Réseaux Quantiques

léments de sécurité et de fiabilité de l'informatic
et des algorithmes dans les réseaux quantiques

http://www.lri.fr/~kempe/ResQuant/

Julia Kempe

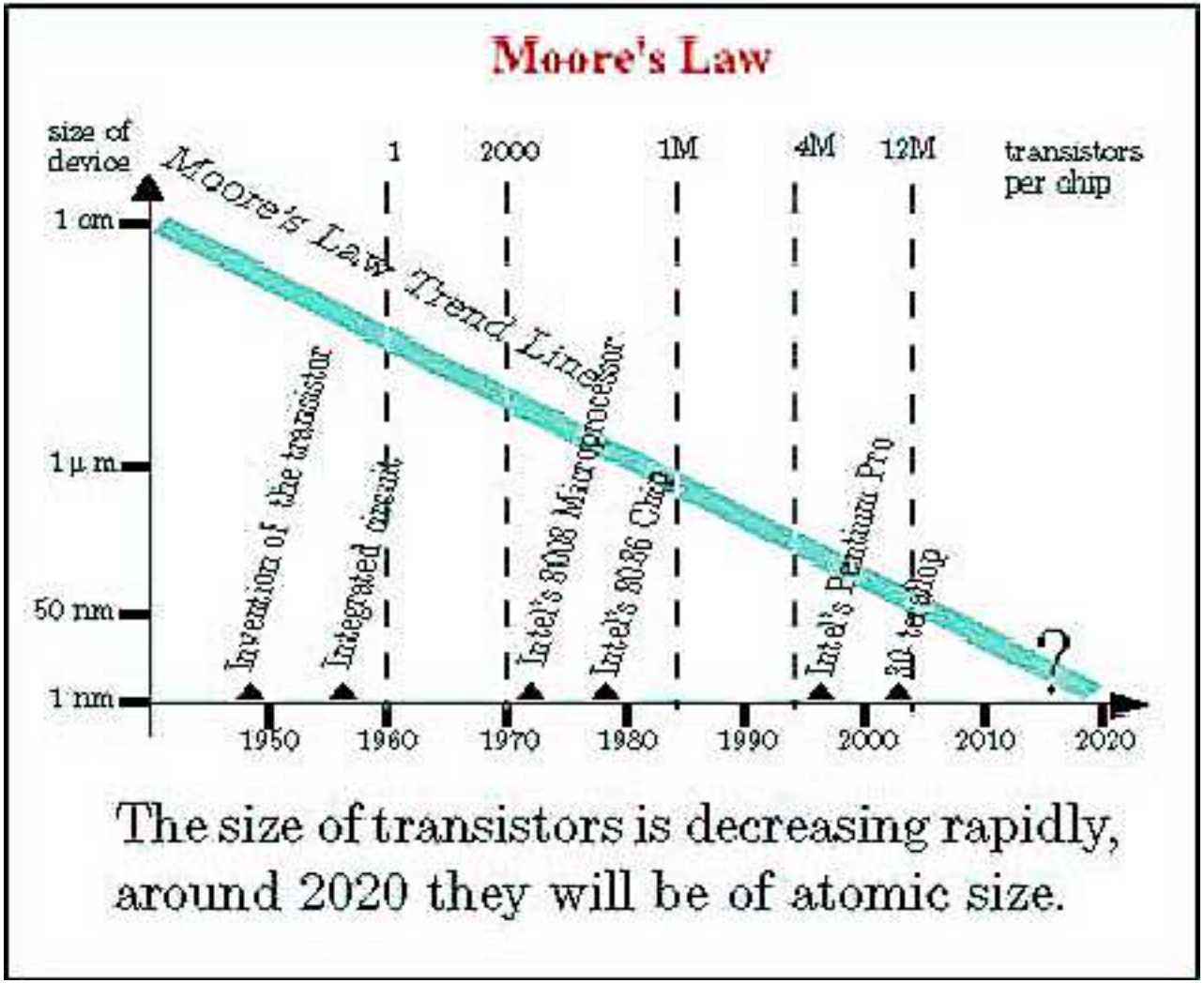
Christoph Dürr
Sophie Laplante
Frédéric Magniez
Miklos Santha

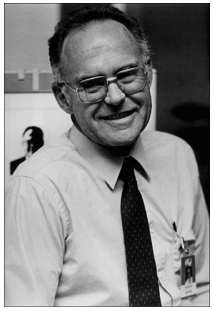
Harold Ollivier

Jean-Pierre Tillich

Jérémie Roland

Fin de la loi de Moore ?





"No exponential is forever. Your job is to
forever.", Andrew Gordon Moore Feb. 20

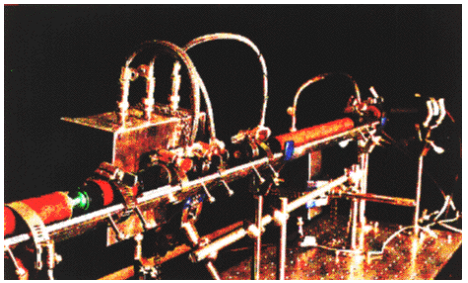
Phénomènes quantiques vers 2020…

- Approche actuelle : les supprimer
- Informatique quantique : les utiliser !

Cryptographie

- Protocole de distribution de clés secrètes [Bennett-Brassard 1984]

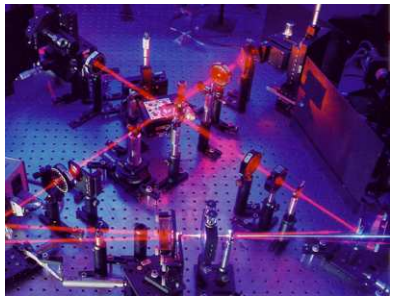
  Implémentation : ~100 km



Information quantique

- Téléportation [Bennett-Brassard-Crépeau-Jozsa-Peres-Wootters 1993]

  Réalisation : 1997 [Innsbruck]



Algorithmique

- Calcul de périodes [Simon, Shor 1994] Factorisation, log. discret...
- Recherche dans une liste non structurée [Grover 1996]

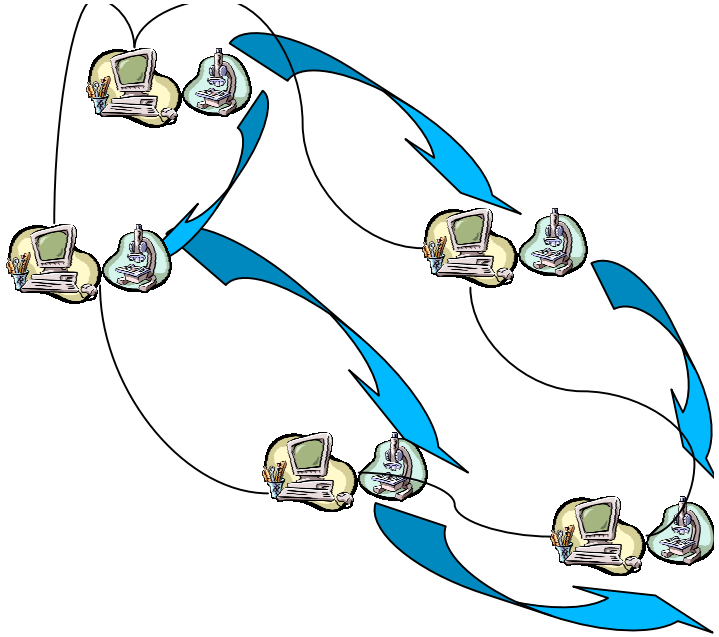
  Implémentation sur combien de qubits ?

  1995 : 2 [ENS], 1998 : 3,

  2000 : 5 [IBM] - 7 [Los Alamos]

  2001 : 8 [IBM]

Nature du réseau



- Postes locaux:
  Petit ordinateur quantique
  Ordinateur *classique*
- Transmission d'information quantique/classique

Objectifs du projet

- Fiabilisation
  codes correcteurs quantiques
  auto-test des architectures quantiques
- Routage
  marches aléatoires quantiques
- algorithmique de graphe
- Nouveaux algorithmes et protocoles de communication
- Characterizer le pouvoir des machines quantiques

ivier and J.-P. Tillich, *"Description of a quantum convolutional code"*, **Phys. Rev. Lett.**91 (17), 177

ivier and J.-P. Tillich, *"Quantum convolutional codes: fundamentals"*, arXiv, quant-ph 0401134 (200

ıara, H. Ollivier and J.-P. Tillich: *"Constructions and performance of classes of quantum LDPC cod* 502086 (2005), sousmis

ivier and J.-P. Tillich *"Interleaved serial concatenation of quantum convolutional codes: gate imple* *e error estimation algorithm"*, in Proc. of 26th **Symp. on Information Theory** in Benelux, 149 (20

n, J. Kempe, S. Simic, S. Sastry: *"Fault-tolerant quantum computation - a dynamical systems appr* **EEE TAC** (2005)

ıpe: *"Approaches to Quantum Error Correction"*, bookchapter, **Decoherence**, Progress in Mathemc es, Birhäuser, to appear (2006)

gniez, D. Mayer, M. Mosca, and H. Ollivier, *"Self-testing of quantum circuits"*, sousmis (2005)

ches quantiques/algorithmes sur les graphes

ıpe: *"Discrete Quantum Walks Hit Exponentially Faster"*, Proceedings of 7th International Works ion and Approximation Techniques in Computer Science (**RANDOM'03)**, p. 354-69 (2003)

; Santha and Mario Szegedi, *"Quantum and classical query complexities of local search are polyno* **oc. 36th Symp. on Theory of Computation (STOC)**, p. 494-501 (2004)

r, M. Heiligman, P. Høyer and M. Mhalla: *"Quantum query complexity of some graph problems"*, **Pro** 481-493, (2004)

bainis, J. Kempe, A. Rivosh: *"Coins Make Quantum Walks Faster"*, **Proc. 16th ACM-SIAM SODA**)

gniez, M. Santha, and M. Szegedy, *"Quantum algorithms for the triangle problem"*, **Proc. 16th AC**

nunication/ Algorithmes

Korff and J. Kempe, *"Quantum Advantage in Transmitting a Permutation"*, **Phys. Rev. Lett.**, Vol. 9
)04)

ıpe and A. Shalev: *"The hidden subgroup problem and permutation group theory"*, **Proc. 16th ACM**
.18-1125 (2005)

ieh, J. Kempe, S. Myrgren, K.B. Whaley *"An explicit universal gate-set for exchange-only quantum*
ı", **Quantum Information Processing**, Vol. 2 (4),p. 289-307 (2003)

orcz, J. Vala, K. Brown, J. Kempe, F.K. Wilhelm, K.B. Whaley: *"Full protection of superconducting q*
om coupling errors", **Phys. Rev. B**, Vol. 72, 064511 (2005)

insky, J. Kempe and R. de Wolf: *"Quantum Communication Cannot Simulate a Public Coin"*, lanl-repo
, sousmis (2005)

insky, J. Kempe, O. Regev and R. de Wolf: *"Bounded-Error Quantum State Identification and Exp*
s in Communication Complexity", lanl-report quant-ph/0511013, sousmis (2005)

voir des machines/réseaux quantiques

lante and F. Magniez *"Lower bounds for randomized and quantum query complexity using Kolmogor*
, **Complexity 2004**, p. 294-304 (2004)

aronov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, O. Regev: *"Adiabatic Quantum Computation is*
d Quantum Computation", **Proc. 45th FOCS**, p. 42-51, (2004)

ıpe, A. Kitaev and O. Regev, *"The Complexity of the Local Hamiltonian Problem"*,
h FSTTCS, p. 372-383 (2004)

ivier, D. Poulin and W. H. Zurek, *"Objective properties from subjective quantum states: environme*
ys. Rev. Lett., Vol. 93, 220401 (2004)

lin, R. Blume-Kohout, R. Laflamme and H. Ollivier, *"Exponential speed-up with a single bit of*
formation: measuring the average fidelity decay", **Phys. Rev. Lett.**, Vol. 92(17), 177906 (2004)

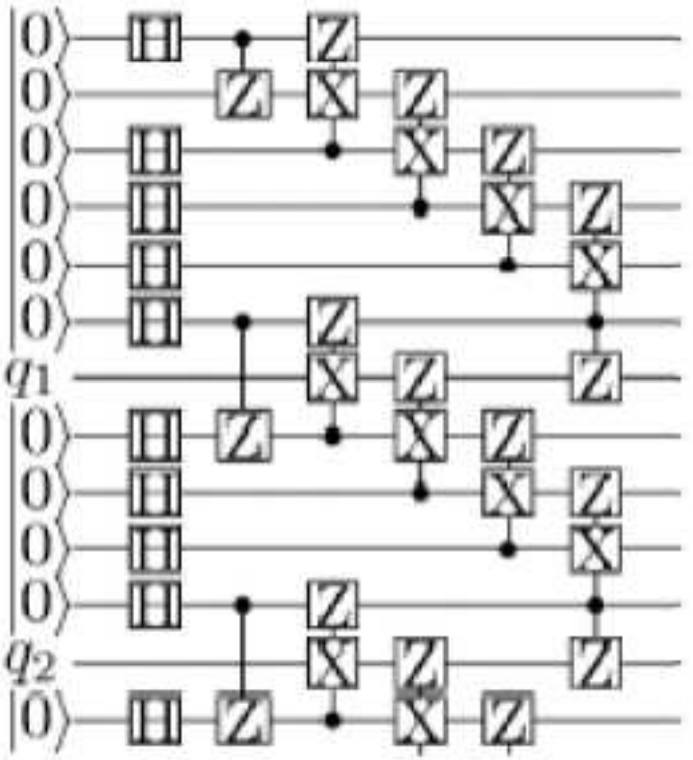
ivier, D. Poulin and W. H. Zurek *"Environment as witness: selective proliferation of information an*

Contexte

- Milieu : air libre ou fibre optique
- Tansmission : information quantique entre processeurs et mémoires

Solution : codes convolutifs

- Codage : complexité linéaire
- Décodage : complexité linéaire
- Application : réduction d'erreur



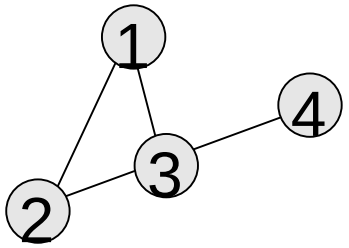
Exemple

- Code (5,1,2)

Extension

- Turbo-codes ✓
- Décodage itératif ✓
- Codes à matrice de parité creuse ✓

Modèle



Matrice d'adjacence Tableau d'adjacence

	1:	2:	3:	4:
1:	0	1	1	0
2:	1	0	1	0
3:	1	1	0	1
4:	0	0	1	0

1: 2 3
2: 3 1
3: 1 4 2
4: 3

n arêtes m nœuds

Problèmes

	Matrice d'adj.	Tableau d
-Connectivité, arbres de plus courts chemins	$\Theta(n^{1.5})$	$\Theta(\sqrt{nr}$
-Présence de triangle	$O(n^{1.3})$	$O(\sqrt{nr}$
-Propriété monotone	$O(n^{2-c})$	

s résultats:

xte

r deboguer un ordinateur quantique ?

faire confiance à des fournisseurs de services
s (cryptographiques)?

on : auto-test

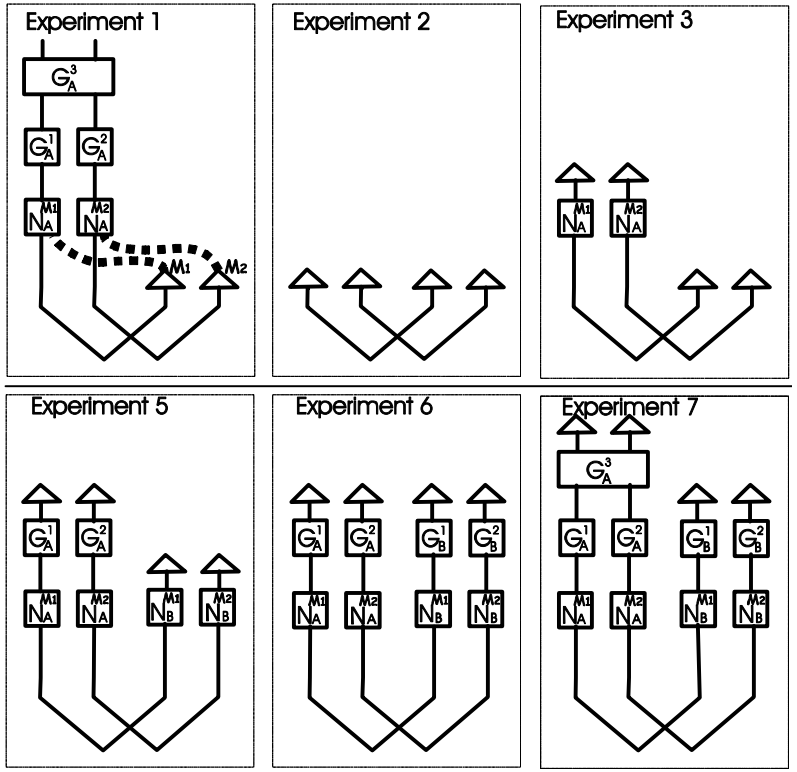
une architecture qui puisse être auto-testée

Auto-test de familles de portes

Auto-test inconditionel d'une paire EPR

ainsi que des appareils de mesure

Test robuste!



ésultats:

Contexte

- Information codée sur des photons
- Stockage difficile

Pas le temps de calculer le chemin !

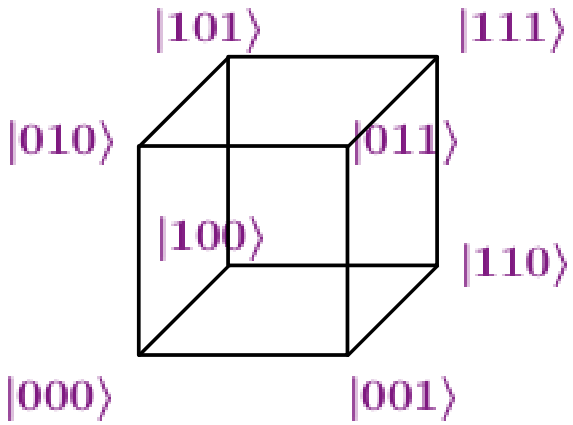
Solution : marche quantique

- Destinataire aléatoire

Temps d'atteinte ?

Cas de l'hypercube

- Classiquement : $O(2^n)$
- Quantiquement : $O(n)$!



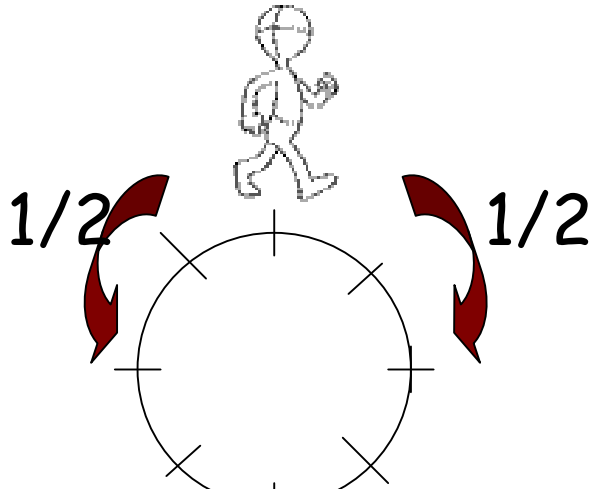
s résultats:

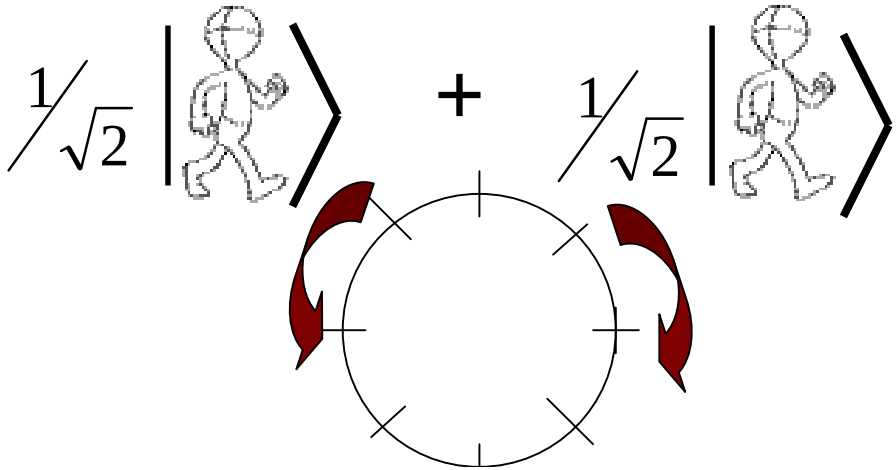
ı: use random walks for network tasks (routing, randomized algorithms)

sical: Randomized algorithms very successful

ı : construct a Markov chain (simple, local transitions)
(1) stationary distribution gives solution to problem ⇒ Mixing time
(2) which hits the desired solution ⇒ Hitting time

/ tool: Quantum Walks!





lassical random walk

Flip coin for direction

Walk conditioned on outcome

...	-2	-1	0	1	

Quantum "coined" walk:

$\{|\rightarrow\rangle,|\leftarrow\rangle\} \otimes$

...	-2	-1	0	1	2

States $|\rightarrow,x\rangle$ and $|\leftarrow,x\rangle$

- Coin flip:

$$|\rightarrow\rangle \Rightarrow \frac{1}{\sqrt{2}}|\rightarrow\rangle+\frac{1}{\sqrt{2}}|\leftarrow\rangle$$

$$|\leftarrow\rangle \Rightarrow \frac{1}{\sqrt{2}}|\rightarrow\rangle-\frac{1}{\sqrt{2}}|\leftarrow\rangle$$

- Shift:

$$|\rightarrow,x\rangle \Rightarrow |\rightarrow,x+1\rangle$$

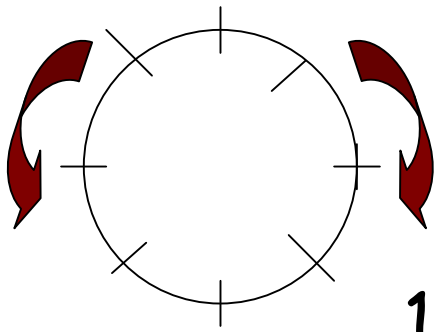
$$|\leftarrow,x\rangle \Rightarrow |\leftarrow,x-1\rangle$$

ıple line:

...	-2	-1	0	1	2	...

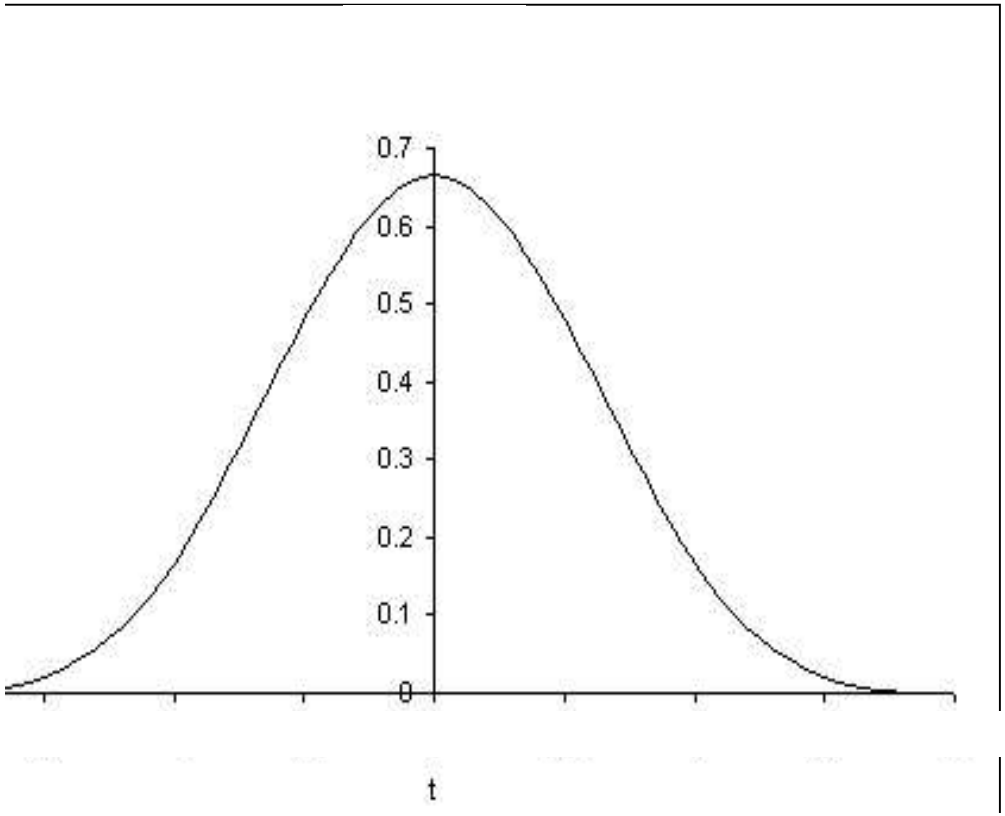
g time on N-circle:

classical: $O(N^2)$ quantum: $O(N)$

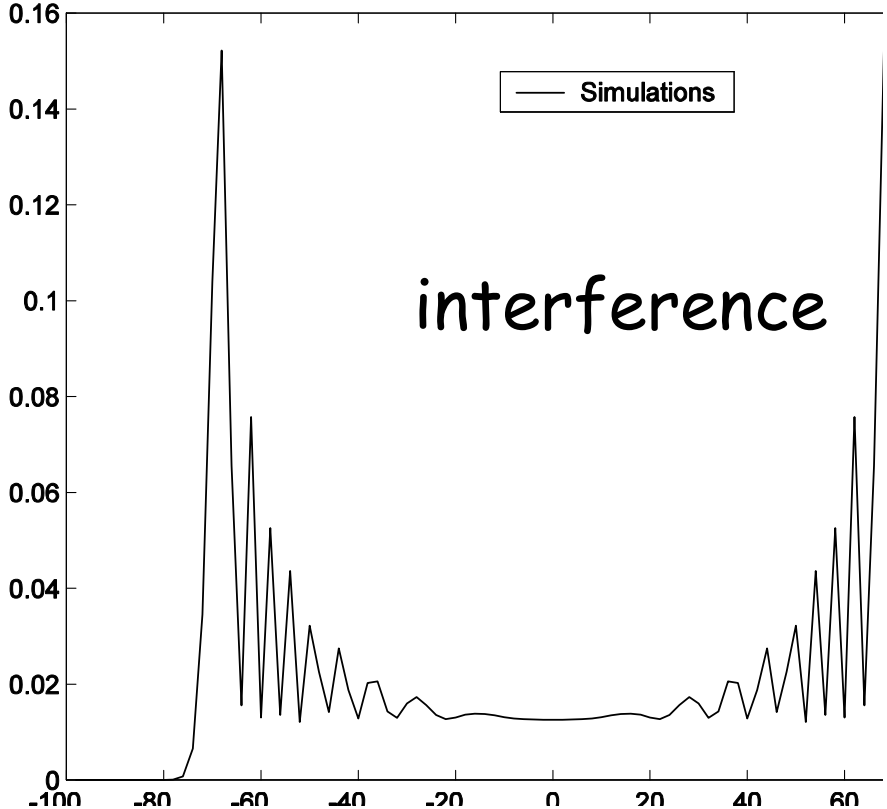


Probability distribution (measurement after T steps):

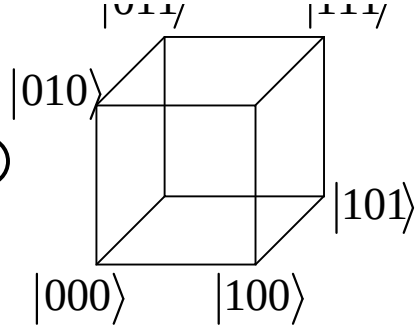
lassical:

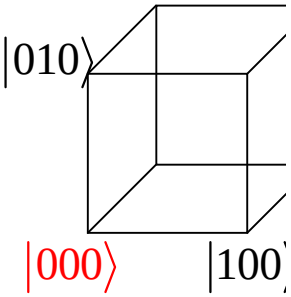


Quantum:



pace: $\{|\leftrightarrow\rangle, |\swarrow\nearrow\rangle, |\updownarrow\rangle\} \otimes$





ssical: from v to opposite corner, hitting-time exponential

$$T = 2^n(1 + O($$

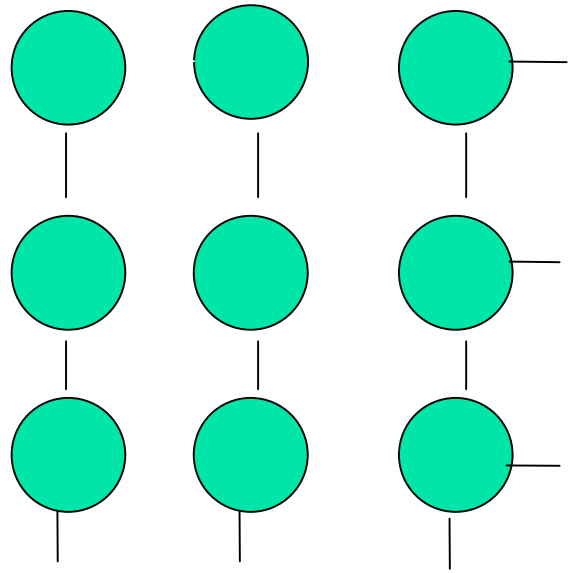
antum: polynomial

Hitting-time from v to opposite corner :

n known: $T \approx \frac{\pi}{2} n$ n unknown: $T = O(n^2)$

or decentralized routing in networks!
outing nodes do not know destination of packet, still routing is
ential advantage over the classical setting.

Set of items S, some marked.



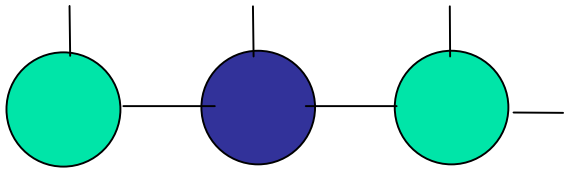
ric Algorithm:

Start with a uniform superposition over all S.

Apply one coin (transition rule) if S marked,

another if S not marked.

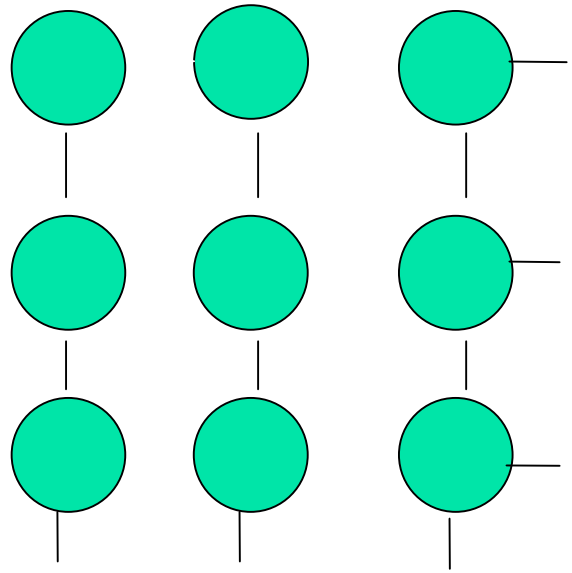
Measure after T steps



tum walk leads to a state in which marked S have higher amplit

"leaky"
Quantum walk

Set of items S, some marked.



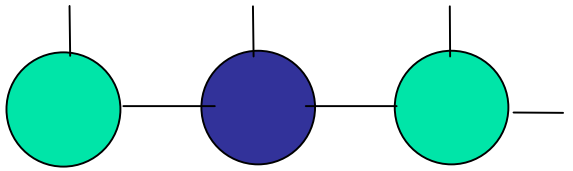
ric Algorithm:

Start with a uniform superposition over all S.

Apply one coin (transition rule) if S marked,

another if S not marked.

Measure after T steps



tum walk leads to a state in which marked S have higher amplit

ications :

spatial search [Ambainis,Kempe,Rivosh'05]

Commmunication

- Nouveaux protocoles de transmission
- Characterisation du pouvoir des modèles de communication

Algorithmes

- Analyse des algorithmes pour isomorphisme de graphe et recherche locale

Pouvoir des machines quantiques

- Etude de la décoherence (bruit)
- Etude des modeles physiques sur réseau
- Analyse des nouveaux modèles de calcul (calcul adiabatique sur réseau)

...