Quantum computation : additional slides

1°) Groups, subgroups, equivalence classes
Lagrange's theorem
along with examples!

2°) Euler's totient function φ
Main properties & a simple lower bound

Finite group

= finite set $G = \{g_1, g_2, \dots, g_n\}$ equipped with internal operation $g_1, g_2 \longmapsto g_1 \cdot g_2$ s.t.

1) $(g \cdot g') \cdot g'' = g \cdot (g' \cdot g'')$ $\forall g, g', g'' \in G$ associativity
2) $\exists e \in G$ s.t. $g \cdot e = e \cdot g = g$ $\forall g \in G$ neutral el.
3) $\forall g \in G, \exists g^{-1} \in G$ s.t. $g \cdot g^{-1} = g^{-1} \cdot g = e$ inverse

On top of that, we say that G is <u>abelian</u> if $g \cdot g' = g' \cdot g$ $\forall g, g' \in G$.

Subgroup

$= \text{set } \emptyset \neq H \subset G$ s.t. if $h, h' \in H$, then $h \cdot h' \in H$

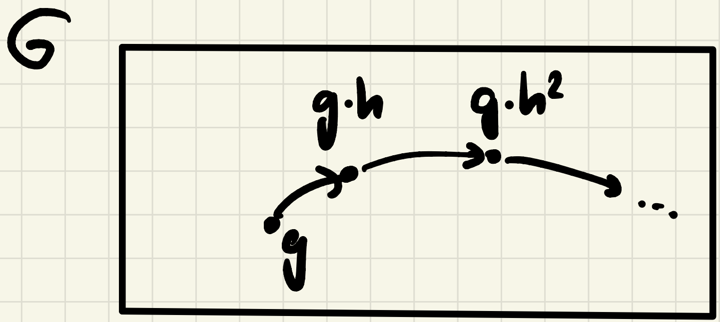
and if $h \in H$, then $h^{-1} \in H$

From this definition, it follows that H is a group, contains the neutral element e, and the associativity law holds inside H.

NB: $H = \{e\}$ & $H = G$ are always subgroups of G

Equivalence classes of a subgroup $H \subset G$

$E_g = \{ g \cdot h \; : h \in H \}$ = set reachable from an element g acting by all possible elements of H:



If G is abelian, then $E_g = \{ h \cdot g \; : h \in H \}$

Fundamental property

If $g \neq g'$ in G, then either $E_g = E_{g'}$ or $E_g \cap E_{g'} = \phi$

This is a direct consequence of Lagrange's thm:

(i) Let $g, g' \in G$; then either $E_g = E_{g'}$ or $E_g \cap E_{g'} = \phi$

(ii) The number of equivalence classes of H is equal to $\dfrac{|G|}{|H|}$, i.e. $|H|$ divides $|G|$.

Notation: The set of equivalence classes of H is also denoted as G/H (the *quotient group*) (so observe that $|G/H| = |G|/|H|$)

Proof of Lagrange's thm:

(i) Let $g, g' \in G$. If $E_g \cap E_{g'} = \emptyset$, there is nothing to prove; assume therefore $\bar{g} \in E_g \cap E_{g'}$. By def., $\exists\, h, h' \in H$ s.t. $\bar{g} = g \cdot h = g' \cdot h'$

So $g' = g \cdot \underbrace{h \cdot (h')^{-1}}_{\in H} \in E_g$; i.e. $E_{g'} \subset E_g$

Likewise, $g = g' \cdot \underbrace{h' \cdot h^{-1}}_{\in H} \in E_{g'}$; i.e. $E_g \subset E_{g'}$ # (i)

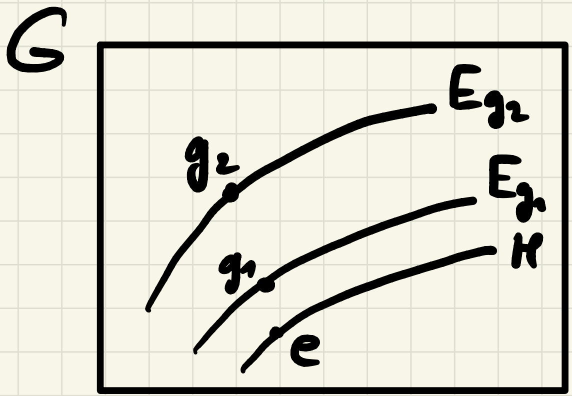
(ii) $|E_g| = |H| \quad \forall g$ because the mapping

$$\begin{cases} H \longrightarrow E_g \\ h \longmapsto g \cdot h \end{cases}$$ is bijective

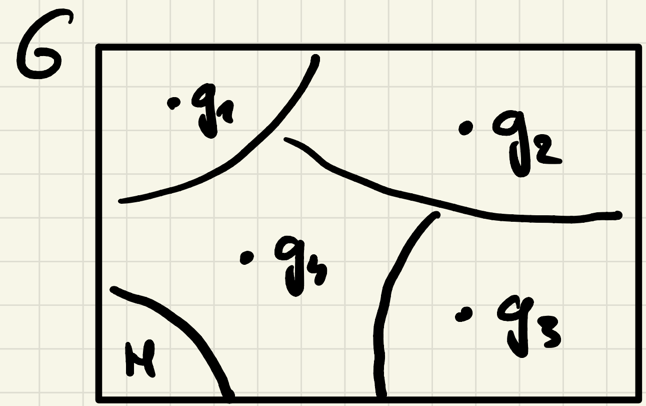
So $|G/H| \cdot |H| = |G|$ # (ii)

(Thanks to part i)

Here are some "pictures":



or



<u>NB</u>: • The equivalence classes of H form a <u>partition</u> of G

• H = subgroup? check first that $|H|$ divides $|G|$!

Examples

1) Let us first consider $G = (\{0,1\}^3, \oplus)$ with the group (abelian) operation

$$x \oplus y = (x_1 \oplus y_1, x_2 \oplus y_2, x_3 \oplus y_3)$$

Note that even though we use a multiplicative notation for groups, here the operation is simply the XOR (addition mod 2).

Likewise, the inverse of an element x is simply equal to itself as $x \oplus x = 0$.

In this example, G is more than a group: it is also a <u>vector space</u> of dimension 3.

We can also define the <u>dual</u> of a <u>subspace</u> H: $H^{\perp} = \{ y \in G : y \cdot x = 0 \ \forall x \in H \}$

<u>not</u> orthogonal

(dot product $\neq$ inner product)

1a) $H = \{(000), (001)\}$ is a subgroup of G, (& subspace) with 4 equivalence classes:

$E_{(000)} = H$ $\qquad$ $E_{(100)} = H \oplus (100)$

$E_{(010)} = H \oplus (010)$ $\qquad$ $E_{(110)} = H \oplus (110)$

$G/H = \{E_{(000)}, E_{(100)}, E_{(010)}, E_{(110)}\}$

$H^{\perp} = \{(000), (100), (010), (110)\}$

H has dimension 1, $H^{\perp}$ has dimension 2

1b) $H = \mathrm{span}\{(100), (010)\}$

$= \{(000), (100), (010), (110)\}$

also a subgroup of G

$E_{(000)} = H$, $E_{(001)} = H \oplus (001)$

$G/H = \{ E_{(000)}, E_{(001)} \}$

$H^{\perp} = \{(000), (001)\}$ $\dim H = 2$, $\dim H^{\perp} = 1$

This seems all intuitive and matching perfectly, but wait for the next example!

1c) $H = \operatorname{span}\{(110), (001)\}$

$= \{(000), (110), (001), (111)\}$

again a subgroup of G

$E_{(000)} = H$, $\quad E_{(100)} = H \oplus (100)$

$G/H = \{E_{(000)}, E_{(100)}\}$

$\dim H = 2$, $\dim H^{\perp} = 1$

<u>but</u> $H^{\perp} = \{(000), (110)\}$ [CH!]

(this surprising fact comes from the fact that $x \cdot y$ is not an inner product)

2) More generally, we may have

- $G = (\{0,1\}^n, \oplus)$ set of length n binary vectors equipped with addition mod 2
- H = k-dimensional subspace of G : $|H| = 2^k$
- In this case, G will be divided into $|G/H| = 2^{n-k}$ equivalence classes
- And $H^\perp$ = $(n-k)$-dim subspace, $|H^\perp| = 2^{n-k}$

3) $G = (\mathbb{Z}, +)$ the set of integer numbers equipped with the usual addition

$H = r \cdot \mathbb{Z}$ with r some positive integer

<u>eq. classes</u>: $E_0 = H$, $E_q = \{ q + n \cdot r : n \in \mathbb{Z} \}$

$0 \leq q \leq r-1$

$G/H = \mathbb{Z}/r\mathbb{Z} = \{0, 1, \ldots, r-1\}$, $|G/H| = r$

integers modulo r

4) $G = \mathbb{Z}/M\mathbb{Z} = \{0, 1, \dots, M-1\}$

$H = \{$ multiples of r between 0 & $M-1$ $\}$ (r fixed)

= subgroup of G if and only if r divides M

Note that is this case, G/H is isomorphic to $\mathbb{Z}/r\mathbb{Z}$

Euler's totient function φ

Def: Let $N \geq 1$ be an integer

$$\varphi(N) := \#\{0 \leq k \leq N-1 : \gcd(k,N) = 1\}$$

Ex: $\varphi(8) = \#\{1,3,5,7\} = 4$

$$\varphi(10) = \#\{1,3,7,9\} = 4$$

$$\varphi(18) = \#\{1,5,7,11,13,17\} = 6$$

More generally:

- $\varphi(P) = P-1$ if P is prime
- $\varphi(P \cdot Q) = (P-1)\cdot(Q-1)$ if P, Q are prime
- $\varphi(P^k) = P^{k-1}(P-1)$ if P is prime & $k \geq 1$
- $\varphi(N) = P_1^{k_1-1}(P_1-1) \cdot P_2^{k_2-1}(P_2-1) \dots P_e^{k_e-1}(P_e-1)$

  if $N = P_1^{k_1} \cdot P_2^{k_2} \dots P_e^{k_e}$ is the (unique) prime factor decomposition of N

Proposition

$$\varphi(N) \geq \frac{N}{4\ln(N)} \qquad \forall N \geq 2$$

Proof

If $N = p_1^{k_1} \cdot p_2^{k_2} \cdots p_\ell^{k_\ell}$, then

$$\varphi(N) = p_1^{k_1}\left(1 - \frac{1}{p_1}\right) p_2^{k_2}\left(1 - \frac{1}{p_2}\right) \cdots p_\ell^{k_\ell}\left(1 - \frac{1}{p_\ell}\right)$$

$$= N \prod_{j=1}^{\ell} \left(1 - \frac{1}{p_j}\right)$$

$$= N \prod_{j=1}^{\ell} \left(1 - \frac{1}{p_j^2}\right) \Big/ \left(1 + \frac{1}{p_j}\right)$$

So $\varphi(N) = N \cdot \prod_{j=1}^{\ell} \left(1 - \frac{1}{p_j^2}\right) \Big/ \prod_{j=1}^{\ell} \left(1 + \frac{1}{p_j}\right)$

Numerator : $\prod_{j=1}^{\ell} \left(1 - \frac{1}{p_j^2}\right) \geq \prod_{i=2}^{N} \left(1 - \frac{1}{i^2}\right)$

$$= \prod_{i=2}^{N} \frac{i^2 - 1}{i^2} = \prod_{i=2}^{N} \frac{(i-1)(i+1)}{i^2} = \frac{1 \cdot \cancel{3}}{2^{\cancel{2}}} \cdot \frac{\cancel{2} \cdot \cancel{4}}{\cancel{3^2}} \cdot \frac{\cancel{3} \cdot \cancel{5}}{\cancel{4^2}} \cdots \frac{\cancel{(N-1)}(N+1)}{N^{\cancel{2}}}$$

$$= \frac{N+1}{2N} \geq \frac{1}{2}$$

Denominator : $\prod_{j=1}^{n} \left(1 + \frac{1}{p_j}\right) \leq \sum_{i=1}^{N} \frac{1}{i}$ (expand the product)

$$\leq 1 + \ln(N) \leq 2\ln(N)$$

This leads to the desired inequality. #