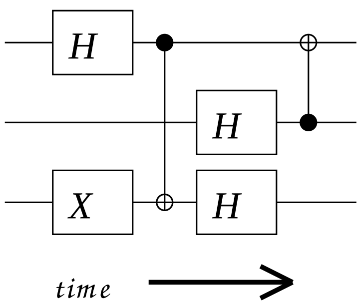
Quantum Fan-out is Powerful

Robert Špalek, CWI
(joint work with Peter Høyer, Calgary)

Quantum circuits

resemble classical reversible circuits:



- Number of (qu)bits stays constant during the computation.
- Reversible gates are ordered into layers and applied in the corresponding order.

Differences:

- State of computation is a unit vector instead of value $0, 1, \ldots, 2^n - 1$.
- Gate is a unitary mapping on some subspace instead of a permutation of the values.

Quantum fan-out

Motivation: *small decoherence time*.

- We want to minimise the depth of the circuit:
  1. Gates on different qubits can be applied in parallel.
  2. *Commuting* gates can be applied on *the same qubits* in parallel.
- We allow unbounded *quantum fan-out* gate:
  - It behaves like a controlled-not-not-...-not gate:

$$|x\rangle|y_1\rangle\dots|y_n\rangle \longrightarrow |x\rangle|y_1 \oplus x\rangle\dots|y_n \oplus x\rangle.$$

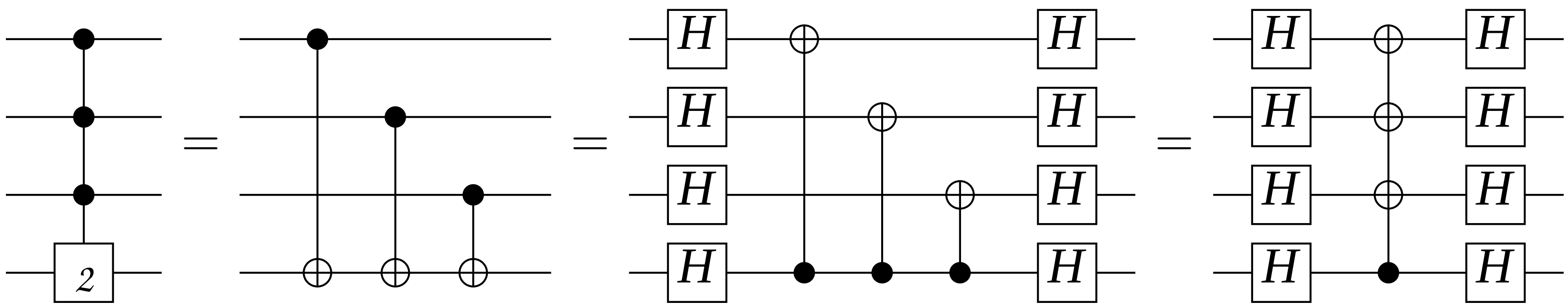
  - This is not quantum cloning!

Physical implementation

- Interaction between more than two qubits in principle possible in ion-trap and NMR models.
- [Fenner, 2003] Fan-out implemented by a Hamiltonian with number of terms quadratic in n.

[Moore, 1999] Parity in constant depth

Parity and fan-out can simulate each other.



- Hadamard gates change the direction of controlled-not.
- Two applications of $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ cancel, i.e. $H^2 = I$.

Parameters of the circuit model

We investigate operators computed by uniform families of circuits:

- depth bounded by $d(n)$, mostly constant,
- polynomial size,
- fixed basis of one-qubit gates:
  - Hadamard gate H,
  - $R_z(\varphi)$ for φ irrational multiple of π,

  and unbounded fan-out gate,
- described by a log-space Turing machine.

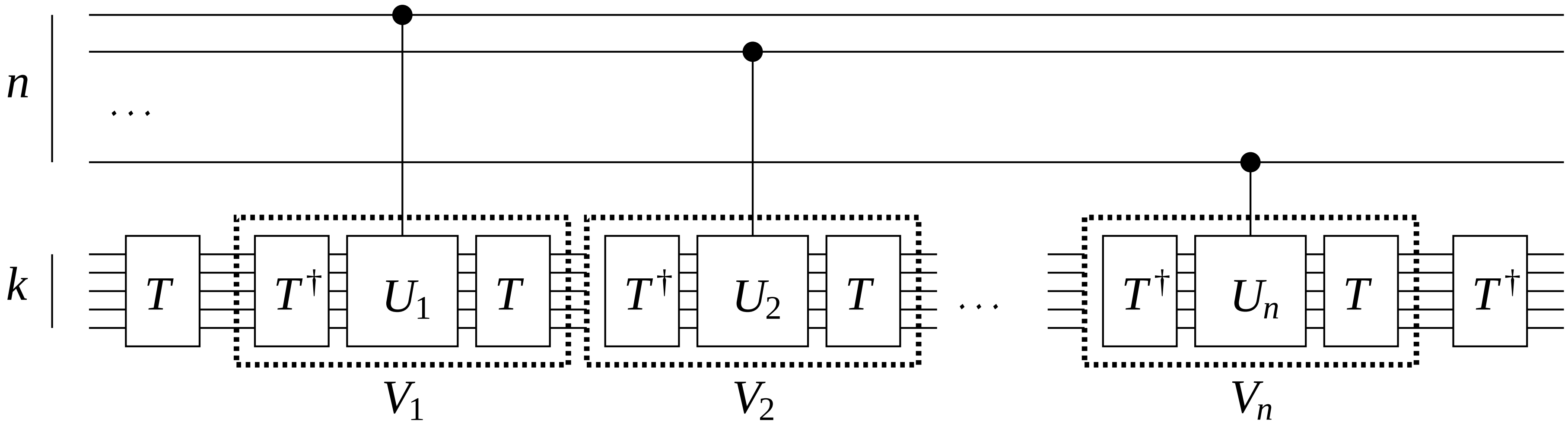
Parallelisation method

Gates can be applied on the same qubits in parallel whenever:

1. they *commute*, and
2. we know the *basis* in which they all are *diagonal* (there is always such a basis), and
3. we can efficiently change into this basis.

Advantages:	**Disadvantages:**
smaller depth	needs ancilla qubits
gates can be controlled	needs basis change

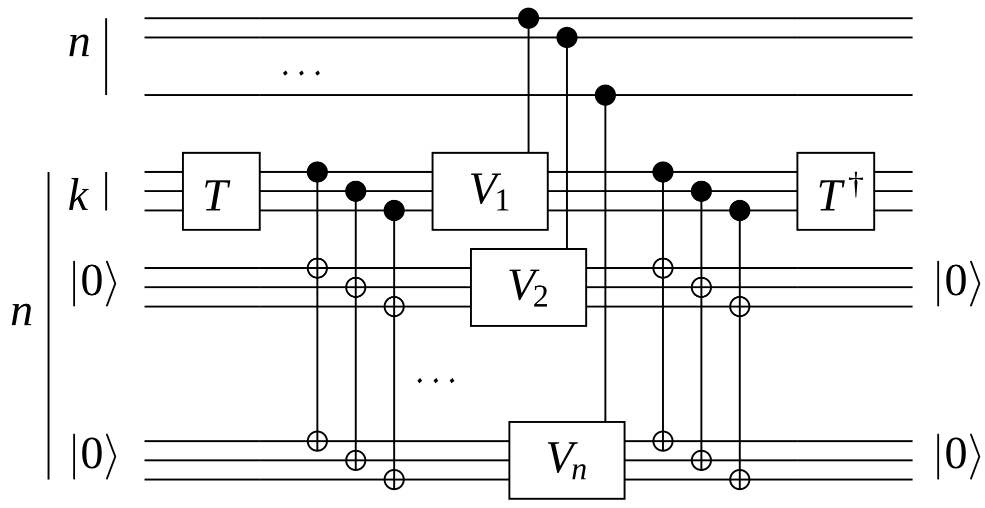
1. Changing the basis



- Put $TT^\dagger = I$ between U_k and U_{k+1}.
- Take $V_k = T^\dagger U_k T$ as new operators.

  They are diagonal in the computational basis.

2. Parallelising diagonal operators



- Fan-out creates/destroys n entangled copies of target qubits.
- V_k are diagonal, so they just impose phase shifts.
- These phase shifts multiply and thus can be applied in parallel.

[Moore, 1999] mod[k] in constant depth

- The number $|x| \bmod k$ can be computed in this way:
  - Initialise ancilla *counter* y to 0, this is $\lceil \log k \rceil$ qubits.
  - Each input bit x_k controls one increment of y modulo k.
  - At the end: $y = |x| \bmod k$.
- The increment gates commute, so can be parallelised.

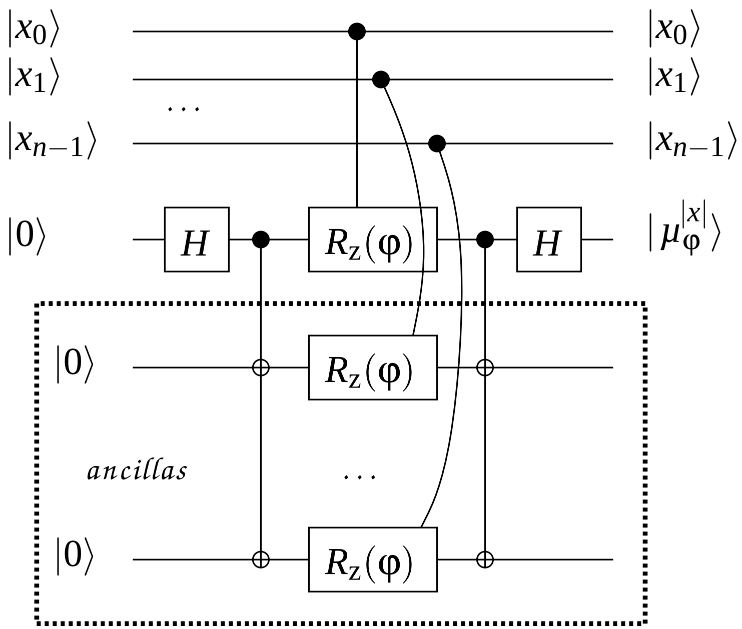
  k is fixed, hence the basis change and the increments can be computed exactly in constant depth.

Rotation by Hamming weight

Define:

$$R_z(\varphi) := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

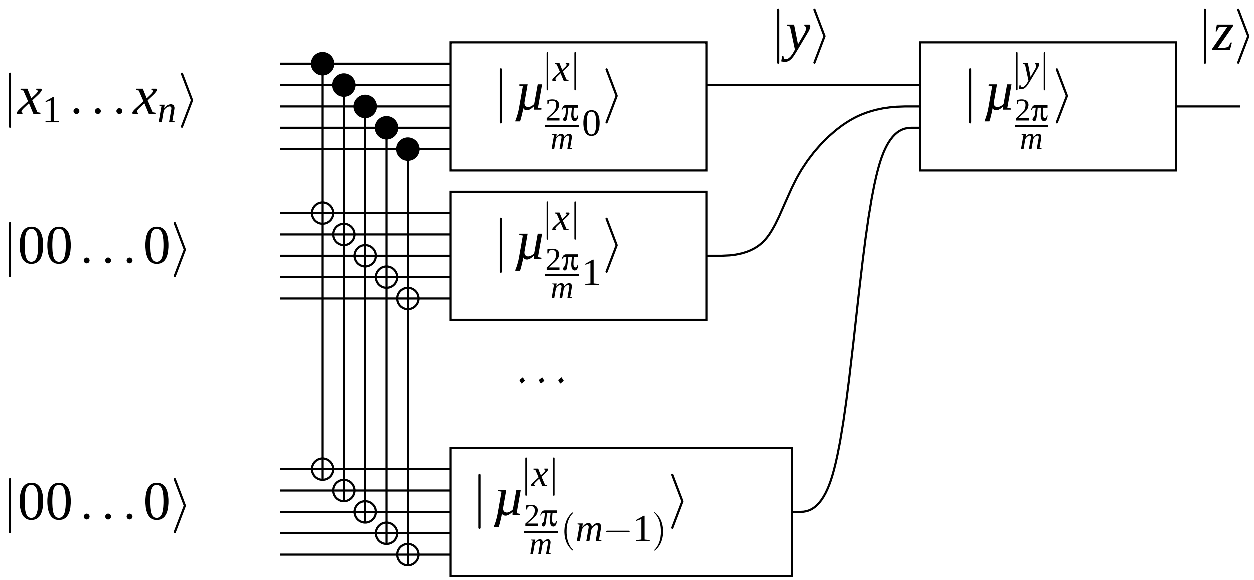
$$|\mu_\varphi^w\rangle := \frac{1+e^{i\varphi w}}{2}|0\rangle + \frac{1-e^{i\varphi w}}{2}|1\rangle$$



The circuit maps $|0\rangle$ to $H\left(\frac{|0\rangle + e^{i\varphi|x|}|1\rangle}{\sqrt{2}}\right) = |\mu_\varphi^{|x|}\rangle$

in depth 5 and linear size.

Approximate circuit for Or



After the first set of rotations, either $|y| = 0$ or $|y| \approx \frac{m}{2}$.

The circuit has constant depth and size $\mathrm{O}(mn) = \mathrm{O}\left(n^2 \log n\right)$.

1st layer of the circuit for Or

- Let $m = n \log n$. For all $k \in \{0, 1, 2, \ldots, m-1\}$, compute in parallel $|y_k\rangle = |\mu_{\varphi_k}^{|x|}\rangle$ for angle $\varphi_k = \frac{2\pi}{m} \cdot k$.
- If $|y_k\rangle$ is measured, the expected value is

$$E[Y_k] = \left| \frac{1 - e^{i\varphi_k |x|}}{2} \right|^2 = \frac{1 - \cos(\varphi_k |x|)}{2}$$

and the expected Hamming weight of $|y\rangle = |y_{m-1} \ldots y_1 y_0\rangle$ is

$$E[|Y|] = \frac{m}{2} - \frac{1}{2} \sum_{k=0}^{m-1} \cos\left(\frac{2\pi k}{m} |x|\right) = \begin{cases} 0 & \text{if } |x| = 0, \\ \frac{m}{2} & \text{if } |x| \neq 0. \end{cases}$$

- Moreover, if $|x| \neq 0$, then $P\left[\left||Y| - \frac{m}{2}\right| \geq \varepsilon m\right] \leq \frac{1}{2^{\varepsilon^2 m}}$.

2nd layer of the circuit for Or

- The register $|y\rangle$ is **not** directly measured, but its Hamming weight controls another rotation on a new ancilla qubit $|z\rangle$.

- Compute $|z\rangle = |\mu_{2\pi/m}^{|y|}\rangle$. Let Z be the outcome after $|z\rangle$ is measured.
  - If $|x| = 0$, then $|y| = 0$ and $Z = 0$ with certainty.
  - It $|x| \neq 0$, then $\left||y| - \frac{m}{2}\right| > \frac{m}{\sqrt{n}}$ with probability $< \frac{1}{2^{m/n}} = \frac{1}{2^{\log n}} = \frac{1}{n}$.
  - If $\left||y| - \frac{m}{2}\right| \leq \frac{m}{\sqrt{n}}$, then $Z = 1$ with high probability and
  $$P[Z=0] = \left|\frac{1+e^{i\frac{2\pi}{m}|y|}}{2}\right|^2 \leq \frac{1-\cos\frac{2\pi}{\sqrt{n}}}{2} = \mathrm{O}\left(\frac{1}{n}\right).$$

- Hence $P[Z=0] = \begin{cases} 1 & \text{if } |x| = 0, \\ \mathrm{O}\left(\frac{1}{n}\right) & \text{if } |x| \neq 0. \end{cases}$

Remarks on the Or gate

- The error is bounded by $\frac{1}{n}$ and one-sided.

  If we need small error $\frac{1}{n^c}$, we create c copies and compute the *exact Or* of them. This can be done in $\log c = \mathrm{O}(1)$ layers.

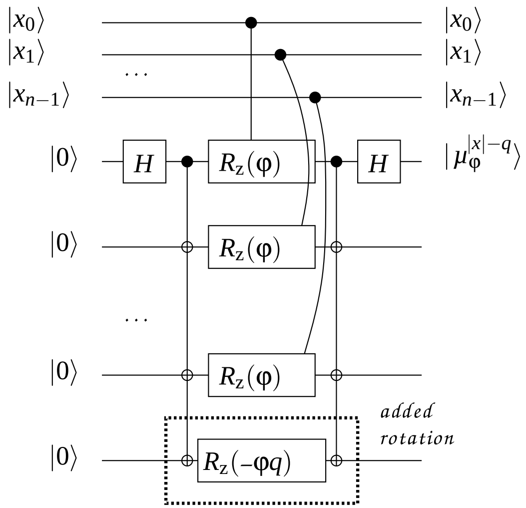
- The construction uses rotations $R_z\left(\pi\frac{k}{m}\right)$ for *arbitrary* k, m.

  We are only allowed to use a *fixed set* of one-qubits gates.

  - Every rotation can be approximated with polynomially small error by $R_z\left(\sqrt{2}\,\pi \cdot q\right)$ for a polynomially large q.
  - q iterations can be done in parallel, so depth is preserved.

Generalisation: exact[q] gate

- Or gate tests whether $|x| = 0$.
  exact[q] gate tests whether $|x| = q$.

- 

  - Can be computed similarly to Or.
  - Add rotation $R_Z(-\varphi q)$ to the first layer and obtain $|\mu_\varphi^{|x|-q}\rangle$ instead of $|\mu_\varphi^{|x|}\rangle$.
  - The second layer stays the same.
  - Measure output qubit $|z\rangle$ and get

$$P[Z=0] = \begin{cases} 1 & \text{if } |x| = q, \\ O\left(\frac{1}{n}\right) & \text{if } |x| \neq q. \end{cases}$$

- exact[q] gates can be used for threshold[t] and counting gates.

Arithmetics and sorting in constant depth

[Siu et al., 1993] The following functions are computed by constant depth threshold circuits:

1. summation and multiplication of n integers,

2. division of two integers,

3. and sorting of n numbers.

The construction uses *weighted threshold gates*.

Quantum circuits with fan-out can approximate also the weighted threshold gate in constant depth.

Exact computation of Or and exact[q]

Exact *reduction* of Or on n qubits to Or on $\log n$ qubits:

- Let $m = \lceil \log(n+1) \rceil$. For all $k \in \{1,2,\ldots,m\}$, compute in parallel $|y_k\rangle = |\mu_{\varphi_k}^{|x|}\rangle$ for angle $\varphi_k = \frac{2\pi}{2^k}$.
  - If $|x| = 0$, then $|y_k\rangle = |0\rangle$ for each k.
  - If $|x| \neq 0$, decompose it into $|x| = 2^a(2b+1)$ and

$$\langle 1|y_{a+1}\rangle = \frac{1 - e^{i\varphi_{a+1}|x|}}{2} = \frac{1 - e^{i\pi(2b+1)}}{2} = \frac{1 - e^{i\pi}}{2} = 1.$$

- It follows that $|x| = 0 \Longleftrightarrow |y| = 0$.
  The reduction is exact, the depth is $O(1)$, and the size is $O(n \log n)$.

After $O(\log^* n)$ iterations, the number of qubits is constant.

Randomised vs quantum depth

Problem	Randomised	Quantum
Or and threshold[t] exactly	$\Theta(\log n)$	$O(\log^* n)$
mod[k] exactly	$\Theta(\log n)$	$\Theta(1)$
Or with error $\frac{1}{n}$	$\Theta(\log\log n)$	$\Theta(1)$
threshold[t] with error $\frac{1}{n}$	$\Omega(\log\log n)$	$\Theta(1)$

- Classical lower bounds are for the model with bounded fan-in of Or and *unbounded parity*.
  (Proven by the polynomial method and Yao's principle.)

- Quantum upper bounds are for the model with bounded fan-in and *unbounded fan-out*.

  The exact algorithm for Or uses arbitrary one-qubit gates, though.

Possible improvements?

1. We can reduce the size of circuit for Or from $\mathrm{O}\left(n^2 \log n\right)$ to $\mathrm{O}(n \log n)$, $\mathrm{O}(n \log\log\ldots\log n)$, or even $\mathrm{O}(n \log^* n)$!

Can it be made linear?

2. Exact circuit for Or of constant depth?

3. Exact circuit for Or of sub-logarithmic depth with a fixed basis of one-qubit gates?

Quantum Fourier transform (QFT)

Performs *Fourier transform* on the *amplitudes* of the state:

$$F : |x\rangle \to |\psi_x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i x y / 2^n} |y\rangle.$$

- [Shor, 1994] Compute QFT in depth $O(n)$, size $O\left(n^2\right)$, without ancillas.
- [Cleve & Watrous, 2000] Approximate QFT with error ε in depth $O\left(\log n + \log\log \frac{1}{\varepsilon}\right)$ and size $O\left(n \log \frac{n}{\varepsilon}\right)$.
- [Høyer & Špalek, 2002] Using fan-out, approximate QFT with polynom. small error in constant depth and polynomial size.

Shallow circuits for QFT

[Cleve & Watrous, 2000] QFT: $|x\rangle \to |\psi_x\rangle$ decomposed into

1.	Fourier state construction:	$|x\rangle|0\rangle\dots|0\rangle$	$\to |x\rangle|\psi_x\rangle|0\rangle\dots|0\rangle$
2.	Copying Fourier state:	$|x\rangle|\psi_x\rangle|0\rangle\dots|0\rangle$	$\to |x\rangle|\psi_x\rangle\dots|\psi_x\rangle$
3.	Uncomputing phase estimation:	$|\psi_x\rangle\dots|\psi_x\rangle|x\rangle$	$\to |\psi_x\rangle\dots|\psi_x\rangle|0\rangle$
4.	Uncopying Fourier state:	$|\psi_x\rangle\dots|\psi_x\rangle|0\rangle$	$\to |\psi_x\rangle|0\rangle\dots|0\rangle$

[CW, 00] Each step approximated in logarithmic depth.

[HŠ, 02] Each step approximated in constant depth *with fan-out*.

Application of QFT

- Counting and threshold[t] in size $\mathrm{O}(n \log n)$.
  (Similar to mod[k] gate: parallelisation of n increments.
  Increment is diagonal in the Fourier basis.)

- [CW, 00] Multiplication of n numbers and QFT suffice for factoring. They both can be approximated in logarithmic depth.

  Hence we can *factor* in polynomial time given oracle quantum circuits of logarithmic depth (QNC^1).

  Assuming factoring is not in BPP, then $\mathrm{QNC}^1 \not\subseteq \mathrm{BPP}$.

- [HŠ, 02] The same arguments hold also for quantum circuits *with fan-out* of constant depth.

Summary

- *Quantum fan-out* can be used for parallelisation of any commuting operations (parity, mod[k])
- Or and exact[q] with *bounded error* in constant depth
- Implies arithmetics and sorting in constant depth
- *Exact* computation in $\log^* n$ depth
- Quantum Fourier transform *approximated* in constant depth