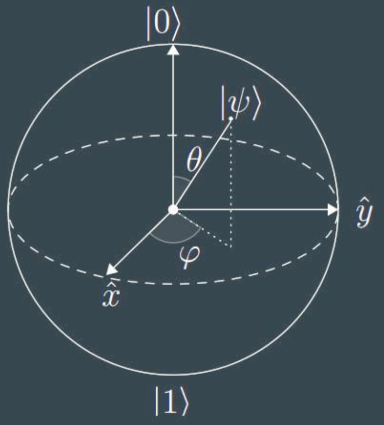
UNIVERSITÀ DEGLI STUDI DI TRIESTE

Entanglement and Robustness of the Quantum Fourier Transform in Shor's Algorithm

Candidate:
Giulia Tranquillini

Supervisor:
Antonello Scardicchio

Basics of quantum computation



$$|\psi >= \cos\frac{\theta}{2}|0> + e^{i\varphi}\sin\frac{\theta}{2}|1>$$

Two-level system

$$\rho = \sum_{k=1}^{n} \lambda_j |\psi_j >< \psi_j|$$

n-level system

$$A = A^{\dagger} = \sum_{\alpha=1}^{n} a_\alpha |\alpha >< \alpha|$$

$$\rho \rightarrow \sum_\alpha P_\alpha \rho P_\alpha$$

$$\mathcal{P} = |< a_\alpha|\psi >|^2$$

Measure

The power of quantum computing

It is possible to define a quantum computational process of size m as the sequence:

$$\mathcal{A}_m = (U_{i_0}, \vec{a_0}), \ldots (U_{i_m}, \vec{a_m}).$$

Integer factorisation

General number field sieve

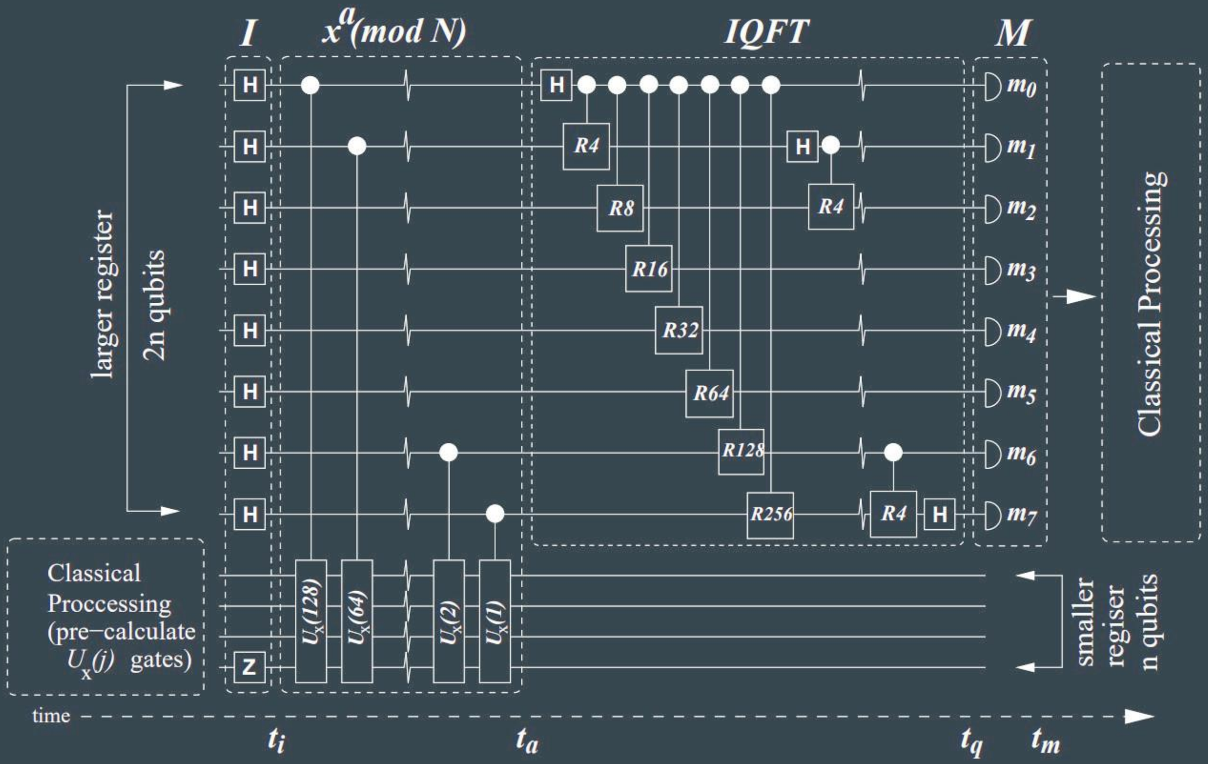
super-polynomial time

Shor's algorithm

polynomial time

Shor's algorithm

$$N = p \cdot q$$
$$n = log_2 N$$



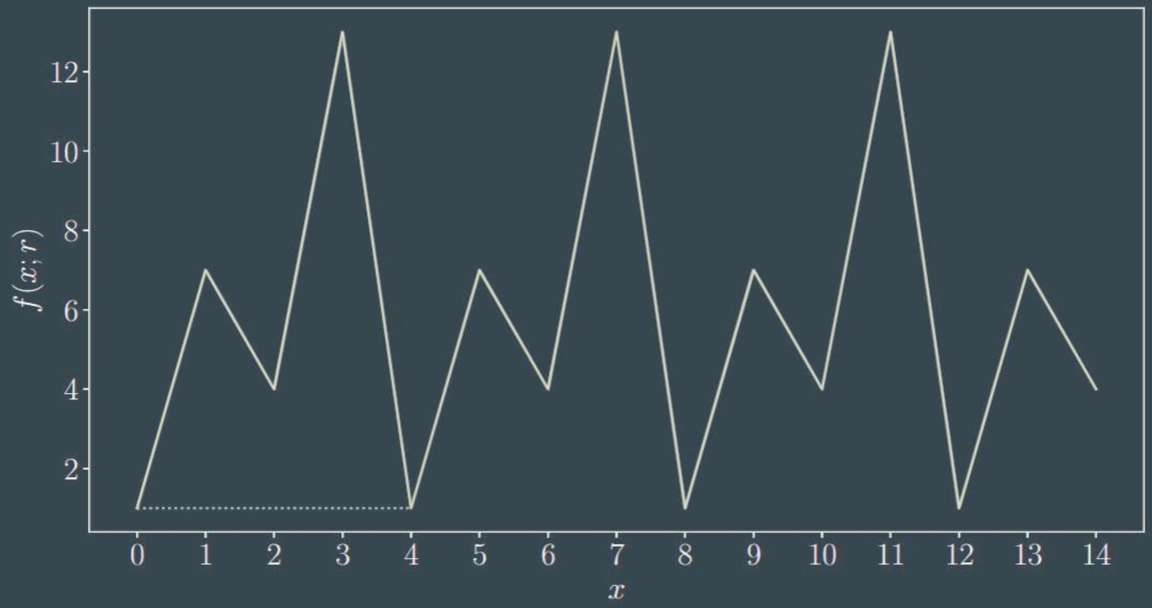
Quantum period finding

$$f(l) = y^l \bmod N$$
$$r : y^r = 1 \bmod N$$

Constraint:

$$\gcd(N, y) = 1$$

$$y \in \{2, \ldots, N-1\}$$



$$N = 15 \, y = 7$$

Classical post-processing

	Register Output c	Phase
0	$10000000(\text{bin}) = 128(\text{dec})$	$128/256 = 0.50$
1	$01000000(\text{bin}) = 64(\text{dec})$	$64/256 = 0.25$
2	$11000000(\text{bin}) = 192(\text{dec})$	$192/256 = 0.75$
3	$00000000(\text{bin}) = 0(\text{dec})$	$0/256 = 0.00$

	Phase	Fraction	Period
0	0.5	1/2	2
1	0.25	1/4	4
2	0.75	3/4	4
3	0.00	0/1	1

$$\frac{c}{2^{2n}} \simeq \frac{k}{r}$$

$$1 \leq k < r$$

$$\boxed{\begin{aligned} p &= \gcd(y^{r/2} + 1, N) \\ q &= \gcd(y^{r/2} - 1, N) \end{aligned}}$$

Entanglement analysis

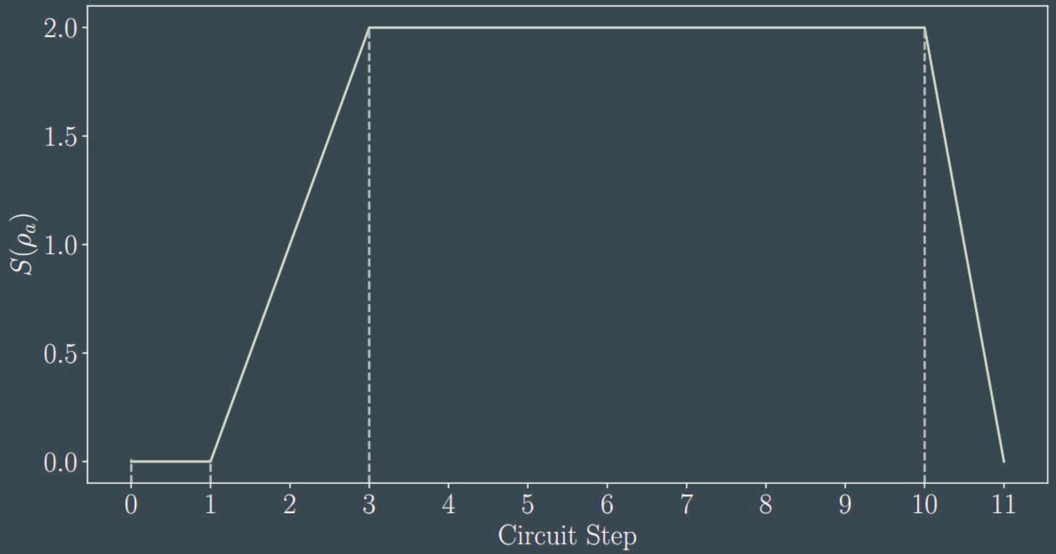
Entanglement within the two registers

The state $\rho \in \mathcal{S}(S_1 + S_2)$ is called entangled if and only if it cannot be written as the tensor product of the density matrices of the sub-systems:

$$\rho \neq \sum_{i,j} \lambda_{ij}\, \rho_1^i \otimes \rho_2^j$$

Given $\rho_1^i \in \mathcal{S}(S_1)$ and $\rho_2^j \in \mathcal{S}(S_2)$ with $\lambda_{ij} \geq 0$ and $\sum_{i,j=1}^{n} \lambda_{ij} = 1$

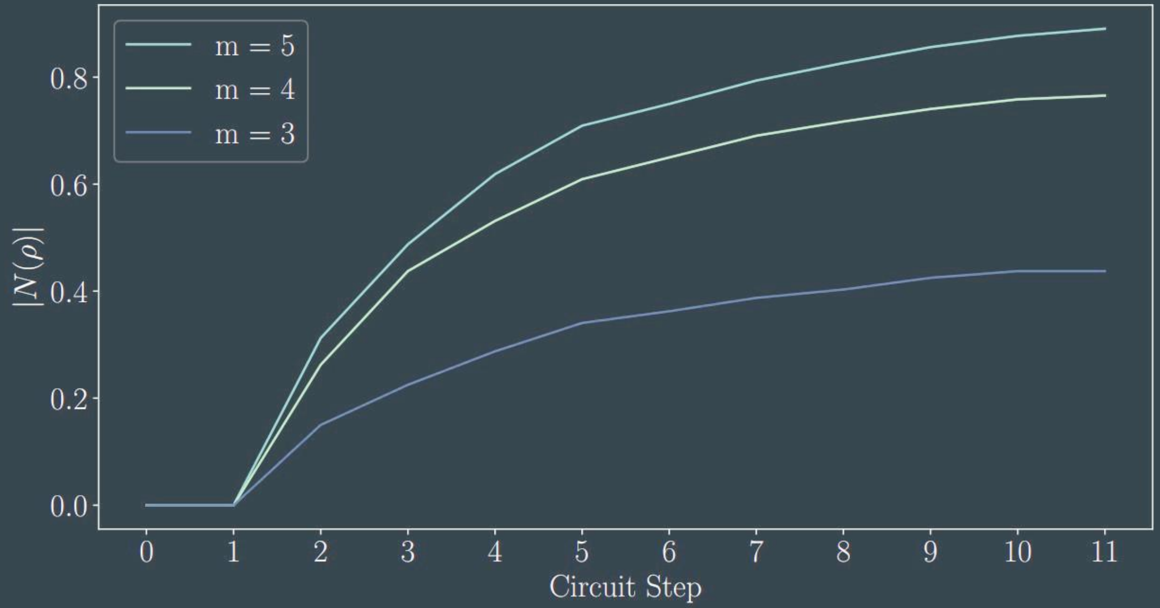
$$\boxed{\mathcal{S}(\rho_a) = -\mathrm{Tr}(\rho_a \log_2 \rho_a)}$$



Entanglement of subsystems

For mixed state the entanglement witness is the sum of negative eigenvalues of the reduced density matrix:

$$N(\rho) = \frac{|\rho^T|_1 - 1}{2}$$



$N = 21\, y = 4$

Error system

A discrete error model is inserted in the localised portion of the circuit performing the IQFT.

$$\boxed{\mathcal{P} \rightarrow \sigma_X \quad 1 - \mathcal{P} \rightarrow \sigma_Z}$$

$$X|\psi >= \alpha_1|1 > +\beta_1|0 >$$

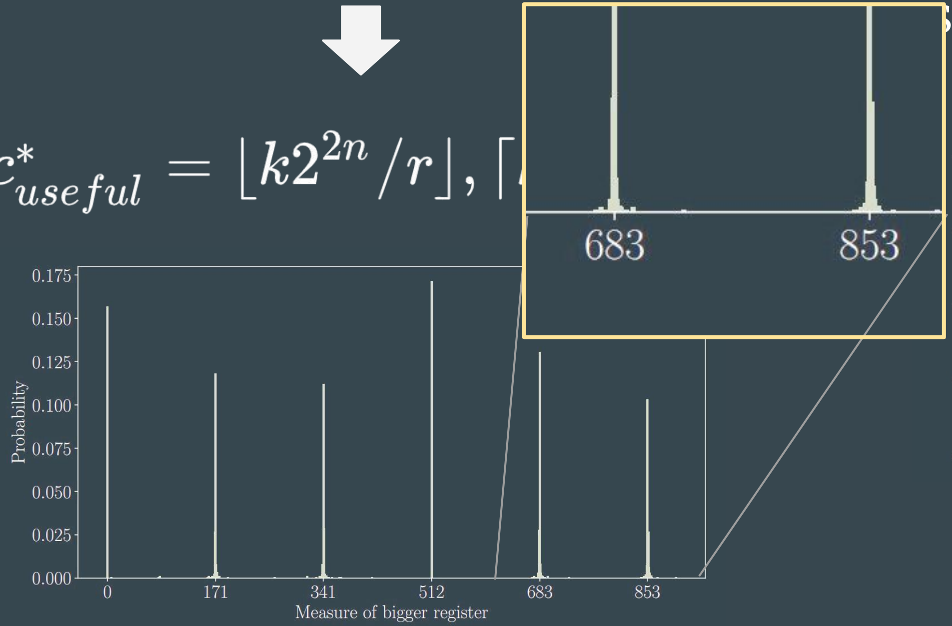
$$|\psi >= \alpha_0|0 > +\beta_0|1 >$$

$$Z|\psi >= \alpha_1|0 > -\beta_1|1 >$$

Checking the algorithm effectiveness

$$\frac{c}{2^{2n}} \simeq \frac{k}{r}$$

$$c^*_{useful} = \lfloor k2^{2n}/r \rfloor, \lceil$$



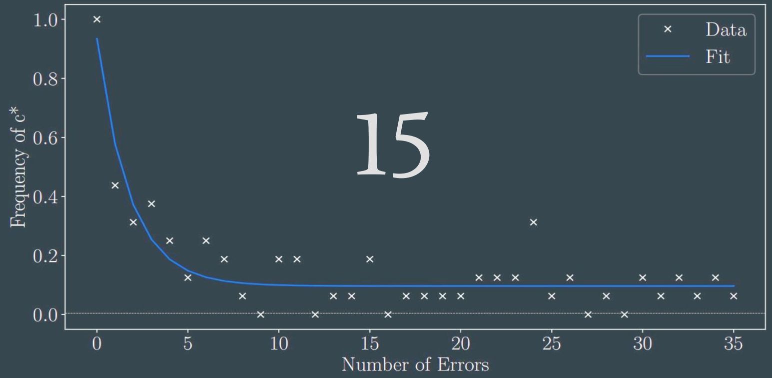
Simulation parameters:

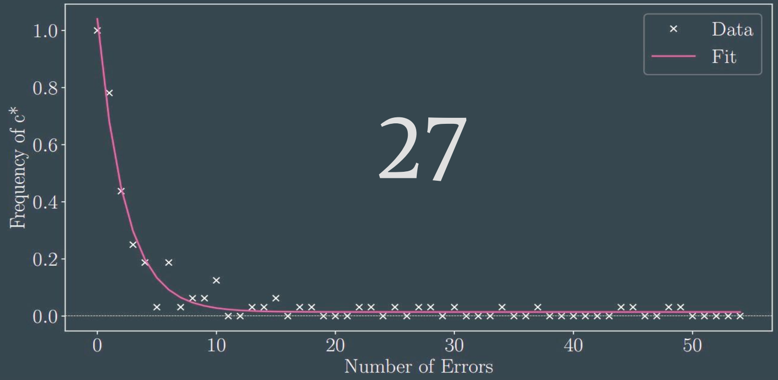
N	y	n	circuit n	$\#_{err}$
15	8	4	12	36
27	8	5	15	55
63	31	6	18	78
247	27	8	24	171

$$s(n, r) = \sum_{c^*_{useful}} p(c^*_i, n, r)$$

Results

Robustness of the algorithm

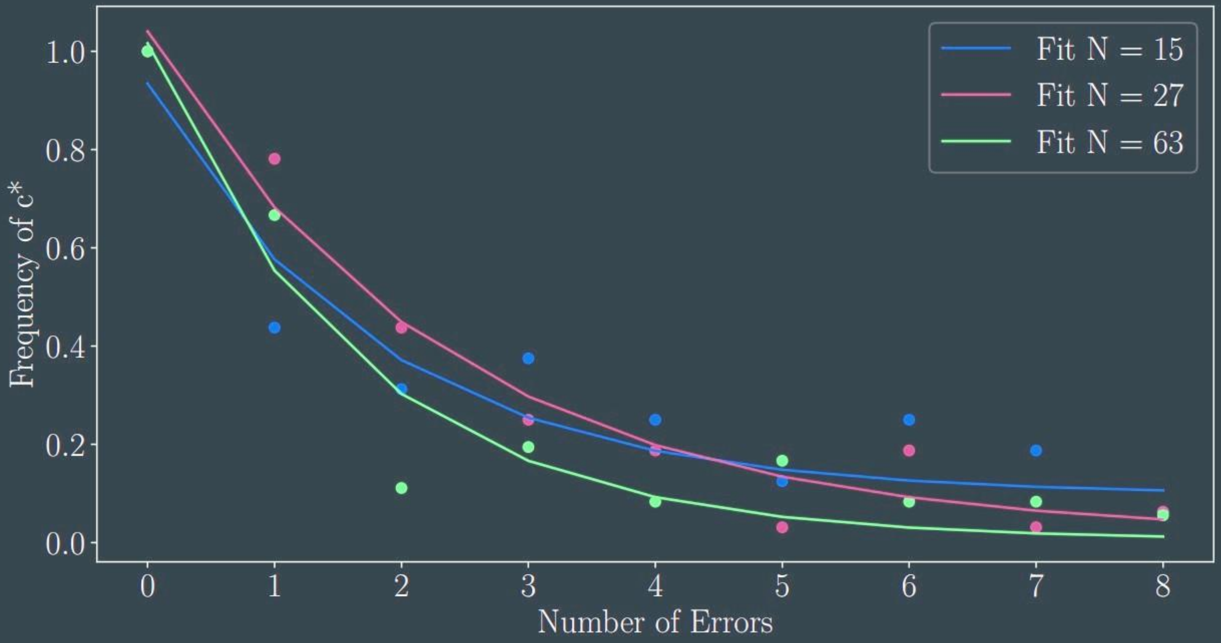




Which is the maximum number of errors n_0 tolerated by the algorithm?

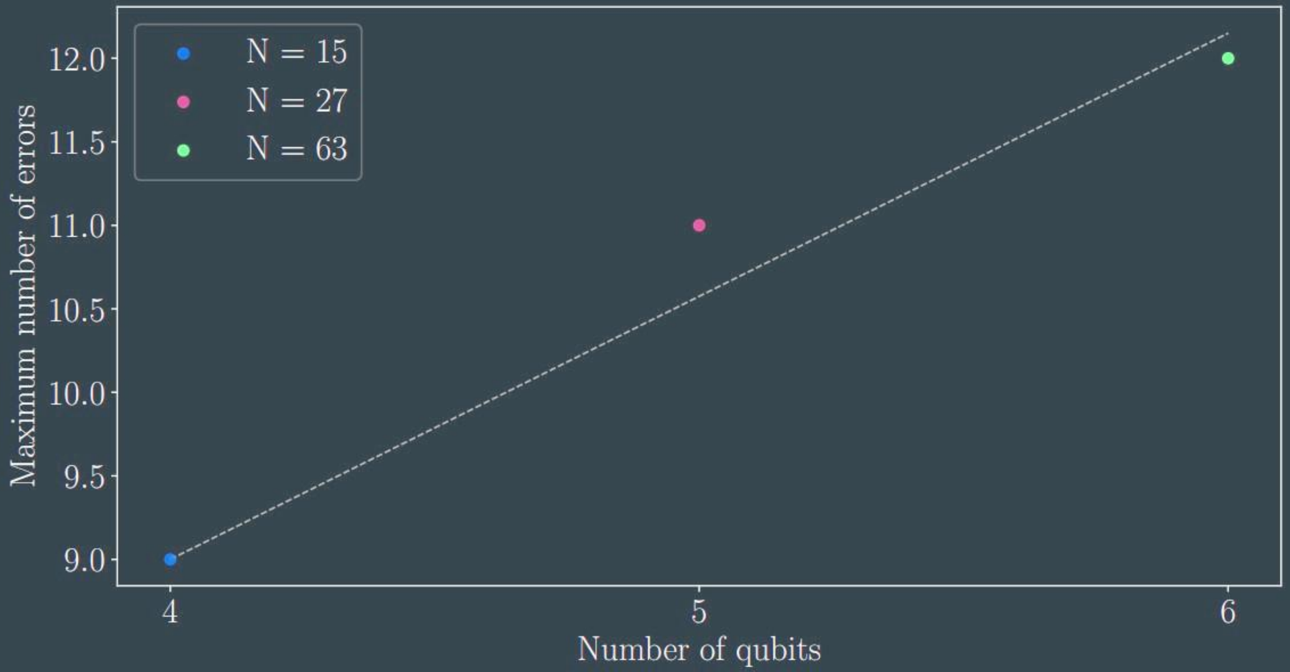
$$y = ae^{-bx} + c$$

$$Pr(n) = Pr(0)e^{-n/n_0}$$



N	b	n_0
15	0.56	1.81
27	0.82	1.22
63	0.61	1.63

Which is the maximum number of errors before complete loss of efficiency?



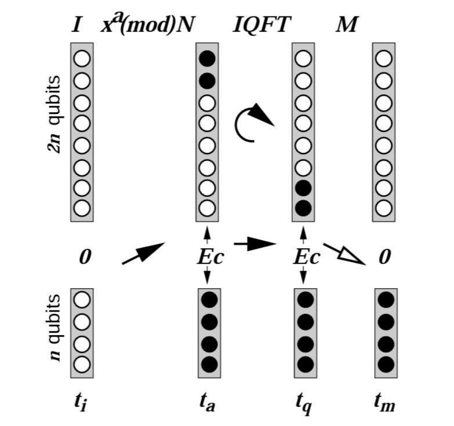
$$y = ax + b$$

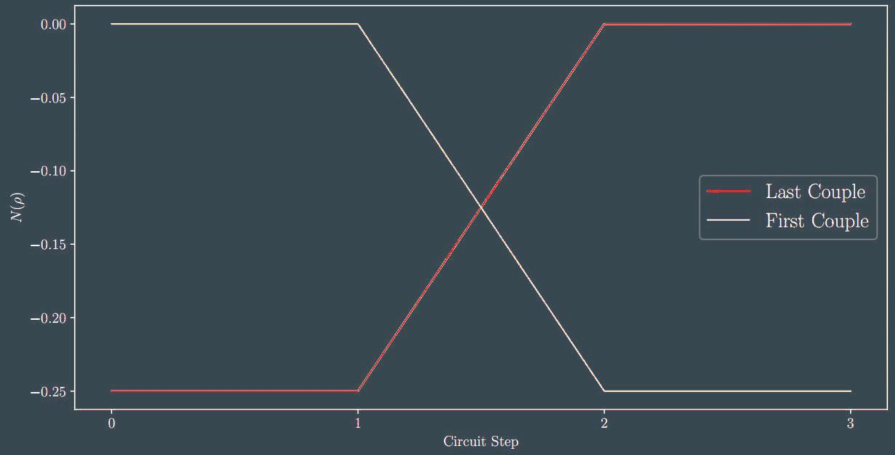
$$\#_{err}^{max} \simeq 2 \cdot n$$

Thank you for your attention

Entanglement Shift

$$F_n = \frac{1}{\sqrt{2^n}} \sum_{q=0}^{2^n-1} \sum_{q'=0}^{2^n-1} e^{\frac{2i\pi qq'}{2^n}} |q><q'| = Q_n R_n$$

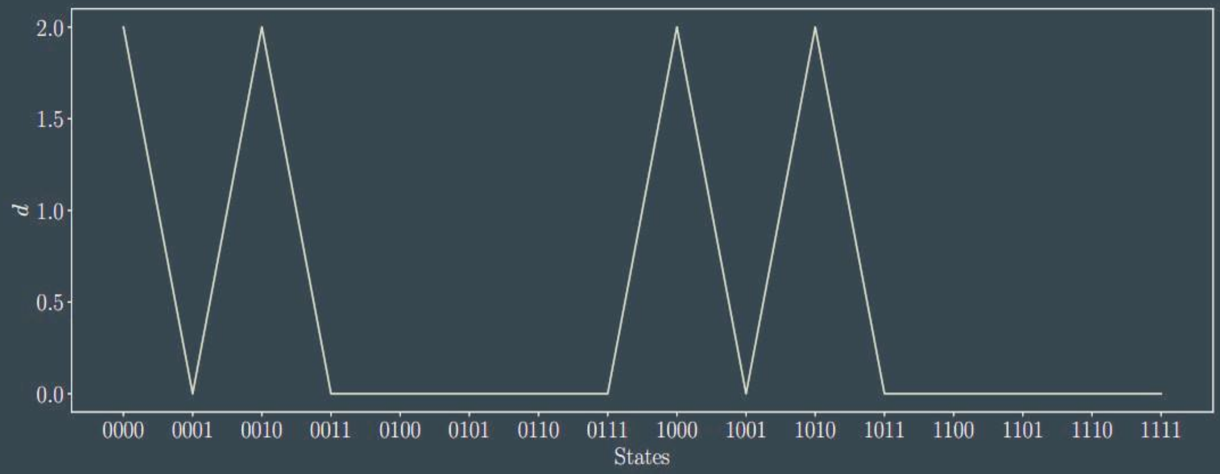




IQFT segment for N = 15

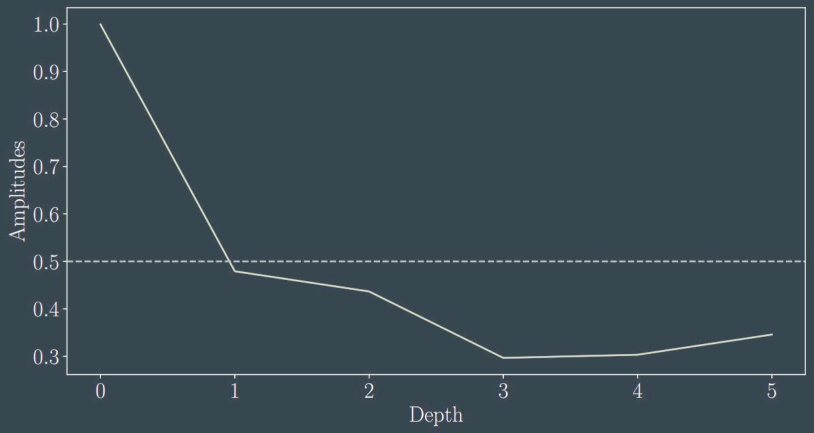
Trace distance with single error

$$d(\rho, \sigma) = \frac{1}{2} \|\rho - \sigma|_1 = \frac{1}{2} \mathrm{Tr} \left[\sqrt{(\rho - \sigma)^\dagger (\rho - \sigma)} \right]$$

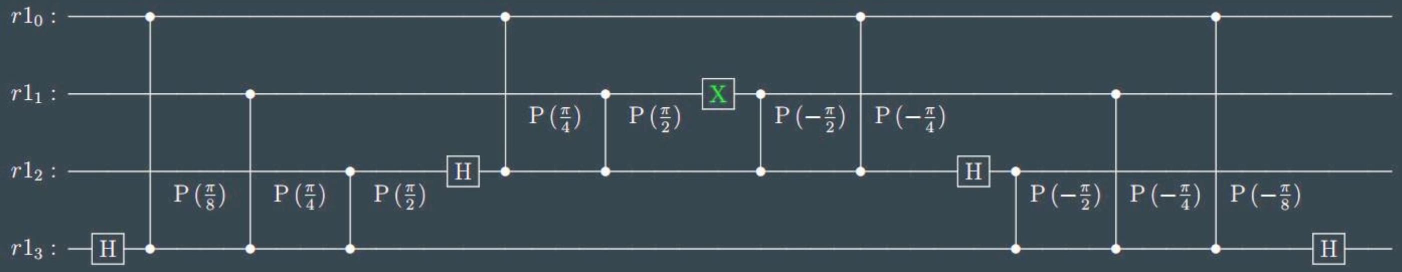


QFT with one X errors on qubit number 1

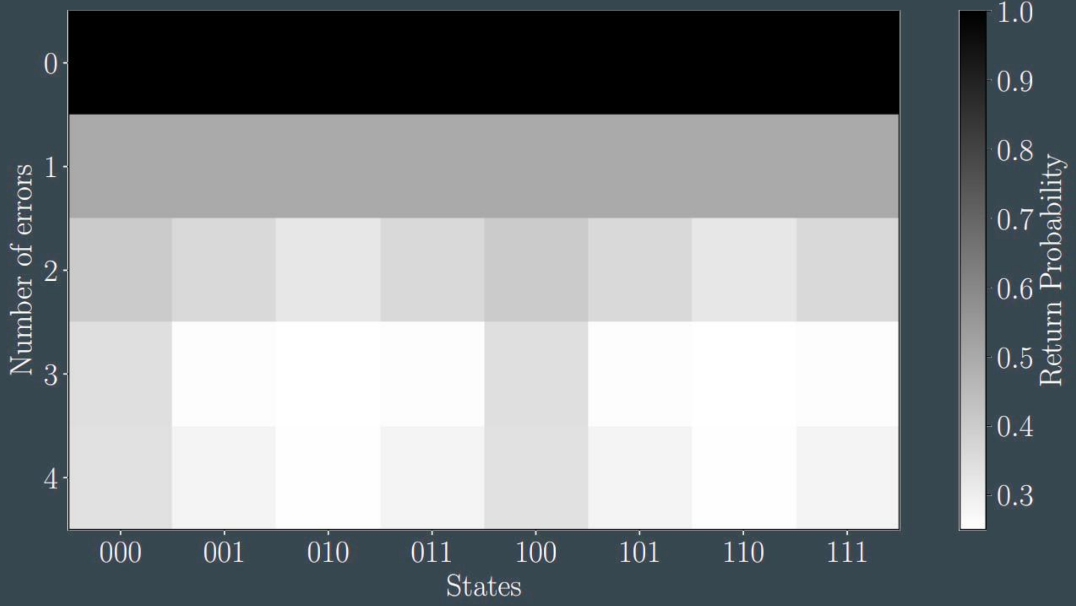
Return probabilities



$$RP = |<\psi_0|U_\varepsilon^\dagger U|\psi_0>|^2$$

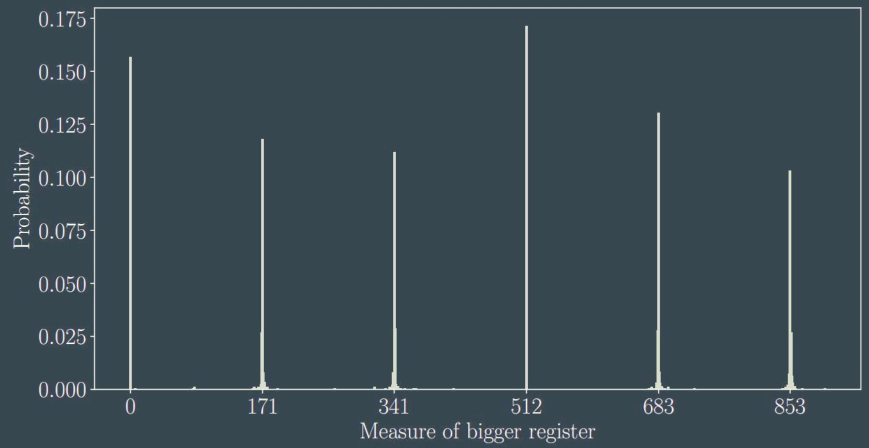


Multiple errors heatmap shows a symmetry



Degree of noise

0 errors



55 errors