Research Statement | Daniel Nagaj

What does nature allow us to compute? Why are some computational problems inherently harder than others? Can we lower bound the number of steps necessary for getting a result as the problem size grows? Can we find efficient algorithms for particular problems? Would their efficiency depend crucially on the model of computation that we use? These questions become even more interesting if we take quantum mechanics into account, in contrast to using only computers based on classical E&M. We want to know what we could (or couldn't) do with the computers we don't even have yet.

Quantum computing has produced new algorithms for interesting computational problems which have been experimentally tested on small problem instances. It broadened our view of computational complexity, even producing proofs of classical results through a quantum detour. In many cases, it promises efficient quantum simulation of quantum many-body systems. Moreover, using a quantum information viewpoint, understanding the systems' structure and symmetries allowed us to channel our resources more efficiently and get better approximation algorithms (for the energies or eigenstates of physical systems). I am fascinated by algorithms built on insights from quantum physics – e.g. annealing and sampling, or scattering in quantum walks. However, even for all the beauty of the theory, it is important not to forget to think about quantum computers as actual physical devices. Even though we might not see fault-tolerant, universal, scalable quantum computers in the nearest future (hopefully only because of technical, not fundamental issues), it makes sense to think about restricted, specific-purpose models. I am motivated by the possibilities of quantum simulation, in the light of recent results connecting quantum information to quantum chemistry or quantum field theory. Moreover, we could discover that some of these are classically simulable. The global properties of these systems derive from their local interactions.

Local Hamiltonians – frustrated and frustration-free

Since my thesis, *Local Hamiltonians in Quantum Computation*, I look at the properties of quantum many-body systems with local interactions. First, finding their ground states, and the ground state properties (e.g. energy) can be surprisingly difficult, even in systems with simple interactions. Second, we can use them to connect condensed matter physics to complexity. Third, such systems can be used to build quantum computers – even without precise time-control.

The first topic is based on a link between computational complexity and physics. If we could easily describe the ground states of local Hamiltonians with particular form, we would also have the power to solve tough computational and optimization problems. Together with Shay Mozes, I have looked at the variants of the Local Hamiltonian problem, showing QMA completeness of 3-local Hamiltonian with all terms having norm 1, without perturbation gadgets [3]. With Sean Hallgren and Sandeep Narayanaswami, I have shown that 2-local Hamiltonian on a line with 8-dimensional qudits is also QMA-complete [20]. My future goal in this area is to prepare a toolkit for translation between problems, usable in a future Quantum PCP theorem. I aim for proving hardness of problems that have restricted locality, geometry, local dimension, form of terms and large eigenvalue and promise gaps. Finally, together with David Gosset, we are now writing up our 2D clock construction that allowed us to finally prove that Quantum 3-SAT is QMA_1 complete.

The second line of my research of Local Hamiltonians focuses on the physical properties of such systems. Classical statistical physics of satisfiability problems has produced a wealth of new techniques. Naturally, I got interested in investigating random instances of Quantum SAT. With Antonello Scardicchio, we have looked at the Adversary SAT problem as an upper bound for a SAT/UNSAT transition in random Quanutm SAT. We presently work on incorporating Shearer's bounds into the picture. With Ramis Movassagh and others we have looked at unfrustrated spin chains [9] and found interesting ground state properties already for four-dimensional qudits. Finally, with Sergey Bravyi and others, we have discovered an unfrustrated qutrit chain [19] with a logarithmic scaling of entanglement entropy in the ground state with a polynomially large MPS description. I now want to find a family of problems related to this model, and show that they are decidable by a pushdown automaton or another restricted model of computation. I want to better understand unfrustration, area laws and quantum correlations in qudit spin chains.

Third, I am fascinated by the possibility of running quantum computation without precise time-control, using only interactions given in the system. We know this is possible in general, but I search for constructions with restricted form, translationally invariant interactions and efficient runtimes. One such model is the Hamiltonian Quantum Cellular Automaton in 1D we have discovered with Pawel Wocjan [10]. Recently, I started a collaboration with Andrew Childs' group, making their universal multi-particle quantum walk in 2D more efficient. I have also worked on universal computation based on railroad-switches, with constant-norm, 2-local interactions [8, 17], whose requirements and runtimes of this model are significantly better those coming from the usual 2-local Hamiltonian problem. We can keep the evolution with-

in a preferred subspace even without the need for large-norm terms – and I want to further develop this approach to encoding computational problems in physical systems.

Computational Complexity – QMA and MQA

The local Hamiltonian problem is complete for QMA – the class of problems easily and soundly verifiable on a quantum computer. Because of the inherent randomness of quantum computation, such probabilistic verification protocols require some margin for error. However, repeating a verification procedure can boost our confidence, as shown by Marriott and Watrous. With Pawel Wocjan and Yong Zhang, we have found a faster, purely quantum version of the QMA amplification scheme [7]. The techniques used there were also useful for a single-copy tomography procedure [12] that together with Eddie Farhi and others helped us break a possible quantum money scheme.

Derandomizing computation is a daunting task, connected to a deep question in complexity theory. Could we make the success probability of the QMA verification procedure be 1 exactly (in accepting cases)? Zachos and Fürer tell us this is possible in the classical world (MA_1=MA). Together with my collaborators, we looked at MQA (QCMA), a subclass of QMA with a classical witness and a quantum verification procedure. We have given a proof that MQA_1 with perfect completeness has the same power as MQA [14], even though an oracle separation exists. Currently, I continue thinking about interactive protocols with one-sided error, i.e. where we can completely convince a verifier in the acceptable cases, while the verifying procedure remains sound.

Quantum Algorithms – walking, sampling and annealing

Quantum computation allows us to use unitary evolution (or transformations) of wavefunctions that can be complicated superpositions of basis states. Quantum walks (see e.g. my review [15]) are a typical example of using superpositions for examining large parts of a search space. The hard part is to pick up the interesting part of the superposition. Sometimes, it helps to look at long-term behavior of quantum walks. With Mária Kieferová, we have looked at mixing (in a time-averaged sense) on necklace graphs [16]. With Pawel Wocjan and collaborators I have looked at efficient implementations of particular quantum walks [6], and used them extensively in a sampling algorithm for approximating partition functions [11]. We now work on developing these ideas in a quantum algorithm for approximating the permanent of a matrix. The basic tool I focus on is efficient preparation of "coherent encodings" of thermal states, for the purpose of sampling, which we have utilized with Man-Hong Yung and others [13].

Adiabatic quantum optimization is a state preparation procedure based on slowly changing Hamiltonians, with jumps between eigenstates suppressed according to the energy gaps in the spectrum. This method is universal for quantum computation, but only its restricted forms (stoquastic Hamiltoninas) are available for practical implementation at the moment. I am investigating the computational power of stoquastic adiabatic or quantum annealing evolutions, and together with Rolando Somma and Mária Kieferová, we have shown [18] an exponential speedup over classical approaches for the randomly-glued trees oracle problem, matching a quantum walk result of Childs et al. Furthermore, with Eddie Farhi and others, we have shown how not to approach adiabatic optimization [4], as structured Hamiltonians are necessary if we want to hope for a quantum speedup better than for unstructured search.

Classical numerics – tensor product states

Finally, the insights from quantum information motivate classical algorithms. Focusing on an ansatz with low entanglement has produced several efficient methods for investigating many-body states. One of them, tensor product states, are especially suitable for systems with a tree-like structure. Motivated by the search for phase transitions in quantum versions of satisfiability, together with Igor Sylvester and others I have looked at various condensed-matter physics models on the Bethe lattice (Cayley-tree) [5] and characterized their phase transition points. These days, in collaboration with Valentin Murg and Frank Verstraete, I focus on using tensor product state networks in quantum chemistry applications and simulation of strongly correlated systems. I use tools learned from the DMRG community (in collaboration with Andrej Gendiar), as well as develop adaptive methods for the underlying geometry choices.

Conclusion

I am deeply convinced about the necessity for a clear communication of my research results. I greatly enjoy preparing and giving talks for varied audiences – whether expert or popular. Communication and collaboration is a basic ingredient of my research – throughout my career I have been blessed with short term encounters at conferences, as well as long-term

projects that have brought our ideas together and sparked a new research direction. After spending several years back in Europe (in Bratislava and Vienna), I now welcome a change of scenery and new inputs, bringing my experience in Hamiltonian complexity, adiabatic computation and quantum walks. I come from a theoretical physics background, but throughout my research career I have been fascinated by the interchange of ideas on the boundary between quantum information, condensed-matter physics and theoretical computer science. With further motivation coming from quantum chemistry, I seek development of quantum algorithms in simulation, classical numerics for quantum many-body systems, and deeper understanding of computational complexity of physical problems.

References

1. **Daniel Nagaj**, Peter Štelmachovič, M. S. Kim, Vladimír Bužek, *Quantum homogenization for continuous variables: Realization with linear optical elements,* Phys. Rev. A 66, 062307 (2002)
2. **Daniel Nagaj**, Iordanis Kerenidis, *On the Optimality of Quantum Encryption Schemes,* J. Math. Phys. 47, 092102 (2006)
3. **Daniel Nagaj**, Shay Mozes, *A new construction for a QMA complete 3-local Hamiltonian,* J. Math. Phys. 48, 072104 (2007)
4. Edward Farhi, Jeffrey Goldstone, Sam Gutmann, **Daniel Nagaj,** *How to make the quantum adiabatic algorithm fail* International Journal of Quantum Information, Vol. 6, No. 3, 503-516 (2008)
5. **Daniel Nagaj**, Edward Farhi, Jeffrey Goldstone, Peter Shor, Igor Sylvester, *The Quantum Transverse Field Ising Model on an Infinite Tree from Matrix Product States,* Phys. Rev. B 77, 214431 (2008)
6. Chen-Fu Chiang, **Daniel Nagaj**, Pawel Wocjan, *Efficient Circuits for Quantum Walks,* QIC Vol.10, No.5&6, 0420-0434 (2010)
7. **Daniel Nagaj**, Pawel Wocjan, Yong Zhang, *Fast Amplification of QMA,* QIC Vol.9, No.11&12, 1053-1068 (2009)
8. **Daniel Nagaj,** *Fast Universal Quantum Computation with Railroad Switch Hamiltonians,* J. Math. Phys., 51 (6), 062201 (2010)
9. Ramis Movassagh, Edward Farhi, Jeffrey Goldstone, **Daniel Nagaj**, Tobias J. Osborne, Peter W. Shor, *Unfrustrated Qudit Chains and their Ground States,* Phys. Rev. A 82, 012318 (2010)
10. **Daniel Nagaj**, Pawel Wocjan, *Hamiltonian Quantum Cellular Automata in 1D,* Phys. Rev. A 78, 032311 (2008)
11. Pawel Wocjan, Chen-Fu Chiang, **Daniel Nagaj**, Anura Abeyesinghe, *Quantum Speed-up for Approximating Partition Functions,* Phys. Rev. A 80, 022340 (2009)
12. Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, **Daniel Nagaj**, Peter W. Shor, *Quantum state restoration and single-copy tomography,* Phys. Rev. Lett. 105, 190503 (2010)
13. Man-Hong Yung, **Daniel Nagaj**, James D. Whitfield, Alán Aspuru-Guzik, *Simulation of Classical Thermal States on a Quantum Computer: A Transfer Matrix Approach,* Phys. Rev. A 82, 060302 (2010)
14. Stephen Jordan, Hirotada Kobayashi, **Daniel Nagaj**, Harumichi Nishimura, *Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems,* QIC Vol.12, No.5&6, 0461-0471 (2012)
15. Daniel Reitzner, **Daniel Nagaj**, Vladimír Bužek, *Quantum Walks,* Acta Physica Slovaca, vol.61, no.6, pp.603-725 (2011)
16. Mária Kieferová, **Daniel Nagaj,** *Quantum Walks on Necklaces and Mixing,* International Journal of Quantum Information, Vol.10, Issue 2, 1250025 (2012)
17. **Daniel Nagaj,** *Universal 2-local Hamiltonian Quantum Computing,* Phys. Rev. A 85, 032330 (2012)
18. Rolando Somma, **Daniel Nagaj**, Mária Kieferová, *Quantum Speedup by Quantum Annealing,* Phys. Rev. Lett. 109, 050501 (2012)
19. Sergey Bravyi, Libor Caha, Ramis Movassagh, **Daniel Nagaj**, Peter Shor, *Criticality without Frustration,* Phys. Rev. Lett. 109, 207202 (2012)
20. Sean Hallgren, **Daniel Nagaj**, Sandeep Narayanaswami, *The Local Hamiltonian on a Line with Eight States is QMA-complete,* accepted for publication in Quantum Information & Computation (2012)