Research agenda of Quantum Computing Group (Michał Oszmaniec, CTP PAS)

1 Motivation and the general goal

Despite the tremendous technological progress in the recent years, in the near future, scientists will be forced to work with noisy and intermediate-scale quantum devices [1]. The natural question to ask is what will be the possible applications and limitation of such near-term devices. Moreover, in spite the intense effort in the course of last 30 years, **the understanding of the relative power between classical and quantum computers remains elusive and, in my opinion, it constitutes one of the most important problems in the field of quantum information.**

The situation presented above is the **main drive and motivation** of my future research which I hope to realize with my future group in the CTP PAS in Warsaw. **I plan to explore, together with my group, the computational power and limitations of near-term intermediate-scale quantum devices, and develop improved methods of manipulation and probing of these systems**. My research plan focuses on the setting of quantum optics (with emphasis on integrated photonic circuits [2]), as well as that of "standard" quantum circuits (it is corrently being realized in systems of superconducting qubits by IBM [3], Rigetti [4], Intel or Google [5]).

2 Research objectives

I devided the proposed research into four distinct objectives that timely problem relevant for the present-day and near-term quantum computers. They correspond to various aspects of **Objectives C and D mentioned in the main mart of teh propolas**.

Objective I: Understanding the limitations and power of noisy quantum computational supremacy proposals.

Quantum Computational Supremacy (QCS) is an intermediate milestone proposed recently in the face of the extreme difficulty to construct scalable quantum computers. Its aim is to demonstrate the computational advantage of quantum mechanics even with the restricted quantum devices whose computational power is limited by their size, possibility to manipulate and address, and the destructive effect of decoherence. The proposals of QCS typically take the form of sampling problems. This means that the task of a device is to produce a sample from a probability distribution, which is believed to be a difficult task for classical computer. **The merit of this objective is primarily to understand the role of noise, decoherence and losses on various QCS proposals. On one hand, it is expected that if too much noise is present, then samples produced even by a complicated quantum system can be easily generated by classical computers. This can lead to computationally efficient benchmarking procedures for complicated, but noisy, quantum devices. On the other hand, small losses might still yield to distributions that are still classically hard. We will also investigate the unexplored territory between these two extreme cases.**

I.1 Noisy boson sampling

Boson sampling [7] is one of the leading proposals for QCS, based on linear-optical circuits, single-photon input states and particle detectors. Despite the recent theoretical [8, 9, 10] and experimental progress [11, 12], it is still not clear whether boson sampling is a promising architecture to demonstrate the advantage over classical computers. In particular, the impact of various kinds of imperfections (particle partial distinguishability, losses, efficiency of detectors and sources) in still not well-understood. A recent work [13], written by myself and Daniel Brod, we achieved a significant progress in assessing the computational hardness of boson sampling in the presence of losses. **Research tasks in this work package aim to (i) extend the results of [13] in numerous ways and (ii) solve a number of important and yet unsolved open problems in this field.** Specific tasks are the following:

1. Study the impact of losses on the QCS proposals like scattershot boson sampling [14] or boson sampling with Gaussian input states [15].

2. Understand the possibility to classically simulate ideal boson sampling via "mean field states" [13]. Attempt to prove the boson sampling anti-concentration conjecture.

3. Applythe methods of [13] in conjunction with theory of partial-distingishability [16, 17] to develop new classical simulation shemes.

4. Show or disprove the possibility to demonstrate QCS linear optical networks of logarithmic depth.

5. Study the possibility of applying weak (cross) Kerr [18] nonlinearity to perform (restricted) error correction to undermine the effect of losses in boson sampling .

I.2 Noisy random quantum circuits

Another important class of QCS proposals is realised in systems of many qubits that are transformed via random unitary operations. The most developed proposals are based on applying sequences of gates randomly chosen from so-called IQP gates [19] or from the family of universal many qubit gates [5, 20]. **Similarly, to the case of boson sampling, the role of noise and decoherence on these proposals of QCS is not well-understood (see however** [21, 22, 23]]**). We will undertake the ambitious goal of solving this timely issue**. Specific tasks are the following:

1. Assessment of the noise/decoherence robustness of IQP quantum supremacy proposals via techniques inspired by those developed in [13].

2. Assessment of the noise/decoherence robustness of QCS proposals based on random gates. This will be done building up on the results of [13] and by developing the general understanding of how noise affects random quantum circuits [24, 25].

Results obtained in point 2 are relevant for understanding of entanglement [26] and scrambling [27, 28] in many-body quantum systems undergoing random many-body dynamics, and will be applied also in these contexts.

Objective II: Developing of new methods of control and manipulation of quantum systems

Virtually any operation performed on a quantum system introduces additional noise and decoherence [29]. For this reason it is desirable to minimise a number of quantum gates required to perform a given task. Moreover, experimental limitations often constrain the possible transformations that can be performed on a given quantum system. **The merit of this objective is to introduce new methods reducing the number of elementary transformations necessary to realise a given unitary transformation to a given precision.** The specific tasks will concern the settings of linear optical networks and quantum circuits :

1. Assessment how well low-depth mode nonlocal bosonic circuits can approximate general linear-optical interferometers;

2. Development of new gate compilation [30] schemes beyon the framework of "Clifford + T" gates and gate decomposition using entangling gates and local unitaries.

The first task is motivated by the necessity of protecting linear optical networks against optical losses [31, 32]. The currently known constructions [33] allow to realize arbitrary linear optical transformation using circuits consisting of mode-local elements that have depth linear in d, i.e. number of modes. H**owever, the filed of integrated photonics recently developed [34] the possibility to implement mode-nonlocal transformations using three-dimensional linear optical chips. Thus, there is hope to reduce the losses encountered by linear optical transformations by using sequences of mode-nonlocal operations.**

The second task is a bold attempt to go beyond the standard approach for compiling of quantum gates. Typically, quantum gates are decomposed first onto the sequence of local unitary and entangling gates [40]. In the secod step single qubit unitaries are decomposed using single qubit Clifford and T gates [44] (this choice is motivated by the theory of quantum error correction). We want to propose the alternative schemes for gate decomposition.

First, we want to replace entangling transformations in the first part of the cheme by so-called Matchgate circuits. They form a low dimensional (Lie) subgroup of the full unitary group [35] (they are also relevant also in other fields of quantum computing such as classical simulability [36, 37]) and can be composed form nearest-neighbour gates available in the architectures of superconducting qubits [38]. When supplemented with additional gates (like standard local unitaries) they yield computational universality. **I expect that mathematical structure of the matchgate circuits (together with the extension of the results from** [39]**) would yield a novel and possibly advantageous method of gate compilation based on matchgates and local unitary transformatio**n (especially for near-term devices where gates are not implemented in fault-tolerant manner).

Concerning the second step (decomposition of single-qubit unitaries), we want to propose alternatives for "Clifford+T" schme. The famous Solovay-Kitaev theorem [41] says that, roughly, all universal sets of gates are equally efficient. More specifically, it guarantees that there is a constant $c \geq 1$ such that for any universal set of gates one needs no more than $A\log^c(1/\varepsilon)$ gates to approximate arbitrary unitary operation with the ε precision. Thus from a purely theoretical point of view, the Solovay-Kitaev theorem puts all universal sets as equally efficient. However, for near-term quantum computing it is particularly important to identify those universal sets for which the depth of the approximating circuit is the shortest. This corresponds to $c = 1$ and the smallest value of constant A. In the recently published papers [42, 43, 44, 45] authors show that for certain gate-sets, like Clifford+T or V-gates, one can obtain much shorter circuits than for others. Moreover, this approximation can be found efficiently in poly-log time using some probabilistic algorithm. As was recently explained by Sarnak [46, 49] similar short circuits can exist for many other sets of gates. Their construction is related to number theoretic techniques used in the seminal papers regarding optimal distributions of points on a sphere. **We will use this results to design new efficient compilation procedures for new optimal sets of gates.**

Objective III Understanding the relative power of projective and generalized measurements for quantum computers

In the abstract quantum information theory [59] it is often assumed that agents involved in processing of quantum information can perform arbitrary measurements (POVMs) allowed in quantum theory. However, in practical situations the class of allowed measurements is usually restricted by practical or fundamental reasons. For example, implementation of a generalized measurement typically requires access to the ancilla of dimension equal to the dimension of the system of interest [60] **The role of this objective is to asses the relative power for quantum information-processing between projective (von- Neumann) measurements and the general POVMs.** Specifically, the performance of these classes of measurements will be compared for the following quantum computing tasks: hidden subgroup problem [61], port-based teleportation [62], discrimination of quantum states and unitaries [63]. If the advantage of POVMs for a given task will be overwhelming, then this means that for this scenario one cannot resort to simpler von Neumann measurements. On the other hand, if the difference in performance is small, then the suboptimal strategy based on projective measurements is likely more feasible for practical implementation [60, 64].

Objective IV: Quantum psaudorandomness

For many applications in quantum information it is desirable to implement operations corresponding to performing averages with respect to the Haar measure on the full unitary group. Relaxation of this condition by requiring that the averages with respect to the physically realizable ensemble of unitaries (approximately) agree with these coming form the Haar measure only on polynomials up to a certain degree gives rise the notion of (approximate) unitary t-design [50]. In recent years there was a big progress in showing that shallow (i.e. of depth logarithmic in the dimension of the system) random quantum circuits form approximate t- designs [24, 25]. The property of being approximate t-design turns out to be important for proposals of quantum supremacy because it implies so-called anticoncentration [51]). **In this objective we aim to check how the aforementioned results are modified by the errors present in quantum circuits. Moreover, we plan to extend the results concerning random circuits to the realm of bosonic linear optics**. Here are the exemplary research tasks:

1. Assess how the property of approximate t-design is affected, if to a sequence of random universal gates we append some noise (on the level of every gate). Will the random circuits still anti-concentrate?

2. Investigate whether shallow optical circuits consisting of (i) nearest-neighbour and (ii) mode nonlocal operations allow to attain approximate t-designs.

3. Study the convergence of the random circuits generated by cross-Kerr gate and passive linear optics to approximate t-designs in the bosonic Hilbert space [52]

The motivation for the second task again steams form quantum tomography [53]. One can also conjecture that ensembles of gate-sets forming approximate t-designs (for sufficiently large t) can lead to sampling problems that are computationally hard (in analogy to the standard proposal of boson sampling).

Concerning the third task, in [52] the cross-Kerr interaction was used to generate, in conjunction with passive linear optics, random sequences of gates that that are approximate t-designs on a bosonic Hilbert space. We plan to examine the convergence to approximate t-design as a function of the strength of the cross-Kerr interaction. More precisely, we expect [54] that the time of convergence will depend of the norm $\|[U_K \otimes U_K, \mathbb{L}_b]\|$, where U_K is a gate generated by the cross-Kerr interaction. The problem of convergence of such random evolutions is potentially relevant for probing the correlations of many-body systems that are driven by some complicated evolutions, which can be interrupted by quenches of "simple" evolutions [55].

4 Feasibility, research team and organisation of work

Expertise of the Project leader—**The proposed project concerns the present research interest of Michał Oszmaniec. He has the experience in both research both topics related to the objectives of the project.** Considering the Objective I, he is the main author of the paper [13] concerning the lossy boson sampling that is directly related to tasks I.1-I.4 a are in fact offspring of this work and an attempt to make an important contribution to the field of quantum computational supremacy. On the other hand, Objective II focuses on the problems of control of quantum systems, which can be addressed via group-theoretic methods. These techniques were used in a recent publication co-authored by the applicant [39]. Objective III is also in the competence of dr Oszmaniec (in fact he is the main author of two publications [64, 60] on related subject). Finally, objective IV is a continiuation of the Homing project realized by the aplicant.

The complementary expertise important for the realisation of the problem will be provided by partners engaged in the project: Michał Horodecki (Gdańsk) - Objectives II and IV , Daniel Brod (Niteroi, Brazil) - objective I and II, and Zoltan Zimboras (Wigner Institute, Hungary) - objective II.

Research team and division of work— The quantum computing group will consist of six people: project leader, a postdoc, suporting stientist, and two PhD students, and one master student. It is expected that all members of the group will be dedicated to realisation of the ambitious goals of the project. Project leader and supporting scientist will be also supervising the students and a postdoc in the course of the project. Two master students will be hired, each for the period of approximately 24 months. He or she will be working on numerical aspects of either of the research objectives I,II or III (deepening on the needs). If Master student exhibit analytical skills, he will be enrolled in a currently active project requiring his competence (the interaction with other members of the tram will be encouraged). PhD students will be both employed for periods of 48 months. Each of them will be working on a different objective of the project (Possibly I or II). It is expected that the research of PhD students will be have both analytical and numerical flavour. Finally, a postdoc will be hired for a period of two years (with a possible extension to the third year). The responsibility of a postdoc will be to work intently on at least two of the objectives of the project. Finally, the supporting scientist will be working on tasks related to objective II and will be supervising students on the daily basis.

Organisation of work— The work in the project will be organised around weekly group meetings where the team members will be presenting intermediate progress and reporting on the recent scientific achievements in subjects relevant for the topic of the project (Journal club). Moreover, project leader will be discussing the ongoing issues with the team on the daily basis. Every week there will a few Skype conferences with the partners. These meetings will be attended by the members of the group engaged in the relevant research tasks. Bilateral visits to partners will also play an important role in the project.

References

[1] J. Preskill, "Quantum Computing in the NISQ era and beyond", Quantum 2, 79 (2018)

[2] J. Carolan, et al., Science 349, 711 (2015)

[3] IBM Q initiative `https://www.research.ibm.com/ibm-q/`

[4] `https://rigetti.com/`

[5] S. Boixo, et al., Nature Physics 14, 595-600 (2018)

[6] J. Preskill, "Quantum computing and the entanglement frontier", arXiv preprint `arXiv:1203.5813` (2012)

[7] S. Aaronson and A. Arkhipov, in Proceedings of the forty-third annual ACM symposium on Theory of computing pp. 333–342 (ACM, 2011)

[8] S. R. Keshari, T. C. Ralph, and C. M. Caves. Phys. Rev. X 6, 021039 (2017)

[9] A. Neville, C. Sparrow, R. Cliord, E. Johnston, P. M. Birchall, A. Montanaro, and A. Laing, Nature Physics 13, 1153 (2017).

[10] P. Cliford and R. Cliford, "The classical complexity of boson sampling" in Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms (2018) pp. 146-155 (2017)

[11] J. C. Loredo et al., Phys. Rev. Lett. 118, 130503 (2017)

[12] Y. He et al. Phys. Rev. Lett. 118, 190501 (2017)

[13] M. Oszmaniec, D. J. Brod, New. J. Phys. 20, 092002 (2018)

[14] A. P. Lund, A. Laing, S. Rahimi-Keshari, T. Rudolph, J. L. O'Brien, and T. C. Ralph, Phys. Rev. Lett. 113, 100502 (2014)

[15] C. S. Hamilton, R. Kruse, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex, Phys. Rev. Lett., 119, 170501 (2017)

[16] J. J. Renema, A. Menssen, W. R. Clements, G. Triginer, W. S. Kolthammer, and I. A. Walmsley, Phys. Rev. Lett. 120, 220502 (2018)

[17] A. E. Moylett, Peter S. Turner, Phys. Rev. A 97, 062329 (2018)

[18] S. Zhou, M. Zhang, J. Preskill, L. Jiang. Nat. Comm. vol. 9, 78 (2018)

[19] M. J. Bremner, A. Montanaro, and D. J. Shepherd Phys. Rev. Lett. 117, 080501 (2016)

[20] R.L. Mann, M. J. Bremner, "On the Complexity of Random Quantum Computations and the Jones Polynomial", `arXiv:1801.06166` (2017)

[21] M. Bremner, A. Montanaro, D.J. Shepherd, Quantum 1, 8 (2017)

[22] X. Gao, L. Duan, "Efficient classical simulation of noisy quantum computation" , `arxiv:1810.03176` (2018)

[23] Man-Hong Yung, Xun Ga, "Can Chaotic Quantum Circuits Maintain Quantum Supremacy under Noise?", `arXiv:1706.08913` (2017)

[24] F. Brandao, Aram W. Harrow, M. Horodecki, Commun. Math. Phys., 346, 2, 397-434 (2016)

[25] F. Brandao, Aram W. Harrow, M. Horodecki, Phys. Rev. Lett. 116, 170502 (2016)

[26] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. 81, 865–942 (2009)

[27] D.Ding, P. Hayden, M. Walter, JHEP 12, 145 (2016)

[28] P. Hosur, X.-L. Qi, D. A. Roberts and B. Yoshida, Chaos in quantum channels, Journal of High Energy Physics, 1–49 (2016)

[29] M. Grace et al., J. Phys. B: At. Mol. Opt. Phys. 40, 103-125 (2007)

[30] F.T. Chong, D. Franklin and M. Martonosi, Nature 549, pages 180–187 (2017)

[31] J. Carolan, C. Harrold, C. Sparrow, E. Martín-López, N. J. Russell, J. W. Silverstone, P. J. Shadbolt, N. Matsuda, M. Oguma, M. Itoh, et al., Science 349, 711 (2015)

[32] F. Flamini, N. Spagnolo, N. Viggianiello, A. Crespi, R. Osellame and F. Sciarrino, Sci. Rep. vol. 7, 15133 (2017)

[33] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. 73, 58 (1994)

[34] A. Crespi, et. al, Nat. Comm. 7, 10469 (2016)

[35] R. Jozsa, A. Miyake, Proc. R. Soc. A 464, 3089-3106 (2008)

[36] L. G. Valiant, Quantum circuits that can be simulated classically in polynomial time.,SIAM Journal of Computing, 31(4): 1229-1254 (2002).

[37] Daniel J. Brod, Phys. Rev. A 93, 062332 (2016)

[38] G. Wendin, Rep. Prog. Phys. 80, 106001 (2017)

[39] M. Oszmaniec and Z. Zimborás, Phys. Rev. Lett. 119, 220502 (2017)

[40] Vivek V. Shende, Stephen S. Bullock, Igor L. Markov, IEEE Trans. on Computer-Aided Design, vol. 25, no. 6, pp.1000 - 1010 (2006)

[41] C. M. Dawson and M. A. Nielsen, The Solovay-Kitaev algorithm, Quant. Inf. Comp. 6, 81, 2006.

[42] A. Bocharov, Y. Gurevich, K. M. Svore. Efficient Decomposition of Single-Qubit Gates into V Basis Circuits. Phys. Rev. A, 88:012313, 2013

[43] V. Kliuchnikov, D. Maslov D, M. Mosca, Practical approximation of single-qubit unitaries by single-qubit quantum Clifford and T circuits, IEEE Transactions on Computers, vol.65, no. 1, p. 161-172, Jan. 2016

[44] V. Kliuchnikov, D. Maslov, and M. Mosca Asymptotically optimal approximation of single qubit unitaries by Clifford and T circuits using a constant number of ancillary qubits, Phys. Rev. Lett., 110, p. 190502, 2013.

[45] N. J. Ross, P. Selinger, Optimal ancilla-free Clifford+T approximation of z-rotations, Quantum Information and Computation 16 (11-12), 901-953, 2016

[46] P. Sarnak, Letter to Aaronson and Pollington on the Solvay-Kitaev Theorem and Golden Gates, http://publications.ias.edu/sarnak/paper/263, 2015

[47] A. Lubotzky, R. Phillips, P. Sarnak, Hecke operators and distributing points on the sphere I, Commun. Pur. Appl. Math. 39(40), S1, S149-S186, 1986

[48] A. Lubotzky, R. Phillips, P. Sarnak, Hecke operators and distributing points on the sphere I, Commun. Pur. Appl. Math. 60, 401-420, 1987

[49] O. Parzanchevski, P. Sarnak, Super-Golden-Gates for PU(2), Advances in Mathematics, Special volume honoring David Kazhdan, 327:869-901, 2018

[50] Richard A. Low, “Pseudo-randomness and Learning in Quantum Computation”, Ph.D. thesis, University of Bristol, `arXiv:1006.5227[quant-ph]` (2010)

[51] Juan Bermejo-Vega, Martin Schwarz, Jens Eisert, Dominik Hangleiter, Quantum 2, 65 (2018)

[52] M. Oszmaniec, R. Augusiak, C. Gogolin, J. Kołodyński, A. Acín, and M. Lewenstein Phys. Rev. X 6, 041044 (2016)

[53] Leonardo Banchi, W. Steven Kolthammer, M.S. Kim, ”Multiphoton Tomography with Linear Optics and Photon Counting”, `arXiv:1806.02436` (2018)

[54] L. Banchi, D. Burgarth, M. J. Kastoryano, Phys. Rev. X 7, 041015 (2017)

[55] A. Elben, B. Vermersch, M. Dalmonte, J. I. Cirac, P. Zoller, Phys. Rev. Lett. 120, 050406 (2018)

[56] F. de Melo, P. Ćwikliński, and B. M. Terhal, New J. Phys. 15 013015 (2013)

[57] M. Oszmaniec, J. Gutt, and M. Kuś, Phys. Rev. A 90, 020302(R)

[58] R. Raussendorf, Phys. Rev. A 88, 022322 (2009)

[59] M. A. Nielsen and I. L. Chuang, Quantum computation and quantum information (Cambridge University Press, 2010)

[60] M. Oszmaniec, L. Guerini, P. Wittek, and A. Acín, Phys. Rev. Lett. 119, 190501 (2017)

[61] Samuel J. Lomonaco, Jr., Louis H. Kauffman, “Quantum Hidden Subgroup Problems: A Mathematical Perspective”,`arXiv:0201095` (2002)

[62] S. Ishizaka, T. Hiroshima, Phys. Rev. Lett. 101, 240501 (2008)

[63] J. Bae and L.-C. Kwek, "Quantum state discrimination and its applications," Journal of Physics A: Mathematical and General, vol. 48, no. 8, p. 083001, (2015)

[64] M. Oszmaniec, F. B. Maciejewski, Z. Puchała, "All quantum measurements can be simulated using projective measurements and postselection" arXiv:1807.08449

[65] GilKalai, "The Quantum Computer Puzzle" arxiv:1605.00992 (2016)

[66] B. C. Hall, *Lie groups, Lie algebras, and representations: an elementary introduction*, Springer, 2003

[67] S. Lloyd, M. Mohseni, and P. Rebentrost, Nature Physics, 10(9):631–633 (2014)

[68] S. Kimmel, C. Yen-Yu Lin, G. Hao Low, M. Ozols, and T. J. Yoder, npj Quantum Information 3:13 (2017)

[69] Sergey Bravyi and Alexei Kitaev Phys. Rev. A 71, 022316 (2005)

[70] C. M. Dawson and M. A. Nielsen, Quant. Inf. Comp 6, 81–95 (2006)

[71] Christian Weedbrook, et al., Rev. Mod. Phys. 84, 621 (2012)

[72] I Pitsios, L Banchi, AS Rab, M Bentivegna, D Caprara, A Crespi, Nat. Communications 8 (1), 1569 (2017)

[73] E. Knill, R. Laflamme, G. Milburn, Nature, 409 (6816): 46–52 (2001)

[74] Quantum Benchmark Inc., quantumbenchmark.com/

[75] F. Flamini, N. Spagnolo, F. Sciarrino, Photonic quantum information processing: a review, arXiv:1803.02790 (2018)