

BQP

$$QP = \{ f : \{0,1\}^* \rightarrow \{0,1\}^* \mid$$

∃ uniform family of Quantum
 circuits C_n : s.t.

$$\forall n : P[C_n(x) = f(x); x \in \{0,1\}^{2n}] \geq \frac{2}{3} \}$$

BQP := QP reduced to predicates

24 BQP versus EXP, PSPACE, PP

Conclusion

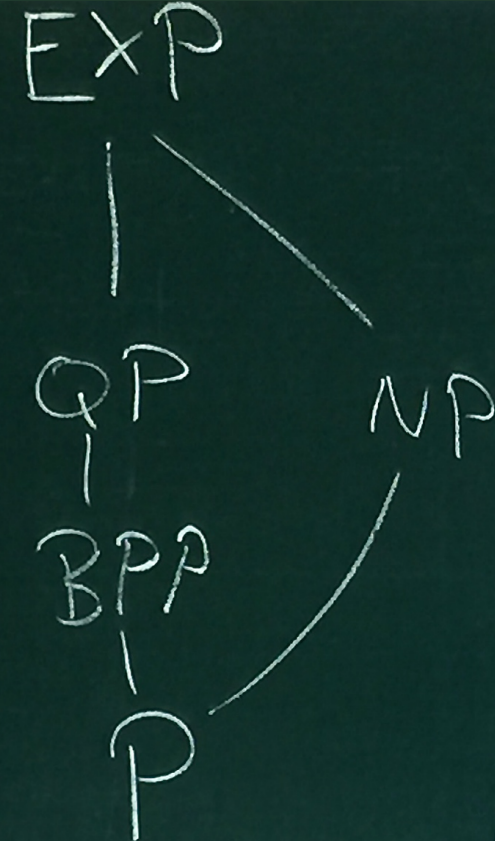
EXP

NP

QP

BPP

P



BQP versus EXP

it suffices to use - H-matrix

- Toffoli gate

CCNOT

not necessary to use

a complex gate

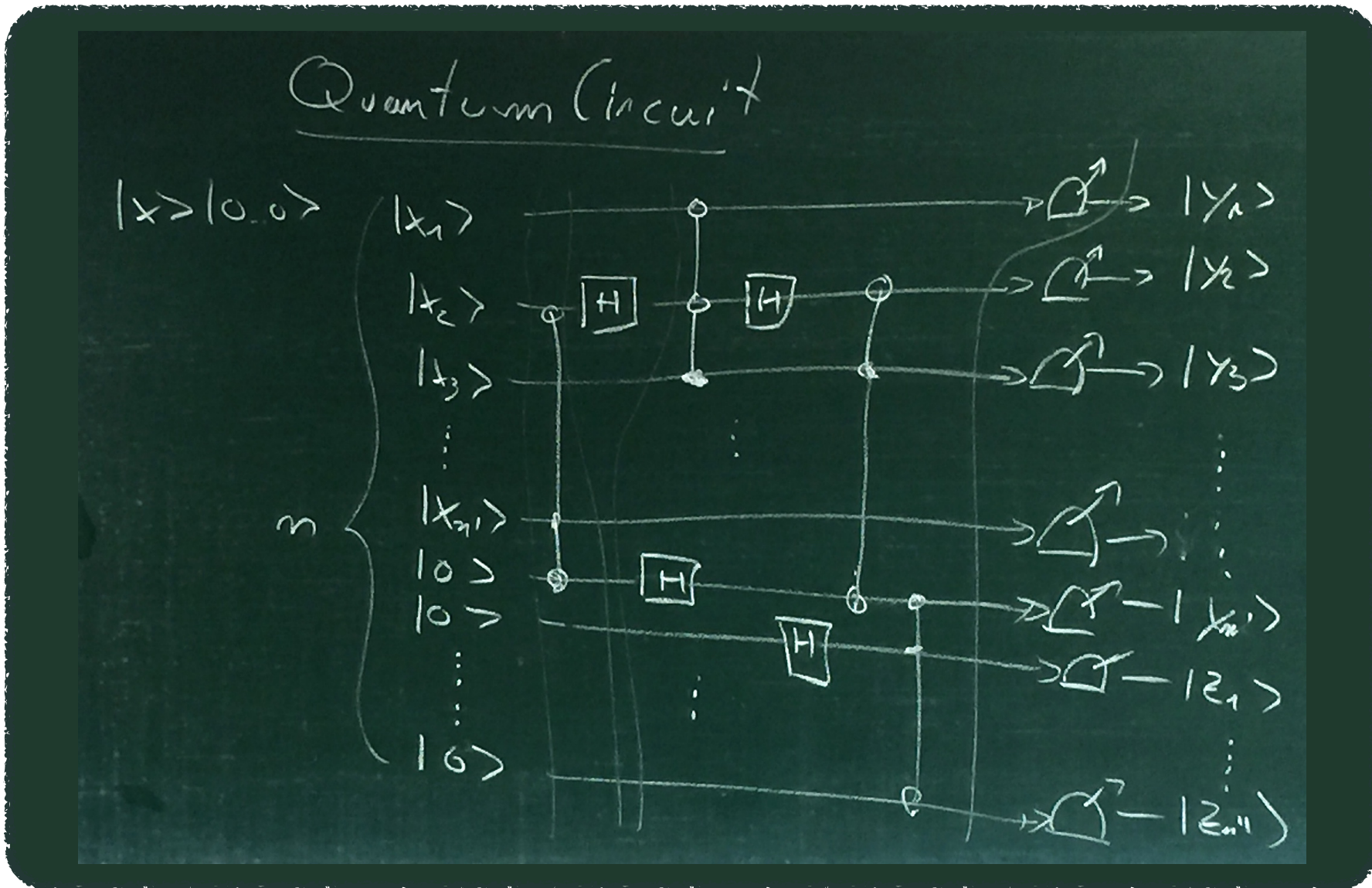
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

CCNOT

1	0	0	0
0	1	0	0
0	0	1	0
0	0	0	1

24 BQP versus EXP, PSPACE, PP

Conclusion



24 BQP versus EXP, PSPACE, PP

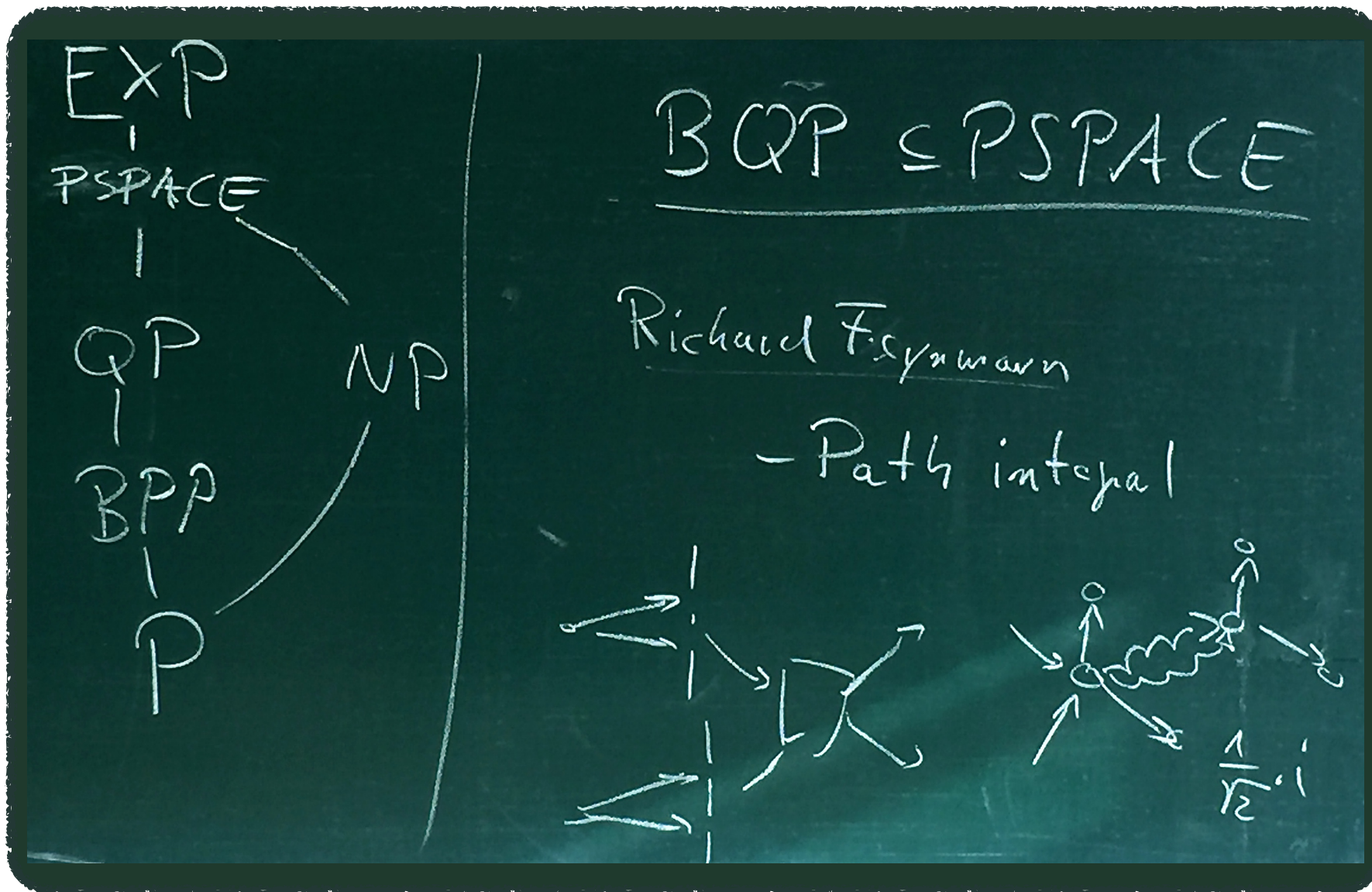
Conclusion

$$|\varphi\rangle = \sum_{\underbrace{00\dots 0}_n} |00\dots 0\rangle + \alpha_{0.01} \cdot |0\dots 01\rangle + \dots$$

- 2^n complex variables $\alpha_{b_1\dots b_m} \cdot 2^{\frac{1}{2}m}$
 inter
- m : no. of Quantum operators
- the size of an integer $\alpha_{b_1\dots b_m} \in 2^{O(m)}$
- each operator can be computed in time $2^n \cdot 2^n \cdot 2^m \in 2^{O(n+m)}$
- run-time of $2^{O(n+m)} \rightarrow \text{BQP} \subseteq \text{EXP}$

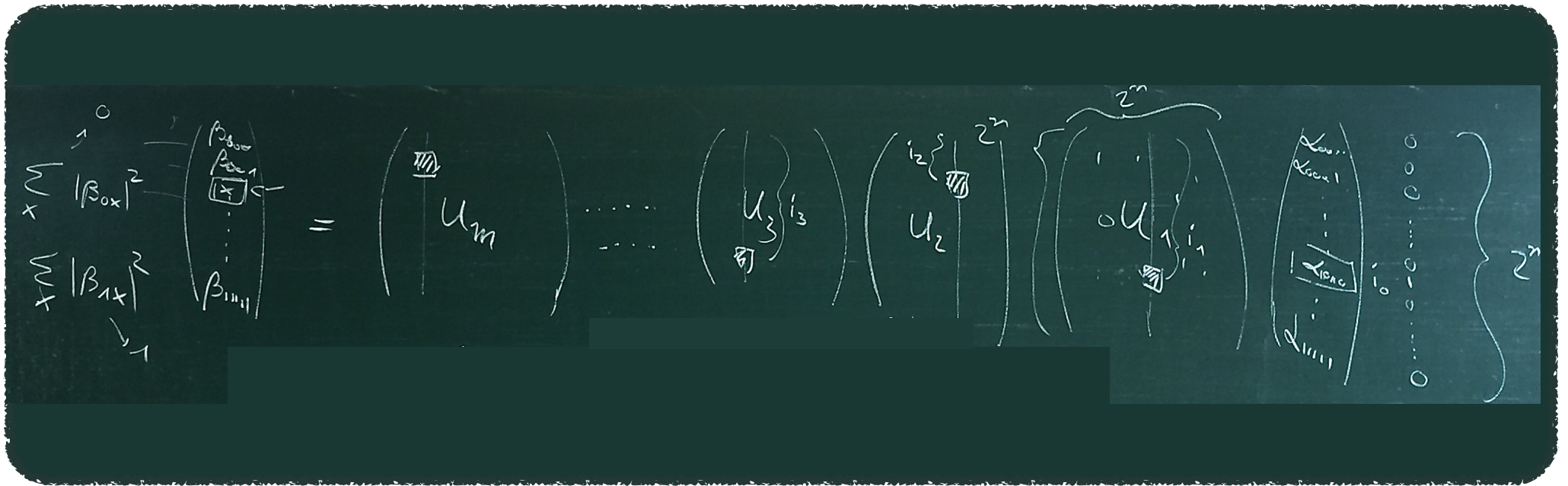
24 BQP versus EXP, PSPACE, PP

Conclusion



24 BQP versus EXP, PSPACE, PP

Conclusion



The image shows a handwritten mathematical derivation on a chalkboard. It starts with a unitary matrix U acting on 2^n qubits, represented as a product of two sums of squares of coefficients β_{0x} and β_{1x} . This is equated to a sequence of unitary operations: U_m , followed by a sequence of U_3 and U_2 operations, and finally a sequence of U_1 operations. The final part of the derivation shows a sequence of 0 and 1 bits, representing the output of the computation.

24 BQP versus EXP, PSPACE, PP

Conclusion

$$\beta_{i_0, i_1, \dots, i_m} = \sum_{j_1, \dots, j_m} \prod_{j=1}^m U_j(i_j, j_m) \cdot \alpha_{i_0}$$

$i_0 \in \{0, \dots, 2^n - 1\}$
 $i_1 \in \dots$
 \vdots
 $i_m \in \{0, \dots, 2^n - 1\}$
 space needed
 $15 \mid n \cdot m$

H for $i, j \in Q$ bit
 CNOT for $i, j \in Q$ bit

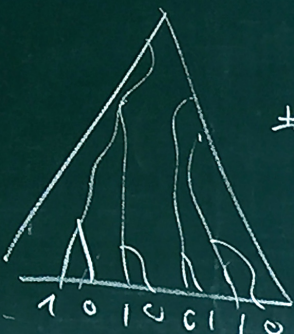
24 BQP versus EXP, PSPACE, PP

Conclusion

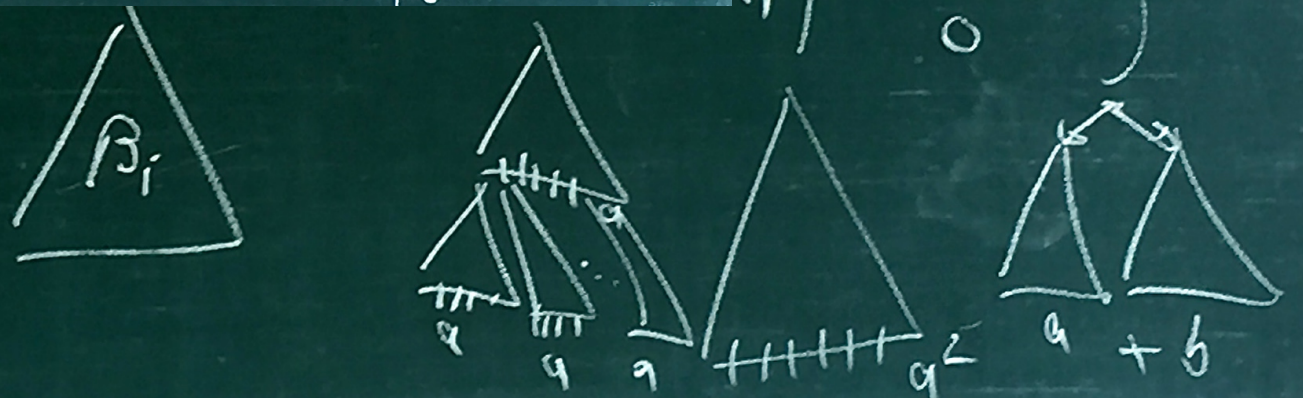
BQP versus PP

$$PP := \left\{ L \subseteq \Sigma^* \mid \exists \text{PTM } M \right.$$

$$\left. \begin{array}{l} \text{pol time} \\ P[L(M)=L] > \frac{1}{2} \end{array} \right\}$$



$$\#_{\text{accept}} \geq \frac{1}{2} \#_{\text{reject}}$$



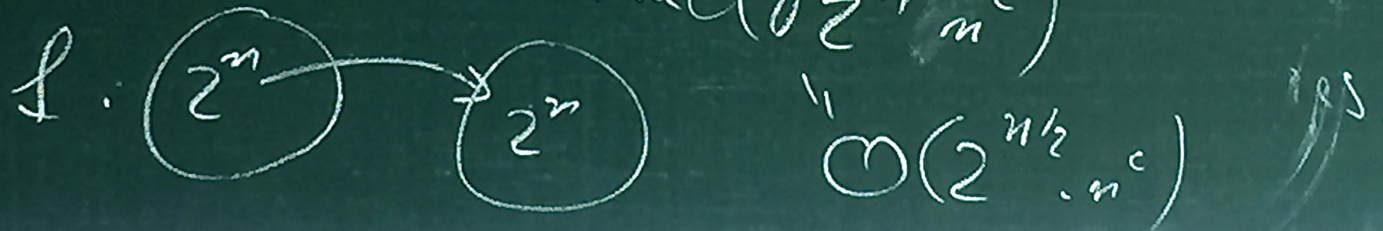
24 BQP versus EXP, PSPACE, PP

Conclusion

Quantum Computing

- Shor '95 . Integer Factoring is in QP
15, 143
- Fourier Transform, CNOT + H
- Discrete logarithm: $x: a^x = b \pmod p$

Grover: - Search in a set of 2^n elements
in time $(\sqrt{2^n} \cdot n^c)$



24 BQP versus EXP, PSPACE, PP

Conclusion

