Integrate Automatic Quantum Oracle Synthesis Into QDK for Resource Estimation

Microsoft

Chaman Gupta*,a, I-Tung Chen*,b, Sara Mouradianb, Mariia Mykhailovac, Mathias Soekend

*These authors contribute equally

Why do we care about Quantum?

Quantum computing is promising in reducing the computation time on certain tasks: e.g., factoring prime numbers (cryptography applications), searching in unstructured data (database), simulating quantum systems (medicine development, new material discovery), or even quantum machine learning (Quantum AI).

Challenges of Quantum Computing:

Several applications need a black-box function or a *"Quantum Oracle"*. The realization of a quantum oracle needs to be **carefully hand-crafted for different situations**. Thus, implementation of a quantum oracle is often difficult and elusive. Further, the oracle needs to be reconfigured for a change in data size, even with the same task. This often hinders the scalability of quantum algorithms.

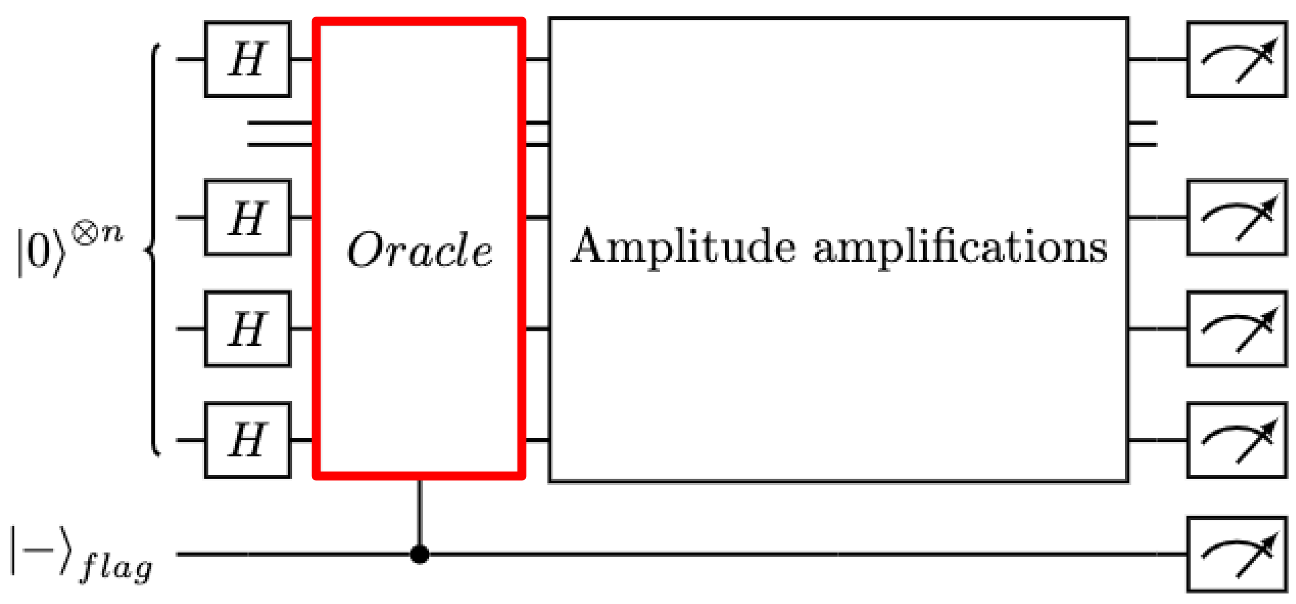
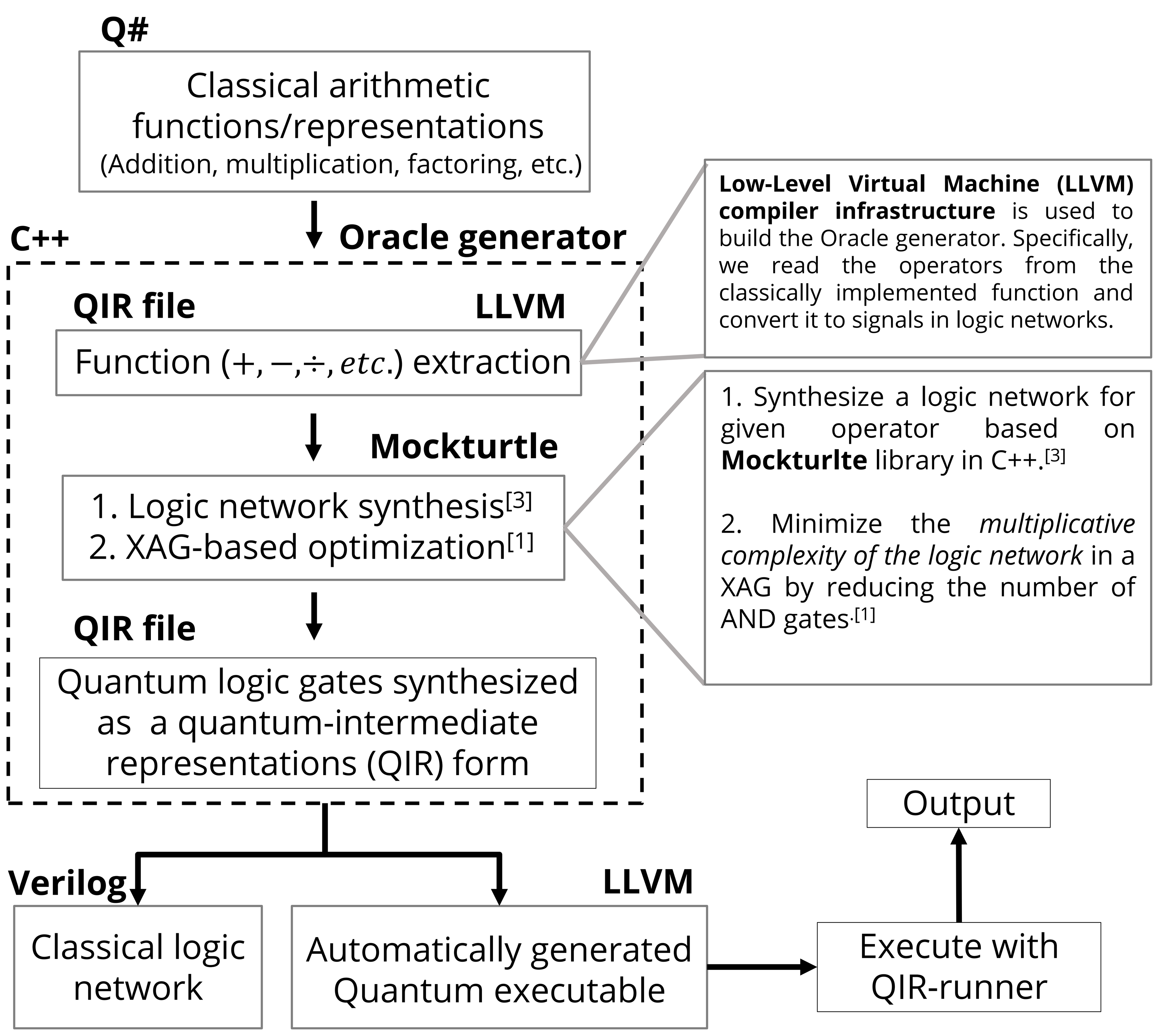


Fig.1 Example circuit of Grover's search algorithm.

Solution we propose:

Automatic oracle synthesis - Given a classical description of the function generate a quantum operation[2].

Technical background and workflow:



Results:

We successfully implemented functionalities for arithmetic functions: $+, -, \times, >, <$, etc. Further, we successfully integrate the automatic oracle generation with the Grover search algorithm.

Realization of classical arithmetic operators

Arithmetic functions	Types	N_{gates}	N_{qubit}
$A + B$	64-int	993 (CX)+126 (CCX)	319
$(A + Bx)$ mod 11	64-int	1360 (CX) + 188 (CCX)	445
$Majority(A, B, C)$	Bool	10(CX) + 2 (CCX)	6

Grover's Search Algorithm Visualization

Grover's algorithm solves a search problem by finding an input x_0 that satisfies the condition $f(x_0) = 1$, where $f(x)$ is a classical function mapping n-bit search space to $\{0, 1\}$.[4] It's quantum algorithm provides a quadratic speedup, requiring approximately $\sqrt{N}$ evaluations compared to the classical approach that requires N evaluations, where $N = 2^n$.

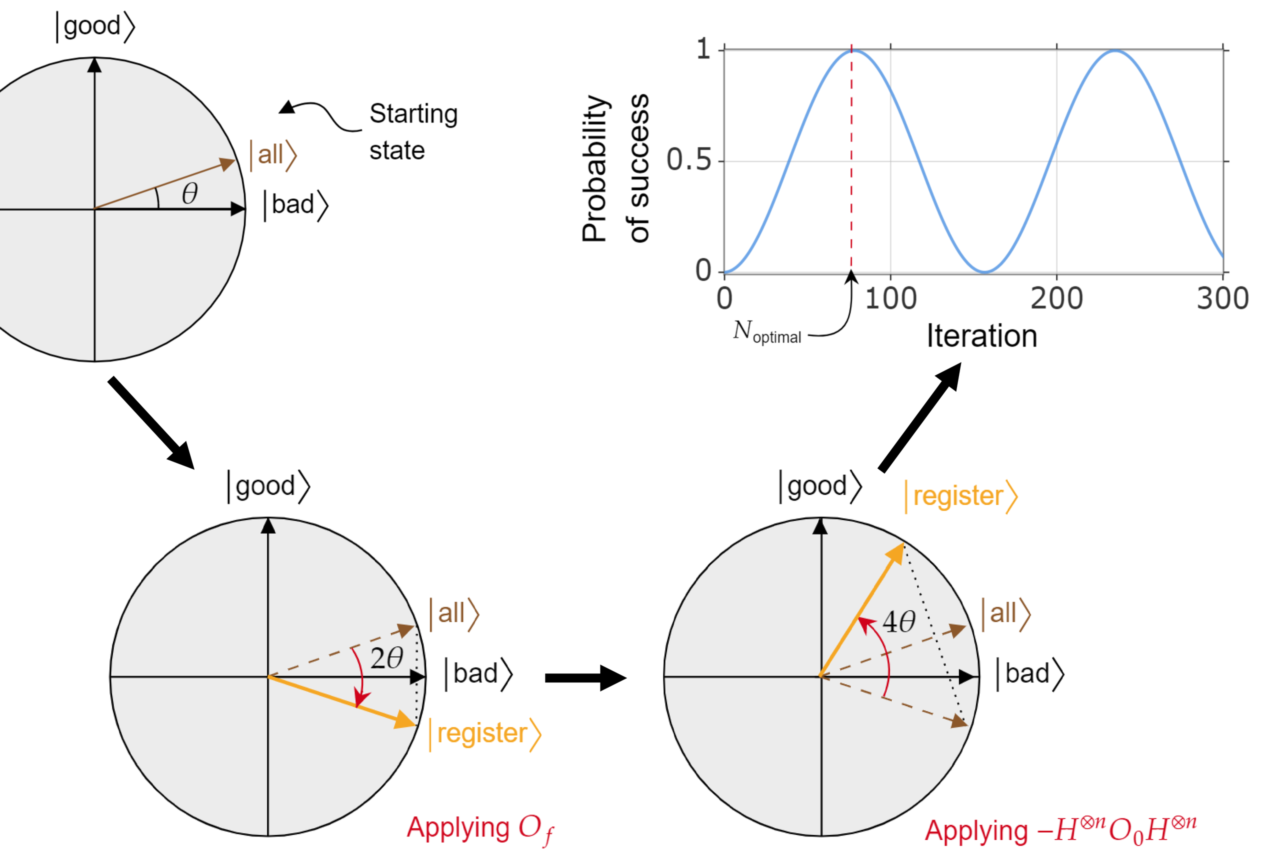


Fig. 2 Grover's search algorithm visualization[4].

Putting all together:

Case study: ISBN missing digit search using oracle generator

In the ISBN 10 system, each ISBN is a 10-digit sequence, and the last digit serves as the check. The full sequence $(x_0, x_1, \dots, x_9)$ should satisfy the following condition: $\left(\sum_{i=0}^{9}(10 - i)x_i\right) \bmod 11 = 0$

```
[i] initial XAG from LLVM: 132 AND gates, 137 XOR gates
[i] optimized XAG:         132 AND gates, 138 XOR gates
Step 8: Running the qir-runner
START
METADATA       EntryPoint
ISBN with missing digit: [0, 3, 0, 6, -1, 0, 6, 1, 5, 2]
Oracle validates: (9 + 6x) mod 11 = 0

Missing digit: 4
Full ISBN: [0, 3, 0, 6, 4, 0, 6, 1, 5, 2]
The missing digit was found in 1 attempt.
```

Fig. 3 QIR-runner output with automatic oracle for Grover's search.

Future Work

After the successful implementation of the Grover's search algorithm as shown above, we are exploring to implement other algorithms like QFT (Quantum Fourier Transform) and QSVD (Quantum Singular Value Decomposition) using the automatic oracle synthesis code we have developed.

ELECTRICAL & COMPUTER ENGINEERING
UNIVERSITY of WASHINGTON

Affiliations:

a) Department of Materials Science and Engineering, University of Washington, Seattle, WA
b) Department of Electrical and Computer Engineering, University of Washington, Seattle, WA, USA
c) Microsoft Quantum, Redmond, WA, USA
d) Microsoft Quantum, Zürich, Switzerland

References:

1. Meuli, G., Soeken, M. & De Micheli, G. *npj Quantum Inf* 8, 7 (2022).
2. M. Soeken and M. Mykhailova, Proceedings of the 59th ACM/IEEE Design Automation Conference, pp. 1363–1366, (2022).
3. M. Soeken, et al., arXiv preprint arXiv:1805.05121, 2018
4. Lopez, S. Theory of grover's search algorithm https://learn.microsoft.com/en-us/azure/quantum/concepts-grovers (2022)