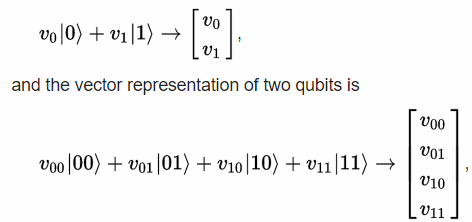
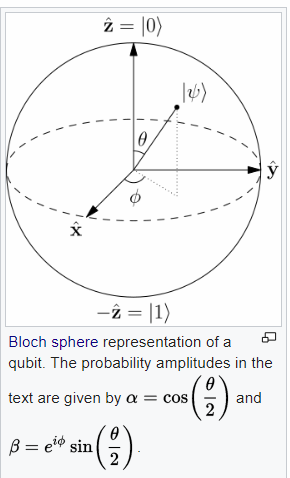
Bra ket, also called dirac notation is convenient notation used, to represent Qubit state,

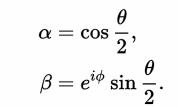


**Example:** 1/sqrt2 \* a\*|0> b\*|1> ; plane for real a,b on blackboard, add that a,b could be complex, so we couldn’t show every state on simple plane. For this reason, we could illustrate quntum state of qubit on bloh sphere.



Have to follow this formula:





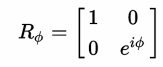
Photon could represent qubit, **example:** bloh sphere with linear polarity as theta. circular as phi. by linear and circular polarization. referred as elliptical polarization.

qbit state/ base vector, measurement probability / bloch sphere/superpozycja entanglement state

outer product

Gates:

NOT (pauli x gate) , **example**

Controled rotation gate. **Example:**  it adds angle phi to base vector one.

Hadamard gate here is special cases that are worth to mention 0> = 0>+1>/sqrt2 , 1> = 0> - 1>/sqrt2, H(H)

preservationn inner product, reversible

We couldn’t use any kind of matrix, because quantum rules limited us that transformation have to preserve norm. so the matrices which we are using, are unitary matrices which could be used to represent realizable transformation.

The matrices looks quiet easy, but of course not every simple matrix could be implemented as quantum gate. It should preserve norm, it is just a simple quantum rule Unitary matrices meet the requirement.

Here is definition: U is an unitary matrix if: UU\* = U\*U = I. I will explain it. Hermitian conjugate identity matrix.

It could be proved that linear transformation U full fill norm preservation requirement.

**example:** two unitary transform is also unitary transform - H\*(CRG\*(CRG(H))

There is also another quantum rule, it is no cloning theorem, which states that it is impossible to create an identical copy of an arbitrary unknown [quantum state](https://en.wikipedia.org/wiki/Quantum_state).

Uncomputing…?

Grover search:

Here is Grover database search algorithm

**Example:** quantum bits and quantum secrets

Grover diffusion operator. 2 |s><s| - I |s><s| is outer product

Uw operator, simple proof:

<https://en.wikipedia.org/wiki/Grover%27s_algorithm#Description_of_U.CF.89>

fig 2.15

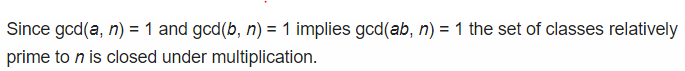
Inversion about the mean – quantum computing devices Goong - p. 68 fig 2.16 prawdopodobienstwo 1 dla 2 qitów?, zlozonosc O(1) ??

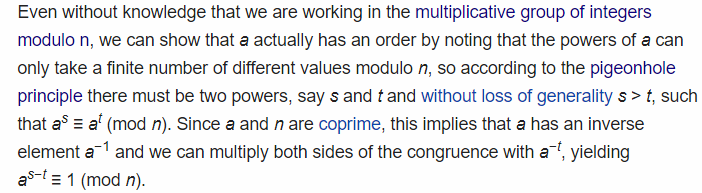
Liczba iteracji > sqrt(N) nie zwieksza precyzji, lecz zmniejsza.

Before we attempt to shor algorithm I would like to present some group theory:

Grupa z względnie pierwszych z N z mod(N), rząd grupy, może jakiś dowód

Multiplicative group of integers modulo n





Shor:

qft: continued fraction , dlaczego nie maksymalna wartość?