMD to query – in sub-second time – at least 100 million documents using only a modest computational infrastructure.

References:

[1] T. Mikolov, K. Chen, G. Corrado, and J. Dean: "Efficient estimation of word representations in vector space", CoRR, abs/1301.3781, 2013.

[2] M. J. Kusner, et al.: "From word embeddings to document distances, ICML 2015: 957–966.

[3] K. Atasu, et al.: "Linear-Complexity Relaxed Word Mover's Distance with GPU Acceleration", IEEE Big Data 2017.

Please contact:
Kubilay Atasu, IBM Research – Zurich, Switzerland
kat@zurich.ibm.com

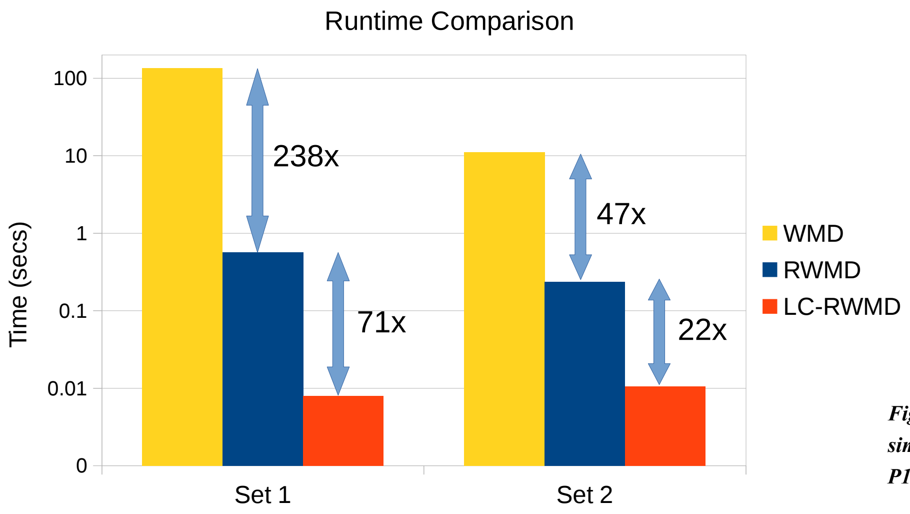


Figure 3: Time to compute the k-most-similar documents using 16 NVIDIA Tesla P100 GPUs.

The CAPTCHA Samples Website

by Alessia Amelio (University of Calabria), Darko Brodić, Sanja Petrovska (University of Belgrade), Radmila Janković (Serbian Academy of Sciences and Arts)

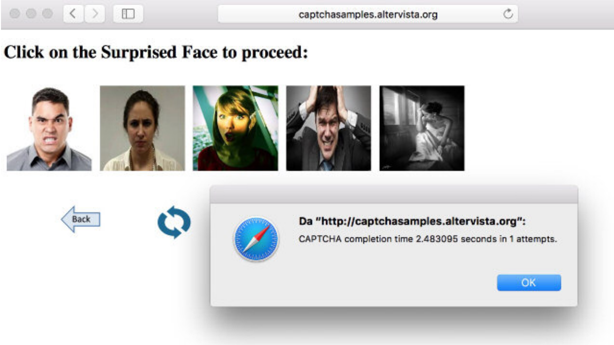
“CAPTCHA Samples” is a new website for testing different types of CAPTCHA specifically designed for research and study purposes.

In recent decades, the CAPTCHA test has received much attention owing to the increasing security problems affecting the web, for which risk prevention plays a key role. CAPTCHA is an acronym of “Completely Automated Public Turing Test to tell Computers and Humans Apart”. This is a test program which an internet user is required to solve in order to prove that he or she is human and thus gain access to a given website. In fact, the CAPTCHA test is designed to be easily solved by a human and difficult to solve for an automatic program which tries to obtain unauthorized access to the website [1]. Recently, different types of CAPTCHA have flourished in the literature, with more sophisticated security mechanisms that guarantee efficacy in risk prevention, and more user-friendly interfaces [2], [3]. In order for researchers to effectively build on the recent work in this area, an analysis of the most recently introduced CAPTCHA tests is needed.

Accordingly, we present CAPTCHA Samples, a new website collecting different CAPTCHA tests for research and analysis purposes. CAPTCHA Samples, available at [L1] (see Figure 1), was born as a joint project involving the Technical Faculty in Bor, University of Belgrade, Serbia, and DIMES University of Calabria, Italy.

Currently, the website reports different samples of image-based CAPTCHA tests, including tests based on facial expressions (animated characters, face of an old woman, surprised face, and worried face). The aim of these CAPTCHA tests is to recognise the correct image from a list of different images, according to the question asked by the test. From the homepage, it is possible to select the CAPTCHA test of interest and access to the corresponding webpage. The CAPTCHA test can be solved in order to obtain useful information about the usability of the test, including: (i) completion time, which is the solution time to the CAPTCHA, and (ii) number of tries to provide the correct solution to the CAPTCHA.

If the CAPTCHA test is not correctly solved, then the failure is notified by a text field of “wrong answer” on the screen, and the user is asked to try again. Otherwise, if the CAPTCHA test is correctly solved, a message in a text field on the screen is visualised, reporting the completion time and the number of tries to find the correct solution. Figure 2 shows an example of a successfully solved “surprised face” CAPTCHA test, which was solved in 2.48 seconds and one attempt.



captchasamples.altervista.org

Click on the Surprised Face to proceed:

Da "http://captchasamples.altervista.org":

CAPTCHA completion time 2.483095 seconds in 1 attempts.

Figure 2: Webpage of CAPTCHA Samples with a message reporting success in solving the test, including completion time and number of attempts.

Every test is completely anonymous because any personal information is registered about the internet user who accesses the CAPTCHA. Also, the main advantage of the website is that the CAPTCHA tests can be accessed from different devices, including smartphones, laptops and tablets. In this way, the difference in terms of CAPTCHA usability between multiple devices can be easily checked. In the future, we are planning to extend the CAPTCHA Samples website with new functionalities, including the selection of other CAPTCHA tests of different typology, which will be added to the website. It will be particularly useful in academic as well as industrial research for anonymously gathering data about the usability of CAPTCHA tests. It could also be the starting point for designing new CAPTCHA types which are appropriate for specific types of internet users. For more detailed information about the image-based CAPTCHA tests included in the CAPTCHA Samples website, please refer to [3].

Link:
[L1] http://captchasamples.altervista.org

References:

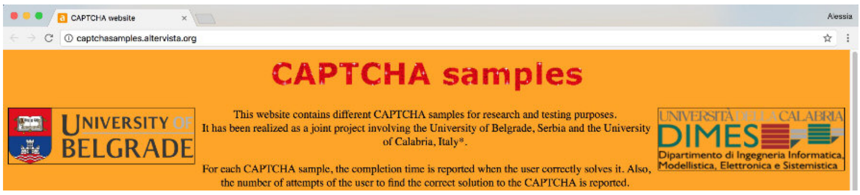
[1] A.M. Turing: “Computing Machinery and Intelligence”, Mind 59:433-460, 1950.

[2] D. Brodić, S. Petrovska, M. Jevtić, Z. N. Milivojević: “The influence of the CAPTCHA types to its solving times”, MIPRO: 1274-1277, 2016.

[3] D. Brodić, A. Amelio, R. Janković: “Exploring the Influence of CAPTCHA Types to the Users Response Time by Statistical Analysis”, Multimedia Tools and Applications, 1-37, 2017.

Please contact:

Alessia Amelio, University of Calabria, Rende, Italy
a.amelio@dimes.unical.it



captchasamples.altervista.org

CAPTCHA samples

This website contains different CAPTCHA samples for research and testing purposes. It has been realized as a joint project involving the University of Belgrade, Serbia and the University of Calabria, Italy*.

For each CAPTCHA sample, the completion time is reported when the user correctly solves it. Also, the number of attempts of the user to find the correct solution to the CAPTCHA is reported.

UNIVERSITY OF BELGRADE
UNIVERSITÀ DELLA CALABRIA
DIMES
Dipartimento di Ingegneria Informatica, Modellistica, Elettronica e Sistemistica

Figure 1: CAPTCHA Samples website.

APOPSIS: A Web-based Platform for the Analysis of Structured Dialogues

by Elisjana Ymeralli, Theodore Patkos and Yannis Roussakis (ICS-FORTH)

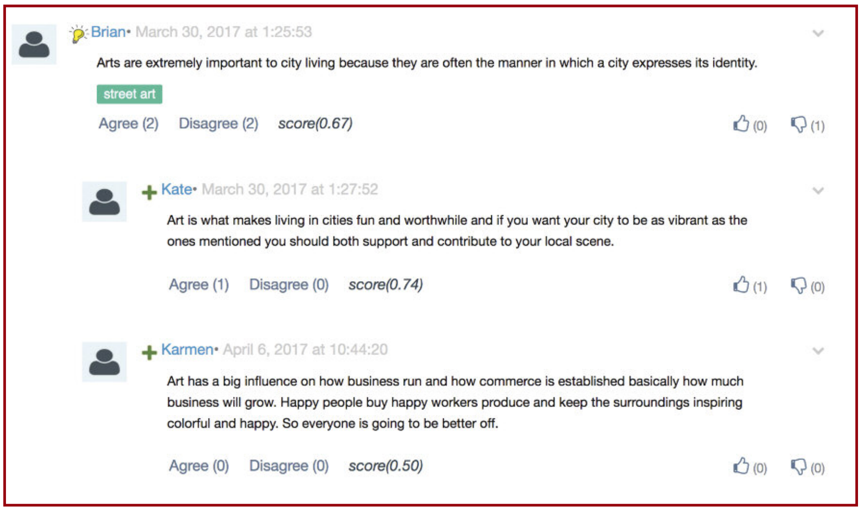
APOPSIS is a web-based platform that aims to motivate online users to participate in well-structured dialogues by raising issues and posting ideas or comments, related to goal-oriented topics of discussion. The primary goal of the system is to offer automated opinion analysis features that help identify useful patterns of relations amongst participants and their expressed opinions. Our system is designed to enable more structured and less confusing argumentative discussions, thus helping sense-makers in understanding the dynamic flow of the dialogue.

Web-based platform APOPSIS can be used in everyday deliberation, as well as decision-making discussions, where users exchange their viewpoints and argue over a plethora of topics. The platform offers well-structured dialogues which can take place in different phases of discussions. As a debating platform, APOPSIS offers the opportunity for a variety of groups to work and collaborate with each other by sharing their ideas in support of or against other opinions. Each dialogue is open for users to defend and justify their statements and vote upon them, respectively. The first phase of the dialogue allows users to participate by providing solutions or statements, in addition to their justified agreements or disagreements, while in the second phase, only the most popular or well-justified solutions remain and become subject to more detailed evaluation by the participants.

Conversations are presented in a tree-like style, where subsequent levels of comments respond to the parent comment. The system supports several features that enrich the system's usability, such as voting, semantic annotation, aspect-based rating and searching functionalities. These features enable APOPSIS to produce and extract useful conclusions that can help sense-makers and expert users to understand and make decisions on specific problems and issues.

In order to interpret and analyse user reactions, such as comments, votes and ratings, the system uses methods from the fields of computational argumentation and machine learning (ML) that enable the structuring and evaluation of the differing opinions expressed in dialogues. Specifically, an argumentation-based approach that has its roots in the IBIS-style argumentation model [1], but with slightly different semantics, is designed to structure the argumentation process [2] and organise the different conceptual components of the dialogue. In order to be able to accommodate (store and retrieve) all these complicated opinions, a formal semantic web ontology, called MACE (Multi Aspect Comment Evaluation), was designed, which can semantically represent the content produced and exchanged within the platform for online communities. Moreover, the system uses the s-mDiCE (symmetric multi-Dimensional Comment Evaluation) argumentation framework [3], for evaluating online discussions and identifying the strongest and most acceptable opinions found in online debates, based on different metrics. The underlying quantitative algorithms are generic enough to capture the features of online communities on the social web and may benefit several platforms, from debate portals to decision-making systems.

A key feature of APOPSIS is the support for automated opinion analysis for analysing user behaviour in online communities. Opinion analysis aims at identifying different groups of users and useful patterns of relationship between participants and opinions, in order to help users to make better sense of the dialogue and the opinion exchange process. Based on user reactions, the system applies ML



Brian• March 30, 2017 at 1:25:53

Arts are extremely important to city living because they are often the manner in which a city expresses its identity.

street art

Agree (2) Disagree (2) *score(0.67)* (0) (1)

Kate• March 30, 2017 at 1:27:52

Art is what makes living in cities fun and worthwhile and if you want your city to be as vibrant as the ones mentioned you should both support and contribute to your local scene.

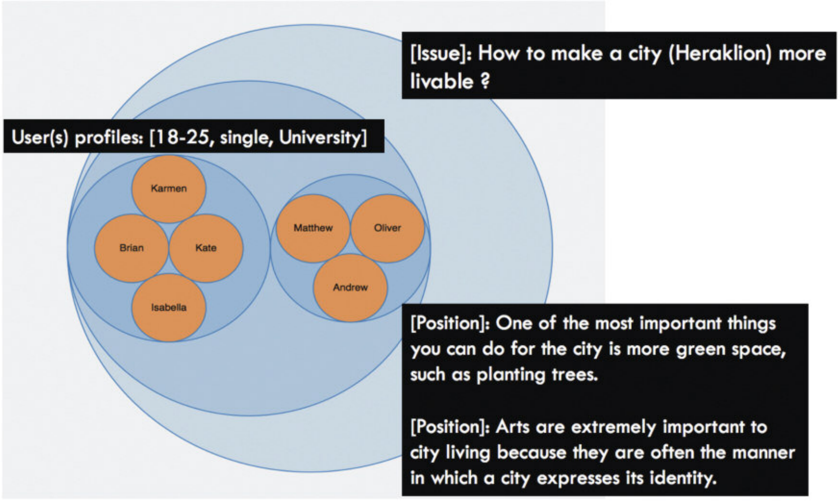
Agree (1) Disagree (0) *score(0.74)* (1) (0)

Karmen• April 6, 2017 at 10:44:20

Art has a big influence on how business run and how commerce is established basically how much business will grow. Happy people buy happy workers produce and keep the surroundings inspiring colorful and happy. So everyone is going to be better off.

Agree (0) Disagree (0) *score(0.50)* (0) (0)

Figure 1: A part of City Planning dialogue.



[Issue]: How to make a city (Heraklion) more livable ?

User(s) profiles: [18-25, single, University]

[Position]: One of the most important things you can do for the city is more green space, such as planting trees.

[Position]: Arts are extremely important to city living because they are often the manner in which a city expresses its identity.

Figure 2: An automated Opinions Analysis.

algorithms for the clustering of features and the extraction of association rules.

The basic ML algorithms used in this platform are:
- Expectation-Maximisation algorithm (EM): Decides the optimal number of clusters.
- K-means algorithm: Identifies different groups of users and opinions.
- Apriori algorithm: Determines interesting and useful relationships among attributes.

Our methodology implements five different information needs emerging from users throughout the sense-making process.
- Same profiles with similar opinions: Identifies different user profiles that share similar opinions on specific positions.
- Sharing similar opinions with specific user: Extracts different groups of users whose opinions are closely related to specific user(s).
- Same users with similar preferences: Determines groups of users who share both similar opinions and profile characteristics.
- Similar opinions based on different profiles: Identifies similar opinions expressed by users with different profile characteristics.
- Different user profiles with similar/dissimilar opinions: Finds different groups of user profiles who share similar or dissimilar opinions.

There are several avenues that are worthy of further investigation, with an emphasis on improving the system's usability. Thorough evaluations with real users and large datasets of discussions will be carried out, including expert walk-through evaluation of the platform and adjustments based on user expert feedback.

Links:
[L1] www.ics.forth.gr/isl/apopsis
[L2] http://www.ics.forth.gr/isl/mace/mace.rdfs
[L3] http://www.ics.forth.gr/isl/mace/MACE%20Ontology_Scope_Notes.pdf

References:

[1] J. Conklin, M.L. Begeman: "gIBIS: A hypertext tool for team design deliberation", Proc. of the ACM conference on Hypertext, ACM, 1987.
[2] J.Schneider, T.Groza, and A.Passant: "A review of argumentation for the social semantic web", Semantic Web 4.2 (2013)
[3] T.Patkos, G.Flouris, and A.Bikakis: "Symmetric Multi-Aspect Evaluation of Comments", ECAI 2016-22nd European Conference on Artificial Intelligence, 2016.

Please contact:

Elisjana Ymeralli, FORTH, Greece
ymeralli@ics.forth.gr (mailto:ymeralli@ics.forth.gr)

Can we Trust Machine Learning Results? Artificial Intelligence in Safety-Critical Decision Support

by Katharina Holzinger (SBA Research), Klaus Mak, (Austrian Army) Peter Kieseberg (St. Pölten University of Applied Sciences), Andreas Holzinger (Medical University Graz, Austria)

Machine learning has yielded impressive results over the last decade, but one important question that remains to be answered is: How can we explain these processes and algorithms in order to make the results applicable as proof in court?

Artificial intelligence (AI) and machine learning (ML) are making impressive impacts in a range of areas, such as speech recognition, recommender systems, and self-driving cars. Amazingly, recent deep learning algorithms, trained on extremely large data sets, have even exceeded human performance in visual tasks, particularly on playing games such as Atari Space Invaders, or mastering the game of Go [L1]. An impressive example from the medical domain is the recent work by Esteva et al. (2017) [1]: they utilised a GoogleNet Inception v3 convolutional neural network (CNN) architecture for the classification of skin lesions, pretrained their network with approximately 1.3 million images (1,000 object categories), and trained it on nearly 130,000 clinical images. The performance was tested against 21 board-certified dermatologists on biopsy-proven clinical images. The results show that deep learning can achieve a performance on par with human experts.

One problem with such deep learning models is that they are considered to be "black-boxes", lacking explicit declarative knowledge representation, hence they have difficulty in generating the required underlying explanatory structures. This is limiting the achievement of their full potential, and even if we understand the mathematical theories behind the machine model, it is still complicated to get insight into the internal workings. Black box models lack transparency and one question is becoming increasingly important: "Can we trust the results?" We argue that this question needs to be rephrased into: "Can we explain how and why a result was achieved?" (see Figure 1). A classic example is the question "Which objects are similar?" This question is the typical pretext for using classifiers to classify data objects, e.g. pictures, into different categories (e.g., people or weapons), based on utilising implicit models derived through training data. Still, an even more interesting question, both from theoretical and legal points of view, is "Why are those objects similar?" This is especially important in situations when the results of AI are not easy to verify. While verification of single items is easy enough in many classical problems solved with machine learning, e.g., detection of weapons in pictures, it can be a problem in cases where the verification cannot be

Figure 1: AI shows impressive success, still having difficulty in generating underlying explanatory structures.

done by a human with (close to) 100 percent precision, as in cancer detection, for example.

Consequently, there is growing demand for AI, which not only performs well, but is also transparent, interpretable and trustworthy. In our recent research, we have been working on methods and models to reenact the machine decision-making process [2], to reproduce and to comprehend the learning and knowledge extraction processes, because for decision support it is very important to understand the causality of learned representations. If human intelligence is complemented by machine learning, and in some cases even overruled, humans must be able to understand, and most of all to be able to interactively influence the machine decision process. This needs sense making to close the gap between human thinking and machine "thinking".

This is especially important when the algorithms are used to extract evidence from data to be used in court. A similar discussion has already been started in the area of digital forensics, with novel forensic processes being able to extract small parts of information from all over the IT-system in question and then combining them in order to generate evidence – which is currently not usable in court, simply owing to the fact that no judge will rule on evidence gathered by a process no one can control and see through.

Our approach will also address rising legal and privacy concerns, e.g., with the new European General Data Protection Regulation (GDPR and ISO/IEC 27001) entering into force on May, 25, 2018. This regulation will make black-box approaches difficult to use in business, because they are not able to explain why a decision has been made. In addition, it must be noted that the "right to be forgotten" [3] established by the European Court of Justice has been extended to become a "right of erasure"; it will no longer be sufficient to remove a person's data from search results when requested to do so, data controllers must now erase that data. This is especially problematic when data is used inside the knowledge base of a machine learning algorithm, as changes here might make decisions taken and results calculated by the algorithm irreproducible. Thus, in order to understand the impact of changes to such results, it is of vital importance to understand the internals of the intrinsic model built by these algorithms. Furthermore, and in spirit with our second research interest in this area, the deletion of data is a highly complicated process in most modern complex environments and gets even more complicated when considering the typical targets of data provisioning environments like databases that are opposing deletion:

- Fast searches: Typically, one main goal in database design is to provide fast and efficient data retrieval. Thus, the internal structures of such systems have been designed in order to speed up the search process by incorporating parts of the content as search keys, yielding a tree structure that is organised along the distribution of key information, thus making deletion a problematic issue.
- Fast data manipulation: Like in modern file systems, data entries that are "deleted" are not actually erased from the disk with overwriting the respective memory for performance reasons, but only unlinked from the search indices and marked for overwriting.
- Crash Recovery: Databases must possess mechanisms in case an operation fails (e.g., due to lack of disk space) or the database crashes in the middle of a data-altering operation (e.g., blackouts) by reverting back to a consistent state that is throughout all data tables. In order to provide this feature, transaction mechanisms must store the data already written to the database in a crash-safe manner, which can be used, for example, in forensic investigations to uncover deleted information.
- Data Replication: Companies have implemented mirror data centres that contain replicated versions of the operative database in order to be safe against failures. Deletion from such systems is thus especially complicated.

With our research, we will be able to generate mechanisms for better understanding and control of the internal models of machine learning algorithms, allowing us to apply fine-grained changes on one hand, and to better estimate the impact of changes in knowledge bases on the other hand. In addition, our research will yield methods for enforcing the right to be forgotten in complex data driven environments.

Link: [L1] https://arxiv.org/abs/1708.01104

References:

[1] A. Esteva, et al.: "Dermatologist-level classification of skin cancer with deep neural networks", Nature, 542, (7639), 115-118, 2017, doi:10.1038/nature21056.
[2] A. Holzinger, et al.: "A glass-box interactive machine learning approach for solving NP-hard problems with the human-in-the-loop", arXiv:1708.01104.
[3] B. Malle, P. Kieseberg, S. Schrittwieser, A. Holzinger: "Privacy Aware Machine Learning and the 'Right to be Forgotten'", ERCIM News 107, (3), 22-23, 2016.

Please contact:

Katharina Holzinger, SBA Research, Vienna, Austria
kholzinger@sba-research.org

Formal Methods for the Railway Sector

by Maurice ter Beek, Alessandro Fantechi, Alessio Ferrari, Stefania Gnesi (ISTI-CNR, Italy), and Riccardo Scopigno (ISMB, Italy)

Researchers from the Formal Methods and Tools group of ISTI-CNR are working on a review and assessment of the main formal modelling and verification languages and tools used in the railway domain, with the aim of evaluating the actual applicability of the most promising ones to a moving block signalling system model provided by an industrial partner. The research is being conducted in the context of the H2020 Shift2Rail project ASTRail.

Compared with other transport sectors, the railway sector is notoriously cautious about adopting technological innovations. This is commonly attributed to the sector's robust safety requirements. An example is smart route planning: while GNSS-based positioning systems have been in use for quite some time now in the avionics and automotive sectors to provide accurate positioning and smart route planning, the current train separation system is still based on fixed blocks – a block being the section of the track between two fixed points. In signalling systems, blocks start and end at signals, with their lengths designed to allow trains to operate as frequently as necessary (i.e., ranging from many kilometres for secondary tracks to a few hundred metres for a busy commuter line). The block sizes are determined based on parameters such as the line's speed limit, the train's speed, the braking characteristics of trains, sighting and reaction time of drivers, etc. However, the faster trains are allowed to run, the longer the braking distance and the longer the blocks need to be, thus decreasing the line's capacity. This is because stringent safety requirements impose the length of fixed blocks to be based on the worst-case braking distance, regardless of the actual speed of the train.

With a moving block signalling system, in contrast, a safe zone around the moving train can be computed, thus optimising the line's exploitation (Figure 1). For this solution to work, it requires the precise absolute location, speed and direction of each train, to be determined by a combination of sensors: active and passive markers along the track, as well as trainborne speedometers. One of the current challenges in the railway sector is to make moving block signalling systems as effective and precise as possible, including GNSS and leveraging on an integrated solution for signal outages (think, e.g., of tunnels) and the problem of multipaths [1]. This is one of the main topics addressed by the project ASTRail: SAtellite-based Signalling and Automation SysTems on Railways along with Formal Method and Moving Block Validation (Figure 2). A subsequent aim of the project is to study the possibility of deploying the resulting precise and reliable train localisation to improve automatic driving technologies in the railway sector.

We are currently reviewing and assessing the main formal modelling and verification languages and tools used in the railway domain in order to identify the ones that are most mature for application in the railway industry [2] [3]. This is done by combining a scientific literature review with interviews with stakeholders of the railway sector. This will shortly result in a classification and ranking, from which we will select a set of languages and tools to be adopted in all the relevant development stages of the systems addressed by ASTRail. In particular, we will formalise and validate a

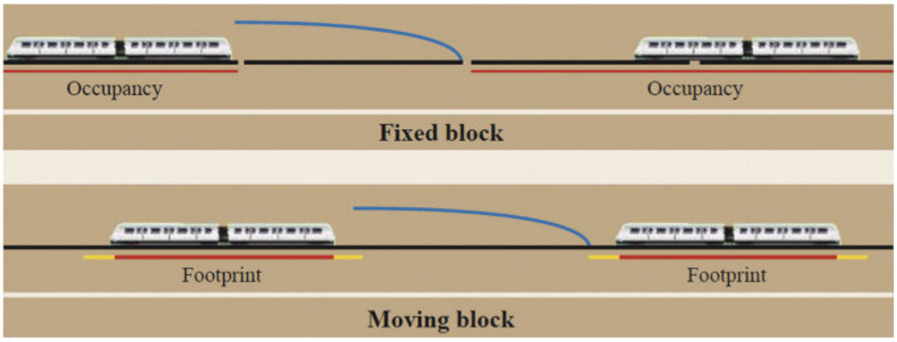


Figure 1: Safe braking distance between trains in fixed block and moving block signalling systems (Image courtesy of Israel.abad/Wikimedia Commons distributed under the CC BY-SA 3.0 license).

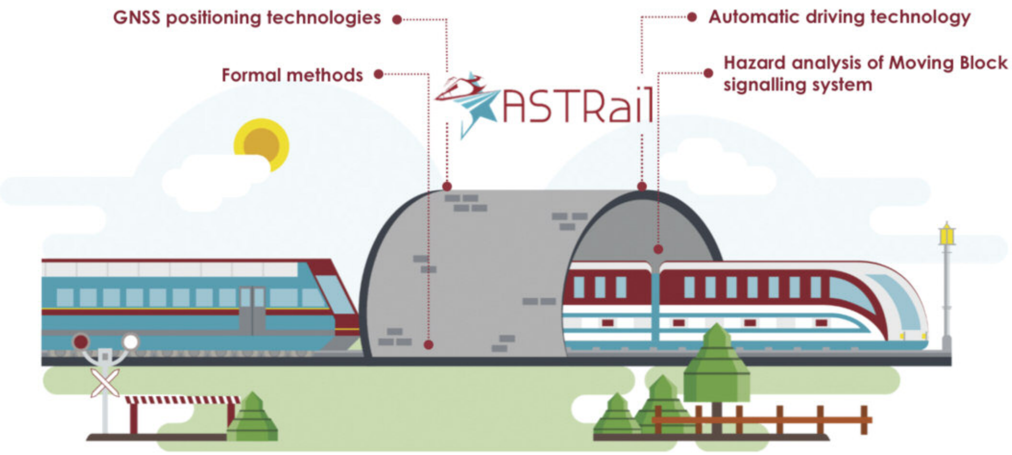

GNSS positioning technologies
Formal methods
ASTRail
Automatic driving technology
Hazard analysis of Moving Block signalling system

Figure 2: Illustrative summary of ASTRail's objectives.

moving block model developed by SIRTI, which is an industry leader in the design, production, installation and maintenance of railway signalling systems.

ASTRail will run until August 2019 and is coordinated by Riccardo Scopigno from the Istituto Superiore Mario Boella sulle Tecnologie dell'Informazione e delle Telecomunicazioni (ISMB, Italy). Other partners are SIRTI S.p.A. (Italy), Ardanuy Ingeniería S.A. (Spain), École Nationale de l'Aviation Civile (ENAC, France), Union des Industries Ferroviaires Européennes (UNIFE, Belgium) and ISTI-CNR (Italy).

Link:
ASTRail: http://www.astrail.eu/

References:

[1] F. Rispoli, et al.: "Recent Progress in Application of GNSS and Advanced Communications for Railway Signaling", in 23rd Intl. Conf. Radioelektronika, IEEE, 2013, 13-22. DOI: 10.1109/RadioElek.2013.6530882

[2] A. Fantechi, W. Fokkink, and A. Morzenti: "Some Trends in Formal Methods Applications to Railway Signaling", Chapter 4 in Formal Methods for Industrial Critical Systems: A Survey of Applications (S. Gnesi and T. Margaria, eds.). John Wiley & Sons, 2013, 61-84. DOI: 10.1002/9781118459898.ch4

[3] A. Fantechi: "Twenty-Five Years of Formal Methods and Railways: What Next?", in Software Engineering and Formal Methods, LNCS, vol. 8368. Springer, 2013, 167-183. DOI: 10.1007/978-3-319-05032-4_13

Please contact:

Stefania Gnesi, ISTI-CNR, Italy
stefania.gnesi@isti.cnr.it

The Impacts of Low-Quality Training Data on Information Extraction from Clinical Reports

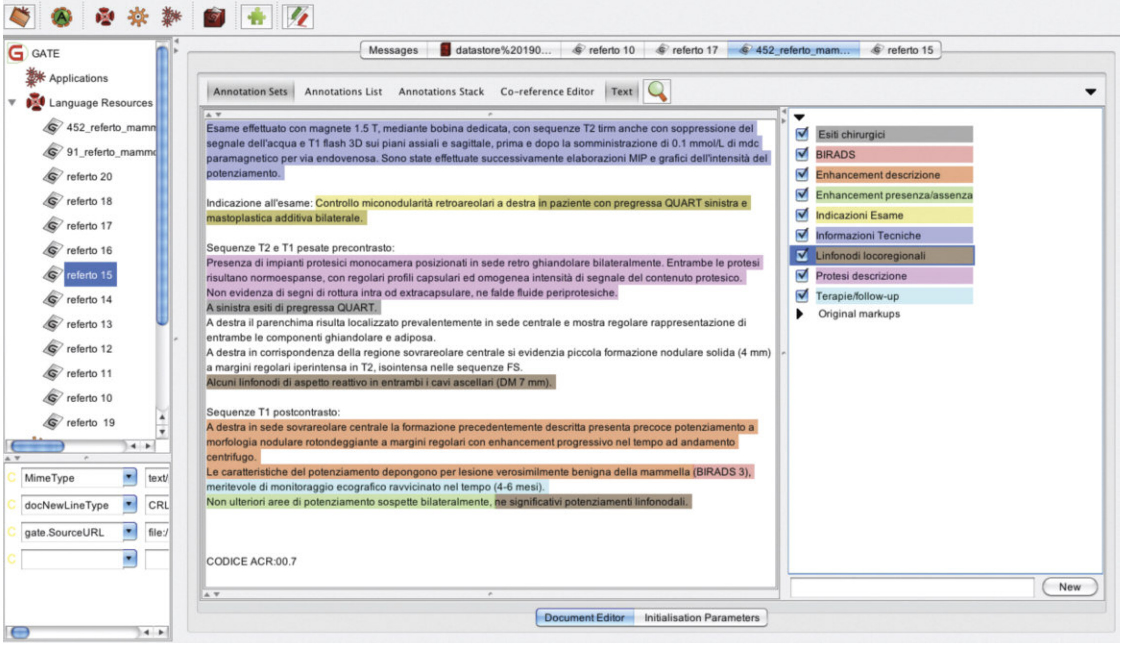
by Diego Marcheggiani (University of Amsterdam) and Fabrizio Sebastiani (CNR)

In a joint effort between the University of Amsterdam and ISTI-CNR, researchers have studied the negative impact that low-quality training data (i.e., training data annotated by non-authoritative assessors) has on information extraction (IE) accuracy.

Information Extraction (IE) is the task of designing software artifacts capable of extracting, from informal and unstructured texts, mentions of particular concepts, such as the names of people, organisations and locations – where the task usually goes by the name of "named entity extraction". Domain-specific concepts, such as drug names, or drug dosages, or complex descriptions of prognoses, are also examples.

Many IE systems are based on supervised learning, i.e., rely on training an information extractor with texts where mentions of the concepts of interest have been manually "labelled" (i.e., annotated via a markup language); in other words, the IE system learns to identify mentions of concepts by analysing what manually identified mentions of the same concepts look like.

It seems intuitive that the quality of the manually assigned labels (i.e., whether the manually identified portions of text are indeed mentions of the concept of interest, and whether their starting points and ending points have been identified precisely) has a direct impact on the accuracy of the extractor that results from the training. In other words, one would expect that learning from inaccurate manual labels will lead



Esame effettuato con magnete 1.5 T, mediante bobina dedicata, con sequenze T2 tirm anche con soppressione del segnale dell'acqua e T1 flash 3D sui piani assiali e sagittale, prima e dopo la somministrazione di 0.1 mmol/L di mdc paramagnetico per via endovenosa. Sono state effettuate successivamente elaborazioni MIP e grafici dell'intensità del potenziamento.

Indicazione all'esame: Controllo miconodularità retroareolari a destra in paziente con pregressa QUART sinistra e mastoplastica additiva bilaterale.

Sequenze T2 e T1 pesate precontrasto:
Presenza di impianti protesici monocamera posizionati in sede retro ghiandolare bilateralmente. Entrambe le protesi risultano normoespanse, con regolari profili capsulari ed omogenea intensità di segnale del contenuto protesico.
Non evidenza di segni di rottura intra od extracapsulare, ne falde fluide periprotesiche.
A sinistra esiti di pregressa QUART.
A destra il parenchima risulta localizzato prevalentemente in sede centrale e mostra regolare rappresentazione di entrambe le componenti ghiandolare e adiposa.
A destra in corrispondenza della regione sovrareolare centrale si evidenzia piccola formazione nodulare solida (4 mm) a margini regolari iperintensa in T2, isointensa nelle sequenze FS.
Alcuni linfonodi di aspetto reattivo in entrambi i cavi ascellari (DM 7 mm).

Sequenze T1 postcontrasto:
A destra in sede sovrareolare centrale la formazione precedentemente descritta presenta precoce potenziamento a morfologia nodulare rotondeggiante a margini regolari con enhancement progressivo nel tempo ad andamento centrifugo.
Le caratteristiche del potenziamento depongono per lesione verosimilmente benigna della mammella (BIRADS 3), meritevole di monitoraggio ecografico ravvicinato nel tempo (4-6 mesi).
Non ulteriori aree di potenziamento sospette bilateralmente, ne significativi potenziamenti linfonodali.

CODICE ACR:00.7

Figure 1: Screenshot displaying a radiological report annotated according to the concepts of interest.

to inaccurate automatic extraction, according to the familiar "garbage in, garbage out" principle.

However, the real extent to which inaccurately labelled training data impact on the accuracy of the resulting IE system, has seldom (if ever) been tested. Knowing how much accuracy we are going to lose by deploying low-quality labels is important, because low-quality labels are a reality in many real-world situations. Labels may be low quality, for example, when the manual labelling has been performed by "turkers" (i.e., annotators recruited via Mechanical Turk or other crowdsourcing platforms), or by junior staff or interns, or when it is old and outdated (so that the training data are no longer representative of the data that the information extractor will receive as input). What these situations share in common is that the training data were manually labelled by one or more "non-authoritative" annotators, i.e., by someone different from the ("authoritative") person who, in an ideal situation (i.e., one where there are no time / cost / availability constraints), would have annotated it.

In this work, the authors perform a systematic study of the extent to which low-quality training data negatively impacts on the accuracy of the resulting information extractors. The study is carried out by testing how accuracy deteriorates when training and test set have been annotated by two different assessors. Naturally enough, the assessor who annotates the test data is taken to be the "authoritative" annotator (since accuracy is tested according to her/his judgment), while the one who annotates the training data is taken to be the "non-authoritative" one. The study is carried out by applying widely used "sequence learning" algorithms (either Conditional Random Fields or Hidden Markov Support Vector Machines) on a doubly annotated dataset (i.e., a dataset in which each document has independently been annotated by the same two assessors) of radiological reports. Such reports, and clinical reports in general, are generated by clinicians during everyday practice, and are thus a challenging type of text, since they tend to be formulated in informal language and are usually fraught with typos, idiosyncratic abbreviations, and other types of deviations from linguistic orthodoxy. The fact that the dataset is doubly annotated allows the systematic comparison between high-quality settings (training set and test set annotated by annotator A) and low-quality settings (training set annotated by annotator NA and test set annotated by annotator A), thereby allowing precise quantification of the difference in accuracy between the two settings.

Link:
http://nmis.isti.cnr.it/sebastiani/Publications/JDIQ2017.pdf

References:

[1] A. Esuli, D. Marcheggiani, F. Sebastiani: "An Enhanced CRFs-based System for Information Extraction from Radiology Reports", Journal of Biomedical Informatics 46, 3 (2013), 425–435.

[2] W. Webber, J. Pickens: "Assessor disagreement and text classifier accuracy", in Proc. of SIGIR 2013,929–932, 2013.

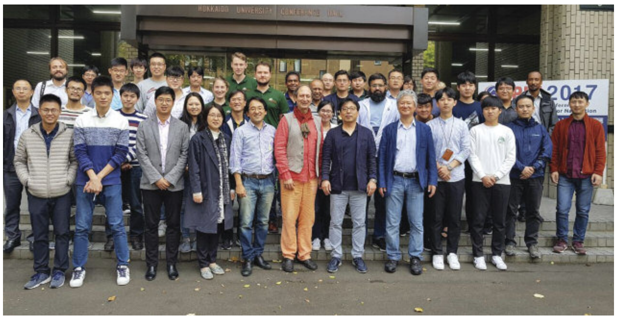
Please contact:

Fabrizio Sebastiani, ISTI-CNR, Italy
+39 050 6212892 fabrizio.sebastiani@isti.cnr.it

4th International Indoor Positioning and Indoor Navigation Competition

The fourth international Indoor Positioning and Indoor Navigation (IPIN) competition, seventh in the EvAAL series, was hosted by the international IPIN conference in Sapporo, Japan, on 17 September 2017.

The aim of the competition is to measure the performance of indoor localisation systems, that are usable in offices, hospitals or other big buildings like warehouses. The 2017 edition has attracted 28 teams and allowed participants to test their localisation solutions with rigorous procedures inside the two-floor structure of the Conference Hall of Hokkaido University.



IPIN participants.

The competition ended with the awarding of four 150.000¥ (1.100€) prizes:

- smartphone-based (Chan Gook Park, Seoul National University, Corea)
- dead reckoning (Chuanhua Lu, Kyushu University, Japan)
- offline smartphone-based (Adriano Moreira, University of Minho, Portugal)
- offline PDR warehouse picking (Yoshihiro Ito, KDDI R&D Laboratories Inc., Japan).

Prizes were awarded by the official sponsors of the competition KICS , ETRI, TOPCON, and PDR Benchmark, respectively.

Francesco Potortì, Antonino Crivello and Filippo Palumbo, researchers at the WNLab group of CNR-ISTI at Pisa, were among the main organisers.

More information on the international competition, including complete results, photos and comments at
http://evaal.aaloa.org

Joint 22nd International Workshop on Formal Methods for Industrial Critical Systems and 17th International Workshop on Automated Verification of Critical Systems

by Ana Cavalcanti (University of York), Laure Petrucci (LIPN, CNRS & Université Paris 13) and Cristina Seceleanu (Mälardalen University)

The yearly workshop of the ERCIM Working Group on Formal Methods for Industrial Critical Systems (FMICS) was organised as a joint event together with the workshop on Automated Verification of Critical Systems (AVoCS). The resulting FMICS-AVoCS 2017 workshop took place on 18-20 September in Turin, hosted by the University of Turin.

The aim of the FMICS workshop series is to provide a forum for researchers interested in the development and application of formal methods in industry. It strives to promote research and development for the improvement of formal methods and tools for industrial applications. The aim of the AVoCS workshop series is to contribute to the interaction and exchange of ideas among members of the international community on tools and techniques for the verification of critical systems.

The workshop was chaired by Laure Petrucci (LIPN, CNRS & Université Paris 13, France) and Cristina Seceleanu (Mälardalen University, Sweden). A special track on "Formal methods for mobile and autonomous robots" took place within the event, and was chaired by Ana Cavalcanti (University of York, UK). The workshop attracted 30 participants from eleven countries.

A total of thirty papers were submitted, including eight specifically for the special track. Fourteen of them were accepted (including four for the special track).

The programme also included two excellent invited keynote lectures: "Replacing store buffers by load buffers in total store ordering" by Parosh Abdulla (Uppsala University, Sweden) and "Towards formal apps: turning formal methods into verification techniques that make the difference in practice" by Kerstin Eder (University of Bristol, UK). Moreover, a half-day tutorial took place: "DIME: Model-based generation of running web applications" by Tiziana Margaria (University of Limerick & Lero, Ireland) and Philip Zweihoff (TU Dortmund, Germany).

The presentations were of extremely good quality. The programme committee awarded two best papers: "A unified formalism for monoprocessor schedulability analysis under uncertainty" by Etienne André, and "Formalising the Dezyne modelling language in mCRL2" by Rutger van Beusekom, Jan Friso Groote, Paul Hoogendijk, Rob Howe, Wieger Wesselink, Rob Wieringa and Tim Willemse. An excellent programme together with a nice weather contributed to the success of the workshops.

Best paper award winners Etienne André (left) and Tim Willemse.

We gratefully acknowledge the support of Springer for publishing the workshop's proceedings and sponsoring the best papers, EasyChair for assisting us in managing the complete process from submission to proceedings, as well as ERCIM and EASST.

The proceedings of FMICS-AVoCS 2017 have been published by Springer as volume 10471 of their LNCS series.

Selected papers are proposed for special issues of the international journals Software Tools for Technology Transfer (STTT) and Science of Computer Programming (SCP).

Links:
FMICS-AVoCS 2017:
http://www.es.mdh.se/conferences/fmics-avocs-2017/
FMICS Working Group: http://fmics.inria.fr/

Reference:

Laure Petrucci, Cristina Seceleanu and Ana Cavalcanti (eds.): "Critical Systems: Formal Methods and Automated Verification -
Joint 22nd International Workshop on Formal Methods for Industrial Critical Systems and 17th International Workshop on Automated Verification of Critical Systems (FMICS-AVoCS'17)", Turin, Italy, 18–20 September 2017, Lecture notes in Computer Science 10471, Springer, 2017.
https://doi.org/10.1007/978-3-319-67113-0

Please contact:

Ana Cavalcanti, University of York
ana.cavalcanti@york.ac.uk

Laure Petrucci, LIPN, CNRS & Université Paris 13
laure.petrucci@lipn.univ-paris13.fr

Cristina Seceleanu, Mälardalen University
cristina.seceleanu@mdh.se

10th International Conference of the ERCIM Working Group on Computational and Methodological Statistics

The 10th International Conference of the ERCIM WG on Computational and Methodological Statistics (CMStatistics 2017) took place at the Senate House and Birkbeck, University of London, UK, 16-18 December 2017. Tutorials were given on Friday 15th of December 2017 and the COST IC1408 CRoNoS Winter Course on Copula-based modelling with R took place the 13-14 December 2017. The conference took place jointly with the 11th International Conference on Computational and Financial Econometrics (CFE 2017).

This annual conference has become a leading joint international meeting at the interface of statistics, econometrics, empirical finance and computing. The conference aims at bringing together researchers and practitioners to discuss recent developments in computational methods for economics, finance, and statistics. The CFE-CMStatistics2017 programme comprised of 375 sessions, 5 plenary talks and over 1550 presentations. There were about 1700 participants. This was the biggest meeting of the conference series in terms of number of participants and presentations. The growth of the conference in terms of size and quality makes it undoubtedly one of the most important international scientific events in the field.

Link:
http://www.cmstatistics.org/

Please contact:
info@cmstatistics.org

Visual Heritage 2018

Vienna, 12-15 November 2018

With the aim of continuing the successful experience of Digital Heritage 2013 (Marseille, France) and Digital Heritage 2015 (Granada, Spain), the next edition of the Eurographics Graphics and Cultural Heritage (EG GCH) Symposium will be organized in cooperation with CHNT (Cultural Heritage and New Technologies) in Vienna. The aim of this federated event is again to bring different communities in the same venue, to share experiences and discuss methodologies concerning digital visual media and their use in the context of cultural heritage applications.

We are looking for a wide participation of our community, as well as the collaboration and inclusion of other structured communities and events, since Visual Heritage 2018 is aimed as an open circle (please contact the organizers at visualheritage2108@gmail.com if you are an organization/community interested in joining us).

The 2018 edition will be a special event, since 2018 has been declared by the European Commission the "European Year of Cultural Heritage". The event in Vienna will also take place during the Austrian term as President of the EC. Therefore, VH2018 will be an ideal context for discussing European policies on digital heritage and digital humanities.

Visual Heritage 2018 will have independent call of papers for each event contributing to the program. The EG GCH 2018 program will be based on a call for papers (full and short papers) with deadline June 20th, 2018

Paper submission

More details on the EG GCH scientific topics, instructions for submitters, call for paper dates, and the selection procedure will be published soon on EG GCH VH2018 web page http://2018.visualheritage.org

More information
http://www.chnt.at/

IFIP Networking 2018

The IFIP Networking 2018 Conference (NETWORKING 2018), to be held in Zurich, Switzerland, from 14-16 May 2018 is the 17th event of the series, sponsored by the IFIP Technical Committee on Communication Systems (TC6). Accepted papers will be published in the IFIP Digital Library and submitted to the IEEE Xplore Digital Library.

The main objective of Networking 2018 is to bring together members of the networking community, from both academia and industry, to discuss recent advances in the broad and quickly-evolving fields of computer and communication networks, to highlight key issues, identify trends, and develop a vision for future Internet technology, operation, and use.

Important Dates:

- Abstract registration: January 2, 2018 (everywhere on earth)
- Full paper submission: January 7, 2018
- Acceptance notification:March 5, 2018
- Camera-ready papers: March 23, 2018

Link:
http://networking.ifip.org/2018/

Web Science Conference 2018

Amsterdam, 27-31 May 2018

The 10th International ACM Conference on Web Science in 2018 (WebSci'18) is a unique conference where a multitude of disciplines converge in a creative and critical dialogue with the aim of understanding the Web and its impacts. The conference brings together researchers from multiple disciplines, like computer science, sociology, economics, information science, anthropology and psychology. Web Science is the emergent study of the people and technologies, applications, processes and practices that shape and are shaped by the World Wide Web.

Keynote speakers include: Tim Berners-Lee, José van Dijck and John Domingue

More information:
https://websci18.webscience.org

2018
CIDOC Conference
ICOM international committee for documentation

CIDOC Conference 2018

Heraklion, Crete, Greece, 29 September – 4 October 2018

Conference theme: Provenance of Knowledge

Participants in the event are invited to consider the theme of this conference, ‘Provenance of Knowledge’, both in its broad sense and in its technical detail. Today, museum professionals have to take into account as much the traditional research and documentation of the history of an object as the contemporary digital interpretation in the sense of the history of the transformations of a digital object. The conference invites participants to share their understanding of the shifting interpretations and uses of the notion of ‘provenance’:

- In what ways can it, or can it not, facilitate grounding in ‘knowledge’?
- What is the role of the museum as mediator of cultural heritage in facilitating and establishing such provenance and knowledge?

Conference topics:

- Documentation & interdisciplinarity
- Object documentation and analytical resources
- Provenance of materials and techniques
- Field research and object documentation
- Object documentation and archival resources
- Oral tradition and witnessing information & connection with objects
- Methods of knowledge verification and documentation of knowledge revision (“subjective” , “objective” and other forms of evidence)
- Documentation for target groups (e.g. special needs, etc)
- Object information as historical source / evidence (ethics of provenance of information)

More information:
www.cidoc2018.com

CWI
Centrum Wiskunde & Informatica

Postdoc Position in the Research Project “Approximation Algorithms, Quantum Information and Semidefinite Optimization”

Centrum Wiskunde & Informatica (CWI) has a vacancy in the Network & Optimization research group for a talented Postdoc in the research project "Approximation Algorithms, Quantum Information and Semidefinite Optimization”.

Job description

The research project “Approximation algorithms, quantum information and semidefinite optimization” aims to explore the limits of efficient computation within classical and quantum computing, using semidefinite optimization as a main unifying tool. The position involves research into the mathematical and computer science aspects of approximation algorithms for discrete optimization, quantum entanglement in communication, and complexity of fundamental problems in classical and quantum computing. The research will be supervised by Prof. Monique Laurent from the CWI Networks & Optimization research group, in collaboration with Prof. Ronald de Wolf from the CWI Algorithms & Complexity research group, and Prof. Nikhil Bansal from the department of mathematics and computer science of the Technical University Eindhoven. The position is funded through an NWO-TOP grant.

Requirements

Candidates are required to have a completed PhD in mathematics and/or computer science, and an excellent research track-record. The ideal candidate will have a strong mathematical background and knowledge in several of the following topics: algorithms, complexity, algebra, combinatorial optimization, semidefinite optimization, quantum information, communication and information theory. The candidate should also have a taste in interdisciplinary research at the frontier between mathematics and computer science. Further needed qualifications for candidates include proven research talent and good academic writing and presentation skills. Candidates are expected to have an excellent command of English.

Terms and conditions

The terms of employment are in accordance with the Dutch Collective Labour Agreement for Research Centres (“CAO-onderzoeksinstellingen”). The gross monthly salary for an employee on a full time basis, depending on relevant work experience, ranges from € 3,409 to € 4,154. Employees are also entitled to a holiday allowance of 8% of the gross annual salary and a year-end bonus of 8.33%. CWI offers attractive working conditions, including flexible scheduling. The appointment will be for a period of one year, starting as soon as possible before September 2018.

Application

Applications can be sent to apply@cwi.nl. We will take applications until getting our position filled. All applications should include a detailed CV, a motivation letter describing research interests and reasons for applying to this project, a research statement, and a short description of the PhD dissertation or of the most relevant publications. The applicant should provide names of up to three scientists who are acquainted with their previous academic performance and can write reference letters.

More information

- Position announcement: https://kwz.me/hBF
- About the Networks and Optimization at CWI: https://www.cwi.nl/research/groups/networks-and-optimization
- For CWI, please visit https://www.cwi.nl or watch our video “A Fundamental Difference” about working at CWI (https://www.cwi.nl/general/a-fundamental-difference).
- About the vacancy, please contact Prof. Monique Laurent, monique@cwi.nl.

ERCIM Membership

After having successfully grown to become one of the most recognized ICT Societies in Europe, ERCIM has opened membership to multiple member institutes per country. By joining ERCIM, your research institution or university can directly participate in ERCIM's activities and contribute to the ERCIM members' common objectives playing a leading role in Information and Communication Technology in Europe:

- Building a Europe-wide, open network of centres of excellence in ICT and Applied Mathematics;
- Excelling in research and acting as a bridge for ICT applications;
- Being internationally recognised both as a major representative organisation in its field and as a portal giving access to all relevant ICT research groups in Europe;
- Liaising with other international organisations in its field;
- Promoting cooperation in research, technology transfer, innovation and training.

About ERCIM

ERCIM – the European Research Consortium for Informatics and Mathematics – aims to foster collaborative work within the European research community and to increase cooperation with European industry. Founded in 1989, ERCIM currently includes 15 leading research establishments from 14 European countries. ERCIM is able to undertake consultancy, development and educational projects on any subject related to its field of activity.

ERCIM members are centres of excellence across Europe. ERCIM is internationally recognized as a major representative organization in its field. ERCIM provides access to all major Information Communication Technology research groups in Europe and has established an extensive program in the fields of science, strategy, human capital and outreach. ERCIM publishes ERCIM News, a quarterly high quality magazine and delivers annually the Cor Baayen Award to outstanding young researchers in computer science or applied mathematics. ERCIM also hosts the European branch of the World Wide Web Consortium (W3C).

> **"Through a long history of successful research collaborations in projects and working groups and a highly-selective mobility programme, ERCIM has managed to become the premier network of ICT research institutions in Europe. ERCIM has a consistent presence in EU funded research programmes conducting and promoting high-end research with European and global impact. It has a strong position in advising at the research policy level and contributes significantly to the shaping of EC framework programmes. ERCIM provides a unique pool of research resources within Europe fostering both the career development of young researchers and the synergies among established groups. Membership is a privilege."**
>
> ***Dimitris Plexousakis, ICS-FORTH, ERCIM AISBL Board***

Benefits of Membership

As members of ERCIM AISBL, institutions benefit from:

- International recognition as a leading centre for ICT R&D, as member of the ERCIM European-wide network of centres of excellence;
- More influence on European and national government R&D strategy in ICT. ERCIM members team up to speak with a common voice and produce strategic reports to shape the European research agenda;
- Privileged access to standardisation bodies, such as the W3C which is hosted by ERCIM, and to other bodies with which ERCIM has also established strategic cooperation. These include ETSI, the European Mathematical Society and Informatics Europe;
- Invitations to join projects of strategic importance;
- Establishing personal contacts with executives of leading European research institutes during the bi-annual ERCIM meetings;
- Invitations to join committees and boards developing ICT strategy nationally and internationally;
- Excellent networking possibilities with more than 10,000 research colleagues across Europe. ERCIM's mobility activities, such as the fellowship programme, leverage scientific cooperation and excellence;
- Professional development of staff including international recognition;
- Publicity through the ERCIM website and ERCIM News, the widely read quarterly magazine.

How to Become a Member

- Prospective members must be outstanding research institutions (including universities) within their country;
- Applicants should address a request to the ERCIM Office. The application should inlcude:
  - Name and address of the institution;
  - Short description of the institution's activities;
  - Staff (full time equivalent) relevant to ERCIM's fields of activity;
  - Number of European projects in which the institution is currently involved;
  - Name of the representative and a deputy.
- Membership applications will be reviewed by an internal board and may include an on-site visit;
- The decision on admission of new members is made by the General Assembly of the Association, in accordance with the procedure defined in the Bylaws (http://kwz.me/U7), and notified in writing by the Secretary to the applicant;
- Admission becomes effective upon payment of the appropriate membership fee in each year of membership;
- Membership is renewable as long as the criteria for excellence in research and an active participation in the ERCIM community, cooperating for excellence, are met.

Please contact the ERCIM Office: contact@ercim.eu

CWI merges with NWO Institutes Organisation

From 1 January 2018, the ERCIM member CWI has been merged with the NWO Institutes Organisation, NWO-I. The other research institutes in the Netherlands that joined the recent merger are ASTRON, NIOZ, NSCR and SRON. The Dutch institutes AMOLF, ARCNL, DIFFER and Nikhef were already part of NWO-I.

In 2015, the Netherlands Organisation for Scientific Research (NWO) started a transition to a new organizational structure. The new NWO is intended to be more flexible, more effective, and more focused on collaboration, which means it will be in a better position to respond to developments in science and society. In the new NWO structure there is a clear distinction between a granting organization, NWO, and a separate institutes organization: the Netherlands Foundation of Scientific Research Institutes, or NWO-I for short.

After the merger, CWI will continue to fulfil its mission to conduct pioneering research in mathematics and computer science, generating new knowledge in these fields and conveying it to industry and to society at large. .The general director of CWI, Jos Baeten, continues to be responsible for the CWI mission, for the day to day management of the institute, for the appointment of all CWI personnel and for the implementation of (research) policies. The foundation board of NWO-I will advise and monitor Baeten.

For more information about the merger, visit the NWO-I website:
https://www.nwo-i.nl/en/

CWI hosts EIT Digital's New Innovation Space

CWI houses a new innovation space of partner EIT Digital, which was opened on 2 November. With this new location in the financial heart of the Netherlands, EIT Digital wants to boost the development of FinTech, together with its partners in the Netherlands and Europe.

Jos Baeten (CWI Director) and Patrick Essers (Node Director EIT Digital in the Netherlands) open EIT Digital's new Innovation Space at CWI.

The new satellite location offers EIT Digital a strong base to help FinTech companies and to develop new digital FinTech initiatives. The reason for opening a second EIT Digital location in the Netherlands is a strongly felt wish of the EIT Digital's partners Bright Cape, CWI, ING Bank, and TNO who cooperate in various FinTech innovation activities within the pan-European ecosystem of EIT Digital. The Municipality of Amsterdam supports this and CWI is offering the new location.

EIT Digital is a leading European innovation and education organization. Its mission is to foster digital technology innovation and entrepreneurial talent for economic growth and quality of life in Europe. It brings together entrepreneurs from a partnership of over 130 European corporations, SMEs, start-ups, universities and research institutes.

Google Awards Grant for Fake News Detection to FORTH and University of Cyprus

As part of its Digital News Initiative (DNI), Google announced a €150 million innovation fund that supports innovation in Digital News Journalism. In its most recent round of funding, Google supported “Check-it: Visualizing fake news on social media”, a collaborative project between FORTH and University of Cyprus.

Check-it empowers users with the tools they need in order to check whether the stories they read on-line are fake or not. In this way (i) users will be able to see if what they read is fake, and (ii) they may be reluctant to forward news which are known to be fake.

The main problem that this project tries to address is that when users view news on social media they usually have little, if any, means to decide whether the information they see is real or fake. Although it is true that some social media allow users to report any fake news they see, most of the social media out there do not provide such functionality. Therefore, they place all the burden of deciding whether a story is fake or real on the end user. In this project we propose to change the way people consume digital news by empowering users with an automated ability to “check” whether a story is fake or not. Towards this end, the project extends the web browser capabilities with a “check it” button (a browser plug-in) that will enable users to check whether a story is true or fake.

For more information, please contact
Evangelos Markatos
(markatos@ics.forth.gr),
Marios Dikaiakos
(MDD@CS.ucy.ac.cy) and
G Pallis (gpallis@cs.ucy.ac.cy)

ERCIM – the European Research Consortium for Informatics and Mathematics is an organisation dedicated to the advancement of European research and development in information technology and applied mathematics. Its member institutions aim to foster collaborative work within the European research community and to increase co-operation with European industry.

ERCIM is the European Host of the World Wide Web Consortium.

Consiglio Nazionale delle Ricerche
Area della Ricerca CNR di Pisa
Via G. Moruzzi 1, 56124 Pisa, Italy
http://www.iit.cnr.it/

Centrum Wiskunde & Informatica
Science Park 123,
NL-1098 XG Amsterdam, The Netherlands
http://www.cwi.nl/

Fonds National de la Recherche
6, rue Antoine de Saint-Exupéry, B.P. 1777
L-1017 Luxembourg-Kirchberg
http://www.fnr.lu/

Foundation for Research and Technology – Hellas
Institute of Computer Science
P.O. Box 1385, GR-71110 Heraklion, Crete, Greece
http://www.ics.forth.gr/

Fraunhofer ICT Group
Anna-Louisa-Karsch-Str. 2
10178 Berlin, Germany
http://www.iuk.fraunhofer.de/

INESC
c/o INESC Porto, Campus da FEUP,
Rua Dr. Roberto Frias, nº 378,
4200-465 Porto, Portugal

Institut National de Recherche en Informatique
et en Automatique
B.P. 105, F-78153 Le Chesnay, France
http://www.inria.fr/

I.S.I. – Industrial Systems Institute
Patras Science Park building
Platani, Patras, Greece, GR-26504
http://www.isi.gr/

Norwegian University of Science and Technology
Faculty of Information Technology, Mathematics and Electrical Engineering, N 7491 Trondheim, Norway
http://www.ntnu.no/

RISE SICS
Box 1263,
SE-164 29 Kista, Sweden
http://www.sics.se/

SBA Research gGmbH
Favoritenstraße 16, 1040 Wien
http://www.sba-research.org/

Magyar Tudományos Akadémia
Számítástechnikai és Automatizálási Kutató Intézet
P.O. Box 63, H-1518 Budapest, Hungary
http://www.sztaki.hu/

University of Cyprus
P.O. Box 20537
1678 Nicosia, Cyprus
http://www.cs.ucy.ac.cy/

Universty of Warsaw
Faculty of Mathematics, Informatics and Mechanics
Banacha 2, 02-097 Warsaw, Poland
http://www.mimuw.edu.pl/

VTT Technical Research Centre of Finland Ltd
PO Box 1000
FIN-02044 VTT, Finland
http://www.vttresearch.com

Subscribe to ERCIM News and order back copies at http://ercim-news.ercim.eu/