1 Correction

use the fact that

\[
\begin{array}{c}
H \\
\hline
H
\end{array}
\quad =
\begin{array}{c}
\bigoplus \\
H
\end{array}
\begin{array}{c}
H
\end{array}
\bigoplus 
\begin{array}{c}
H
\end{array}
\]
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 estimation”
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 $x^{-1} \in G$

$x e = x = e x$, $(xy) z = x (yz)$ and $x x^{-1} = e = x^{-1} x$

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 $1/x$.
- $\mathbb{Z}_n$ is a group under addition, where multiplication is modulo $N$. ($\{0, 1, 2...N-1\}$ with 0 as identity)
- $(\mathbb{Z}_n)^x$ is a group under multiplication. [Set $x \in \mathbb{Z}_N : \gcd(x, N) = 1$, 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 $G \times H = \{(x, y) : x \in G, y \in H\}$
$(u, v)(x, y) = (ux, vy), \ (x, y)^{-1} = (x^{-1}, y^{-1})$
5  Finitely Abelian Group

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

6  Some Important groups

6.1  Dihedral Group

Elements are \( r^i s^j \) for \( i \in \mathbb{Z}_n, j \in \mathbb{Z}_2, r^N = 1, s^2 = 1 \)

6.2  Heisenberg Group

Elements are 3x3 matrices of \( \mathbb{Z}_p \) 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 $gS \cap hS = \phi$.

8 Hidden Subgroup Problem (HSP)

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

Example: if $G = (\mathbb{Z}_N)^x$ and $f(x) = y^x \ (\text{mod N})$

Find the order $r$ for which $f(x+r) = f(x)$ i.e. $(\mathbb{Z}_r)^x$