Complexity classes BPP and BQP

BPP = " bounded error-probability, probabilistic, polynomial time"

Def.: Probabalistic Turing machine (PTM) formally exactly as non-deterministic T.M., particularly with transition-relations,

$$\delta : (s, a) \longmapsto \{ (s_1, a_1, m_1), (s_2, a_2, m_2), \vdots, (s_k, a_k, m_k) \},$$

but now with alternative interpretation: prob. T.M. choses one rule $r_i \in \delta(s, a)$ at random with equal probability $1/k$.

→ $k \xleftarrow{r_i} k'$ with prob. $1/k$

→ prob. T.M. M on input x holds in x' with probability $p(x'|x)$.

Def.: Comp. class BPP

$L \in BPP :\Leftrightarrow$ L decided by PTM in polynomial time with error probability $p_{err} \leq 1/4$; i.e.

$\exists\, a \in \mathbb{N}$, PTM M s.t.

(1) $\forall x \in \Sigma^*$: $time_M(x) \leq |x|^a$.

(2) $\forall x \in L$: M accepts x with prob. $p \geq 3/4$

(3) $\forall x \notin L$: M accepts x with prob. $p \leq 1/4$

["M accepts x" = "M holds on input x with output 1"

Rmrks.:

1) PTM <=> standard computer with true random number generator

!?

<=> standard computer with pseudo rand. numb. gen.

2) complexity theory finds strong evidence for BPP = P !

("derandomization")

3) BPP = "class of problems that can be efficiently solved by Monte Carlo Methods"

4) error bounds can be strongly relaxed: e.g. for $\varepsilon > 0$, $q \in]\varepsilon, 1-\varepsilon[$

$\forall\, x \in L$: M accepts x with prob.

$$p \geq q + \varepsilon$$

$\forall\, x \notin L$: M accepts x with prob.

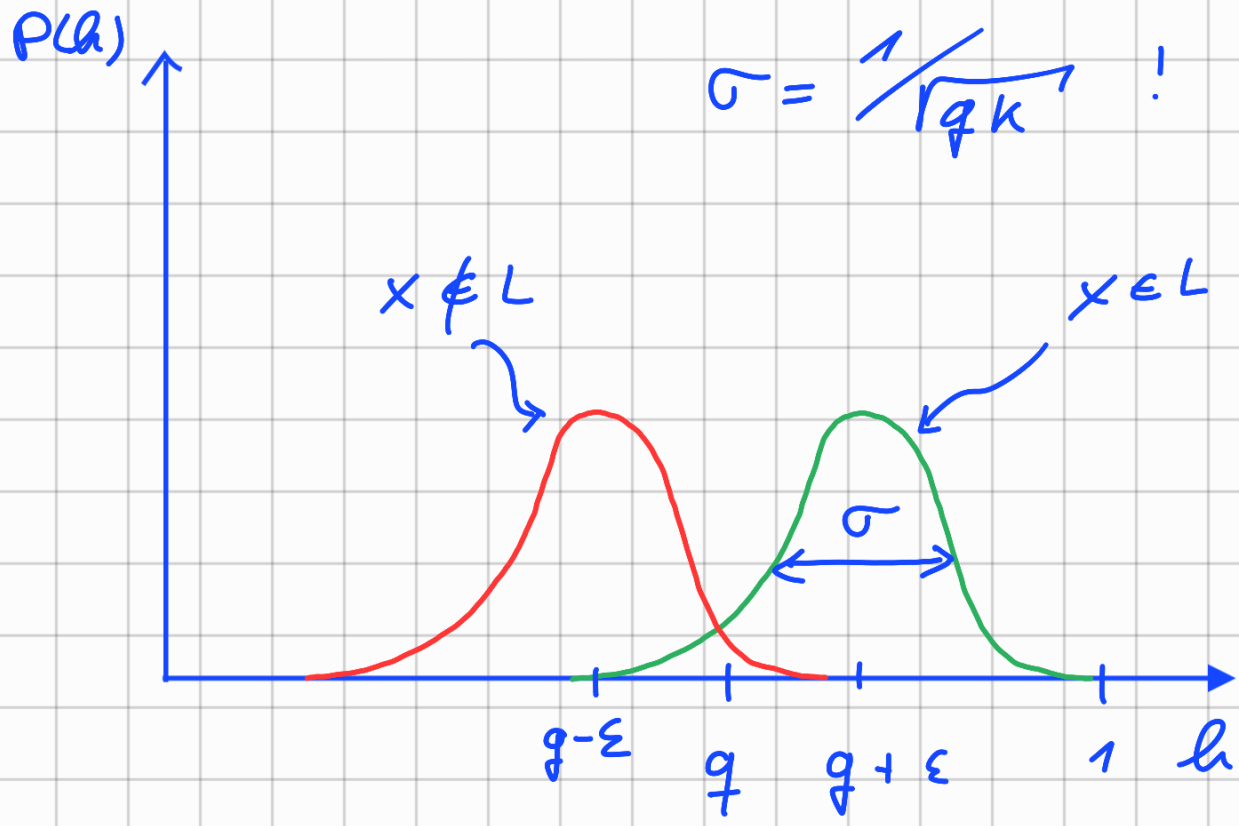
$$p \leq q - \varepsilon$$

Why? run (ε, q)-PTM k times on same input x, chose k suff. large:

def $h = \frac{k_{\text{accepts}}}{k}$ = relative freq. of acceptions in k runs on inp. x,

- accept x if $h > q$
- reject x if $h \leq q$!

→



$$\rightarrow \quad p_{err} \sim e^{-\varepsilon^2/2\sigma^2} = e^{-qk\varepsilon^2/2}$$

$$\rightarrow \quad \text{for} \quad k \gg \frac{1}{q\varepsilon^2}$$

p_{err} exponentially small !

Similarly: for any $c > 0$, $q \in]0,1[$:

$\forall x \in L$: M accepts x with

$$p \geq q + |x|^{-c}$$

$\forall\, x \notin L$: M accepts x with

$$p \leq q - |x|^{-c}$$

$\rightarrow$ chose $K = |x|^{2c+d}$!

Quantum complexity class BQP

("bounded error-prob., quantum, poly. time")

BQP = "class of problems that can be solved with quantum computer in polynomial time"

problem: make sure that used quantum circuits can be build with reasonable ($\hat{=}$ polynomial in $|x|$) effort!

$\longrightarrow$

Def.:

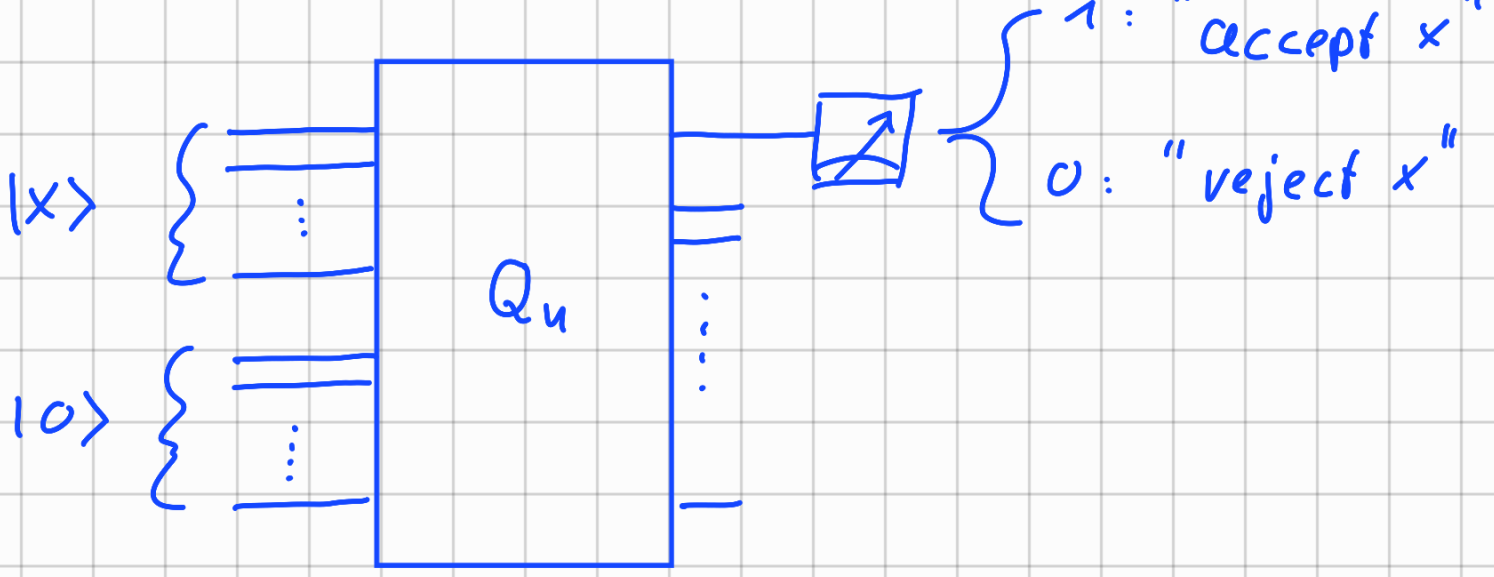
- Family of circuits $\{Q_n\}_{n \in \mathbb{N}}$ is

  polynomial-time generated

  $:\Leftrightarrow$ $\exists$ T.M. M which on input n outputs (encoding of) circuit Q_n in polynomial time:

  $$time_M(n) \leq n^\alpha$$

- acceptance of $x \in \Sigma^*$ by circuit Q_n, $n = |x|$:



Def: Quantum comp. class BQP

$L \in BQP \iff \exists$ polynomial-time generated $\{Q_n\}_{n \in \mathbb{N}}$ s.t.

$\forall x \in L$: $Q_{|x|}$ accepts x with $p \geq 3/4$

$\forall x \notin L$: $Q_{|x|}$ accepts x with $p \leq 1/4$

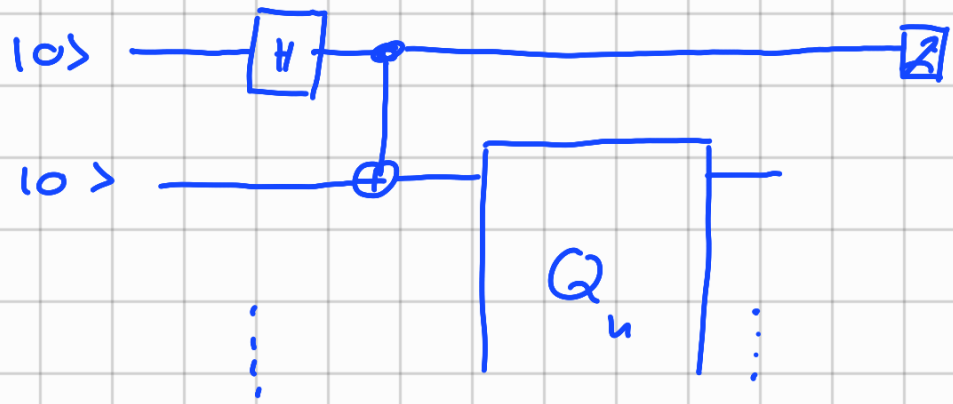
Rmrks.:

1) error-probabilities as described as in BPP

2) obviously $BPP \subseteq PQP$

- $P \subset BQP$ ✓
- random bits: $|0\rangle$ — H — Z ✓

alternatively:



3) strong evidence for $BPP \subsetneq PQP$

↑ FACTOR $\in$ BQP (Shor!)

but probably FACTOR $\notin$ BPP

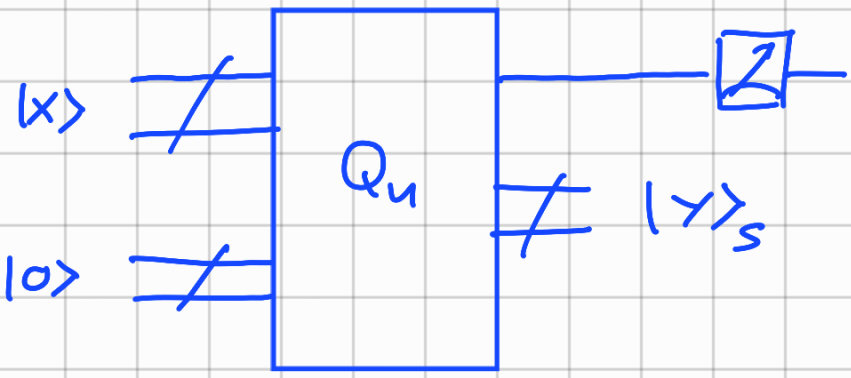
4) no evidence for $NP \subset BQP$!

apart from speeding-up search for solutions with Grover's algorithm

no systematic improvements by quantum algorithms in sight!

5) BQP $\subseteq$ PSPACE

"classical" computation of $P_{accept}(x)$ in <u>polynomial space</u> possible by summing up (sequentially many) <u>path-amplitudes</u>:



$$P_{accept}(x) = \sum_{y \in \{0,1\}^s} \underbrace{\left| \langle 1, y | Q_u | x, 0 \rangle \right|^2}_{\in \mathbb{C} : A_y}$$

assume that Q_u is composed of $T = |x|^\alpha$ elementary gates $G_1, G_2, \ldots, G_T$ $\longrightarrow$:

$$A_y = \langle 1, y | \, G_T \, G_{T-1} \cdots G_2 \, G_1 \, | x, 0 \rangle$$

$$= \sum_{i_1, \ldots, i_{T-1} \in \{0,1\}^{s+1}} \langle 1, y | \, G_T \, | i_{T-1} \rangle \cdot$$

$$\cdot \underbrace{\langle i_{T-1} | \, G_{T-1} \, | i_{T-2} \rangle \cdots \langle i_1 | \, G_1 \, | x, 0 \rangle}_{\text{computable in PSPACE}}$$

computable in PSPACE !

$\rightsquigarrow$ $p_{accept}(x) = \sum_y |A_y|^2$ computable in PSPACE.

Relationship of P, BPP, BQP, NP, PSPACE: