Advanced oracle construction with the phase/state duality

Matthew Amy
(joint work with Neil Julien Ross)

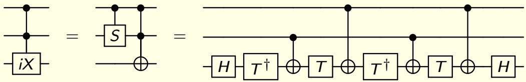
Simon Fraser University, Burnaby, Canada

Bristol Quantum Information Theory Seminar

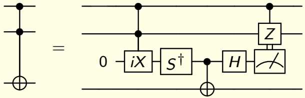
Outline

The reversible circuit construction zoo

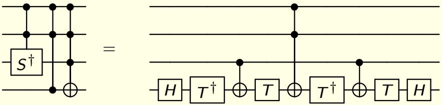
- ancilla-free multiply-controlled iX gates [Sel13, GS13]



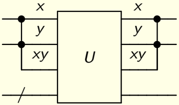
- T-count 4 measurement-assisted Toffoli [Jones13]



- ancilla-free, T-count 8 relative-phase Toffoli-4 [Mas16]



- T-count 4 temporary logical-AND [Gid18]



Goal

Generalize these constructions and unify them within a framework of reusable, automatable *design techniques.*

Result?

Gate	Ancillary state	T-count	Valid	Notes
$U_{f\cdot g}$	$\|00\rangle$	$2\tau(U_f)+\tau(U_g)+8$	–	
$U_{f\cdot g}$	–	$2\tau(U_f)+2\tau(U_g)+4$	–	Relative phase in the controls
$U_{f\cdot g}$	–	$2\tau(U_f)+\tau(U_g)+4$	–	Relative phase in the controls & targe
$\Lambda_k(X)$	$\|z\rangle$	$16(k-1)$	$k\geq 6$	Prior art
$\Lambda_k(X^\bullet)$	$\|z\rangle$	$8(k-2)+4$	$k\geq 2$	Relative phase in the controls & ancilla
$\Lambda_k(X)$	$\|z\rangle$	$16(k-2)$	$k\geq 4$	
$\Lambda_k(X)$	$\|0\rangle$	$16(k-3)$ or $16(k-3)+4$	$k\geq 4$	Measurement-assisted
$\Lambda_k(iX)$	–	$16(k-2)+4$	$k\geq 6$	Prior art; Relative phase in the controls
$\Lambda_k(iX)$	–	$16(k-3)+4$	$k\geq 4$	Relative phase in the controls
$\Lambda_k(X^\bullet)$	–	$16(k-4)+4$	$k\geq 5$	Relative phase in the controls
$\Lambda_k(X^\star)$	–	$8(k-2)$	$k\geq 3$	Relative phase in the controls & target
$\Lambda_k(X^\star)$	$\|0\rangle^{\otimes m}$	$4m+8(k-m-2)$	$k\geq 5$	Relative phase in the controls & target
U_{f_k}	$\|z\rangle$	$8(k-1)$	$k\geq 2$	
U_{f_k}	–	$4(k-1)$	$k\geq 2$	Relative phase in the controls & target
3-AND	$\|0\rangle$	8	–	Prior art; Relative phase in the controls
3-AND†	–	3 or 4	–	Relative phase; Measurement-assisted
k-AND	$\|0\rangle$	$16(k-3)+4$	$k\geq 4$	
k-AND†	–	0 or $16(k-4)+4$	$k\geq 6$	Measurement-assisted
k-AND	$\|0\rangle$	$8(k-2)$	$k\geq 3$	Relative phase in the controls
k-AND†	–	$8(k-4)$ or $8(k-4)+4$	$k\geq 4$	Relative phase; Measurement-assisted

It's a process. It's a process. It's a process

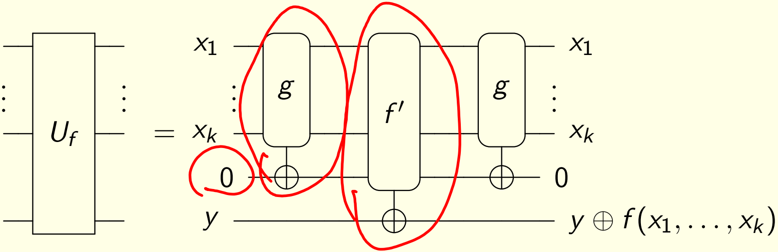
Outline

Classical oracles

Given a Boolean function $f : \mathbb{Z}_2^k \to \mathbb{Z}_2$, we want to implement

$$U_f : |x_1 \cdots x_k\rangle\, |y\rangle \mapsto |x_1 \cdots x_k\rangle\, |y \oplus f(x_1, \ldots, x_k)\rangle$$

Typical solutions use **clean ancillas** to store temporary values

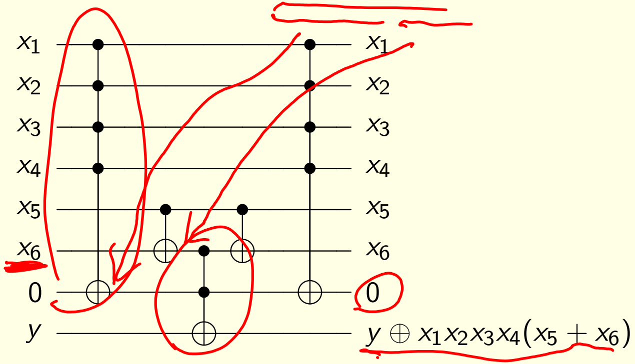


$f'(x, g(x)) = f(x)$

Example

Suppose $f(x_1, \ldots, x_6) = x_1x_2x_3x_4x_5 + x_1x_2x_3x_4x_6$

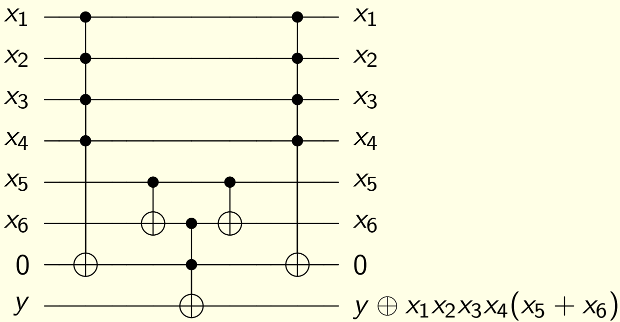
With one clean ancilla we can factor as $x_1x_2x_3x_4(x_5 + x_6)$ and write



Example

Suppose $f(x_1, \ldots, x_6) = x_1x_2x_3x_4x_5 + x_1x_2x_3x_4x_6$

With one clean ancilla we can factor as $x_1x_2x_3x_4(x_5 + x_6)$ and write

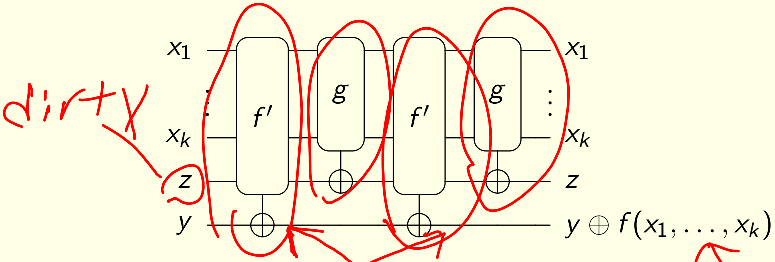


Out of space! Now what?

Dirty ancillas

Unused data qubits can also be used as temporary scratch space

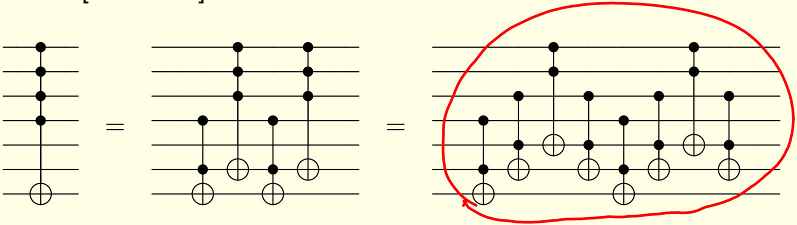
We call these **dirty ancillas**



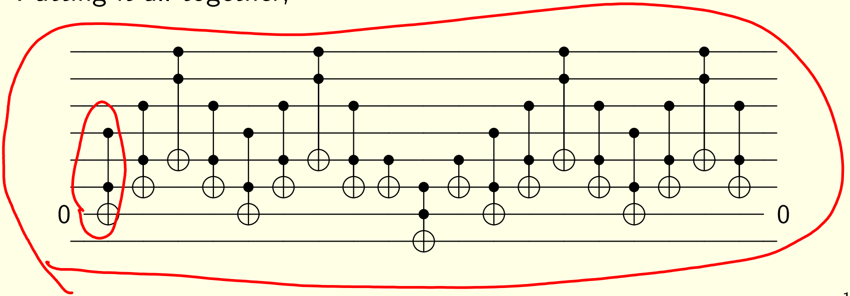
$f'(x_1 z \oplus g(x)) = f'(x_1 z) + f'(x_1 g(x))$

Back to our example

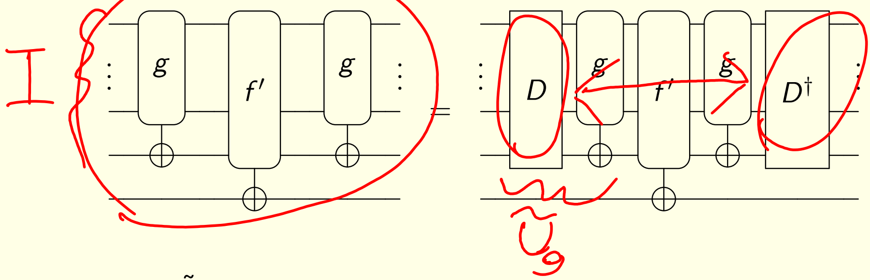
The 4 control Toffoli can be written using Toffolis and 2 dirty ancillas [BBC+95]



Putting it all together,



For any **diagonal** gate D, we have the following equivalence



We say $\tilde{U}_f$ implements an oracle U_f **up to relative phase** if for some diagonal gates D, D',

$$DU_f = \tilde{U}_f = U_f D'$$

Brief history of relative phases

Pre-history

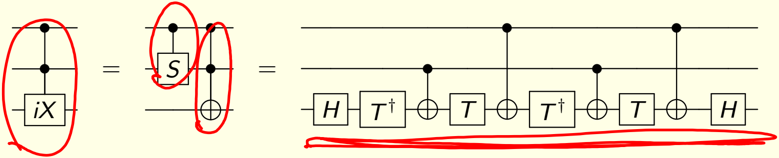
- (Margolus ???) Toffoli can be implemented up to phase with 3 two-qubit gates vs. 5 two-qubit gates exactly
- (DiVincenzo and Smolin 1994) "relative phases are dangerous"
- (Barenco et al. 1995) "it's fine if only classical computations in the middle..."

Modern history

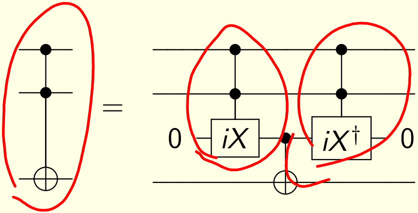
- (Selinger 2013) 4 T gate relative phase Toffoli
- (Giles and Selinger 2013) ancilla-free, relative phase multiply-controlled Toffoli gate
- (Jones 2013) 4 T-gate Toffoli
- (Maslov 2016) 8 T-gate relative phase 4-qubit Toffoli
- (Gidney 2018) 4 T-gate temporary logical AND

The *cciX* gate

Peter Selinger's *cciX* gate [Sel13]:

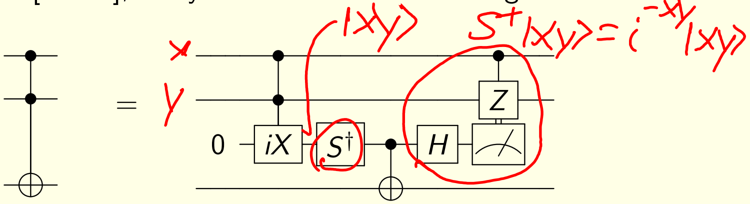


Selinger used the *cciX* gate as an efficient primitive for temporary products



The Cody Jones Toffoli

Shortly after [Jon13], Cody Jones discovered a 4-T gate Toffoli

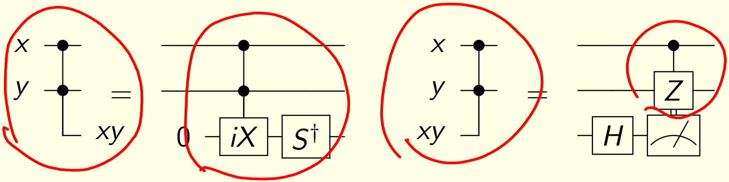


Cody Jones's main observations were:

1. the relative phase could be corrected with **a single $S^\dagger$ gate** if the ancilla is clean, and
2. the temporary product could be uncomputed **without T gates** by using measurement and classical control

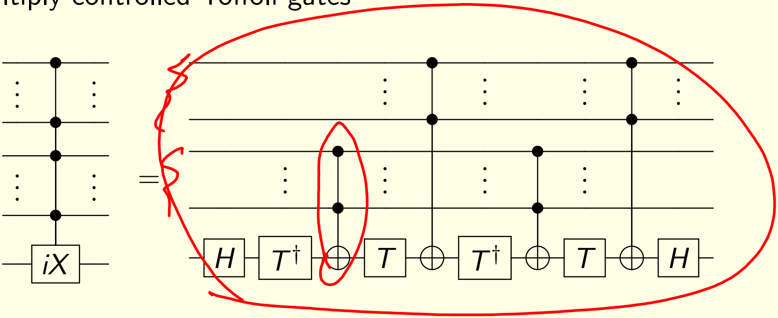
Temporary logical AND

Craig Gidney later [Gid18] turned these observations into primitives for **computing** and **uncomputing** 2-bit products



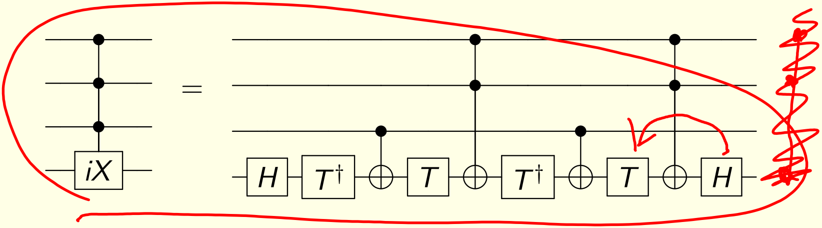
Multiply-controlled iX

Giles & Selinger [GS13] discovered a **multiply-controlled** iX gate by replacing the $CNOT$s in Selinger's $cciX$ circuit with multiply-controlled Toffoli gates

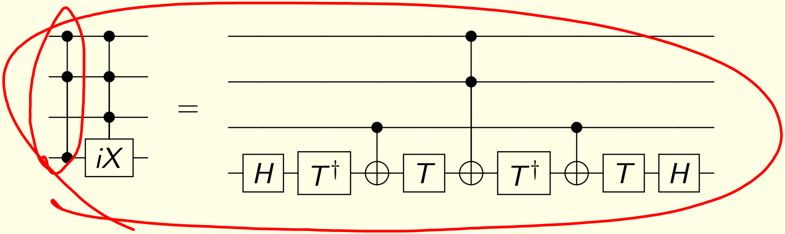


T-count scaling: $16k + O(1)$

Maslov's relative phase Toffoli-4



Dmitri Maslov [Mas16] realized that the final Toffoli gate can be dropped, giving a **relative phase 4-qubit Toffoli** with T-count 8:



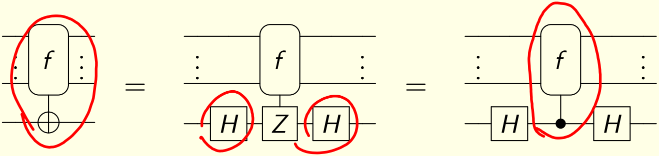
Outline

The phase/state duality

Conjugation by H gates swaps state and (-1) phases

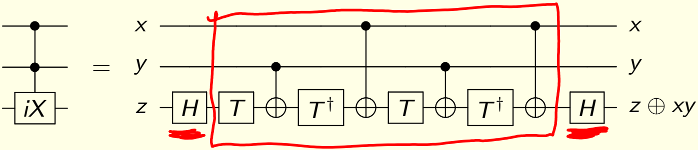
$$|y \oplus f(x)\rangle \langle y| \xleftrightarrow{\phi_H(\cdot)} (-1)^{yf(x)} |y\rangle \langle y|$$

Or, as circuits

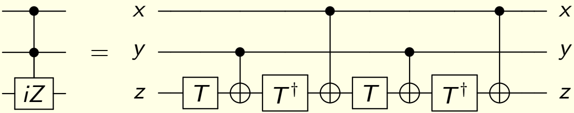


$X = HZH$

A closer look at *cciX*



A closer look at *cciX*

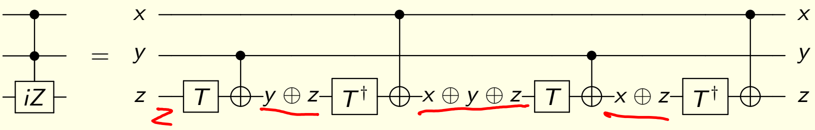


The relevant computation is *ccZ* gate

$$|xyz\rangle \mapsto (-1)^{xyz}\,|xyz\rangle$$

up to a relative phase independent of z

A closer look at *cciX*



The relevant computation is *ccZ* gate

$$|xyz\rangle \mapsto (-1)^{xyz}\,|xyz\rangle$$

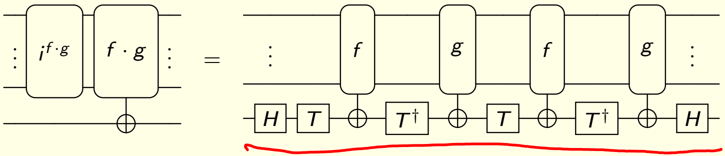
up to a relative phase independent of z

In particular, $\omega^{z-(y\oplus z)+(x\oplus y\oplus z)-(x\oplus z)} = i^{xy}(-1)^{xyz}$, where i^{xy} is the relative phase.

Replacing x and y in $(-1)^{xyz}$ with oracles $f(x)$ and $g(x)$ gives

$$\omega^{z - z\oplus f(x) - z\oplus g(x) + z\oplus f(x)\oplus g(x)} = i^{f(x)g(x)}(-1)^{zf(x)g(x)},$$

so the Giles-Selinger construction gives a method of multiplying oracles **up to phase**



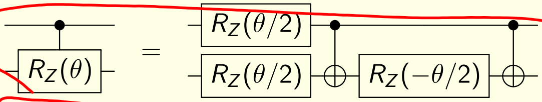
Can we **a priori** find the relative phase that reduces T-count?

General construction of relative phases

The Boolean Fourier expansion,

$$x_1 \cdots x_n = \frac{1}{2^{n-1}} \sum_{S \subseteq \{1,\ldots,n\}} (-1)^{|S|-1} \chi_S(x_1, \ldots, x_n),$$

decomposes a diagonal gate over $\{CNOT, R_Z\}$ [AAM18]



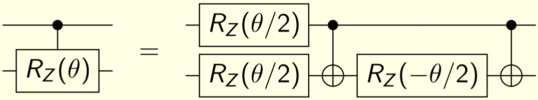
$e^{i\theta xy} = e^{i\theta/2\, x + \theta/2\, y - \theta/2\, x \oplus y}$

General construction of relative phases

The Boolean Fourier expansion,

$$x_1 \cdots x_n = \frac{1}{2^{n-1}} \sum_{S \subseteq \{1,\ldots,n\}} (-1)^{|S|-1} \chi_S(x_1, \ldots, x_n),$$

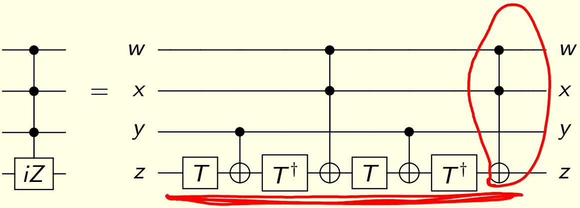
decomposes a diagonal gate over $\{CNOT, R_Z\}$ [AAM18]



Dropping terms that **depend on the target** gives a relative phase!

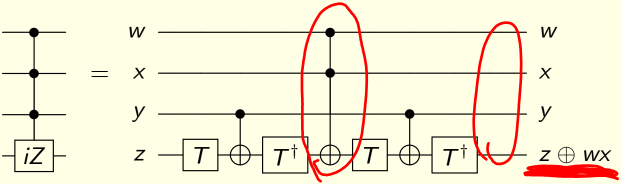
$$
\begin{aligned}
(-1)^{xyz} &= \omega^{x+y+z-(x\oplus y)-(x\oplus z)-(y\oplus z)+(x\oplus y\oplus z)} \\
&= \omega^{x+y-(x\oplus y)} \omega^{z-(y\oplus z)+(x\oplus y\oplus z)-(x\oplus z)} \\
&= i^{xy} \omega^{z-(y\oplus z)+(x\oplus y\oplus z)-(x\oplus z)}
\end{aligned}
$$

The relative phase Toffoli-4



The relevant computation is in the **phase**, but the final Toffoli just cleans the **state garbage**

The relative phase Toffoli-4

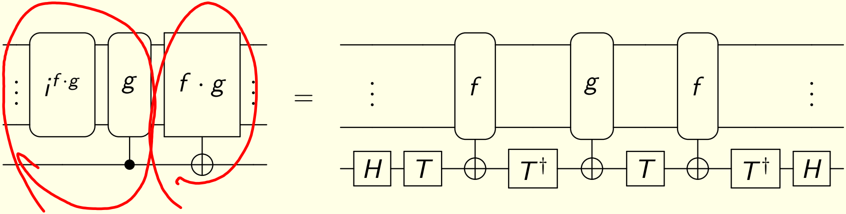


The relevant computation is in the **phase**, but the final Toffoli just cleans the **state garbage**

Conjugating with Hadamard gates instead **swaps** it into the phase

$$i^{wxy}(-1)^{wxyz} |z \oplus wx\rangle \langle z| \xleftrightarrow{\phi_H(\cdot)} i^{wxy}(-1)^{wxz} |z\rangle \langle z \oplus wxy| \,,$$

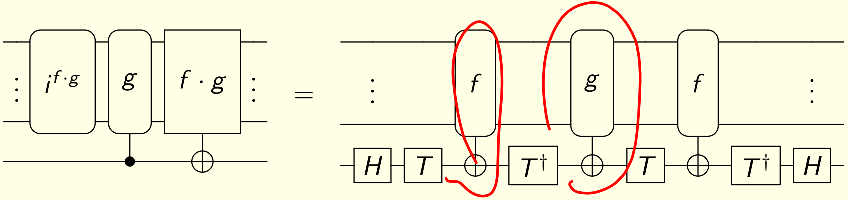
Applying to our oracle multiplication circuit...



Construction

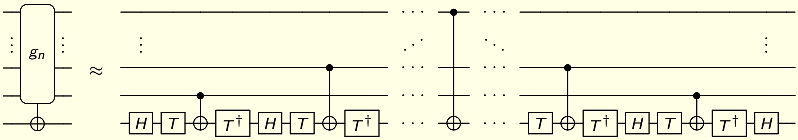
Unbalanced ancilla-free oracle multiplication

Applying to our oracle multiplication circuit...



Can we iterate unbalanced multiplication?

Setting $f_i(x) = x_i$, and $g_i = f_i \cdot g_{i-1}$ generates **high degree, non-Toffoli oracles** with low T-count, up to phase



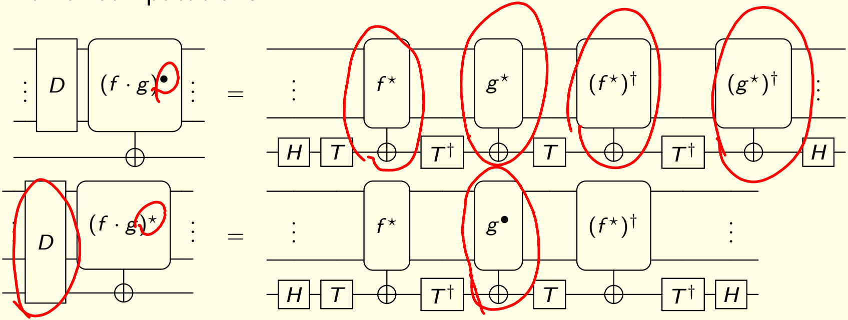
For example, $g_4(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4 + x_1x_4 + x_3x_4$

- T-count: $4(k-1)$ deg k
- Previous best: $16(k-1) + O(1)$
- **Matches multiplicative complexity-based synthesis without using ancillas**

Target-dependant relative phase

The extra terms previously arise from iterating with a **target-dependant** relative phase

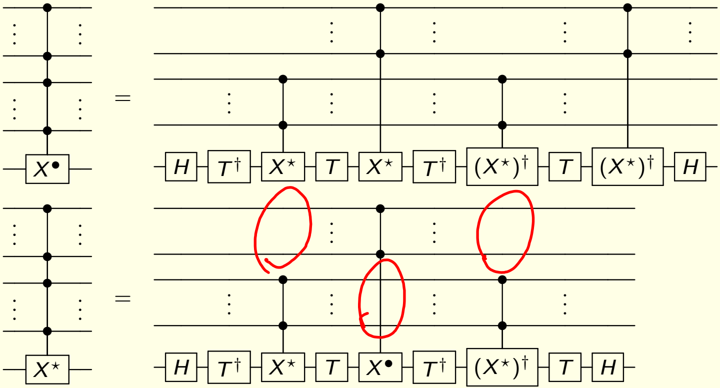
We can eliminate target-dependant phases by matching them up with uncomputations:



Multiply-controlled Toffoli

Attempt 1

Construction of a multiply-controlled Toffoli up to relative phase:



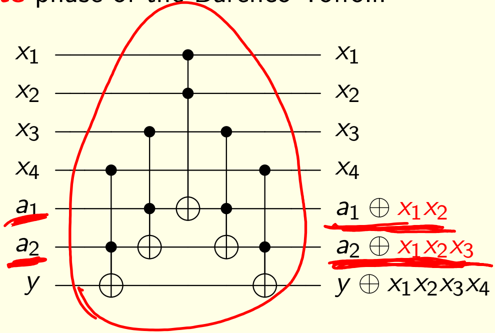
Problem: scales **non-linearly**!

Can we build efficient relative phase Toffolis with ancillas?

State garbage = relative phase

$$|y \oplus f(x)\rangle \langle y| \xleftrightarrow{\phi_H(\cdot)} (-1)^{yf(x)} |y\rangle \langle y|$$

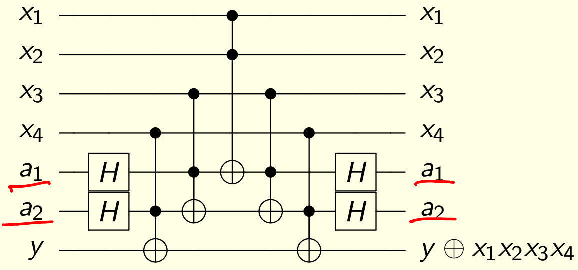
Recall the **compute** phase of the Barenco Toffoli:



State garbage = relative phase

$$|y \oplus f(x)\rangle \langle y| \xleftrightarrow{\phi_H(\cdot)} (-1)^{yf(x)} |y\rangle \langle y|$$

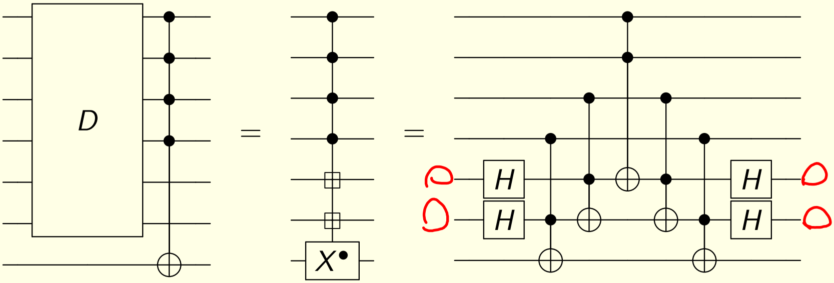
Recall the **compute** phase of the Barenco Toffoli:



Rather than **uncompute** the temporary values in red, we can trade them for a relative phase

Construction

Relative-phase dirty ancilla Toffoli

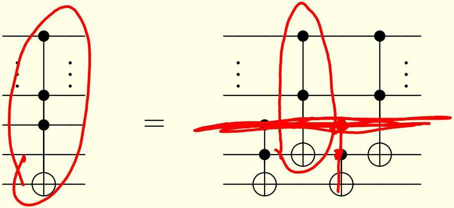


- T-count: $8(k-1)-4$ for k controls
- Previous best: $8(k-1)$ for k controls
- Matches the usual clean ancilla construction
- **Still not good enough!**

Getting it down to a single number (of ancillas)

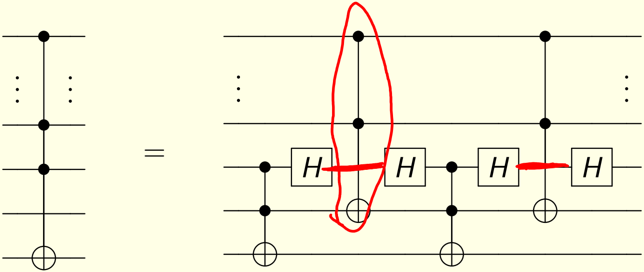
Getting it down to a single number (of ancillas)

Barenco's dirty ancilla Toffoli gives a uniform recursive construction, but with **exponential** gate count since each recursive stage needs to clean up its garbage



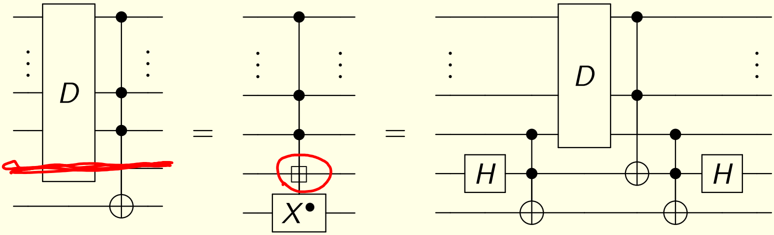
Ancilla catalysis

By swapping to the **phase space**, we can catalyze an auxiliary dirty ancilla **that doesn't need to be cleaned**



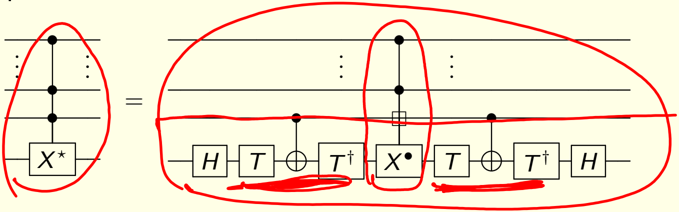
Construction

Single dirty ancilla Toffoli up to phase



- T-count: $8(k-1)-4$ for k controls **with one ancilla**
- T-count: $16(k-2)$ for k controls with phase correction
- Previous best: $16(k-1)$

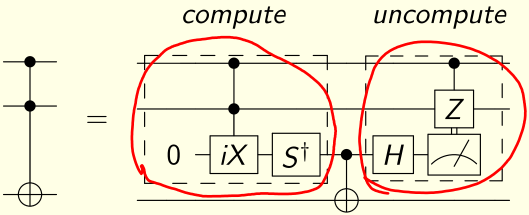
We can now use the single dirty ancilla Toffoli to bootstrap a relative-phase ancilla free Toffoli



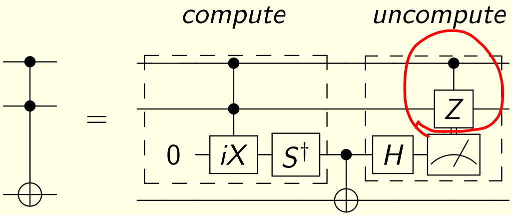
- T-count: $8(k-2)$
- Previous best: $16(k-2)+4$
- Reduces T-count for $< \lceil \frac{k-2}{2} \rceil$ clean ancillas

Outline

A closer look at Jones' T-count 4 Toffoli



A closer look at Jones' T-count 4 Toffoli



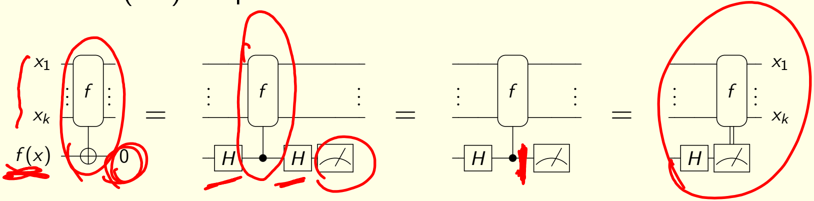
The uncompute circuit works because

$$H|xy\rangle = \frac{1}{\sqrt{2}} \sum_{z \in \mathbb{Z}_2} (-1)^{xyz} |z\rangle,$$

which leaves a phase of 0 if measurement returns 0, or $(-1)^{xy}$ otherwise

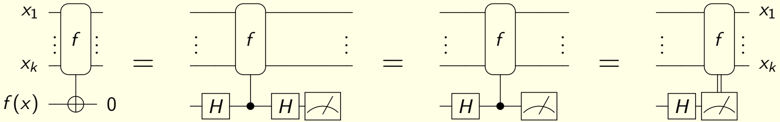
Termination by X-basis measurements

More generally, terminating an ancilla in the temporary state $|f(x)\rangle$ is equivalent to an X basis measurement and a classically controlled $(-1)^{f(x)}$ phase:



Termination by X-basis measurements

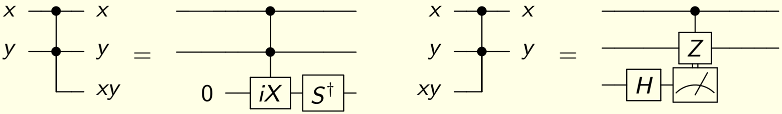
More generally, terminating an ancilla in the temporary state $|f(x)\rangle$ is equivalent to an X basis measurement and a classically controlled $(-1)^{f(x)}$ phase:



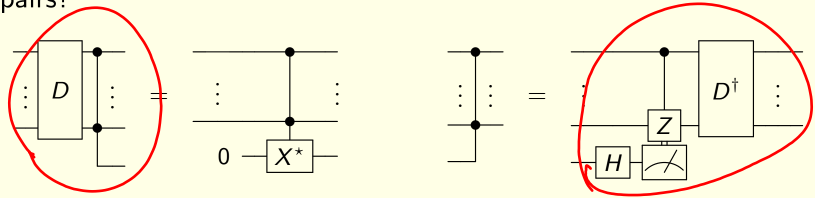
However, correction is not Clifford if deg$(f) \geq 3$

Temporary products

Gidney revived Jones' work by turning it into a **temporary product**



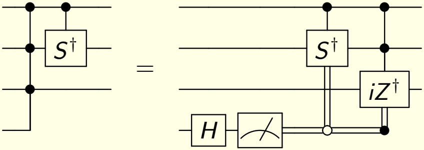
Can we construct similar (resource-efficient) compute/uncompute pairs?



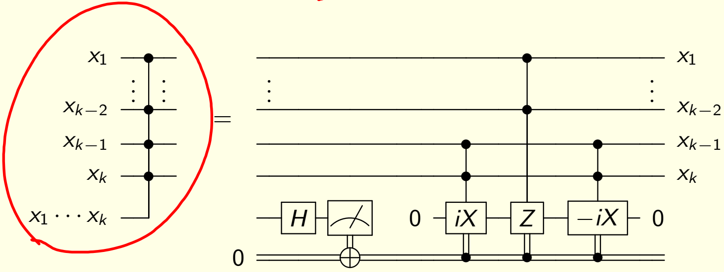
Construction

un-logical-AND

Uncomputing Maslov's Toffoli



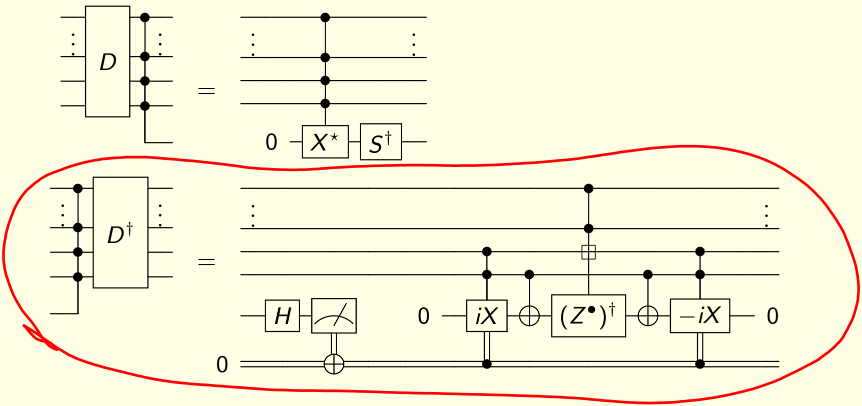
T-count: 3.5 on average (vs. 8)



T-count: $8(k-4)+2$ on average (vs. $16(k-2)$)

Construction

Temporary k-AND



- T-count $8(k-2)$ to compute
- T-count $8(k-4)$ or $8(k-4)+4$ to uncompute
- **Lowest T-count, ancilla free compute & uncompute circuits for k-control products**

Outline

1. Overview
2. Oracle implementation
3. Generalizing Selinger's construction
4. Generalizing Jones' construction
5. Conclusion

Conclusions

Conclusions

In this talk...

- classes of degree k functions with T-count $4(k-1)$
- temporary logical-k-ANDs with T-count down to $8(k-2)$
- measurement-assisted uncomputation of a k-AND with average T-count $8(k-4)+2$

Main takeaway: improvements can be made by designing oracles with both phase and state in mind

References

[BBC+95] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. Physical Review A, 52:3457–3467, 1995.

[Sel13] P. Selinger. Quantum circuits of T-depth one. Physical Review A, 87:042302, 2013

[GS13] B. Giles and P. Selinger. Exact synthesis of multiqubit Clifford+T circuits. Physical Review A, 87:032332, 2013.

[Jon13] C. Jones. Low-overhead constructions for the fault-tolerant toffoli gate. Physical Review A, 87:022328, 2013.

[Mas16] D. Maslov. Advantages of using Relative-Phase Toffoli Gates with an Application to Multiple Control Toffoli Optimization. Physical Review A, 93:022311, 2016.

[Gid18] C. Gidney. Halving the cost of quantum addition. Quantum, 2:74, 2018.

[AAM18] M. Amy, P. Azimzadeh, M. Mosca. On the CNOT-complexity of CNOT-Phase circuits. Quantum Science & Technology 4(1), 2018.

[AR21] M. Amy, N. J. Ross. The phase/state duality in reversible circuit design. Physical Review A 104, 052602, 2021.

Thank you!