Zusammenfassung Quantum Computing

Henrik Tscherny

7. September 2023

Inhaltsverzeichnis

1 Basic

1.1 QBits

- **state of a single QB**: $|s\rangle = a_0|0\rangle + a_1|1\rangle = a_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + a_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$
- **state of two QBs**: $|s\rangle = a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle$
- **basis vectors**: $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- $P(|0\rangle) = |a_0|^2$, $P(|1\rangle) = |a_1|^2$
- $\sum_{i=0}^{2^n-1} |a_n| = 1$ (for n-qubit system)
- **tensor product**: $|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ 0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$
- **entanglement**: non-serperable state (can not be written as the product of qubits, the qubits are statistical dependent)
  Example: $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

1.2 Complex Numbers

- $z = a + ib$
  $= r \cdot e^{i\varphi}$
  $= r \cdot (cos\varphi + i \cdot sin\varphi)$
  with $a, b \in \mathbb{R}$ and $i^2 = -1$
- **conjugate**: $\bar{z} = a - bi$

1.3 Matrices

- **Transpose**: $A^\top$ swap rows and cols
- **Conjugate**: A^* each entry is the conjugate
- **Adjunct**: $A^\dagger$ transpose + conjugate
- **Unitary**: $UU^\dagger = UU^{-1} = I = U^\dagger U$ adjunct is also the inverse
- Note: every unitary operator can be written as its eigenbases

2 Gates

- every gate is reversible (as gates are unitary matrices)
- **Hardamard Gate**:
  - $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
  - $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - applying H splits the probabilities in $\frac{1}{2}$ for each (simulate coinflip)
  - H is self inverse as it is unitary
  - **recursive definition for Hardamard**:
    $H^{\otimes n} = H \otimes H^{\otimes n-1} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes H^{\otimes n-1} = \frac{1}{\sqrt{2}} \begin{bmatrix} H^{\otimes n-1} & H^{\otimes n-1} \\ H^{\otimes n-1} & -H^{\otimes n-1} \end{bmatrix}$
    $H^{\otimes 1} = H$
- **Pauli Gates**:
  - **Pauli-X**: Swaps $|0\rangle$ and $|1\rangle$, $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
  - **Pauli-Y**: Swaps amplitudes, (adds phase ?), negates amplitudes of $|1\rangle$
    $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
  - **Pauli-Z**: Negates amplitudes of $|1\rangle$ $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- **CNot**:
  - negates the target if the controller is active

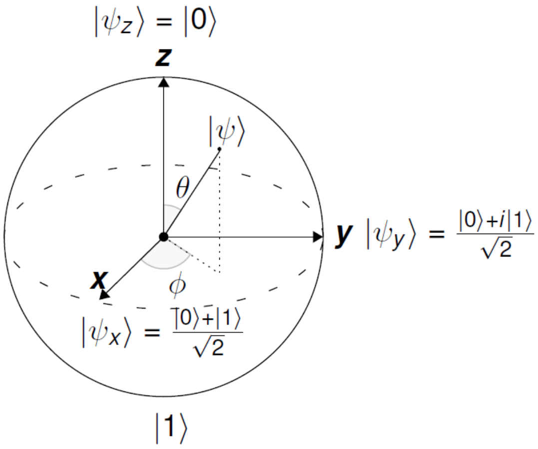
- permutation matrix
- $CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

2.1 Phase Kickback

- U: one qubit unitary gate
- $|\phi\rangle$: some base state
- applying U to $|\psi\rangle$ yields $e^{i\phi}|\psi\rangle$
- the global phase factor of a quantum state is not measurable (symmetry)
- using **ancilla** qubits the global phase can be turned intro a relative phase which is measurable

2.2 Bloch Sphere

- a Bloch Sphere can be used to visualize the state of a single qubit

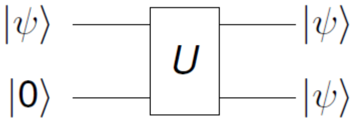


-

2.3 No-Cloning-Theorem

- it is impossible to create an identical copy of an arbitrary quantum state

- the depicted setup does not exist:

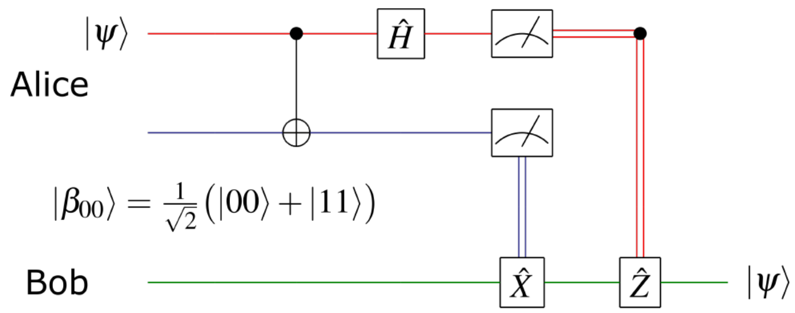


  there exists no unitary transformation that copies $|\psi\rangle$

- Proof:
  - Assume towards contradiction it is possible to clone $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
  - If $\alpha = 1, \beta = 0$ then $U|00\rangle = |00\rangle$
  - If $\alpha = 0, \beta = 1$ then $U|10\rangle = |11\rangle$
  - more general: $U(|\psi\rangle|0\rangle) = U\big((\alpha|0\rangle + \beta|1\rangle)|0\rangle\big) = \alpha|00\rangle + \beta|11\rangle$
  - however we need to obtain: $|\psi\psi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$
  - however $\alpha|00\rangle + \beta|11\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$ is not possible
  - Contradiction !

2.4 Quantum Teleportation

- not copying a quantum state but transferring it
- use quantum entanglement and classical communication
- setup:
  - A, B generate an entangled pair of qubits (Bell state) $\beta_{00} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
  - A, B separate but take their entangled bits with them
  - A create a quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ which shall be send to B
  -



- Input state: $|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\right)$
- Perform CNot: $\frac{1}{\sqrt{2}}\left(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\right)$
- Apply Hadamard: $\frac{1}{2}\left(\alpha(|0\rangle+|1\rangle)(|00\rangle+|11\rangle)+\beta(|0\rangle-|1\rangle)(|10\rangle+|01\rangle)\right)$
- A now measures the first to qubits and can infer the state of Bs bits
  - $|00\rangle \rightarrow \alpha|0\rangle + \beta|1\rangle$
  - $|01\rangle \rightarrow \alpha|1\rangle + \beta|0\rangle$
  - $|10\rangle \rightarrow \alpha|0\rangle - \beta|1\rangle$
  - $|11\rangle \rightarrow \alpha|1\rangle - \beta|0\rangle$
- depending on the outcome A gives B a classical message to manipulate Bs bits accordingly

3 Measurement

- Measurements are described by a set of operators $\{M_m\}$ with $M_m^\dagger M_m = I$ the index m refers to the possible measurement outcomes
- $P(m) = \langle\psi|M^\dagger M|\psi\rangle$
- after measurement the system is in state: $\dfrac{M_m|\psi\rangle}{\sqrt{\langle\psi|M^\dagger M|\psi\rangle}}$
- Measurement collapses the state to a basis vector with probabilities of the square of the amplitudes

3.1 Projective Measurement

- described by an **Observable** M, which is a Hermitian operator

- the possible outcomes of the measurement correspond to the eigenvalues of the observable
- getting result m when measuring $|\psi\rangle$ with probability $P(m) = \langle\psi|P_m|\psi\rangle$
- expected value: $E(M) = \sum_m m \cdot P(m)$
- given that outcome m occurred the state is now: $\frac{P_m|\psi\rangle}{\sqrt{P(m)}}$

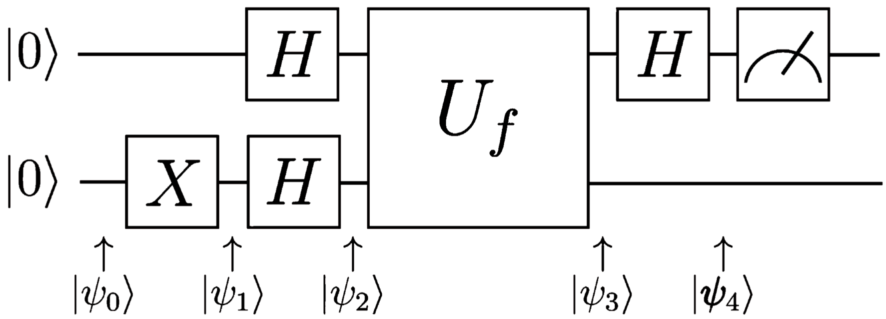
Example: Measuring in computational base

- $M_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$
- $M_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$
- Be $|\psi\rangle = a|0\rangle + b|1\rangle$
  - $P(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|P_0|\psi\rangle = \begin{bmatrix} a^* & b^* \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = |a|^2$
  - $P(1) = \langle\psi|M_1^\dagger M_1|\psi\rangle = \langle\psi|P_1|\psi\rangle = \begin{bmatrix} a^* & b^* \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = |b|^2$
- $M = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
  (measuring the computational base is like measuring the observable Pauli-Z)

4 Deutsch Algorithm

- function $f : \{0,1\} \rightarrow \{0,1\}$ that is either balanced or constant
- classical: compute f on every input
- quantum: one call of f is needed
- quantum oracle:
  - $U_f : |x\rangle|y\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle$
  - $|x\rangle$ input to function
  - $|y\rangle$ qubit to write function result to

- $|y \oplus f(x)\rangle$, the XOR ensures that the oracle is reversible (as each image has a unique preimage)
- initializing $y = |0\rangle$ we only get the function value $|x\rangle|f(x)\rangle$ as $0 \oplus x = x$
- initializing $y = |-\rangle$ we get phase kickback to $|x\rangle|-\rangle \xrightarrow{U_f} (-1)^{f(x)}|x\rangle|-\rangle$ (a phase is applied to the input qubit)
  $\begin{cases} |x\rangle|-\rangle & f(x) = 0 \\ -|x\rangle|-\rangle & f(x) = 1 \end{cases}$
- Note: this is called a phase oracle ($U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$)



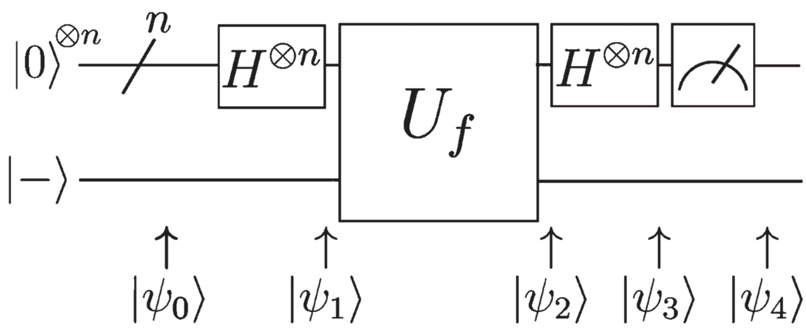
•
  - $|\psi_0\rangle = |00\rangle$
  - $|\psi_1\rangle = |01\rangle$
  - $|\psi_2\rangle = |+-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|-\rangle + |1\rangle|-\rangle)$
  - $|\psi_3\rangle = U_f \frac{1}{\sqrt{2}}(|0\rangle|-\rangle + |1\rangle|-\rangle) = \frac{1}{\sqrt{2}}(U_f|0\rangle|-\rangle + U_f|1\rangle|-\rangle) \overset{\text{phase oracle}}{=} \frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle|-\rangle + (-1)^{f(1)}|1\rangle|-\rangle)$
    ($|-\rangle$ can be omitted as its not needed)
  - case $f(0) = f(1)$: $\begin{cases} |\psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), & f(0) = f(1) = 0 \\ |\psi_3\rangle = -\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), & f(0) = f(1) = 1 \end{cases}$
    $|\psi_3\rangle = \pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \pm|+\rangle$
  - case $f(0) \neq f(1)$: $\begin{cases} |\psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), & f(0) = 0 \wedge f(1) = 1 \\ |\psi_3\rangle = -\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), & f(0) = 1 \wedge f(1) = 0 \end{cases}$

$|\psi_3\rangle = \pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \pm|-\rangle$

– $|\psi_4\rangle = \begin{cases} \pm|0\rangle, & f(0) = f(1) \\ \pm\,|1\rangle, & f(0) \neq f(1) \end{cases}$

- measuring 0 iff function is constant and 1 iff function is balanced

5 Deutsch-Jozsa Algorithm

- generalized version of Deutsch Algorithm to n qubits
- $f : \{0,1\}^n \to \{0,1\}$
- f is constant iff $\forall x, f(x) = c$
- f is balanced iff $|\{x \mid f(x) = 0\}| = |\{x \mid f(x) = 1\}|$
- classical: $2^{n-1} + 1$ function calls (input half the possible inputs)
- quantum: one call of f in needed (exponential speed up)
- 

  – $|\psi_0\rangle = |00...0\rangle|-\rangle = |0\rangle^{\otimes n}|-\rangle$ (we can get the $|-\rangle$ by $H|1\rangle$)

  – $|\psi_1\rangle = H^{\otimes n}|0\rangle^{\otimes n}|-\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|-\rangle$ (uniform distribution)

  – $|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} U_f|x\rangle|-\rangle \overset{\text{phase oracle}}{=} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle|-\rangle$ ($|-\rangle$ can be omitted)

  – Note: $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z}|z\rangle, \ (*)$

- $|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} H^{\otimes n}|x\rangle|-\rangle$
  $\overset{(*)}{=} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z}|z\rangle$
  $= \frac{1}{2^n} \sum_{x\in\{0,1\}^n} \sum_{z\in\{0,1\}^n} (-1)^{f(x)+x\cdot z}|z\rangle$
- consider the amplitude of $|0\rangle^{\otimes n}$ is $\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}$ case f constant:
  $\begin{cases} \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^0 = \frac{1}{2^n} 2^n = 1, & f(x) = 0 \\ \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^1 = \frac{1}{2^n}(-2^n) = -1, & f(x) = 1 \end{cases}$
- hence if f is constant the probability of measuring all zeros is 1
- hence if f is balanced half of the sum is 1 and half is -1 hence the probability of measuring all zeros is 0
- $\rightarrow$ measure and iff we get 000...0 then $f(x)$ is constant else balanced

6 Grovers Algorithm

- Problem: given an unstructured database, find an element $\hat{x}$ within this database
- $f : \{0,1\}^n \rightarrow \{0,1\}$ with $f(\hat{x}) = 1, f(\neg\hat{x}) = 0 \qquad (x, \hat{x} \in \{0,1\}^n)$
- classical: $\frac{N+1}{2} \in O(N)$
- quantum: $\frac{\pi}{4}\sqrt{N} \in O(\sqrt{N})$
- Steps:
  1. generate uniform distribution on all elements:
     - $H^{\otimes n}|000...0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$
     - $|s\rangle = H^{\otimes n+1}|000...0\rangle|1\rangle = |0\rangle^{\otimes n}|-\rangle$
  2. Grover Iteration:
     (a) Negate the amplitude of $\hat{x}$ (Oracle $\hat{U}_f$)
        - $\hat{U}_f|s\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} H^{\otimes n}|x\rangle|-\rangle$ (as in Deutsch-Josza)

(b) Mirror/Reflect/Diffuse all amplitudes a at the mean value m(Diffusion $\hat{D}$)

- $a := 2 \cdot m - a$
- mirroring as a quantum state: $\sum_{i=0}^{N-1} a_i |i\rangle$ $(*)$
- mean value of amplitudes: $\sum_{j=0}^{N-1} \frac{a_j}{N}$ $(**)$
- combining $(*)$ and $(**)$ we get: $|s\rangle = \sum_{i=0}^{N-1} \left(2 \cdot \sum_{j=0}^{N-1} \frac{a_j}{N} - a_i\right) |i\rangle$
- $D_N = \begin{bmatrix} -1 + \frac{2}{N} & \dots & \frac{2}{N} \\ \vdots & -1 + \frac{2}{N} & \vdots \\ \frac{2}{N} & \dots & -1 + \frac{2}{N} \end{bmatrix}$
- Note: D_N can be expressed as a local operation ($leq3$ bits involved)

3. Measure $|x\rangle$ and return it off $\hat{x} > c$ (c is some constant)

- The number of grover iterations T is capped by $(2T + 1)\frac{1}{\sqrt{N}}$ since every iteration rotates by $\frac{2}{\sqrt{N}} \Rightarrow T = \frac{\pi}{4}\sqrt{4}$
- doing more than the necessary number of iteration degrades the result

7 Simons Algorithms

Precursor to Shors algorithm

- function $f : \{0, 1\}^n \to \{0, 1\}^n$
- Goal: is the function a bijection or does f have a period s
- $\exists s \in \{0, 1\}^n, \forall x, y \in \{0, 1\}^n : f(x) = f(y) \leftrightarrow x \oplus y \in \{0^n, s\}$

1. Input Quantum Oracle $U_f : |a\rangle|b\rangle \to |a\rangle|b \oplus f(a)\rangle$
2. Initialize register R with $|a\rangle|b\rangle = |0...0\rangle|0...0\rangle$
3. bring a in uniform superposition $H^{\otimes n}|a\rangle|b\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|0...0\rangle$

4. apply U_f to R yields $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$
   Entangles Registers
5. measure $y := |b\rangle$
   - the state to measure is $\frac{1}{\sqrt{2}}(|\hat{x}\rangle + |\hat{x} \oplus s\rangle)|f(\hat{x}\rangle$
   - if f is a bijection then we get $f^{-1}(y)$
   - if f is periodical there are two preimages (x, x') of y with $x \oplus x' = s$
6. apply Hadamard to $|a\rangle$: $H^{\otimes n}|a\rangle$
   - state: $\frac{1}{\sqrt{2}} \sum_{z \in \{0,1\}^n} \frac{1}{\sqrt{2}} \left((-1)^{\hat{x} \cdot z} + (-1)^{(\hat{x} \oplus s) \cdot z}\right) |z\rangle |\hat{x}\rangle$
   - amplitudes: $a_z = \frac{1}{\sqrt{2^{n+1}}} \left((-1)^{\hat{x} \cdot z} + (-1)^{(\hat{x} \oplus s) \cdot z}\right)$
   - $z \cdot s$ is even then $a_z = \pm \frac{1}{\sqrt{2^{n+1}}}$
   - $z \cdot s$ is odd: $a_z = 0$
7. measure $z := |a\rangle$
8. return z

- since we square we only get values of z that are even
- those are half of the possible values (the rest is odd) (2^{n-1} many)
- $n-1$ of them are linearly independent and define a lin. sys. of equations ($z_1 \cdot t = 0, z_2 \cdot t = 0, ..., z_{n-1} \cdot t = 0$
- if $f(0) = f(s)$ return periodic, else bijective

8 Shors Algorithm

Goal: Find prime factor $z \cdot r = n$ for some $n \in \mathbb{N}$ that is not a prime power

1. Make a random guess $a \in \{2, ..., n-1\}$
2. calculate $z := gcd(a, n)$ and return z if $z \neq 1$
   (the guess was very lucky and a prime factor was guessed, other factor is $\frac{n}{z}$)
3. calculate the period of a in $(\mathbb{Z}/n\mathbb{Z})^{\times}$: $a^p \equiv 1 \mod n$ (**Quantum**)
   (Ordnung von a innerhalb der primen Restklassengruppe)

   - choose q with $n^2 \leq q < 2n^2$

- initialize input quantumregister with: $\frac{1}{\sqrt{q}}\sum_{p=0}^{q-1}|p\rangle|0\rangle$
  (superposition of all possible periods)
- initialize output quantumregister with: $\frac{1}{\sqrt{q}}\sum_{p=0}^{q-1}|p\rangle|a^p \mod n\rangle$
  (superposition of the remainders of the calculation $a^p \mod n$)
- Example $q = 16, a = 7$:
  $\frac{1}{4}(|0\rangle|1\rangle) + |2\rangle|4\rangle + |3\rangle|13\rangle +$
  $|4\rangle|1\rangle + |5\rangle|1\rangle) + |6\rangle|4\rangle + |7\rangle|13\rangle +$
  $|8\rangle|1\rangle + |9\rangle|1\rangle) + |10\rangle|4\rangle + |11\rangle|13\rangle +$
  $|12\rangle|1\rangle + |13\rangle|1\rangle) + |14\rangle|4\rangle + |15\rangle|13\rangle)$
  (Clearly the period $p = 4$ with $(1, 7, 4, 13)$
- measuring the output/reminder register yields a superposition of all elements with the same reminder (uniformly random which exactly)
  Example: $\frac{1}{2}(|1\rangle + |5\rangle + |9\rangle + |13\rangle)|7\rangle$ (all elements with reminder 7)
- apply QFT_n to input register to get the period p
  Example: $\frac{1}{2}(|0\rangle + |4\rangle + |8\rangle + |12\rangle)$
  (amplitudes for each element may have changed sign/phase)
- measuring the input register yields $\{\frac{j \cdot n}{p} | j = 0, ..., 3\}$
  Example:$\{0, 4, 8, 12\}$
- calculate p using $\frac{j}{p} = \frac{y}{n}$ (y...output measurement)
  (only works if j and p have no common divisors hence measuring 0 or 8 in the Example necessitates a new run as the state is now destroyed)

4. GoTo (1) if: p is odd (we cannot calculate $\frac{p}{2} \in \mathbb{N}$)

5. calculate $z := gcd(a^{\frac{p}{2}} - 1, n)$

   - return z if $z \neq 1$ as its a factor of n

6. calculate $z := gcd(a^{\frac{p}{2}} + 1, n)$

   - if $z = n$ Goto (1), as we have a multiple of n
   - else return z

- $(a^{\frac{p}{2}} - 1) \cdot (a^{\frac{p}{2}} + 1) = a^p - 1 = k \cdot n$
- hence either the first or the second term must have a common divisor with n

Note: applying QFT to $|0\rangle$ yields a uniform superposition as a Hadamard-transformation

8.1 RSA

- asymetric encryption
- key generation:
  1. choose $p, q \in \mathbb{P}$ at random
  2. calculate $n = p \cdot q$ (this is the modulus for the public/private key)
  3. compute $\varphi(n) = (p-1)(q-1)$ (number of coprime integers)
  4. choose e s.t. $1 < e < \varphi(n)$ and e and $\varphi(n)$ are coprime (e: encryption exponent)
  5. calculate $e \cdot d \equiv 1 (mod\, \varphi(n))$ (d: decryption exponent) (calculation by adv. eucl. alg.)
  6. keys are:
     - Public: (e, n)
     - Private: (d, n)

9 Adiabatic Quantum Computing

- **Hermitian Matrix**: conjugate transpose is self inverse ($A^\dagger = A$)
- alternative approach to quantum computing based on **time evolution** of quantum states
- time evolution is described by **Schrödingers equation** ($i\hbar \frac{\partial |\psi(t)\rangle}{\partial t} = \mathscr{H})|\psi(t)\rangle$)
- $|\psi(t)\rangle = \sum_{j=1}^{n} \alpha_j e^{-i\lambda_j t/\hbar} |\phi_j\rangle$
  (j: energy level, $|\phi_j\rangle$: energy state of j-th level, λ_j: energy of j-th level)
- **Adiabatic Theorem**: a systems energy state does not change under adiabatic change of the Hamiltonian over time
- $T \propto \frac{1}{(\min_t \Delta\lambda_t)^2}$
- update equation: $\mathscr{H}_t = \left(1 - \frac{t}{T}\right)\mathscr{H}_{init} + \frac{t}{T}\mathscr{H}_{final}$
- basic ideal: Morphing a initial Hamiltonian gradually into a final one without changing the energy states of the system

-

$\mathcal{H}_{init}$ Eigen Vector	Initial Energy		Final Energy	$\mathcal{H}_{final}$ Eigen Vector
$\|00\rangle$	1		-1	$\frac{\|00\rangle+\|01\rangle+\|10\rangle+\|11\rangle}{2}$
$\|01\rangle$	2	Adiabatic Process $\longrightarrow$	0	$\frac{\|00\rangle-\|01\rangle+\|10\rangle-\|11\rangle}{2}$
$\|10\rangle$	3		1	$\frac{\|00\rangle+\|01\rangle-\|10\rangle-\|11\rangle}{2}$
$\|11\rangle$	4		2	$\frac{\|00\rangle-\|01\rangle-\|10\rangle+\|11\rangle}{2}$

- **Quantum Annealing** accelerates the transition by ignoring the adiabatic theorem
-

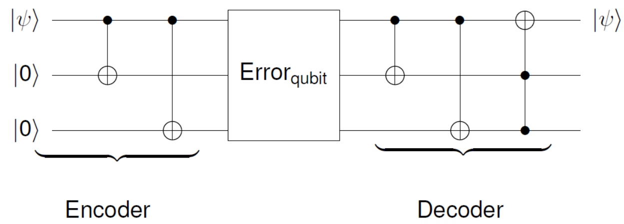
10 Error Correction

- qubits cannot be completely shielded from the environment, hence they interact with it
- quantum computers are considered open systems
- the environment is denoted as $|e\rangle$ which is usually quite complex
- types of errors that can occur are:
  - no error: $I\ :\ \alpha|0\rangle + \beta|1\rangle$
  - phase flip: $Z\ :\ \alpha|0\rangle - \beta|1\rangle$
  - bit flip:: $X\ :\ \alpha|1\rangle + \beta|0\rangle$
  - both: $X \cdot Z\ :\ \alpha|1\rangle - \beta|0\rangle$
- all possible errors in a system can be reduced to a combination of those errors
- Idea: use redundancy for error correction ($0 \to 000, 1 \to 111$)
- **Bit correction**:
  - σ_x-error
  - $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \to \alpha|000\rangle + \beta|111\rangle$
  - through the use of two CNot gates the error can be located an fixed using Pauli gates

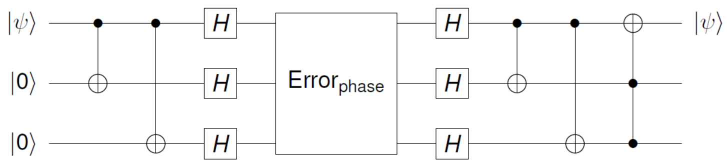
– possible errors and fixes:

Error location	$\lvert\psi^{\text{encoded}}\rangle$	$\lvert\psi^{\text{decoded}}\rangle$	M.o.	Operator on 1st qubit
no-error	$\alpha\lvert000\rangle+\beta\lvert111\rangle$	$\alpha\lvert000\rangle+\beta\lvert100\rangle$	$\lvert00\rangle$	None
1*st* qubit	$\alpha\lvert100\rangle+\beta\lvert011\rangle$	$\alpha\lvert111\rangle+\beta\lvert011\rangle$	$\lvert11\rangle$	$\hat{X}$ on 1*st* qubit
2*nd* qubit	$\alpha\lvert010\rangle+\beta\lvert101\rangle$	$\alpha\lvert010\rangle+\beta\lvert110\rangle$	$\lvert10\rangle$	None
3*rd* qubit	$\alpha\lvert001\rangle+\beta\lvert110\rangle$	$\alpha\lvert001\rangle+\beta\lvert101\rangle$	$\lvert01\rangle$	None

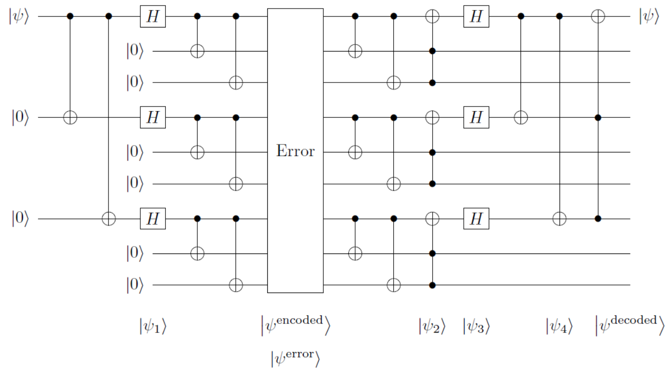
– the encoding works using CNot gates, the decoding uses CNots and a Tofoli Gate:



- **Phase correction**:
  - σ_z-error
  - Similar approach as bit correction but change to sign base first
  - $\lvert0\rangle \rightarrow \lvert+++\rangle = \frac{\lvert000\rangle+\lvert111\rangle}{\sqrt{2}}, \lvert1\rangle \rightarrow \lvert---\rangle = \frac{\lvert000\rangle-\lvert111\rangle}{\sqrt{2}}$
  - perform encode/decode using Hardamard gates
  - circuit for phase correction:



- both corrections can be combined into one (**Shors 9-Qubit Code**)
  - both encodings for phase and bit flips are applied
  - $\lvert0\rangle \rightarrow \frac{(\lvert000\rangle+\lvert111\rangle)(\lvert000\rangle+\lvert111\rangle)(\lvert000\rangle+\lvert111\rangle)}{\sqrt{8}} = \lvert0_L\rangle$
  - $\lvert1\rangle \rightarrow \frac{(\lvert000\rangle-\lvert111\rangle)(\lvert000\rangle-\lvert111\rangle)(\lvert000\rangle-\lvert111\rangle)}{\sqrt{8}} = \lvert1_L\rangle$
  - circuit for the 9-qubit shor code:



11 Quantum Complexity Theory

- **P**: Deterministic Polynomial Time
- **NP**: Non-deterministic Polynomial Time
  - $L \in NP$: solution can be verified in polynomial time by a DTM
  - L is NP-hard: $\forall \bar{L} \in NP : \bar{L} \leq_p L$ (all problems in NP can be reduced to L)
  - NPC: $L \in NP$ and L is NP-hard (those are the hardest problems in NP (only polynomial time differences))
- **RP**: Randomized Polynomial
  - : $P = 1$ if $w \notin L$
  - $P > 0.5$ if $w \in L$
  - runtime is P
- **BPP**: Bounded Error Probabilistic Polynomial
  - $P \geq 0.75$ if $w \in L$
  - $P \geq 0.75$ if $w \notin L$
  - runtime is P
- **PSPACE**: Deterministic Polynomial Space
- **EXP**: Deterministic Exponential Time
- **IP**: Interactive Polynomial Time
  - V: Verifier, $V(w, r, m_1...m_i) = m_{i+1} : \Gamma^* \times \Gamma^* \times \Gamma^* \rightarrow \Gamma^* \cup \{\text{accept}, \text{reject}\}$

- P: Prover, has unlimited computational power, $P(w, m_1 ... m_i) = m_{i+1} : \Gamma^* \times \Gamma^* \to \Gamma^*$
- V and P interact, $(V(w, r) \leftrightarrow P(w))(w, r) =$ accept if exists a message sequence that accepts
- $w \in L \to Pr(V \leftrightarrow P$ accetps $w) \geq 2/3$
- $w \notin L \to Pr(V \leftrightarrow \bar{P}$ accetps $w) \leq 1/3$

- **QIP**: Quantum Interactive Polynomial Time
- **MA**: Merlin-Arthur
  - like IP but only message, message length is poly and poly many random bits
- **QMA**: Quantum Merlin-Arthur

11.1 Relations between Classes

$$P \subseteq RP \subseteq \left\{ \begin{matrix} NP \subseteq MA \\ \rotatebox{45}{$\subsetneq$} \\ BPP \subseteq BQP \end{matrix} \right\} \subseteq QMA \subseteq \left\{ \begin{matrix} PSPACE \\ = \\ IP \\ = \\ QIP \end{matrix} \right\} \subseteq EXP \subseteq R \subsetneq \left\{ \begin{matrix} RE \\ = \\ MIP^* \end{matrix} \right\} \subsetneq ALL$$

12 Quantum Cryptography

12.1 BB84 Protocol

1. A, B want to communicate securely
2. A generates random bits and random bases
3. A measures each bit in its randomly assigned base and remembers measurement and initialization
4. A send the measurements to B
5. B guesses that bases man measures the received qubits
6. B remembers measurement
7. A, B publish measurement bases

8. A, B use measurement where to bases agree to forge a secret key
9. A, B convert + to 0 and - to 1
10. an eavesdropper will be detected when A, B compare their keys