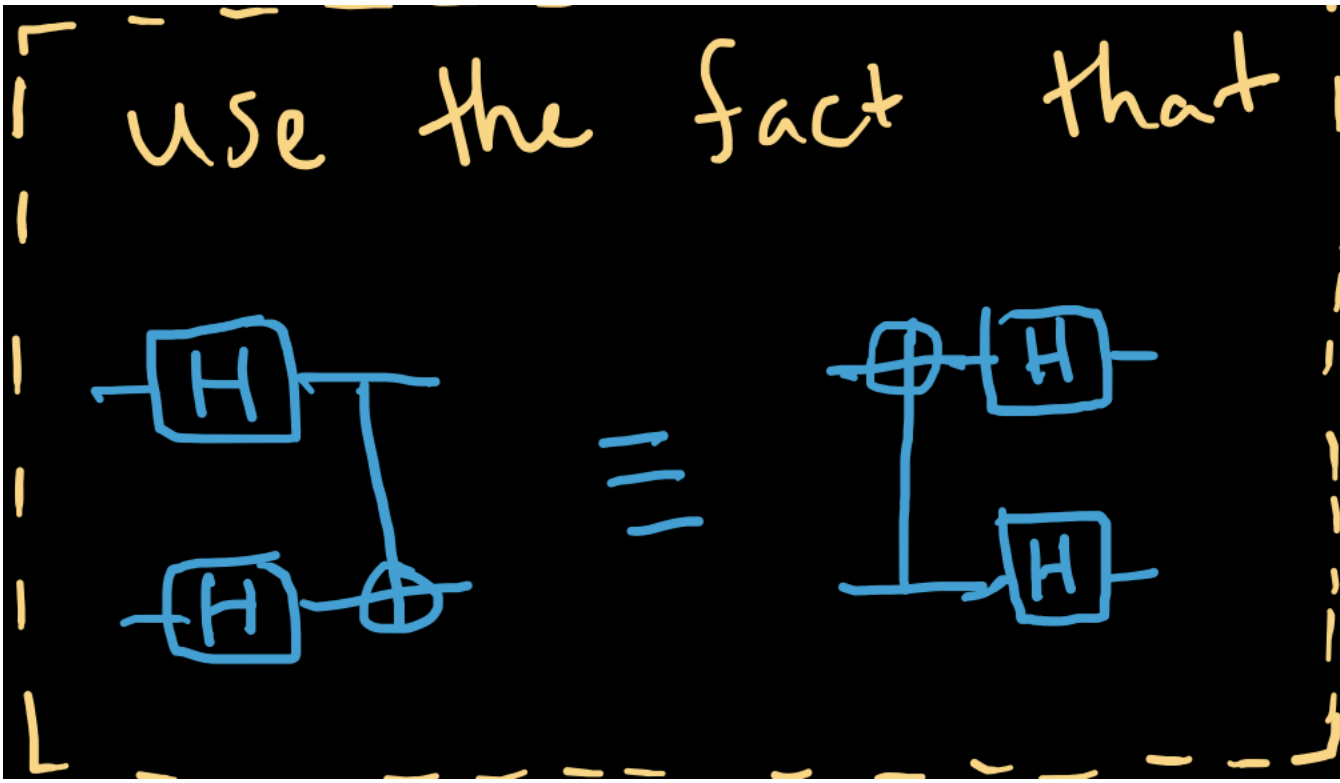
CSE 490Q Lecture notes

Ajay Rawat
(ajay712@cs.washignton.edu)
1962171

7 December, 2020

1 Correction



2 Shor's algorithm

2.1 Description

-Used for factoring
- RSA encryption system relies on the hardness of factoring.
- Classical: $O(2^{n/3})$
-Quantum (Shor) : $O(n^3)$ (much faster)

2.2 Post-Shor Algorithm

- Most of the work after Shor's algorithm was developed was focused on generalising it to solve other problems
- Alexei Kitaev generalised the algorithm for "phase estiamtion"

3 Groups

3.1 Definition

A group (G) is a set such that:
- The identity element e $\in$ G
- if x,y $\in$ G, then xy $\in$ G
- if x $\in$ G, then $x^{-1} \in$ G

xe= x =ex,x(yz)= (xy)z and xx^{-1} = e = xx^{-1}

4 Abelian Group

: Named after Mathematician Abel.

if xy = yx for all x, y in G

4.1 Examples

- Set of Real numbers is a group under multiplication, where 1 is identity and the inverse of x is 1/x.
- $Z_n$is a group under addition, where multiplication is modulo N. ({0,1,2...N-1} with 0 as identity)
- $(Z_n)^x$ is a group under multiplication. [Set $x \in Z_N : gcd(x, N) = 1$, with 1 as the identity]

4.2 Non-Abelian Group Examples

- Set of 2x2 Unitary matrices and their Hermitian conjugates
- Pauli Group (I,X,Y,Z) scaled by 1,1,i,-i

4.3 Products of Groups

If G and H, then GxH = {(x,y) :$x \in G, y \in H$}
(u,v)(x,y) = (ux,vy), $(x, y)^{-1} = (x^{-1}, y^{-1})$

5 Finitely Abelian Group

Theorem: If G is a finite abelian group, then there are integers: $N_1, ...N_k$ such that G = $Z_1 x ... x Z_k$

6 Some Important groups

6.1 Dihedral Group

Elements are $r^i s^j$ for $i \in Z_n, j \in Z_2$, $r^N = 1, s^2 = 1$

6.2 Heisenberg Group

Elements are 3x3 martices of Z_p prime numbers: $\begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}$

7 Subgroups

7.1 Definition

A sub group is a sub set of a group that is also a group.

7.2 Cosets

$S \subseteq G, g \in G$
Coset: gS = $\{gs : s \in S\}$

If g, h $\in$ G, then either have gS = hS or gS $\cap$ hS = ϕ.

8 Hidden Subgroup Problem (HSP)

Given a function f : G to $\{0,1\}^k$ that is constant on cosets of some subgroup H, find the subgroup H.

Example: if G = $(Z_N)^x$ and f(x) = y^x (mod N)
Find the order r for which f(x+r) = f(x) i.e. $(Z_r)^x$