COST Action IC1405
Reversible Computation
Extending Horizons of Computing

Working Group 3 - Reversible Circuit Design
Final report

May 27, 2019

COST Action IC1405: Reversible Computation - Extending Horizons of Computing

Final Report for WG3

This report summarizes the results obtained in Working Group 3 of the COST Action IC 1405 on reversible computations in the years 2015-2019. The respective contributions are structured along the categories

- Function Representations and Classes,
- Gate Libraries,
- Embedding,
- Synthesis algorithms for reversible functions,
- Synthesis algorithms for non-reversible functions,
- Synthesis algorithms based on HDLs, and
- Applications

which have been introduced in the WG3 State-of-the-art Report which is accessible through https://github.com/COST-IC1405/wg3-soar-report/blob/master/README.md.

Function Representations and Classes

F.Z. Hadjam, C. Moraga: A symbolic calculus for a class of quantum computing circuits. *Electronics Letters* **51**(9), 2015, 682-683.

This paper introduces a symbolic calculus to evaluate the output signals at the target line(s) of quantum computing subcircuits using controlled negations and controlled-Q gates, where Q represents the k-th root of [0 1; 1 0], the unitary matrix of NOT, and k is a power of two. The controlling signals are GF(2) expressions possibly including Boolean expressions. The method does not require operating with complex-valued matrices. The method may be used to verify the functionality and to check for possible minimization of a given quantum computing circuit using target lines. The method does not apply for a whole circuit if there are interactions among target lines. In this case the method applies for the independent subcircuits.

P. Kerntopf, C. Moraga,K. Podlaski, and R.S. Stanković: Towards classification of reversible functions with homogeneous component functions. in: *IWBP* **12**, 2016, 21-28.

Although during the last 15 years the field of reversible circuit synthesis has been intensively studied very few publications have been devoted to classification of reversible functions. In the paper we consider whether all component functions of a reversible function either can belong to the same equivalent class in some classifications or can have the same property in the sense of classical logic synthesis. This problem has a direct relationship to studying different aspects of classification of reversible functions. We have calculated all NPN-equivalence classes of balanced Boolean functions up to 4 variables (never published) and all NPNP-equivalence classes of reversible functions of 3 variables (correcting earlier data). We also present component functions of any number of variables belonging to the same equivalence class or having the same property.

P. Kerntopf, K. Podlaski, C. Moraga and R.S. Stanković: Study of reversible ternary functions with homogeneous component functions. in: *ISMVL* **47**, 2017, 191-196.

In an earlier paper the authors considered whether all component functions of a reversible Boolean function either can have the same property in the sense of classical logic synthesis or can belong to the same equivalent class under some equivalent relations. This problem has a direct relationship to studying different aspects of classification of reversible functions. In this paper solutions of the problem are presented for reversible ternary functions. It is shown that for linear/affine functions the results in binary and ternary cases differ significantly.

P. Kerntopf.,C. Moraga,K. Podlaski, and R.S. Stanković: Towards classification of reversible functions. in: *Further Improvements in the Boolean Domain*, Bernd Steinbach (ed.), Cambridge Scholars Publishing, 2017, 21 pp.

In this chapter reversible functions with component functions which have the same known property or belong to the same equivalence class in some classifications are studied. Investigating such problems may lead to new classifications which would be interesting from the point of view of reversible circuit synthesis. The presented results show that for $n \geq 3$ there exist reversible Boolean functions having all component functions being homogeneous and non-degenerate.

P. Niemann and R. Wille: *Compact Representations for the Design of Quantum Logic*. Springer, 2017.

This book discusses modern approaches and challenges of computer-aided design (CAD) of quantum circuits with a view to providing compact representations of quantum functionality. Focusing on the issue of quantum functionality, it presents Quantum Multiple-Valued Decision Diagrams (QMDDs – a means of compactly and efficiently representing and manipulating quantum logic. For future quantum computers, going well beyond the size of present-day prototypes, the manual design of quantum circuits that realize a given (quantum) functionality on these devices is no longer an option. In order to keep up with the technological advances, methods need to be provided which, similar to the design and synthesis of conventional circuits, automatically generate a circuit description of the desired functionality. To this end, an efficient representation of the desired quantum functionality is of the essence. While straightforward representations are restricted due to their (exponentially) large matrix descriptions and other decision diagram-like structures for quantum logic suffer from not comprehensively supporting typical characteristics, QMDDs employ a decomposition scheme that more naturally models quantum systems. As a result, QMDDs explicitly support quantum-mechanical effects like phase shifts and are able to take more advantage of corresponding redundancies, thereby allowing a very compact representation of relevant quantum functionality composed of dozens of qubits. This provides the basis for the development of sophisticated design methods as shown for quantum circuit synthesis and verification.

P. Niemann, A. Zulehner, R. Wille, and R. Drechsler: Efficient construction of QMDDs for irreversible, reversible, and quantum functions, in: *RC* **9**, 2017.

In reversible as well as quantum computation, unitary matrices (so-called transformation matrices) are employed to comprehensively describe the respectively considered functionality. Due to the

exponential growth of these matrices, dedicated and efficient means for their representation and manipulation are essential in order to deal with this complexity and handle reversible/quantum systems of considerable size. To this end, Quantum Multiple-Valued Decision Diagrams (QMDDs) have shown to provide a compact representation of those matrices and have proven their effectiveness in many areas of reversible and quantum logic design such as embedding, synthesis, or equivalence checking. However, the desired functionality is usually not provided in terms of QMDDs, but relies on alternative representations such as Boolean Algebra, circuit netlists, or quantum algorithms. In order to apply QMDD-based design approaches, the corresponding QMDD has to be constructed first - a gap in many of these approaches. In this paper, we show how QMDD representations can efficiently be obtained for Boolean functions, both reversible and irreversible ones, as well as general quantum functionality.

K. Podlaski: Cycle structures of the reversible Hidden Weighted Bit function. in: *RM Workshop* **13**, 2017, 73-78.

Reversible Hidden Weighted Bit function (HWBnxn) is very often used as one of the “hardest” benchmarks for synthesis algorithms. In the area of reversible synthesis some of the best known algorithms are based on cycle representation of reversible functions. The structure of cycles for a given function has an impact on size of the circuit implemented with usage of cycle-based methods. Although many papers have been published on reversible functions there are no works focused on cycle structure of HWBnxn. This paper presents some results on analysis of cycles for HWBnxn functions. These results can be used to develop new synthesis algorithms or function complexity measures.

P. Kerntopf, C. Moraga, K. Podlaski, R.S. Stanković: Towards Classification of Reversible Functions. in: *Further Improvements in the Boolean Domain* (B. Steinbach, Ed.) Cambridge Scholars Publishing, 2018, 384-404.

In this paper the question whether all component functions of a reversible function of any number of variables can either belong to the same equivalence class in some classifications or can have the same property in the sense of classical switching theory is considered. This problem has a direct relationship to studying different aspects of the classification of reversible functions.

P. Kerntopf, R.S. Stanković, K. Podlaski, and C. Moraga: Ternary/MV reversible functions with component functions from different equivalence classes. in: *ISMVL* **48**, 2018, 109-114.

In an earlier paper the authors considered whether all component functions of a ternary reversible function either can belong to the same equivalent class in some classifications or can have the same property in the sense of classical logic synthesis. In this paper it is shown that there exist ternary/MV reversible functions of any number of variables with all component functions belonging to different P-equivalence classes.

P. Kerntopf, K. Podlaski, C. Moraga, R.S. Stanković: New results on reversible functions having component functions with specified properties. in: *IWBP* **13**, 2018, 151-166.

In the traditional logic synthesis different classifications of non-reversible Boolean functions have found many applications. Recently, some attempts to deal with classification of reversible functions

have been published. In this paper, solutions to two problems which have not been addressed yet are presented. The solutions were find by extrapolation of cycle structures for 3 and 4-variable reversible functions obtained in the course of enumerative computations.

K. Podlaski: Reversible Functions in Walsh-Hadamard Domain. in: *IWBP* **13**, 2018, 73-83.

Spectral methods has been used in analysis and design of classical Boolean circuits for a very long time. Recently, application of some of these methods have been studied in the field of reversible functions and circuits. In the paper the Walsh spectrum is considered in the context of reversible circuit synthesis. A general idea of synthesis procedure that does not add ancilla lines is also presented.

R. Wille, P. Niemann, A. Zulehner, and R. Drechsler: Decision diagrams for the design of reversible and quantum circuits. in: *International Symposium on Devices, Circuits and Systems (ISDCS)*, 2018.

Reversible circuits found great interest in the past as an alternative computation paradigm which can be beneficial e.g. for encoder circuits, low power design, adiabatic circuits, verification, and much more. Besides that, reversible circuits provide the basis for many components of quantum circuits, which by themselves emerged as a very promising computing technology that, particularly these days, gains more and more relevance. All that led to a steadily increasing demand for methods that efficiently and correctly design such circuits. Decision diagrams play an important role in the design of conventional circuitry. In the meantime, also their benefits for the design of the newly emerging reversible and quantum circuits become evident. In this overview paper, we review and illustrate past work on decision diagrams for such circuits and sketch corresponding design methods relying on them. By this, we demonstrate how broadly decision diagrams can be employed in this area and what benefits they yield for these emerging technologies.

A. Zulehner, P. Niemann, R. Drechsler, and R. Wille: Accuracy and compactness in decision diagrams for quantum computation. in: *DATE*, 2019.

Quantum computation is a promising research field since it allows to conduct certain tasks exponentially faster than on conventional machines. As in the conventional domain, decision diagrams are heavily used in different design tasks for quantum computation like synthesis, verification, or simulation. However, unlike decision diagrams for the conventional domain, decision diagrams for quantum computation as of now suffer from a trade-off between accuracy and compactness that requires parameter fine-tuning on a case-by-case basis. In this work, we - for the first time - describe and evaluate the effects of this trade-off. Moreover, we propose an alternative approach that utilizes an algebraic representation of the occurring irrational numbers and outline how this can be incorporated in a decision diagram in order to overcome this trade-off.

Gate Libraries

M. Lukac, C. Moraga,and M. Kameyama: The CnF logic gates derived from CnNOT gates. in: *IWBP* **12**, 2016, 29-34.

The C2NOT gate is one of the simplest Turing universal reversible logic gate. Implemented in quantum circuit technologies in the CV/CV†/CNOT model the C2NOT gate is in general built by two components: a classical set of single variables controlled CV/CV† gates implementing some quantum function interference pattern and a set of quantum gates implementing a quantum function

controlled by a symmetric like function. These two components allow to overcome the limitation of the inability of classical reversible two qubit gates in generating a Turing universal function. In this paper we analyze both of these components and study what other functions can be created using this two qubit gates. The application of this study is the possible use of low cost reconfiguration of a reversible or quantum FPGA.

C. Moraga: Quantum p-valued Toffoli and Deutsch gates with conjunctive or disjunctive mixed polarity control, in: *ISMVL* **46**, 2016, 241-246.

In this paper the models of reversible Toffoli and quantum Deutsch gates are extended to the p-valued domain. Their structural parameters are determined and their behavior is proven. Both conjunctive and disjunctive control strategies with positive and mixed polarities are introduced for the first time in a p-valued domain. The design is based on elementary Muthukrishnan-Stroud quantum gates, hence the realizability of the extended gates in the context of ion traps should be possible.

C. Moraga: Design of p-valued Deutsch quantum gates with multiple control signals and mixed polarity, in: *RC* **8**, 2016, 175-180.

This paper presents a detailed study of the realization of p–valued Deutsch quantum gates with $n > 2$ controlling signals, both under conjunctive and disjunctive control, and including zero or mixed polarity of the controlling signals. It is shown that the realization complexity is in $O(pn - 1)$. The realization comprises only Muthukrishnan-Stroud elementary quantum gates.

M. Soeken, N. Abdessaied,and G. De Micheli: Enumeration of reversible functions and its application to circuit complexity, in: *RC* **8**, 2016, 255-270.

A new theoretical result relates Boolean function classification for reversible functions to the multiple-controlled Toffoli gate library.

M. Yüksel; S.O. Erbil, A.B. Ari, and M.S. Hanay: Design and fabrication of CSWAP gate based on nano-electromechanical systems, in: *RC* **8**, 2016.

In order to reduce undesired heat dissipation, reversible logic offers a promising solution where the erasure of information can be avoided to overcome the Landauer limit. Among the reversible logic gates, Fredkin (CSWAP) gate can be used to compute any Boolean function in a reversible manner. To realize reversible computation gates, Nano-electromechanical Systems (NEMS) offer a viable platform, since NEMS can be produced en masse using microfabrication technology and controlled electronically at high-speeds. In this work-in-progress paper, design and fabrication of a NEMS-based implementation of a CSWAP gate is presented. In the design, the binary information is stored by the buckling direction of nanomechanical beams and CSWAP operation is accomplished through a mechanism which can selectively allow/block the forces from input stages to the output stages. The gate design is realized by fabricating NEMS devices on a Silicon-on-Insulator substrate.

Z. Hu, V. Deibuk: Design of ternary reversible/quantum sequential elements. *Journal of Thermoelectricity*, no. 1, 2018, 5-17.

The extensive use of the principles of reversible computing makes it possible to minimize energy losses during the operation of computer devices. The design of reversible memory elements of the ternary logic is an actual task because they are necessary devices of modern electronics. In the paper, the main reversible sequential elements of the ternary logic were synthesized on the base of the permutative one-input and two-input gates proposed by Muthukrishnan and Stroud (MS-gates). Using the improved adaptive genetic algorithm, we proposed ternary reversible D-, T-, and JK-latches and flip-flops. To the best of our knowledge, ternary reversible T- and JK-flip-flops are synthesized for the first time on this basis. The proposed algorithm is also used for the synthesis of a reversible ternary Fredkin gate, resulting in the improvement of a quantum cost compared to the existing counterparts. The sequential elements synthesized in this work can be built by the liquid ion trap quantum technology thanks to the used MS-gates. Improvements with respect to the quantum cost, number of constant inputs, delay time, and number of garbage outputs are reported. This work is intended to attract the attention of specialists in thermoelectricity to the possibility of using reversible electronics to the design of thermoelectric devices

M. Lukac, C. Moraga: The CnF Logic Functions derived from CnNOT Gates. in: *Further Improvements in the Boolean Domain* (B. Steinbach, Ed.). Cambridge Scholars Publishing, 2018, 405-413.

In this paper we closely look and study some of the properties related to fast switching of functions using one of the possible realizations of the CnNOT quantum gates. We analyze in details how the CnNOT gates can be transformed into different functions and what is the fastest and least expensive possible change.

O. I. Rozhdov, I. M. Yuriychuk and V. G. Deibuk: Building a Generalized Peres Gate with Multiple Control Signals. in: Z. Hu, S. Potoukhov, I. Dychka and M. He (Eds.), *ICCSEEA 2018, International Conference on Advances in Computer Science for Engineering and Education, Advances in Intelligent Systems and Computing* **754**, Springer, 2019, 155-164

The paper presents a physical realization of the generalized quantum Peres and Toffoli gates with *n*-control signals, implemented in a one-dimensional chain of nuclear spins (one half) in a strong magnetic field coupled by an Ising interaction. Quantum algorithms in such system can be performed by transverse electromagnetic radio-frequency field using a number of resonant π-pulses on the initial states. The maximum number of π-pulses needed for the implementation of the Peres gate with *n*-control signals is discussed. It is found, that required number of π-pulses linearly scales with the number *n* of the control signals of the generalized quantum Peres gate. Comparison of our studies with the known values of the quantum cost of the generalized Peres gate allows us to suggest that proposed physical implementation of the gate is more efficient. The fidelity parameter is used to study the performance of the generalized Peres gate as a function of the relative error of the resonance frequency. The limits of an imbalance of the generator settings remaining the gate well defined are determined.

Reversible Computation Gates with Nanoelectromechanical Systems. *Project No 115E833* supported by the Scientific and Technological Council of Turkey (TUBITAK), January 1, 2026 – January 1, 2019, Department of Mechanical Engineering and National Nanotechnology Research Center (UNAM), Bilkent University, Ankara, Turkey

In this project, two reversible logic gates, Feynman and Majority-Voter Gates, were realized using Nanoelectromechanical Systems technology. The project contributes to the reversible computation

technology, an emerging field for niche applications and ensure the contribution of Turkey to the relevant COST action.

It is important to develop computation platforms alternative to CMOS-based digital electronics systems, both for fundamental research and niche applications - military, cryptologic, space etc. Especially, a new approach called reversible computation, which does not increase entropy, is important for two ways. First, reversible computation processes do not have to consume energy in principle. Second, it is possible to rewind the state of the system in architectures based on reversible computation. This capability enables efficient debugging and fault tolerance in these architectures. Apart from these expected advantages, unanticipated capabilities may emerge with further progress in the field.

Nanoelectromechanical Systems (NEMS), the platform to implement reversible computation, is defined as electronically controllable mechanical structures with at least one submicrometer dimensions. NEMS devices is a promising platform for alternative information processing technologies as NEMS can be produced in masses using microchip fabrication technology, can be controlled electronically, can be operated at high temperatures, can be operated at high speeds and can be used for reversible computation. In this project, NEMS technology will be used to implement two reversible logic gates. The first gate is the Feynman gate where the control bit being 0 or 1 determines whether the data on the second bit is kept intact or reversed. The other gate, Majority-Voter gate, signals whether 0 or 1 is represented more among the three bits. With this project, the realization of reversible logic technology will proceed on notch further and nanomechanical computation will be implemented.

Two different approaches were used to store and process data with NEMS technology. With Static NEMS approach, the buckling of a nanomechanical beam either to left or right stores the data. To implement gates between the interaction of beams, mechanical linkages were used.

In the other approach taken, NEMS structures will be dynamically driven to parametric resonance condition. In this technique, the spring constant of the structure is modulated periodically, which then causes the structure to undergo resonant oscillations. In this situationm the phase difference between the mechanical vibration and the parametric drive signal is either 0° or 180°. The former case is designated as logic-0 and the latter case is logic-1. To process information between bits encoded in mechanical vibrations, signals that will induce coupling between different modes will be applied to the device. These interaction signals are at the difference frequency between the modes and their application will transfer the mechanical energy from one mode to another mode while controlling phase information. The applied control signal either preserves or flips the data and in this way implements the Feynman gate.

The methods undertaken in this project can be summarized as:

- Production of NEMS devices through nanofabrication,
- Characterization of NEMS structures through electrostatic drive and piezoresistive readout,
- Data storage through the buckling of NEMS structures and implementation of three-bit Majority-Voter gate,
- Excitation of NEMS structures through parametric resonance and two-bit data storage in two vibrational modes,
- Implementation of Feynman gate through the intermodal coupling.

The project has shown the potential of NEMS technology in the field of information processing. With this project, the smallest and fastest NEMS structure for information processing purposes were realized. At the end of the project, a NEMS based platform was developed for the study of even more complex information processing tasks. Throughout the project, junior researchers were trained in the field of NEMS/MEMS, one of the areas deemed high-priority by Tubitak. The project was the source for two MS and one PhD theses.

S. O. Erbil, U. Hatipoglu, C. Yanik, M. Ghavami, A. B. Ari, M. Yuksel and M. S. Hanay: Full electrostatic control of nanomechanical buckling. *Preprint, arXiv* 1902.05037, 2019

Buckling at the micro- and nano-scale generates distant bistable states which can be beneficial for sensing, shape-reconfiguration and mechanical computation applications. Although different approaches have been developed to access buckling at small scales, such as the use heating or pre-stressing beams, very little attention has been paid so far to dynamically and precisely control all the critical bifurcation parameters — the compressive stress and the lateral force on the beam. Precise and on-demand generation of compressive stress on individually addressable microstructures is especially critical for morphologically reconfigurable devices. Here, we develop an all-electrostatic architecture to control the compressive force, as well as the direction and amount of buckling, without significant heat generation on micro/nano structures. With this architecture, we demonstrated fundamental aspects of device function and dynamics. By applying voltages at any of the digital electronics standards, we have controlled the direction of buckling. Lateral deflections as large as 12% of the beam length were achieved. By modulating the compressive stress and lateral electrostatic force acting on the beam, we tuned the potential energy barrier between the post-bifurcation stable states and characterized snap-through transitions between these states. The proposed architecture opens avenues for further studies that can enable efficient actuators and multiplexed shape-shifting devices.

Embedding

A. Zulehner and R. Wille: Make it reversible: Efficient embedding of non-reversible functions. in: *DATE*, 2017.

Reversible computation became established as a promising concept due to its application in various areas like quantum computation, energy-aware circuits, and further areas. Unfortunately, most functions of interest are non-reversible. Therefore, a process called embedding has to be conducted to transform a non-reversible function into a reversible one – a coNP-hard problem. Existing solutions suffer from the resulting exponential complexity and, hence, are limited to rather small functions only. In this work, an approach is presented which tackles the problem in an entirely new fashion. We divide the embedding process into matrix operations, which can be conducted efficiently on a certain kind of decision diagram. Experiments show that improvements of several orders of magnitudes can be achieved using the proposed method. Moreover, for many benchmarks exact results can be obtained for the first time ever

A. Zulehner and R. Wille: Pushing the number of qubits below the minimum: Realizing compact Boolean components for quantum logic. in: *DATE*, 2018.

Research on quantum computers has gained attention since they are able to solve certain tasks significantly faster than classical machines (in some cases, exponential speed-ups are possible). Since quantum computations typically contain large Boolean components, design automation techniques are required to realize the respective Boolean functions in quantum logic. They usually introduce a significant amount of additional qubits – a highly limited resource. In this work, we propose an alternative method for the realization of Boolean components for quantum logic. In contrast to the current state-of-the-art, we dedicatedly address the main reasons causing the additionally required qubits (namely the number of the most frequently occurring output pattern as well as the number of primary outputs of the function to be realized) and propose to manipulate the function so that both issues are addressed. The resulting methods allow to push the number of required qubits below what is currently considered the minimum.

A. Zulehner, P. Niemann, R. Drechsler, and R. Wille: One additional qubit is enough: Encoded embeddings for Boolean components in quantum circuits. in: *ISMVL* **49**, 2019.

Research on quantum computing has recently gained significant momentum since first physical devices became available. Many quantum algorithms make use of so-called oracles that implement Boolean functions and are queried with highly superposed input states in order to evaluate the implemented Boolean function for many different input patterns in parallel. To simplify or enable a realization of these oracles in quantum logic in the first place, the Boolean reversible functions to be realized usually need to be broken down into several non-reversible sub-functions. However, since quantum logic is inherently reversible, these sub-functions have to be realized in a reversible fashion by adding further qubits in order to make the output patterns distinguishable (a process that is also known as embedding). This usually results in a significant increase of the qubits required in total. In this work, we show how this overhead can be significantly reduced by utilizing coding. More precisely, we prove that one additional qubit is always enough to embed any non-reversible function into a reversible one by using a variable-length encoding of the output patterns. Moreover, we characterize those functions that do not require an additional qubit at all. The made observations show that coding often allows one to undercut the usually considered minimum of additional qubits in sub-functions of oracles by far.

Synthesis algorithms for reversible functions

M. Rawski: Application of functional decomposition in synthesis of reversible circuits, in: *RC* **7**, 2015.

In this paper application of 'divide and conquer' paradigm is proposed that adopts for reversible logic synthesis a concept of functional decomposition developed for conventional logic synthesis. The initial function is decomposed into a network of smaller sub-functions that are easier to analyze and synthesize into reversible blocks. The final circuit is then composed of these blocks. The results of experiments reported in this work demonstrate the potential of the proposed approach.

M. Rawski and P. Szotkowski: Reversible logic synthesis of Boolean functions using functional decomposition. in: *MIXDES* **22**, 2015.

This paper presents the application of functional decomposition, developed for conventional logic synthesis, as a potentially crucial step in synthesis of reversible logic. A decomposition of a Boolean function into a network of smaller sub-functions, subsequently synthesized into reversible blocks and composed into a reversible system, often yields better results than direct reversible synthesis of the original Boolean function. The experimental results presented in this paper demonstrate the potential of the proposed approach.

S. Stojkovic, M. Stankovic, and C. Moraga: Complexity reduction of Toffoli networks based on FDD, *Facta Universitatis, Series E.E.* **28**, 2015, 251-262.

This paper presents a method for the reduction of the number of lines and gates in the Toffoli gate realization of Boolean functions based on their Functional Decision Diagram (FDD) representation. Experiments show that, when the proposed reduction is used, the realization of the given function based on FDD will, on the average, be smaller in terms of the number of lines and the number of gates than the realizations based on an OKFDD, an optimal BDD or based on a FDD by using previously defined algorithms.

F. Hadjam and C. Moraga: Distributed RIMEP2: a comparative study between a hierarchical model and the islands model in the context of reversible circuits design. in: *IWBP* **12**, 2016, 13-20.

A distributed hierarchical evolutionary system, named DRIMEP2, for the design of reversible circuits was earlier successfully introduced. In the present work we extend the concept of distributed evolutionary design algorithm, enlarging DRIMEP2 to a family of distributed systems including the hierarchical model, the Island Model, and two hybrid architectures: one comprising a hierarchical model with islands at the lower level, and another one consisting of islands of hierarchical models. A set of 17 randomly chosen 4-bit reversible benchmarks has been evolved under similar parameter environments for the four studied systems. For each benchmark, 100 independent runs were realized and statistics such as “average quantum cost”, “average successful runs” and “total execution time” were considered in the comparison. The results show that in most cases the straight hierarchical model and the hierarchical model with islands of workers are the best in terms of “quantum cost”, although all four distributed DRIMEP2 systems obtained a close performance.

J. Jegier and P. Kerntopf: Gate count minimal reversible circuits, in: *Problems and New Solutions in the Boolean Domain*, Cambridge Scholars Publishing, Bernd Steinbach (ed.), 2016, 342-355.

A few sequences of reversible functions of an arbitrary number of variables, e.g., hwbn and nth prime inc, have been proposed as benchmarks, but these functions are quite complex and no minimal gate count or minimal quantum cost circuits are known for them for n > 4. Thus, developing methods of constructing functions with known minimal circuits is needed. In this paper, two infinite sequences of functions of any number of variables are presented for which we have constructed gate count minimal circuits (proofs of their minimality are given).

K. Podlaski: Reversible circuit synthesis using binary decision diagrams, in: *MIXDES* **23**, 2016, 235-238.

In this paper a new implementation of the known transformation based algorithm is presented. The existing transformation based algorithms use truth tables during computation. This leads to memory restrictions. On the other hand any Boolean function can be represented using Binary Decision Diagrams (BBD). This representation is more compact and uses less memory than truth table representation. The presented new implementation of the transformation based algorithm can be used for synthesis of much larger reversible functions than the original version of the algorithm.

M. Soeken and A. Chattopadhyay: Unlocking efficiency and scalability of reversible logic synthesis using conventional logic synthesis, in: *DAC* **53**, 2016.

This paper applies hierarchical synthesis to a higher level compared to decision diagrams. The irreversible input function is represented as an And-inverter graph (AIG). Subgraphs in the AIG are determined, which are then optimally embedded and synthesized using symbolic functional heuristic algorithms.

M. Soeken, G.W. Dueck, and D.M. Miller: A fast symbolic transformation based algorithm for reversible logic synthesis, in: *RC* **8**, 2016, 307-321.

This paper presents a symbolic variant of the transformation based synthesis approach for reversible logic. The approach allows the realization of larger reversible functions without additional ancilla lines. It exploits a property considering the ordering in which assignments need to be considered for adjustment. Both a BDD and a SAT based implementation of the symbolic synthesis algorithm have been presented.

M. Soeken, L. Tague, G.W. Dueck, and R. Drechsler: Ancilla-free synthesis of large reversible functions using binary decision diagrams, *J. Symb. Comput.* **73**, 2016, 1-26.

This paper proposes a symbolic variant of the truth table based variant introduced by De Vos and Van Rentergem. It works on the binary decision diagram representation of the reversible function. The paper also introduces how simple algebraic operations can be performed on the BDD representation of reversible functions, e.g., gate composition or reversibility checking.

S. Stojković,C. Moraga, M.M. Stanković, R.S. Stanković: Procedure for FDD-based reversible synthesis by levels, in: *IWBP* **12**, 2016, 5-12.

Decision diagrams are a data structure suitable for reversible circuit synthesis, since the design procedure is reduced to traversing the diagram and replacement of nodes with reversible modules. Decision diagrams differ with respect to decomposition rules assigned to the nodes. This difference reflects into complexity of reversible modules replacing the nodes in the diagram. In this paper, we compare reversible circuits produced from Binary decision diagrams (BDDs), Bidirectional binary decision diagrams (BBDDs), and Functional decision diagrams (FDDs) with different polarity of Davio nodes. Experimental results over benchmark functions show that these diagrams in many cases produce reversible circuits with both smaller quantum cost and number of lines compared to BDDs and BBDDs.

R. Wille, E. Schönborn, M. Soeken, and R. Drechsler: SyReC: A hardware description language for the specification and synthesis of reversible circuits, in: *Integration* **53**, 2016, 39-53.

This paper presents the findings proposed before in a more comprehensive fashion, including a grammar of the proposed SyReC language as well as detailed description of the synthesis for the data and control flow.

K. Gracki: Reversible gate and circuits descriptions. in: *IEEE-SPIE Joint Symposium on Photonics, Web Engineering, Electronics for Astronomy and High Energy Physics Experiment* ,**40** 2017, 8 pp.

During synthesis of reversible circuits it is needed to use a compact notation of gates in a reversible circuit. The paper presents a method of reversible circuit description. The most popular library is the set of three types of gates called NCT (NOT, CNOT and Toffoli). The presented gate indexing method has been developed for the CNT library of gates.

F. Hadjam, C. Moraga: A hierarchical distributed linear evolutionary system for the synthesis of 4-bit reversible circuits. in: *Studies in Fuzziness and Soft Computing*, R. Seising, H. Allende-Cid (Eds.) Springer International Publishing AG, 2017, 233- 249.

Abstract In this chapter we introduce a distributed version of the RIMEP2 system for the evolutionary synthesis of reversible circuits. A new hierarchical topology of multiple populations is used and a new communication policy is introduced. Such an architecture helps the genetic programming evolutionary algorithm to explore and exploit the search space in an efficient way. The obtained results outperform most of the already published 4-bit reversible circuits achieving lower quantum cost realizations.

Z. Hu, I. Yuriychuk, and V. Deibuk: Ternary reversible/quantum latches. in: *IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, 2017, 904-907.

Ternary reversible latches on the basis of one- and two-qutrit permutative Muthukrishnan-Stroud (MS) gates were synthesized for the first time. Such gates can be physically implemented on the basis of liquid ion-trap quantum technology. The use of adaptive genetic algorithm allowed designing the circuits of latches that are optimal with respect to quantum cost, number of gates, and delay time. Comparisons of synthesized circuits with known results of other authors were carried out.

J. Jegier and P. Kerntopf: PPRM-based approach to synthesis of reversible functions, in: *IEEE-SPIE Joint Symposium on Photonics, Web Engineering, Electronics for Astronomy and High Energy Physics Experiments* **40**, 2017.

This work proposes a PPRM-based technique for the synthesis of reversible circuits with reduced quantum cost (QC) in generated circuits. Initially, a PPRM cube-list structure is provided as input. Next, the PPRM cubes shared by coordinate functions of a given reversible function are grouped together and each cube is translated to a group of Toffoli reversible gates, similarly to ESOP-based methods. Experimental results show that for important benchmarks with up to 17 variables the presented approach generates circuits with smaller QC than the most successful previous approaches.

J. Jegier and P. Kerntopf: Application of the maximum weighted matching to quantum cost reduction in reversible circuits. in: *MIXDES* **24**, 2017.

In this paper the maximum weighted matching (PMWM) method, well-known from the graph theory, is applied to reduction of quantum cost (QC) in reversible sub-circuits with a common target line. In this way, possibility of application of the PMWM method to optimization of QC is showed for the first time in literature on reversible circuit synthesis. Experimental results have shown that this approach leads to substantial reduction of QC.

J. Jegier: PPRM-based synthesis of reversible logic circuits (in Polish). *PhD thesis*, Department of Electronics and Information Methods, Warsaw University of Technology, Warsaw, Poland, December 2017, 108 pp.

A PPRM-based synthesis approach is presented in this work which has enabled for reducing quantum cost of circuits - in comparison with the best solutions - by 20% on average -, at the expense of using additional lines in the circuit. Additionally, at the postsynthesis stage, algorithms for solving the known maximum weighted matching problem have been applied – for the first time in the literature – to reduction of quantum cost. Moreover, new sequences of benchmark functions and the circuits implementing them were constructed - again for the first time in the literature –as well as proofs of gate count minimality of these circuits for arbitrary number of variables are presented in the thesis.

M. Lukac, P. Kerntopf, and M. Kameyama: An analytic sifting approach to optimization of LNN reversible circuits. in: *RM Workshop* **13**, 2017, 87-92.

In this paper an analytic approach to the variable sifting based on weighting of qubits and gates is presented. The proposed scheme allows to optimally sift multi-control single-target reversible gates within a linear number of steps of computation. In general, it provides smaller amount of SWAP gates required to transform a reversible circuit into a Linear Nearest Neighbor (LNN) model than other approaches. The method is analyzed for two different models of implementation and verified on many benchmarks. The experimental results are compared to state-of-the-art algorithms for design of LNN circuits.

M. Lukac, P. Kerntopf, and M. Kameyama: An analytic sifting approach to optimization of LNN reversible circuits. in: *International Conference on Information Digital Technologies (IDT)* **13**, 2017, 6 pp.

In this paper an analytic approach to the variable sifting based on weighting of qubits and gates is presented. The proposed scheme allows to optimally sift multi-control single-target reversible gates within a linear number of steps of computation and provides in general smaller amount of SWAP gates required to transform a reversible circuit into a Linear Nearest Neighbor (LNN) model than other competing approaches. The method is analyzed for two different models of implementations, is verified on experimental data and the results are compared to the state-of-the-art algorithms for the design of LNN circuits.

M. Rawski and P. Szotkowski: Reversible synthesis of incompletely specified Boolean functions using functional decomposition. in: *IEEE-SPIE Joint Symposium on Photonics, Web Engineering, Electronics for Astronomy and High Energy Physics Experiments* **40** 2017, 8 pp.

The paper presents the application of functional decomposition as a crucial step in synthesis of reversible logic that cost-efficiently implements incompletely specified Boolean functions. A decomposition of an incompletely specified Boolean function into a network of smaller sub-functions, subsequently synthesized into reversible blocks and composed into a reversible system, yields significantly better results than direct reversible synthesis of the original, incompletely specified Boolean function. The experimental results presented in the paper demonstrate the potential of the proposed approach.

A. Skorupski: A method of reversible circuits synthesis based on S-maps. in: *IEEE-SPIE Joint Symposium on Photonics, Web Engineering, Electronics for Astronomy and High Energy Physics Experiments* **40**, 2017, 11 pp.

The paper presents an original method to designing reversible circuits. The main problem of reversible circuits synthesis is designing optimal reversible circuits, i.e. circuits with the minimal number of gates implementing the given reversible function. To design reversible circuits a set of gates must be chosen. The most popular library is the set called NCT (NOT, CNOT and Toffoli) which contains three types of gates. The method presented in this paper is based on the CNT gates. A graphical representation of the reversible function called s-map is introduced in the paper. This representation allows to find optimal solutions.

A. Skorupski: Graphical method of reversible circuits synthesis. Journal of Electronics and Telecommunications (IJET), **63(**3), 2017, 235-240.

The paper presents a new approach to designing reversible circuits. The main problem of reversible logic is designing optimal reversible circuits, i.e. circuits with the minimal number of gates implementing the given reversible function. There are many types of reversible gates. Most popular library is the set of three types of gates so called NCT (NOT, CNOT and Toffoli). The method presented in this paper is based only on the NCT gates. A graphical representation of the reversible function called s-map is introduced in the paper. This representation allows to find optimal reversible circuits.

A. Zulehner and R. Wille: Improving synthesis of reversible circuits: Exploiting redundancies in paths and nodes of QMDD, in: *RC* **9**, 2017.

In recent years, reversible circuits have become an established emerging technology through their variety of applications. Since these circuits employ a completely different structure from conventional circuitry, dedicated functional synthesis algorithms have been proposed. Although scalability has been achieved by using approaches based on decision diagrams, the resulting circuits employ a significant complexity measured in terms of quantum cost. In this paper, we aim for a reduction of this complexity. To this end, we review QMDD-based synthesis. Based on that, we propose optimizations that allow for a substantial reduction of the quantum costs by jointly considering paths and nodes in the decision diagram that employ a certain redundancy. In fact, in our experimental evaluation, we observe substantial improvements of up to three orders of magnitudes in terms of runtime and up to six orders of magnitudes (a factor of one million) in terms of quantum cost.

C. Barbieri, C. Moraga: A Complexity analysis of the cycles-based synthesis of ternary reversible circuits. in: *IWBP* **13**, 2018, 63-71.

The paper studies the main aspects of the realization of 2×2 ternary reversible circuits based on cycles using as a benchmark all 362,880 2×2 ternary reversible functions. It is shown that in most cases, realizations obtained with the MMD+ algorithm have a lower complexity (in terms of cost) than realizations based on cycles. It is shown under which conditions realizations based on transpositions may have the same cost as realizations using larger cycles. Finally it is shown that there are a few special cases where realizations based on transpositions have a lower cost than the MMD+ based realizations. Aspects of scalability are considered in terms of 2×2-based $n\times n$ reversible circuits.

F. Hadjam and C. Moraga: Distributed evolutionary design of reversible circuits. in: *Further Improvements in the Boolean Domain*, B. Steinbach (Ed.), Cambridge Scholars Publishing, 2018, 372-383.

A distributed hierarchical evolutionary system, named DRIMEP2, for the design of reversible circuits was earlier successfully introduced. In the present work we extend the concept of distributed evolutionary design algorithm, enlarging DRIMEP2 to a family of distributed systems including the hierarchical model, the Islands Model, and two hybrid architectures: one comprising a hierarchical model with islands at the lower level, and another one consisting of islands of hierarchical models. A set of 17 selected 4-bit reversible benchmarks has been evolved under similar parameter environments for the four studied systems. For each benchmark, 100 independent runs were realized and statistics such as average quantum cost, average successful runs and total execution time were considered in the comparison. The results show that in most cases the straight hierarchical model and the hierarchical model with islands of workers are the best in terms of quantum cost, although all four distributed DRIMEP2 systems obtained a close performance.

G. Meuli, M. Soeken, and G. De Micheli, Sat-based {CNOT, T} quantum circuit synthesis. in: *RC* **10**, 2018, 175-187.

The prospective of practical quantum computers has lead researchers to investigate automatic tools to program them. A quantum program is modeled as a Clifford+T quantum circuit that needs to be optimized in order to comply with quantum technology constraints. Most of the optimization algorithms aim at reducing the number of T gates. Nevertheless, a secondary optimization objective should be to minimize the number of two-qubit operations (the CNOT gates) as they show lower fidelity and higher error rate when compared to single-qubit operations. We have developed an exact SAT-based algorithm for quantum circuit rewriting that aims at reducing CNOT gates without increasing the number of T gates. Our algorithm nds the minimum {CNOT, T} circuit for a given phase polynomial description of a unitary transformation. Experiments conrm a reduction of CNOT in T-optimized quantum circuits. We synthesize quantum circuits for all single-target gates whose control functions are one of the representatives of the 48 spectral equivalence classes of all 5-input Boolean functions. Our experiments show an average CNOT reduction of 26.84%.

A. Skorupski: The method of reversible circuits design with one-gate prediction, *International Journal of Electronics and Telecommunications (IJET)* **64**(4), 2018, 535-540

The paper presents an original method of designing reversible circuits. This method is destined to most popular gate set with three types of gates CNT (Control, NOT and Toffoli). The presented algorithm based on graphical representation of the reversible function is called s-maps. This algorithm allows to find optimal or quasi-optimal reversible circuits.

S. Stojković, M. M. Stanković, C. Moraga, and R. S. Stanković: FDD-based reversible synthesis by levels. in: *Further Improvements in the Boolean Domain,* B. Steinbach (Ed.) , Cambridge Scholars Publishing, 2018, 372-383, ISBN 978-1-5275-0371-7.

Decision diagrams are a data structure suitable for reversible circuit synthesis, since the design procedure is reduced to traversing the diagram and replacement of nodes with reversible modules. Decision diagrams differ with respect to decomposition rules assigned to the nodes. This difference reflects into complexity of reversible modules replacing the nodes in the diagram. In this paper, a comparison of reversible circuits produced from Binary decision diagrams (BDDs), Bidirectional binary decision diagrams (BBDDs), and Functional decision diagrams (FDDs) with different polarity of

Davio nodes is presented. Experimental results over benchmark functions show that these diagrams in many cases produce reversible circuits with both smaller quantum cost and number of lines compared to BDDs and BBDDs.

A. Zulehner, P. M. N. Rani, K. Datta, I. Sengupta, and R. Wille: Generalizing the Concept of Scalable Reversible Circuit Synthesis for Multiple-valued Logic. in: *ISMVL* **48**, 2018.

Research on reversible circuits has gained significance due to its application in quantum computations and many further areas such as the design of encoders. At the same time, the use of multiple-valued logic gained importance since this reduces the number of required entities in physical systems (e.g. in a future quantum computer). While most research is still conducted in the Boolean domain, there exist only few approaches which realize reversible circuits for multiple-valued logic. Moreover, most of the previously proposed solutions for synthesis of multiple-valued reversible circuits are not scalable and consider ternary (i.e. 3-valued circuits) only. Instead of overcoming these issues by developing new synthesis approaches for multiple-valued reversible circuits from scratch, we propose to utilize the recent accomplishments in the design of Boolean reversible circuits and to generalize them for multiple-valued logic. To this end, we discuss how to generalize Quantum Multiple-valued Decision Diagram based (QMDD-based) synthesis – a synthesis approach for Boolean reversible circuits which has been proven to be scalable and which has been used in several recently developed design flows. The discussions eventually show how to bridge the development gap between Boolean and multiple-valued logic for reversible circuits.

D. Bhattacharjee, M. Soeken, S. Dutta, A. Chattopadhyay, and Giovanni De Micheli: Reversible Pebble Games For Reducing Qubits In Hierarchical Quantum Circuit Synthesis. in: *ISMVL* **49**, 2019, 6 pp.

Hierarchical reversible logic synthesis can find quantum circuits for large combinational functions. The price for a better scalability compared to functional synthesis approaches is the requirement for many additional qubits to store temporary results of the hierarchical input representation. However, implementing a quantum circuit with large number of qubits is a major hurdle. In this paper, it is demonstrated and established how reversible pebble games can be used to reduce the number of stored temporary results, thereby reducing the qubit count. Our proposed algorithm can be constrained with number of qubits, which is aimed to meet. Experimental studies show that the qubit count can be significantly reduced (by up to 63.2%) compared to the state-of-the-art algorithms, at the cost of additional gate count.

B. Schmitt, M. Soeken, G. De Micheli, A. Mishchenko: Scaling-up ESOP synthesis for quantum compilation. in: *ISMVL* **49**, 2019, 6 pp.

Today's rapid advances in quantum computing hardware call for scalable synthesis methods to map combinational logic represented as multi-level Boolean networks (e.g., an and-inverter graph, AIG) to quantum circuits. Such synthesis process must yield reversible logic function since quantum circuits are reversible. Thus, logic representations using exclusive sum-of products (ESOP) are advantageous because of their natural relation to Toffoli gates, one of the primitives in reversible logic. This motivates developing effective methods to collapse AIG logic networks into ESOPs. In this work, we present two state-ofthe-art methods to collapse an AIG into an ESOP expression, describe their shortcomings and introduce a new approach based on the divide-and-conquer paradigm. We demonstrate the effectiveness of our method in collapsing IEEE-compliant half precision floating

point networks. Results show that our method can collapse designs—which were previously not solvable within a week—in less than 5 minutes. We also describe a technique capable of taking advantage of this new method to generate quantum circuits with up to 50% fewer T gates compared to state-of-the-art methods.

A. Skorupski, K. Gracki: The transforming method between two reversible functions. *Journal of Electronics and Telecommunications (IJET)* **65**(1), 2019

This paper presents an original method of designing some special reversible circuits. This method is intended for the most popular gate set with three types of gates CNT (Control, NOT and Toffoli). The presented algorithm is based on two types of cascades with these reversible gates. The problem of transformation between two reversible functions is solved. This method allows to find optimal reversible circuits.

M. Soeken, F. Mozafari, B. Schmitt, G. De Micheli: Compiling permutations for superconducting QPUs. In: *DATE*, 2019, 6 pp.

In this paper the compilation of quantum state permutations into quantum gates for physical quantum computers is considered. A sequence of generic single-target gates, which realize the input permutation, are extracted using a decomposition based reversible logic synthesis algorithm. We present a compilation algorithm that translates single-target gates into a quantum circuit composed of the elementary quantum gate sets that are supported by IBM's 5-qubit and 16-qubit, and Rigetti's 8-qubit and 19-qubit superconducting transmon QPUs. Compared to generic state-of-the-art compilation techniques, our technique improves gate volume and gate depth by up to 59% and 53%, respectively.

M. Soeken, M. Roetteler, N. Wiebe, G. De Micheli: LUT-based hierarchical reversible logic synthesis. *IEEE TCAD*, 2019, in print.

We present a synthesis framework to map logic networks into quantum circuits for quantum computing. The synthesis framework is based on LUT networks (lookup-table networks), which play a key role in conventional logic synthesis. Establishing a connection between LUTs in a LUT network and reversible single-target gates in a reversible network allows us to bridge conventional logic synthesis with logic synthesis for quantum computing, despite several fundamental differences. We call our synthesis framework LUT-based Hierarchical Reversible Logic Synthesis (LHRS). Input to LHRS is a classical logic network representing an arbitrary Boolean combinational operation; output is a quantum network (realized in terms of Clifford+T gates). The framework allows one to account for qubit count requirements imposed by the overlying quantum algorithm or target quantum computing hardware. In a fast first step, an initial network is derived that only consists of single-target gates and already completely determines the number of qubits in the final quantum network. Different methods are then used to map each single-target gate into Clifford+T gates, while aiming at optimally using available resources. We demonstrate the versatility of our method by conducting a design space exploration using different parameters on a set of large combinational benchmarks. On the same benchmarks, we show that our approach can advance over the state-of-the-art hierarchical reversible logic synthesis algorithms.

E. Testa, M. Soeken, L.G. Amaru, G. De Micheli: Logic synthesis for established and emerging computing. *Proceedings of the IEEE* **107**(1), 2019, 165-184.

Logic synthesis is an enabling technology to realize integrated computing systems, and it entails solving computationally intractable problems through a plurality of heuristic techniques. A recent push toward further formalization of synthesis problems has shown to be very useful toward both attempting to solve some logic problems exactly-which is computationally possible for instances of limited size today-as well as creating new and more powerful heuristics based on problem decomposition. Moreover, technological advances including nanodevices, optical computing, and quantum and quantum cellular computing require new and specific synthesis flows to assess feasibility and scalability. This review highlights recent progress in logic synthesis and optimization, describing models, data structures, and algorithms, with specific emphasis on both design quality and emerging technologies. Example applications and results of novel techniques to established and emerging technologies are reported.

Synthesis algorithms for non-reversible functions

I. Lemberski: Asynchronous logic implementation based on factorized DIMS, *Journal of Circuits, Systems and Computer* **26**, 2017, 9 pp.

One of popular methods of asynchronous logic implementation is based on so called Delay-Insensitive-Minterm-System (DIMS), where a sum-of-minterms function is given and each minterm is represented using a state-holding (C-) element. However, such implementation is rather expensive since minterm minimization is not allowed. The structure, called factorized DIMS is proposed. It is shown that under realistic delay limitation, instead of sum-of-minterms, strong indication can be ensured for the sum of mutually orthogonal product terms resolved into factorized form. It reduces significantly implementation complexity.

M. Soeken, M. Roetteler, N. Wiebe, and G. De Micheli: Design automation and design space exploration for quantum computers, in: *DATE* 2017, 470-475.
M. Soeken, M. Roetteler, N. Wiebe, and G. De Micheli: Hierarchical reversible logic synthesis using LUTs, in: *DAC* **54**, 2017.

It has been demonstrated that by combining existing reversible logic synthesis methods with conventional logic synthesis algorithms, it is possible to create scalable design flows for reversible logic with application to quantum computing [SRWM17a]. Input is a Verilog gate level netlist, which is then optimised and resynthesised to meet the requirements of various reversible logic synthesis algorithms. The choice of the underlying reversible logic synthesis algorithm allows design space elaboration by trading off the number of qubits to the number of quantum operations. Based on this work, a new reversible logic synthesis algorithm called LUT-based hierarchical reversible logic synthesis (LHRS) has been presented [SWRM17b]. An open source of the synthesis algorithm is available in RevKit (command: lhrs). The research resulted from a newly commenced collaboration with Microsoft (StationQ, QuArC).

A. Zulehner and R. Wille. Skipping embedding in the design of reversible circuits. in: *ISMVL* **47**, 2017, 173-178.

Synthesis of reversible circuits finds application in many promising domains but has to deal with the fact that the underlying circuits require a unique mapping from the inputs to the outputs. Existing solutions addressed this problem by additionally performing a so-called embedding process prior to synthesis or by naively mapping building blocks of conventional logic to their corresponding reversible counterparts. This leads to solutions that either suffer from limited scalability or yield circuits with a huge number of additionally required circuit lines. In this work, we conduct investigations to overcome these problems. To this end, we simply ignore the fact that an arbitrary Boolean function to be synthesized might be non-reversible and deal with the resulting problem of ensuring a unique input/output mapping during the actual synthesis process. Experimental evaluations indicate that, following this approach, could provide the basis for an alternative synthesis scheme that allows for synthesizing arbitrary Boolean functions in reasonable time and without the need of a prior embedding process.

A. Zulehner and R. Wille: One-pass design of reversible circuits: Combining embedding and synthesis for reversible logic. *IEEE TCAD*, 2017.

Reversible computation is a heavily investigated emerging technology due to its promising characteristics in low-power design, its application in quantum computations, and several further application areas. The currently established functional synthesis flow for reversible circuits is composed of two distinct steps. First, an embedding process is conducted which makes non-unique output patterns distinguishable by adding further variables. Then, this function is passed to a synthesis method which eventually yields a reversible circuit. However, the separate consideration of the embedding and synthesis tasks leads to significant drawbacks: In fact, embedding is not necessarily conducted in a fashion which is suited for the following synthesis process. In addition, embedding adds further variables to the function to be synthesized which exponentially increases its corresponding representation in the worst case. In this work, we propose one-pass design of reversible circuits, which combines embedding and synthesis. This allows for conducting synthesis with a high degree of freedom, since the embedding that suits best is inherently chosen during synthesis. We propose two solutions (an exact an a heuristic one) following this scheme that improve the currently established synthesis flow by magnitudes in terms of runtime – allowing to synthesize a reversible circuit with a minimum number of lines for some of the frequently considered benchmark functions for the first time. Furthermore, a significant reduction of the costs of the resulting circuits (up to several orders of magnitude) is achieved with this new design flow.

A. Zulehner and R. Wille: Exploiting coding techniques for logic synthesis of reversible circuits. in: *ASP-DAC* **23**, 2018.

Reversible circuits are composed of a set of circuit lines that are passed through a cascade of reversible gates. Since the number of circuit lines is crucial, functional logic synthesis approaches have been proposed which realize circuits where the number of circuit lines is minimal. However, since the function to be realized is often non-reversible, additional variables have to be added to the function in order to establish reversibility – leading to a significant overhead that affects the scalability of the synthesis method and yields rather complex circuits. In this work, we propose to overcome these problems by exploiting coding techniques in the logic synthesis of reversible circuits.

To this end, we propose an intermediate encoding of the output patterns that requires fewer additional inputs and outputs. Using this synthesis scheme allows to perform the majority of the synthesis on significantly fewer variables and to exploit several don't care values in the code. Experimental evaluations – where we obtain better scalability and circuits with magnitudes fewer costs – confirmed the benefits of the proposed synthesis approach.

A. Zulehner and R. Wille: QMDD-based one-pass design of reversible logic: Exploring the available degree of freedom. in: *RC* **10**, 2018, 244—250.

Research on synthesis of reversible circuits has found substantial consideration in the past. Corresponding methods can be categorized into functional approaches (which often require a prior embedding step) and structural ones (which are often based on mapping). While functional approaches are less scalable and yield circuits with significantly larger costs, structural approaches typically yield circuits where the number of circuit lines is magnitudes above the minimum. Recently, also the idea of a one-pass design flow has been proposed, which aims to overcome the contradictory shortcomings of both approaches by combining the embedding and the synthesis step of the functional design flow. While this yields further opportunities for a more efficient synthesis, the actually available degree of freedom has not fully been explored yet—not to mention fully exploited. In this work-in-progress-report, we are discussing this issue and explore in detail the potential offered by the one-pass design flow. To this end, we consider the implementation of this flow using QMDD-based synthesis as a representative. The conducted investigations provide a more detailed understanding of this recently proposed flow and demonstrate its potential to be exploited in future work.

I. Lemberski, A. Suponenkovs, M. Uhanova: LUT-Oriented Asynchronous Logic Design Based on Resubstitution, in: *International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS 2019)* **14**, 2019, 4pp.

The method of asynchronous logic synthesis targeting area minimization (number of Look-Up-Tables - LUTs) is proposed. Initially, a single-rail multi-level network is created using ABC synthesis system script. The improvement is done using the resubstitution. For the network compact representation and optimization, an extended PLA table is proposed. The resubstitution is formulated and solved as a covering task: the output of the node which input has been selected for the resubstitution is split into the set of dichotomies. The selected input is removed and the minimal number of inputs are sought to cover the dichotomies. Two-step procedure is proposed: 1) the resubstitution for a network produced by ABC is done; 2) the obtained network is transformed into dual-rail one and the resubstitution is done further. In each step, nodes with zero fan-outs are removed. The procedure guarantees indicating logic. The experiments show, that the result is more that 20% better w.r.t. number of nodes.

Asynchronous Logic Circuits: Methods and Tools for the Design in Reconfigurable Environment. *Project* supported by European Regional Development Fund (ERDF) and the Latvian Government, duration of the project: 3 years (2017-2020).

The project aim is to develop theory and evaluate methodology, design flow and tools of asynchronous circuits implementation on the reconfigurable logic.
Asynchronous hardware attracts an increasing interest because asynchronous circuits are extremely robust. This means, the design is able to adapt to variations of manufacturing process parameters, gate and wire delays, temperature changes, noise, etc. The correct behavior is guaranteed, only the operational speed changes adaptively. Asynchronous circuit speed is higher than synchronous one. Its switching activity and power consumption is lower.

Commercially available reconfigurable logic containing functional blocks (Look-up-Tables - LUTs) that can be (re-)programmed to implement any logic function of given number of variables is state-of-the art design environment.
The design methodology is based on the step-by-step transformation of the initial description into a sub-functions network that can be mapped into LUT–based reconfigurable logic.
The activities include proposing an implementation model matching reconfigurable logic architecture, development methods and tools for:

- Decomposition
- Function minimization
- Completion detection
- Placement and routing

and evaluation of design flow effectiveness.

Synthesis algorithms based on HDLs

R. Wille, O. Keszocze, L. Othmer, M. K. Thomsen, and R. Drechsler: Generating and checking control logic in the HDL-based design of reversible circuits, in: *ISED*, 2016.

Although different from the conventional computing paradigm, reversible computation received significant interest due to its applications in various (emerging) technologies. Here, computations can be executed not only from the inputs to the outputs, but also in the reverse direction. This leads to significantly different design challenges to be addressed. In this work, we consider problems that occur when describing a reversible control flow using Hardware Description Languages (HDLs). Here, the commonly used conditional statements must, in addition to the established if-condition for forward computation, be provided with an additional fi-condition for backward computation. Unfortunately, deriving correct and consistent fi-conditions is often not obvious. Moreover, HDL descriptions exist which may not be realized with a reversible control flow at all. In this work, we propose automatic solutions which generate the required fi-conditions and check whether a reversible control flow indeed can be realized. The solution utilizes predicate transformer semantics based on Hoare logic. This has exemplary been implemented for the reversible HDL SyReC and evaluated with a variety of circuit description examples. The proposed solution constitutes the first automatic method for these important designs steps in the domain of reversible circuit design.

Z. Al-Wardi, R. Wille, and R. Drechsler: Extensions to the reversible hardware description language SyReC. In: *ISMVL* **47**, 2017, 185-190.

Hardware Description Languages (HDL) are proposed to facilitate the design of complex circuits and to allow for scalable synthesis. While rather established for conventional circuits, HDLs for the design and synthesis of reversible circuits are at the beginning. SyReC is a representative of such an HDL which already has successfully be applied to realize complex functionality in reversible logic. Nevertheless, the grammar and, by this, the functional scope of this language is rather limited. In this work, we propose extensions to the SyReC HDL which will enhance the usability of the language. For each extension, we additionally provide corresponding synthesis schemes. Overall, this yields a new (extended) SyReC HDL, which will simplify the design and realization of corresponding circuits.

Z. Al-Wardi, R. Wille, and R. Drechsler: Towards VHDL-based design of reversible circuits, in: *RC* **9**, 2017.

Hardware Description Languages (HDL) facilitate the design of complex circuits and allow for scalable synthesis. While rather established for conventional circuits, HDLs for reversible circuits are in their infancy and usually require a deep understanding of the reversible computing concepts. This motivates the question whether reversible circuits can also efficiently be designed with conventional HDLs, such as VHDL. This work discusses this question. By this, it provides the basis towards a design ow that requires no or only little knowledge of the reversible computation paradigm which could ease the acceptance of this non-conventional computation paradigm amongst designers and stakeholders.

Z. Al-Wardi, R. Wille, and R. Drechsler: Synthesis of reversible circuits using conventional hardware description languages. in: *ISMVL* **48**, 2018.

Hardware Description Languages (HDL) facilitate the design of complex circuits and allow for scalable synthesis. While rather established for conventional circuits, HDL-based design of reversible circuits is in its infancy. This motivates the question whether conventional HDLs can also be efficiently used for the design of reversible circuits. This work investigates this question and provides a basis towards a design flow that requires only little knowledge of reversible computation. This eases the acceptance of this non-conventional paradigm amongst designers and stakeholders.

Applications

M. Bryk, K. Gracki, P. Kerntopf, M. Pawłowski, and A. Skorupski: Encryption using reconfigurable reversible logic gate and its simulation in FPGAs, in: *MIXDES* **23**, 2016, 203-206.

This paper presents a solution to designing encryption schemes based entirely on reversible logic. In our solution a building block of an encryption scheme is a cascade of 4-input reversible gates which can perform any reversible 4-variable function. For this purpose a reconfigurable reversible gate has been proposed. The design of such a reconfigurable gate built from standard reversible gates, i.e. NOT, CNOT, Toffoli and Fredkin gates, is presented.

A. De Vos and S.De Baerdemacker: Block-ZXZ synthesis of an arbitrary quantum circuit. in: *Physical Review A*, 2016.

At the Universiteit Gent (Belgium), in 2016, De Vos and De Baerdemacker [1] studied the unification of quantum circuit design and classical reversible circuit design. Thanks to the 2015 Führ and Rzeszotnik decomposition of an arbitrary unitary matrix, they succeeded in finding two (dual) synthesis methods for quantum circuits. One of them turns out to have the synthesis of classical circuits as a special case. This leads to a unification of quantum and classical computing.

M. Lukac, M. Kameyama, M. Perkowski, P. Kerntopf, and C. Moraga: Fault models in reversible and quantum circuits, in: *Advances in Unconventional Computing*, A. Adamatzky (Ed.), Springer, 2016.

In this chapter we describe faults that can occur in reversible circuit as compared to faults that can occur in classical irreversible circuits. Because there are many approaches from classical irreversible

circuits that are being adapted to reversible circuits, it is necessary to analyze what faults that exists in irreversible circuits can appear in reversible circuit as well. Thus we focus on comparing faults that can appear in classical circuit technology with faults that can appear in reversible and quantum circuit technology. The comparison is done from the point of view of information reversible and information irreversible circuit technologies. We show that the impact of reversible computing and quantum technology strongly modifies the fault types that can appear and thus the fault models that should be considered. Unlike in the classical non-reversible transistor based circuits, in reversible circuits it is necessary to specify what type of implementation technology is used as different technologies can be affected by different faults. Moreover, the level of faults and their analysis must be revised to precisely capture the effects and properties of quantum gates and quantum circuits that share several similarities with reversible circuits. By not doing so the available testing approaches adapted from classical circuits would not be able to properly detect relevant faults. In addition, if the classical faults are directly applied without revision and modifications, the presented testing procedure would be testing for such faults that cannot physically occur in the given implementation of reversible circuits. The observation and analysis of these various faults presented in this chapter clearly demonstrates what faults can occur and what faults cannot occur in various reversible technologies. Consequently the results from this chapter can be used to design more precise tests for reversible logic circuits. Moreover the clearly described differences between faults occurring in reversible and irreversible circuits means that new algorithms for fault detection should be implemented specifically for particular reversible technologies.

C. Moraga: Aspects of reversible and quantum computing in a p-valued domain. in: *IEEE JETCAS* **6**, 2016, 44-52.

This work presents basic aspects of non-binary reversible and quantum computing in a p-valued environment, since there are no physical reasons for quantum computing to be necessarily binary. A “quantum technology” is not yet available, but different alternatives at the level of laboratory experiments are promising. A theoretical background is needed to face the challenge of designing circuits for quantum computing. Pauli matrices are introduced in the p-valued domain and their properties are explained. The Vilenkin-Chrestenson matrix is shown to produce superposition of states. Entanglement of quantum states in the p-valued environment is introduced and its measurement effect is illustrated. It is shown that in the p-valued domain, the binary Toffoli gate may be given different generalizations with different functionalities. An ancillary-free realization of a new generalized p-valued Toffoli gate based on Muthukrishnan-Stroud elementary gates is presented, its functionality is extended to two kinds of control, and a proof of its performance is given.

A. Paler, A. G. Fowler, and R. Wille: Online scheduled execution of quantum circuits protected by surface codes. *Quantum Information & Computation (QIC)*, 2017.

Quantum circuits are the preferred formalism for expressing quantum information processing tasks. Quantum circuit design automation methods mostly use a waterfall approach and consider that high level circuit descriptions are hardware agnostic. This assumption has lead to a static circuit perspective: the number of quantum bits and quantum gates is determined before circuit execution and everything is considered reliable with zero probability of failure. Many different schemes for achieving reliable fault-tolerant quantum computation exist, with different schemes suitable for different architectures. A number of large experimental groups are developing architectures well

suited to being protected by surface quantum error correcting codes. Such circuits could include unreliable logical elements, such as state distillation, whose failure can be determined only after their actual execution. Therefore, practical logical circuits, as envisaged by many groups, are likely to have a dynamic structure. This requires an online scheduling of their execution: one knows for sure what needs to be executed only after previous elements have finished executing. This work shows that scheduling shares similarities with place and route methods. The work also introduces the first online schedulers of quantum circuits protected by surface codes. The work also highlights scheduling efficiency by comparing the new methods with state of the art static scheduling of surface code protected fault-tolerant circuits.

A. Paler, A. G. Fowler, and R. Wille: Synthesis of arbitrary quantum circuits to topological assembly: systematic, online and compact. *Scientific Reports*, **7**(1), 2017.

It is challenging to transform an arbitrary quantum circuit into a form protected by surface code quantum error correcting codes (a variant of topological quantum error correction), especially if the goal is to minimize overhead. One of the issues is the efficient placement of magic state distillation sub circuits, so-called distillation boxes, in the space-time volume that abstracts the computation's required resources. This work presents a general, systematic, online method for the synthesis of such circuits. Distillation box placement is controlled by so-called schedulers. The work introduces a greedy scheduler generating compact box placements. The implemented software, whose source code is available online, is used to illustrate and discuss synthesis examples. Synthesis and optimisation improvements are proposed.

S. M. Saeed, N. Mahendran, A. Zulehner, R. Wille, and R. Karri: Identifying synthesis approaches for IP piracy of reversible circuits. in: *International Conference on Computer Design (ICCD)*, 2017.

Reversible circuits are vulnerable to intellectual property and integrated circuit piracy. To show these vulnerabilities, a detailed understanding on how to identify the function embedded in a reversible circuit is crucial. To obtain the embedded function, one needs to know the synthesis approach used to generate the reversible circuit in the first place. We present a machine learning based scheme to identify the synthesis approach using telltale signs in the design.

A. Zulehner, S. Gasser, and R. Wille: Exact global reordering for nearest neighbor quantum circuits using A*. in: *RC* **9**, 2017.

Since for certain realizations of quantum circuits only adjacent qubits may interact, qubits have to be frequently swapped - leading to a significant overhead. Therefore, optimizations such as exact global reordering have been proposed, where qubits are reordered such that the overall number of swaps is minimal. However, to guarantee minimality all n! possible permutations of qubits have to be considered in the worst case { which becomes intractable for larger circuits. In this work, we tackle the complexity of exact global reordering using an A* search algorithm. The sophisticated heuristics for the search algorithm proposed in this paper allow for solving the problem in a much more scalable fashion. In fact, experimental evaluations show that the proposed approach is capable of determining the best order of the qubits for circuits with up to 25 qubits, whereas the recent state-of-the-art already reaches its limits with circuits composed of 10 qubits.

A. Zulehner and R. Wille: Taking one-to-one mappings for granted: Advanced logic design of encoder circuits. in: *DATE*, 2017.

Encoders play an important role in many areas such as memory addressing, data demultiplexing, or for interconnect solutions. However, design solutions for the automatic synthesis of corresponding circuits suffer from various drawbacks, e.g. they are often not scalable, do not exploit the full degree of freedom, or are applicable to realize certain codes only. All these problems are caused by the fact that existing design solutions have to explicitly guarantee a one-to-one mapping. In this work, we propose an alternative design approach which relies on dedicated description means for both, the specification of an encoder as well as its circuit. Based on that, synthesis can be conducted without the need to explicitly take care of guaranteeing one-to-one mappings. Experiments show that this indeed overcomes the drawbacks of current design solutions and leads to an improvement in the resulting number of gates by up to 92%.

W. Castryck, J. Demeyer, A. De Vos, O. Keszocze, M. Soeken: Translating between the roots of identity in quantum circuits. in: *ISMVL* **48**, 2018.

The Clifford+T quantum computing gate library for single qubit gates can create all unitary matrices that are generated by the group <H, T>. The matrix T can be considered the fourth root of Pauli Z, since T_4 = Z or also the eighth root of the identity I. The Hadamard matrix H can be used to translate between the Pauli matrices, since $(HTH)_4$ gives Pauli X. We are generalizing both these roots of the Pauli matrices (or roots of the identity) and translation matrices to investigate the groups they generate: the so-called Pauli root groups. In this work we introduce a formalization of such groups, study finiteness and infiniteness properties, and precisely determine equality and subgroup relations.

X. Cui, S. M. Saeed, A. Zulehner, R. Wille, K. Wu, R. Drechsler, and R. Karri: On the difficulty of inserting Trojans in reversible computing architectures. *IEEE Transactions on Emerging Topics in Computing (TETC)*, 2018.

Fabrication-less design houses outsource their designs to third-party foundries to lower fabrication cost. However, this creates opportunities for a rogue in the semiconductor foundry to introduce hardware Trojans, which stay inactive most of the time and cause unintended consequences to the system when triggered. Hardware Trojans in traditional CMOS-based circuits have been studied, and Design-for-Trust (DFT) techniques have been proposed to detect them. Different from traditional circuits in many ways, reversible circuits implement one-to-one input/output mappings. We will investigate the security implications of reversible circuits with a particular focus on susceptibility to hardware Trojans. This work studies reversible functions implemented using reversible circuits as well as irreversible functions embedded in reversible circuits.

G. Meuli, M. Soeken, M. Roetteler, N. Wiebe, and G. De Micheli: A best-fit mapping algorithm to facilitate ESOP-decomposition in Clifford+T quantum network synthesis. in: *ASP-DAC* **23**, 2018, 664-669

Currently, there is a large research interest and a significant economical effort to build the first practical quantum computer. Such quantum computers promise to exceed the capabilities of conventional computers in fields such as computational chemistry, machine learning and cryptanalysis. Automated methods to map logic designs to quantum networks are crucial to fully realizing this dream, however, existing methods can be expensive both in computational time as well

as in the size of the resultant quantum networks. This work introduces an efficient method to map reversible single-target gates into a universal set of quantum gates (Clifford+T). This mapping method is called best-fit mapping and aims at reducing the cost of the resulting quantum network. It exploits fc-LUT mapping and the existence of clean ancilla qubits to decompose a large single-target gate into a set of smaller single-target gates. In addition, this work proposes a post-synthesis optimization method to reduce the cost of the final quantum network, based on two cost-minimization properties. Results show a cost reduction for the synthesized EPFL benchmark up to 53% in the number T gates.

M. Pawlowski and Z. Szymanski: Symmetric block encoder based on reversible circuits. in: R. S. Romaniuk, M. Linczuk (Eds.), *Proceedings of SPIE, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments* **41**, 10808, 2018, 7 pp.

The goal of the paper is a project of a novel symmetric block encoder. The basic processing elements are cascades of reconfigurable reversible gates changing the type of gates depending on the encryption key. The presented solution proposes the use of sixteen 8-bit cascades which configuration requires a 640-bit key. The input information is processed in 5 rounds. The encryption keys in the subsequent rounds differ. The design was modeled in VHDL language and placed in am FPGA chip. The project is scalable, i.e. depending on the needs, it can be modified by changing the number of gates in the cascade, the width of the information block being processed, which may result in an increase or decrease in the width of the encryption key. The number of rounds may also be modified. The large size of the encryption key should ensure the safety of the encrypted data.

M. Soeken, T. Haener, and M. Roetteler: Programming quantum computers using design automation. in: *DATE*, 2018, 137-146

Recent developments in quantum hardware indicate that systems featuring more than 50 physical qubits are within reach. At this scale, classical simulation will no longer be feasible and there is a possibility that such quantum devices may outperform even classical supercomputers at certain tasks. With the rapid growth of qubit numbers and coherence times comes the increasingly difficult challenge of quantum program compilation. This entails the translation of a high-level description of a quantum algorithm to hardware-specific low-level operations which can be carried out by the quantum device. Some parts of the calculation may still be performed manually due to the lack of efficient methods. This, in turn, may lead to a design gap, which will prevent the programming of a quantum computer. In this paper, we discuss the challenges in fully-automatic quantum compilation. We motivate directions for future research to tackle these challenges. Yet, with the algorithms and approaches that exist today, we demonstrate how to automatically perform the quantum programming flow from algorithm to a physical quantum computer for a simple algorithmic benchmark, namely the hidden shift problem. We present and use two tool flows which invoke RevKit. One which is based on ProjectQ and which targets the IBM Quantum Experience or a local simulator, and one which is based on Microsoft's quantum programming language Q#.

A. Skorupski, K. Gracki: Novel algorithm for symmetric encryption. in: R. S. Romaniuk, M. Linczuk (Eds.), *Proceedings of SPIE, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments* **41**, 10808, 2018, 7 pp.

The paper presents a new algorithm for block cipher with symmetric encryption and decryption algorithm. The main features of this idea are the large size of the key and high processing speed. This algorithm is based on reversible logic. The physical implementation of reversible gates will be done in the future. These gates can be modeled using FPGA structures. Contemporary FPGA chips contains very large numbers of elements and this feature allows implementation of complex reversible

circuits. These circuits consist of long gates cascades and in one chip it is possible to embed many of them. Usually the encryption algorithms are implemented as programs using a processor with proper software. The algorithm presented in this paper allows to build a cipher with one FPGA chip.

A. Bhattacharjee, C. Bandyopadhyay, R. Wille, R. Drechsler, and H. Rahaman: A novel approach for nearest neighbor realization of 2d quantum circuits. in: *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2018, 305-310.

Since decades, quantum computing has received tremendous attention among the researchers due to its dominance over classical computing. But simultaneously it has faced some design challenges and implementation constraints in this long run. One such constraint to build quantum circuits is to satisfy the so-called Nearest Neighbor (NN) property in the implemented circuits. Using SWAP gates, this constraint can be satisfied. But this leads to another design issue, namely how to determine such NN designs with a minimum use of SWAP gates. In way to further explore this area, in this work, we propose a heuristic approach for efficient NN complaint representation of quantum circuits in 2D space. The developed technique is segmented in three stages – qubit selection, qubit placement and SWAP gate insertion. The stated approach has been tested over a wide spectrum of benchmarks and reductions in cost parameters are observed. Improvement of more than 17%, 3% over 2D designs and 35%, 22% over 1D designs on SWAP count and quantum cost can be reported, respectively.

T. Haener, M. Soeken, M. Roetteler, K.M. Svore: Quantum circuits for floating-point arithmetic. in: *RC* **10** 2018, 162-174

Quantum algorithms to solve practical problems in quantum chemistry, materials science, and matrix inversion often involve a significant amount of arithmetic operations which act on a superposition of inputs. These have to be compiled to a set of fault-tolerant low-level operations and throughout this translation process, the compiler aims to come close to the Pareto-optimal front between the number of required qubits and the depth of the resulting circuit. In this paper, we provide quantum circuits for floating-point addition and multiplication which we find using two vastly different approaches. The first approach is to automatically generate circuits from classical Verilog implementations using synthesis tools and the second is to generate and optimize these circuits by hand. We compare our two approaches and provide evidence that floating-point arithmetic is a viable candidate for use in quantum computing, at least for typical scientific applications, where addition operations usually do not dominate the computation. All our circuits were constructed and tested using the software tools LIQU i|i and RevKit.

S.M. Saeed, N. Mohendran, A. Zulehner, R. Wille, and R. Karri: Identification of synthesis approaches for IP/IC piracy of reversible circuits. *Journal on Emerging Technologies in Computing Systems*, 2018.

Reversible circuits employ a computational paradigm that is beneficial for several applications includingthe design of encoding and decoding devices, low-power design, and emerging applications inquantumcomputation. However, similar to conventional logic, reversible circuits are expected to be subject to Intellectual Property/Integrated Circuit piracy. To counteract such attacks, an understanding of how to identify the targetfunction from a reversible circuit is a crucial first step. In contrast to conventional logic, the target functionis (implicitly or explicitly) embedded into the reversible circuit. Numerous synthesis approaches have beenproposed for this embedding task. To recover the target function embedded in a reversible circuit, one needsto know what synthesis approach has been used to embed the circuit.We propose a machine learning-based scheme to determine the used reversible synthesis approach basedon the telltale signs it leaves in the synthesized reversible circuit. We study the impact of optimizing thesynthesis approaches on the

telltale signs that they leave. Our analysis shows that the synthesis approachescan be determined in the vast majority of cases even if optimized versions of the synthesis approaches areused.

S.M. Saeed, M. Samah, X, Cui, A. Zulehner, R. Wille, R. Drechsler, K. Wu, and R. Karri: IC/IP piracy assessment of reversible logic. in: *ICCAD*, 2018.

Reversible logic is a building block for adiabatic and quantum computing in addition to other applications. Since common functions are non-reversible, one needs to embed them into proper-size reversible functions by adding ancillary inputs and garbage outputs. We explore the Intellectual Property (IP) piracy of reversible circuits. The number of embeddings of regular functions in a reversible function and the percent of leaked ancillary inputs measure the difficulty of recovering the embedded function. To illustrate the key concepts, we study reversible logic circuits designed using reversible logic synthesis tools based on Binary Decision Diagrams and Quantum Multi-valued Decision Diagrams.

A. Zulehner, A. Paler, and R. Wille: Efficient mapping of quantum circuits to the IBM QX architecture. in: *DATE*, 2018.

In March 2017, IBM launched the project IBM Q with the goal to provide access to quantum computers for a broad audience. This allowed users to conduct quantum experiments on a 5-qubit and, since June 2017, also on a 16-qubit quantum computer (called IBM QX2 and IBM QX3, respectively). In order to use these, the desired quantum functionality (e.g. provided in terms of a quantum circuit) has to properly be mapped so that the underlying physical constraints are satisfied – a complex task. This demands for solutions to automatically and efficiently conduct this mapping process. In this paper, we propose such an approach which satisfies all constraints given by the architecture and, at the same time, aims to keep the overhead in terms of additionally required quantum gates minimal. The proposed approach is generic and can easily be configured for future architectures. Experimental evaluations show that the proposed approach clearly outperforms IBM’s own mapping solution with respect to runtime as well as resulting costs.

A. Zulehner, A. Paler, and R. Wille: An efficient methodology for mapping quantum circuits to the IBM QX architectures. *IEEE TCAD*, 2018.

In the past years, quantum computers more and more have evolved from an academic idea to an upcoming reality. IBM's project IBM Q can be seen as evidence of this progress. Launched in March 2017 with the goal to provide access toquantum computers for a broad audience, this allowed users to conduct quantum experiments on a 5-qubit and, since June 2017, also on a 16-qubit quantum computer (called IBM QX2 and IBM QX3, respectively). Revised versions of these 5-qubit and 16-qubit quantum computers (named IBM QX4 and IBM QX5, respectively) are available since September 2017. In order to use these, the desired quantum functionality (e.g. provided in terms of a quantum circuit) has to be properly mapped so that the underlying physical constraints are satisfied - a complex task. This demands solutions to automatically and efficiently conduct this mapping process. In this paper, we propose a methodology which addresses this problem, i.e. maps the given quantum functionality to arealization which satisfies all constraints given by the architecture and, at the same time, keeps the overhead in terms of additionally required quantum gates minimal. The proposed methodology is generic, can easily be configured for similar future architectures, and is fully integrated into IBM's SDK. Experimental evaluations show that the proposed approach clearly outperforms IBM'sown mapping solution. In fact, for many quantum circuits, the proposed approach determines a mapping to the IBM architecture within minutes, while IBM's solution suffers from

long runtimes and runs into a timeout of 1 hour in several cases. As an additional benefit, the proposed approach yields mapped circuits with smaller costs (i.e. fewer additional gates are required). All implementations of the proposed methodology is publicly available at http://iic.jku.at/eda/research/ibm_qx_mapping.

A. Zulehner and R. Wille: Advanced simulation of quantum computations. *IEEE TCAD*, 2018.

Quantum computation is a promising emerging technology which, compared to conventional computation, allows for substantial speed-ups e.g. for integer factorization or database search. However, since physical realizations of quantum computers are in their infancy, a significant amount of research in this domain still relies on simulations of quantum computations on conventional machines. This causes a significant complexity which current state-of-the-art simulators try to tackle with a rather straight forward array-based representation and by applying massive hardware power. There also exist solutions based on decision diagrams (i.e. graph-based approaches) that try to tackle the exponential complexity by exploiting redundancies in quantum states and operations. However, these existing approaches do not fully exploit redundancies that are actually present. In this work, we revisit the basics of quantum computation, investigate how corresponding quantum states and quantum operations can be represented even more compactly, and, eventually, simulated in a more efficient fashion. This leads to a new graph-based simulation approach which outperforms state-of-the-art simulators (array-based as well as graph-based). Experimental evaluations show that the proposed solution is capable of simulating quantum computations for more qubits than before, and in significantly less run-time (several magnitudes faster compared to previously proposed simulators). An implementation of the proposed simulator is publicly available online at http://www.jku.at/iic/eda/quantum_simulation.

A. Bhattacharjee, C. Bandyopadhyay, R. Wille, R. Drechsler, and H. Rahaman: Improved look-ahead approaches for nearest neighbor synthesis of 1D quantum circuits. in: *International Conference on VLSI Design (VLSI Design)*, 2019.

In the present era of computation, quantum computing may offer a new direction as it allows to solve certain problems significantly faster than classical solutions. But it also has been found that there are several constrains in performing a successful realization of quantum circuits. One such constraint is the nearest neighbor (NN) criterion which states that qubits which interact with each other have to be adjacent. Motivated by this objective, in this work we propose a linear qubit placement technique that effectively rearranges the qubits and transforms quantum circuits to improved NN-based designs by inserting SWAPs. Furthermore, for placing these SWAPs in appropriate positions, we implemented a look-ahead strategy that considers the effect of the rest of the gates and computes a corresponding impact value which guides the insertion of the SWAP gates. To this extent, we consider three different strategies to evaluate the corresponding “look-ahead effects” and their influence on existing gates. At the end of this work, we have evaluated the developed methodology over a wide range of benchmarks and compared the results with existing related works. In this comparison, we have seen that the proposed technique outperforms the related works and provides substantial reductions in SWAP overhead.

M. Soeken, F. Mozafari, B. Schmitt, G. De Micheli: Compiling permutations for superconducting QPUs. In: *DATE*, 2019, 6 pp.

In this paper the compilation of quantum state permutations into quantum gates for physical quantum computers is considered. A sequence of generic single-target gates, which realize the input

permutation, are extracted using a decomposition based reversible logic synthesis algorithm. We present a compilation algorithm that translates single-target gates into a quantum circuit composed of the elementary quantum gate sets that are supported by IBM's 5-qubit and 16-qubit, and Rigetti's 8-qubit and 19-qubit superconducting transmon QPUs. Compared to generic state-of-the-art compilation techniques, our technique improves gate volume and gate depth by up to 59% and 53%, respectively.

A. Zulehner, H. Bauer, and R. Wille: Evaluating the flexibility of A* for mapping quantum circuits. in: *RC* **11**, 2019.

Mapping quantum circuits to real quantum architectures (while keeping the respectively considered cost as small as possible) has become an important research task since it is required to execute algorithms on real devices. Since the underlying problem is NP-complete, several heuristic approaches have been proposed. Recently, approaches utilizing A* search to map quantum circuits to, e.g., Nearest Neighbor architectures or IBM QX architectures have gained substantial interest. However, their performance usually has only been evaluated in a rather narrow context, i.e., for single architectures and objectives only. In this work, we evaluate the flexibility of A* in the context of mapping quantum circuits to physical devices. To this end, we review the underlying concepts and show its flexibility with respect to the considered architecture. Furthermore, we demonstrate how easy such solutions can be adjusted towards optimizing different design objectives or cost metrics by providing a generalized and parameterizable cost function for the A* search that can also be easily extended to support future cost metrics.

R. Wille, L. Burgholzer, and A. Zulehner: Mapping quantum circuits to IBM QX architectures using the minimal number of SWAP and H operations. in: *DAC* **56**, 2019.

The recent progress in the physical realization of quantum computers (the first publicly available ones - IBM's QX architectures - have been launched in 2017) has motivated research on automatic methods that aid users in running quantum circuits on them. Here, certain physical constraints given by the architectures which restrict the allowed interactions of the involved qubits have to be satisfied. Thus far, this has been addressed by inserting SWAP and H operations. However, it remains unknown whether existing methods add a minimum number of SWAP and H operations or, if not, how far they are away from that minimum—an NP-complete problem. In this work, we address this ization problem that is solved using reasoning engines like Boolean satisfiability solvers. By this, we do not only provide a method that maps quantum circuits to IBM's QX architectures with a minimal number of SWAP and H operations, but also show by experimental evaluation that the number of operations added by IBM's heuristic solution exceeds the lower bound by more than 100% on average. An implementation of the proposed methodology is publicly available at http://iic.jku.at/eda/research/ibm_qx_mapping.

A. Zulehner, and R. Wille: Compiling SU(4) quantum circuits to IBM QX architectures. in: *ASP-DAC* **24**, 2019, 185-190.

The Noisy Intermediate-Scale Quantum (NISQ) technology is currently investigated by major players in the field to build the first practically useful quantum computer. IBM QX architectures are the first ones which are already publicly available today. However, in order to use them, the respective quantum circuits have to be compiled for the respectively used target architecture. While first approaches have been proposed for this purpose, they are infeasible for a certain set of SU(4) quantum circuits which have recently been introduced to benchmark corresponding compilers. In this work, we analyze the bottlenecks of existing compilers and provide a dedicated method for compiling this kind of circuits to IBM QX architectures. Our experimental evaluation (using tools provided by IBM) shows that the proposed approach significantly outperforms IBM's own solution

regarding fidelity of the compiled circuit as well as runtime. Moreover, the solution proposed in this work has been declared winner of the IBM QISKit Developer Challenge. An implementation of the proposed methodology is publicly available at http://iic.jku.at/eda/research/ibm_qx_mapping.

A. Paler, A. G. Fowler, and R. Wille: Faster manipulation of large quantum circuits using wire label reference diagrams. *Microprocessors and Microsystems* **66**, 2019, 55-66.

Large scale quantum computing is highly anticipated, and quantum circuit design automation needs to keep up with the transition from small scale to large scale problems. Methods to support fast quantum circuit manipulations (e.g. gate replacement, wire reordering, etc.) or specific circuit analysis operations have not been considered important and have been often implemented in a naive manner thus far. For example, quantum circuits are usually represented in term of one-dimensional gate lists or as directed acyclic graphs. Although implementations for quantum circuit manipulations are often only of polynomial complexity, the sheer number of possibilities to consider with increasing scales of quantum computations make these representations highly inefficient – constituting a serious bottleneck. At the same time, quantum circuits have structural characteristics, which allow for more specific and faster approaches. This work utilises these characteristics by introducing a dedicated representation for large quantum circuits, namely wire label reference diagrams. We apply the representation to a set of very common circuit transformations, and develop corresponding solutions which achieve orders of magnitude performance improvements for circuits which include up to 80 000 qubits and 200 000 gates. The implementation of the proposed method is available online.

A. Zulehner, M.P. Frank, and R. Wille: Design automation for adiabatic circuits. in: *ASP-DAC* **24**, 2019, 669—674.

Adiabatic circuits are heavily investigated since they allow for computations with an asymptotically close to zero energy dissipation per operation—serving as an alternative technology for many scenarios where energy efficiency is preferred over fast execution. Their concepts are motivated by the fact that the information lost from conventional circuits results in an entropy increase which causes energy dissipation. To overcome this issue, computations are performed in a (conditionally) reversible fashion which, additionally, have to satisfy switching rules that are different from conventional circuitry—crying out for dedicated design automation solutions. While previous approaches either focus on their electrical realization (resulting in small, hand-crafted circuits only) or on designing fully reversible building blocks (an unnecessary overhead), this work aims for providing an automatic and dedicated design scheme that explicitly takes the recent findings in this domain into account. To this end, we review the theoretical and technical background of adiabatic circuits and present automated methods that dedicatedly realize the desired function as an adiabatic circuit. The resulting methods are further optimized - leading to an automatic and efficient design automation for this promising technology. Evaluations confirm the benefits and applicability of the proposed solution.

A. Zulehner, and R. Wille: Matrix-Vector vs. Matrix-Matrix multiplication: Potential in DD-based simulation of quantum computations. in: *DATE*, 2019.

The simulation of quantum computations basically boils down to the multiplication of vectors (describing the respective quantum state) and matrices (describing the respective quantum operations). However, since those matrices/vectors are exponential in size, most of the existing solutions (relying on arrays for their representation) are either limited to rather small quantum systems or require substantial hardware resources. To overcome these shortcomings, solutions based on decision diagrams (DD-based simulation) have been proposed recently. They exploit redundancies in quantum states as well as matrices and, by this, allow for a compact representation

and manipulation. This offers further (unexpected) potential. In fact, simulation has been conducted thus far by applying one operation (i.e. one matrix-vector multiplication) after another. Besides that, there is the possibility to combine several operations (requiring a matrix-matrix multiplication) before applying them to a vector. But since, from a theoretical perspective, matrix-vector multiplication is significantly cheaper than matrix-matrix multiplication, the potential of this direction was rather limited thus far. In this work, we show that this changes when decision diagrams are employed. In fact, their more compact representation frequently makes matrix-matrix multiplication more beneficial - leading to substantial improvements by exploiting the combination of operations. Experimental results confirm the proposed strategies for combining operations lead to speed-ups of several factors or - when additionally exploiting further knowledge about the considered instance— even of several orders of magnitudes.