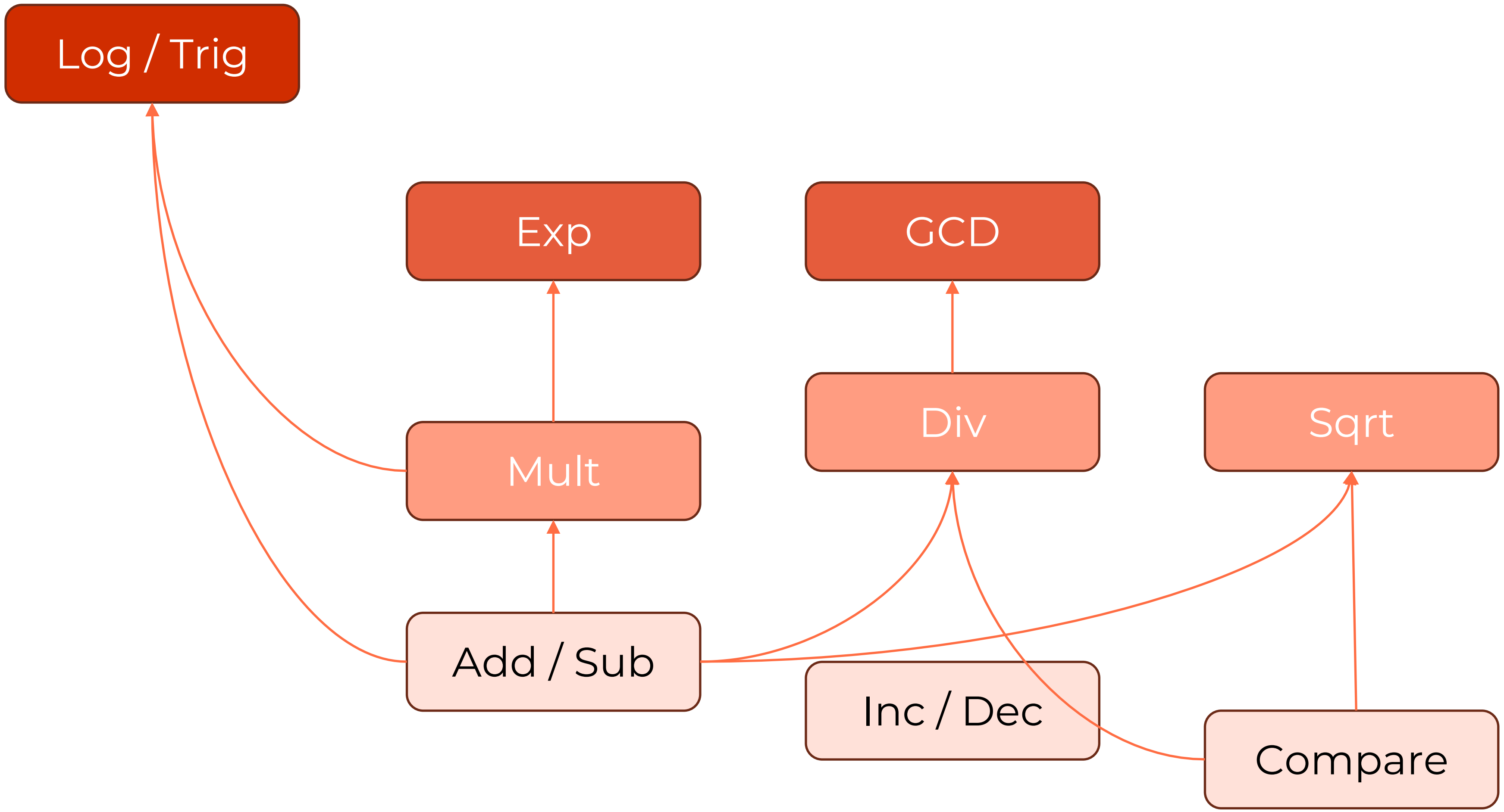
Optimizing T and CNOT gates in quantum ripple-carry adders

Maxime REMAUD

ReAQCT 2024

Relations between arithmetic operators



Why do we care ?

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1] and Martin Ekerå[2]

An Efficient Quantum Factoring Algorithm

Oded Regev*

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Block-encoding structured matrices for data input in quantum computing

Christoph Sünderhauf[1], Earl Campbell[1,2], and Joan Camps[1]

Improved quantum circuits for elliptic curve discrete logarithms

Thomas Häner[1], Samuel Jaques[2] *†, Michael Naehrig[3], Martin Roetteler[1], and Mathias Soeken[1]

Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3

Matthew Amy[1,4], Olivia Di Matteo[2,4], Vlad Gheorghiu[3,4], Michele Mosca[3,4,5,6], Alex Parent[2,4], and John Schanck[3,4]

Addition

$$a \in \mathbb{Z}_{2^n} \quad \longleftrightarrow \quad (a_{n-1}, \ldots, a_0) \in \{0,1\}^n \quad \left(a = \sum_{i=0}^{n-1} a_i 2^i \right)$$

$$b \in \mathbb{Z}_{2^n} \quad \longleftrightarrow \quad (b_{n-1}, \ldots, b_0) \in \{0,1\}^n \quad \left(b = \sum_{i=0}^{n-1} b_i 2^i \right)$$

$$a + b =: s \in \mathbb{Z}_{2^{n+1}} \quad \longleftrightarrow \quad (s_n, \ldots, s_0) \in \{0,1\}^{n+1} \quad \left(s = \sum_{i=0}^{n} s_i 2^i \right)$$

$$\begin{array}{cccccccl} & 1 & 0 & 0 & 1 & 1 & 0 & \longrightarrow \text{carries} \\ & & 1 & 0 & 0 & 0 & 1 & \longrightarrow a = 17 \\ + & & 1 & 1 & 0 & 1 & 1 & \longrightarrow b = 27 \\ \hline & 1 & 0 & 1 & 1 & 0 & 0 & \longrightarrow s = 44 \end{array}$$

$$c_i = \begin{cases} 0 & \text{if } i = 0 \\ a_{i-1}b_{i-1} \oplus b_{i-1}c_{i-1} \oplus c_{i-1}a_{i-1} & \text{for } i \in [\![1, n]\!] \end{cases}$$

$$s_i = \begin{cases} a_i \oplus b_i \oplus c_i & \text{for } i \in [\![0, n-1]\!] \\ c_n & \text{if } i = n. \end{cases}$$

We want an operator with the following action: $|a\rangle_n |b\rangle_n |z\rangle \mapsto |a\rangle_n |s\rangle_n |z \oplus s_n\rangle$

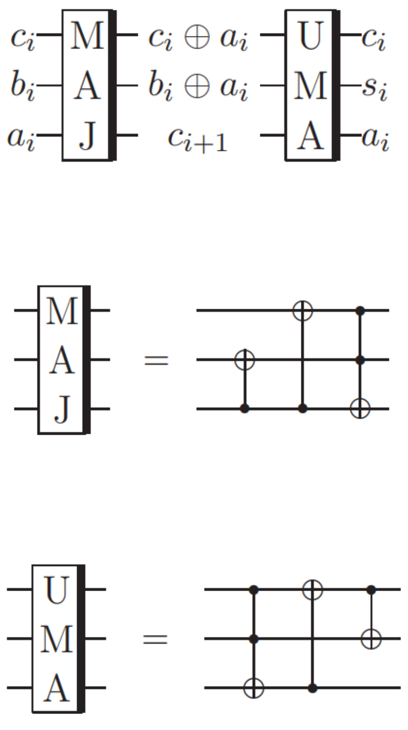
Complexity of quantum addition

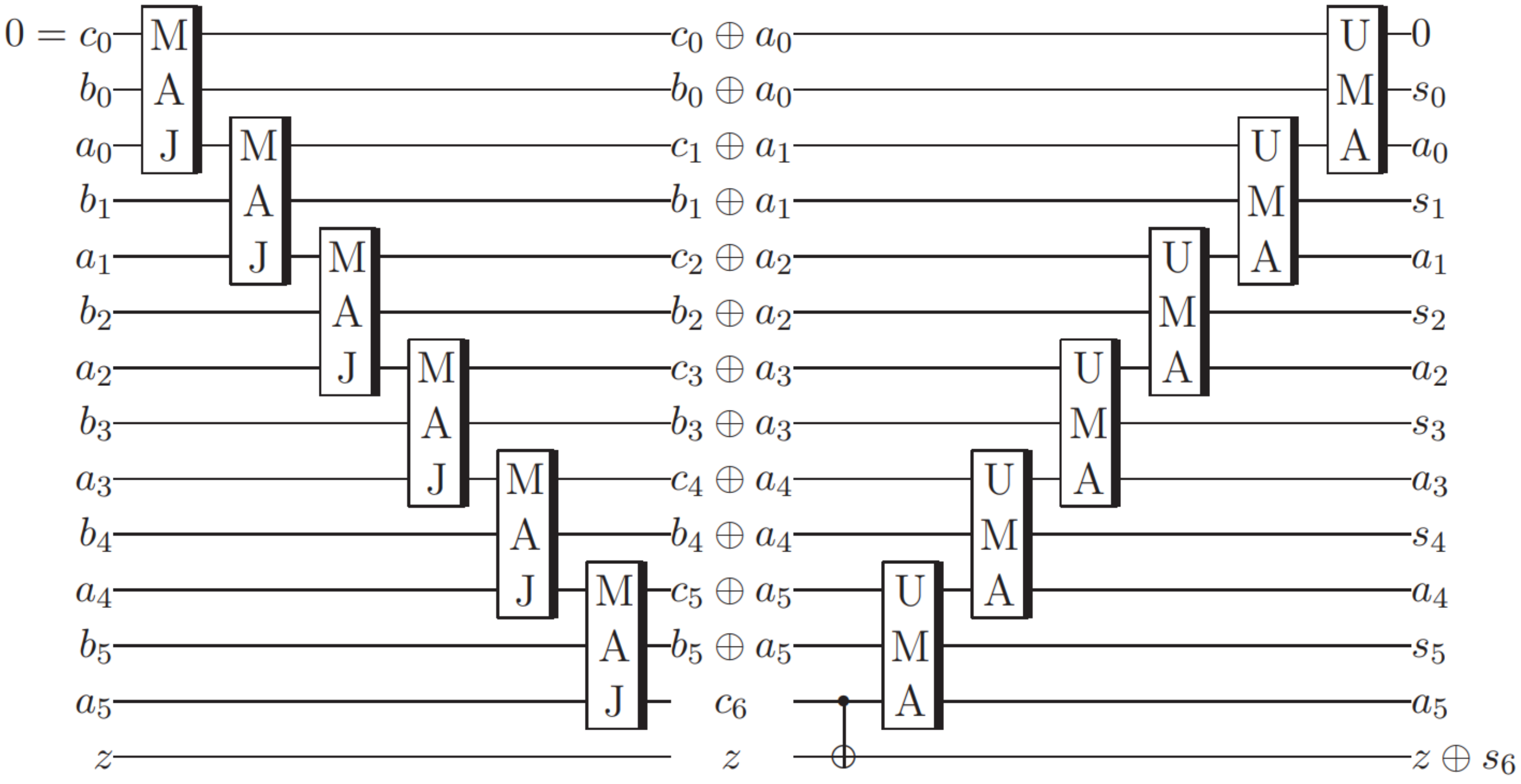
$$|a\rangle_n |b\rangle_n |z\rangle \mapsto |a\rangle_n |s\rangle_n |z \oplus s_n\rangle$$

	Method	Depth	Ancillae	Size
Class. Arith.	Ripple-Carry	$O(n)$	$O(1)$	$O(n)$
	Carry-Lookahead	$O(\log n)$	$O(n)$	$O(n)$
QFT Arith.	QFT-based	$O(\log n)$	0	$O(n^2)$

We consider only *garbage-free* ripple-carry adders (and comparators), using *at most 1 ancilla*, with *no phase approximation* and *no measurement.*

Ripple-carry technique (Cuccaro et al. adder (1))

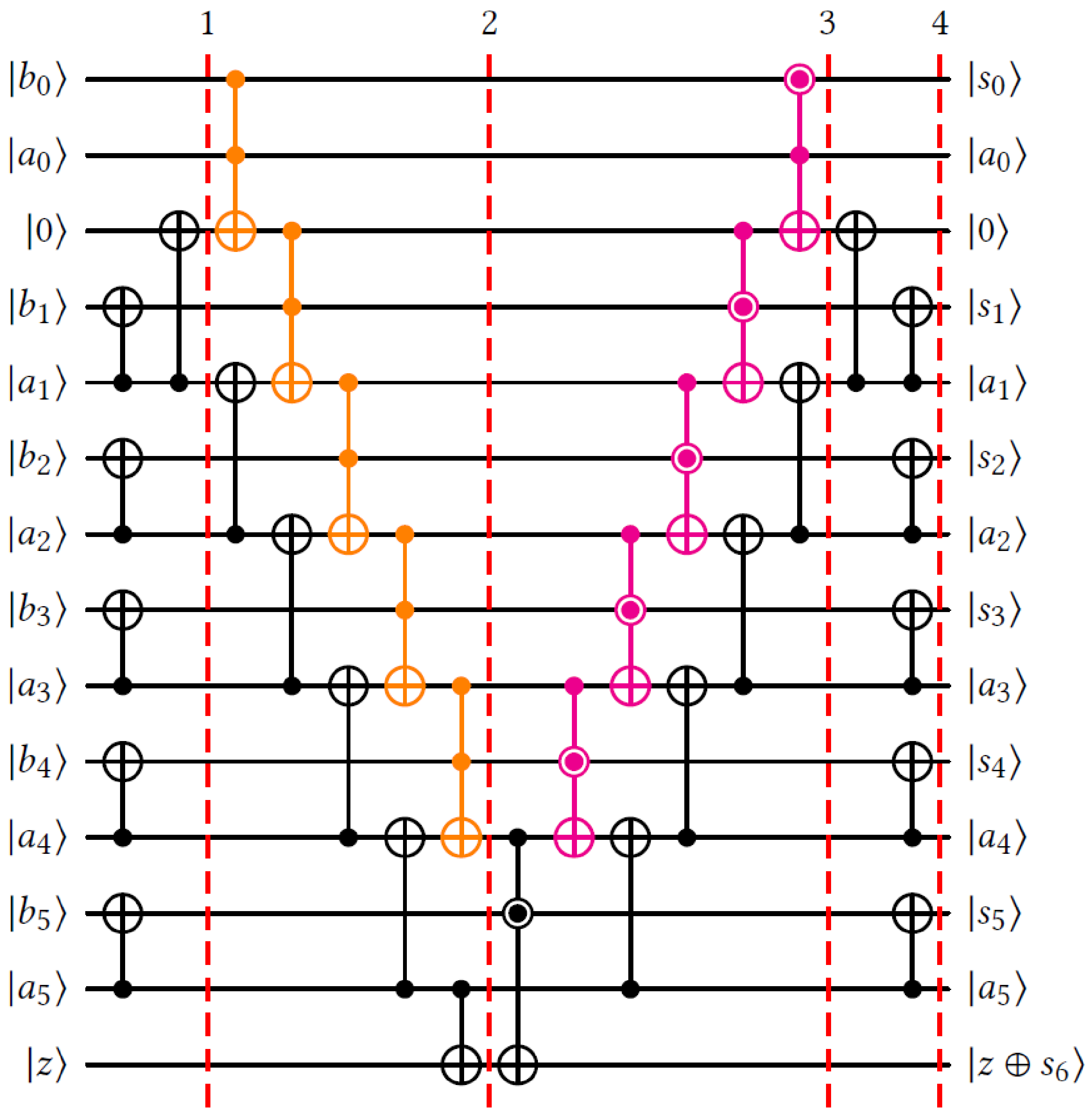




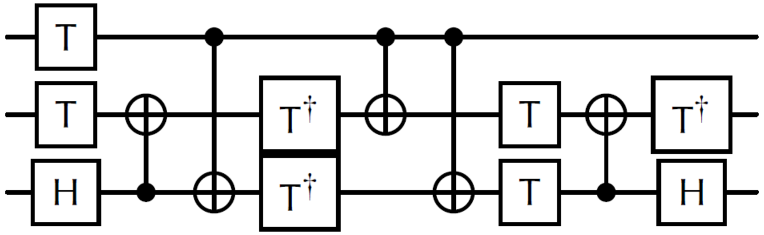
Cuccaro et al. adder (2)

Step	1	2	3	4
CNOT-count	n	$n-1$	$n-2$	n
CCNOT-count		$n-1$		
Peres-count			n	
CNOT-depth	2			2
CCNOT-depth		$n-1$		
Peres-depth			n	

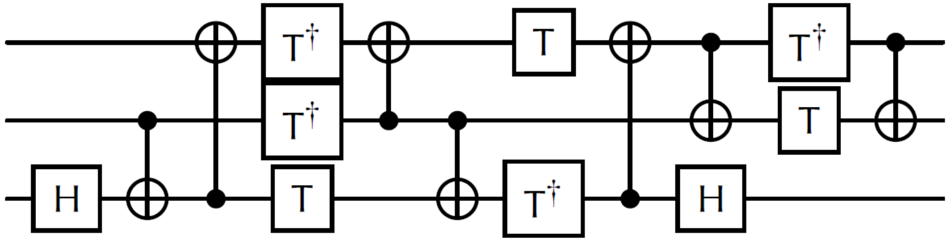
$$\text{CNOT-count} = 4n - 3$$
$$\text{CNOT-depth} = 4$$
$$\text{CCNOT} = n - 1$$
$$\text{Peres} = n$$



Clifford+T gate set



A decomposition of the Peres gate with 5 CNOT and a T-depth of 4.



A decomposition of the CCNOT with 7 CNOT and a T-depth of 3.

The complexity of Cuccaro et al. adder becomes:

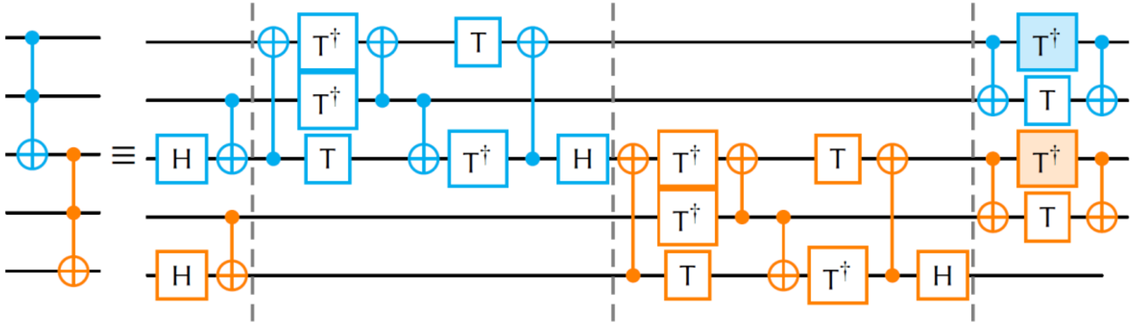
$$\begin{aligned}\mathsf{CNOT}\text{-count} &= 17n + O(1)\\ \mathsf{CNOT}\text{-depth} &= 13n + O(1)\\ \mathsf{T}\text{-count} &= 14n + O(1)\\ \mathsf{T}\text{-depth} &= 6n + O(1)\end{aligned}$$

Ripple-carry adders

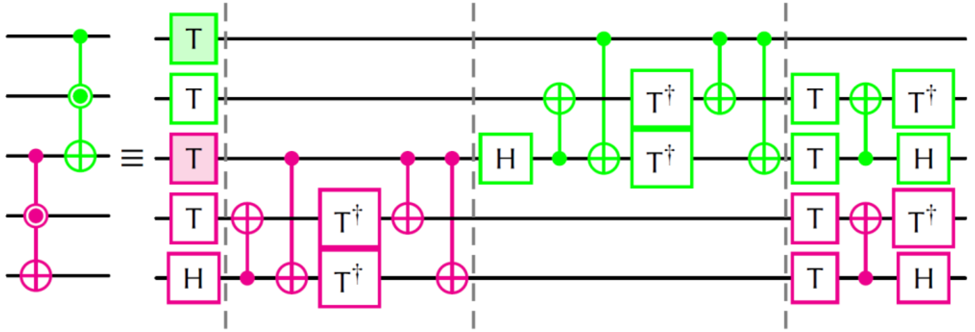
	Algorithm	CNOT-depth	CNOT-count	T-depth	T-count	Ancilla
	[TK05]	$26n$	$34n$	$9n$	$28n$	0
	[SRV08]	$16n$	$18n$	$6n$	$14n$	1
	[CDKM04] (1)	$16n$	$18n$	$6n$	$14n$	1
	[TTK10]	$15n$	$17n$	$6n$	$14n$	0
	[TR11]	$14n$	$18n$	$6n$	$14n$	1
	[CDKM04] (2)	$13n$	$17n$	$6n$	$14n$	1
This paper	Opt. [CDKM04] (1)	$11n$	$14n$	$4n$	$10n$	1
This paper	Opt. [TTK10]	$10n$	$16n$	$3n$	$12n$	0
This paper	Opt. [CDKM04] (2)	$8n$	$16n$	$3n$	$12n$	1

Note: $+O(1)$ are omitted.

Optimization rules (depth)



Left cascade of CCNOT gates.



Right cascade of Peres gates.

For a cascade of n gates:

CNOT-depth: $7n \longrightarrow 4n + 3$

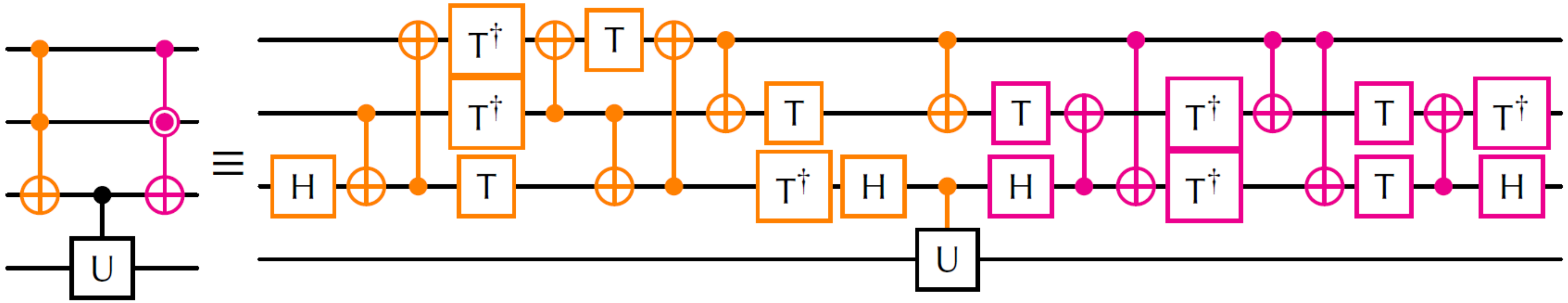
T-depth: $3n \longrightarrow 2n + 1$

For a cascade of n gates:

CNOT-depth: $5n \longrightarrow 4n + 1$

T-depth: $4n \longrightarrow n + 3$

Optimization rules (count)



V-shape with CCNOT on the left branch and Peres gates on the right one.

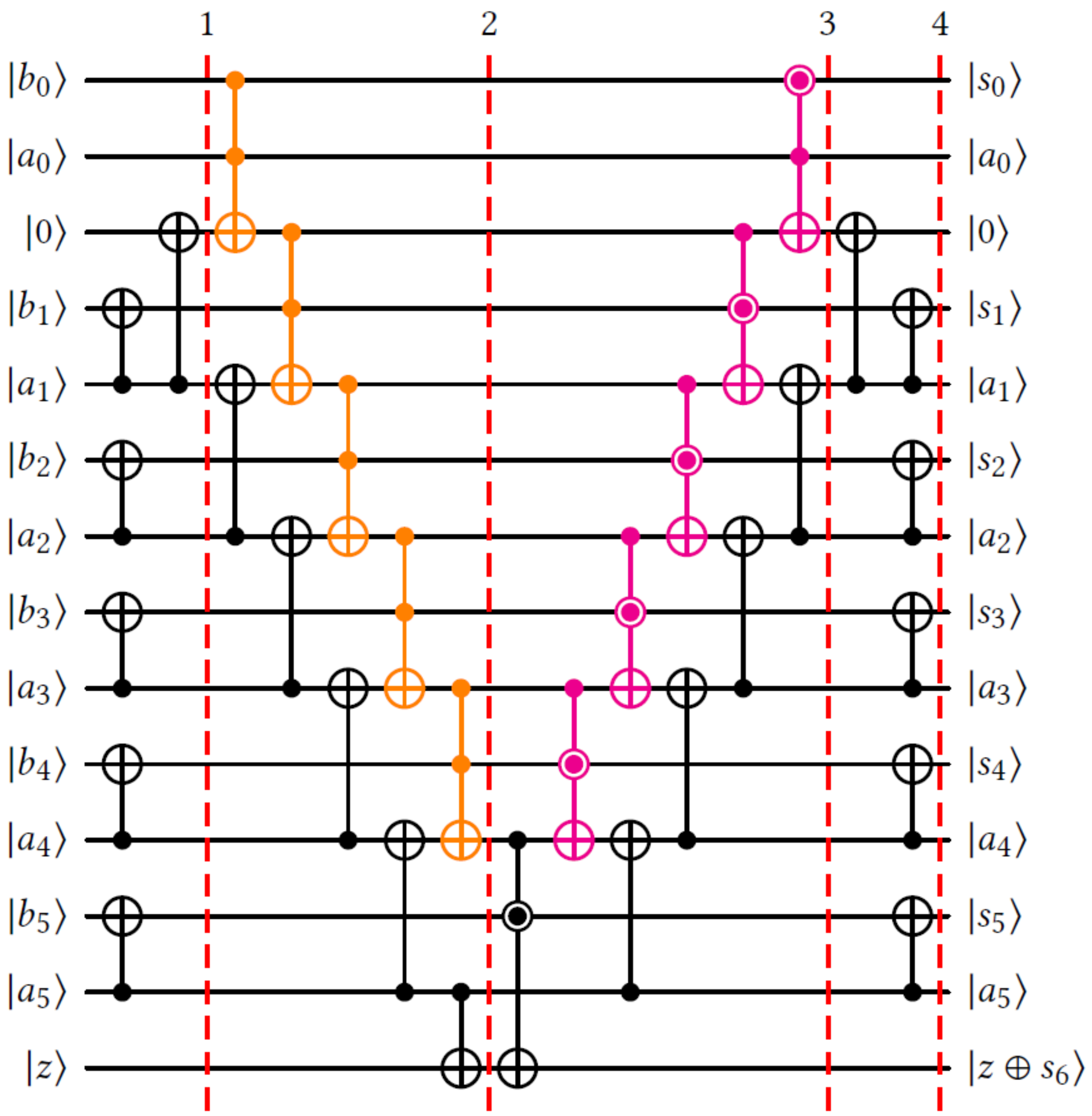
For a V-shape with n levels:

$$\begin{aligned} \mathsf{CNOT}\text{-count:} &\qquad 12n \longrightarrow 12n \\ \mathsf{T}\text{-count:} &\qquad 14n \longrightarrow 12n \end{aligned}$$

Opt. Cuccaro et al. adder (2)

Step	1	2	3	4
CNOT-count T-count	n	$8n-8$ $6n-6$	$6n-2$ $6n+1$	n
CNOT-depth T-depth	2	$4n-1$ $2n-1$	$4n+1$ $n+3$	2

$$\text{CNOT-count} = 16n - 10$$
$$\text{CNOT-depth} = 8n + 4$$
$$\text{T-count} = 12n - 5$$
$$\text{T-depth} = 3n - 2$$



Take away

- Precise state of the art of quantum ripple-carry adders
- We show that in the Clifford+T, the typical T-depth is $3n$ instead of $6n$
- Similarly, there are comparators with T-depth of $4n$ instead of $6n$
- The optimization rules can be reused (ongoing work on other arith. operators)

EVIDEN

Questions ?

For more information, please contact me:
maxime.remaud@eviden.com