Basic Principles of Quantum Error-Correction

webpage see: www.markus-grassl.de

1. Abstract Model of Quantum Computation

1.1 Outline of a quantum algorithm

a) Preparation of a fix pure initial state

$$|\psi_0\rangle \in \mathcal{H} \cong \mathbb{C}^d$$

b) sequence of unitary operations on $\mathcal{H}$

$U_1, \ldots, U_T$

$$|\psi_t\rangle = U_t\,|\psi_{t-1}\rangle \qquad 1 \leq t \leq T$$

$$|\psi_T\rangle = U_T \cdot U_{T-1} \cdot \ldots U_1\,|\psi_0\rangle$$

c) measurement of the final state $|\psi_T\rangle$ with respect to a fixed basis

1.2 Quantum registers

The state space of a quantum computer is a Hilbert space which is the tensor product of quantum registers

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_m$$

let $\mathcal{B}_i = \{ |b_j^{(i)}\rangle : j = 1, .., d_i \}$ where

$$d_i = \dim \mathcal{H}_i$$

$$|\psi\rangle = \sum_{j_1,\ldots,j_m} \alpha_{j_1,\ldots,j_m} |b_{j_1}^{(1)}\rangle |b_{j_2}^{(2)}\rangle \ldots |b_{j_m}^{(m)}\rangle$$

The decomposition into subsystems should be compatible with the operations we can perform on our system resp. the "physical decomposition" of the system.

mainly: n-qubit q-computer:

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

The basis states are labelled by binary strings of length n. "computational basis"

1.3 Elementary Quantum Operations

An elementary quantum operation is a unitary operation or projective measurement that operates on a bounded number of quantum registers, each of which has bounded dimension.

Remark: In particular, we may consider n-qubit q-computers and two-qubit operations.

Allowing operations on k qubits for fixed ~~set~~ number of registers k only yields a speed-up by a constant factor.

But it is (in computer science) not allowed to use gates / operations that operate on an unbounded number of registers.

1.4 LOOP / WHILE - Programs

If a program contains only FOR - LOOPS, its termination is guaranteed, but one cannot compute all functions.
So a "universal program" must have some WHILE - LOOPS (branching and repetition)
Then one cannot decide, looking only at the program, whether the computation terminates.
The HALTING proplem is undecible!

1.5 Hybrid Quantum Algorithms

A hybrid q-algorithm consists of the following steps (in arbitrary order):

- unitary operations on a bounded, (fixed) number of registers
- adding a bounded number of additional registers in a fixed state "adding blank qubits" $|0\rangle \ldots |0\rangle$

- measuring some registers with respect to a fixed basis, yielding a classical (bit-) string y

state after the measurement

$$|\psi'\rangle = |\varphi(y)\rangle \otimes |y\rangle$$

quantum state depending on y

classical information y

$\Longrightarrow$ Use the classical information y to determine how to proceed, in particular, whether to terminate the computation or not.

$\Longrightarrow$ This type of quantum algorithm can be seen as classical algorithms using quantum subroutines with a fixed number of steps (which, of course, might depend on the status of the classical program).
For this, we have to postpone all intermediate measurements to the end of each quantum subroutine.

1.6 Conditional quantum operations

Consider w.l.o.g. two registers, i.e. $\mathcal{H} = \mathbb{C}_1^{n_1} \otimes \mathbb{C}_2^{n_2}$

Let the eigenstates of a measurement on the second register be $\mathcal{B}_2 = \{ |0\rangle_2, \ldots, |n_2-1\rangle_2 \}$.

The operations on the first register depend on the measurement result, given by the label j:

$$U : \{0, 1, \ldots, n-1\} \to \mathcal{U}(\mathbb{C}^{n_1})$$
$$j \mapsto U_j$$

Define

$$U^{(12)} := \sum_{j=0}^{n_2-1} U_j \otimes |j\rangle\langle j|$$

$$= \begin{bmatrix} \boxed{U_0} & & & 0 \\ & \boxed{U_1} & & \\ & & \ddots & \\ 0 & & & U_{n_2-1} \end{bmatrix} \quad \text{block diagonal}$$

$U^{(12)}$ commutes with the measurement w.r.t $\mathcal{B}_2$.

$\Longrightarrow$ move all measurements to the end of the quantum subroutine.

2. Classical Channel Models

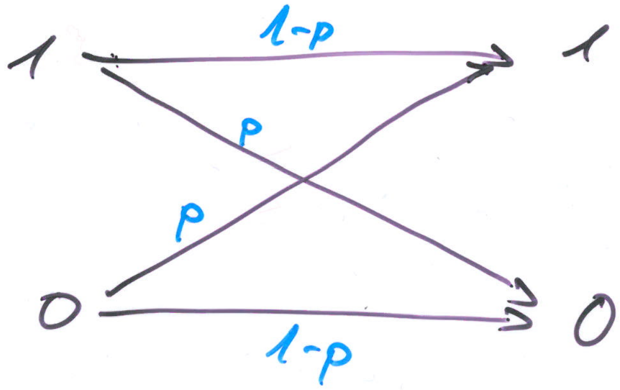
(brief overview)

2.1 binary symmetric channel (BSC)

input: $x \in \{0, 1\}$

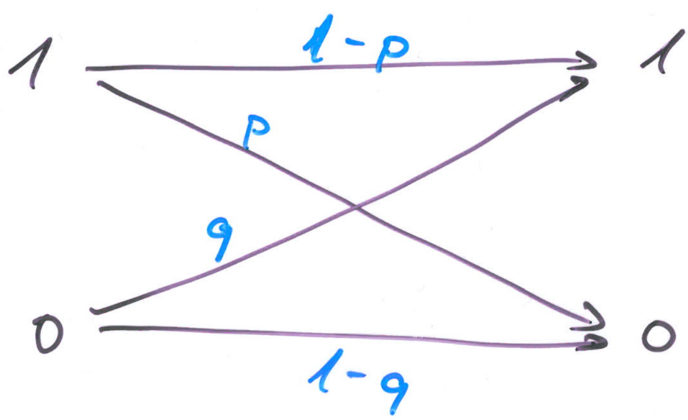
output: $y \in \{0, 1\}$

transition probabilities:

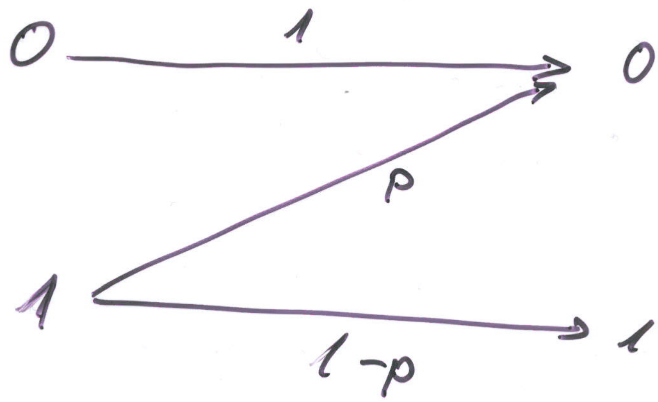


with prob. p the input ~~[illegible]~~ bit x is flipped

generalization: (channel without memory)



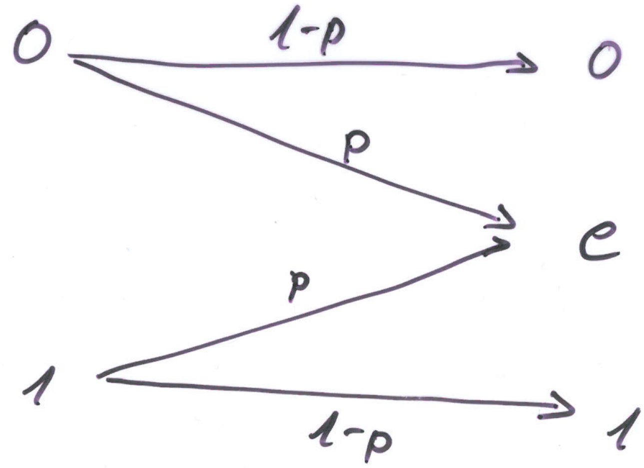
extremal case: Z-channel



the input 0 is transmitted reliably
the input 1 is flipped with probability p

If the output is $y=1$, then we know with certainty that the input was $x=1$

2.2 Binary Erasure Channel (BEC)

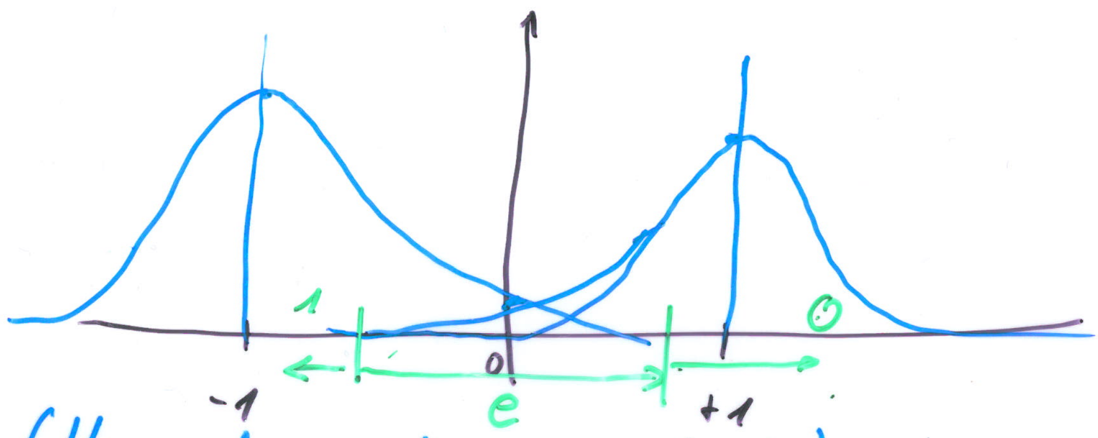


If the output is the symbol e, we know that an error occurred; otherwise, there was no error.

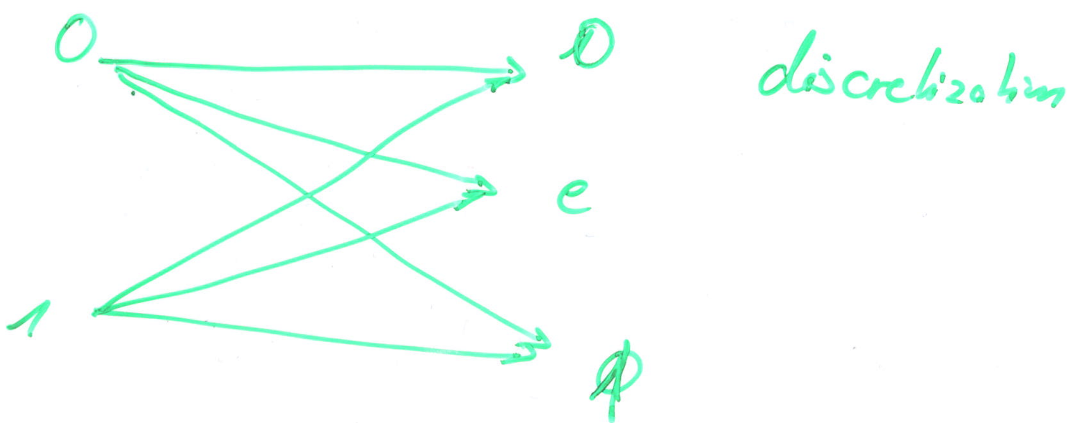
2.3 Additive White Gaussian Noise (AWGN) Channel

input: finite set of real values, e.g.
$\{-1, +1\}$

channel adds some noise with a Gaussian distribution



(this should be symmetric!)



Or: use reliability information of the discretized values