Computational Power of Observed Quantum Turing Machines

Simon Perdrix

PPS, Université Paris Diderot
& LFCS, University of Edinburgh

New Worlds of Computation, January 2009

Quantum Computing Basics

State space

in a classical world of computation: countable A.
in a quantum world: Hilbert space $\mathbb{C}^A$

ket map

$$|.\rangle : A \to \mathbb{C}^A$$

s.t. $\{|x\rangle, x \in A\}$ is an orthonormal basis of $\mathbb{C}^A$

Arbitrary states

$$\mathbf{\Phi} = \sum_{x \in A} \alpha_x |x\rangle$$

s.t. $\sum_{x \in A} |\alpha_x|^2 = 1$

Quantum Computing Basics

bra map

$$\langle . | \quad : \quad A \quad \rightarrow \quad \mathbf{L}(\mathbb{C}^A, \mathbb{C})$$

s.t. $\forall x, y \in A$,

$$\langle y| \, |x\rangle = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases} \qquad \text{“ Kronecker ”}$$

$\forall v, t \in A, |v\rangle\langle t| : \mathbb{C}^A \rightarrow \mathbb{C}^A$:

$$(|v\rangle\langle t|) \, |x\rangle = |v\rangle \, (\langle t| \, |x\rangle) = \begin{cases} |v\rangle & \text{if } t = x \\ \mathbf{0} & \text{otherwise} \end{cases} \qquad \text{“ } |v\rangle\langle t| \approx t \mapsto v \text{ ”}$$

Evolution of isolated systems: Linear map $U \in \mathbf{L}(\mathbb{C}^A, \mathbb{C}^A)$

$$U = \sum_{x,y \in A} u_{x,y} \, |y\rangle\langle x|$$

which is an isometry ($U^\dagger U = I$).

Observation

$$\text{Let } \mathbf{\Phi} = \sum_{x \in A} \alpha_x |x\rangle$$

(Full) measurement in standard basis:

The probability to observe $a \in A$ is $|\alpha_a|^2$.

If $a \in A$ is observed, the state becomes $\mathbf{\Phi}_a = |a\rangle$.

Partial measurement in standard basis: Let $K = \{K_\lambda, \lambda \in \Lambda\}$ be a partition of A.

The probability to observe $\lambda \in \Lambda$ is $p_\lambda = \sum_{a \in K_\lambda} |\alpha_a|^2$

If $\lambda \in \Lambda$ is observed, the state becomes

$$\mathbf{\Phi}_\lambda = \frac{1}{\sqrt{p_\lambda}} P_\lambda \mathbf{\Phi} = \frac{1}{\sqrt{p_\lambda}} \sum_{a \in K_\lambda} \alpha_a |a\rangle$$

where $P_\lambda = \sum_{a \in K_\lambda} |a\rangle\langle a|$.

Observation

$$\text{Let } \mathbf{\Phi} = \sum_{x \in A} \alpha_x |x\rangle$$

(Full) measurement in standard basis:

The probability to observe $a \in A$ is $|\alpha_a|^2$.

If $a \in A$ is observed, the state becomes $\mathbf{\Phi}_a = |a\rangle$.

Partial measurement in standard basis: Let $K = \{K_\lambda, \lambda \in \Lambda\}$ be a partition of A.

The probability to observe $\lambda \in \Lambda$ is $p_\lambda = \sum_{a \in K_\lambda} |\alpha_a|^2$

If $\lambda \in \Lambda$ is observed, the state becomes

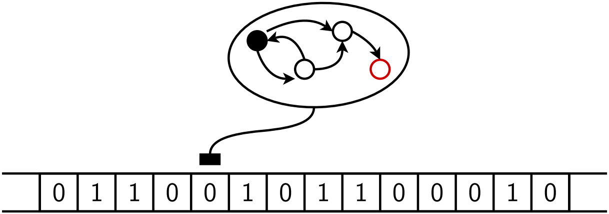
$$\mathbf{\Phi}_\lambda = \frac{1}{\sqrt{p_\lambda}} P_\lambda \mathbf{\Phi} = \frac{1}{\sqrt{p_\lambda}} \sum_{a \in K_\lambda} \alpha_a |a\rangle$$

where $P_\lambda = \sum_{a \in K_\lambda} |a\rangle\langle a|$.

Deterministic Turing Machine (DTM)

Classical Turing machine (Q, Σ, δ):

$$\delta : Q \times \Sigma \to Q \times \Sigma \times \{-1, 0, 1\}$$

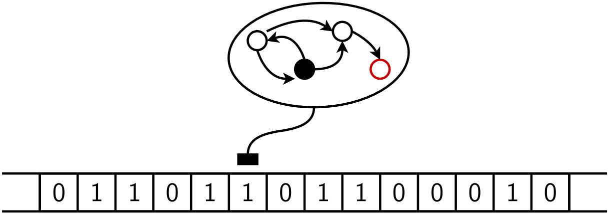


$(q, T, x) \in Q \times \Sigma^* \times \mathbb{Z}$ is a classical configuration.

Deterministic Turing Machine (DTM)

Classical Turing machine (Q, Σ, δ):

$$\delta : Q \times \Sigma \to Q \times \Sigma \times \{-1, 0, 1\}$$

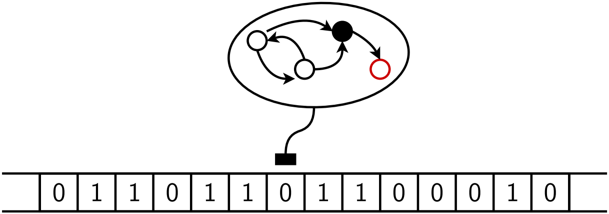


$(q, T, x) \in Q \times \Sigma^* \times \mathbb{Z}$ is a classical configuration.

Deterministic Turing Machine (DTM)

Classical Turing machine (Q, Σ, δ):

$$\delta : Q \times \Sigma \to Q \times \Sigma \times \{-1, 0, 1\}$$

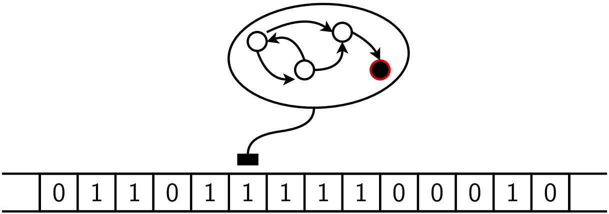


$(q, T, x) \in Q \times \Sigma^* \times \mathbb{Z}$ is a classical configuration.

Deterministic Turing Machine (DTM)

Classical Turing machine (Q, Σ, δ):

$$\delta : Q \times \Sigma \rightarrow Q \times \Sigma \times \{-1, 0, 1\}$$

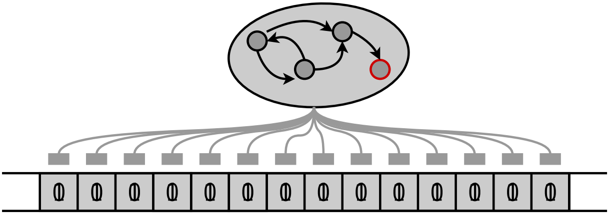


$(q, T, x) \in Q \times \Sigma^{*} \times \mathbb{Z}$ is a classical configuration.

Quantum Turing Machine (QTM)

Quantum Turing machine $M = (Q, \Sigma, \delta)$:

$$\delta : Q \times \Sigma \times Q \times \Sigma \times \{-1, 0, 1\} \to \mathbb{C}$$



A quantum configuration is a superposition of classical configurations

$$\sum_{q \in Q, T \in \Sigma^*, x \in \mathbb{Z}} \alpha_{q,T,x} \, |q, T, x\rangle \in \mathbb{C}^{Q \times \Sigma^* \times \mathbb{Z}}$$

Evolution operator

$$U_M = \sum_{p,q\in Q,\sigma\in\Sigma,d\in\{-1,0,1\},T\in\Sigma^*,x\in\mathbb{Z}} \delta(p,T_x,q,\sigma,d)\,|q,T_x^\sigma,x+d\rangle\,\langle p,T,x|$$

A QTM (Q,Σ,δ) has to satisfy some well-formedness conditions...

Well-formedness conditions

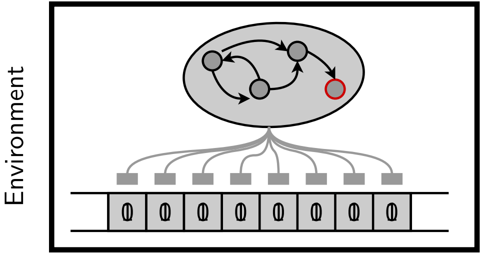
Definition: A QTM M is well-formed iff U_M is an isometry, i.e. $U_M^\dagger U_M = I$

- The evolution of the machine does not violate the postulates of quantum mechanics.
- During the computation, the machine is isolated from the rest of the universe.

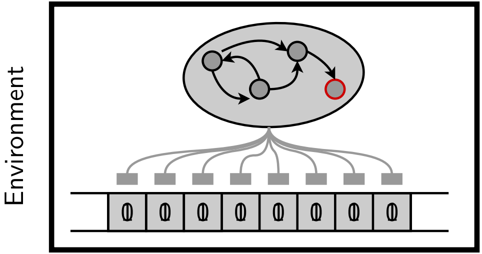
Well-formedness conditions

Definition: A QTM M is well-formed iff U_M is an isometry, i.e. $U_M^\dagger U_M = I$

- The evolution of the machine does not violate the postulates of quantum mechanics.
- During the computation, the machine is isolated from the rest of the universe.

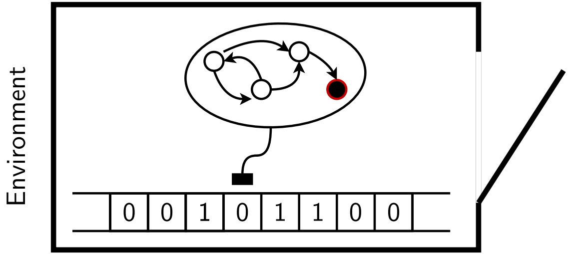


Halting of QTM



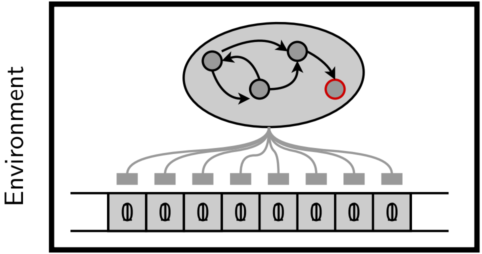
At the end of the computation, the QTM is ‘observed’.

Halting of QTM



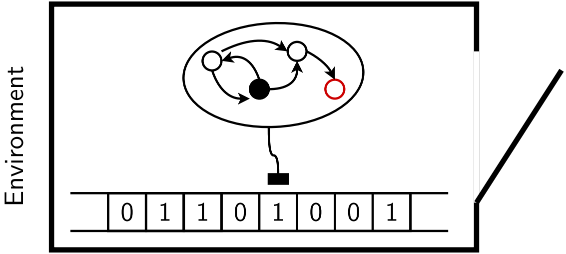
At the end of the computation, the QTM is 'observed'.

Halting of QTM



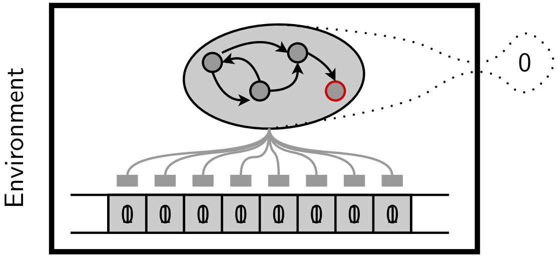
At the end of the computation, the QTM is 'observed'.

Halting of QTM



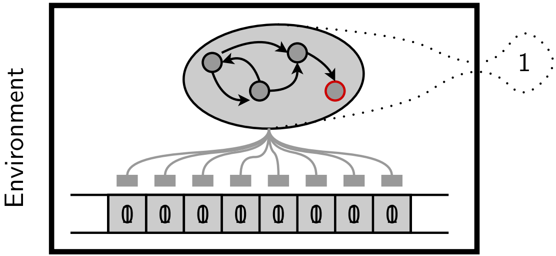
If the halting state is not reached, the computation is useless.

Halting of QTM



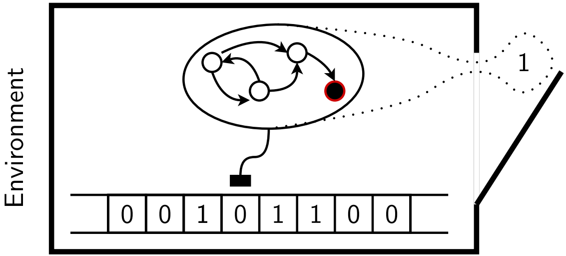
Halting qubit (Ad hoc)

Halting of QTM



Halting qubit (Ad hoc)

Halting of QTM



Halting qubit (Ad hoc)

‘Un-isolated’ QTM

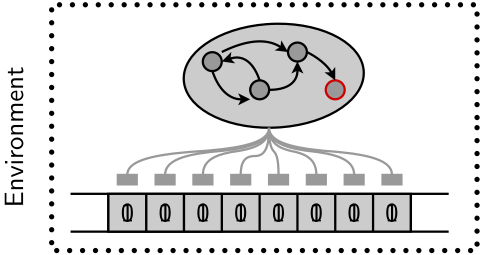
Isolation assumption is probably too strong

- technical issues like the halting of QTM,
- models of QC (one-way model, measurement-only model) based on measurements.
- PTM and DTM are not well-formed QTM (reversible DTM does)
- quest of a universal QTM: a classical control is required.

'Un-isolated' QTM

Isolation assumption is probably too strong

- technical issues like the halting of QTM,
- models of QC (one-way model, measurement-only model) based on measurements.
- PTM and DTM are not well-formed QTM (reversible DTM does)
- quest of a universal QTM: a classical control is required.



Modelling Environment: Observed QTM

Environment is modelled as a partial measurement of the configuration, characterised by a partition $K = \{K_\lambda\}_{\lambda \in \Lambda}$ of $Q \times \Sigma^* \times \mathbb{Z}$.

Definition: For a given QTM $M = (Q, \Sigma, \delta)$ and a given partition $K = \{K_\lambda\}_{\lambda \in \Lambda}$ of $Q \times \Sigma^* \times \mathbb{Z}$, $[M]_K$ is an Observed Quantum Turing Machine (OQTM).

Evolution of OQTM

One transition of $[M]_K$ is composed of:

1. partial measurement K of the quantum configuration;
2. transition of M;
3. partial measurement K of the quantum configuration.

Definition: An OQTM $[M]_K$ is well-observed iff

$$\sum_{\lambda \in \Lambda} P_\lambda U_M^\dagger U_M P_\lambda = I$$

where $P_\lambda = \sum_{(p,T,x) \in K_\lambda} |p, T, x\rangle \langle p, T, x|$.

Lemma: If a QTM M is well-formed then $[M]_K$ is a well-observed OQTM for any K.

Proof:

$$\begin{aligned}
\sum_{\lambda\in\Lambda} P_\lambda U_M^\dagger U_M P_\lambda &= \sum_{\lambda\in\Lambda} P_\lambda P_\lambda \\
&= \sum_{\lambda\in\Lambda} P_\lambda \\
&= \sum_{\lambda\in\Lambda} \sum_{p,T,x\in K_\lambda} |p,T,x\rangle\langle p,T,x| \\
&= \sum_{p,T,x\in Q\times\Sigma^*\times\mathbb{Z}} |p,T,x\rangle\langle p,T,x| \\
&= I
\end{aligned}$$

a weaker condition

Lemma: If a QTM M is well-formed then $[M]_K$ is a well-observed OQTM for any K.

Proof:

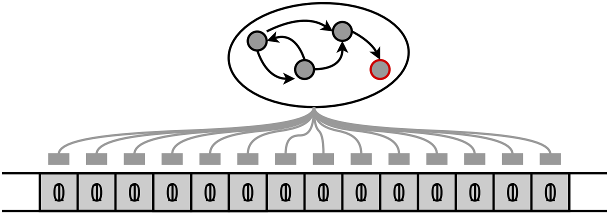
$$\begin{array}{rcl} \sum_{\lambda \in \Lambda} P_\lambda U_M^\dagger U_M P_\lambda & = & \sum_{\lambda \in \Lambda} P_\lambda P_\lambda \\ & = & \sum_{\lambda \in \Lambda} P_\lambda \\ & = & \sum_{\lambda \in \Lambda} \sum_{p,T,x \in K_\lambda} |p,T,x\rangle \langle p,T,x| \\ & = & \sum_{p,T,x \in Q \times \Sigma^* \times \mathbb{Z}} |p,T,x\rangle \langle p,T,x| \\ & = & I \end{array}$$

Example: halting of QTM

For a given QTM $M = (Q, \Sigma, \delta)$ s.t. $q_h \in Q$ is the unique halting state.

$$\begin{array}{lcl} K_h & = & \{q_h\} \times \Sigma^* \times \mathbb{Z} \\ K_{\bar{h}} & = & K \setminus K_h \end{array}$$

$[M]_{\{K_h, K_{\bar{h}}\}}$ evolves as follows:

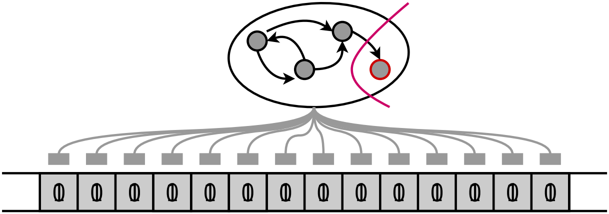


Example: halting of QTM

For a given QTM $M = (Q, \Sigma, \delta)$ s.t. $q_h \in Q$ is the unique halting state.

$$\begin{array}{rcl} K_h & = & \{q_h\} \times \Sigma^* \times \mathbb{Z} \\ K_{\bar{h}} & = & K \setminus K_h \end{array}$$

$[M]_{\{K_h, K_{\bar{h}}\}}$ evolves as follows:

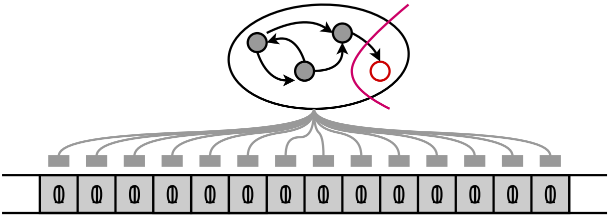


Example: halting of QTM

For a given QTM $M = (Q, \Sigma, \delta)$ s.t. $q_h \in Q$ is the unique halting state.

$$\begin{array}{rcl} K_h & = & \{q_h\} \times \Sigma^* \times \mathbb{Z} \\ K_{\bar{h}} & = & K \setminus K_h \end{array}$$

$[M]_{\{K_h, K_{\bar{h}}\}}$ evolves as follows:

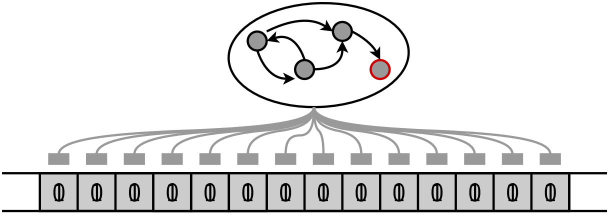


Example: halting of QTM

For a given QTM $M = (Q, \Sigma, \delta)$ s.t. $q_h \in Q$ is the unique halting state.

$$\begin{array}{rcl} K_h & = & \{q_h\} \times \Sigma^* \times \mathbb{Z} \\ K_{\bar{h}} & = & K \setminus K_h \end{array}$$

$[M]_{\{K_h, K_{\bar{h}}\}}$ evolves as follows:

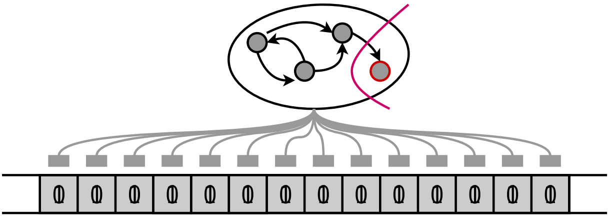


Example: halting of QTM

For a given QTM $M = (Q, \Sigma, \delta)$ s.t. $q_h \in Q$ is the unique halting state.

$$\begin{array}{rcl} K_h & = & \{q_h\} \times \Sigma^* \times \mathbb{Z} \\ K_{\bar{h}} & = & K \setminus K_h \end{array}$$

$[M]_{\{K_h, K_{\bar{h}}\}}$ evolves as follows:

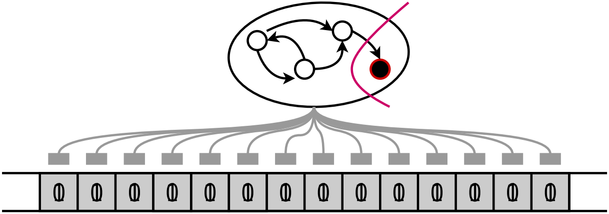


Example: halting of QTM

For a given QTM $M = (Q, \Sigma, \delta)$ s.t. $q_h \in Q$ is the unique halting state.

$$\begin{aligned} K_h &= \{q_h\} \times \Sigma^* \times \mathbb{Z} \\ K_{\bar{h}} &= K \setminus K_h \end{aligned}$$

$[M]_{\{K_h, K_{\bar{h}}\}}$ evolves as follows:



OQTM more expressive than QTM

Lemma: For any DTM $M = (Q, \Sigma, \delta)$, $[M]_{\{\{c\}, c \in Q \times \Sigma^* \times \mathbb{Z}\}}$ is a well-observed OQTM.

OQTM, a too powerful model ?!?

Theorem: There is a well-observed OQTM $[M_h]_{K_h}$ for deciding (with high probability), for any DTM M and any input u, whether M halts on input u.

(Proof) Hadamard QTM

Let $M_h = (\{q_0, q_1, q_2, q_h, q_{\bar{h}}\}, \Sigma, \delta_h)$ be a well-formed QTM, s.t. q_h and $q_{\bar{h}}$ are the halting states and for $\sigma \in \Sigma$

$$\begin{array}{rcr} \delta_h(q_0, \sigma, q_1, \sigma, 0) & = & 1/\sqrt{2} \\ \delta_h(q_0, \sigma, q_2, \sigma, 0) & = & 1/\sqrt{2} \\ \delta_h(q_1, \sigma, q_h, \sigma, 0) & = & 1/\sqrt{2} \\ \delta_h(q_1, \sigma, q_{\bar{h}}, \sigma, 0) & = & 1/\sqrt{2} \\ \delta_h(q_2, \sigma, q_h, \sigma, 0) & = & 1/\sqrt{2} \\ \delta_h(q_2, \sigma, q_{\bar{h}}, \sigma, 0) & = & -1/\sqrt{2} \end{array}$$

$\forall w \in \Sigma^*$,

$$\begin{array}{rcl} U_{M_h}^2 |q_0, w\rangle & = & U_{M_h}(\frac{1}{\sqrt{2}}(|q_1, w\rangle + |q_2, w\rangle)) \\ & = & \frac{1}{2}(|q_h, w\rangle + |q_{\bar{h}}, w\rangle + |q_h, w\rangle - |q_{\bar{h}}, w\rangle) \\ & = & |q_h, w\rangle \end{array}$$

For any DTM M and any input u, let $w_{M,u} \in \Sigma^*$ be an 'encoding' of M and u.

$$\begin{array}{rcl} K_0 & = & \{(q_1, w_{M,u}) \text{ s.t. } M(u) \text{ does not halt}\} \cup \{(q_{\bar{h}}, w)\} \\ K_1 & = & \{(q, w) \text{ s.t. } (q, w) \notin K_1\} \end{array}$$

What is the evolution of $[M_h]_{\{K_0,K_1\}}$ if the initial configuration is $(q_0, w_{M,u})$?

Evolution of M_h: $|q_0, w_{M,u}\rangle \to \frac{1}{\sqrt{2}}(|q_1, w_{M,u}\rangle + |q_2, w_{M,u}\rangle) \to |q_h, w_{M,u}\rangle$

- If $M(u)$ halts, then $(q_1, w_{M,u}), (q_2, w_{M,u}) \in K_1$, thus the evolution of $[M_h]_{\{K_0,K_1\}}$ is

$$|q_0, w_{M,u}\rangle \to^* |q_h, w_{M,u}\rangle$$

- If $M(u)$ does not halt, then $(q_1, w_{M,u}) \in K_0$, and $(q_2, w_{M,u}) \in K_1$ moreover $(q_{\bar{h}}, w_{M,u}) \in K_0$ and $(q_h, w_{M,u}) \in K_1$, thus:

$$|q_0, w_{M,u}\rangle \to^* \begin{cases} |q_h, w_{M,u}\rangle & \text{with probability } 1/2 \\ |q_{\bar{h}}, w_{M,u}\rangle & \text{with probability } 1/2 \end{cases}$$

For any DTM M and any input u, let $w_{M,u} \in \Sigma^*$ be an 'encoding' of M and u.

$$\begin{array}{rcl} K_0 & = & \{(q_1, w_{M,u}) \text{ s.t. } M(u) \text{ does not halt}\} \cup \{(q_{\bar{h}}, w)\} \\ K_1 & = & \{(q, w) \text{ s.t. } (q, w) \notin K_1\} \end{array}$$

What is the evolution of $[M_h]_{\{K_0,K_1\}}$ if the initial configuration is $(q_0, w_{M,u})$?

Evolution of M_h: $|q_0, w_{M,u}\rangle \to \frac{1}{\sqrt{2}}(|q_1, w_{M,u}\rangle + |q_2, w_{M,u}\rangle) \to |q_h, w_{M,u}\rangle$

- If $M(u)$ halts, then $(q_1, w_{M,u}), (q_2, w_{M,u}) \in K_1$, thus the evolution of $[M_h]_{\{K_0,K_1\}}$ is

$$|q_0, w_{M,u}\rangle \to^* |q_h, w_{M,u}\rangle$$

- If $M(u)$ does not halt, then $(q_1, w_{M,u}) \in K_0$, and $(q_2, w_{M,u}) \in K_1$ moreover $(q_{\bar{h}}, w_{M,u}) \in K_0$ and $(q_h, w_{M,u}) \in K_1$, thus:

$$|q_0, w_{M,u}\rangle \to^* \begin{cases} |q_h, w_{M,u}\rangle & \text{with probability } 1/2 \\ |q_{\bar{h}}, w_{M,u}\rangle & \text{with probability } 1/2 \end{cases}$$

For any DTM M and any input u, let $w_{M,u} \in \Sigma^*$ be an 'encoding' of M and u.

$$\begin{array}{rcl} K_0 & = & \{(q_1, w_{M,u}) \text{ s.t. } M(u) \text{ does not halt}\} \cup \{(q_{\bar{h}}, w)\} \\ K_1 & = & \{(q, w) \text{ s.t. } (q, w) \notin K_1\} \end{array}$$

What is the evolution of $[M_h]_{\{K_0,K_1\}}$ if the initial configuration is $(q_0, w_{M,u})$?

Evolution of M_h: $|q_0, w_{M,u}\rangle \to \frac{1}{\sqrt{2}}(|q_1, w_{M,u}\rangle + |q_2, w_{M,u}\rangle) \to |q_h, w_{M,u}\rangle$

- If $M(u)$ halts, then $(q_1, w_{M,u}), (q_2, w_{M,u}) \in K_1$, thus the evolution of $[M_h]_{\{K_0,K_1\}}$ is

$$|q_0, w_{M,u}\rangle \to^* |q_h, w_{M,u}\rangle$$

- If $M(u)$ does not halt, then $(q_1, w_{M,u}) \in K_0$, and $(q_2, w_{M,u}) \in K_1$ moreover $(q_{\bar{h}}, w_{M,u}) \in K_0$ and $(q_h, w_{M,u}) \in K_1$, thus:

$$|q_0, w_{M,u}\rangle \to^* \begin{cases} |q_h, w_{M,u}\rangle & \text{with probability } 1/2 \\ |q_{\bar{h}}, w_{M,u}\rangle & \text{with probability } 1/2 \end{cases}$$

For any DTM M and any input u, let $w_{M,u} \in \Sigma^*$ be an 'encoding' of M and u.

$$\begin{array}{rcl} K_0 & = & \{(q_1, w_{M,u}) \text{ s.t. } M(u) \text{ does not halt}\} \cup \{(q_{\bar{h}}, w)\} \\ K_1 & = & \{(q, w) \text{ s.t. } (q, w) \notin K_1\} \end{array}$$

What is the evolution of $[M_h]_{\{K_0,K_1\}}$ if the initial configuration is $(q_0, w_{M,u})$?

Evolution of M_h: $|q_0, w_{M,u}\rangle \to \frac{1}{\sqrt{2}}(|q_1, w_{M,u}\rangle + |q_2, w_{M,u}\rangle) \to |q_h, w_{M,u}\rangle$

- If $M(u)$ halts, then $(q_1, w_{M,u}), (q_2, w_{M,u}) \in K_1$, thus the evolution of $[M_h]_{\{K_0,K_1\}}$ is

$$|q_0, w_{M,u}\rangle \to^* |q_h, w_{M,u}\rangle$$

- If $M(u)$ does not halt, then $(q_1, w_{M,u}) \in K_0$, and $(q_2, w_{M,u}) \in K_1$ moreover $(q_{\bar{h}}, w_{M,u}) \in K_0$ and $(q_h, w_{M,u}) \in K_1$, thus:

$$|q_0, w_{M,u}\rangle \to^* \begin{cases} |q_h, w_{M,u}\rangle & \text{with probability } 1/2 \\ |q_{\bar{h}}, w_{M,u}\rangle & \text{with probability } 1/2 \end{cases}$$

Towards a new definition of OQTM

- Initial proposition: K is a partition of $Q \times \Sigma^* \times \mathbb{Z}$.

- Focus on the (classical) control: K is a partition of $Q \times \mathbb{Z}$.

  Theorem: There is a QTM M_h' and a partition K of $Q \times \mathbb{Z}$, s.t. $[M_h]_K$ is well observed and decides (with high probability), for any DTM M and any input u, whether M halts on input u.

- Finite partition: K is a partition of $Q \times \Sigma$. (Q: internal states; Σ: symbol pointed out by the head.)

Towards a new definition of OQTM

- Initial proposition: K is a partition of $Q \times \Sigma^* \times \mathbb{Z}$.
- Focus on the (classical) control: K is a partition of $Q \times \mathbb{Z}$.

  Theorem: There is a QTM M'_h and a partition K of $Q \times \mathbb{Z}$, s.t. $[M_h]_K$ is well observed and decides (with high probability), for any DTM M and any input u, whether M halts on input u.
- Finite partition: K is a partition of $Q \times \Sigma$. (Q: internal states; Σ: symbol pointed out by the head.)

Towards a new definition of OQTM

- Initial proposition: K is a partition of $Q \times \Sigma^* \times \mathbb{Z}$.

- Focus on the (classical) control: K is a partition of $Q \times \mathbb{Z}$.

  Theorem: There is a QTM M'_h and a partition K of $Q \times \mathbb{Z}$, s.t. $[M_h]_K$ is well observed and decides (with high probability), for any DTM M and any input u, whether M halts on input u.

- Finite partition: K is a partition of $Q \times \Sigma$. (Q: internal states; Σ: symbol pointed out by the head.)

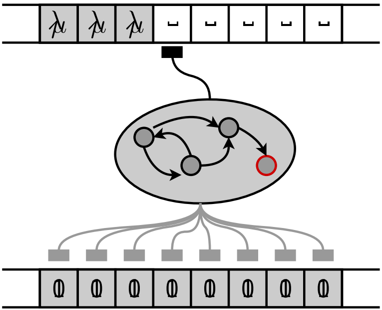
Simulation

Theorem: For any well-observed OQTM $[M]_K$ there exists a well-formed QTM M' which simulates $[M]_K$ within a quadratic slowdown.

Step one

If $M = (Q, \Sigma, \delta)$ and $K = \{K_\lambda\}_{\lambda \in \Lambda}$, let $\tilde{M} = (Q, \Sigma, \Lambda, \tilde{\delta})$ be a 2-tape QTM s.t.

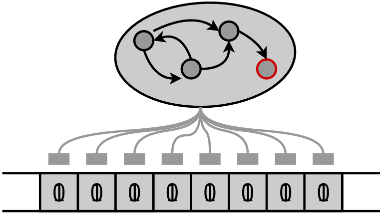
$$\tilde{\delta}(p, \tau, \llcorner\!\lrcorner, q, \sigma, \lambda, d, +1) = \begin{cases} \delta(p, \tau, q, \sigma, d) & \text{if } (p, \tau) \in K_\lambda \\ 0 & \text{otherwise} \end{cases}$$

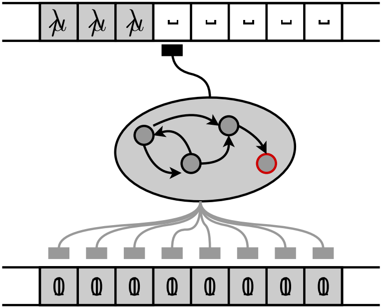


Lemma: $\tilde{M}$ is well formed.

Step two

Lemma: $[\tilde{M}]_{\tilde{K}}$ simulates $[M]_K$, where $\tilde{K} = \{Q \times \Sigma \times \{\lambda\}\}_{\lambda \in \Lambda}$





Step three

Since they act on distinct systems (the second head always moves to the right), the measurements can be postponed to the end of the computation:

Lemma: $\tilde{M}$ simulates $[\tilde{M}]_{\tilde{K}}$.

Lemma: There exists a well-formed 1-tape QTM M' which simulates $\tilde{M}$ within a quadratic slowdown.

Conclusion

- OQTM: extension of QTM with measurements;
- a more expressive (but not overpowerfull) machine: QTM, DTM, halting QTM.

Perspectives:

- Universal quantum Turing machine;
- what is the minimal k for which any OQTM $[M]_K$ can be efficiently simulated by an OQTM $[M']_{K'}$ where all regions of K' have a size less than k ?