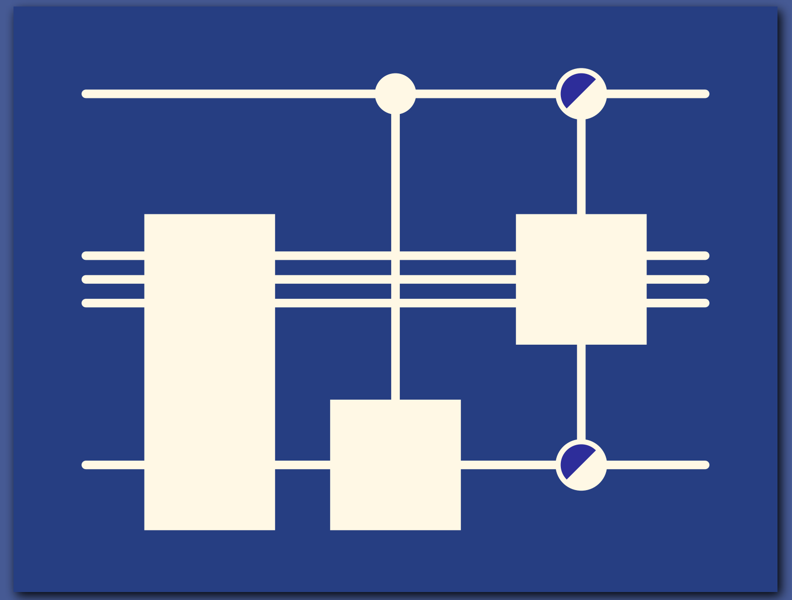
Quantum Information Processing Conference | RIGA 2026



slides: slote.org/qip

Quantum precomputation:

Parallelizing cascade circuits and the Moore–Nilsson conjecture is false

Joe Slote (Caltech → UW)

Joint with Adam Bene Watts, Charles R. Chen, and J. William Helton

Joint with:

Adam Bene Watts
U Calgary

Charles R. Chen
UC San Diego

J. William Helton
UC San Diego

Classical parallelization

Guiding question. Can every program be parallelized?

Classical parallelization

Guiding question. Can every program be parallelized?

Guiding question (formal)**.** Suppose $f : \{0,1\}^n \to \{0,1\}$ has a size-s circuit (s-many gates). Can f be implemented by a circuit of depth $\mathsf{polylog}(s)$ and size $\mathsf{poly}(s)$?

Classical parallelization

Guiding question. Can every program be parallelized?

Guiding question (formal)**.** Suppose $f : \{0,1\}^n \to \{0,1\}$ has a size-s circuit (s-many gates). Can f be implemented by a circuit of depth $\mathsf{polylog}(s)$ and size $\mathsf{poly}(s)$?

Example.

$f = \mathsf{AND}_8$

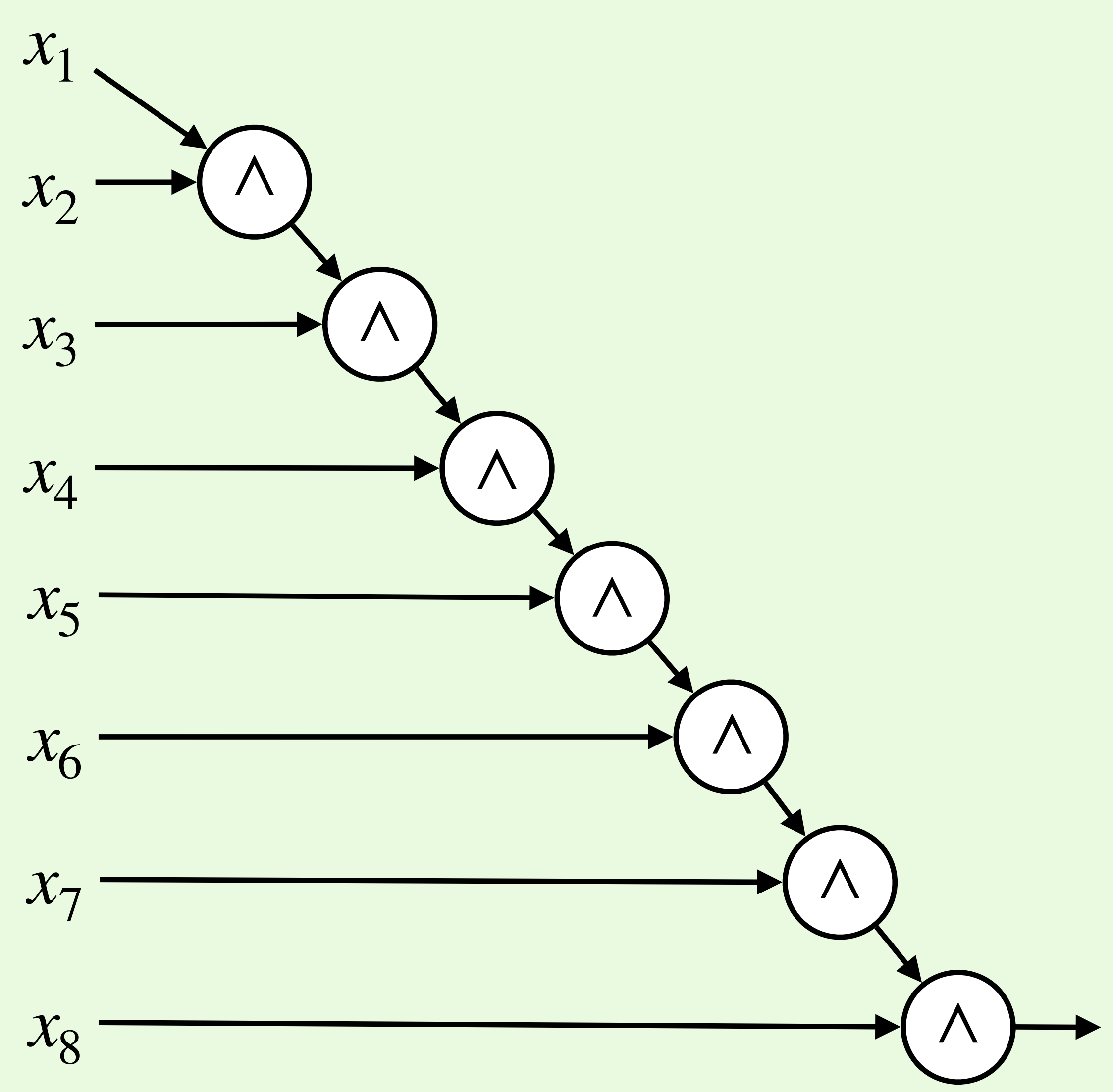
Classical parallelization

Guiding question. Can every program be parallelized?

Guiding question (formal)**.** Suppose $f : \{0,1\}^n \to \{0,1\}$ has a size-s circuit (s-many gates). Can f be implemented by a circuit of depth polylog(s) and size poly(s)?

Example.

$f = \mathsf{AND}_8$



Circuit model: NC
(const. fan-in & fan-out)

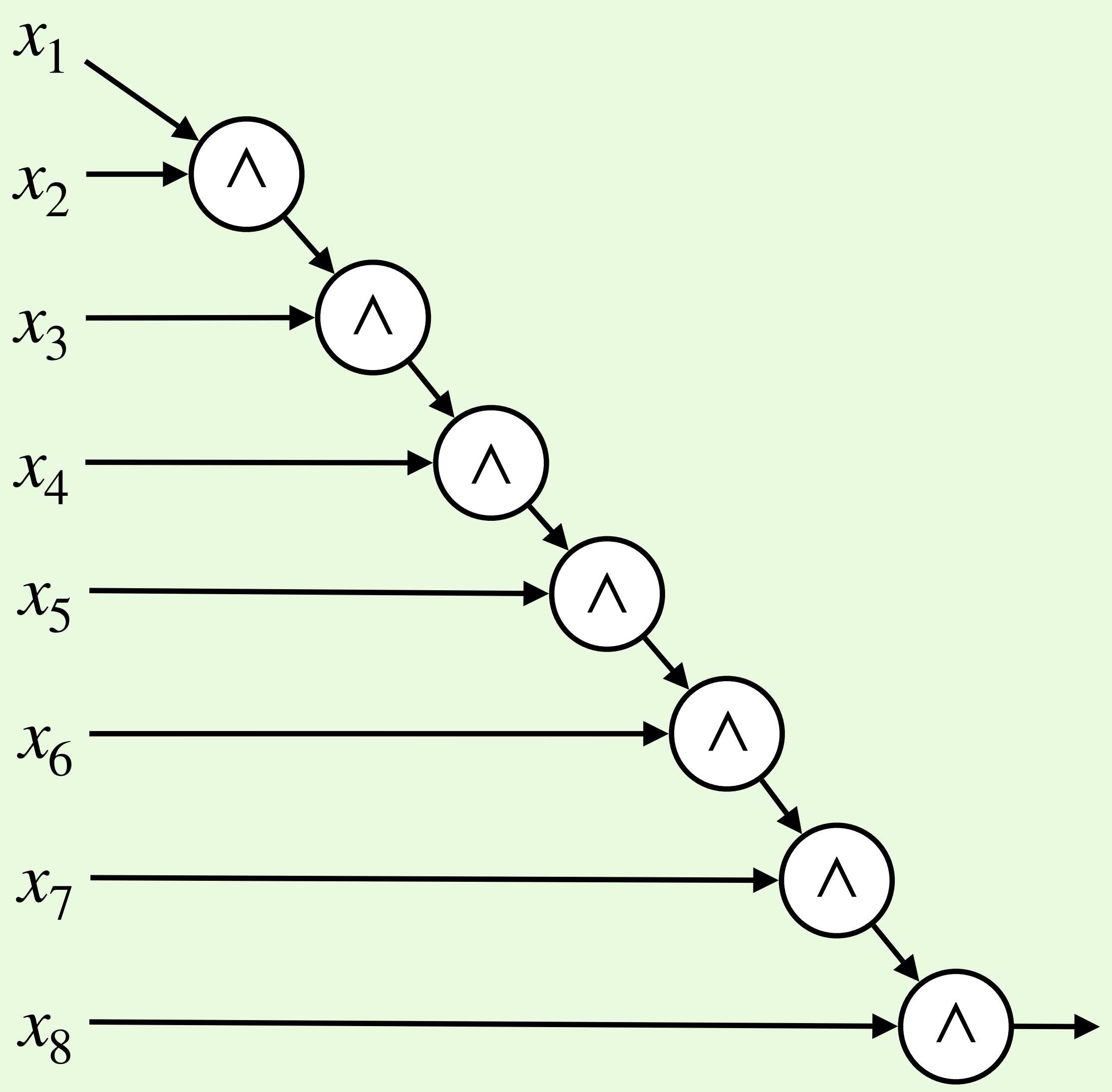
Classical parallelization

Guiding question. Can every program be parallelized?

Guiding question (formal)**.** Suppose $f : \{0,1\}^n \to \{0,1\}$ has a size-s circuit (s-many gates). Can f be implemented by a circuit of depth $\mathsf{polylog}(s)$ and size $\mathsf{poly}(s)$?

Example.

$f = \mathsf{AND}_8$



Circuit model: NC
(const. fan-in & fan-out)

size: 7, depth: 7

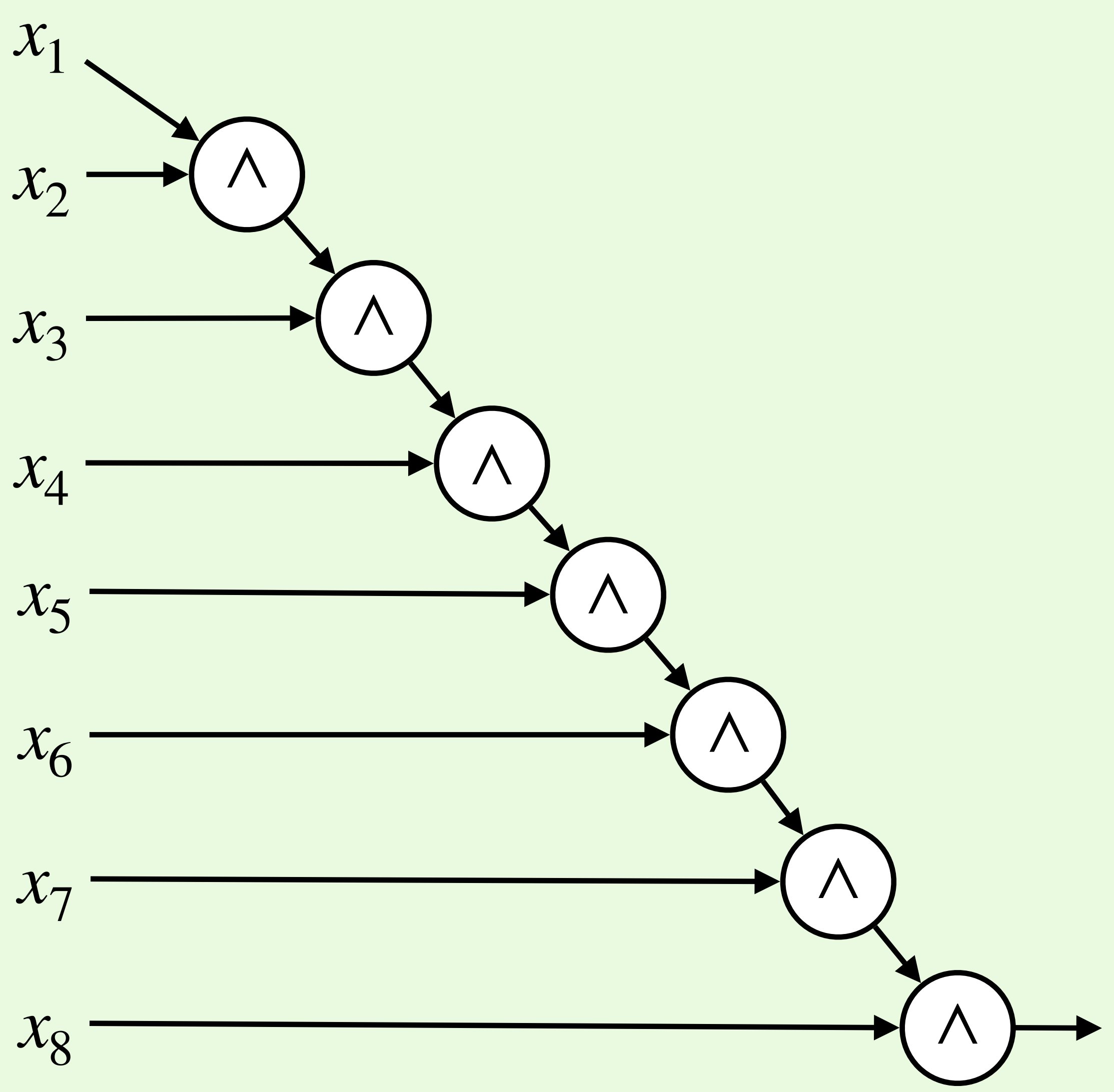
Classical parallelization

Guiding question. Can every program be parallelized?

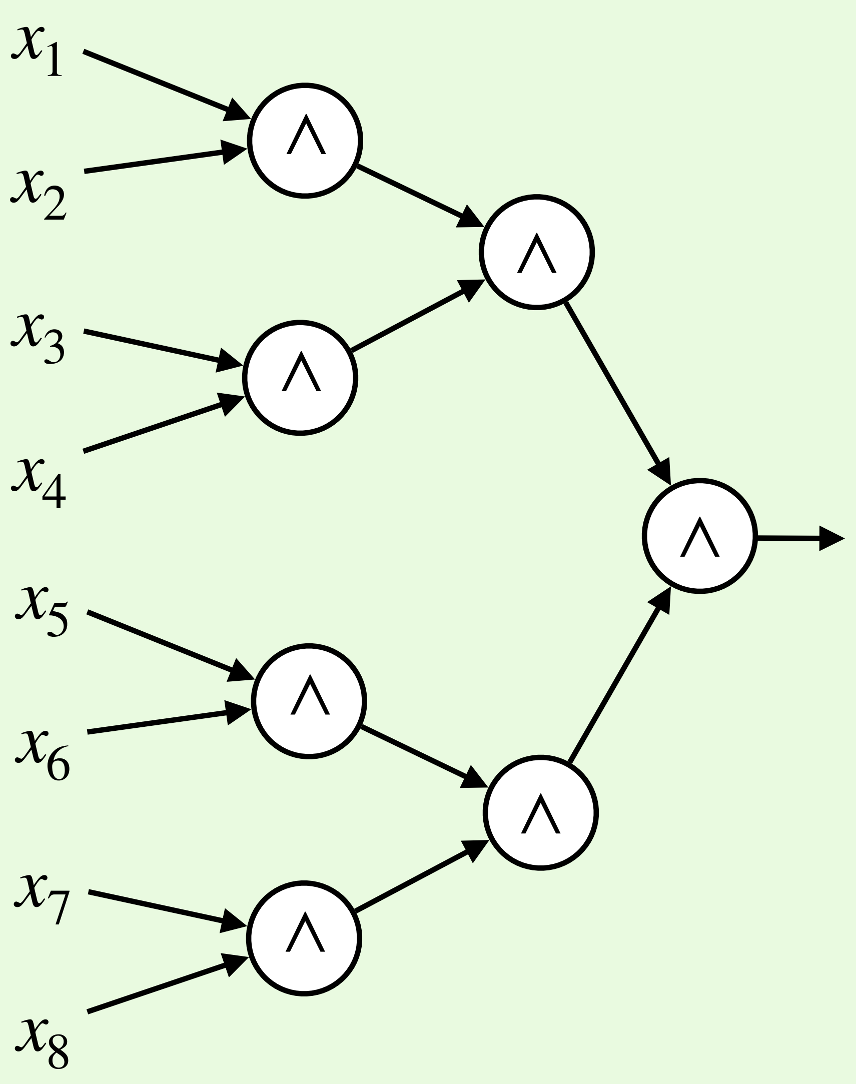
Guiding question (formal)**.** Suppose $f : \{0,1\}^n \to \{0,1\}$ has a size-s circuit (s-many gates). Can f be implemented by a circuit of depth $\mathsf{polylog}(s)$ and size $\mathsf{poly}(s)$?

Example.

$f = \mathsf{AND}_8$



size: 7, depth: 7



size: 7, depth: 3

Circuit model: NC
(const. fan-in & fan-out)

Classical parallelization

Classical parallelization

Question (The $\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ problem). If f has a circuit of size $\mathrm{poly}(n)$, does f have a circuit of depth $\mathrm{polylog}(n)$ and size $\mathrm{poly}(n)$?

Classical parallelization

Question (The $\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ problem)**.** If f has a circuit of size $\mathbf{poly}(n)$, does f have a circuit of depth $\mathbf{polylog}(n)$ and size $\mathbf{poly}(n)$?

Strongly expected that $\mathsf{NC} \neq \mathsf{P}$; *i.e.*, some efficient algorithms are *inherently sequential.*

Classical parallelization

Question (The $\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ problem)**.** If f has a circuit of size $\mathsf{poly}(n)$, does f have a circuit of depth $\mathsf{polylog}(n)$ and size $\mathsf{poly}(n)$?

Strongly expected that $\mathsf{NC} \neq \mathsf{P}$; *i.e.*, some efficient algorithms are *inherently sequential.*

Classical parallelization

Question (The $\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ problem). If f has a circuit of size $\mathsf{poly}(n)$, does f have a circuit of depth $\mathsf{polylog}(n)$ and size $\mathsf{poly}(n)$?

Strongly expected that $\mathsf{NC} \neq \mathsf{P}$; *i.e.*, some efficient algorithms are *inherently sequential.*

In fact, $\mathsf{NC} \neq \mathsf{P}$ is *required* by some cryptography:

Classical parallelization

Question (The $\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ problem)**.** If f has a circuit of size $\mathsf{poly}(n)$, does f have a circuit of depth $\mathsf{polylog}(n)$ and size $\mathsf{poly}(n)$?

Strongly expected that $\mathsf{NC} \neq \mathsf{P}$; *i.e.*, some efficient algorithms are *inherently sequential.*

In fact, $\mathsf{NC} \neq \mathsf{P}$ is *required* by some cryptography:

- Time-lock puzzles, with applications to *e.g.* decentralized auctions.

Classical parallelization

Question (The $\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ problem)**.** If f has a circuit of size $\mathsf{poly}(n)$, does f have a circuit of depth $\mathsf{polylog}(n)$ and size $\mathsf{poly}(n)$?

Strongly expected that $\mathsf{NC} \neq \mathsf{P}$; *i.e.*, some efficient algorithms are *inherently sequential.*

In fact, $\mathsf{NC} \neq \mathsf{P}$ is *required* by some cryptography:

- Time-lock puzzles, with applications to *e.g.* decentralized auctions.
- Security seems independent of standard cryptographic hardness assumptions.

Classical parallelization

Question (The $\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ problem)**.** If f has a circuit of size $\mathsf{poly}(n)$, does f have a circuit of depth $\mathsf{polylog}(n)$ and size $\mathsf{poly}(n)$?

Strongly expected that $\mathsf{NC} \neq \mathsf{P}$; *i.e.*, some efficient algorithms are *inherently sequential.*

In fact, $\mathsf{NC} \neq \mathsf{P}$ is *required* by some cryptography:

- Time-lock puzzles, with applications to *e.g.* decentralized auctions.
- Security seems independent of standard cryptographic hardness assumptions.

If $\mathsf{NC} = \mathsf{P}$, parallelomania! (Imagine fully-parallel gradient descent...)

Classical parallelization

Question (The $\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ problem)**.** If f has a circuit of size $\mathsf{poly}(n)$, does f have a circuit of depth $\mathsf{polylog}(n)$ and size $\mathsf{poly}(n)$?

Strongly expected that $\mathsf{NC} \neq \mathsf{P}$; *i.e.*, some efficient algorithms are *inherently sequential.*

If $\mathsf{NC} = \mathsf{P}$, parallelomania! (Imagine fully-parallel gradient descent...)

In fact, $\mathsf{NC} \neq \mathsf{P}$ is *required* by some cryptography:

- Time-lock puzzles, with applications to *e.g.* decentralized auctions.
- Security seems independent of standard cryptographic hardness assumptions.

Classical parallelization

Question (The $\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ problem)**.** If f has a circuit of size $\mathsf{poly}(n)$, does f have a circuit of depth $\mathsf{polylog}(n)$ and size $\mathsf{poly}(n)$?

Strongly expected that $\mathsf{NC} \neq \mathsf{P}$; *i.e.*, some efficient algorithms are *inherently sequential.*

In fact, $\mathsf{NC} \neq \mathsf{P}$ is *required* by some cryptography:

- Time-lock puzzles, with applications to *e.g.* decentralized auctions.
- Security seems independent of standard cryptographic hardness assumptions.

If $\mathsf{NC} = \mathsf{P}$, parallelomania! (Imagine fully-parallel gradient descent...)

$\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ is difficult.

Classical parallelization

Question (The $\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ problem). If f has a circuit of size $\mathsf{poly}(n)$, does f have a circuit of depth $\mathsf{polylog}(n)$ and size $\mathsf{poly}(n)$?

Strongly expected that $\mathsf{NC} \neq \mathsf{P}$; *i.e.*, some efficient algorithms are *inherently sequential.*

In fact, $\mathsf{NC} \neq \mathsf{P}$ is *required* by some cryptography:

- Time-lock puzzles, with applications to *e.g.* decentralized auctions.
- Security seems independent of standard cryptographic hardness assumptions.

If $\mathsf{NC} = \mathsf{P}$, parallelomania! (Imagine fully-parallel gradient descent...)

$\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ is difficult.

- Open since the birth of circuit complexity [Cook 81]

Classical parallelization

Question (The $\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ problem)**.** If f has a circuit of size $\mathbf{poly}(n)$, does f have a circuit of depth $\mathbf{polylog}(n)$ and size $\mathbf{poly}(n)$?

Strongly expected that $\mathsf{NC} \neq \mathsf{P}$; *i.e.*, some efficient algorithms are *inherently sequential.*

In fact, $\mathsf{NC} \neq \mathsf{P}$ is *required* by some cryptography:

- Time-lock puzzles, with applications to *e.g.* decentralized auctions.
- Security seems independent of standard cryptographic hardness assumptions.

If $\mathsf{NC} = \mathsf{P}$, parallelomania! (Imagine fully-parallel gradient descent...)

$\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ is difficult.

- Open since the birth of circuit complexity [Cook 81]
- Best lower bound is $(3 - o(1))\log(n)$ [Håstad 93]

Classical parallelization

Question (The $\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ problem)**.** If f has a circuit of size $\mathsf{poly}(n)$, does f have a circuit of depth $\mathsf{polylog}(n)$ and size $\mathsf{poly}(n)$?

Strongly expected that $\mathsf{NC} \neq \mathsf{P}$; *i.e.*, some efficient algorithms are *inherently sequential.*

In fact, $\mathsf{NC} \neq \mathsf{P}$ is *required* by some cryptography:

- Time-lock puzzles, with applications to *e.g.* decentralized auctions.
- Security seems independent of standard cryptographic hardness assumptions.

If $\mathsf{NC} = \mathsf{P}$, parallelomania! (Imagine fully-parallel gradient descent...)

$\mathsf{NC} \stackrel{?}{=} \mathsf{P}$ is difficult.

- Open since the birth of circuit complexity [Cook 81]
- Best lower bound is $(3 - o(1))\log(n)$ [Håstad 93]

What about the quantum version?

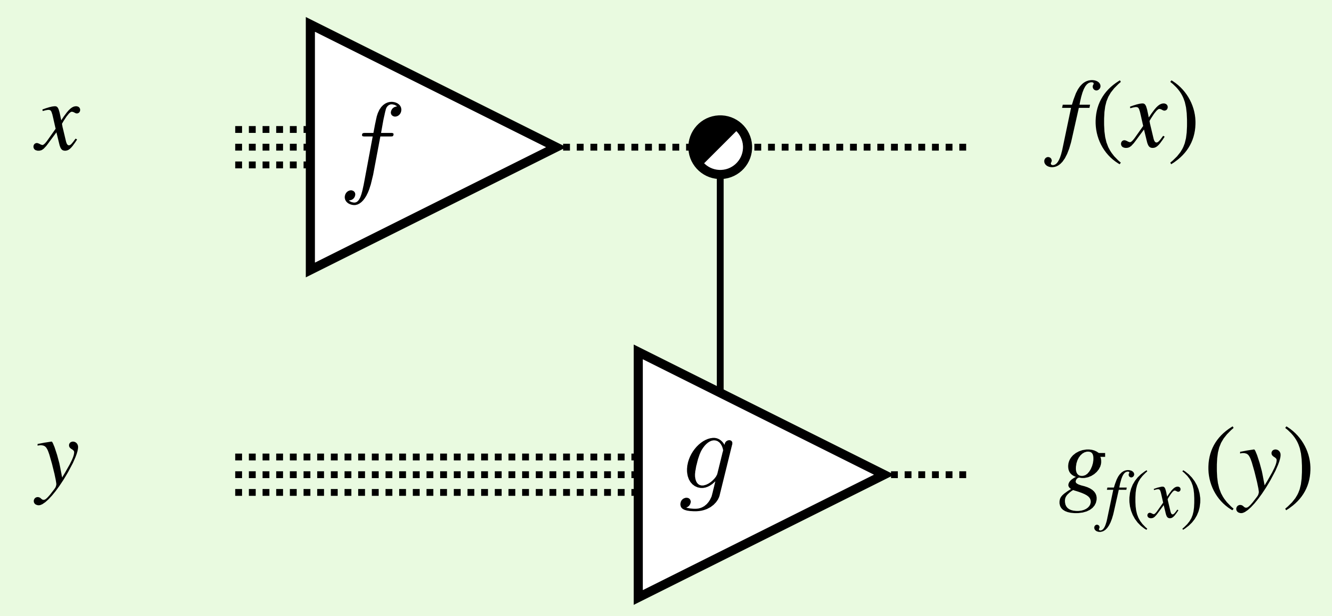
Quantum parallelization: a fundamental difference?

Quantum parallelization: a fundamental difference?

Example (Classical)**.** With $f, g_0, g_1 : \{0,1\}^n \to \{0,1\}$ all requiring $T(n)$ depth, consider...

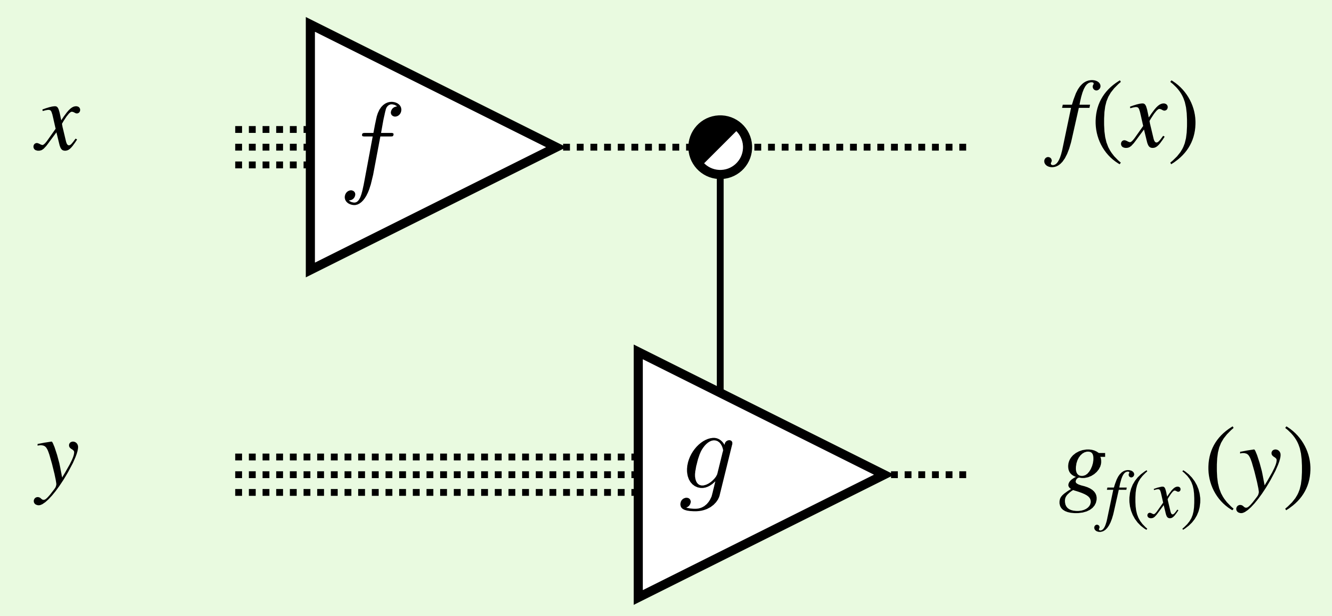
Quantum parallelization: a fundamental difference?

Example (Classical). With $f, g_0, g_1 : \{0,1\}^n \to \{0,1\}$ all requiring $T(n)$ depth, consider...



Quantum parallelization: a fundamental difference?

Example (Classical). With $f, g_0, g_1 : \{0,1\}^n \to \{0,1\}$ all requiring $T(n)$ depth, consider...

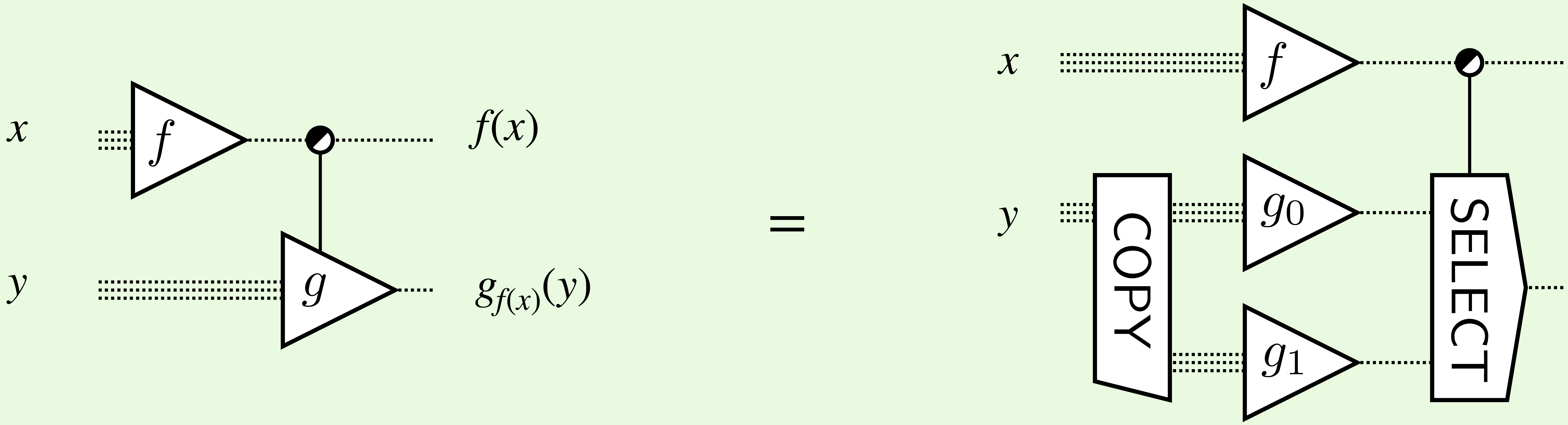


Naive depth: $T(n) + T(n)$

$= 2T(n)$

Quantum parallelization: a fundamental difference?

Example (Classical)**.** With $f, g_0, g_1 : \{0,1\}^n \to \{0,1\}$ all requiring $T(n)$ depth, consider...

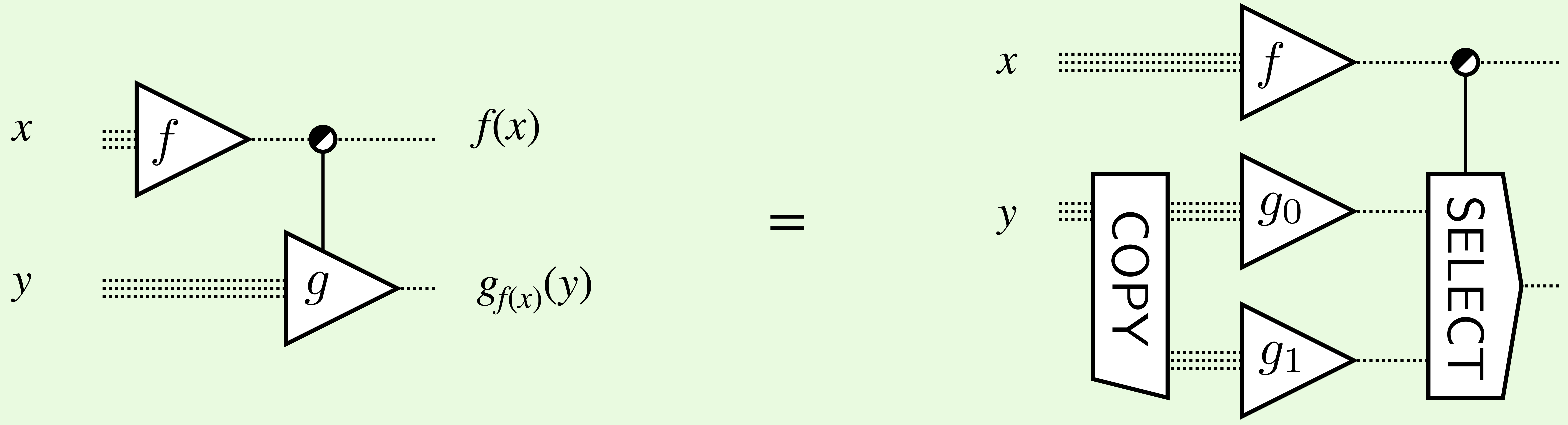


Naive depth: $T(n) + T(n)$

$= 2T(n)$

Quantum parallelization: a fundamental difference?

Example (Classical). With $f, g_0, g_1 : \{0,1\}^n \to \{0,1\}$ all requiring $T(n)$ depth, consider...

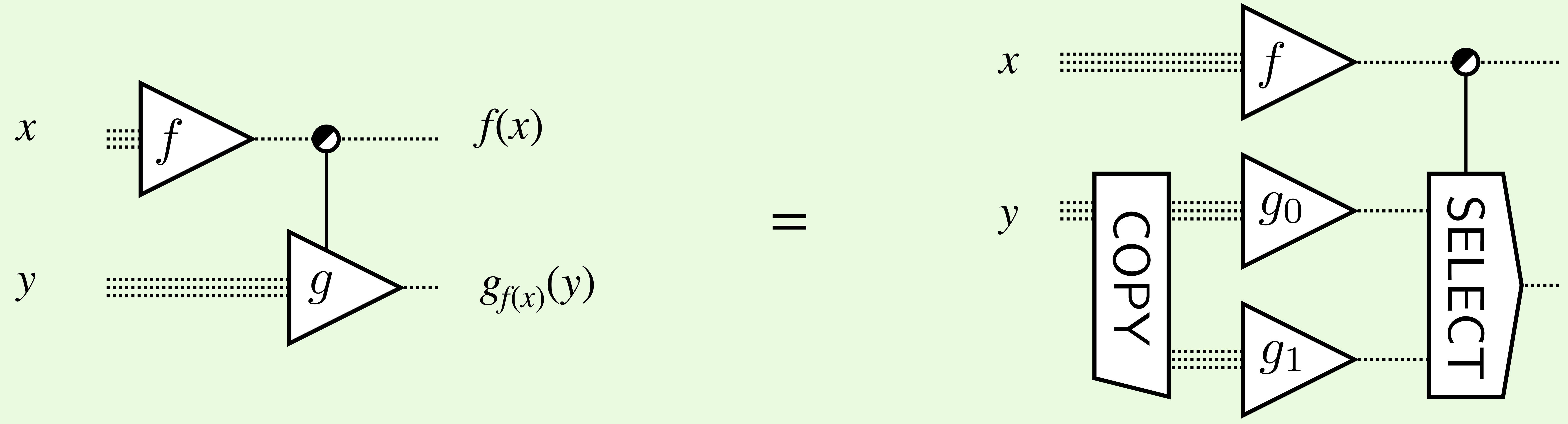


Naive depth: $T(n) + T(n) = 2T(n)$

Improved depth: $O(1) + T(n) + O(1) = T(n) + O(1)$

Quantum parallelization: a fundamental difference?

Example (Classical)**.** With $f, g_0, g_1 : \{0,1\}^n \to \{0,1\}$ all requiring $T(n)$ depth, consider...



Naive depth: $T(n) + T(n) = 2T(n)$

Improved depth: $O(1) + T(n) + O(1) = T(n) + O(1)$

Upshot: a precomputation trick halved computation time

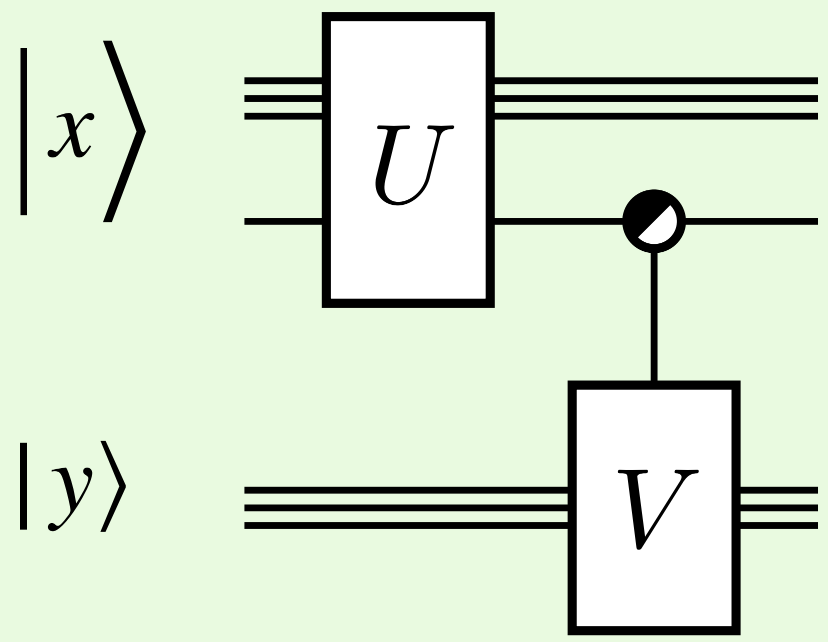
Quantum parallelization: a fundamental difference?

Quantum parallelization: a fundamental difference?

Example (Quantum)**.** With U, V_0, V_1 n-qubit unitaries requiring $T(n)$ depth, consider...

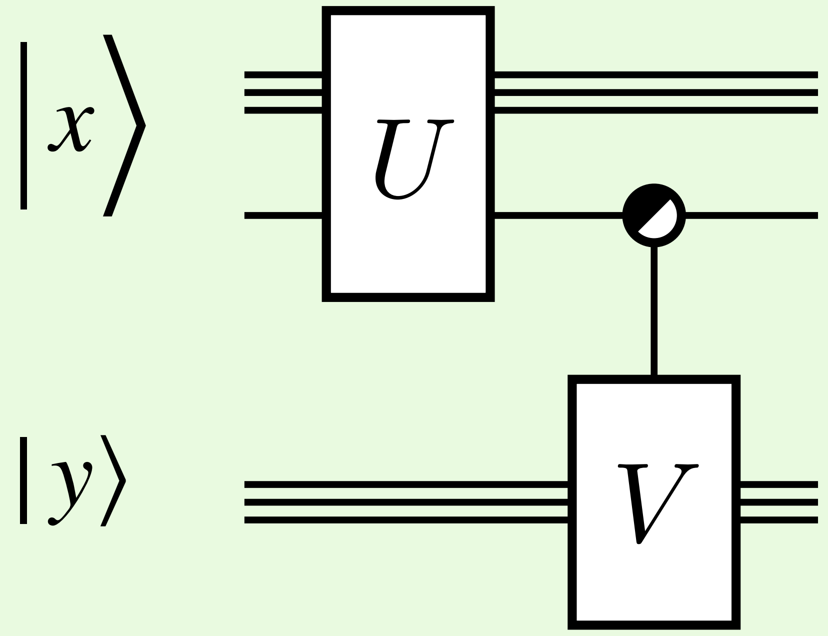
Quantum parallelization: a fundamental difference?

Example (Quantum)**.** With U, V_0, V_1 n-qubit unitaries requiring $T(n)$ depth, consider...

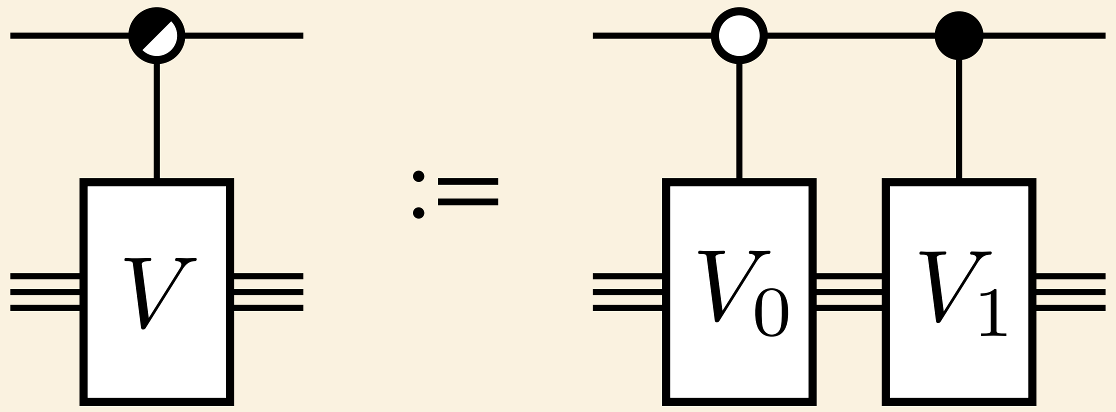


Quantum parallelization: a fundamental difference?

Example (Quantum)**.** With U, V_0, V_1 n-qubit unitaries requiring $T(n)$ depth, consider...



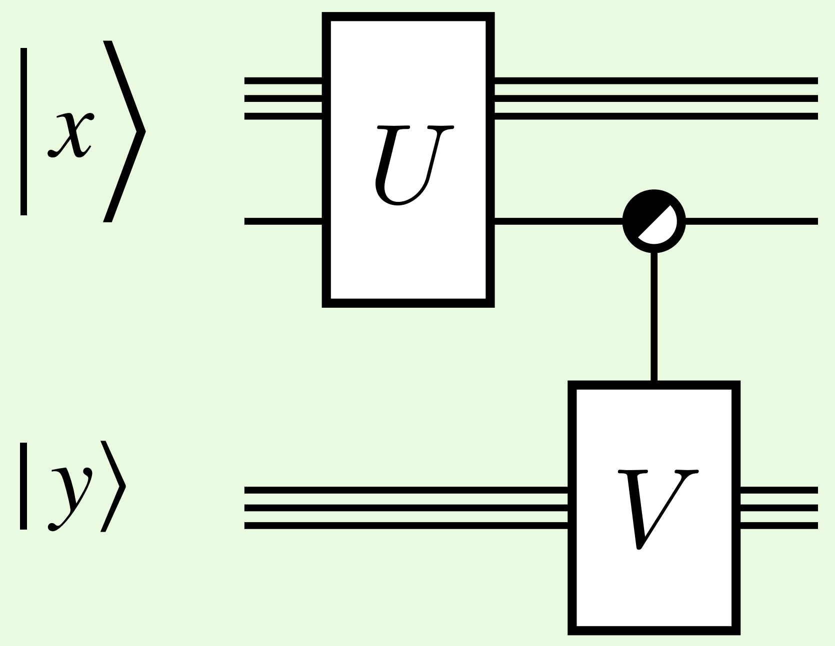
Notation.



$$= \begin{pmatrix} V_0 & \mathbf{0} \\ \mathbf{0} & V_1 \end{pmatrix}$$

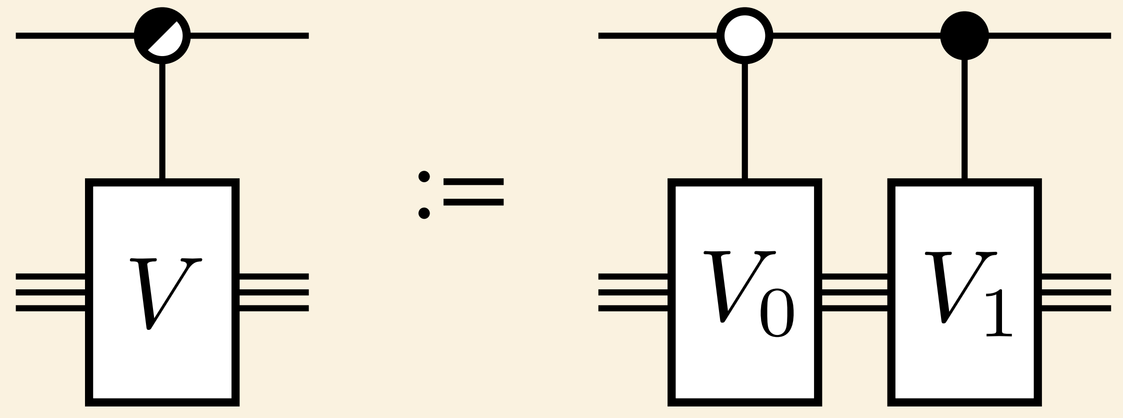
Quantum parallelization: a fundamental difference?

Example (Quantum). With U, V_0, V_1 n-qubit unitaries requiring $T(n)$ depth, consider...



Naive depth: $T(n) + T(n) = 2T(n)$

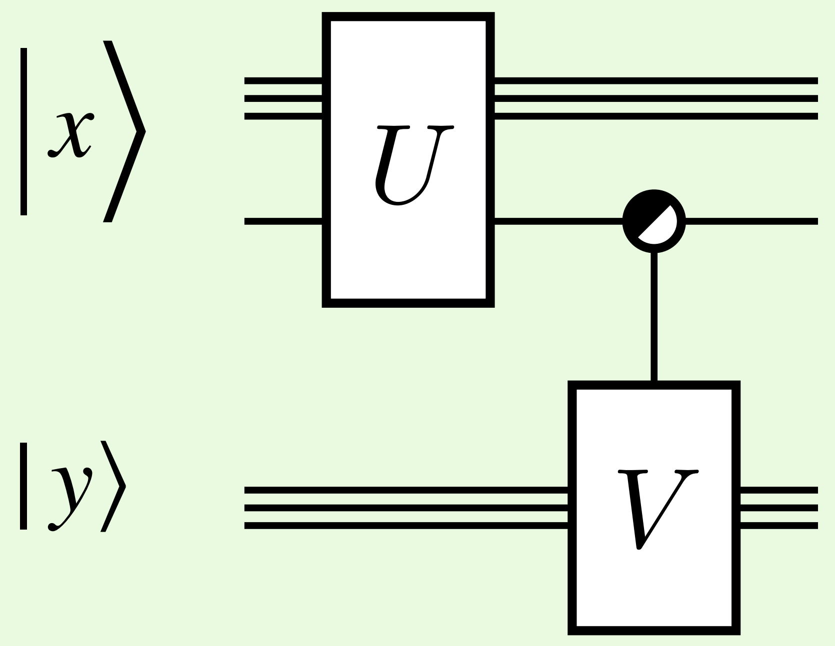
Notation.



$$= \begin{pmatrix} V_0 & \mathbf{0} \\ \mathbf{0} & V_1 \end{pmatrix}$$

Quantum parallelization: a fundamental difference?

Example (Quantum). With U, V_0, V_1 n-qubit unitaries requiring $T(n)$ depth, consider...

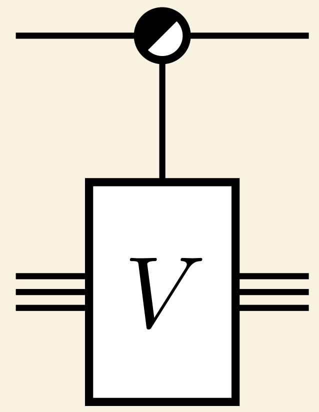


$=$ **?**

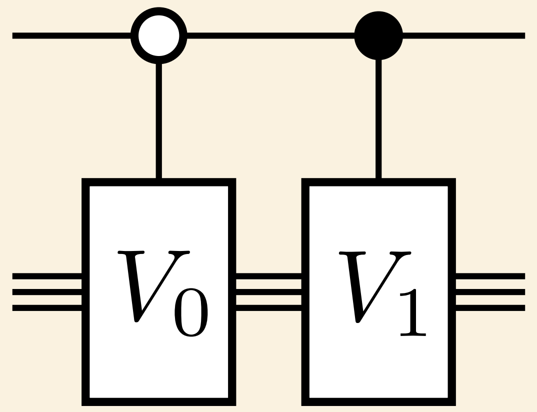
Naive depth: $T(n) + T(n)$

$= 2T(n)$

Notation.



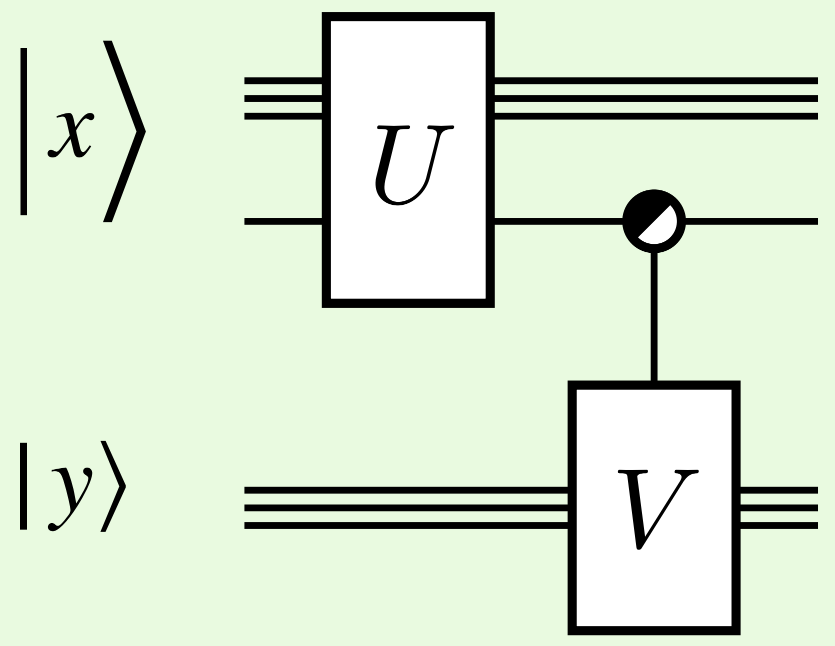
$:=$



$= \begin{pmatrix} V_0 & \mathbf{0} \\ \mathbf{0} & V_1 \end{pmatrix}$

Quantum parallelization: a fundamental difference?

Example (Quantum)**.** With U, V_0, V_1 n-qubit unitaries requiring $T(n)$ depth, consider...



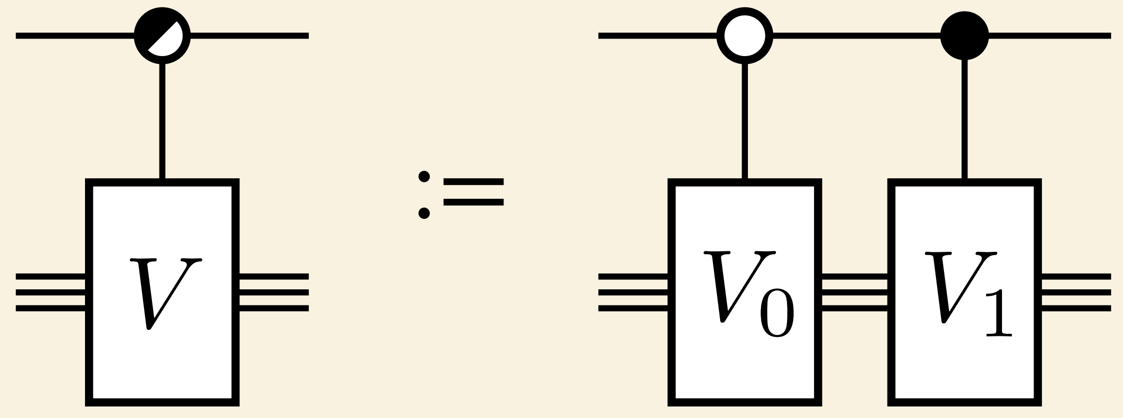
$=$ **?**

Apparent obstruction from no-cloning

Naive depth: $T(n) + T(n)$

$= 2T(n)$

Notation.



$$:= \quad = \begin{pmatrix} V_0 & \mathbf{0} \\ \mathbf{0} & V_1 \end{pmatrix}$$

The Moore–Nilsson conjecture

Parallel Quantum Computation and Quantum Codes

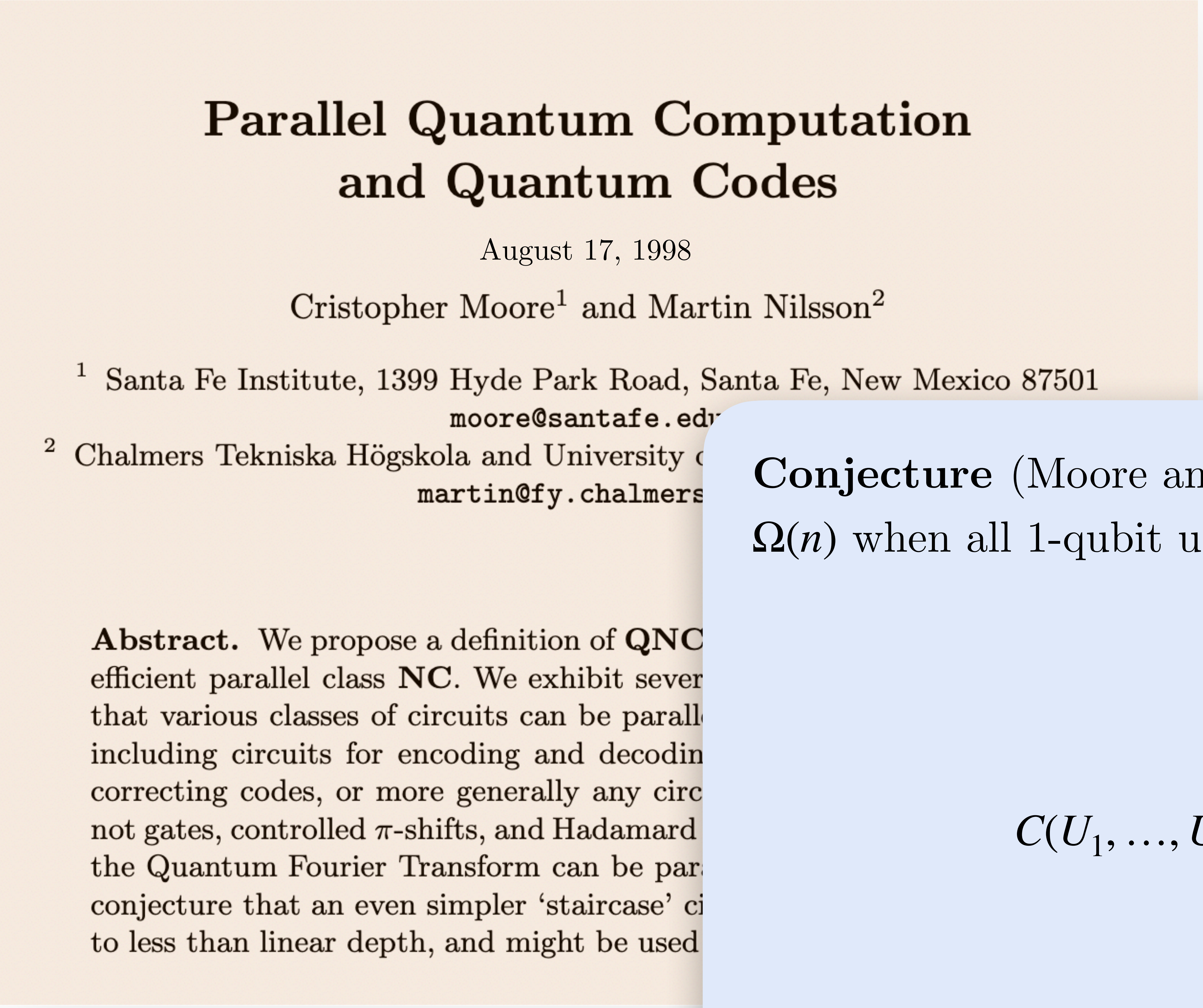
August 17, 1998

Cristopher Moore[1] and Martin Nilsson[2]

[1] Santa Fe Institute, 1399 Hyde Park Road, Santa Fe, New Mexico 87501
moore@santafe.edu
[2] Chalmers Tekniska Högskola and University of Göteborg, Göteborg, Sweden
martin@fy.chalmers.se

Abstract. We propose a definition of **QNC**, the quantum analog of the efficient parallel class **NC**. We exhibit several useful gadgets and prove that various classes of circuits can be parallelized to logarithmic depth, including circuits for encoding and decoding standard quantum error-correcting codes, or more generally any circuit consisting of controlled-not gates, controlled π-shifts, and Hadamard gates. Finally, while we note the Quantum Fourier Transform can be parallelized to linear depth, we conjecture that an even simpler 'staircase' circuit cannot be parallelized to less than linear depth, and might be used to prove that $\mathbf{QNC} < \mathbf{QP}$.

The Moore–Nilsson conjecture



Parallel Quantum Computation
and Quantum Codes

August 17, 1998

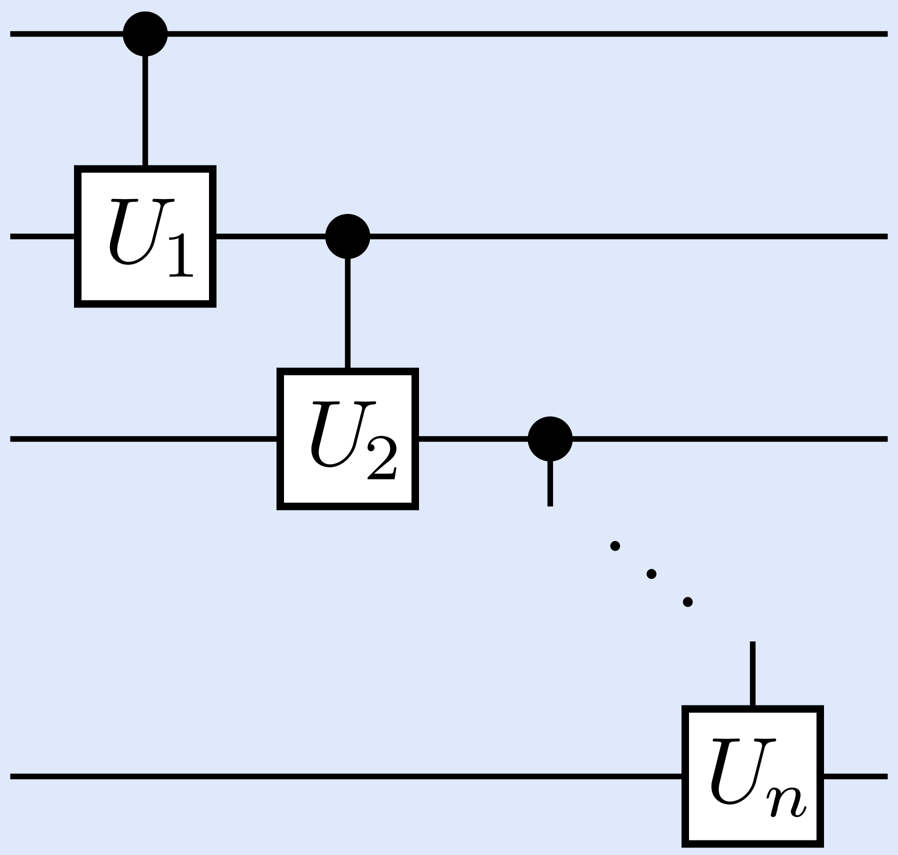
Cristopher Moore[1] and Martin Nilsson[2]

[1] Santa Fe Institute, 1399 Hyde Park Road, Santa Fe, New Mexico 87501
moore@santafe.edu
[2] Chalmers Tekniska Högskola and University o
martin@fy.chalmers

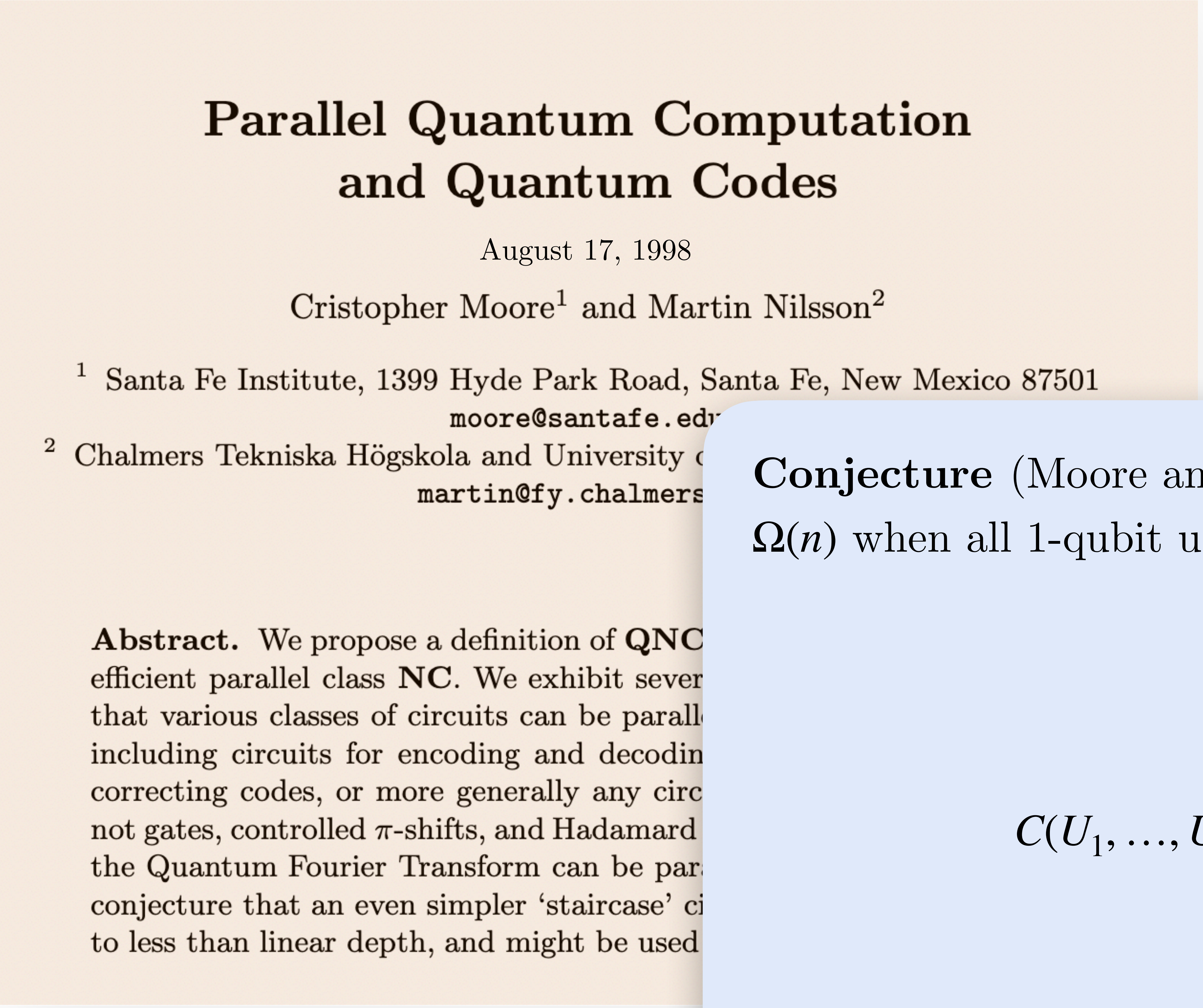
Abstract. We propose a definition of **QNC**
efficient parallel class **NC**. We exhibit sever
that various classes of circuits can be parall
including circuits for encoding and decodin
correcting codes, or more generally any circ
not gates, controlled π-shifts, and Hadamard
the Quantum Fourier Transform can be par
conjecture that an even simpler 'staircase' ci
to less than linear depth, and might be used

Conjecture (Moore and Nilsson, 1998)**.** The following unitary has minimum depth $\Omega(n)$ when all 1-qubit unitaries $U_1, \ldots, U_n$ are not diagonal or anti-diagonal.

$$C(U_1, \ldots, U_n) \quad :=$$



The Moore–Nilsson conjecture


Parallel Quantum Computation and Quantum Codes

August 17, 1998

Cristopher Moore[1] and Martin Nilsson[2]

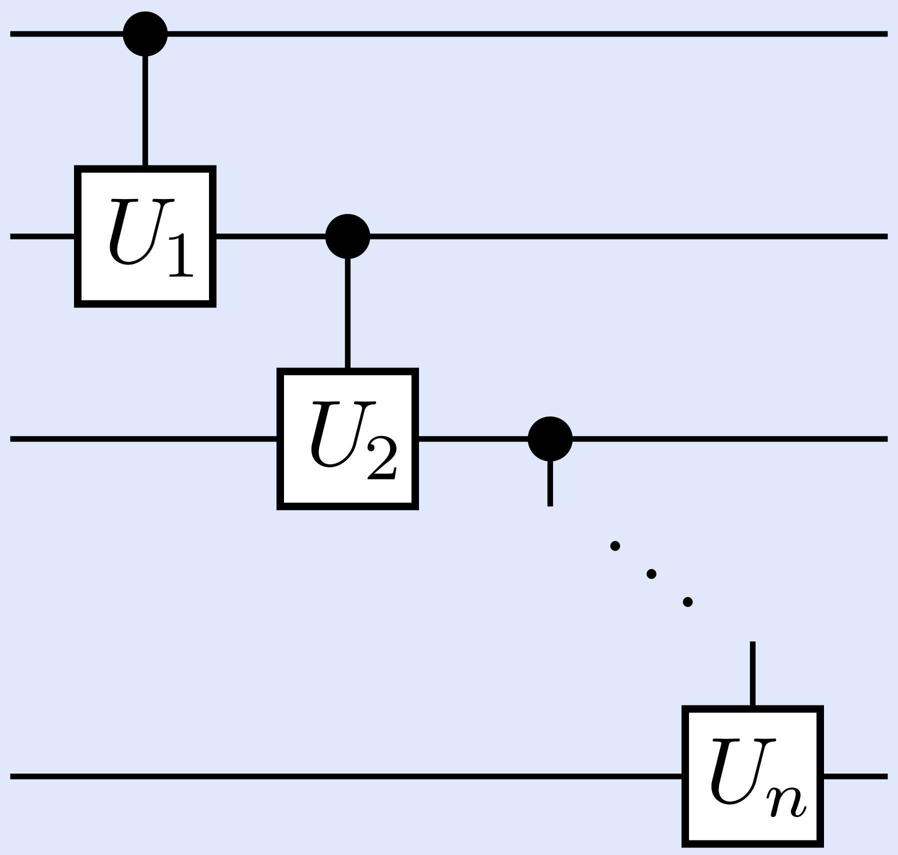
[1] Santa Fe Institute, 1399 Hyde Park Road, Santa Fe, New Mexico 87501
moore@santafe.edu
[2] Chalmers Tekniska Högskola and University
martin@fy.chalmers

Abstract. We propose a definition of **QNC**
efficient parallel class **NC**. We exhibit sever
that various classes of circuits can be parall
including circuits for encoding and decodin
correcting codes, or more generally any circ
not gates, controlled π-shifts, and Hadamard
the Quantum Fourier Transform can be par
conjecture that an even simpler 'staircase' ci
to less than linear depth, and might be used

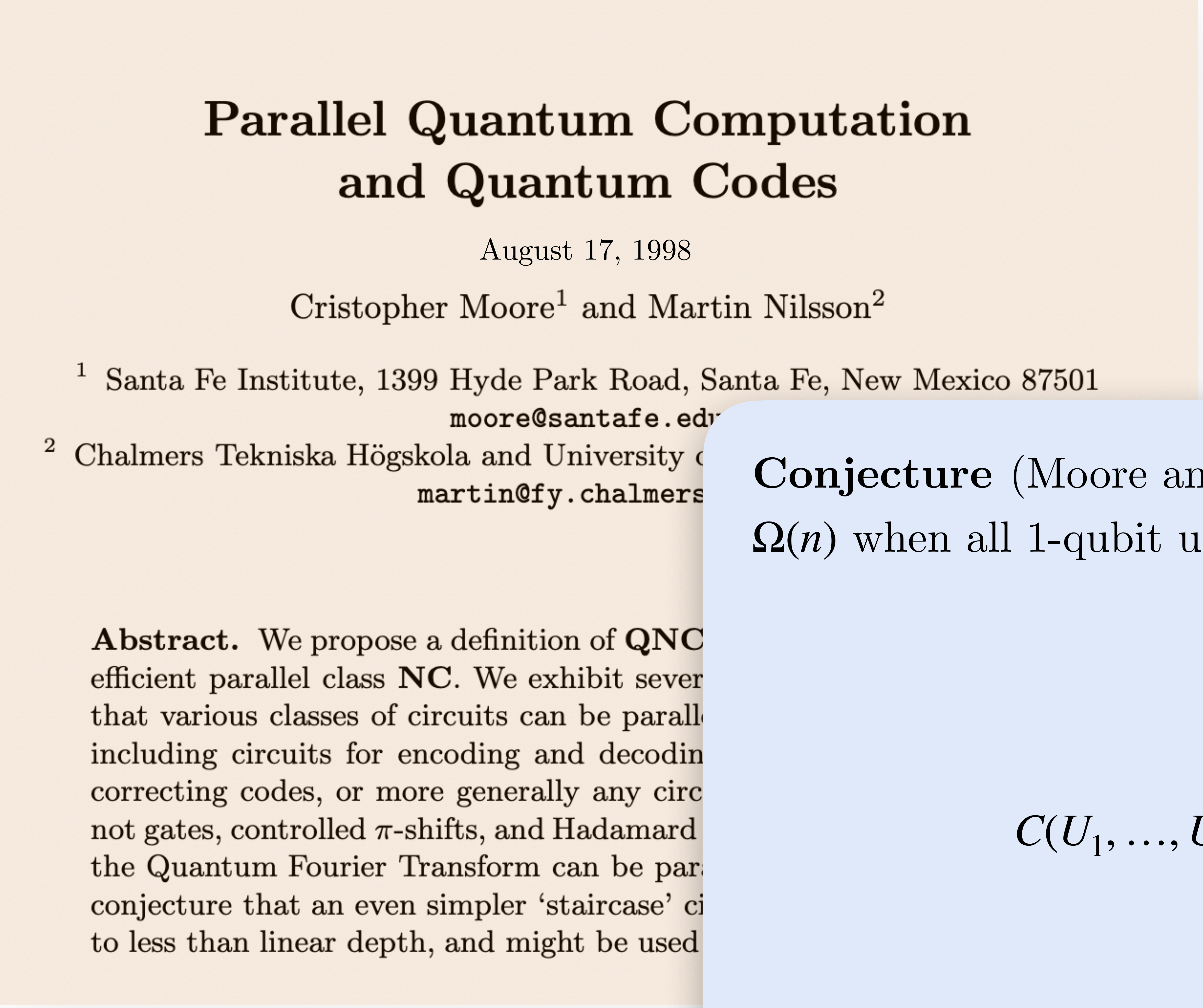
- Seemingly no classical analogue.

Conjecture (Moore and Nilsson, 1998)**.** The following unitary has minimum depth $\Omega(n)$ when all 1-qubit unitaries $U_1, \ldots, U_n$ are not diagonal or anti-diagonal.

$$C(U_1, \ldots, U_n) \quad :=$$



The Moore–Nilsson conjecture


Parallel Quantum Computation and Quantum Codes

August 17, 1998

Cristopher Moore[1] and Martin Nilsson[2]

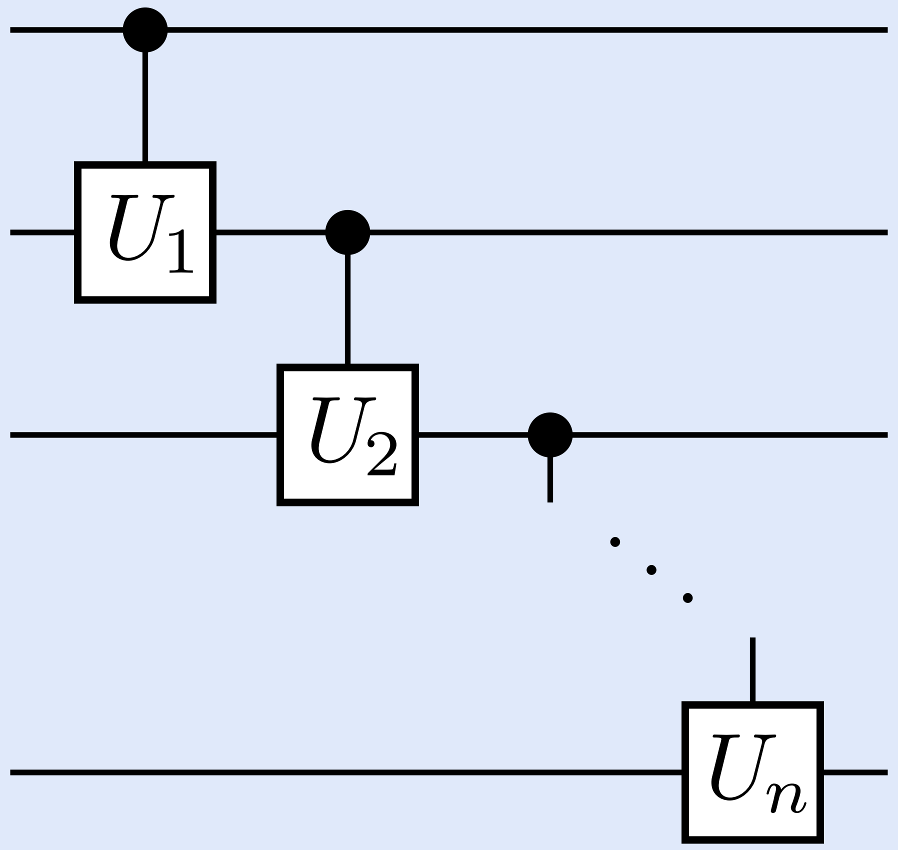
[1] Santa Fe Institute, 1399 Hyde Park Road, Santa Fe, New Mexico 87501
moore@santafe.edu
[2] Chalmers Tekniska Högskola and University of
martin@fy.chalmers

Abstract. We propose a definition of **QNC**
efficient parallel class **NC**. We exhibit sever
that various classes of circuits can be parall
including circuits for encoding and decodin
correcting codes, or more generally any circ
not gates, controlled π-shifts, and Hadamard
the Quantum Fourier Transform can be par
conjecture that an even simpler 'staircase' ci
to less than linear depth, and might be used

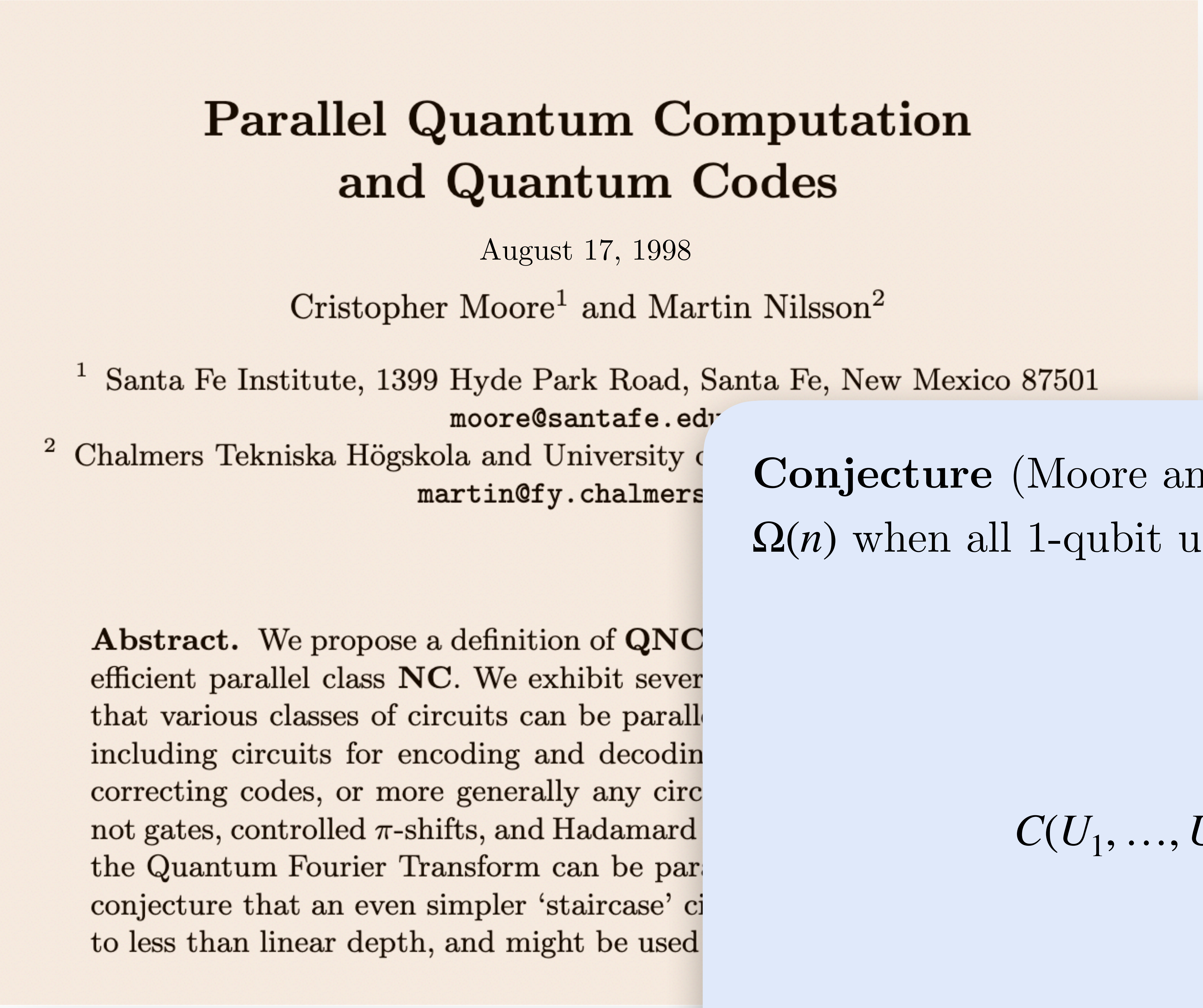
- Seemingly no classical analogue.
- Appealing candidate for "inherently sequential" unitary.

Conjecture (Moore and Nilsson, 1998)**.** The following unitary has minimum depth $\Omega(n)$ when all 1-qubit unitaries $U_1, \ldots, U_n$ are not diagonal or anti-diagonal.

$$C(U_1, \ldots, U_n) \quad :=$$



The Moore–Nilsson conjecture


Parallel Quantum Computation and Quantum Codes

August 17, 1998

Cristopher Moore[1] and Martin Nilsson[2]

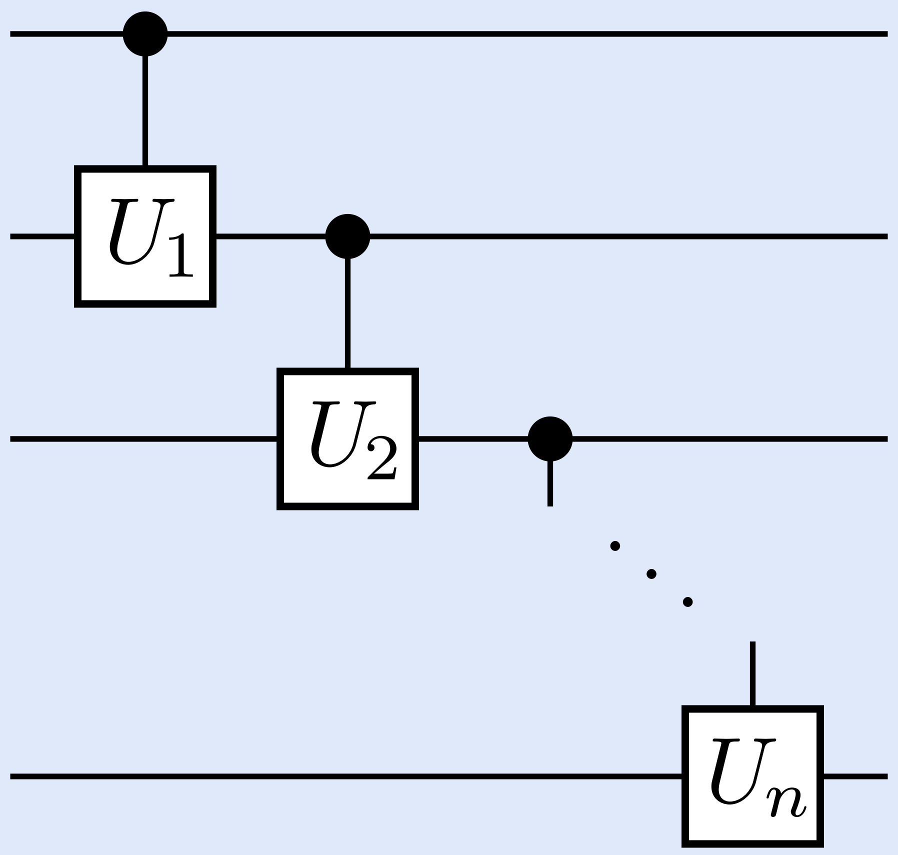
[1] Santa Fe Institute, 1399 Hyde Park Road, Santa Fe, New Mexico 87501
moore@santafe.edu
[2] Chalmers Tekniska Högskola and University o
martin@fy.chalmers

Abstract. We propose a definition of **QNC**
efficient parallel class **NC**. We exhibit sever
that various classes of circuits can be parall
including circuits for encoding and decodin
correcting codes, or more generally any circ
not gates, controlled π-shifts, and Hadamard
the Quantum Fourier Transform can be par
conjecture that an even simpler 'staircase' ci
to less than linear depth, and might be used

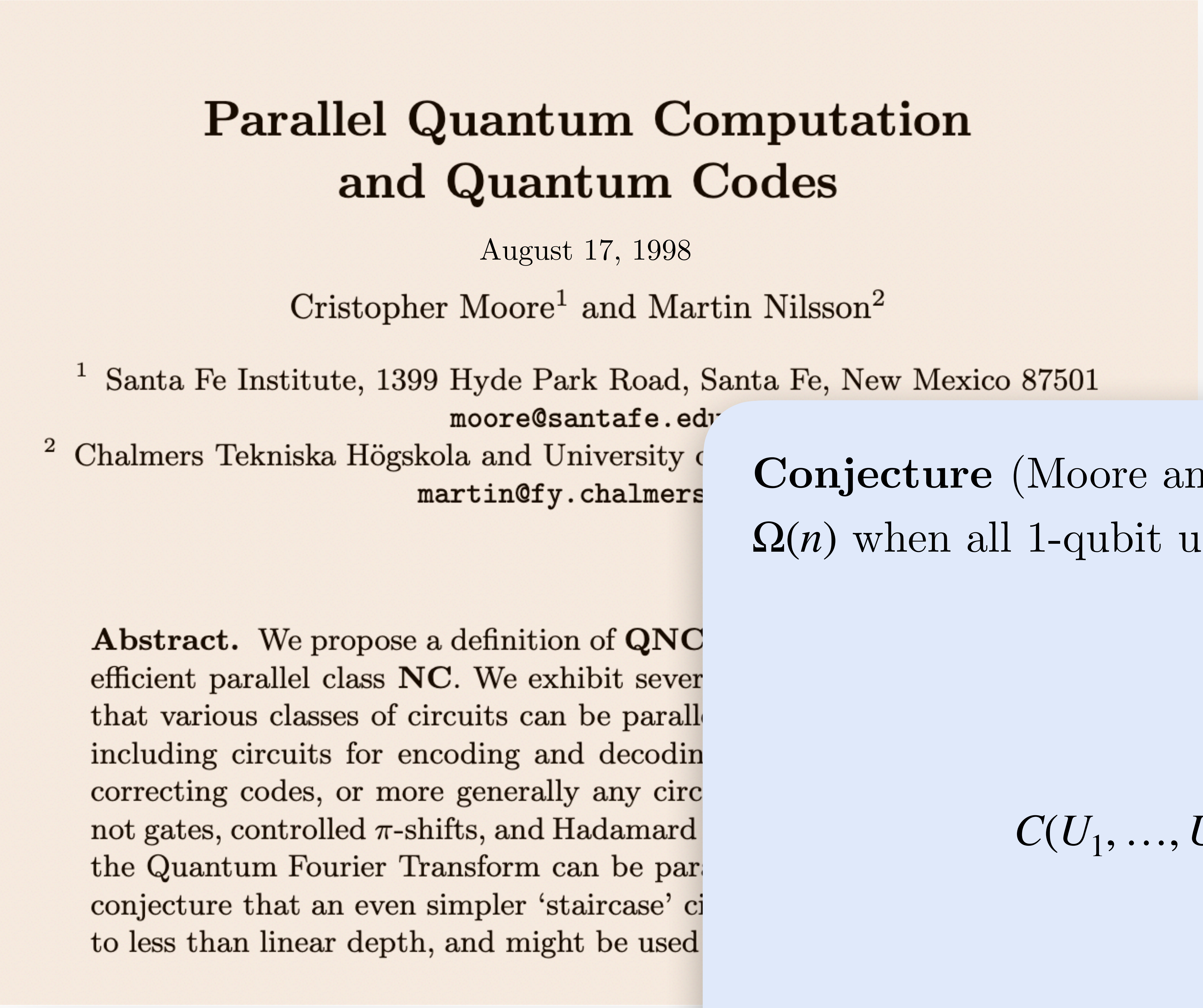
- Seemingly no classical analogue.
- Appealing candidate for "inherently sequential" unitary.
  - Simple quantum circuits cannot be parallelized?

Conjecture (Moore and Nilsson, 1998)**.** The following unitary has minimum depth $\Omega(n)$ when all 1-qubit unitaries $U_1, \ldots, U_n$ are not diagonal or anti-diagonal.

$$C(U_1, \ldots, U_n) \quad :=$$



The Moore–Nilsson conjecture



Parallel Quantum Computation
and Quantum Codes

August 17, 1998

Cristopher Moore[1] and Martin Nilsson[2]

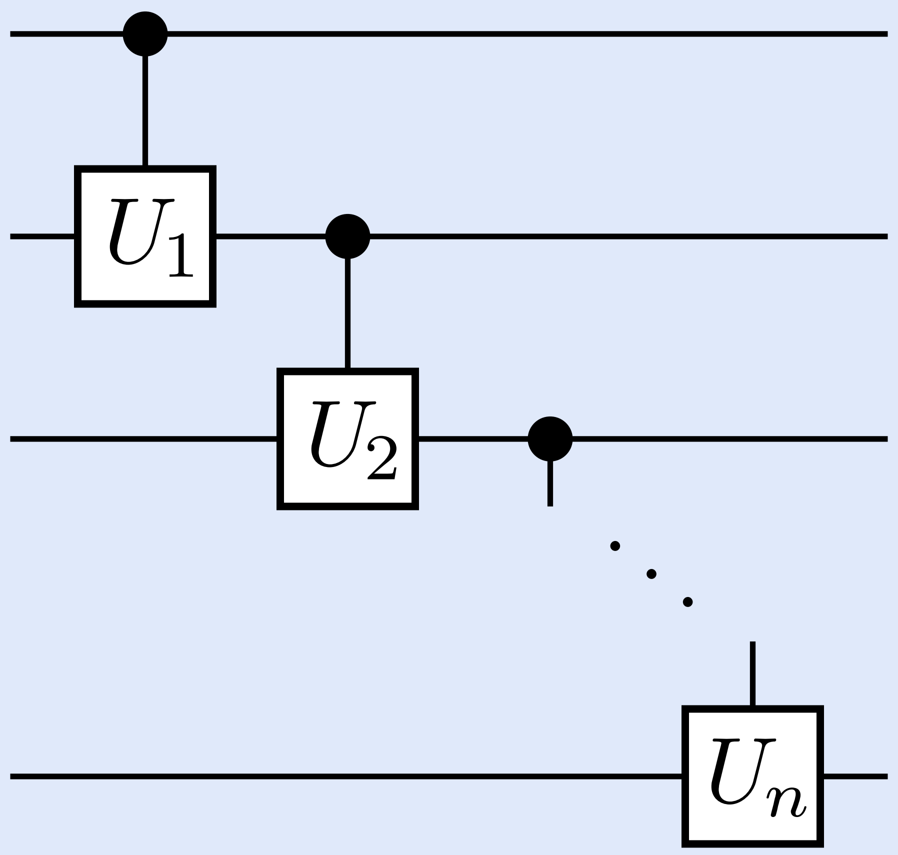
[1] Santa Fe Institute, 1399 Hyde Park Road, Santa Fe, New Mexico 87501
moore@santafe.edu
[2] Chalmers Tekniska Högskola and University o
martin@fy.chalmers

Abstract. We propose a definition of **QNC**
efficient parallel class **NC**. We exhibit sever
that various classes of circuits can be parall
including circuits for encoding and decodin
correcting codes, or more generally any circ
not gates, controlled π-shifts, and Hadamard
the Quantum Fourier Transform can be par
conjecture that an even simpler 'staircase' ci
to less than linear depth, and might be used

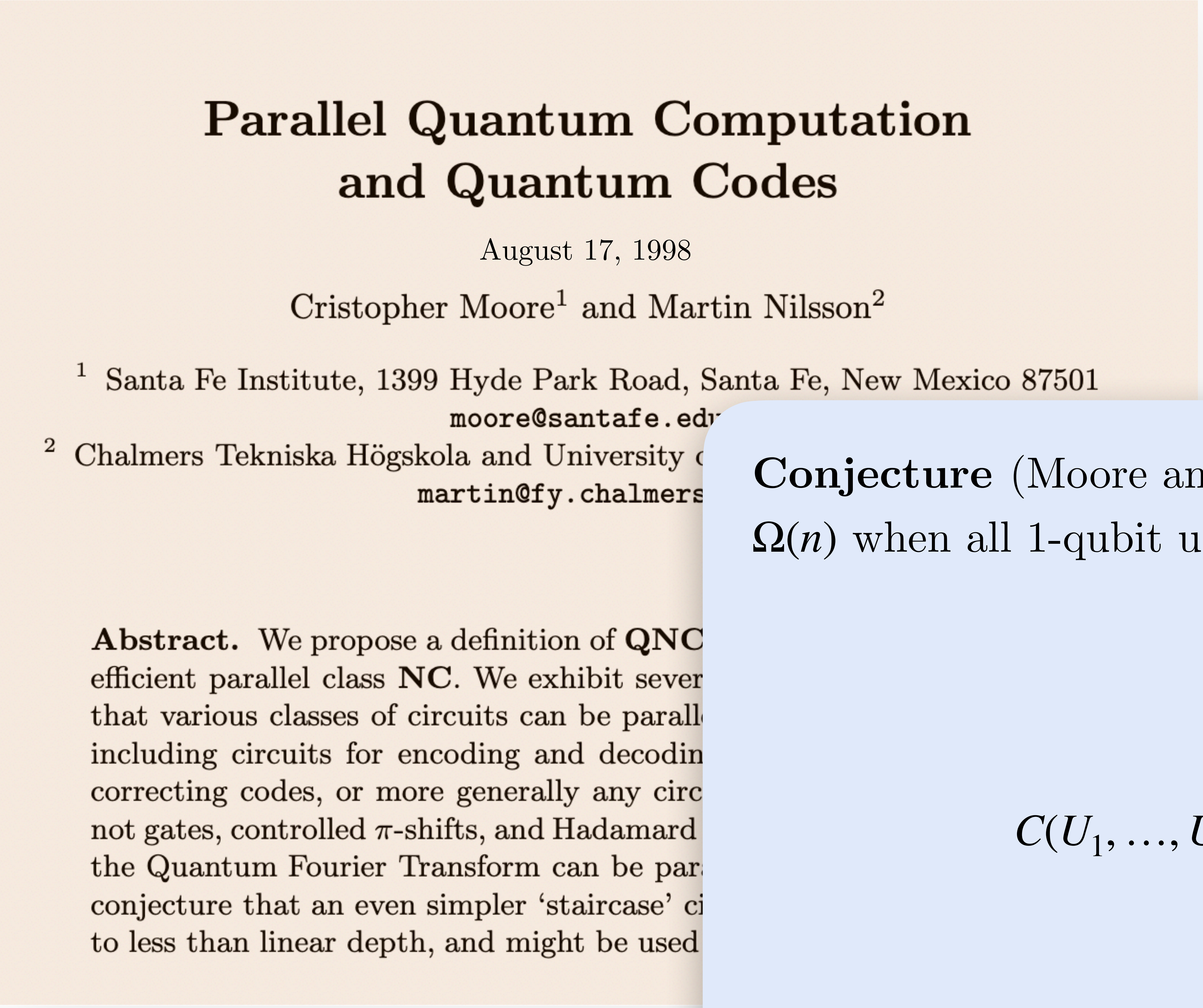
- Seemingly no classical analogue.
- Appealing candidate for "inherently sequential" unitary.
  - Simple quantum circuits cannot be parallelized?
  - Large coherence times necessary for quantum computing?

Conjecture (Moore and Nilsson, 1998)**.** The following unitary has minimum depth $\Omega(n)$ when all 1-qubit unitaries $U_1, \ldots, U_n$ are not diagonal or anti-diagonal.

$C(U_1, \ldots, U_n) \quad :=$



The Moore–Nilsson conjecture


Parallel Quantum Computation and Quantum Codes

August 17, 1998

Cristopher Moore[1] and Martin Nilsson[2]

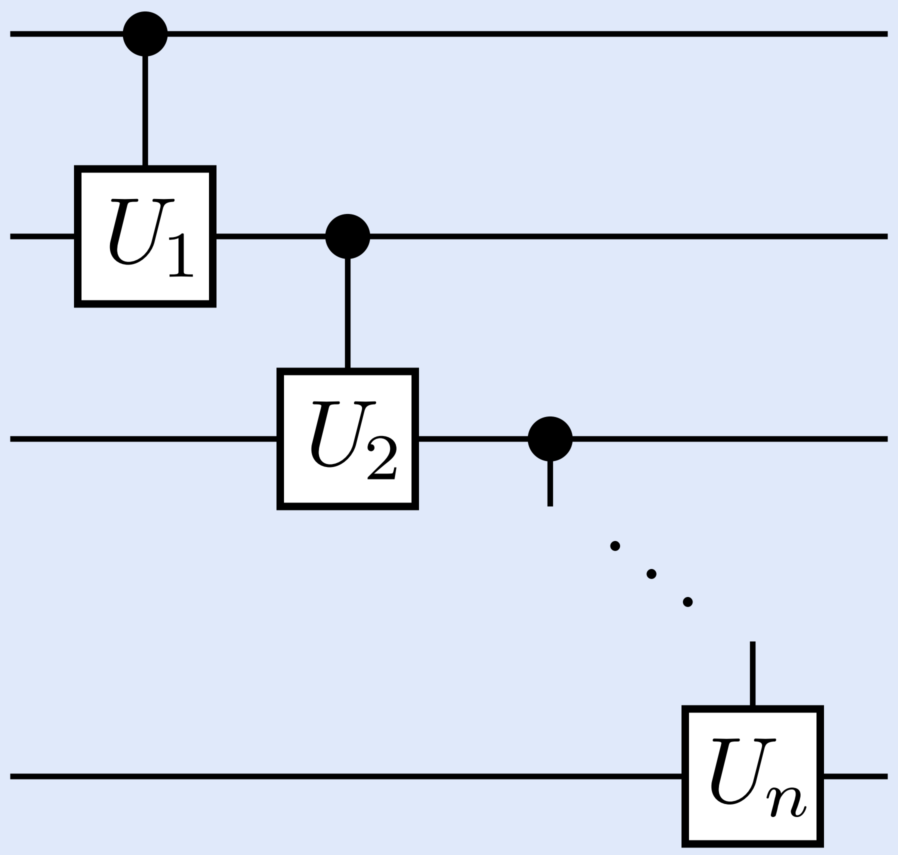
[1] Santa Fe Institute, 1399 Hyde Park Road, Santa Fe, New Mexico 87501
moore@santafe.edu
[2] Chalmers Tekniska Högskola and University o
martin@fy.chalmers

Abstract. We propose a definition of **QNC**
efficient parallel class **NC**. We exhibit sever
that various classes of circuits can be parall
including circuits for encoding and decodin
correcting codes, or more generally any circ
not gates, controlled π-shifts, and Hadamard
the Quantum Fourier Transform can be par
conjecture that an even simpler 'staircase' ci
to less than linear depth, and might be used

- Seemingly no classical analogue.
- Appealing candidate for "inherently sequential" unitary.
  - Simple quantum circuits cannot be parallelized?
  - Large coherence times necessary for quantum computing?
  - Schemes for verifying device depth?

Conjecture (Moore and Nilsson, 1998)**.** The following unitary has minimum depth $\Omega(n)$ when all 1-qubit unitaries $U_1, \ldots, U_n$ are not diagonal or anti-diagonal.

$$C(U_1, \ldots, U_n) \quad :=$$



The Moore–Nilsson conjecture highlights dual motivations for studying quantum parallelization:

The Moore–Nilsson conjecture highlights dual motivations for studying quantum parallelization:

- Need for quantum parallelization techniques: can we at least recover quantum versions of classical parallelization ideas?

The Moore–Nilsson conjecture highlights dual motivations for studying quantum parallelization:

- Need for quantum <u>parallelization techniques</u>: can we at least recover quantum versions of classical parallelization ideas?

- <u>Depth lower bounds</u> for quantum problems? Maybe it's easier to prove *quantum* transformations are inherently sequential? Separate quantum-input QNC from BQP?

Our results

Our results

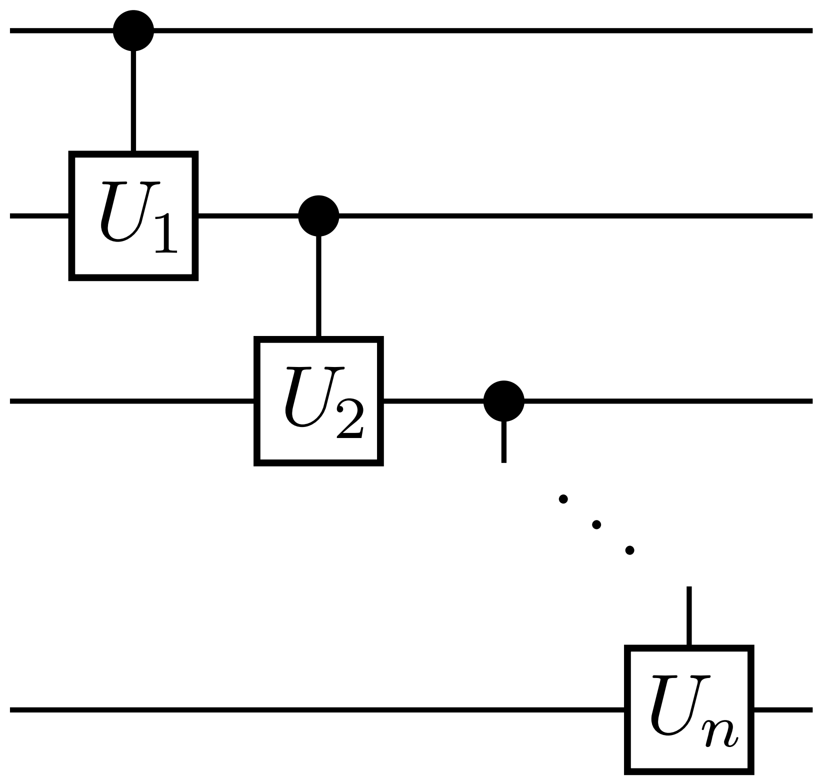
1. Moore–Nilsson unitaries have $O(\log n)$-depth circuits

Our results

1. Moore–Nilsson unitaries have $O(\log n)$-depth circuits

Theorem. For any 1-qubit unitaries $U_1, \ldots, U_n$, the unitary

$$C(U_1, \ldots, U_n) \quad :=$$



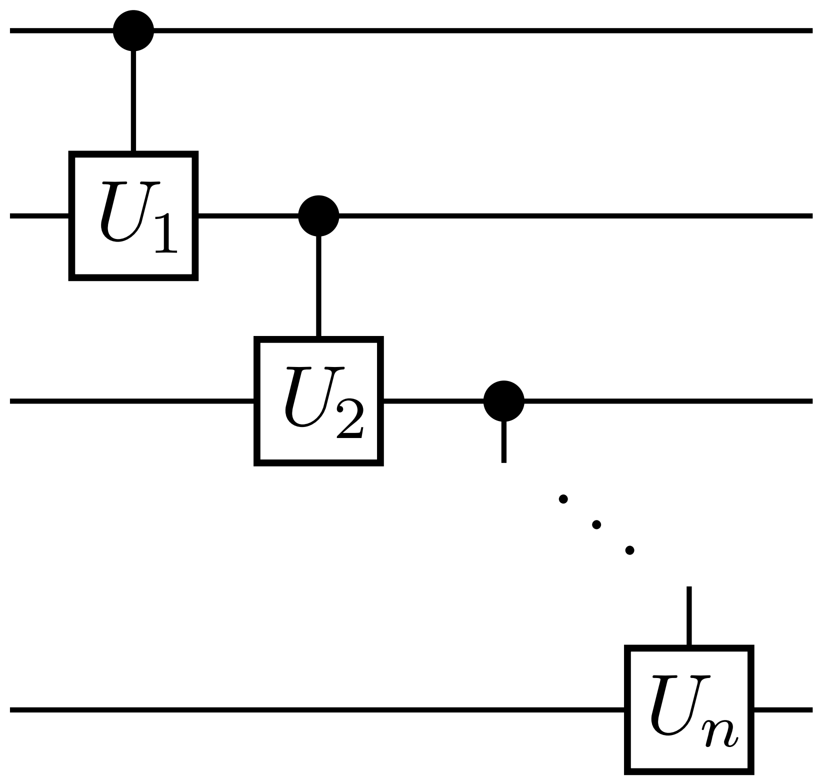
has an exact, ancilla-free circuit of depth $O(\log n)$.

Our results

1. Moore–Nilsson unitaries have $O(\log n)$-depth circuits

Theorem. For any 1-qubit unitaries $U_1, \ldots, U_n$, the unitary

$C(U_1, \ldots, U_n) \quad :=$



has an exact, ancilla-free circuit of depth $O(\log n)$.

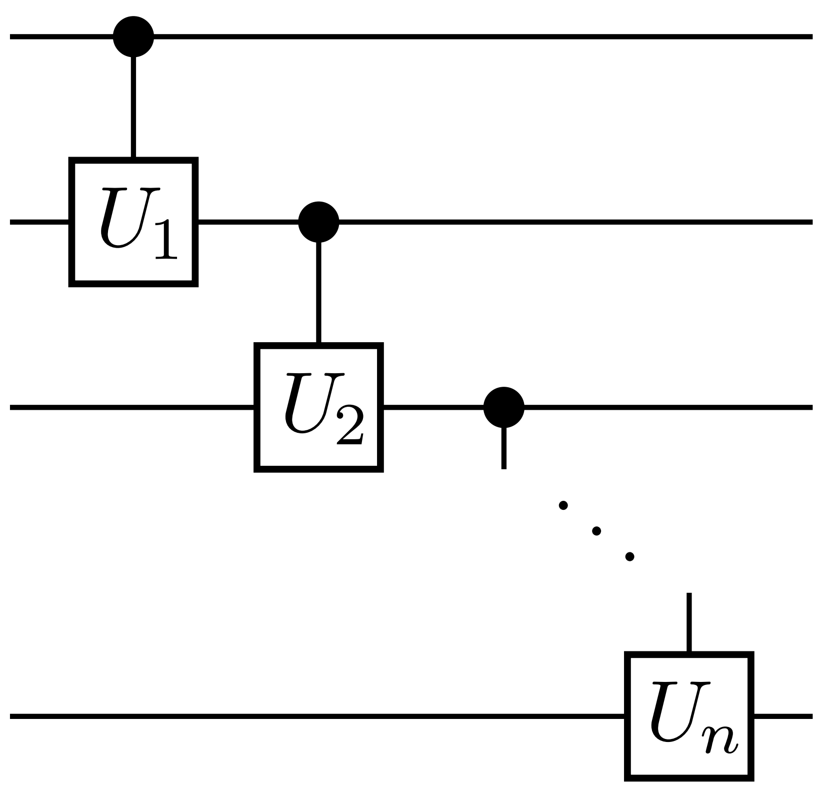
Bonus: in regime of 2D geometrically-local circuits: $O(\sqrt{n})$ depth, $O(n)$ ancillae

Our results

1. Moore–Nilsson unitaries have $O(\log n)$-depth circuits

Theorem. For any 1-qubit unitaries $U_1, \ldots, U_n$, the unitary

$C(U_1, \ldots, U_n) \quad :=$



has an exact, ancilla-free circuit of depth $O(\log n)$.

Bonus: in regime of 2D geometrically-local circuits: $O(\sqrt{n})$ depth, $O(n)$ ancillae

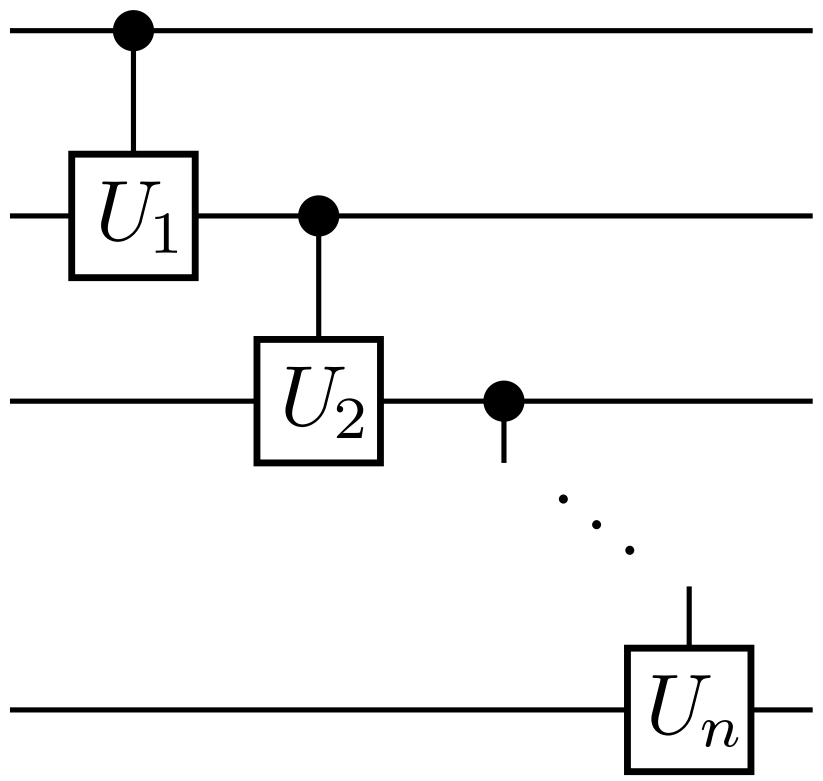
2. Depth reductions for general "control-cascade circuits"

Our results

1. Moore–Nilsson unitaries have $O(\log n)$-depth circuits

Theorem. For any 1-qubit unitaries $U_1, \ldots, U_n$, the unitary

$$C(U_1, \ldots, U_n) \quad :=$$



has an exact, ancilla-free circuit of depth $O(\log n)$.

Bonus: in regime of 2D geometrically-local circuits: $O(\sqrt{n})$ depth, $O(n)$ ancillae

2. Depth reductions for general "control-cascade circuits"

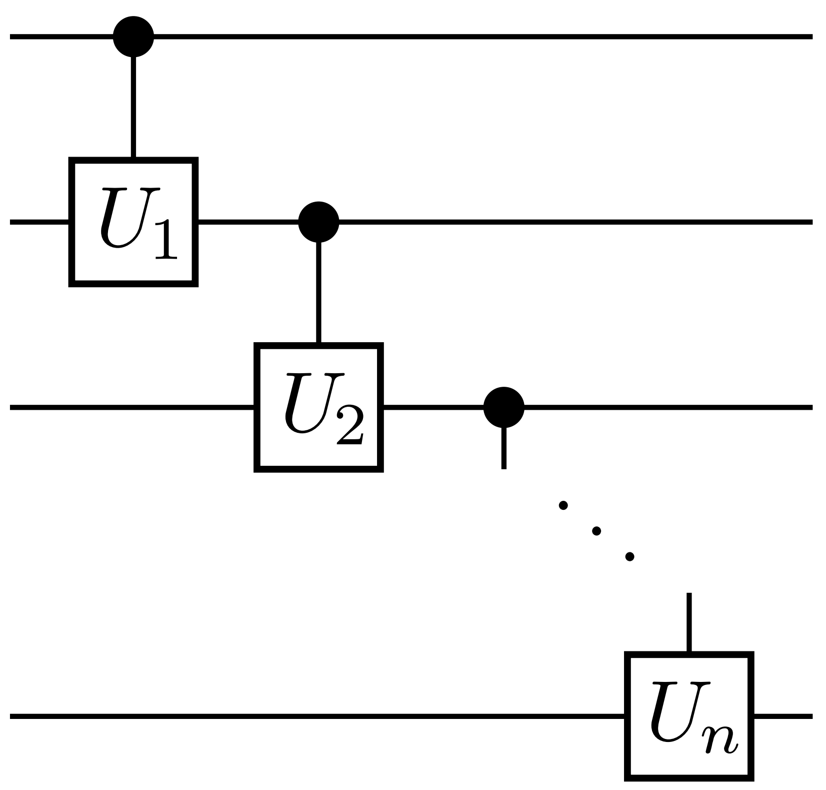
Example corollary. For all $(2 \log n)$-qubit unitaries $U_1, \ldots, U_n$, the unitary $C(U_1, \ldots, U_n)$ has an exact circuit of depth $O(n \log n)$ using $O(n^{3/2})$ ancillae.

Our results

1. Moore–Nilsson unitaries have $O(\log n)$-depth circuits

Theorem. For any 1-qubit unitaries $U_1, \ldots, U_n$, the unitary

$$C(U_1, \ldots, U_n) \quad :=$$



has an exact, ancilla-free circuit of depth $O(\log n)$.

Bonus: in regime of 2D geometrically-local circuits: $O(\sqrt{n})$ depth, $O(n)$ ancillae

2. Depth reductions for general "control-cascade circuits"

C.f. the naive depth of $\widetilde{O}(n^2)$

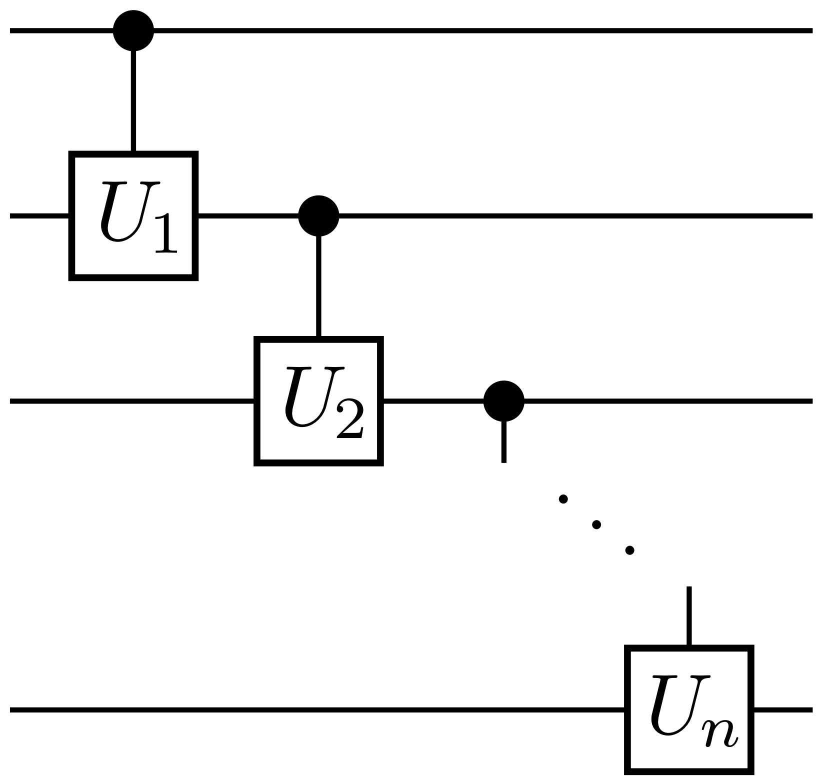
Example corollary. For all $(2\log n)$-qubit unitaries $U_1, \ldots, U_n$, the unitary $C(U_1, \ldots, U_n)$ has an exact circuit of depth $O(n \log n)$ using $O(n^{3/2})$ ancillae.

Our results

1. Moore–Nilsson unitaries have $O(\log n)$-depth circuits

Theorem. For any 1-qubit unitaries $U_1, \dots, U_n$, the unitary

$C(U_1, \dots, U_n) :=$



has an exact, ancilla-free circuit of depth $O(\log n)$.

Bonus: in regime of 2D geometrically-local circuits: $O(\sqrt{n})$ depth, $O(n)$ ancillae

Start here

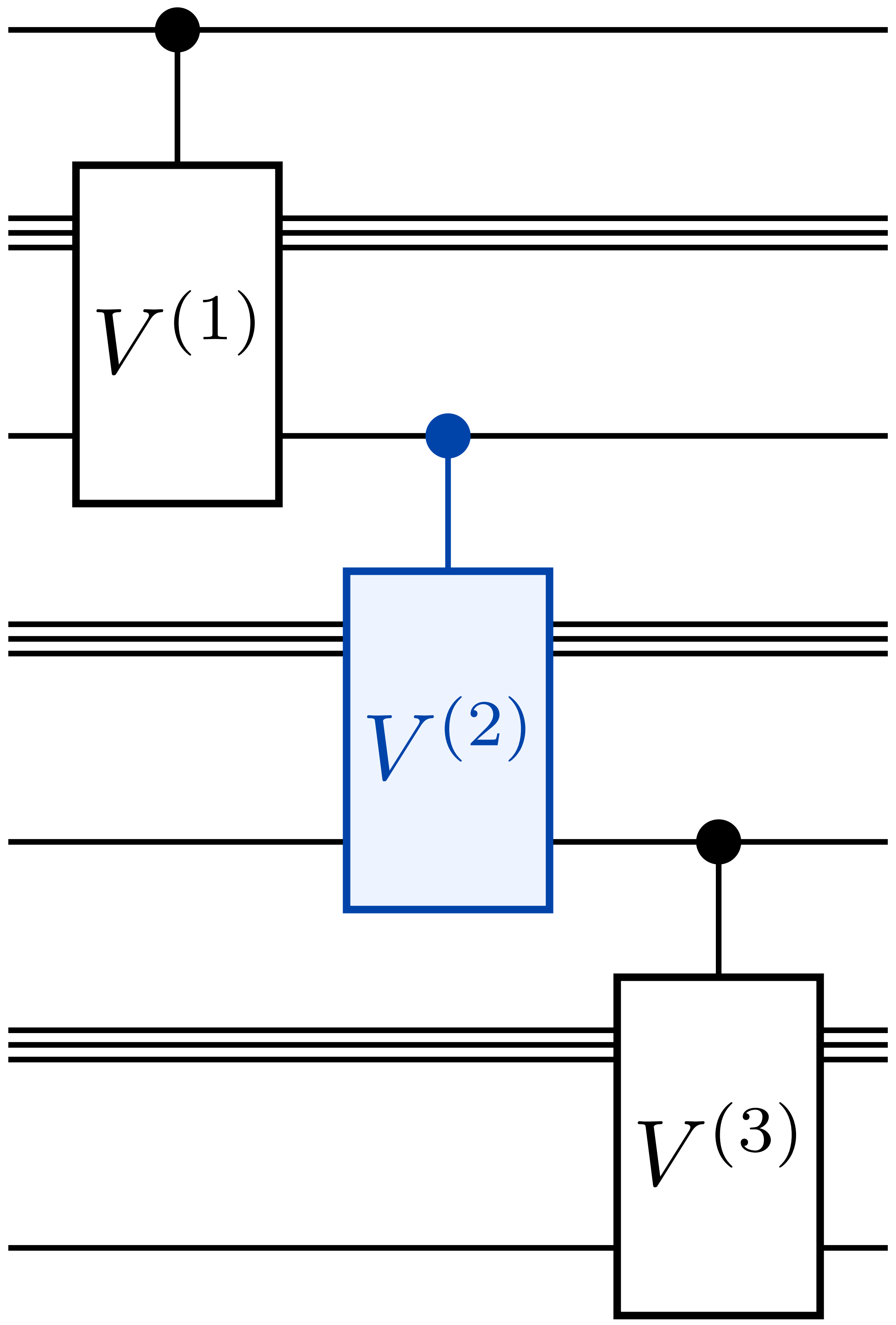
2. Depth reductions for general "control-cascade circuits"

C.f. the naive depth of $\widetilde{O}(n^2)$

Example corollary. For all $(2 \log n)$-qubit unitaries $U_1, \dots, U_n$, the unitary $C(U_1, \dots, U_n)$ has an exact circuit of depth $O(n \log n)$ using $O(n^{3/2})$ ancillae.

Quantum precomputation: some intuition

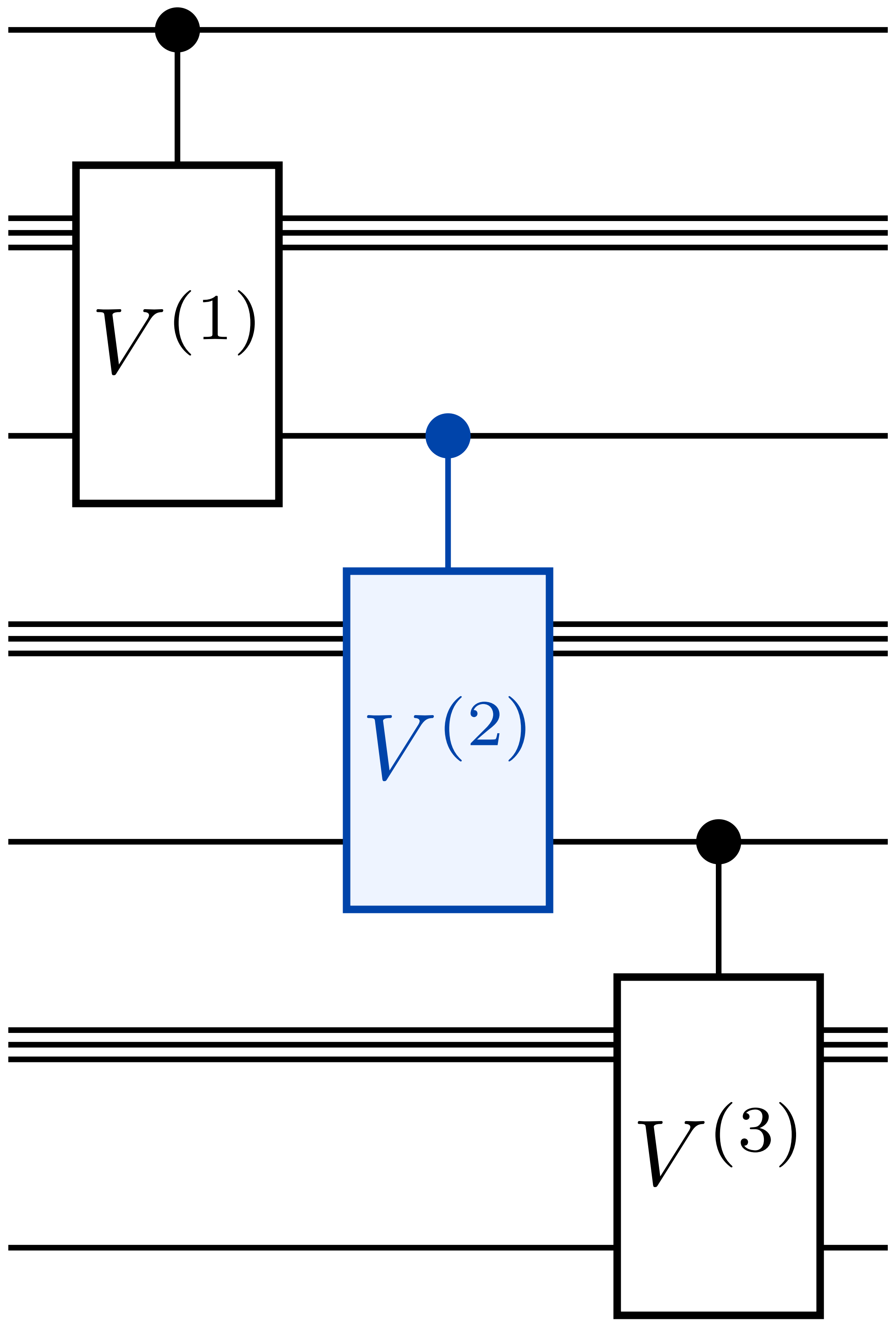
Quantum precomputation: some intuition



Consider a cascade of m-many k-qubit controlled unitaries

Quantum precomputation: some intuition

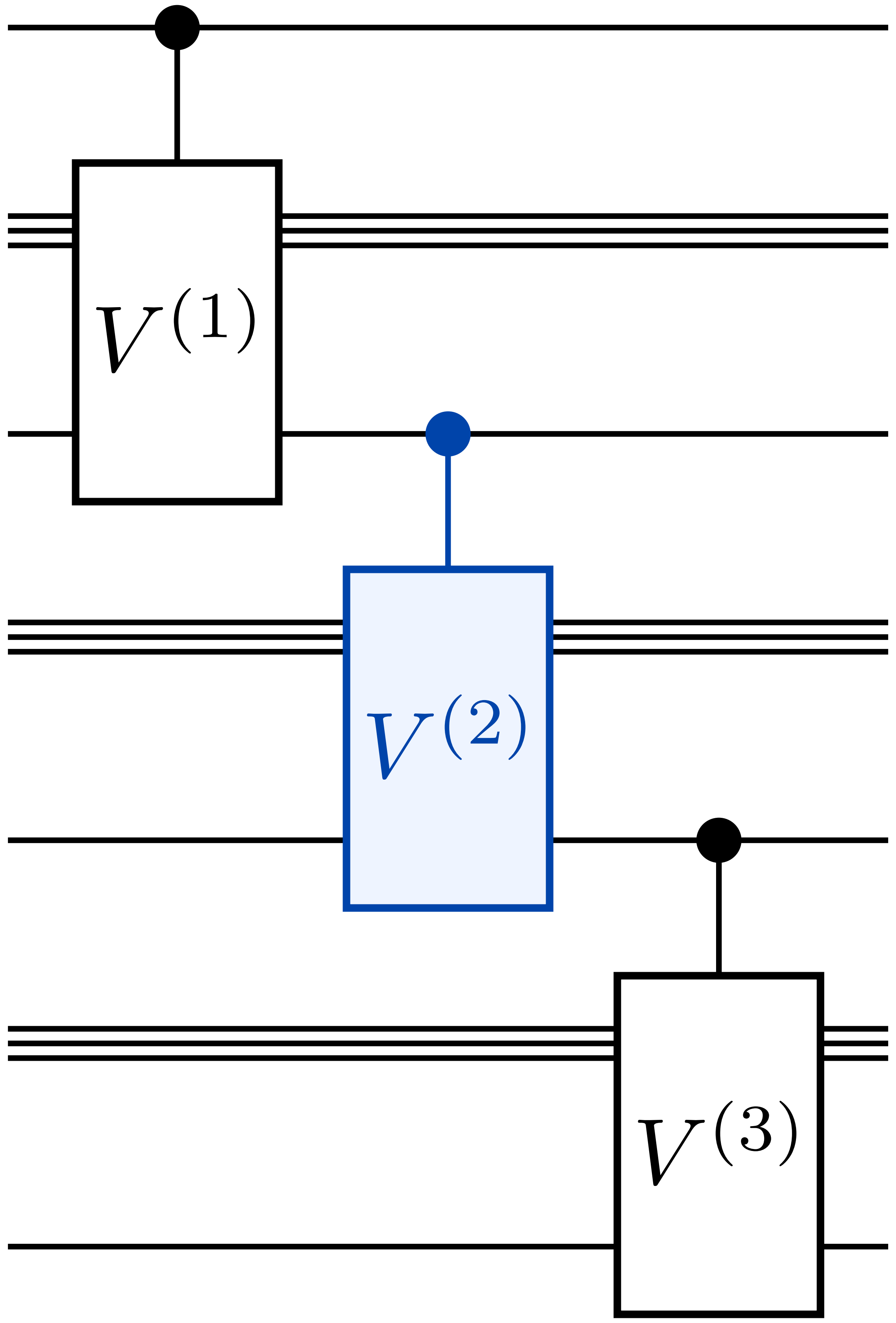
Fact ([STYYZ23]). Ancilla-free circuits for general k-qubit unitaries have worst-case depth $\Theta(4^k/k)$.



Consider a cascade of m-many k-qubit controlled unitaries

Quantum precomputation: some intuition

Fact ([STYYZ23]). Ancilla-free circuits for general k-qubit unitaries have worst-case depth $\Theta(4^k/k)$.



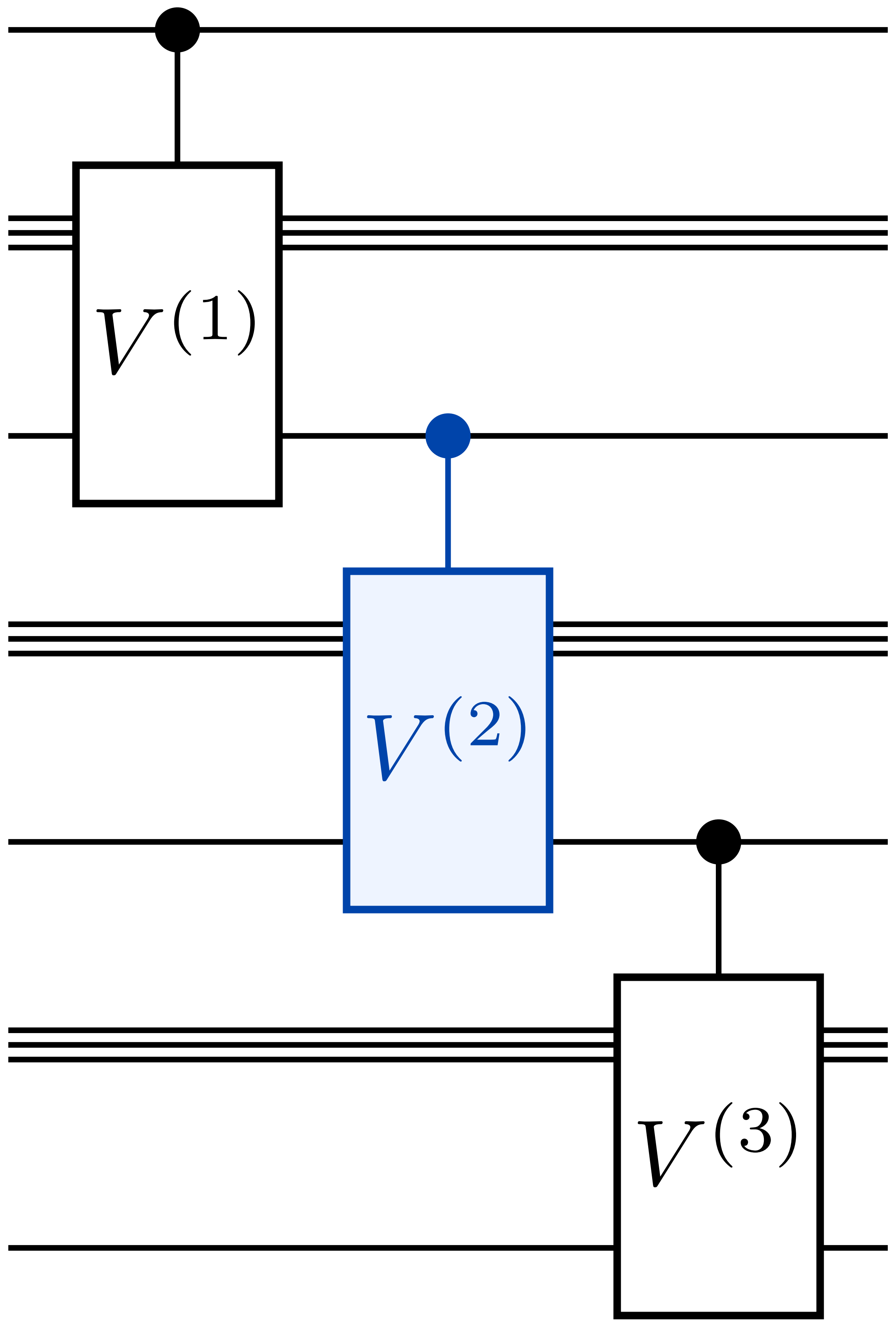
Consider a cascade of m-many k-qubit controlled unitaries

$$4^k + 4^k + 4^k \approx m \cdot 4^k$$

Quantum precomputation: some intuition

Fact ([STYYZ23]). Ancilla-free circuits for general k-qubit unitaries have worst-case depth $\Theta(4^k/k)$.

Observation: diagonal unitaries are pretty cheap



Consider a cascade of m-many k-qubit controlled unitaries

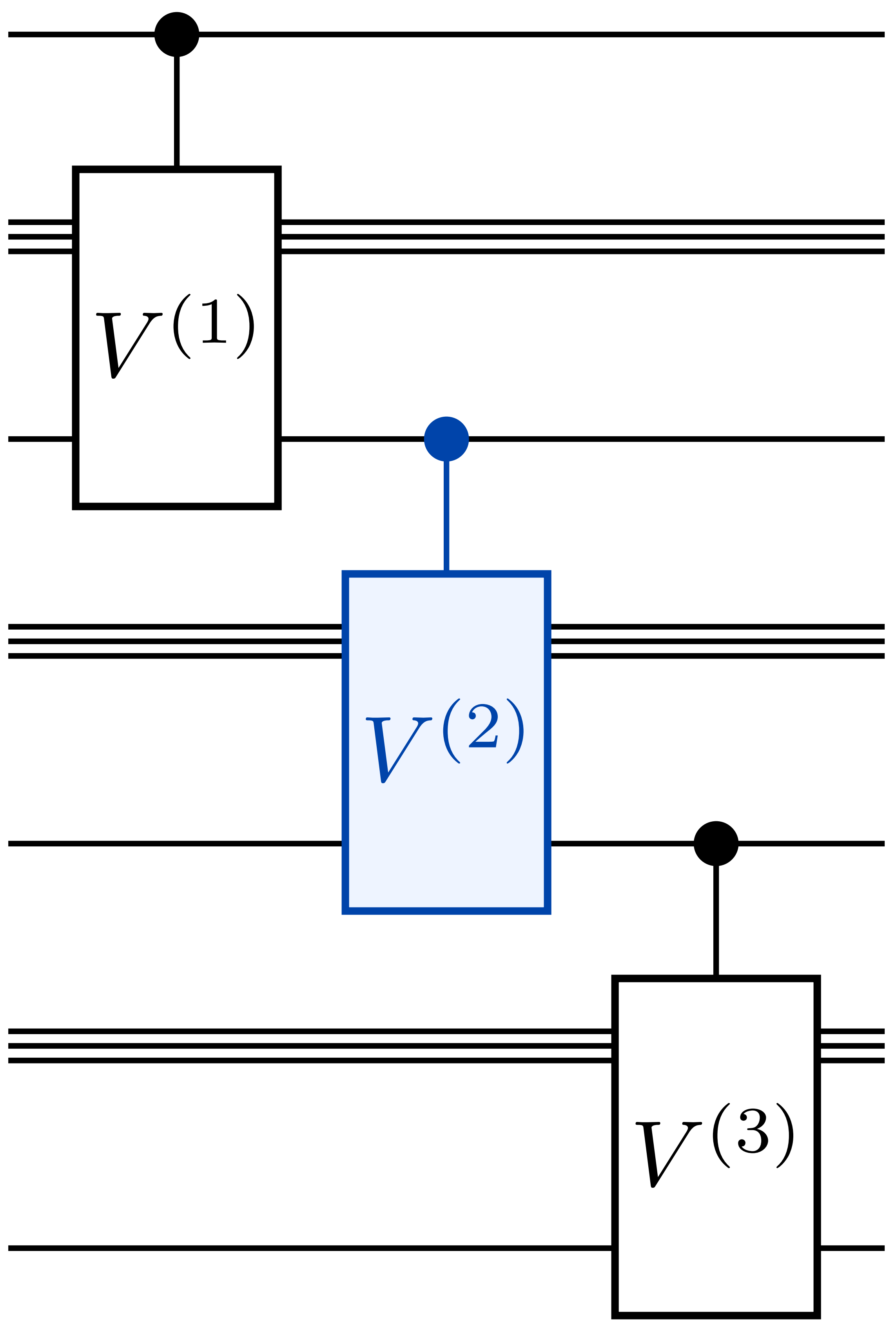
$4^k + 4^k + 4^k \approx m \cdot 4^k$

Quantum precomputation: some intuition

Fact ([STYYZ23]). Ancilla-free circuits for general k-qubit unitaries have worst-case depth $\Theta(4^k/k)$.

Observation: diagonal unitaries are pretty cheap

Fact ([STYYZ23]). Ancilla-free circuits for **diagonal** k-qubit unitaries have worst-case depth $\Theta(2^k/k)$.



Consider a cascade of m-many k-qubit controlled unitaries

$$4^k \; + \; 4^k \; + \; 4^k \quad \approx \quad m \cdot 4^k$$

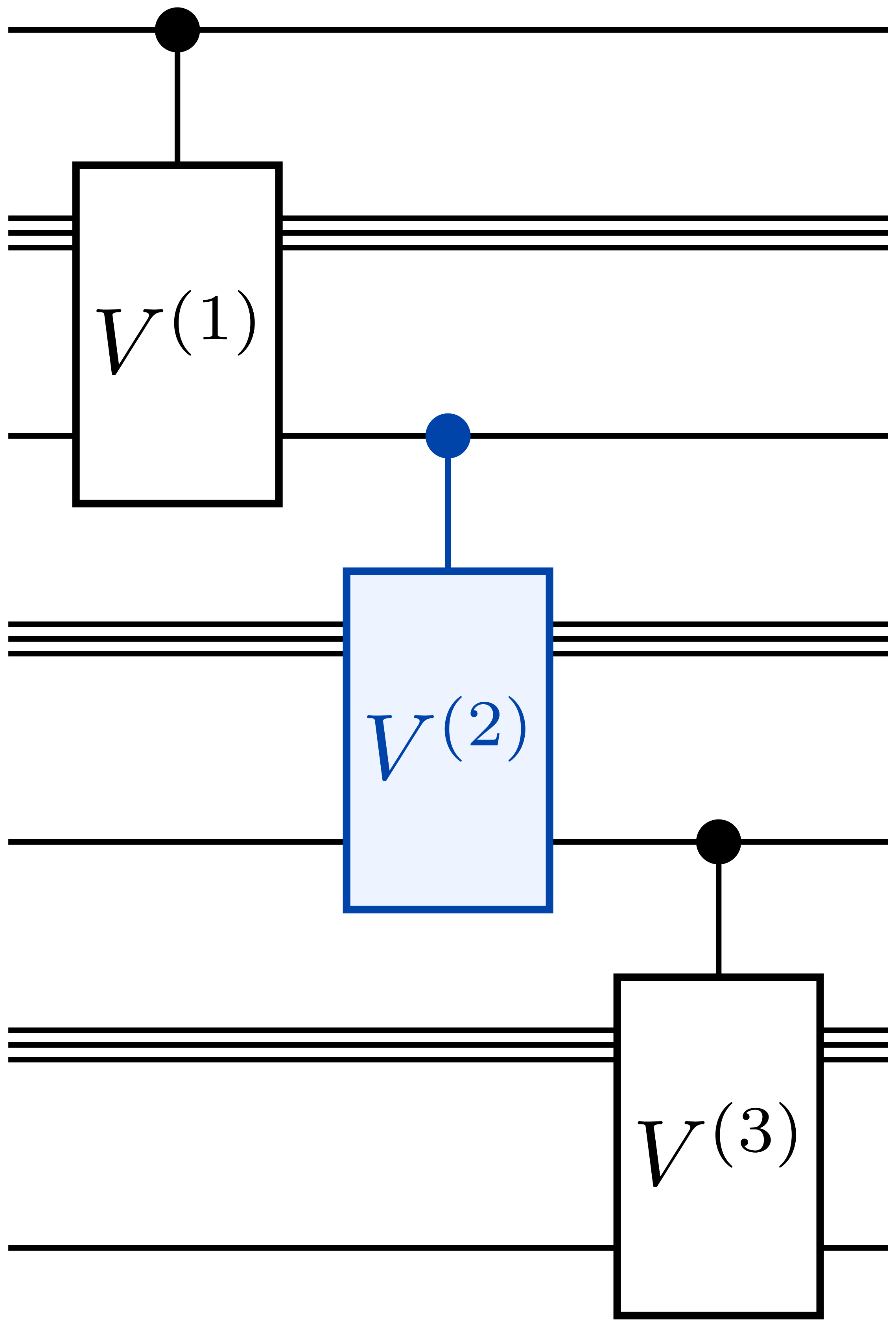
Quantum precomputation: some intuition

Fact ([STYYZ23]). Ancilla-free circuits for general k-qubit unitaries have worst-case depth $\Theta(4^k/k)$.

Observation: diagonal unitaries are pretty cheap

Fact ([STYYZ23]). Ancilla-free circuits for **diagonal** k-qubit unitaries have worst-case depth $\Theta(2^k/k)$.

Goal: make the V's diagonal somehow

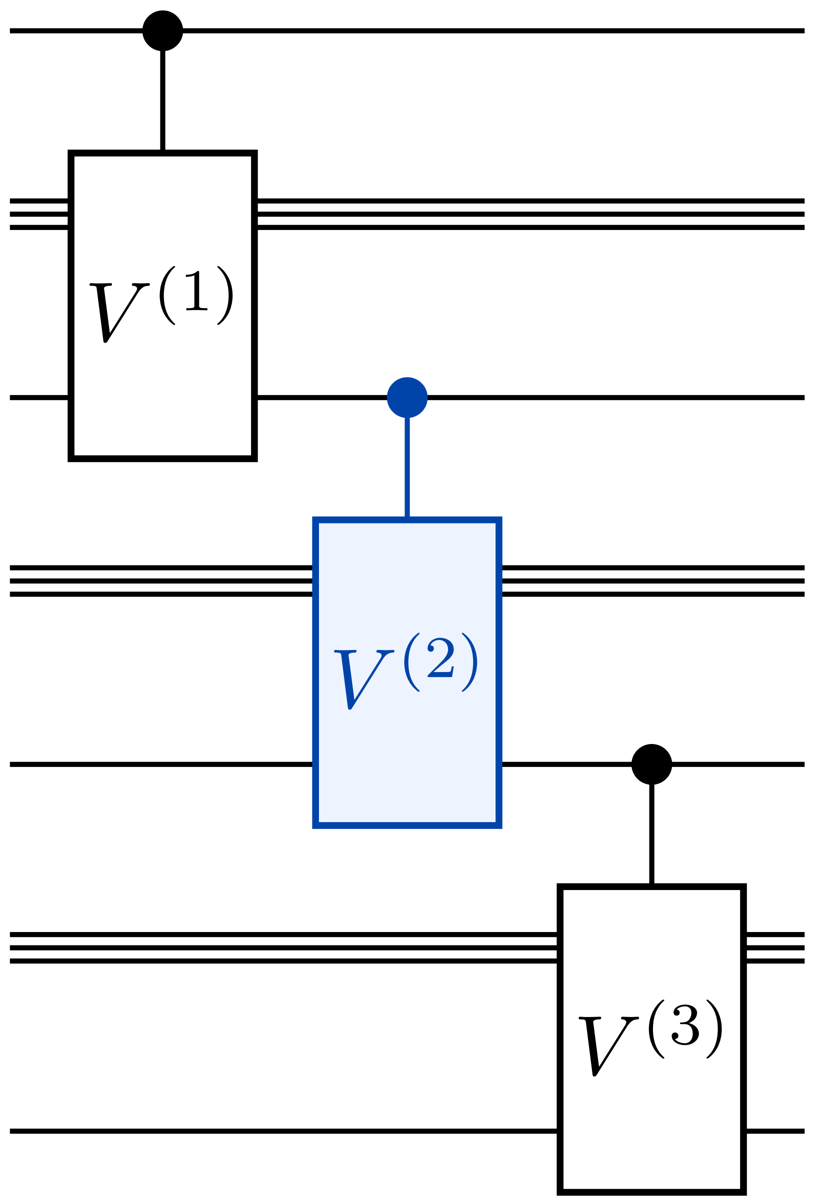


Consider a cascade of m-many k-qubit controlled unitaries

$$4^k + 4^k + 4^k \approx m \cdot 4^k$$

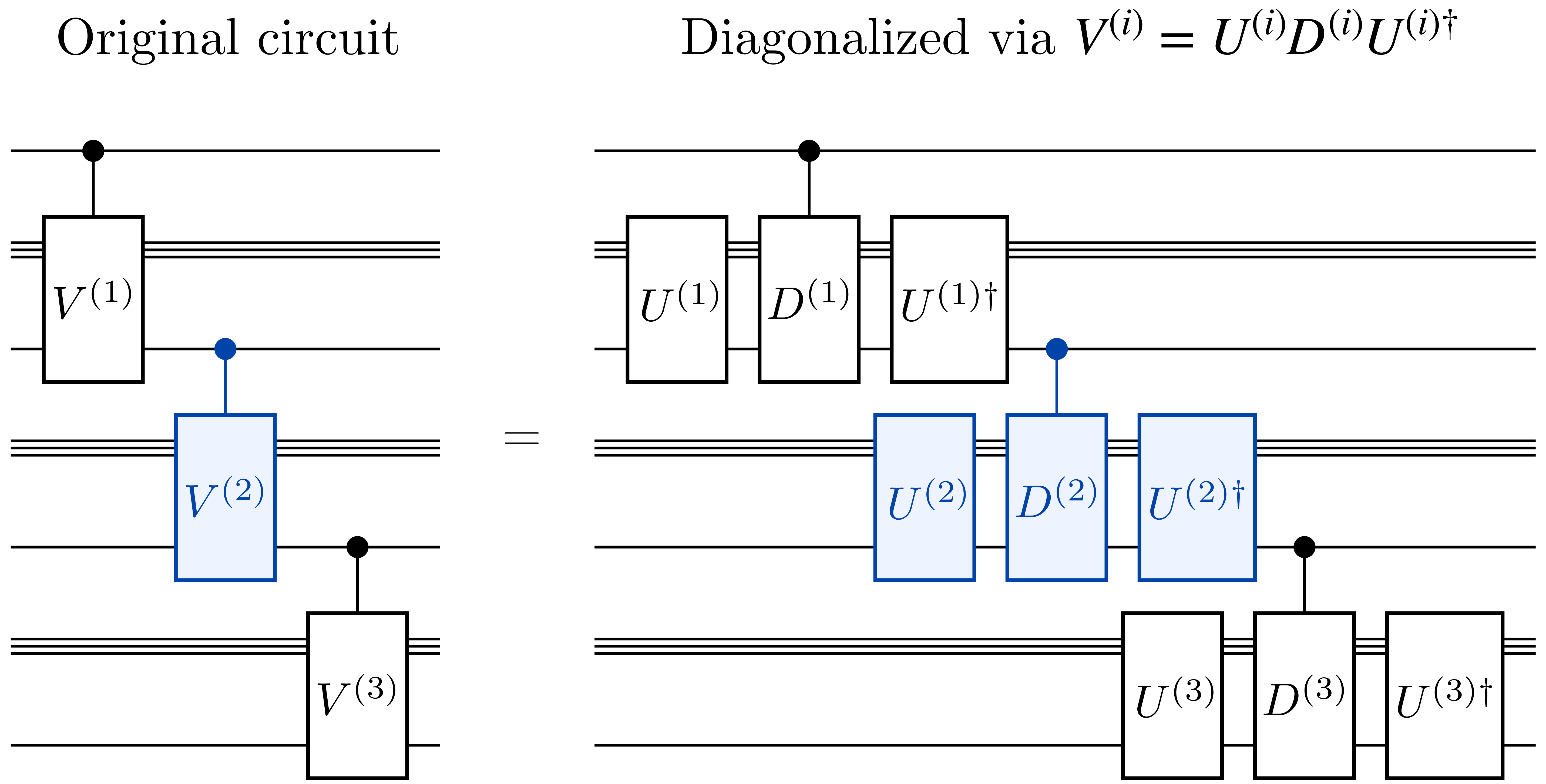
First attempt: diagonalization?

Original circuit



Quantum precomputation: some intuition

First attempt: diagonalization?



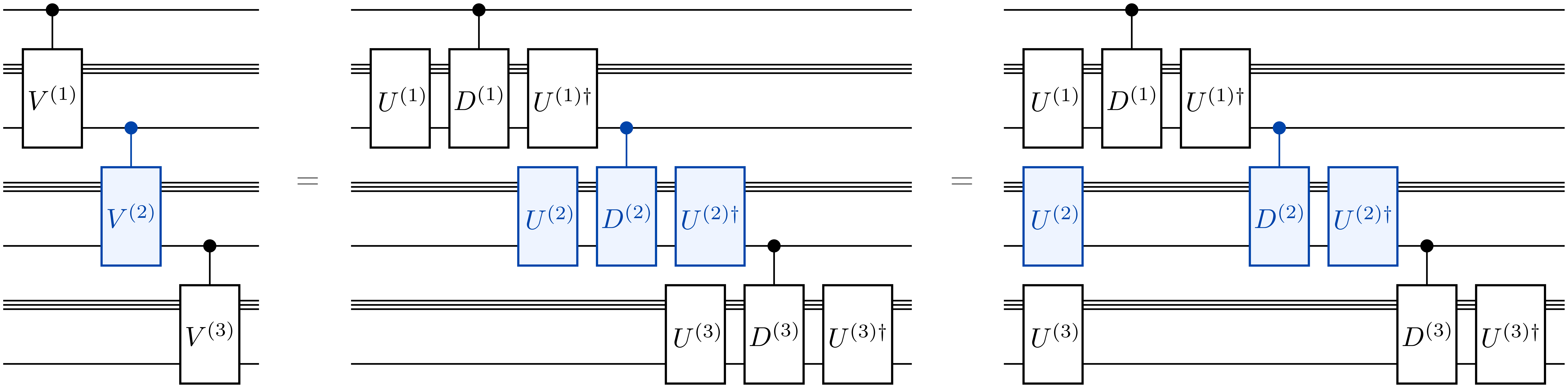
Quantum precomputation: some intuition

First attempt: diagonalization?

Original circuit

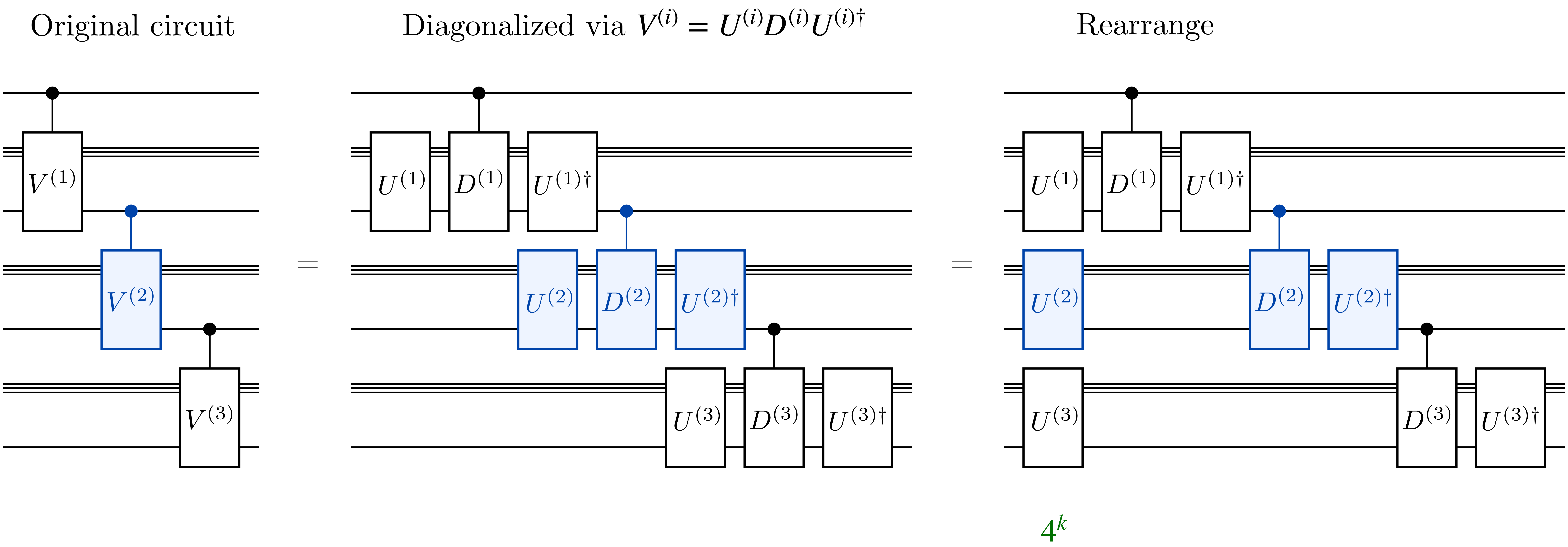
Diagonalized via $V^{(i)} = U^{(i)} D^{(i)} U^{(i)\dagger}$

Rearrange



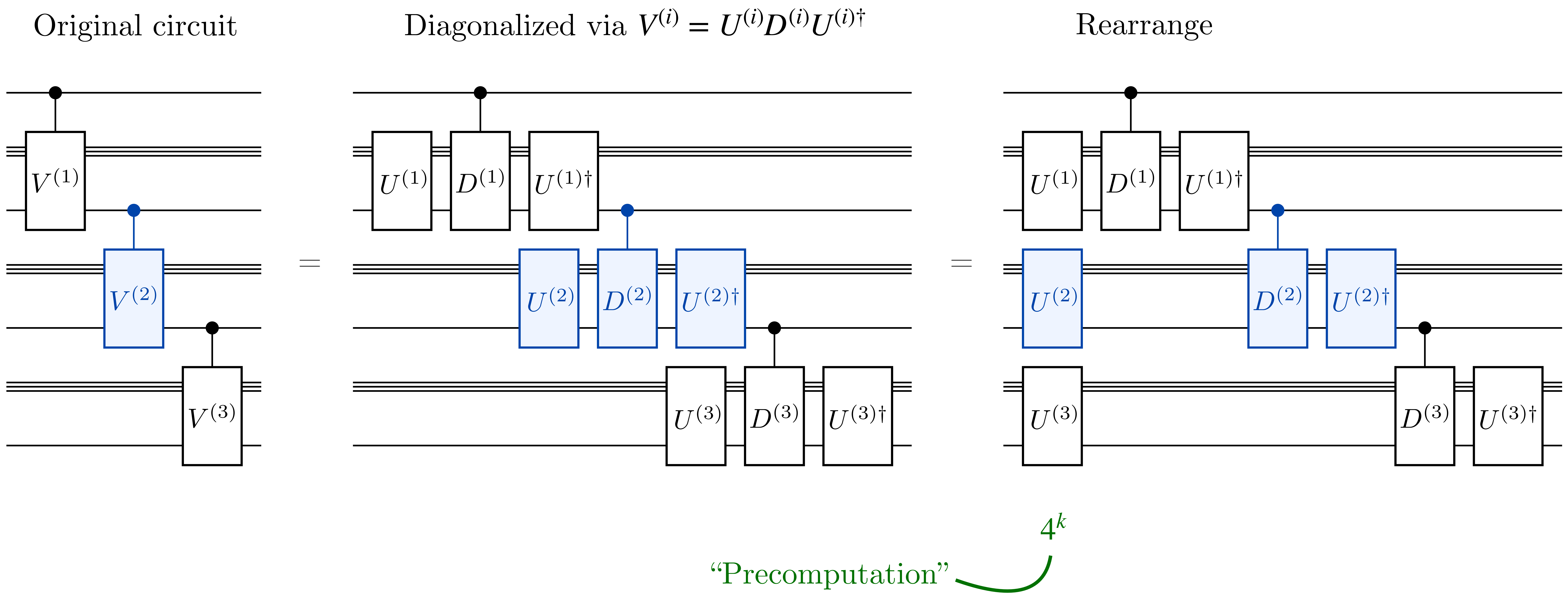
Quantum precomputation: some intuition

First attempt: diagonalization?



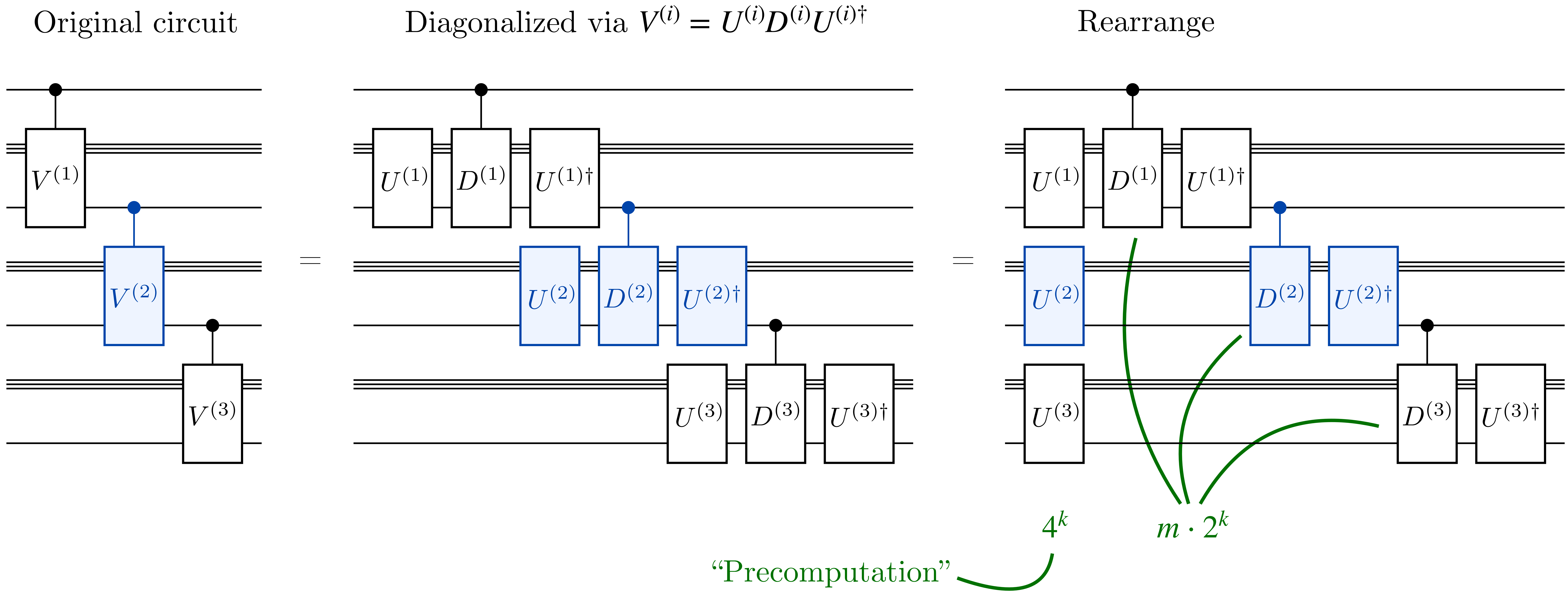
Quantum precomputation: some intuition

First attempt: diagonalization?



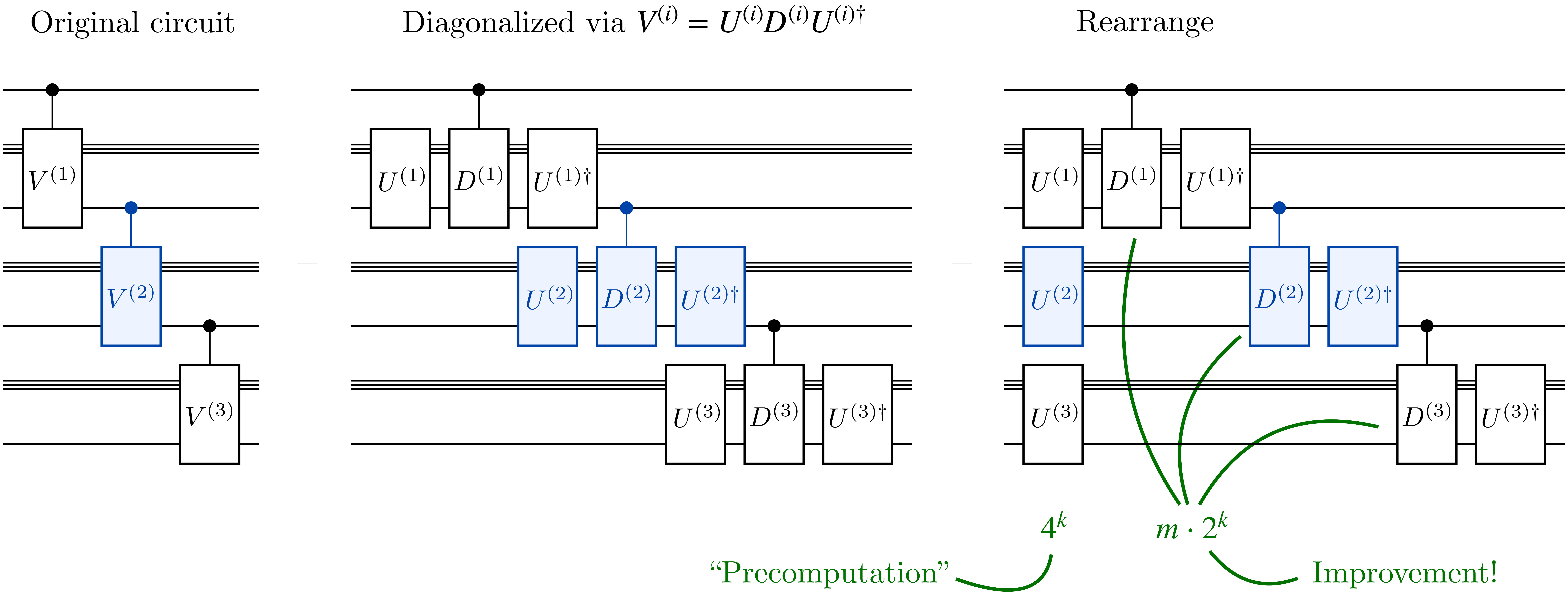
Quantum precomputation: some intuition

First attempt: diagonalization?



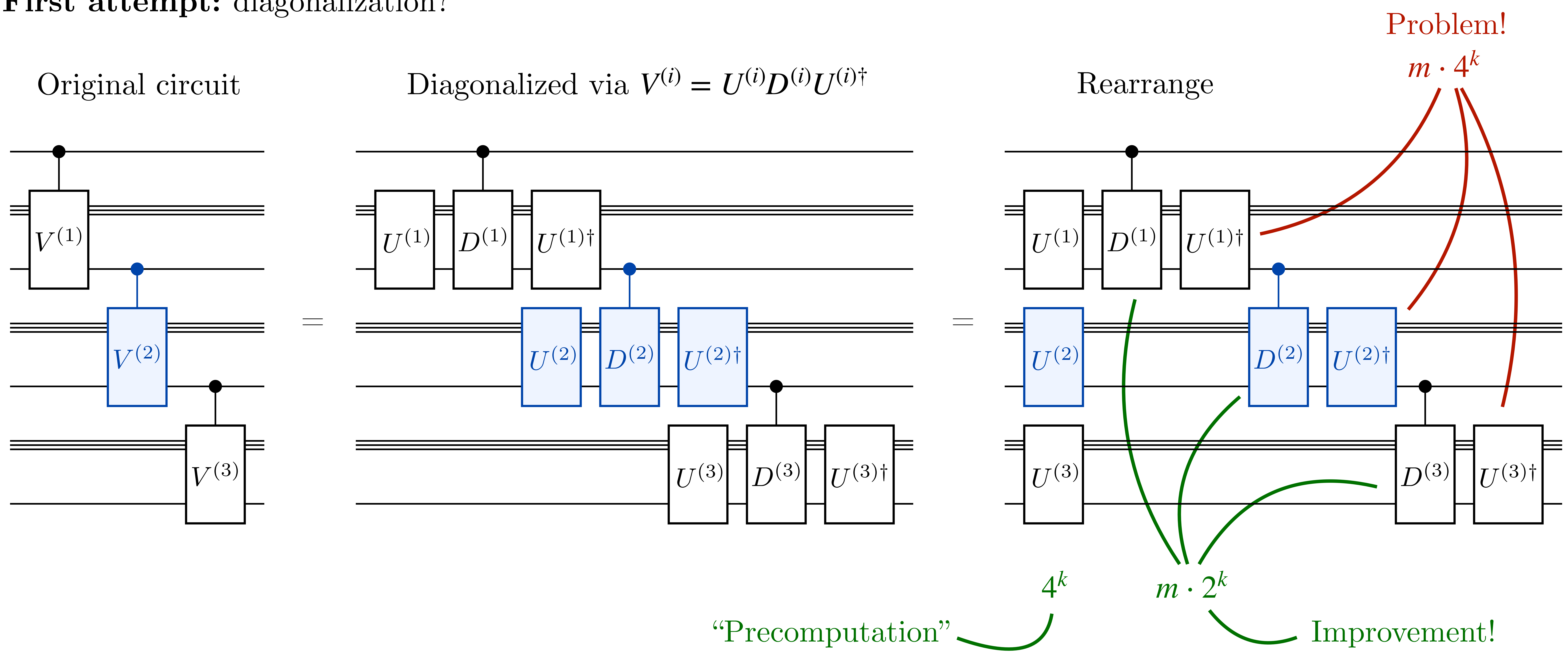
Quantum precomputation: some intuition

First attempt: diagonalization?



Quantum precomputation: some intuition

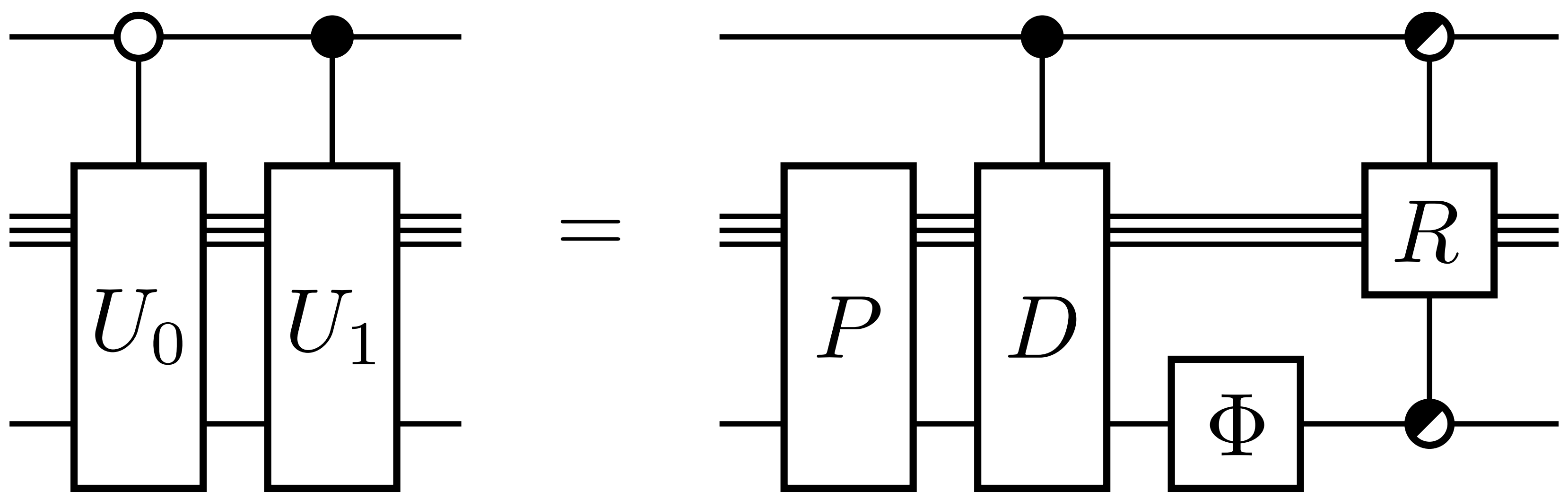
First attempt: diagonalization?



Quantum precomputation: a better identity

Quantum precomputation: a better identity

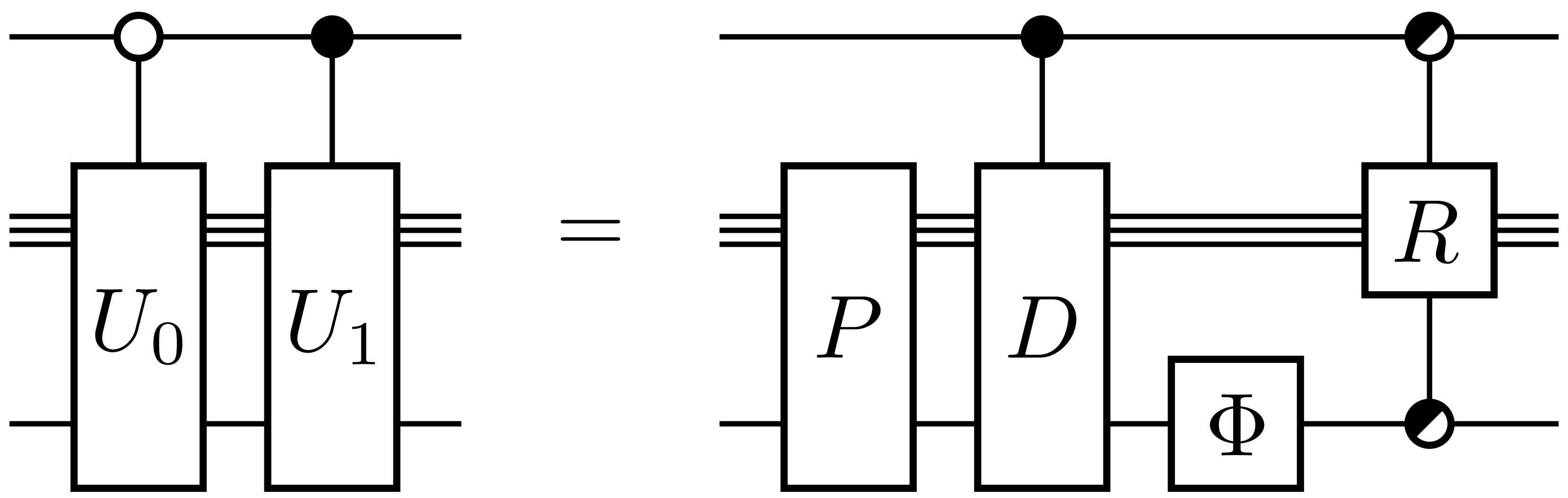
Lemma (Precomputation identity)**.** For any many-qubit U_0, U_1, there are P, diagonal D, and R such that



where $\mathbf{\Phi}$ a universal (fixed) unitary.

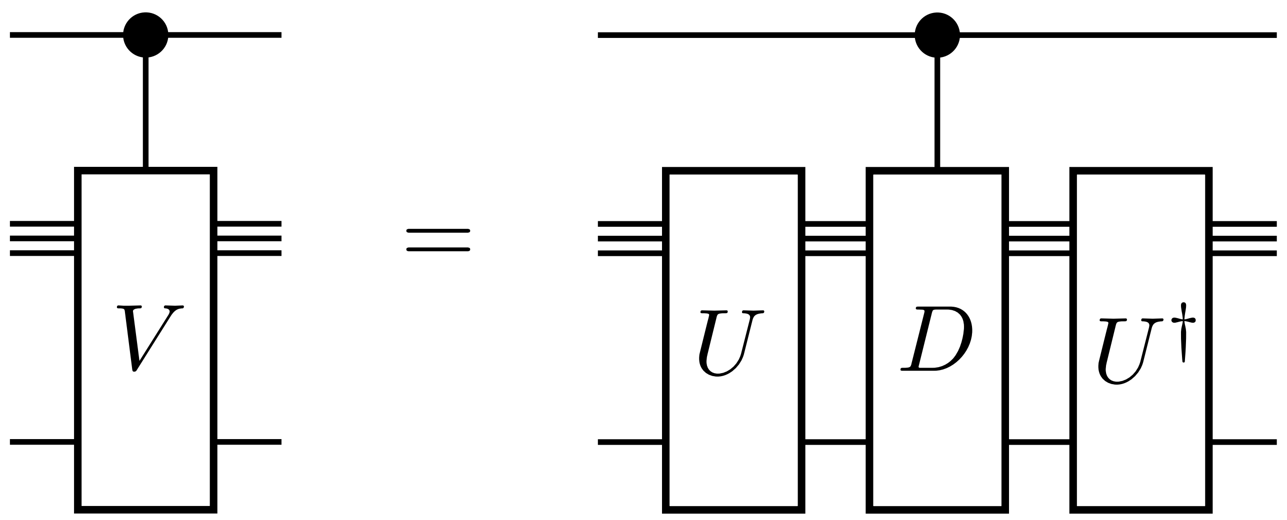
Quantum precomputation: a better identity

Lemma (Precomputation identity)**.** For any many-qubit $U_0, U_1,$ there are P, diagonal D, and R such that

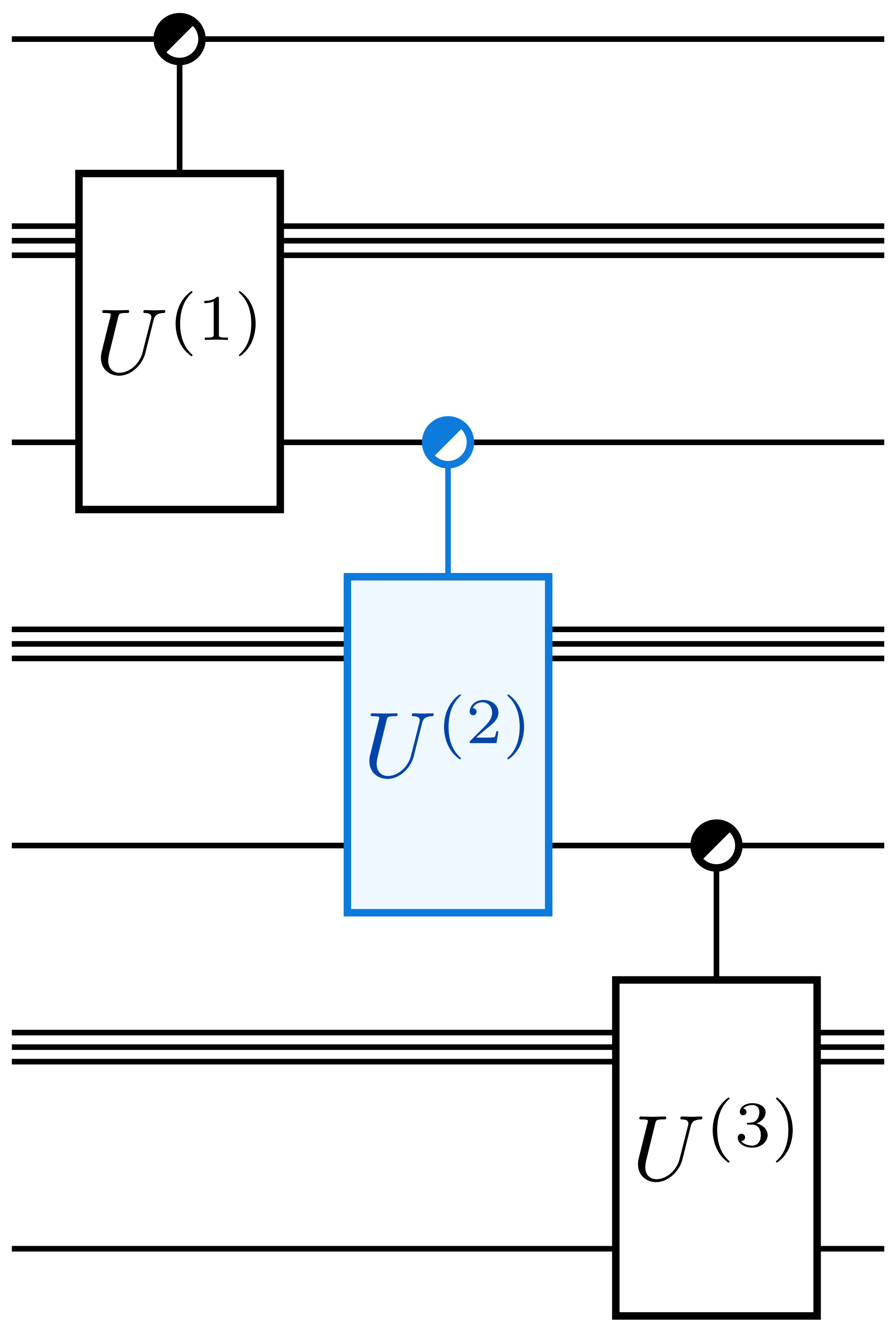


where $\mathbf{\Phi}$ a universal (fixed) unitary.

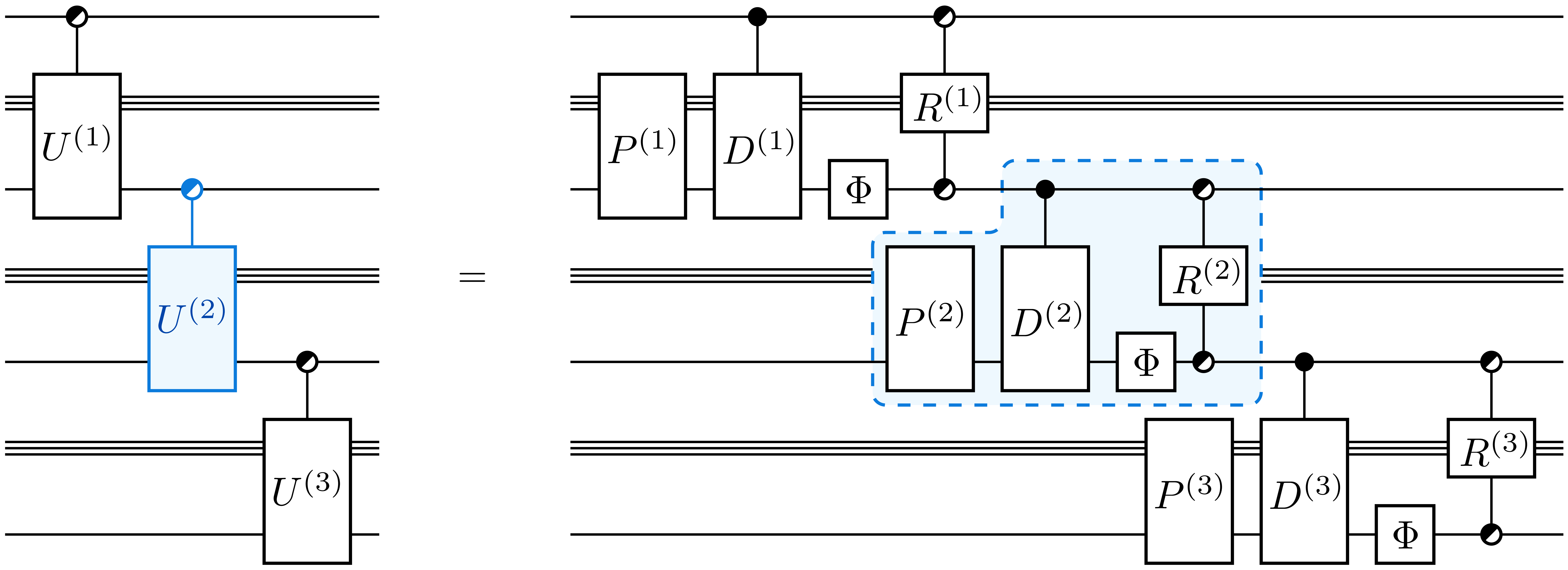
C.f. Naive diagonalization



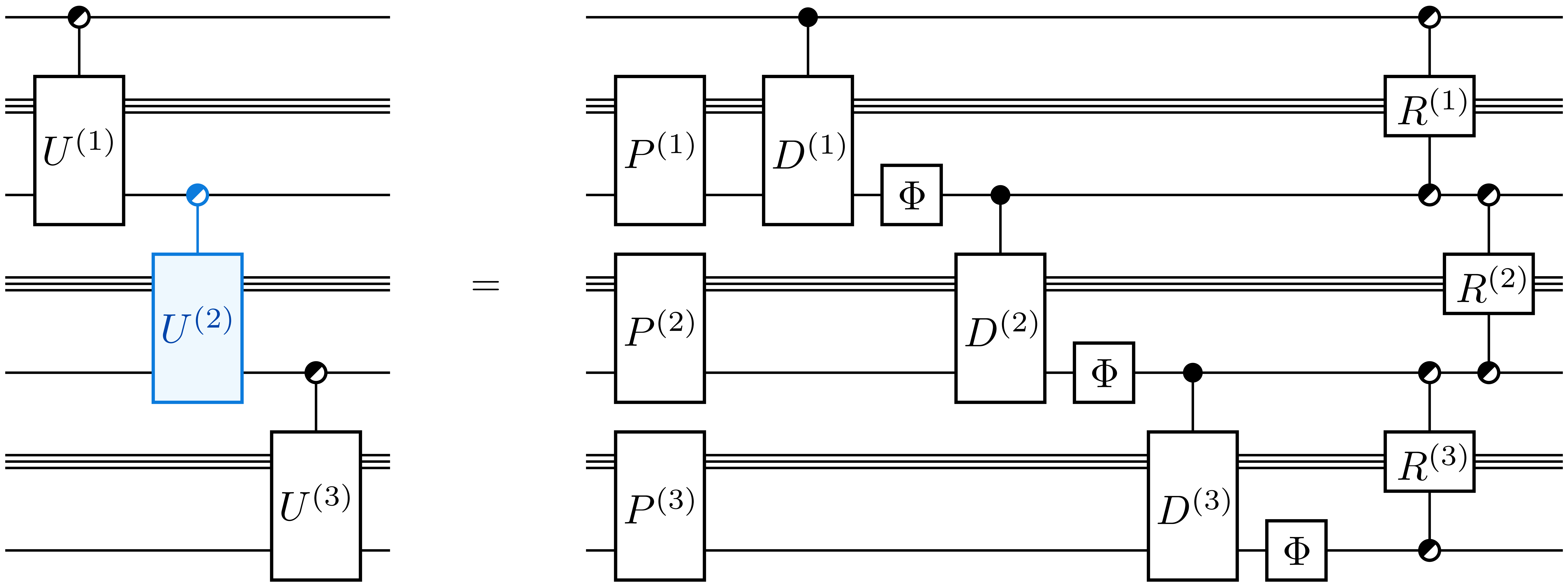
Quantum precomputation: applying the identity



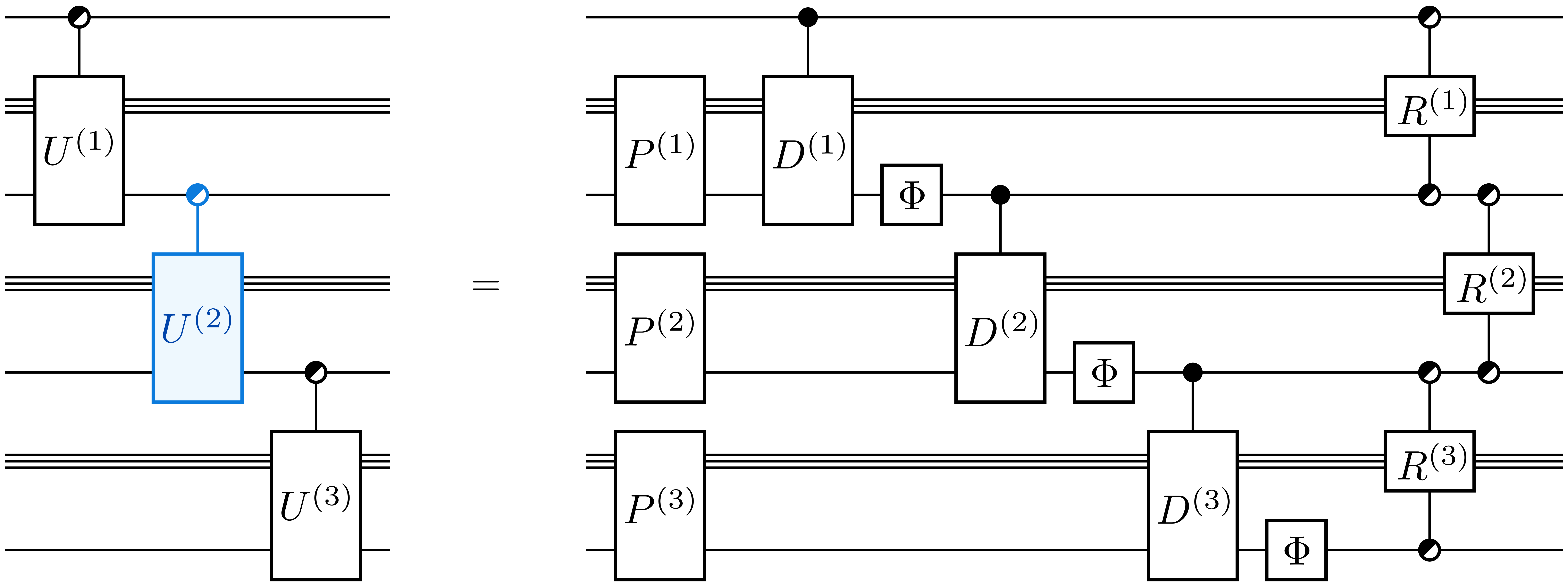
Quantum precomputation: applying the identity



Quantum precomputation: applying the identity

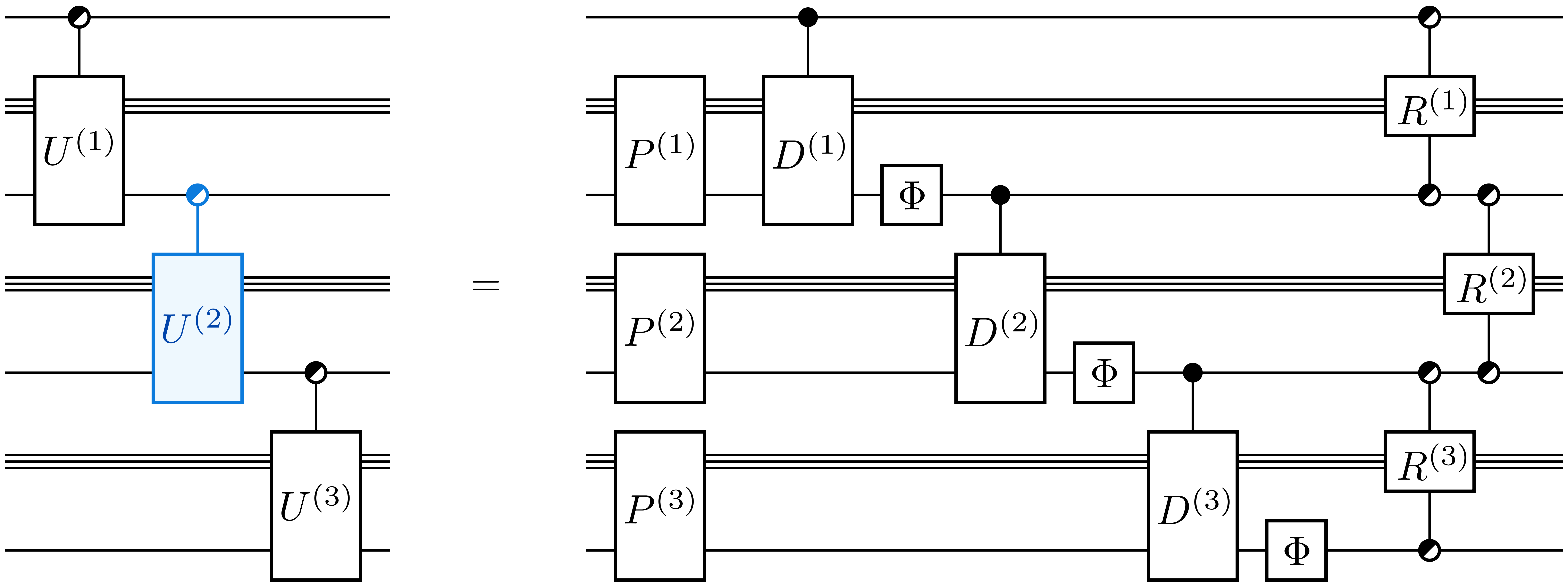


Quantum precomputation: applying the identity



Original circuit: $O(m4^k)$ depth

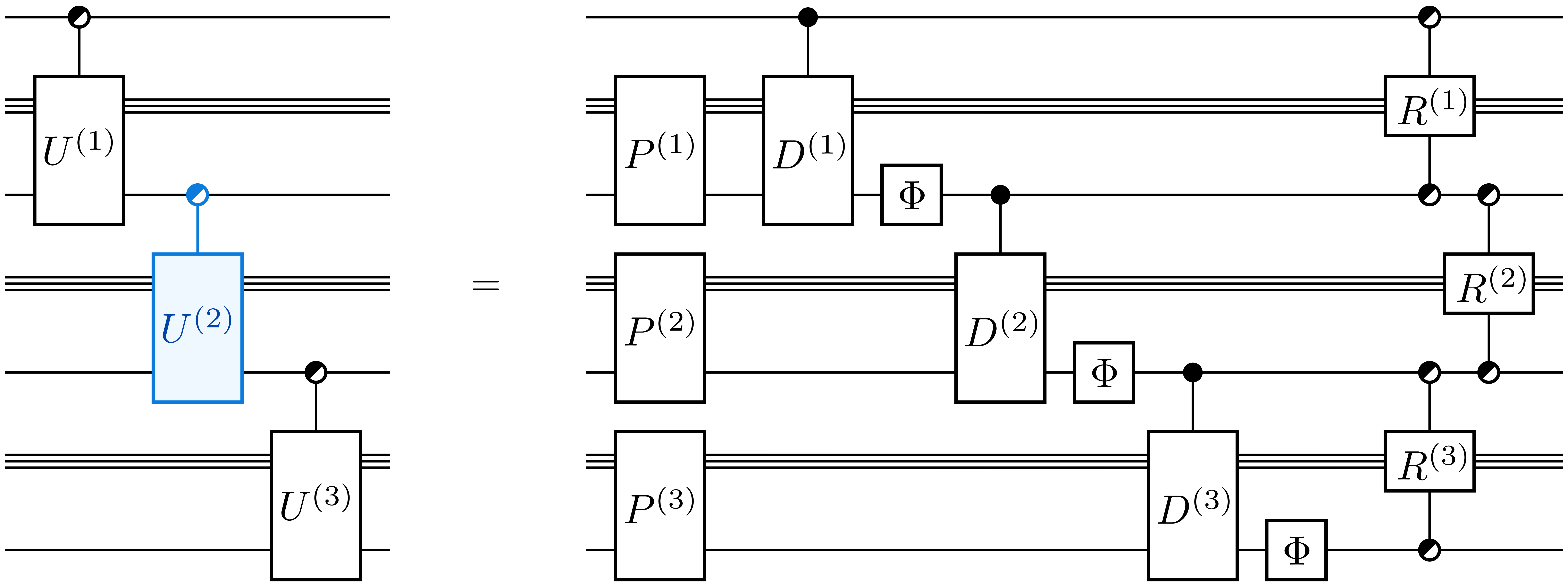
Quantum precomputation: applying the identity



Original circuit: $O(m4^k)$ depth

New circuit: $O(4^k + m2^k)$ depth

Quantum precomputation: applying the identity

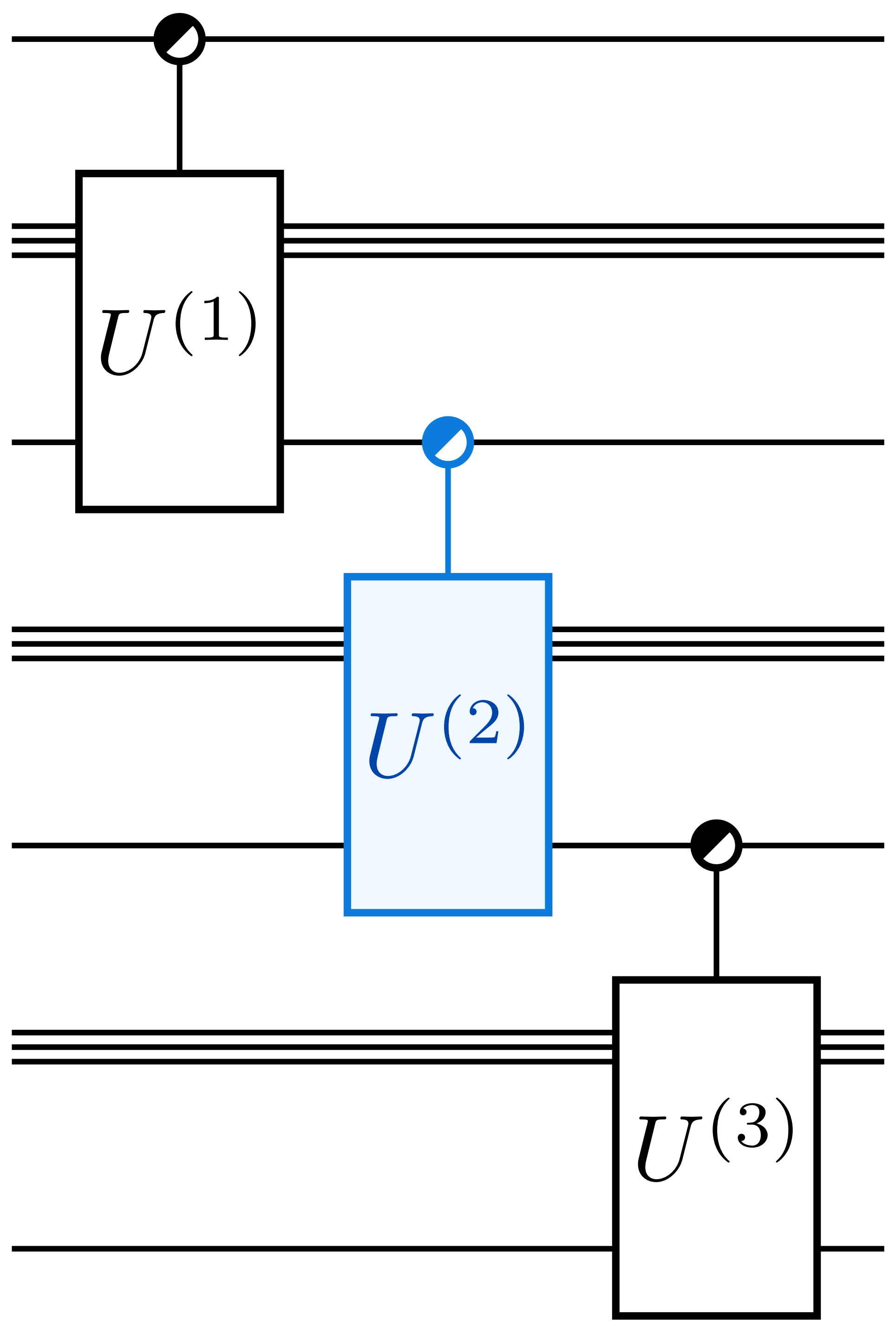


Original circuit: $O(m4^k)$ depth

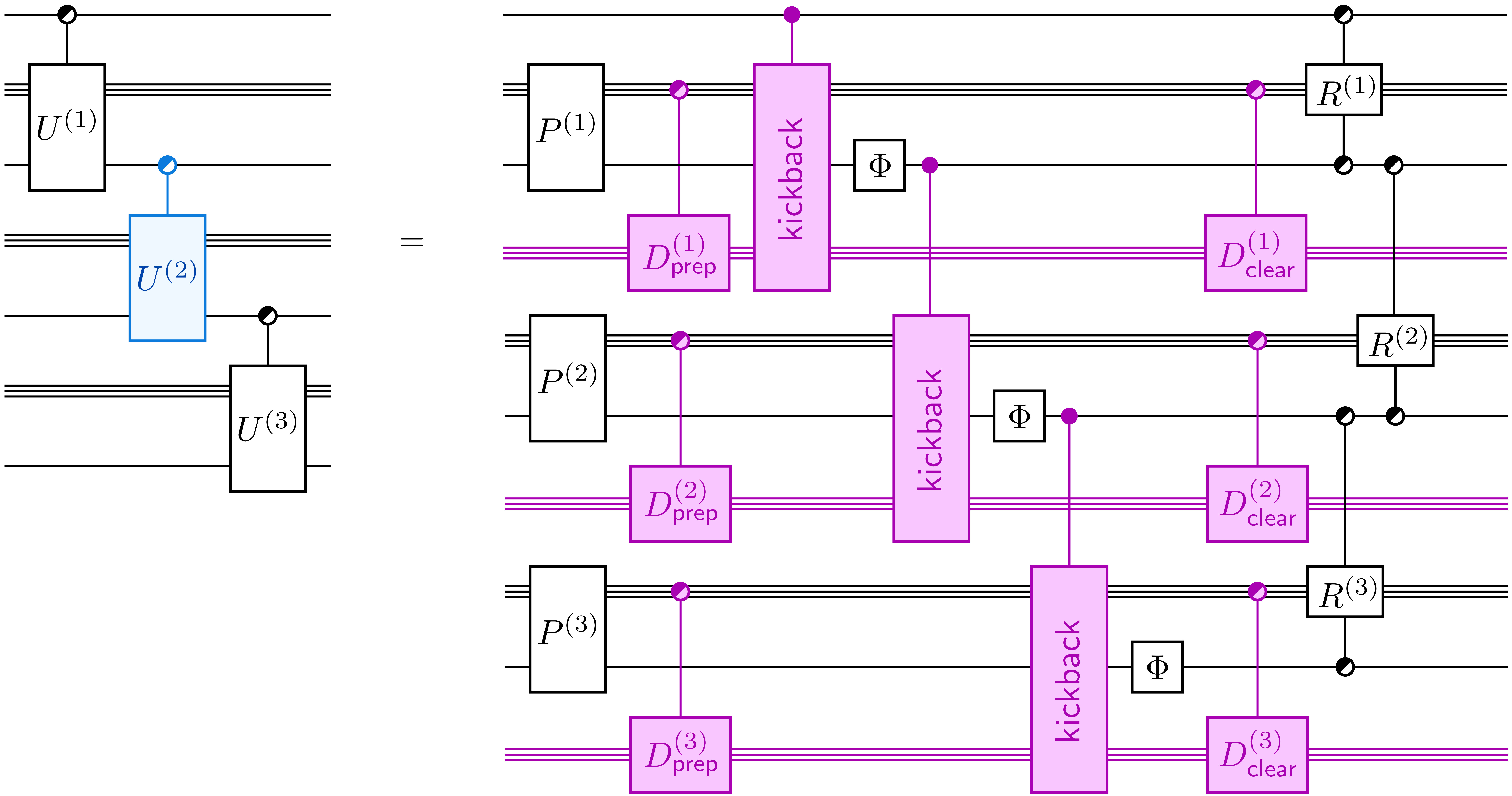
New circuit: $O(4^k + m2^k)$ depth

Example. Put $m = n, k = \log(n)$. Then depths are $O(n^3)$ (naive) vs. $O(n^2)$ (using precomputation)

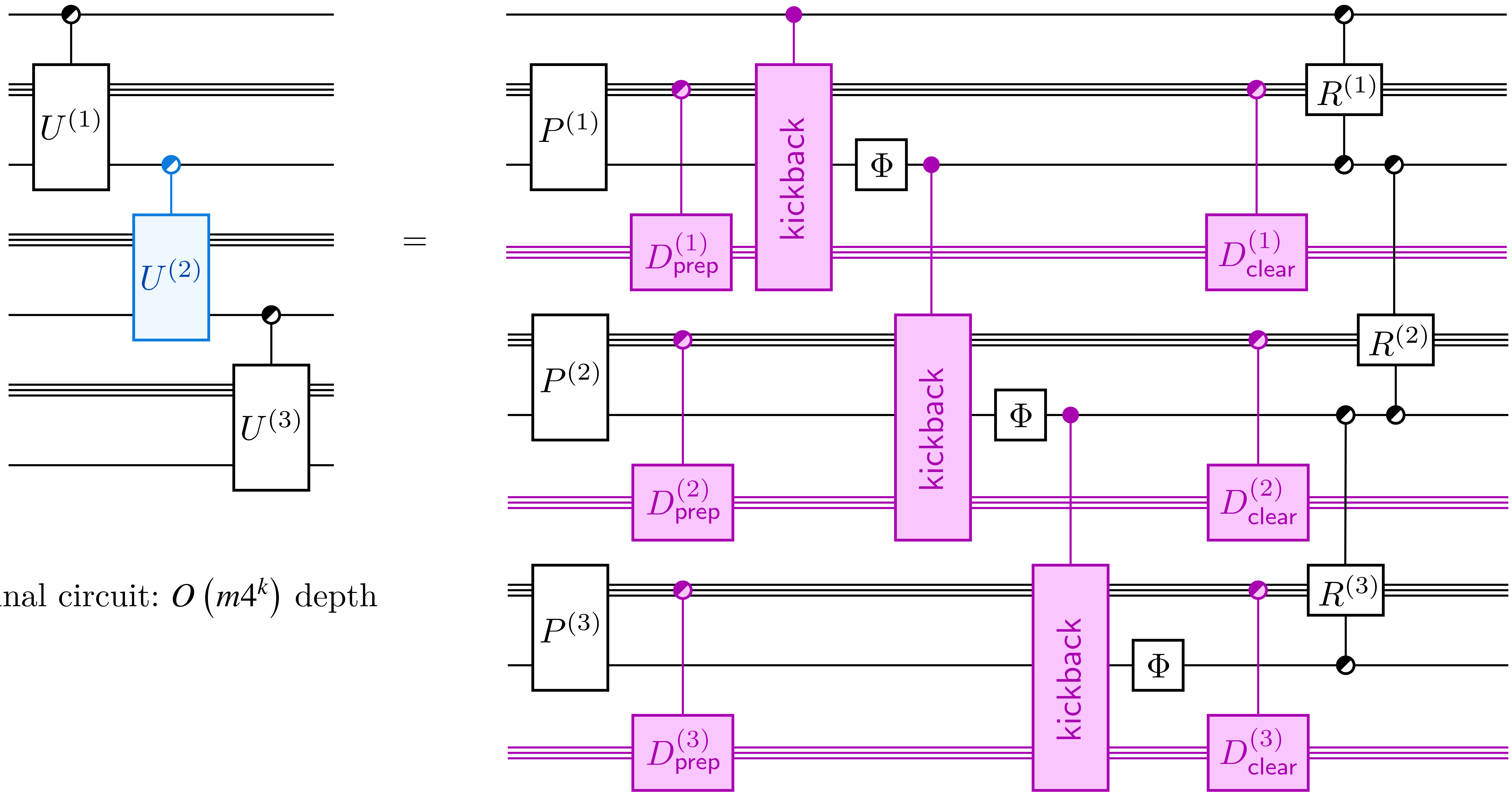
Quantum precomputation: with ancillae



Quantum precomputation: with ancillae

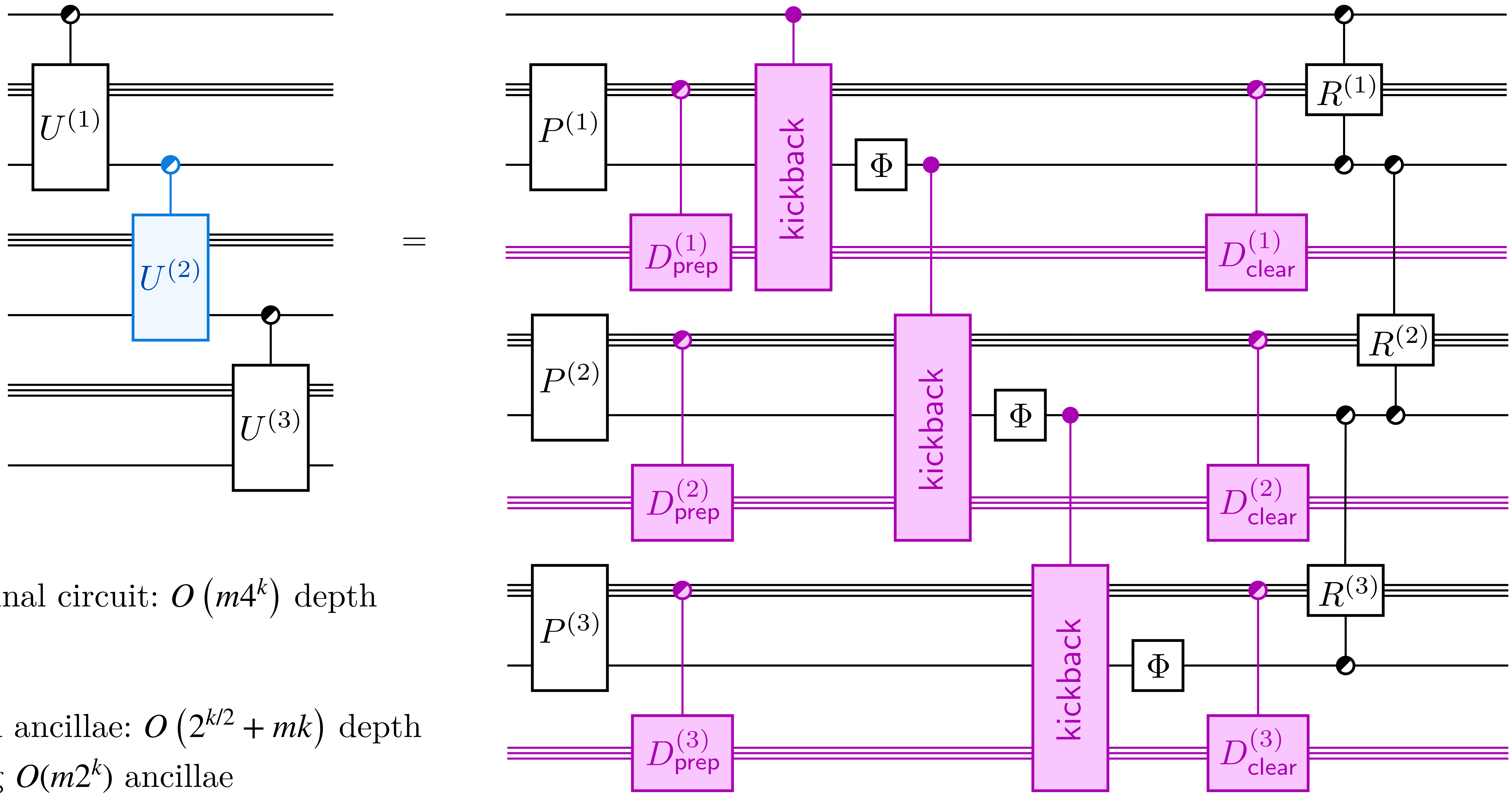


Quantum precomputation: with ancillae



Original circuit: $O\left(m4^k\right)$ depth

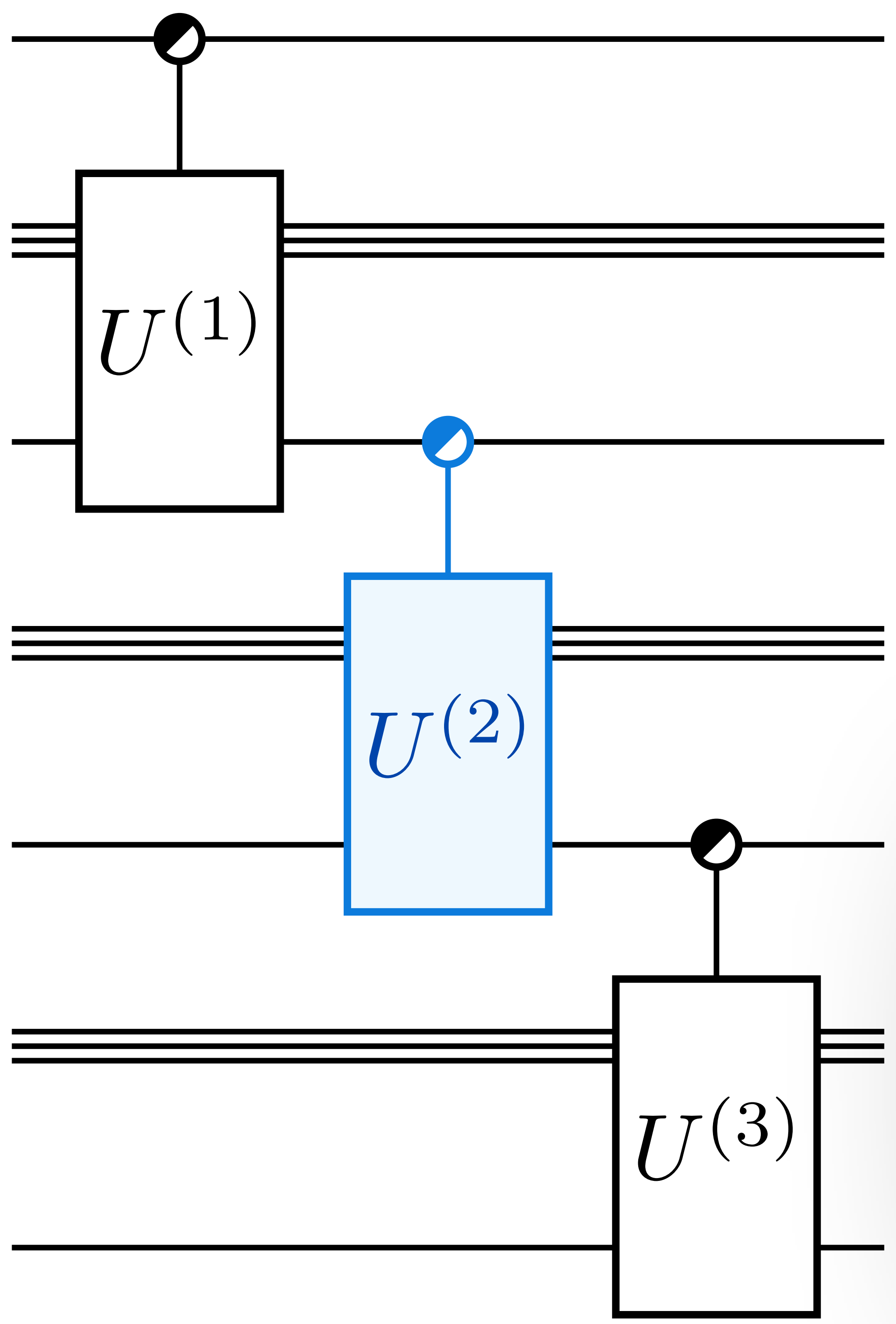
Quantum precomputation: with ancillae



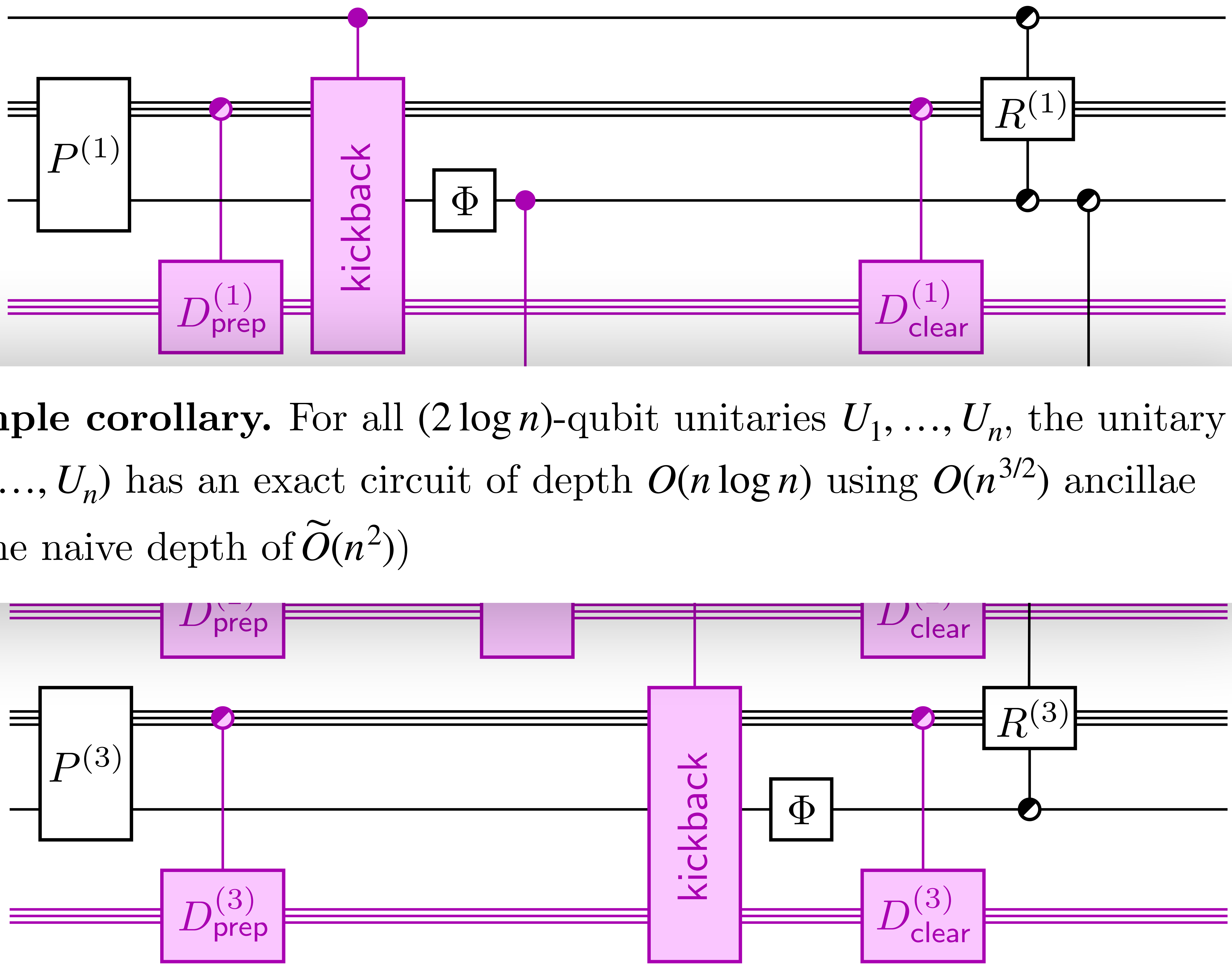
Original circuit: $O\left(m4^k\right)$ depth

With ancillae: $O\left(2^{k/2} + mk\right)$ depth
using $O(m2^k)$ ancillae

Quantum precomputation: with ancillae



=

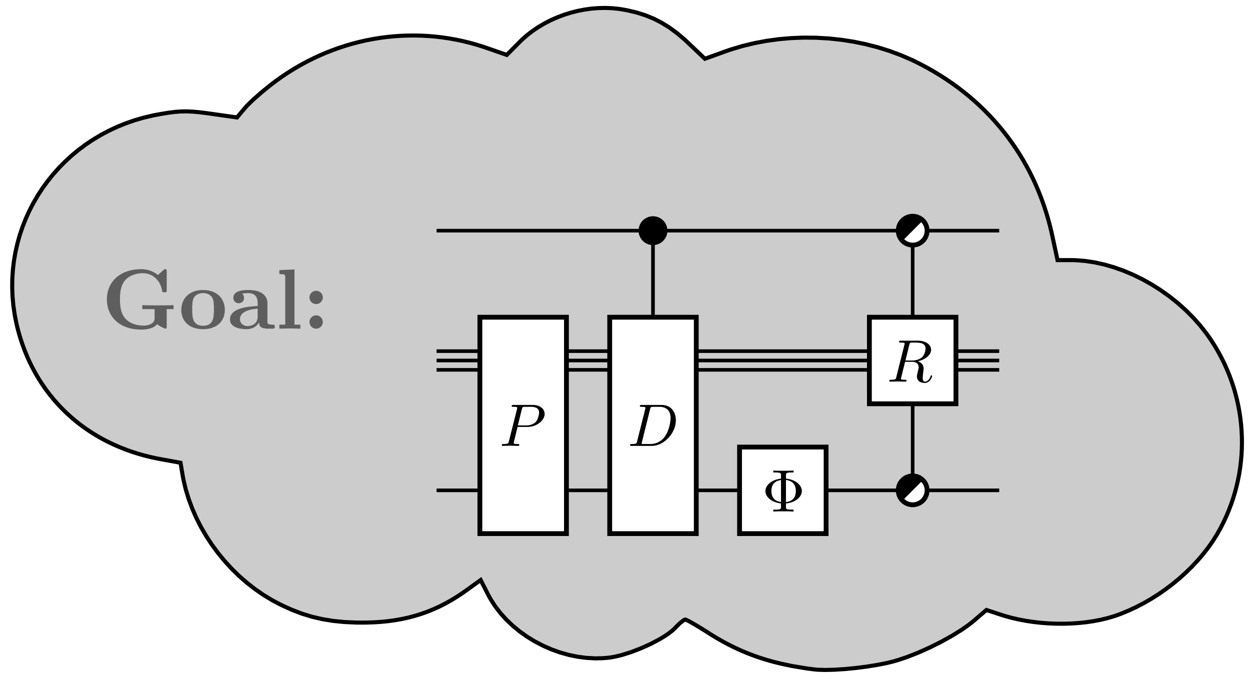


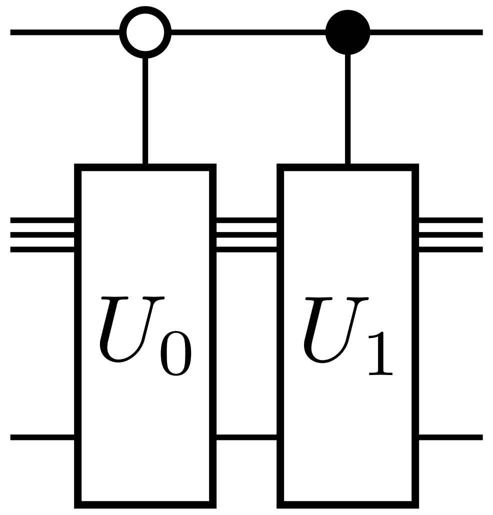
Example corollary. For all $(2\log n)$-qubit unitaries $U_1, \ldots, U_n$, the unitary $C(U_1, \ldots, U_n)$ has an exact circuit of depth $O(n \log n)$ using $O(n^{3/2})$ ancillae (vs. the naive depth of $\widetilde{O}(n^2)$)

Original circuit: $O\left(m4^k\right)$ depth

With ancillae: $O\left(2^{k/2} + mk\right)$ depth using $O(m2^k)$ ancillae

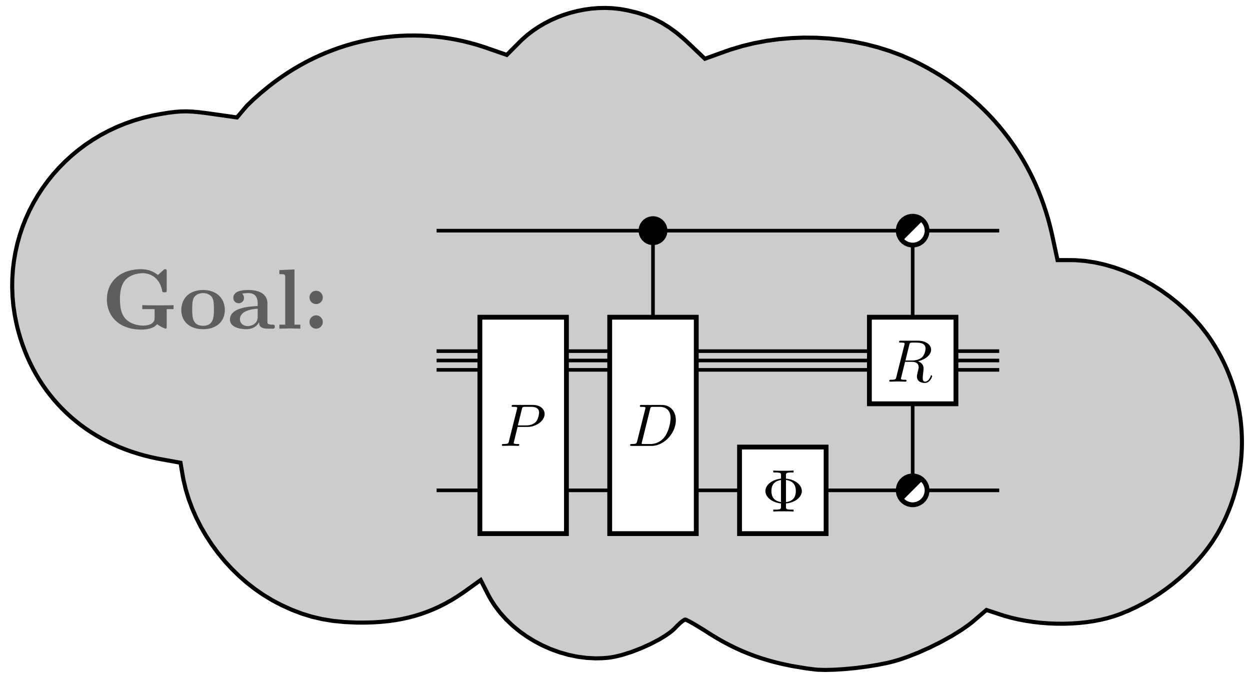
Precomputation identity: proof

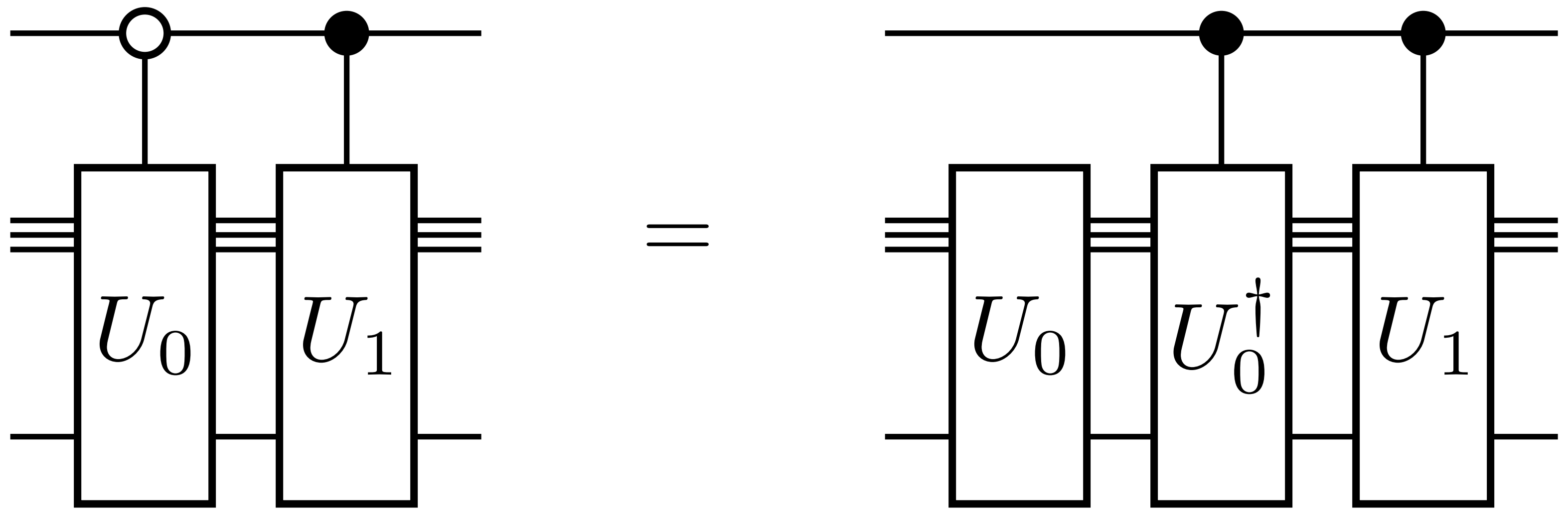




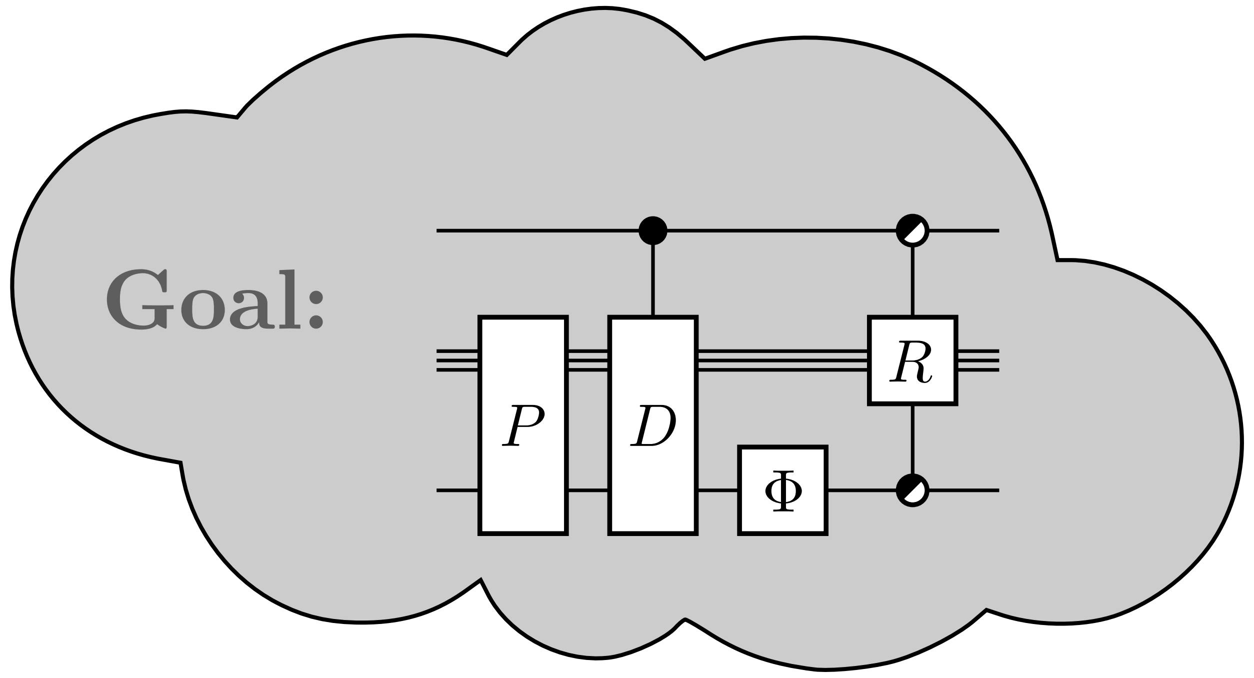
$=$

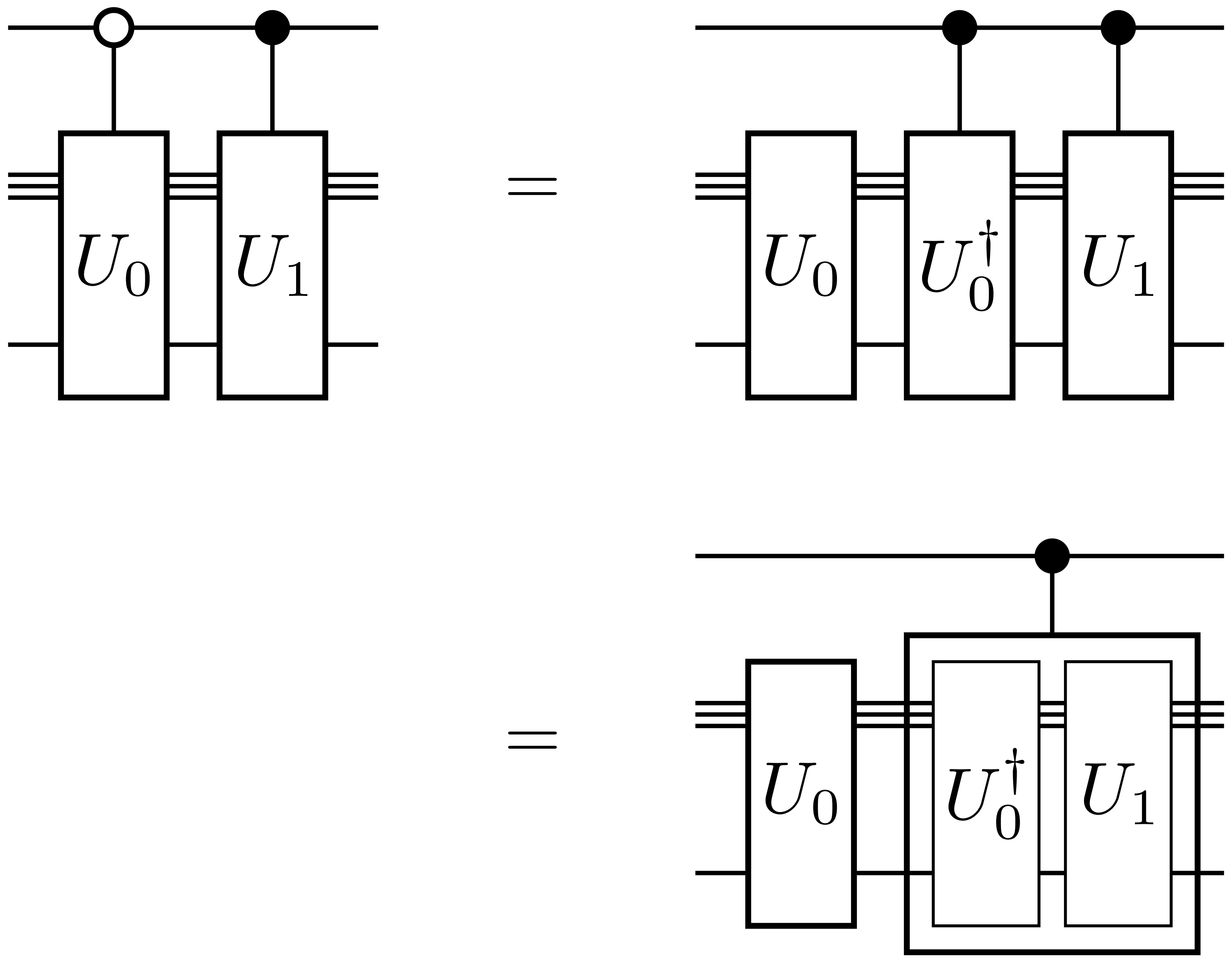
Precomputation identity: proof



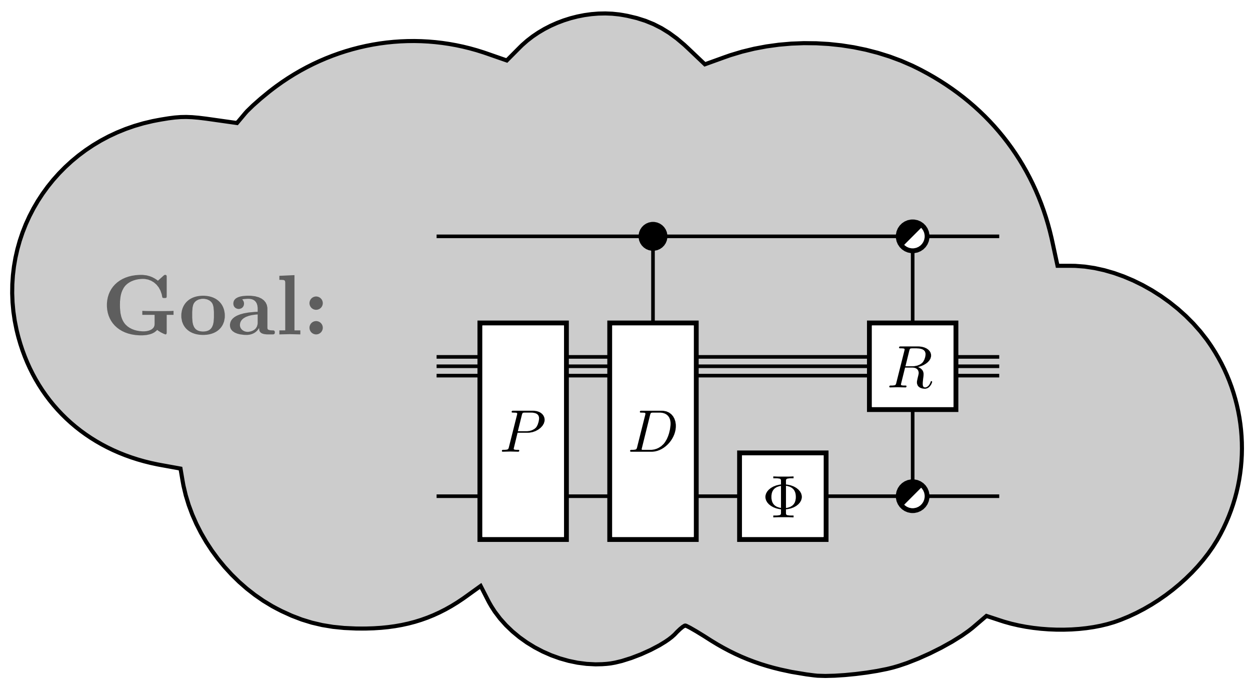


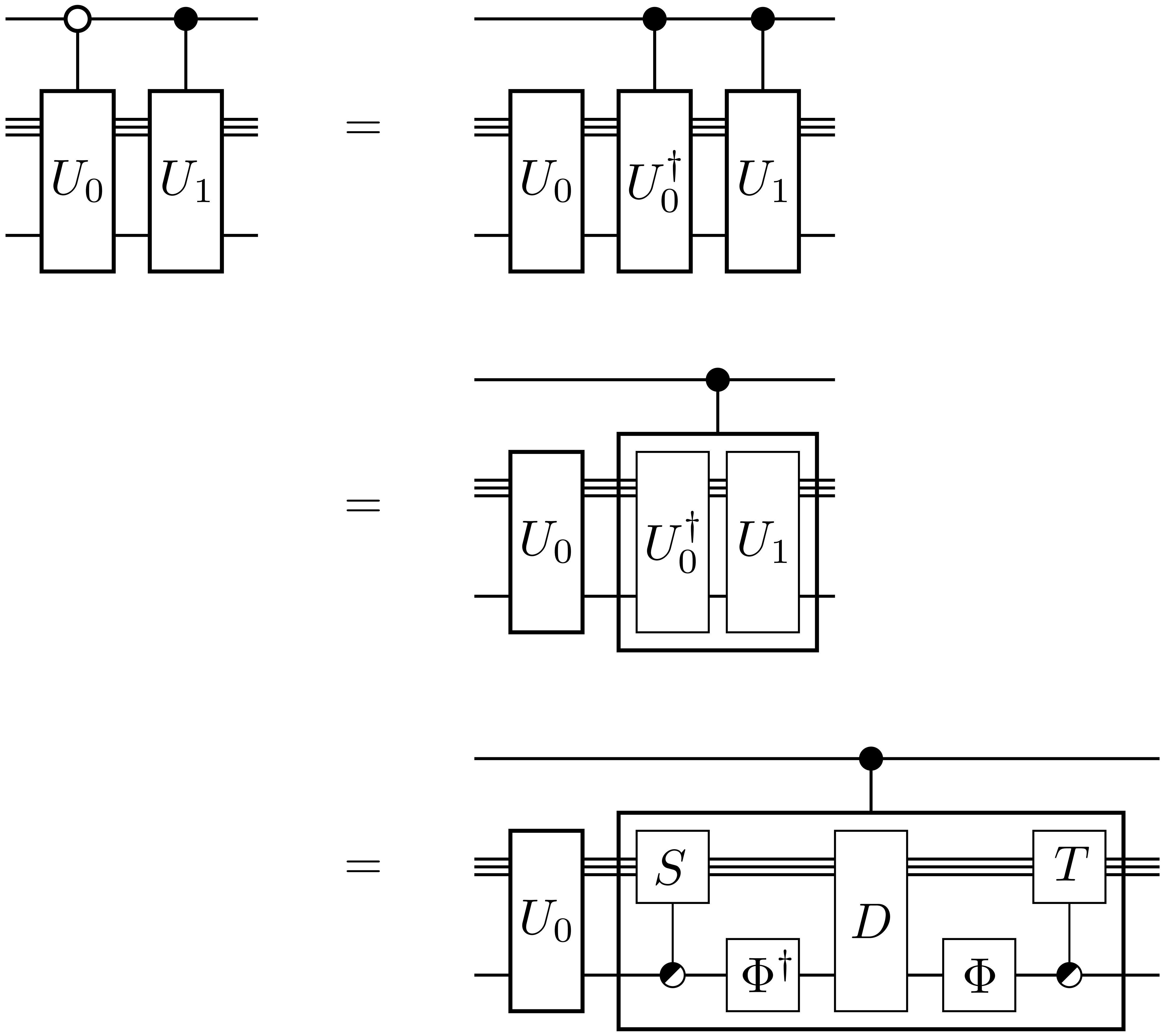
Precomputation identity: proof





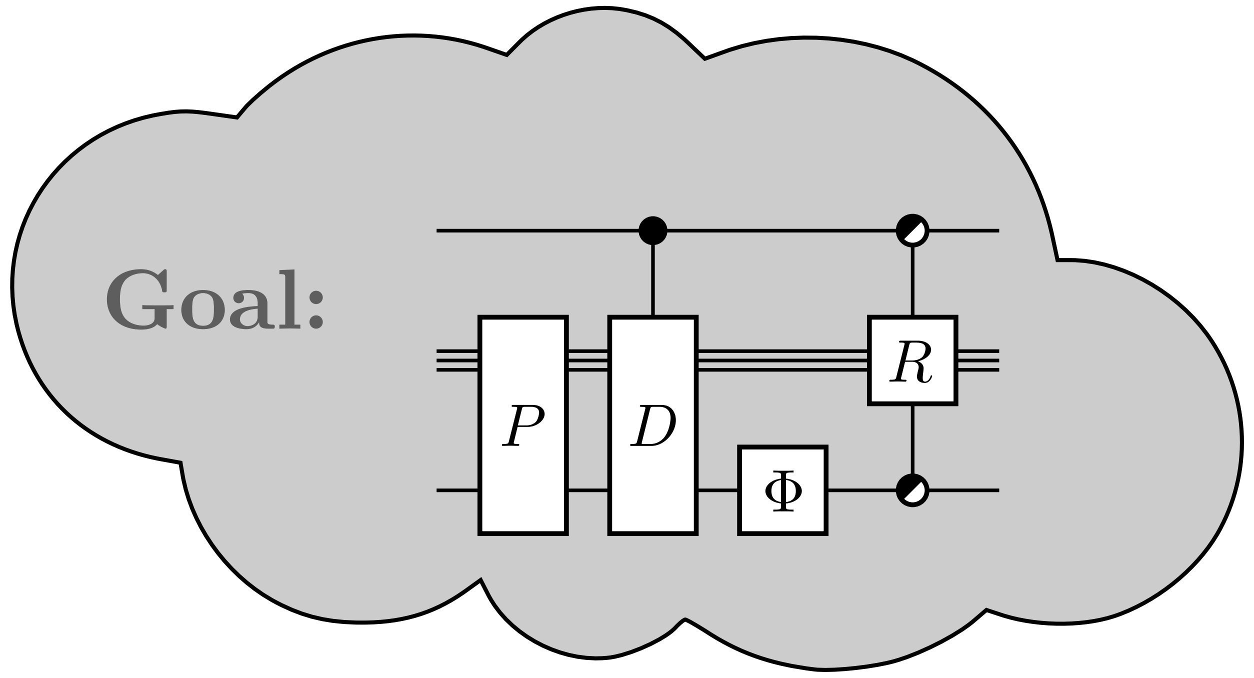
Precomputation identity: proof

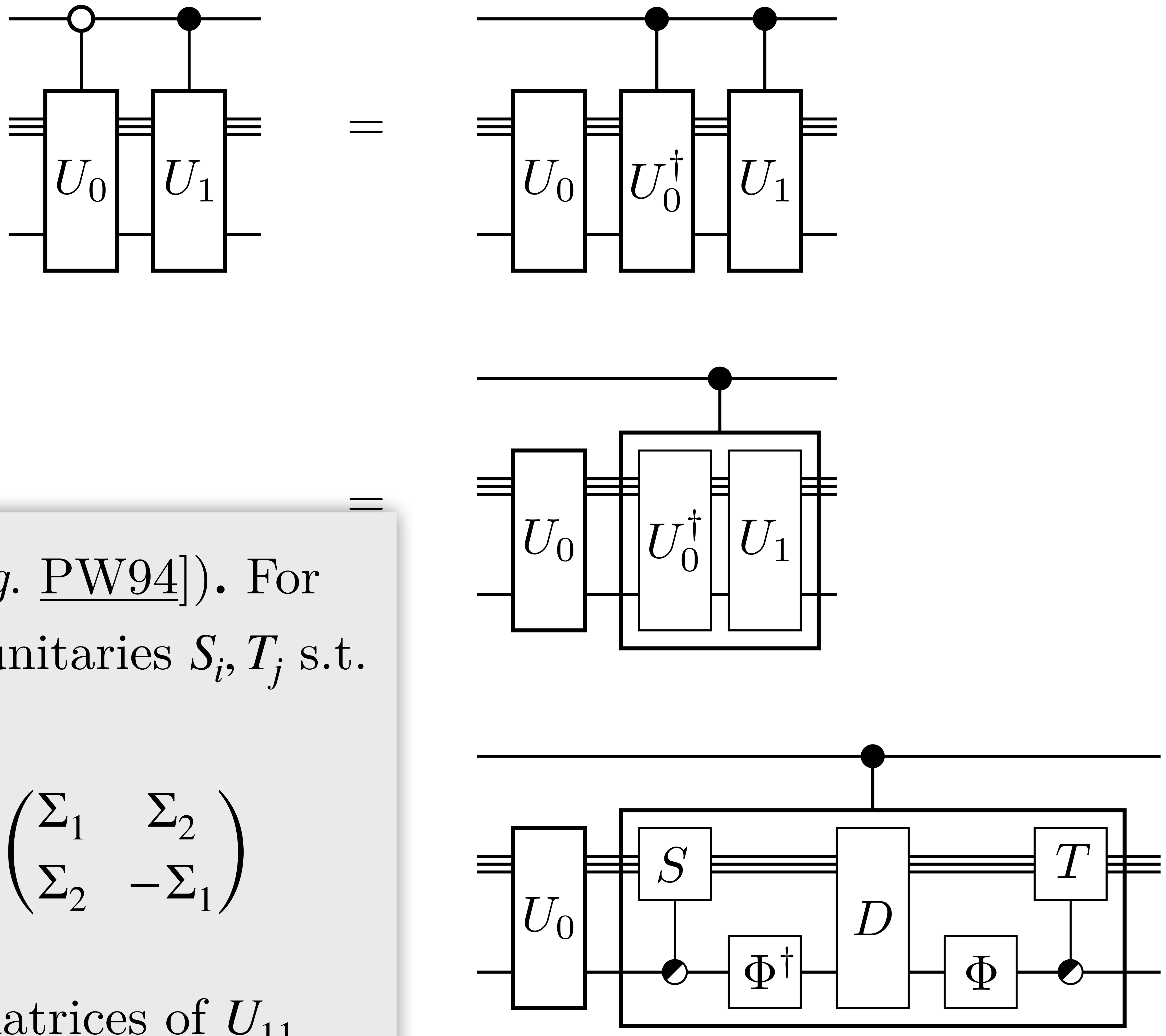




Cosine-Sine decomposition

Precomputation identity: proof





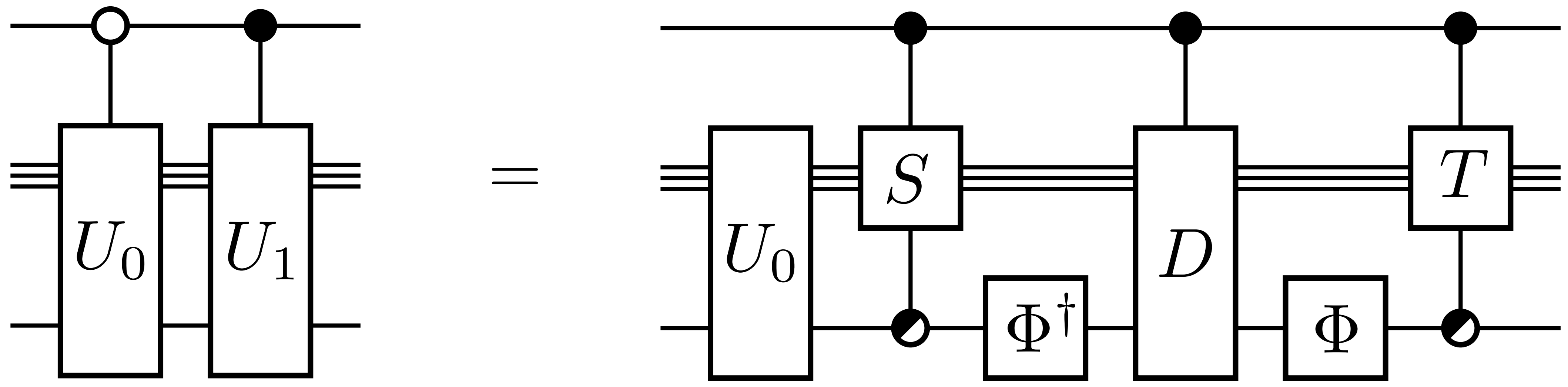
Cosine-Sine decomposition

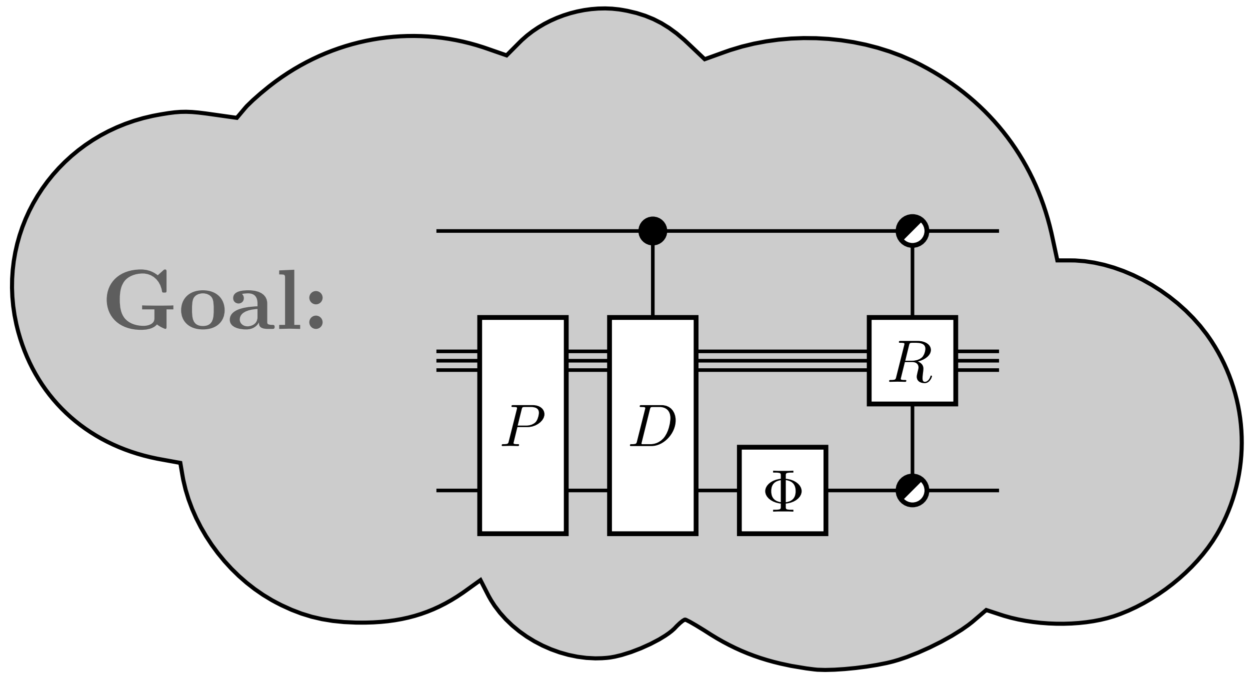
Fact (Cosine-Sine Decomposition [*e.g.* PW94]). For any unitary $U = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix}$, there are unitaries S_i, T_j s.t.

$$\begin{pmatrix} S_1 & 0 \\ 0 & S_2 \end{pmatrix} \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \begin{pmatrix} T_1 & 0 \\ 0 & T_2 \end{pmatrix} = \begin{pmatrix} \Sigma_1 & \Sigma_2 \\ \Sigma_2 & -\Sigma_1 \end{pmatrix}$$

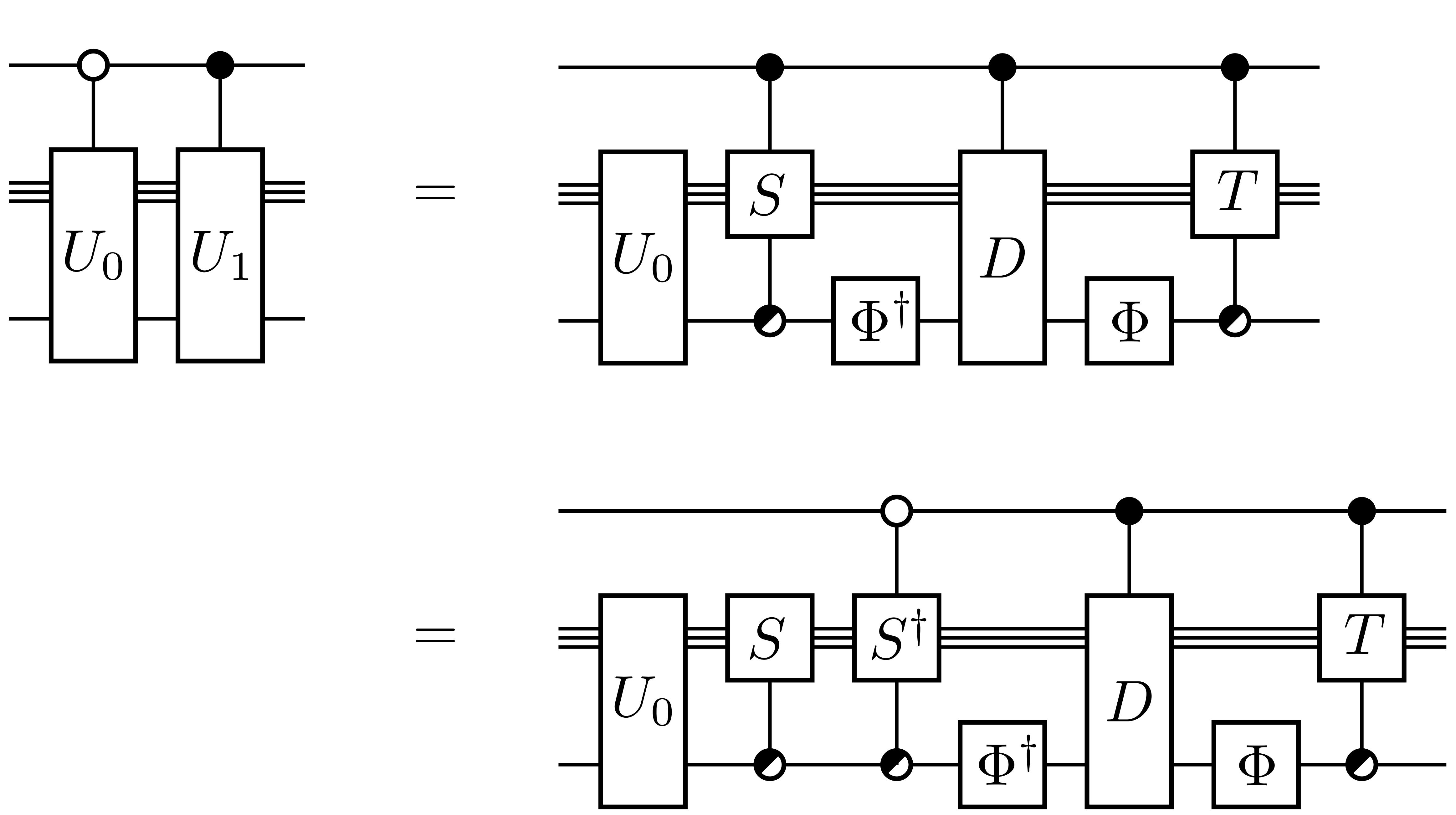
where Σ_1, Σ_2 are the singular value matrices of U_{11} and U_{12} respectively.

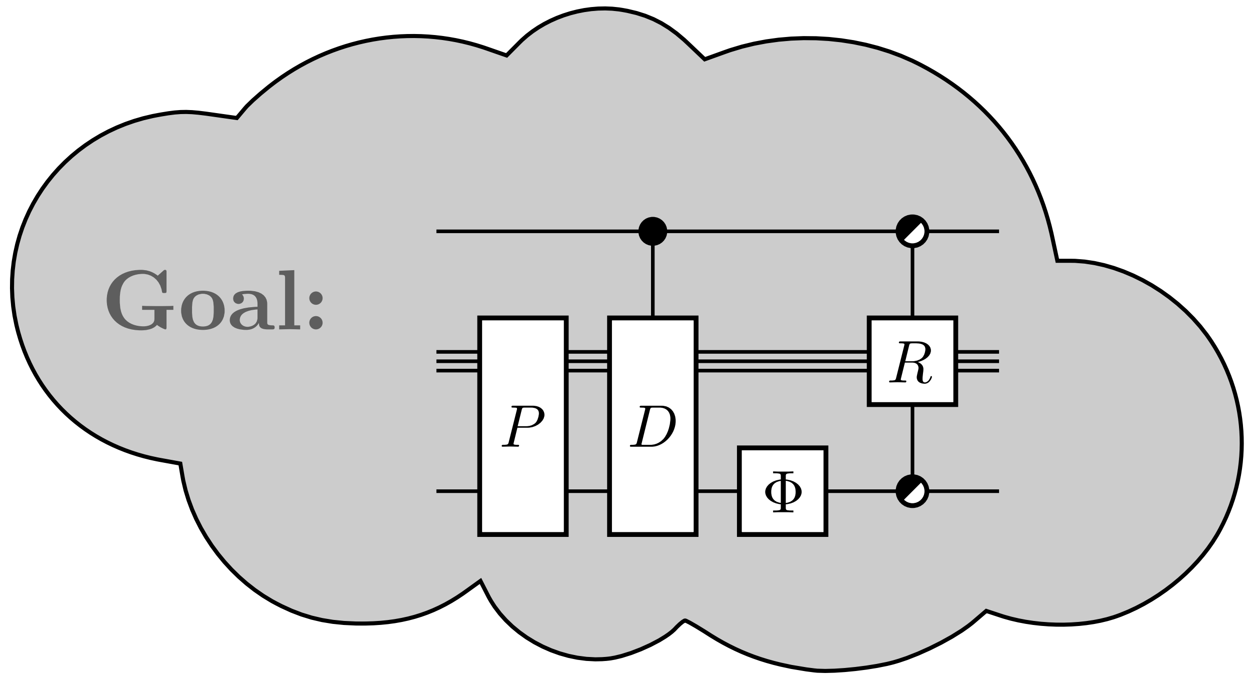
Precomputation identity: proof



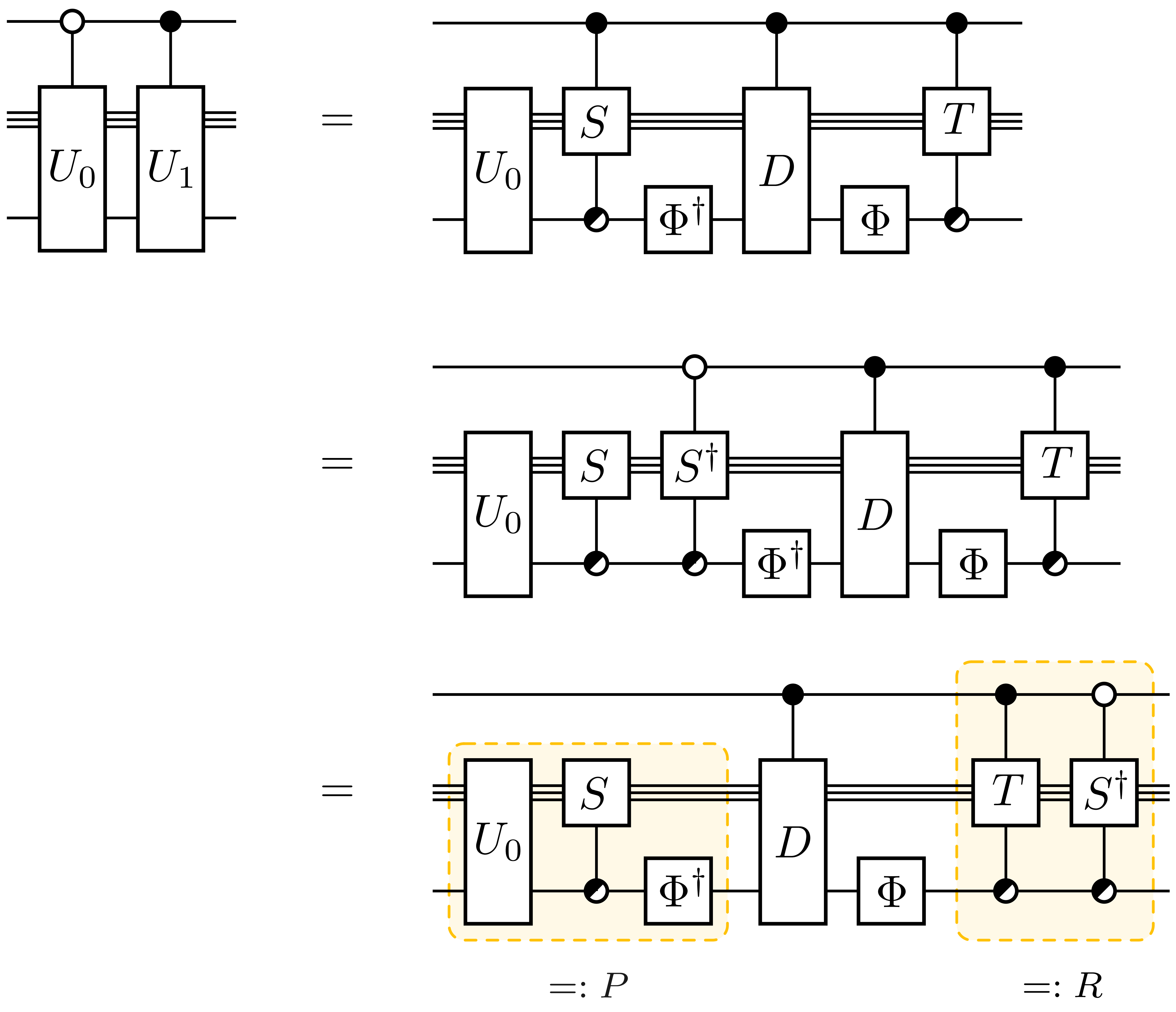


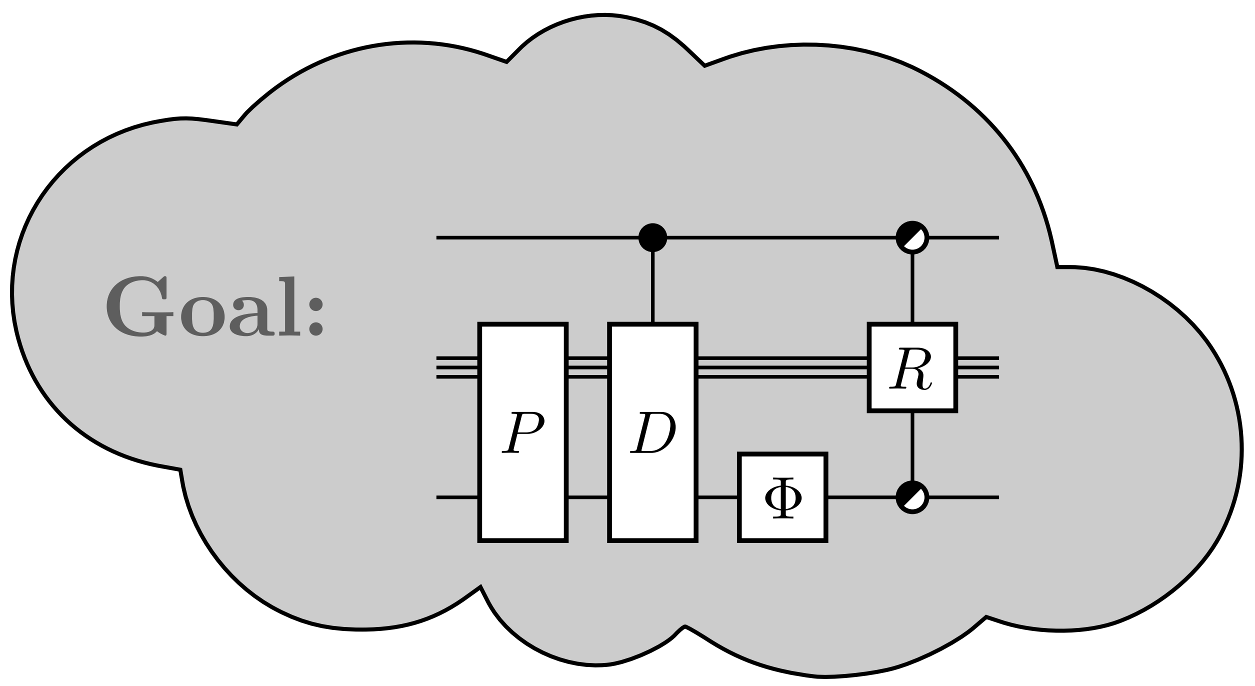
Precomputation identity: proof



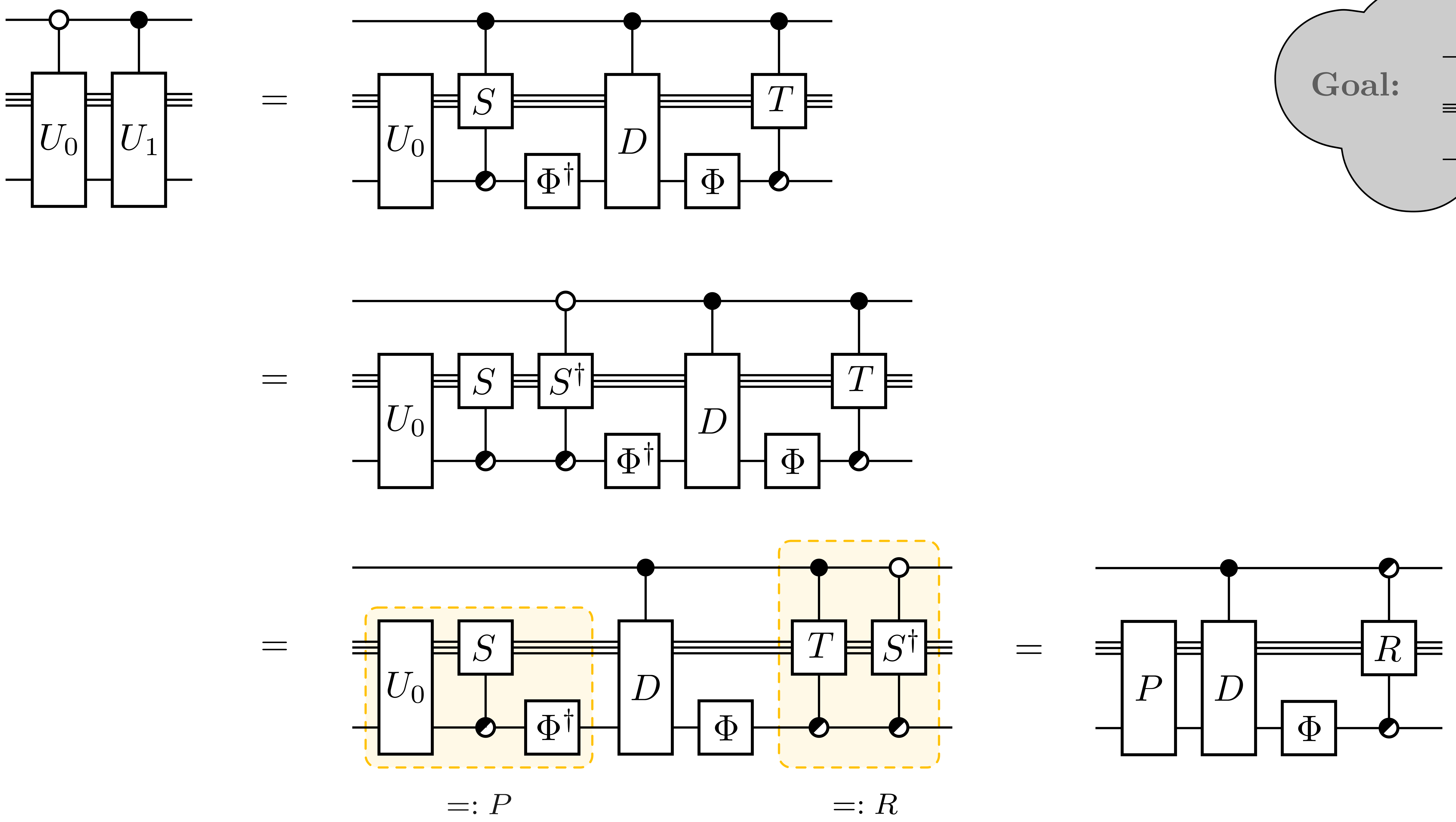


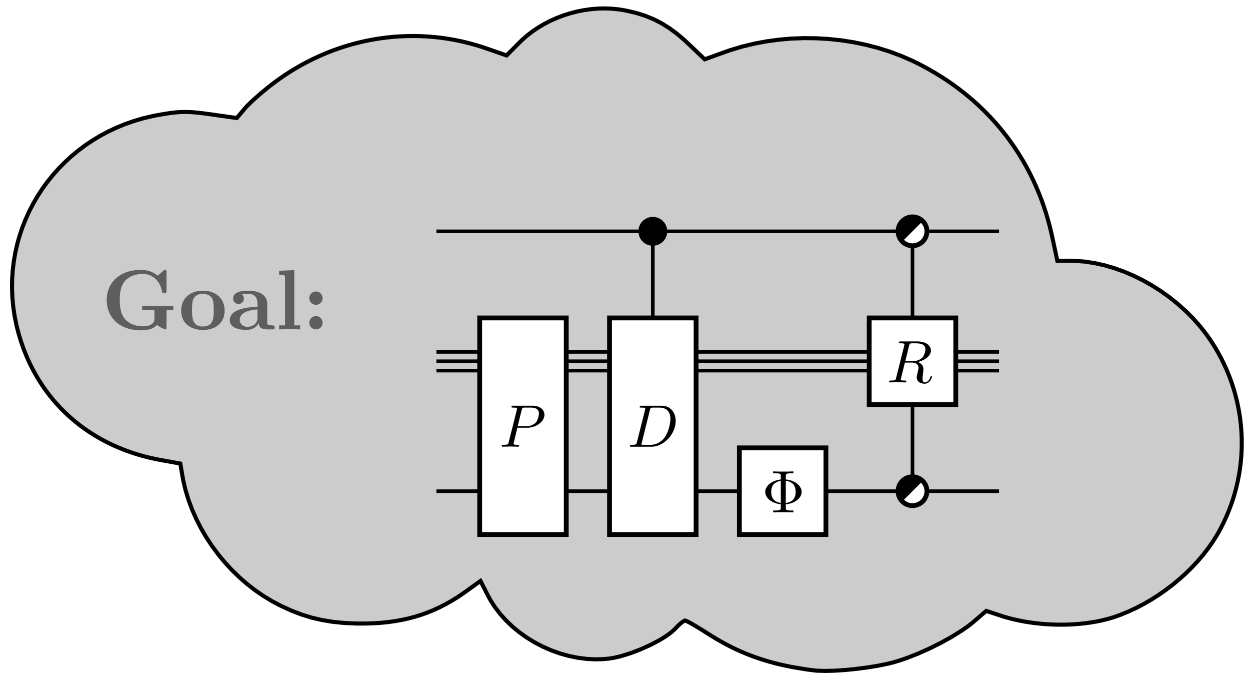
Precomputation identity: proof





Precomputation identity: proof





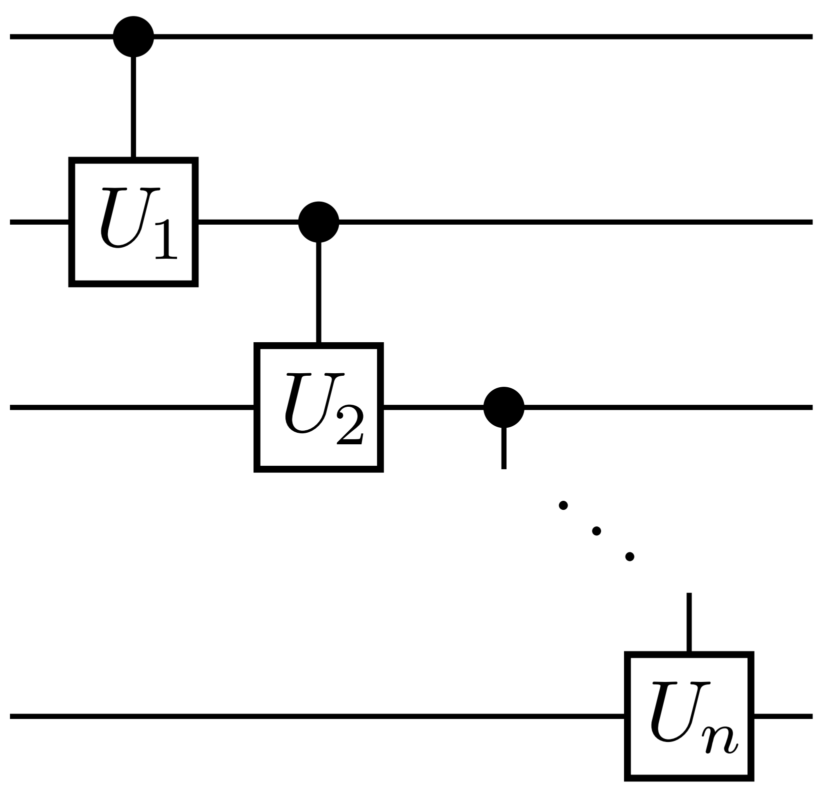
□

Our results

1. Moore–Nilsson unitaries have $O(\log n)$-depth circuits

Theorem. For any 1-qubit unitaries $U_1, \ldots, U_n$, the unitary

$C(U_1, \ldots, U_n) \quad :=$



has an exact, ancilla-free circuit of depth $O(\log n)$.

Bonus: in regime of 2D geometrically-local circuits: $O(\sqrt{n})$ depth, $O(n)$ ancillae

Done

2. Depth reductions for general "control-cascade circuits"

Example corollary. For all $(2 \log n)$-qubit unitaries $U_1, \ldots, U_n$, the unitary $C(U_1, \ldots, U_n)$ has an exact circuit of depth $O(n \log n)$ using $O(n^{3/2})$ ancillae.

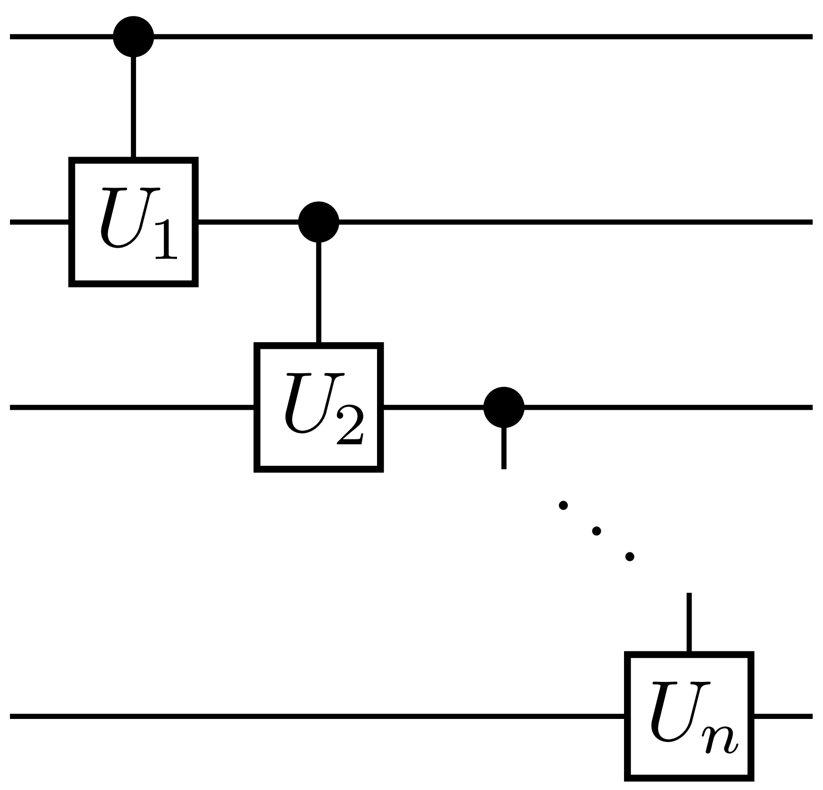
Our results

1. Moore–Nilsson unitaries have $O(\log n)$-depth circuits

Up Next

Theorem. For any 1-qubit unitaries $U_1, \ldots, U_n$, the unitary

$C(U_1, \ldots, U_n) \quad :=$



has an exact, ancilla-free circuit of depth $O(\log n)$.

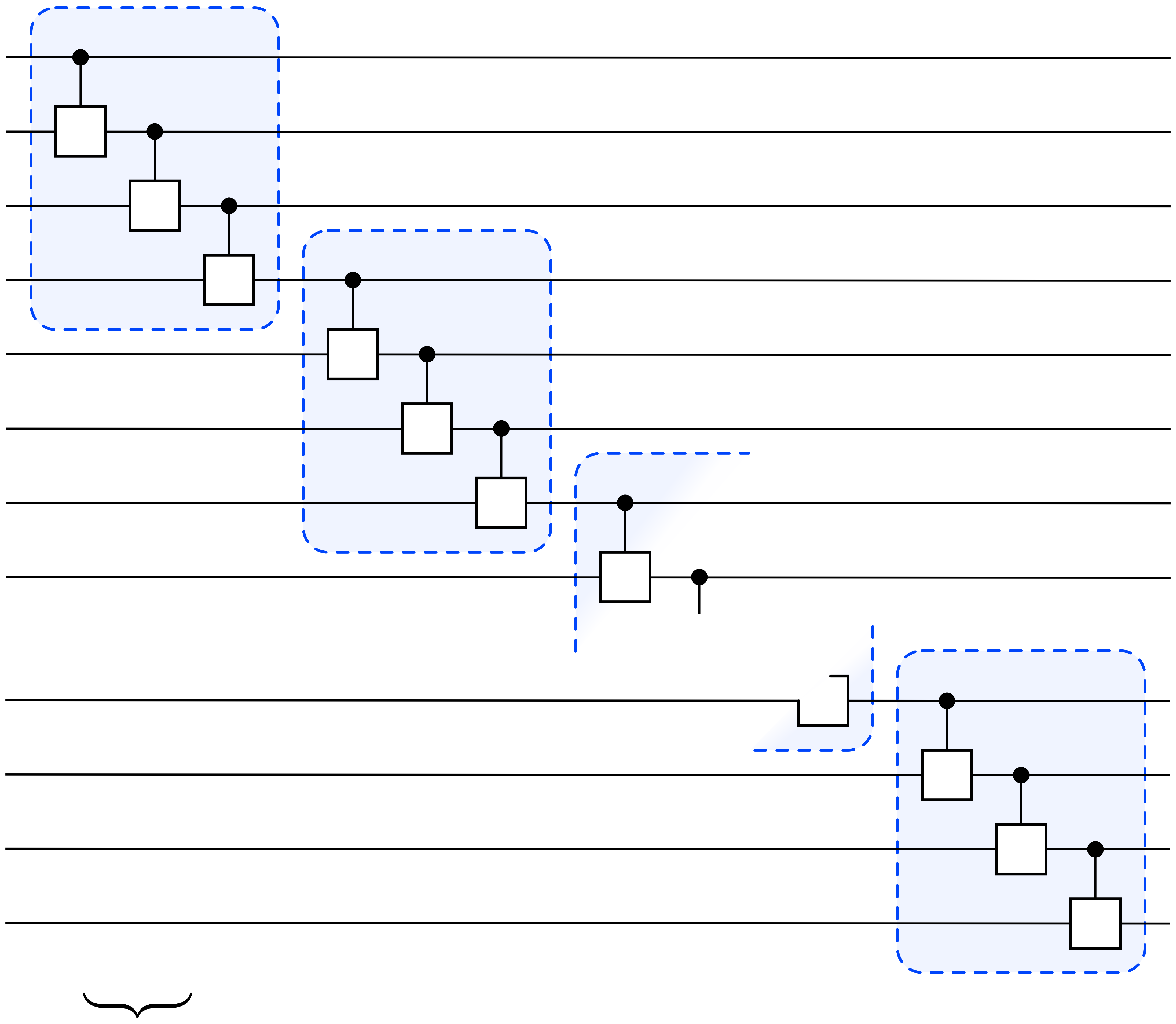
Bonus: in regime of 2D geometrically-local circuits: $O(\sqrt{n})$ depth, $O(n)$ ancillae

2. Depth reductions for general "control-cascade circuits"

Example corollary. For all $(2 \log n)$-qubit unitaries $U_1, \ldots, U_n$, the unitary $C(U_1, \ldots, U_n)$ has an exact circuit of depth $O(n \log n)$ using $O(n^{3/2})$ ancillae.

Refuting the Moore–Nilsson conjecture

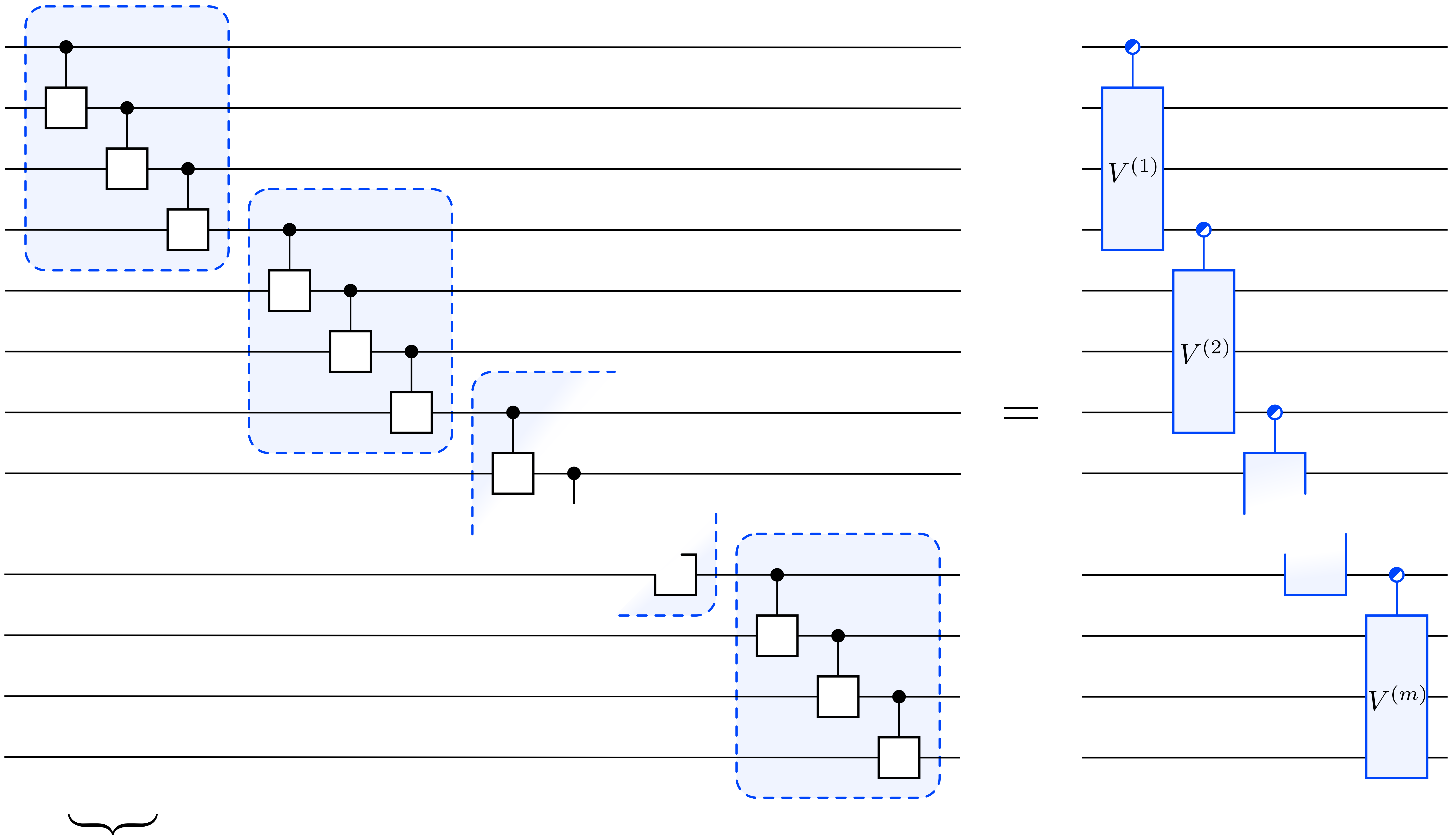
Step 1. Group control-U's into blocks



k-many Control-U's per block

Refuting the Moore–Nilsson conjecture

Step 1. Group control-U's into blocks



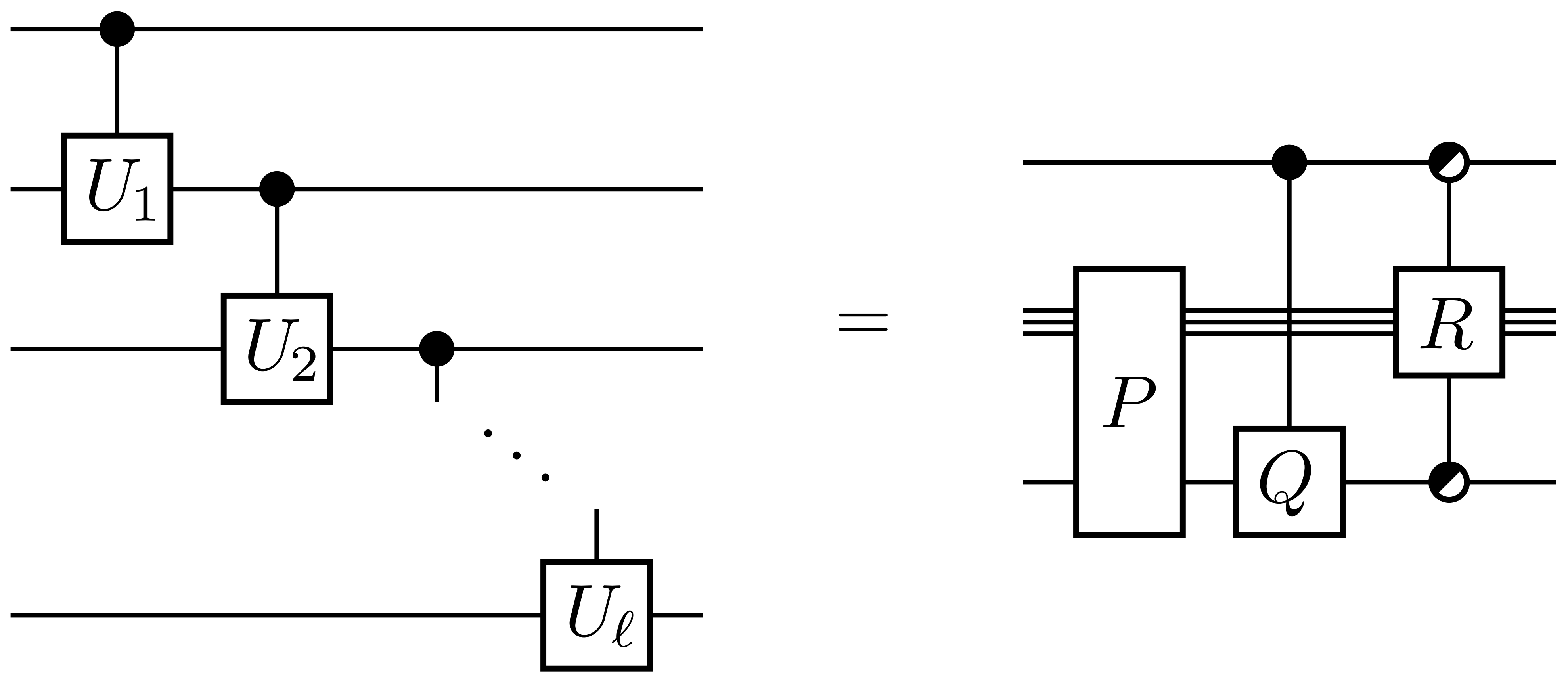
k-many Control-U's per block

$m = n/k$ different $V^{(i)}$'s

Refuting the Moore–Nilsson conjecture

Lemma (Precomputation for Moore–Nilsson circuits)**.**

There exist unitaries P, Q, R on ℓ, 1, and $\ell - 1$ qubits respectively so that

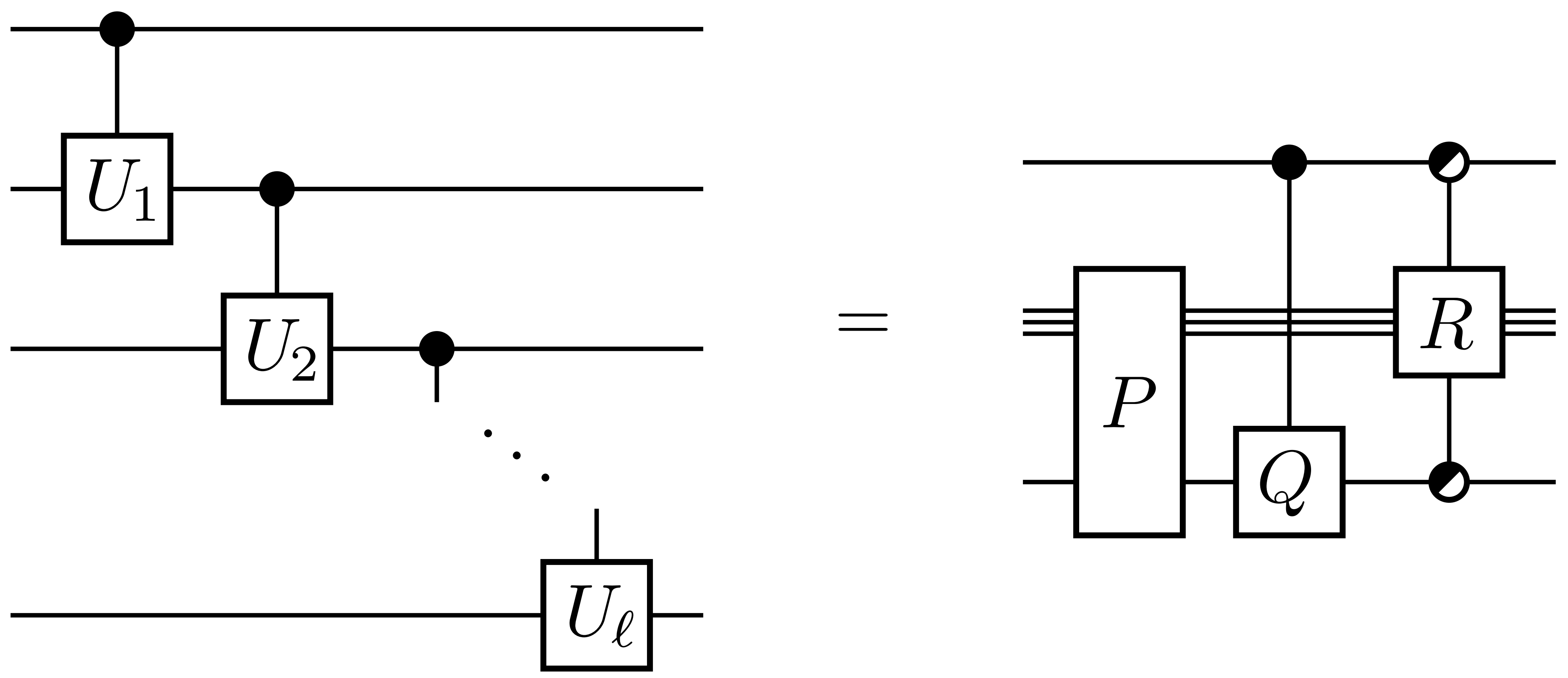


Step 2. Prove a better precomputation identity

Refuting the Moore–Nilsson conjecture

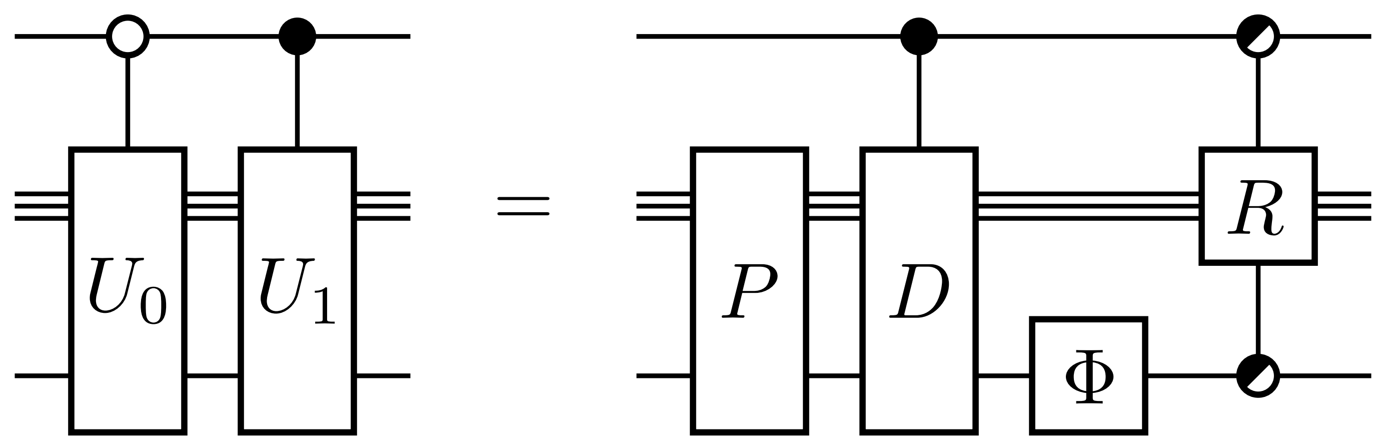
Lemma (Precomputation for Moore–Nilsson circuits)**.**

There exist unitaries P, Q, R on ℓ, 1, and $\ell - 1$ qubits respectively so that

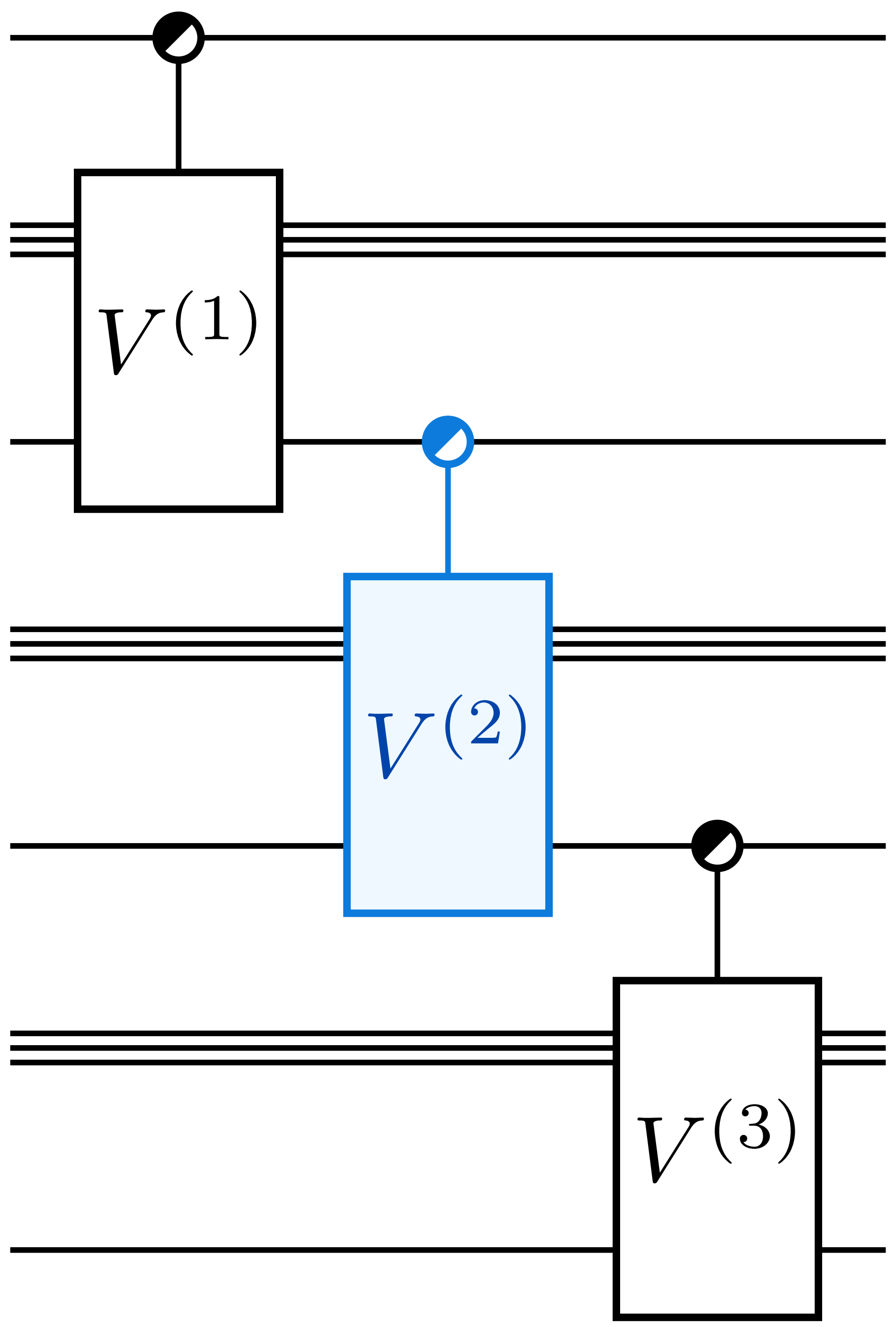


Step 2. Prove a better precomputation identity

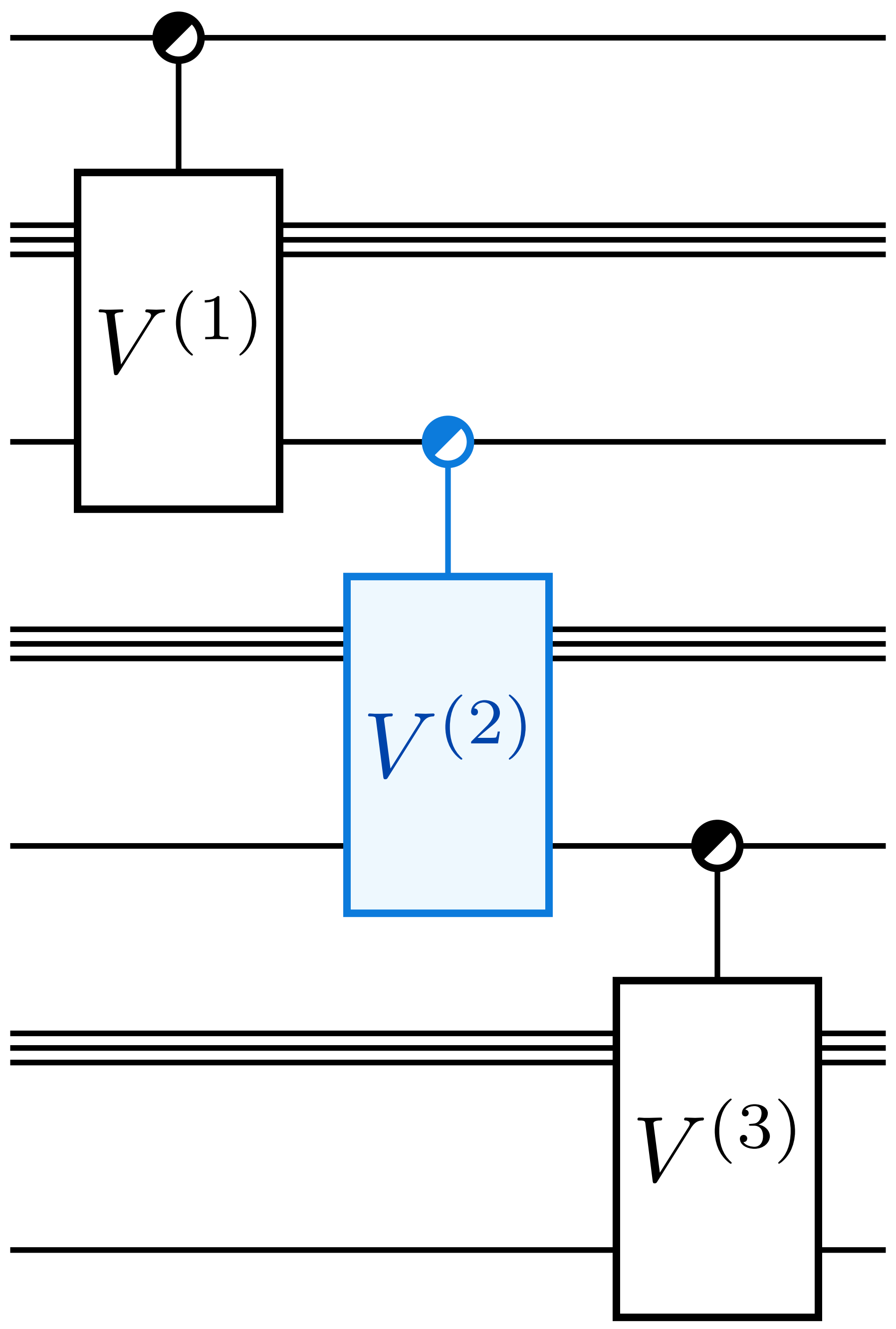
C.f. generic precomputation identity



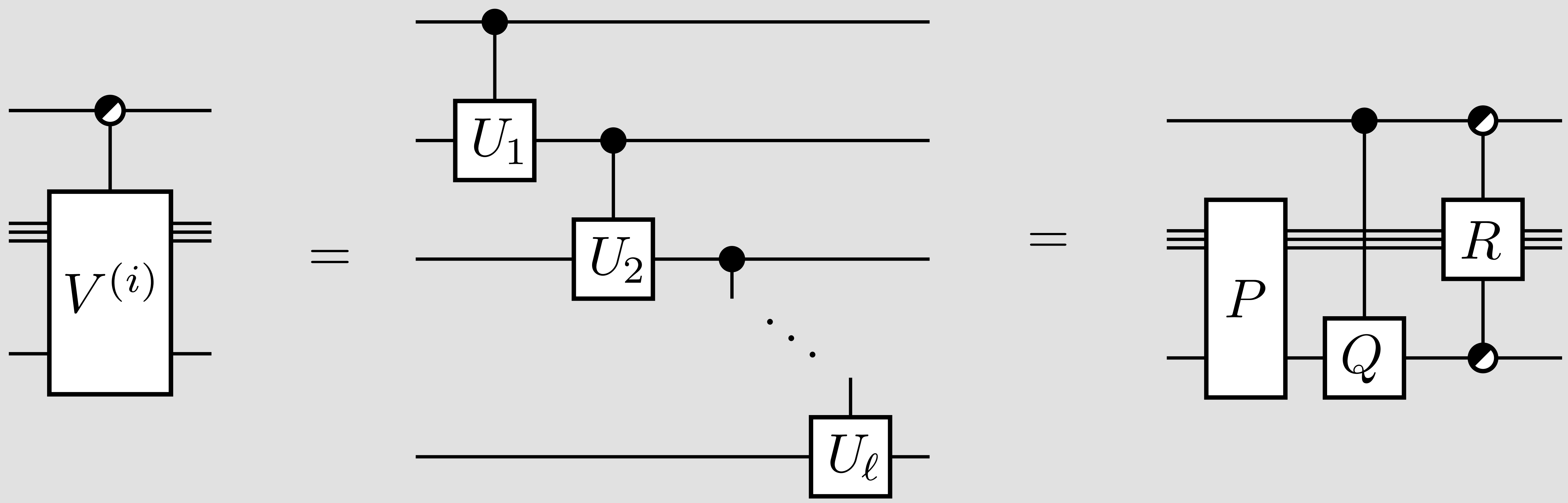
for D diagonal and Φ a universal (fixed) unitary.

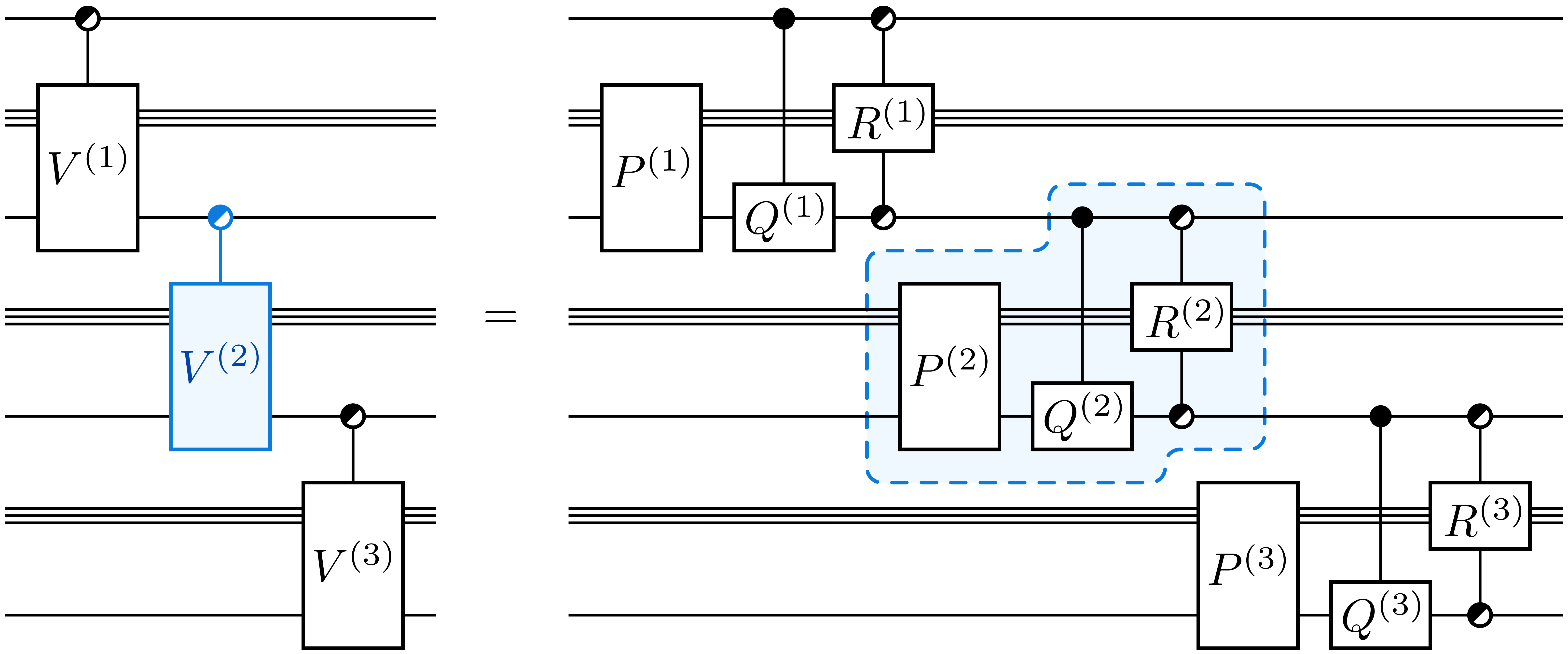


$V^{(1)}$
$V^{(2)}$
$V^{(3)}$

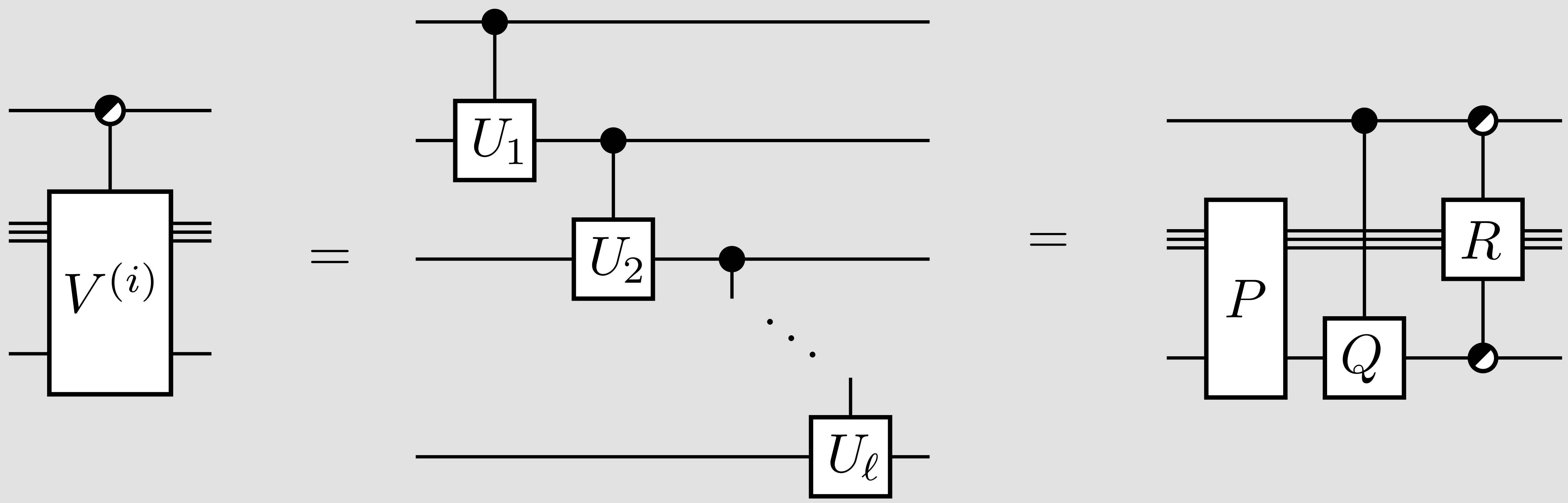


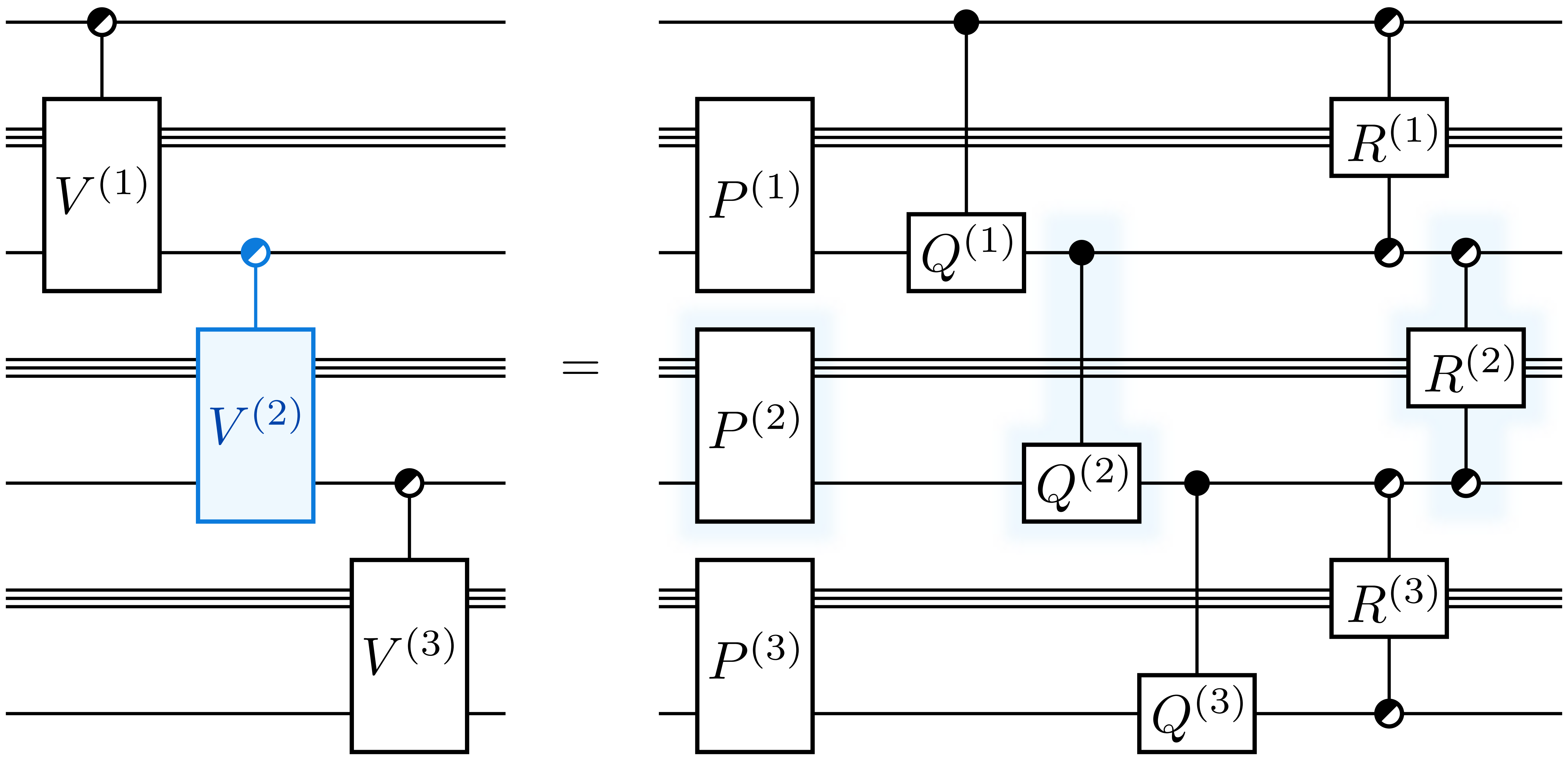
With



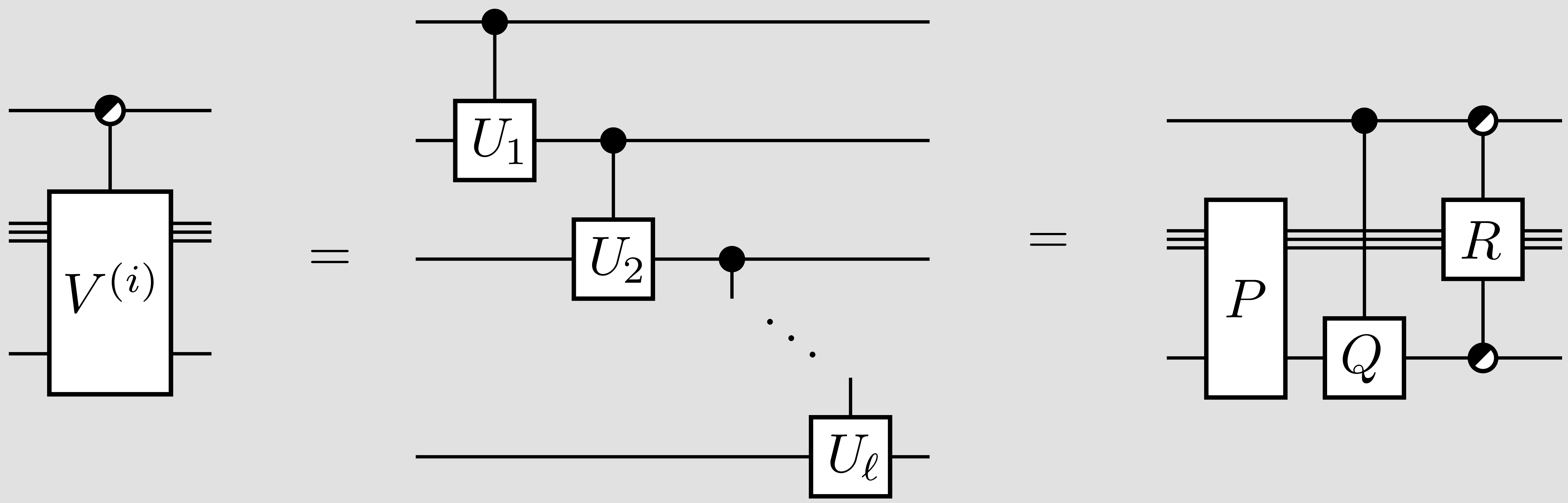


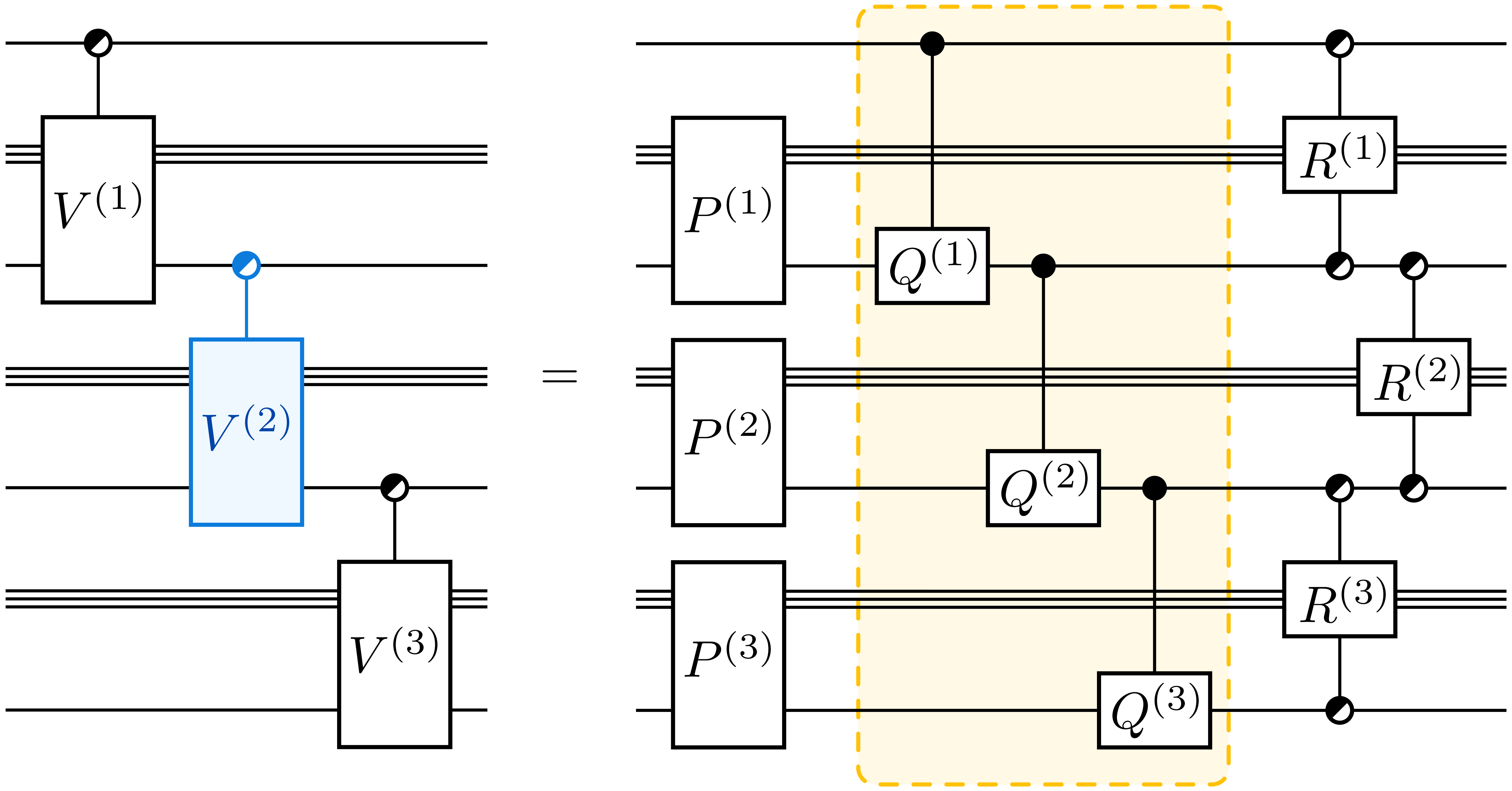
With





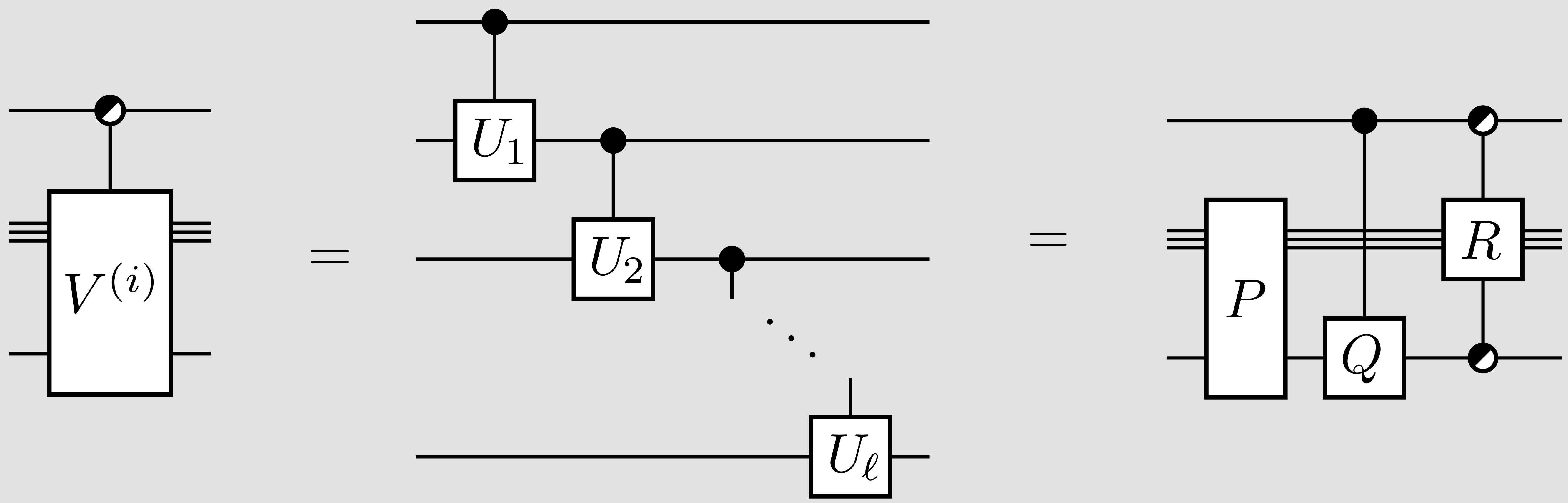
With

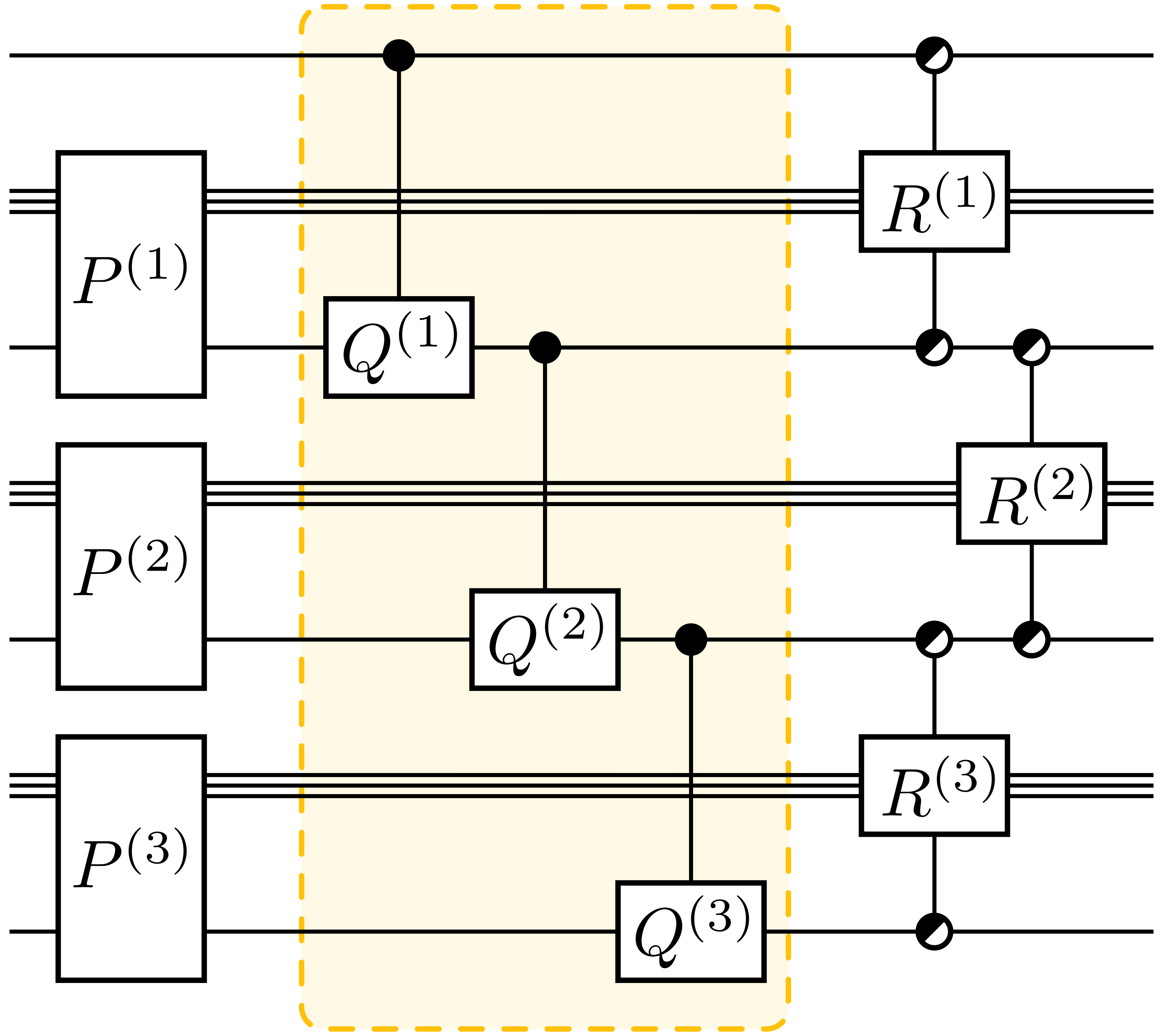




$=: \mathcal{C}(Q^{(1)}, Q^{(2)}, \ldots)$

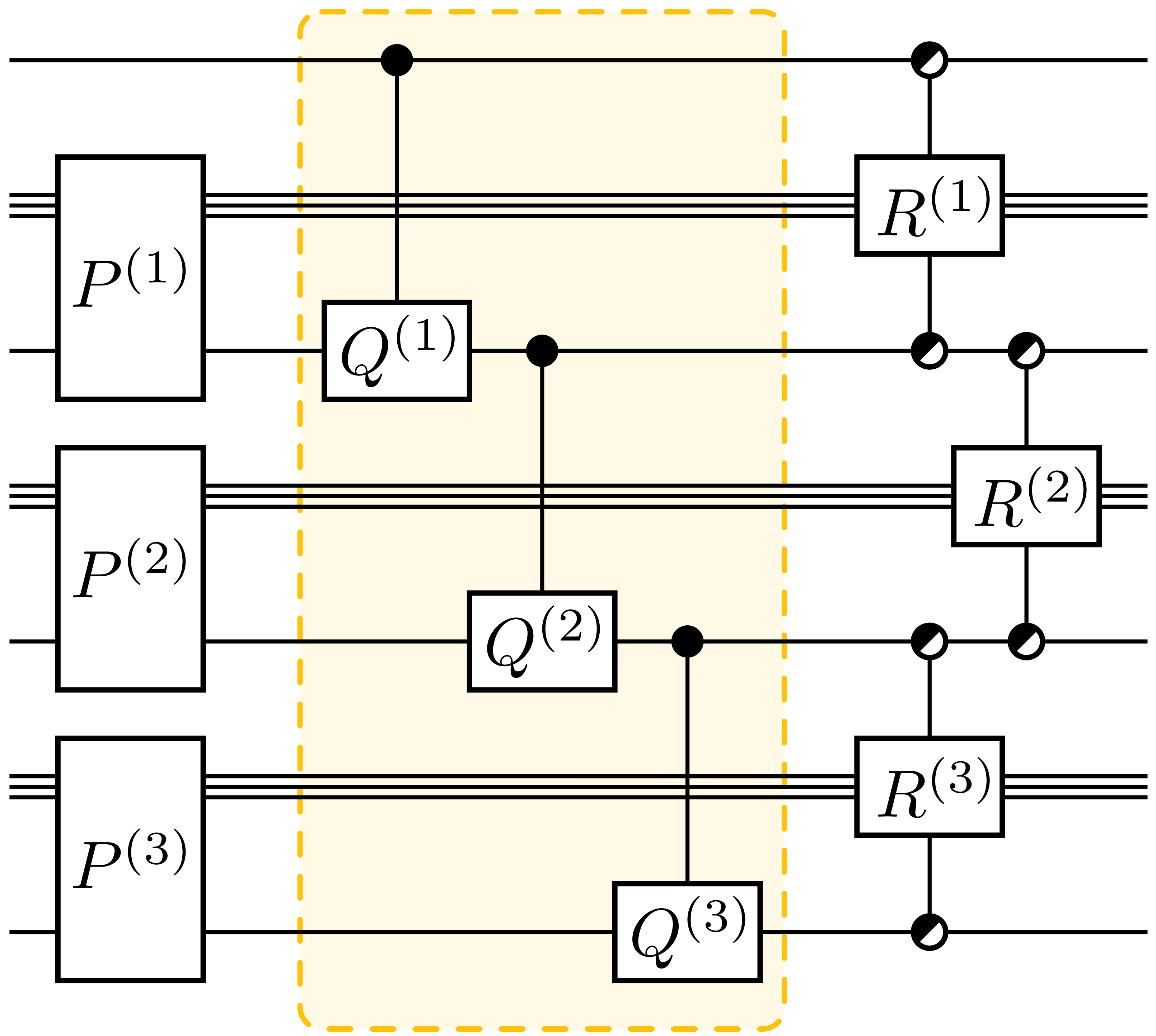
With

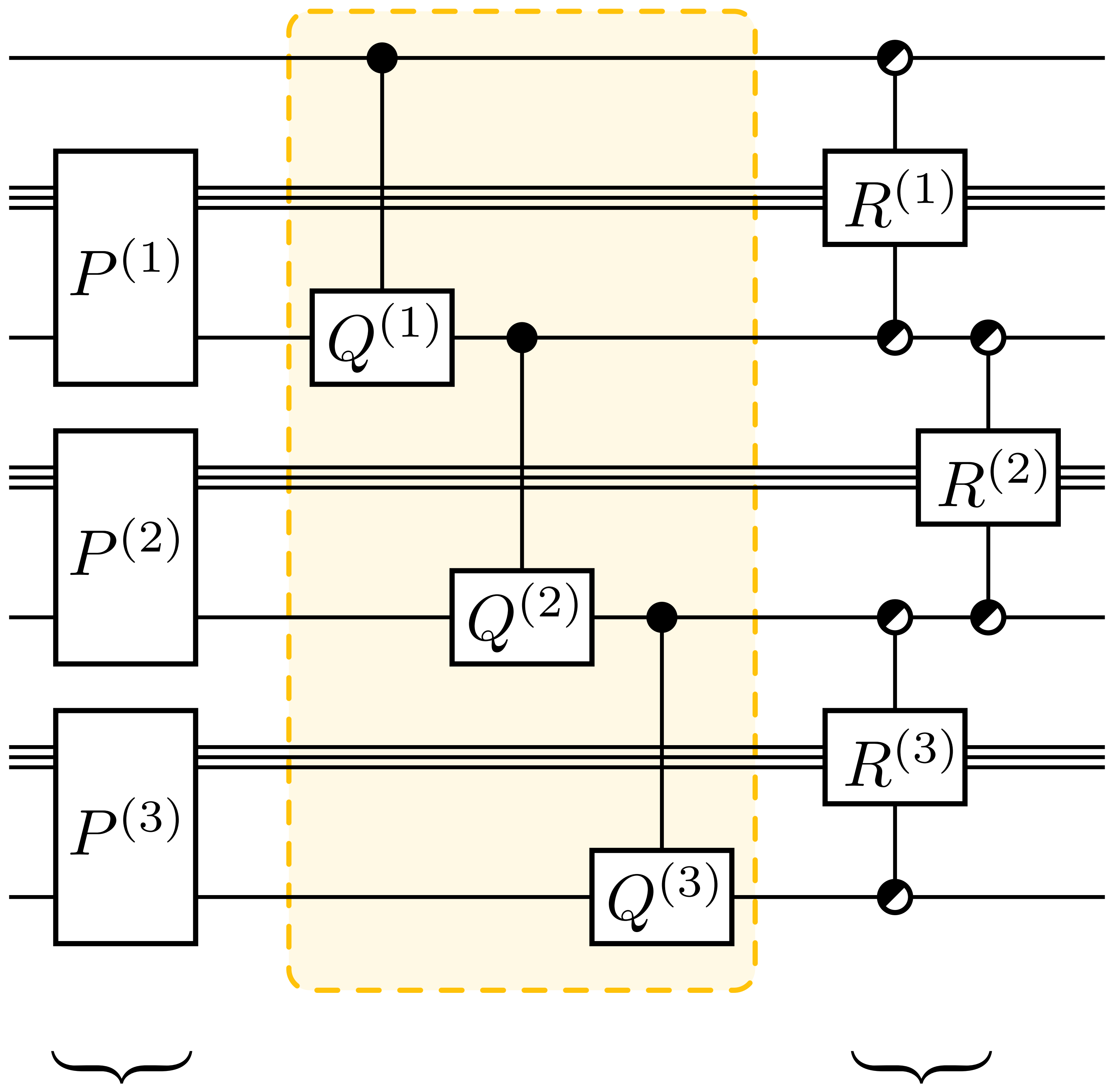




$P^{(1)}$
$P^{(2)}$
$P^{(3)}$
$Q^{(1)}$
$Q^{(2)}$
$Q^{(3)}$
$R^{(1)}$
$R^{(2)}$
$R^{(3)}$

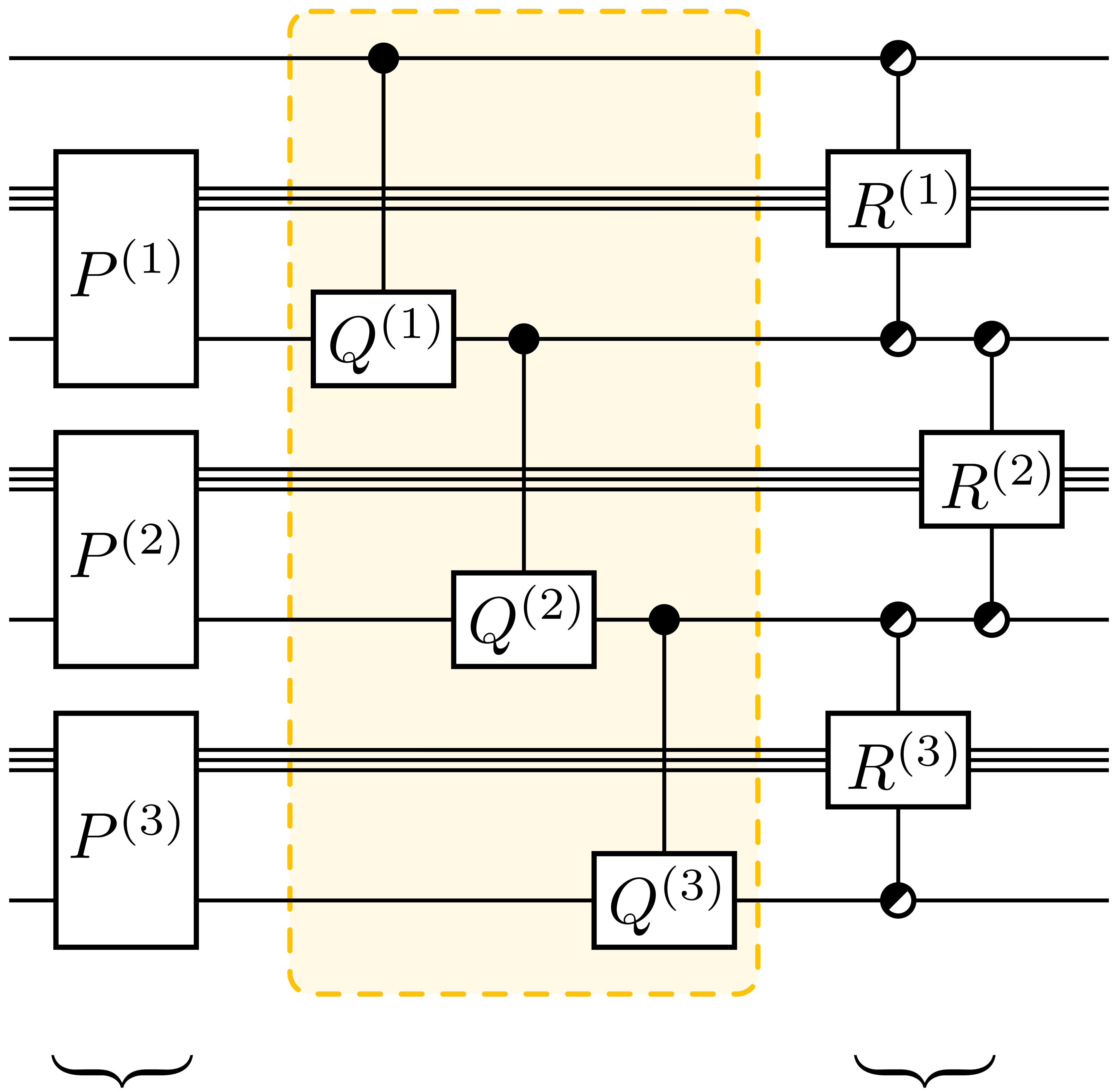
Definition. Let $\mathbf{MN}(n)$ be the minimum depth of $C(\overrightarrow{U})$.





Definition. Let MN(n) be the minimum depth of $C(\overrightarrow{U})$.

Then $$\mathrm{MN}(n) \leq \underbrace{}_{4^k} + \mathrm{MN}\left(\frac{n}{k}\right) + \underbrace{}_{4^k}$$

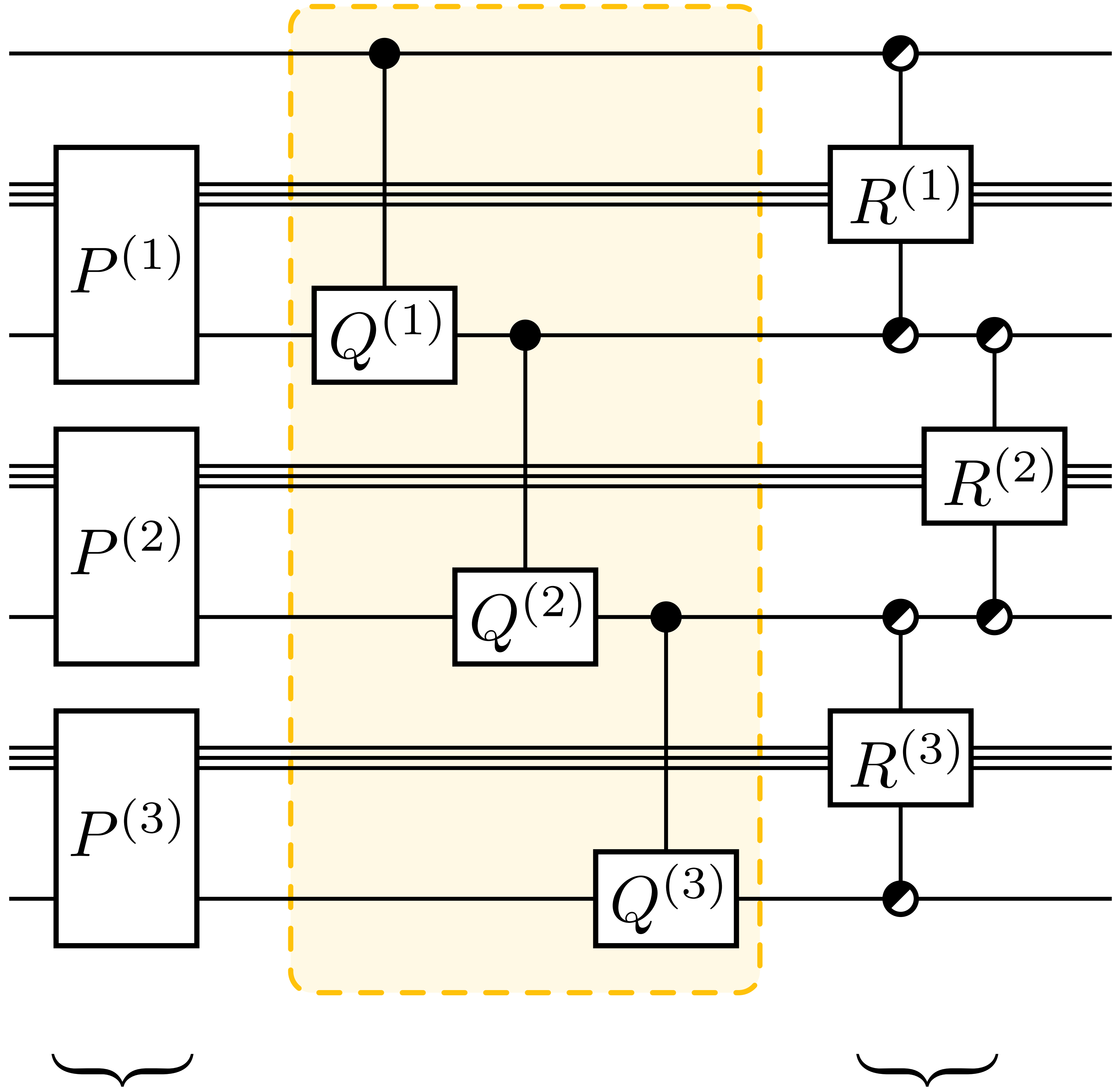


Definition. Let MN(n) be the minimum depth of $C(\overrightarrow{U})$.

Then $$\mathrm{MN}(n) \leq 4^k + \mathrm{MN}\left(\frac{n}{k}\right) + 4^k$$

And after ℓ iterations:

$$\mathrm{MN}(n) \leq 2\ell \cdot 4^k + \mathrm{MN}\left(\frac{n}{k^\ell}\right)$$



Definition. Let MN(n) be the minimum depth of $C(\overrightarrow{U})$.

Then

$$\mathrm{MN}(n) \leq 4^k + \mathrm{MN}\left(\frac{n}{k}\right) + 4^k$$

And after ℓ iterations:

$$\mathrm{MN}(n) \leq 2\ell \cdot 4^k + \mathrm{MN}\left(\frac{n}{k^\ell}\right)$$

Put $\ell = \Theta(\log n)$ and $k = \Theta(1)$:

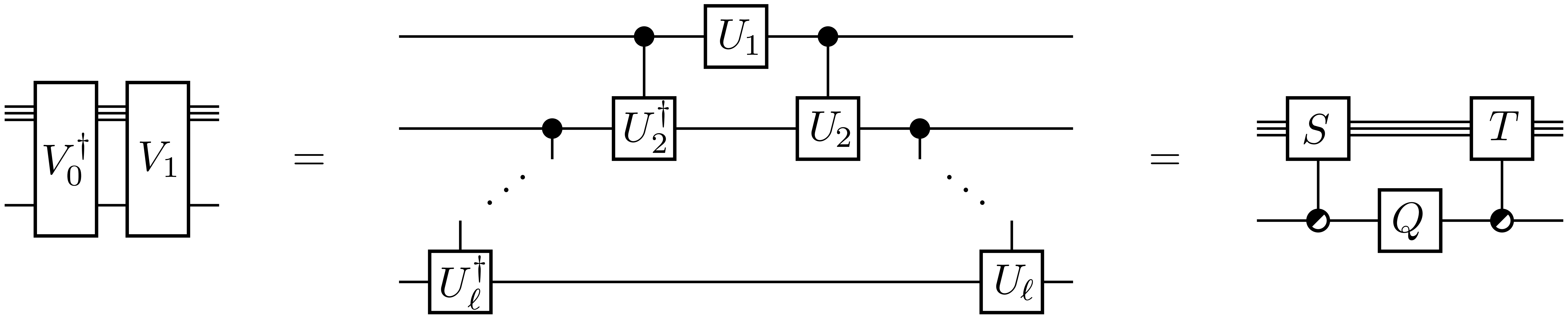
$$\mathrm{MN}(n) \leq O(\log n)$$

□

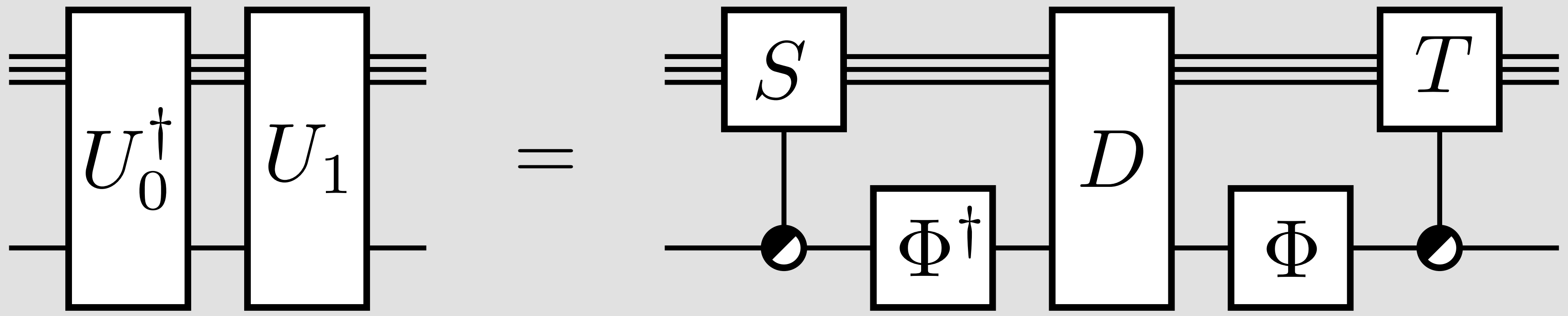
Refuting the Moore–Nilsson conjecture: improved precomputation

Under the hood: a special structure for the relevant Cosine-Sine Decomposition

For the Moore–Nilsson circuits $C(\vec{U})$,



C.f. the general case from the CS decomposition



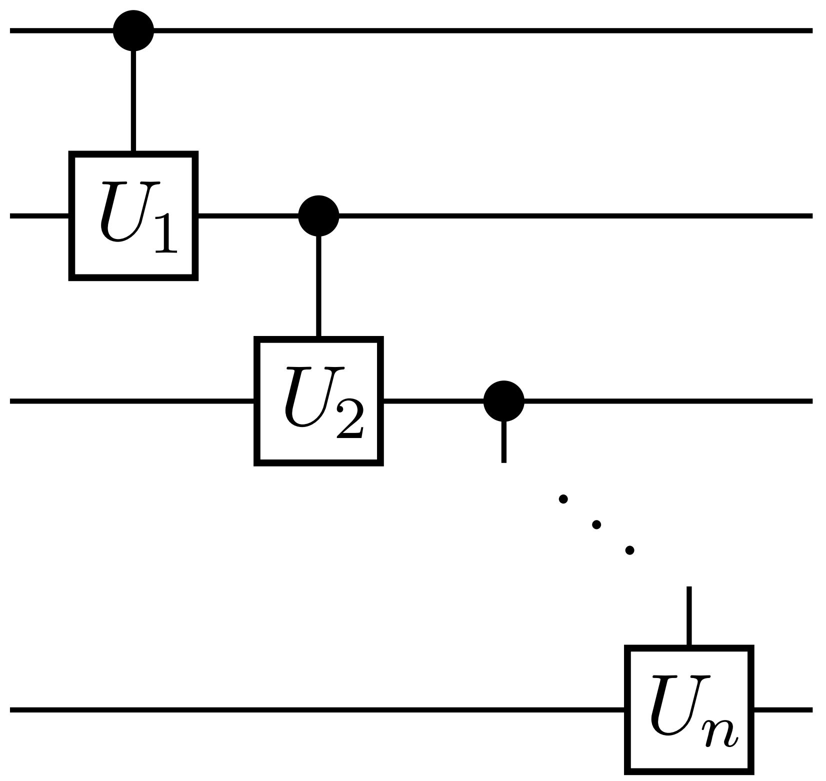
Our results

1. Moore–Nilsson unitaries have $O(\log n)$-depth circuits

Done

Theorem. For any 1-qubit unitaries $U_1, \ldots, U_n$, the unitary

$C(U_1, \ldots, U_n) \quad :=$



has an exact, ancilla-free circuit of depth $O(\log n)$.

Bonus: in regime of 2D geometrically-local circuits: $O(\sqrt{n})$ depth, $O(n)$ ancillae

Done

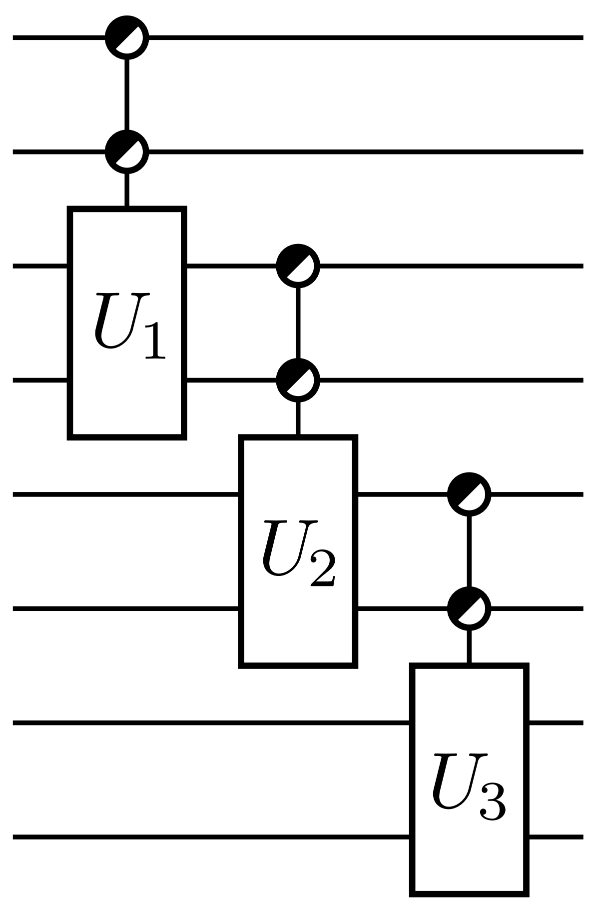
2. Depth reductions for general "control-cascade circuits"

Example corollary. For all $(2 \log n)$-qubit unitaries $U_1, \ldots, U_n$, the unitary $C(U_1, \ldots, U_n)$ has an exact circuit of depth $O(n \log n)$ using $O(n^{3/2})$ ancillae.

Next steps

Next steps

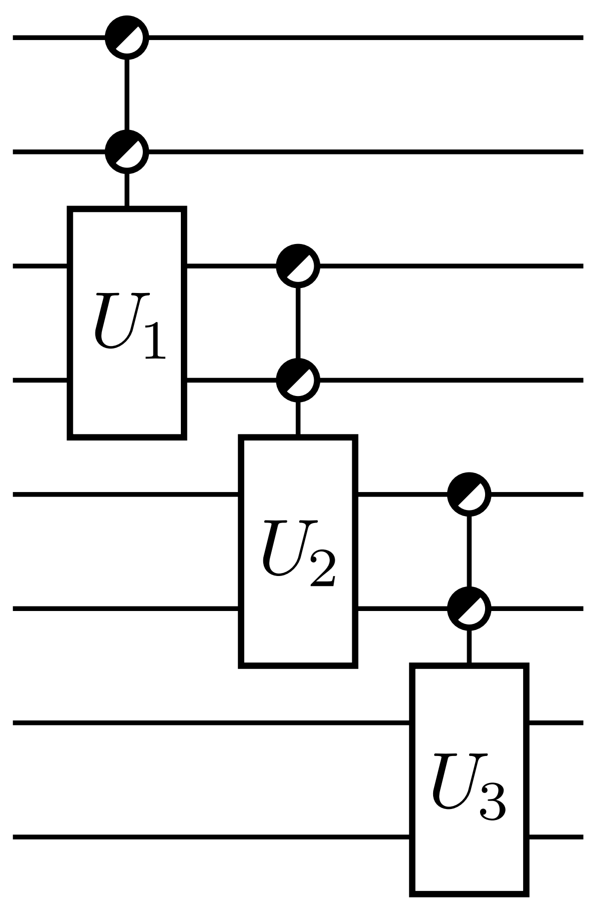
Beyond one qubit of control



Cosine-Sine decomposition approach already blocked at qutrit controls...

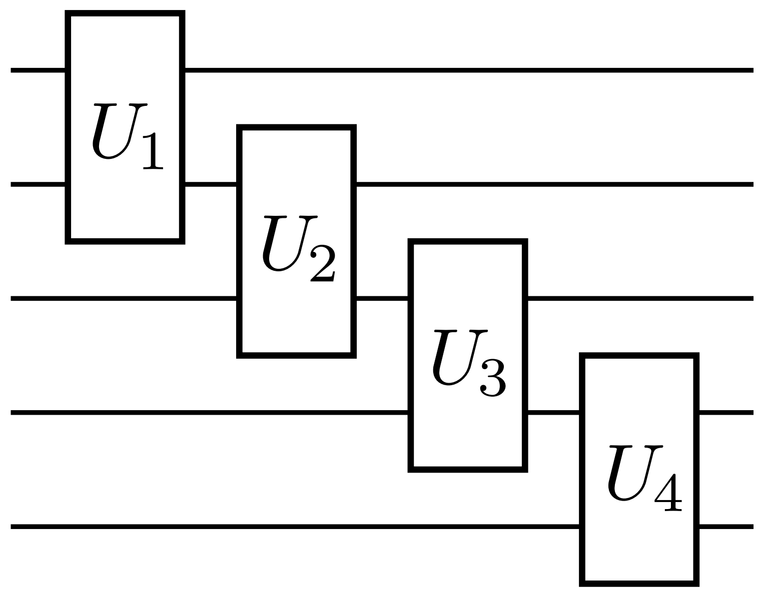
Next steps

Beyond one qubit of control



Cosine-Sine decomposition approach already blocked at qutrit controls...

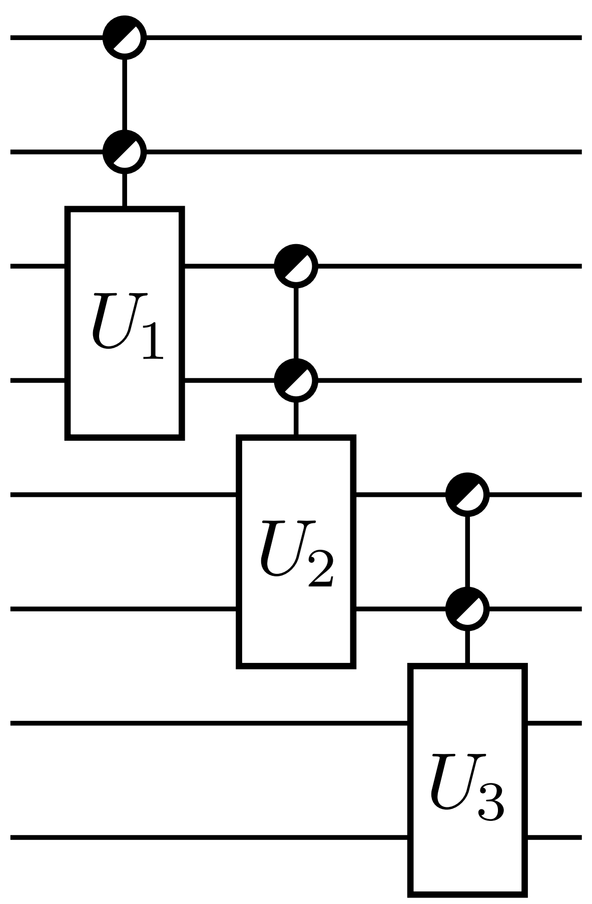
Cascades of general unitaries



Unclear how to prove a precomputation identity here...

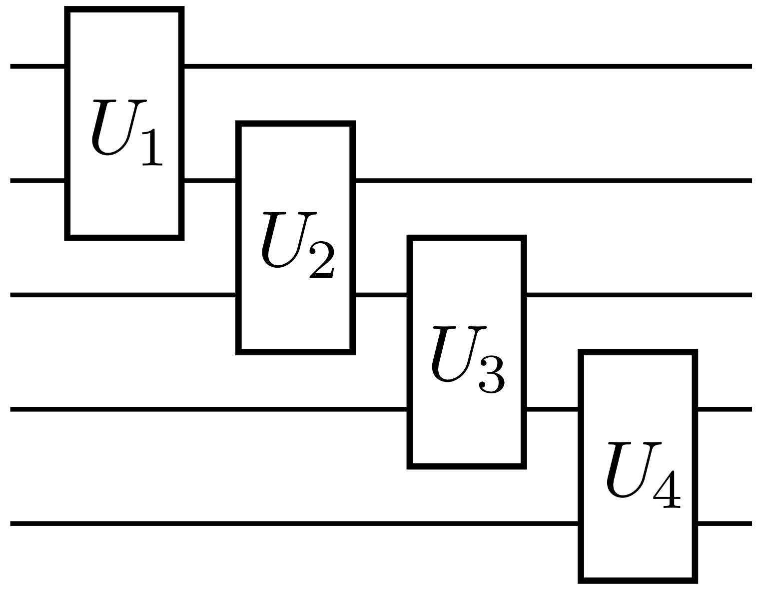
Next steps

Beyond one qubit of control



Cosine-Sine decomposition approach already blocked at qutrit controls...

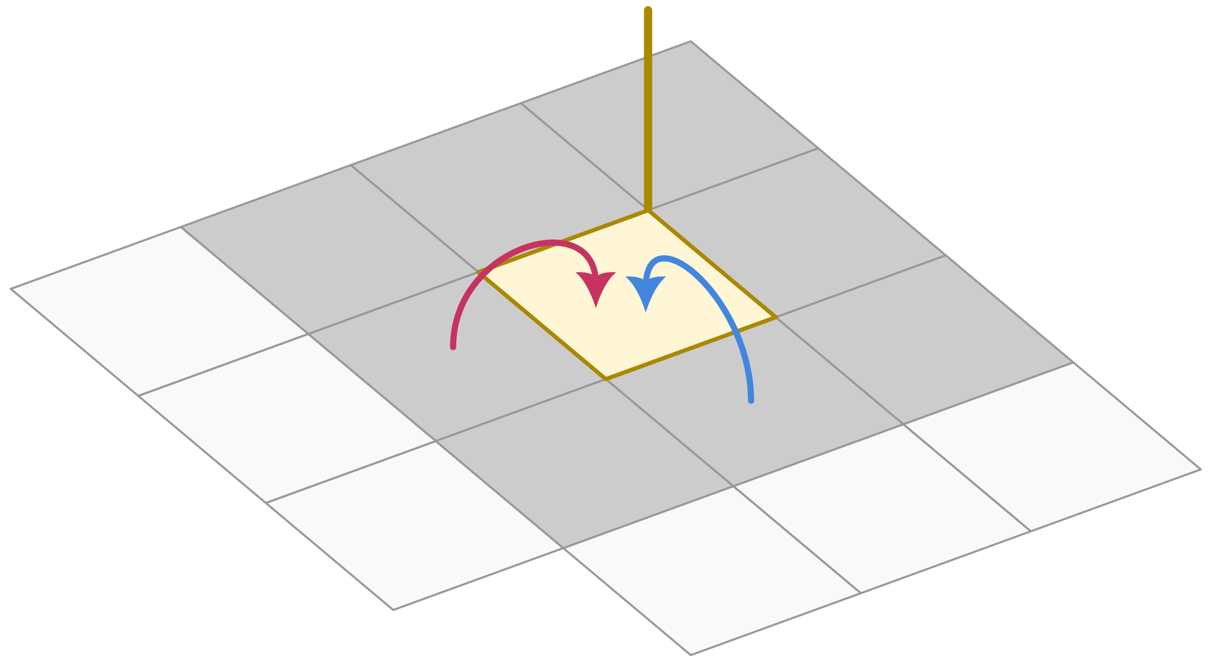
Cascades of general unitaries

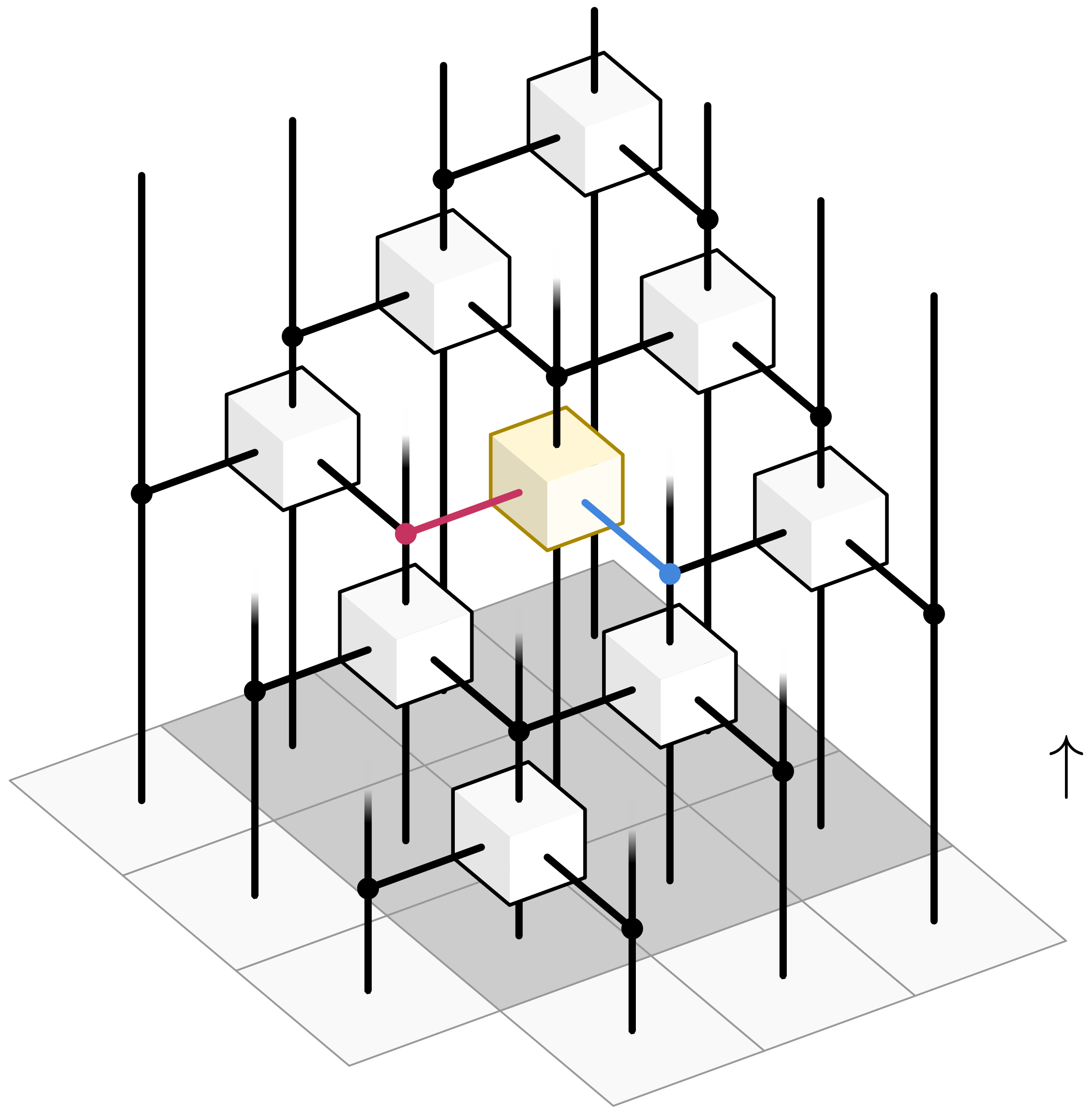


Unclear how to prove a precomputation identity here...

Quantum dynamic programming?

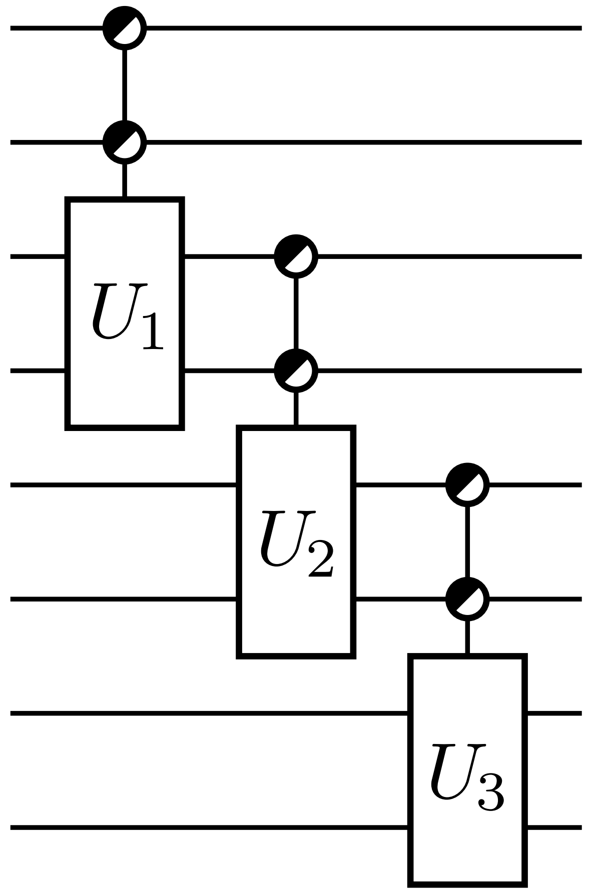
$$T(m,n) = f\big(T(m-1,n), T(m,n-1)\big)$$





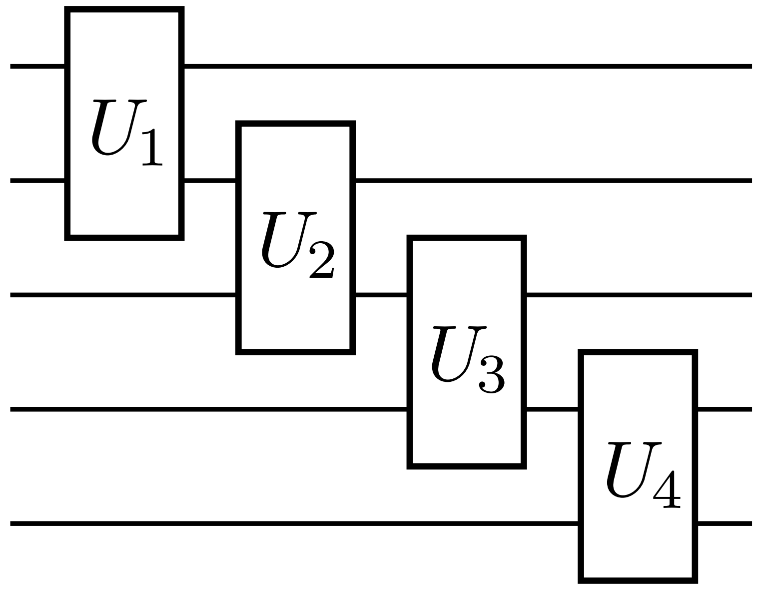
Next steps

Beyond one qubit of control



Cosine-Sine decomposition approach already blocked at qutrit controls...

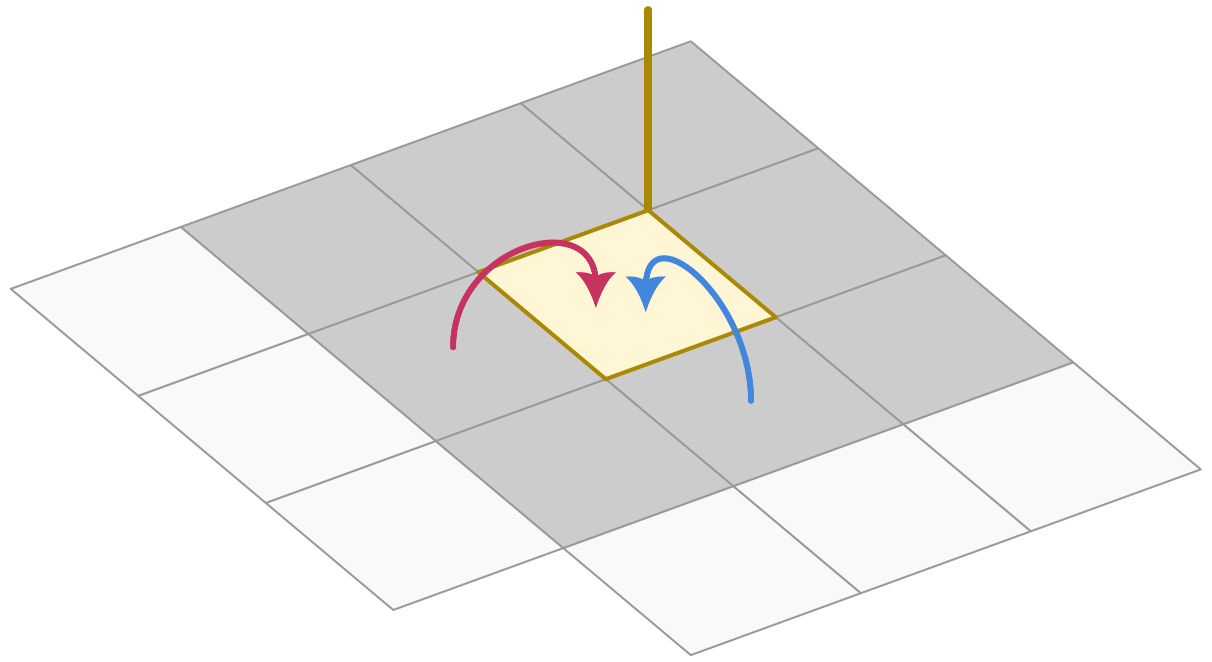
Cascades of general unitaries

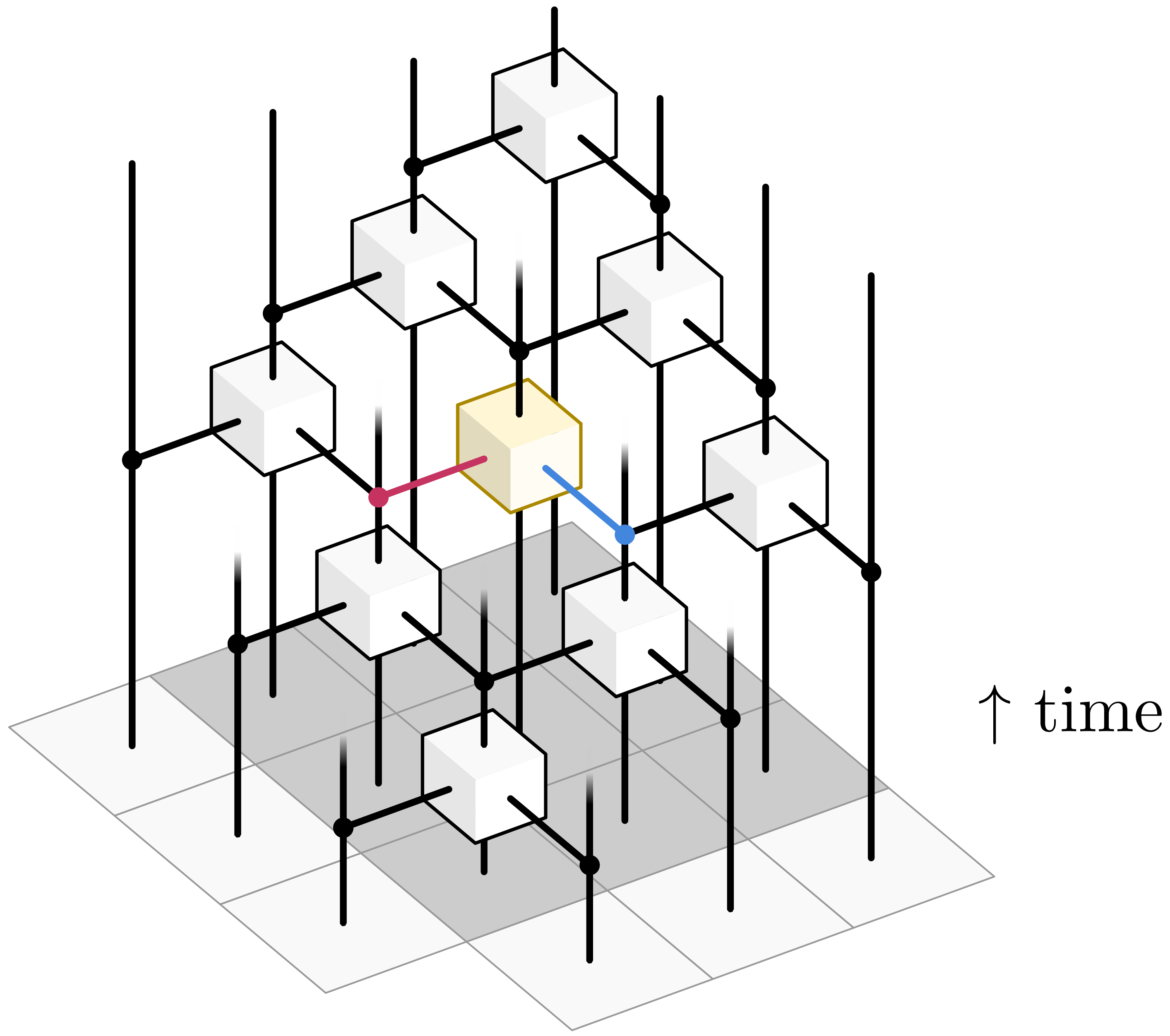


Unclear how to prove a precomputation identity here...

Quantum dynamic programming?

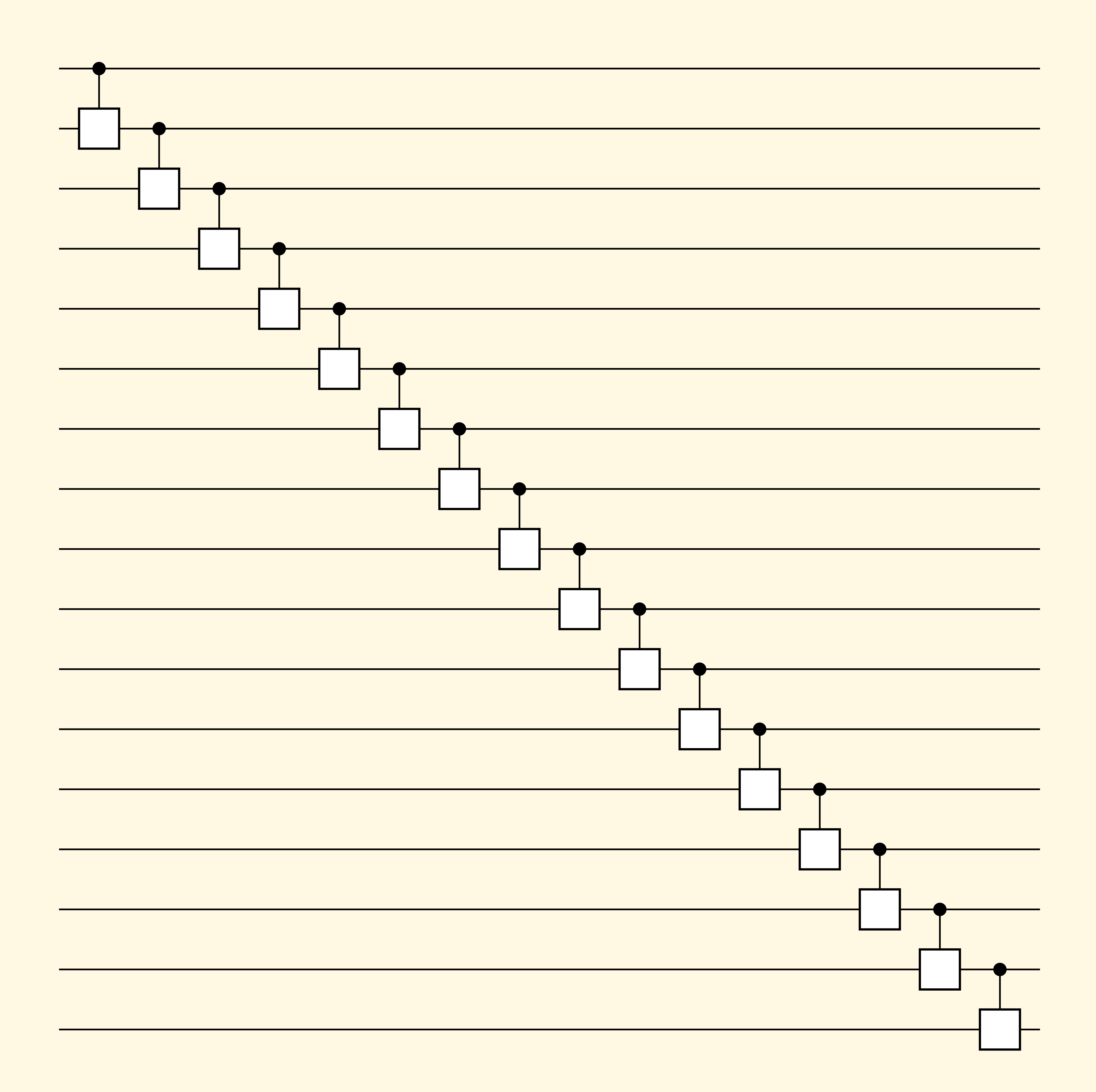
$$T(m,n) = f\big(T(m-1,n), T(m,n-1)\big)$$

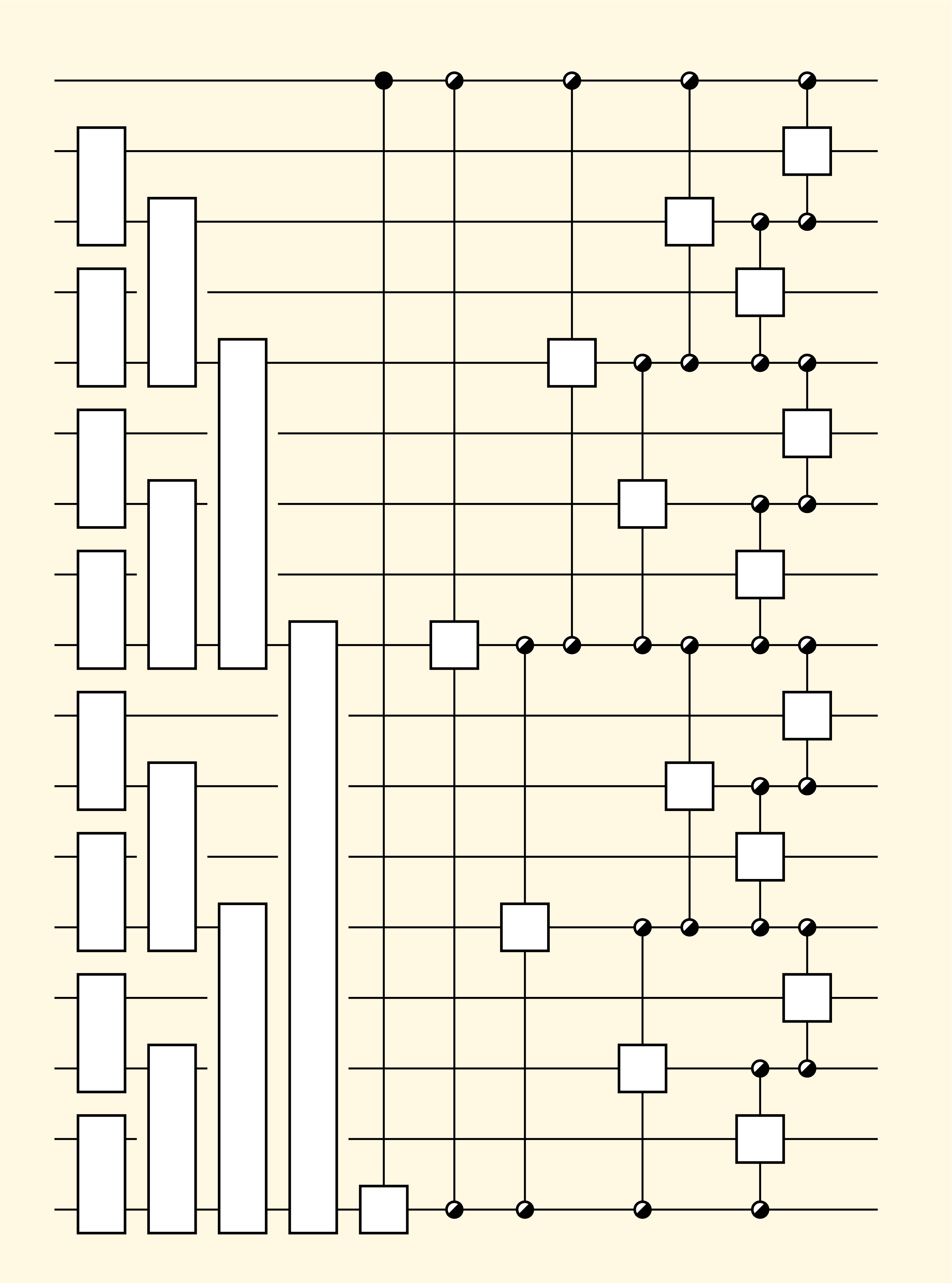




Question for the audience:

What circuits would *you* like to be parallelized?





Thanks! Questions?