The computational power of normalizer circuits over infinite and black-box groups

Juan Bermejo-Vega[1], Cedric Yen-Yu Lin[2], and Maarten Van den Nest[1]

[1] *Max-Planck-Institut für Quantenoptik, Theory Division, Garching, Germany.*
[2] *Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, USA*

Our submission contains two contributions [1, 2], both of which are available at arXiv.org (arXiv:1409.3208 and arXiv:1409.4800).

Normalizer circuits [3, 4] are a family of quantum circuits which generalize Clifford circuits [5–8] to Hilbert spaces associated with arbitrary finite abelian groups $G = \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n}$. Normalizer circuits are composed of normalizer gates. Important examples are quantum Fourier transforms (QFTs), which play a central role in quantum algorithms, such as Shor's [9]. Refs. [3, 4] showed that normalizer circuits of arbitrary size can be *efficiently classically simulated*, thereby serving as example-families of quantum computations that fail to harness the power of QFTs to achieve achieve exponential quantum speed-ups.

In this work we generalize the normalizer circuit framework in two ways [1] [2] and characterize the computational power of these generalizations. In summary our results are as follows:

1. Normalizer circuits over infinite groups [1]. We define normalizer circuits where the associated abelian group G can be *infinite*. We focus on groups of the form $\mathbb{Z}^a \times F$, where F is a finite abelian group as above. The motivation for adding $\mathbb{Z}$ is that several number theoretical problems are naturally connected to problems over the integers (cf. factoring being related to the hidden subgroup over $\mathbb{Z}$). We will show that all resulting normalizer circuits can be simulated classically in polynomial time, thereby extending the classical simulation results obtained in [3, 4].

2. Black box normalizer circuits [2]. This family extends the previous class by allowing finite abelian groups that are *black box groups* $\mathbf{B}$ (as introduced in [10]), i.e. we look at groups of the form $\mathbb{Z}^a \times F \times \mathbf{B}$. With this modification, we will show that several important quantum algorithms providing *superpolynomial speed-ups*—such as Shor's algorithms [9] and other hidden subgroup problems—*are* in fact normalizer circuits. We thus obtain a precise formal connection between this class of powerful quantum algorithms and the framework of normalizer circuits. Furthermore we give a characterization of the power of black-box normalizer circuits by providing a complete problem for this class.

In order to prove our simulability and hardness we develop several **new techniques** for simulating and analyzing normalizer circuits, which provide (altogether) a generalization of the celebrated *stabilizer formalism* [5–8, 11–16, 3, 4]. The most novel feature of our stabilizer formalism over black-box groups, is that it allows us to describe famous quantum algorithms such as Shor's and study exponential quantum speed-ups from a new perspective. In this work we apply this precise connection between Clifford circuits and Shor's algorithm to draw practical statements for quantum algorithm design.

Previous Setting

We first review the setting in previous refs. [3, 4]. In these works one considers a finite Abelian group, given in the form $G_{\text{old}} = \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n}$, to which we associate a Hilbert space $\mathcal{H}$ (the physical system) with a standard basis $\{|g\rangle\}$ labeled by the elements of the group $g \in G_{\text{old}}$. A unitary gate is a *normalizer gate over* G_{old} if it belongs to one of the following categories:

- Gates that compute automorphisms of G_{old};
- Gates that compute quadratic functions of G_{old};
- The quantum Fourier transform over a cyclic subgroup $\mathbb{Z}_{d_i}$ of G_{old}.

A *normalizer circuit over* G_{old} is any quantum circuit composed of normalizer gates.

Our Setting

First, our aim is to extend the notion of normalizer circuits to infinite groups of the form $G = \mathbb{Z}^m \times G_{\text{old}}$. To achieve such a construction we have to take mathematical features of infinite groups into consideration which complicate the treatment compared to finite groups. We deal here with the following issues:

1. Infinite dimensions. The physical system associated with G is now an infinite dimensional Hilbert space $\mathcal{H} = L^2(G)$.

2. Adding the torus group $\mathbb{T}$. As the group of characters of $\mathbb{Z}^m$ is not isomorphic to itself but to $\mathbb{T}^m$ (the m-dimensional torus group), the QFT over $\mathbb{Z}$ maps $L^2(\mathbb{Z})$ unitarily onto a different Hilbert space, i.e., $L^2(\mathbb{T})$. This is an important difference compared to finite abelian groups G_{old}, where the QFT maps $\mathcal{H}$ to itself. This phenomenon has important consequences. In particular, in order to construct a closed normalizer formalism, we have to consider groups of the form

$$\mathbb{Z}^a \times \mathbb{T}^b \times G_{\text{old}}. \tag{1}$$

Note that $\mathbb{T}^m$ is a continuous group.

Secondly, we consider normalizer circuits over black-box groups. Recall that every finite abelian group is isomorphic to a group of the form G_{old}. However, computing this decomposition is in general computationally hard (this is e.g. the case for the multiplicative group $\mathbb{Z}_N^\times$ [17]). Finite abelian groups for which such a direct product product decomposition is a priori unknown are formalized by considering the notion of black-box groups. In this work, a *black-box group* $\mathbf{B}$ is a finite Abelian group whose elements have unique encodings[1] and whose elements can be *efficiently* multiplied/added ("efficiently" here means "in classical polynomial time" or, alternatively, "at unit cost by an oracle", which is the black box). In our work, a **black box normalizer circuit** is simply a normalizer circuit over a group G which contains a black-box group $\mathbf{B}$: in other words, the group G is of the form

$$\mathbb{Z}^a \times \mathbb{T}^b \times G_{\text{old}} \times \mathbf{B}. \tag{2}$$

[1] Black box groups were introduced in [10] in a more general setting; in general, they neither have to be Abelian nor uniquely encoded.

Main Results

Classical simulability of normalizer circuits over $\mathbb{Z}^a \times \mathbb{T}^b \times G_{\text{old}}$.

We show that normalizer circuits over such groups can be efficiently simulated classically, thereby generalizing the simulation results for normalizer circuits over finite abelian groups obtained in [3, 4].

For the simulation we develop new *stabilizer formalism* techniques. Our simulations differ from previous stabilizer simulations because they can handle **continuous infinite groups** G as well as continuous-infinite stabilizer groups. In fact, the groups under consideration are notoriously difficult to handle: they are neither finite, nor finitely generated, nor countable; they are not vector spaces and do not have bases; and they are not compact. The techniques we develop to deal with these groups are as follows:

- *Groups are described in terms of maps.* We show that infinite spaces with the above properties can be efficiently described as real maps acting on simple domains. We apply this technique to store infinitely-generated *stabilizer groups* that encode the evolution of quantum systems. Previous work on stabilizer simulations, in contrast, relied on the fact that generating sets of stabilizer groups could be efficiently stored in their settings.
- *Normal forms* for quadratic functions and homomorphisms are developed and used to find algorithms to track the dynamical evolution of a stabilizer group under the action of a normalizer circuit, again, in terms of real maps.
- *Sampling techniques.* We develop methods to construct ε-nets within groups using Smith normal forms and use these methods to devise an algorithm to simulate measurements at the end of a normalizer circuit.

Black-box normalizer circuits can realize Shor's factoring algorithm.

In contrast to our classical simulation result for groups of the form $\mathbb{Z}^a \times \mathbb{T}^b \times G_{\text{old}}$, allowing black-box groups in our setting dramatically changes the complexity of normalizer circuits. We show that many of the best known quantum algorithms are particular instances of normalizer circuits over black-box groups $\mathbb{Z}^a \times \mathbb{T}^b \times G_{\text{old}} \times \mathbf{B}$. This shows that normalizer circuits over black box groups can offer ***exponential quantum speed-ups*** and break widely used public-key cryptographic systems. Namely, the following algorithms are examples of black-box normalizer circuits (or have equivalent normalizer versions):

- Shor's algorithm for computing discrete logarithms [9]: $G = \mathbb{Z}_{p-1} \times \mathbb{Z}_p^\times$;
- Shor's factoring algorithm [9]: $G = \mathbb{Z} \times \mathbb{Z}_N^\times$;
- Simon's algorithm [18] and other oracular Abelian hidden subgroup problem algorithms [19, 20], are normalizer circuits over groups of the form $G \times \mathbf{B}$, where G and $\mathbf{B}$ are a group and a black-box group determined by the input of the HSP;
- Cheung-Mosca's algorithm for decomposing black-box finite Abelian groups [21, 22] is a combination of several types of black-box normalizer circuits.

Finally, we also show that the problem of decomposing black-box groups is ***complete*** for the considered class: once an oracle to solve that problem (for example an implementation of Cheung-Mosca's algorithm[21, 22]) is provided, our simulation techniques render normalizer circuits simulable classically. This connection suggest that the computational power of these circuits is encapsulated precise in the classical hardness of decomposing black-box groups. This yields a **no-go theorem** for finding new quantum algorithms within the class of black-box normalizer circuits considered.

References

[1] J. Bermejo-Vega, C. Y.-Y. Lin, and M. Van den Nest, "Normalizer circuits and a Gottesman-Knill theorem for infinite-dimensional systems," arXiv:1409.3208 [quant-ph].

[2] J. Bermejo-Vega, C. Y.-Y. Lin, and M. Van den Nest, "The computational power of normalizer circuits over black-box groups," arXiv:1409.4800 [quant-ph].

[3] M. Van den Nest, "Efficient classical simulations of quantum Fourier transforms and normalizer circuits over Abelian groups," *Quantum Information and Computation* **0** no. 1, (2012) , arXiv:1201.4867v1 [quant-ph].

[4] J. Bermejo-Vega and M. Van Den Nest, "Classical simulations of Abelian-group normalizer circuits with intermediate measurements," *Quantum Info. Comput.* **14** no. 3-4, (2014) , arXiv:1210.3637 [quant-ph].

[5] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*. PhD thesis, California Institute of Technology, 1997. quant-ph/9705052v1.

[6] D. Gottesman, "The Heisenberg representation of quantum computers," in *Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*. International Press, 1999. quant-ph/9807006v1.

[7] E. Knill, "Non-binary unitary error bases and quantum codes," tech. rep., Los Alamos National Laboratory, 1996. quant-ph/9608048.

[8] D. Gottesman, "Fault-tolerant quantum computation with higher-dimensional systems," in *Selected papers from the First NASA International Conference on Quantum Computing and Quantum Communications*. Springer, 1998. quant-ph/9802007v1.

[9] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Sci. Statist. Comput. 26* (1997) .

[10] L. Babai and R. Beals, "A polynomial-time theory of black-box groups I," in *Groups St Andrews 1997 in Bath*, vol. I of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 1999.

[11] J. Dehaene and B. De Moor, "Clifford group, stabilizer states, and linear and quadratic operations over GF(2)," *Phys. Rev. A* **68** (2003) , quant-ph/0304125v1.

[12] S. Aaronson and D. Gottesman, "Improved simulation of stabilizer circuits," *Phys. Rev. A* **70** (2004) , quant-ph/0406196.

[13] E. Hostens, J. Dehaene, and B. De Moor, "Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic," *Phys. Rev. A* **71** (2005) , quant-ph/0408190v2.

[14] N. de Beaudrap, "A linearized stabilizer formalism for systems of finite dimension," *Quantum Info. Comput.* **13** no. 1-2, (2013) , arXiv:1102.3354v3 [quant-ph].

[15] M. Van den Nest, "Classical simulation of quantum computation, the Gottesman-Knill theorem, and slightly beyond," *Quantum Info. Comput.* **10** no. 3, (2010) , arXiv:0811.0898 [quant-ph].

[16] R. Jozsa and M. Van Den Nest, "Classical simulation complexity of extended Clifford circuits," *Quantum Info. Comput.* **14** no. 7&8, (2014) , arXiv:1305.6190 [quant-ph].

[17] V. Shoup, *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2nd ed., 2008.

[18] D. R. Simon, "On the power of quantum computation," *SIAM Journal on Computing* **26** (1994) .

[19] A. Y. Kitaev, "Quantum measurements and the Abelian stabilizer problem," 1995. arXiv:quant-ph/9511026v1.

[20] D. Boneh and R. Lipton, "Quantum cryptanalysis of hidden linear functions," in *Advances in Cryptology — CRYPT0' 95*, D. Coppersmith, ed., vol. 963 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 1995.

[21] M. Mosca, *Quantum computer algorithms*. PhD thesis, University of Oxford, 1999.

[22] K. K. H. Cheung and M. Mosca, "Decomposing finite Abelian groups," *Quantum Info. Comput.* **1** no. 3, (2001) , cs/0101004.