# *Quantum Computer*

*Prof. M.R.Asharif*

*2014, Oct. 6*

*Department of Information Engineering*

*University of the Ryukyus*

# Quantum Computer

- **A quantum computer is a computation system that makes direct use of quantum-mechanical phenomena**

# Quantum computer

- Quantum computers are different from digital computers based on transistors each of which is always in one of two definite states (0 or 1).
- quantum computation uses qubits (quantum bits), which can be in superpositions of states.
- Quantum computers share theoretical similarities with non-deterministic and probabilistic computers;

# Quantum computer

- One example is the ability to be in more than one state simultaneously.
- As of 2014 quantum computing is still in its infancy but experiments have been carried out in which quantum computational operations were executed on a very small number of qubits.
- Both practical and theoretical research continues

# Quantum computer

- Large-scale quantum computers will be able to solve certain problems much quicker than any classical computer (one year computational time shrinks to only few minutes).
- A classical computer has a memory made up of bits.
- A quantum computer maintains a sequence of qubits. A single qubit can represent a one, a zero, or any quantum superposition of these two qubit states; moreover, a pair of qubits can be in any quantum superposition of 4 states (00,01,10,11).

# Quantum computer

- Three qubits in any superposition of 8.
- In general, a quantum computer with *n* qubits can be in an arbitrary superposition of up to *2^n* different states simultaneously.
- a normal computer that can only be in *one* of these *2^n* states at any one time.
- **Bits vs. qubits……quantum computing**
- **http://en.wikipedia.org/wiki/Quantum_computer**

# Quantum computer

- Shor's Algorithm: $|x,f(x)>$
- Where $x=0,1,2,\ldots$ & $f(x)=\cos(\pi x)+1$
- For example: $x=5$, then $f(x)=0$
- In binary from: $|101,000>$

# Reversible Logic Gates

- When discussing logic gates, “reversible” means that the unknown values of the inputs can be reconstructed from the known outputs.
- For example, a single-bit inverter (N-gate) is reversible.
- Reversibility is an important requirement for quantum computing

# Control-Not Gate

The CN-gate uses 2 inputs. The control bit's value is unchanged by the gate's operation. However, it's value is used to conditionally change the target bit's value.

*af=ai ,*

*bf={bi , if ai=0 ; <u>bi</u> , if ai=1}*

$$bf = ai \oplus bi$$

*If we know the output af, bf then we can find the input ai, bi*

# Control-Not Gate

| ai | bi | af | bf |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 |

# Control-Control-Not Gate

- The CCN-gate uses 3 inputs.
- Two control bits are unchanged.
- The target bit is inverted only if both ai = bi= 1.
- $af=ai\ ,bf=bi$
- $cf=\underline{ci}$ , *if* $ai=bi=1$
- $cf=ci$ , *otherwise*
- $cf=aibi \oplus ci$

# Fredkin-Gate

- The F-gate is a 3-bit reversible gate, also known as the Control-Exchange-gate.
- The control bit *ai* causes the target bits *bi* and *ci* to exchange their values if *ai =1*.
- *af=ai*
- (*bf,cf )=(bi,ci) if ai=0*
- (*bf,cf )=*(*ci,bi) if ai=1*

# Fredkin-Gate

| ai | bi | ci | af | bf | cf |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 1 | 0 |
| 1 | 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 |

The Fredkin gate is universal and capable of achieving any operation,including the AND gate.

***Thank you***