Formal Methods for Concurrency in Quantum-Based Systems

Kirstin Peters

June 29, 2023
OPCT @ Bertinoro

classical bit

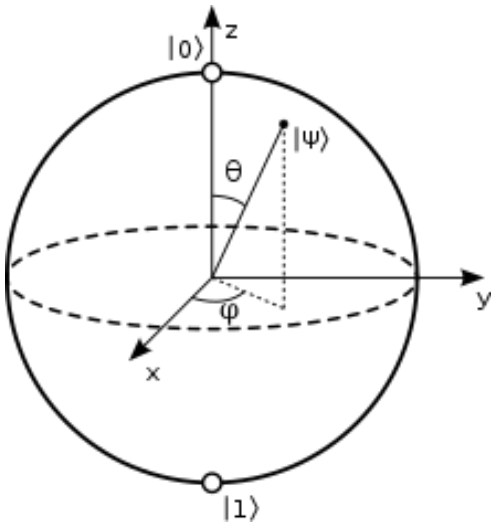
b

where $b \in \{0, 1\}$

quantum bit (qubit)

q

where q is a two-state quantum-mechanical system



Bloch Sphere

superposition: q can be in both states $|0\rangle$ and $|1\rangle$ simultaneously

pure state: state $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ is a point on the surface

mixed state: state can be a point *inside* the Bloch sphere due to **entanglement** with another qubit

Operations on Qubits

- **unitary transformations**: preserve pure states
  - Pauli matrices:

$$\mathsf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \mathsf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \mathsf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \mathsf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

    e.g. $\mathsf{X}(\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle$

  - Hadamard $\mathsf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
  - controlled not CNOT : $|a\rangle|b\rangle \mapsto |a\rangle|a \oplus b\rangle$
    leads to **entangled** states such as the bell pair $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
- **super operators**:
  - also contains non-unitary transformations,
    i.e., transformations that result in a mixed state
  - are used e.g. to model noise
- **measurement**: e.g. in $\alpha|0\rangle + \beta|1\rangle$ we measure 0 with probability α^2

- because of entanglement, the quantum register is usually modelled as a separate register, i.e., the state is not part of the process
- configuration $\langle P, \rho \rangle$,
  where P is a process and ρ is the current state of the register

It is impossible to determine the exact state of an arbitrary qubit.

The No-Cloning Principle:

It is impossible to copy the exact state of a qubit.

- this has some practical consequences:
  - after transmitting a qubit,
    this qubit is no longer available for the sender
  - processes at different locations cannot have access to the same qubit
  - getting the exact state is impossible,
    but also approximating it is difficult
    - measurement destroys superposition
    - copying is not possible
    - we have to generate the state several times
      in order to approximate the amplitudes

Problem

There is no classical way to transmit the state of a qubit.

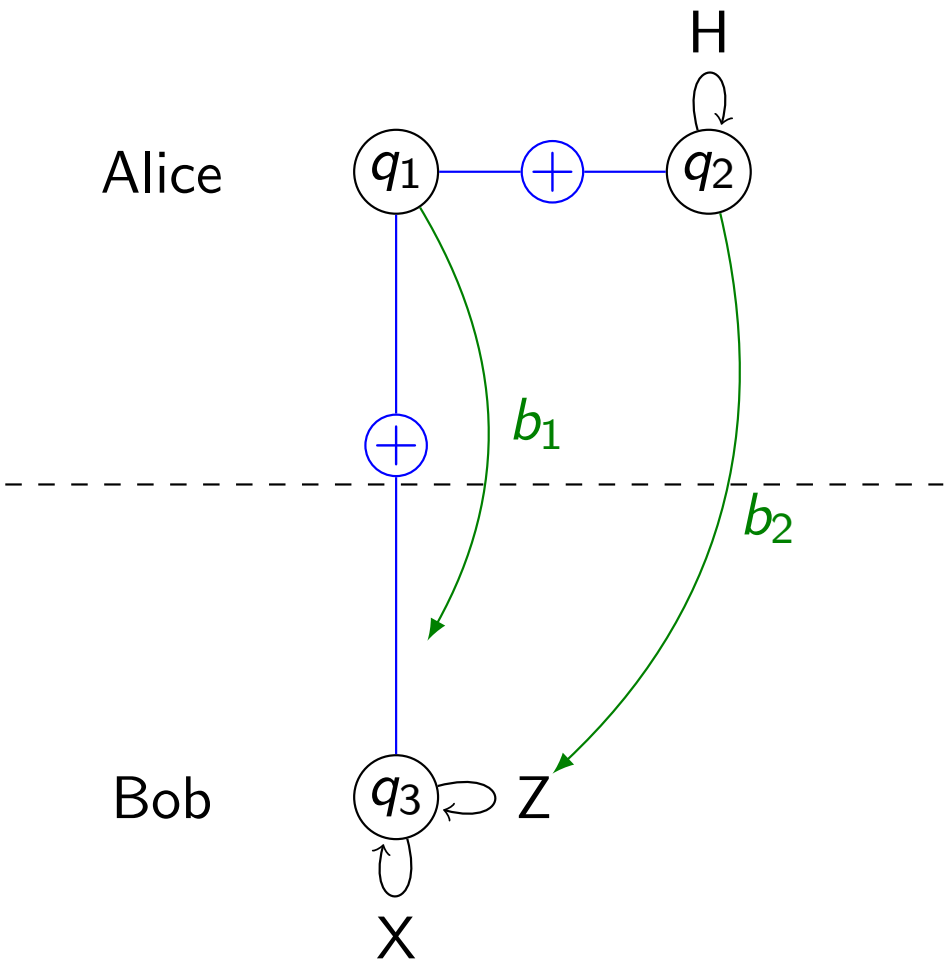
Quantum Teleportation

is the transfer of *quantum information* to a distant location.

requires:

- an entangled pair of qubits
- a channel for classical information between the locations

- the sender does not need to know the state of the qubit
  - following the intuition that it is impossible to determine the exact state of a qubit
- the qubit of the sender is destroyed in the process
  - following the non-cloning principle

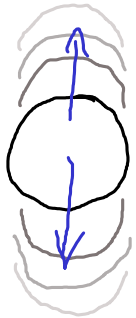


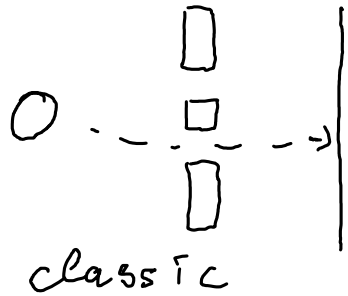
0. Alice and Bob share an entangled pair of qubits q_1, q_3 qubit q_2 should be teleported q_2 is in state $|\psi\rangle$
1. Alice entangles q_1 and q_2 (by applying CNOT)
2. Alice applies H on q_2
3. Alice measures q_1 and q_2 and sends the results b_1, b_2 to Bob
4. if $b_1 = 1$, Bob applies X on q_3
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
5. if $b_2 = 1$, Bob applies Z on q_3
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
6. q_3 is in state $|\psi\rangle$

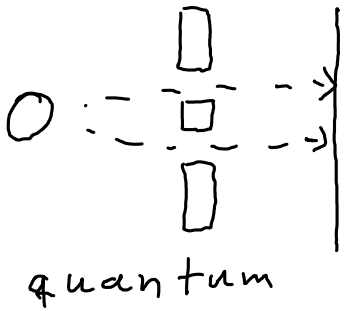
Magic in Quantum-Based Systems

There are two behaviours of qubits that are magical,
i.e., that cannot easily be explained by behaviours of classical systems.

- **Superposition**
- **Entanglement**







- one way to allow a qubit to take the states $|0\rangle$ and $|1\rangle$ is to use spinning of an electron
- e.g. up for $|0\rangle$ and down for $|1\rangle$
- **Superposition:** an electron can be prepared to spin up and down at the same time
- illustrated by the double-slit experiment
- the behaviour of the qubit in superposition can**not** be expressed with a single bit
- and also **not** with a bit and probabilities
- its behaviour is described by the linear combination of two states

Superposition allows to speed up computations.

- superposition is a very interesting and powerful feature
- but its main practical applications concern computations
- accordingly it is not obvious, whether this is relevant for concurrency
- entanglement is obviously relevant for concurrency

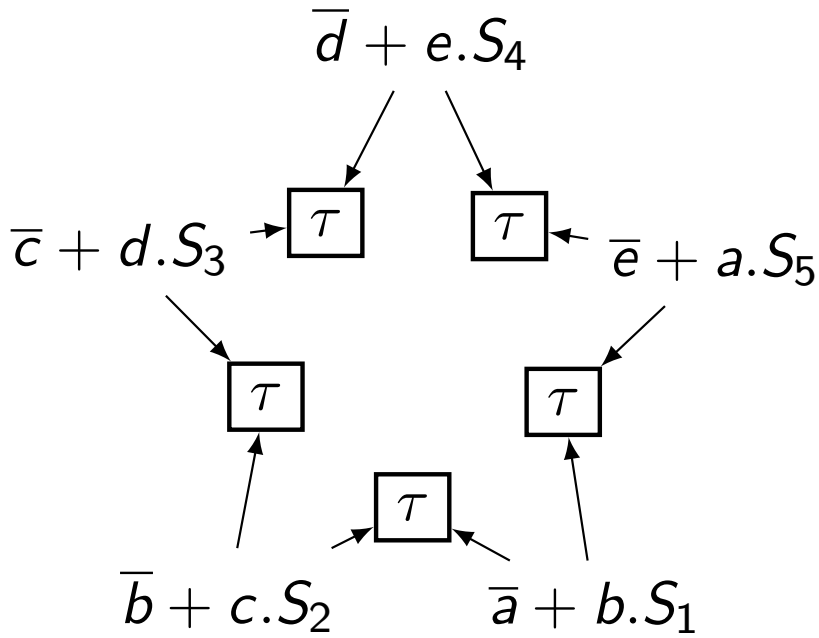
- the states of two qubits can be entangled
- entangled states are to *some extend* dependent on each other
- e.g. Bell-States (fully entangled states of e.g. two qubits)
  - two fully entangled qubits in state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
  - measuring any of the two qubits will return 0 or 1 with equal probability
  - but measuring both (regardless of the timing or order) will return exactly the same value
- there are also partial entanglements
- entanglements can be intentional (e.g. by CNOT) or accidental (e.g. due to noise)

Entanglement is very relevant for concurrency theory, because distributed components may influence each other without any kind of interaction.

- one **fundamental** result of concurrency theory is that
  the problem of leader election distinguishes synchronous from asynchronous distributed systems
- proved e.g. for the π-calculus by C. Palamidessi in *Comparing the expressive power of the synchronous and the asynchronous π-calculus* at POPL'97
- but distributed quantum-based systems can solve leader election (in a fully symmetric way) without any interaction
  - assume 8 processes to decide a number in $\{0, \ldots, 7\}$
  - give every process i 3 qubits $1 \leq j \leq 3$
  - such that all qubits $q_{i,j}$ with the same j are entangled
  - let all processes measure their qubits
  - elected value is the number $x_1x_2x_3$ resulting from measurement

Leader election does no longer distinguishes synchronous and asynchronous distributed systems in the case of quantum-based systems.

- we generalised leader election to $\star$s
- a $\star$ is a state in an LTS requiring certain kind of steps
- some of these steps need to be in conflict to each other and other steps need to be *distributable*
- *distributable* steps are steps of distributed parts without interaction between these parts
- in classical systems distributable steps are completely independent



In quantum-based systems distributable steps might influence other parts.
Can capture the effect of such an influence?
What results of concurrency theory have to be adapted and how?