CS201

Mathematics for Computer Science I

Lecture 21

Necklace Problem

- Given Red and Black beads, how many distinct necklaces can be made of n beads?
- Represent a necklace by a sequence of n letters, each either R or B, denoting color of bead in every location of necklace.
- Let S be the set of all such sequences.
- We know, $|S| = 2^n$.
- However, not all sequences represent distinct necklaces: rotating or flipping a sequence does not change the necklace being represented.

Symmetry Group

- Define $\phi, \psi : S \mapsto S$ as:

$$\begin{aligned} \phi(c_0 c_1 \cdots c_{n-1}) &= c_{n-1} c_0 c_1 \cdots c_{n-2} \\ \psi(c_0 c_1 \cdots c_{n-1}) &= c_0 c_{n-1} c_{n-2} \cdots c_1 \end{aligned}$$

- ϕ and ψ can also be viewed as bijections from $[0, n-1]$ to itself.
- As observed, the set of bijections of $[0, n-1]$ to itself is a non-commutative group under composition.
- This group is referred as symmetry group on n elements, and denoted as S_n.

Symmetries of Necklace

- Bijection ϕ denotes right rotation by one and ψ denotes a flip pivoting on first bead.
- These two capture all the sequences representing same necklace in the following way:
  - For a given sequence, any number of rotations and flips do not change the necklace represented.
  - Flip pivoting on any other bead can be expressed as left rotation to make the bead first one, flip pivoting on first bead, and then a right rotation to take back the bead to its original place.
  - Hence, the set of bijections preserving the necklace are precisely the following subgroup of S_n:

$$N = \{\phi^{i_1}\psi^{j_1}\phi^{i_2}\psi^{j_2}\cdots\phi^{i_k}\psi^{j_k} \mid i_r, j_r \in \mathbb{Z}\}$$

where $\phi^i = \underbrace{\phi \circ \phi \circ \cdots \circ \phi}_{i \text{ times}}$.

Symmetries of Necklace

- The subgroup N can be simplified:
  - $\phi^n = e$, hence $0 \leq i_r < n$.
  - $\psi^2 = e$, hence $0 \leq j_r \leq 1$.
  - We have:

$$\begin{aligned}
\psi \circ \phi \circ \psi \circ \phi(c_0 c_1 \cdots c_{n-1}) &= \psi \circ \phi \circ \psi(c_{n-1} c_0 \cdots c_{n-2}) \\
&= \psi \circ \phi(c_{n-1} c_{n-2} \cdots c_0) \\
&= \psi(c_0 c_{n-1} \cdots c_1) \\
&= c_0 c_1 \cdots c_{n-1}.
\end{aligned}$$

  - Therefore, $\phi \circ \psi = \psi^{-1} \circ \phi^{-1} = \psi \circ \phi^{n-1}$. So,

$$N = \{\psi^j \phi^i \mid 0 \leq j \leq 1, 0 \leq i < n\}.$$

- Hence, $|N| = 2n$.

Counting Necklaces

- Define a relation R on the set of sequences S as: $t_1 R t_2$ for $t_1, t_2 \in S$ if there exists $\eta \in N$ such that $\eta(t_1) = t_2$.
- Relation R is an equivalence relation:
  - tRt since $e(t) = t$ and $e \in N$.
  - If $t_1 R t_2$ then $\eta(t_1) = t_2$ for $\eta \in N$.
  - This implies $\eta^{-1}(t_2) = t_1$ and $\eta^{-1} \in N$ showing $t_2 R t_1$.
  - If $t_1 R t_2$ and $t_2 R t_3$ then $\eta_1(t_1) = t_2$ and $\eta_2(t_2) = t_3$ for $\eta_1, \eta_2 \in N$.
  - This implies $\eta_2 \circ \eta_1(t_1) = t_3$ and $\eta_2 \circ \eta_1 \in N$ showing $t_1 R t_3$.

Counting Necklaces

- The number of distinct necklaces equals the number of equivalence classes of S under R.
- Unfortunately, the size of different equivalence classes can be different, and so no simple way is available to count number of equivalence classes:
  - For $t = \underbrace{RR\cdots R}_{n-1 \text{ times}} B$, the size of equivalence class containing t is n.
  - For $t = \underbrace{RR\cdots R}_{n \text{ times}}$, the size of equivalence class containing t is 1, the minimum possible.
- Therefore, we need to dive deeper to count!

Counting Necklaces

- For $t \in S$, let $[t]$ denote the equivalence class under R that t belongs to, and $|[t]|$ its size.
- For $t \in S$, define $N_t = \{\eta \mid \eta(t) = t, \eta \in N\}$.
- N_t is a subgroup of N:
  - Since $e(t) = t$, $e \in N_t$.
  - If $\eta_1, \eta_2 \in N_t$ then $\eta_1 \circ \eta_2 \in N_t$.
  - If $\eta \in N_t$ then $\eta^{-1} \in N_t$.

Counting Necklaces

- N_t splits N into equivalence classes of size $|N_t|$.
- We have: $|[t]| * |N_t| = |N|$:
  - For $\eta_1, \eta_2 \in N$, $\eta_1(t) = \eta_2(t)$ iff $\eta_1 \circ \eta_2^{-1} \in N_t$.
  - Therefore, the number of equivalence classes of N is exactly $|[t]|$.

Counting Necklaces

- For any $\eta \in N$, let $F_\eta = \{t \mid t \in S, \eta(t) = t\}$.
- For $\eta \in N$ and $t \in S$, let $\chi_{\eta,t} = 1$ if $\eta(t) = t$, 0 otherwise.
- We have:

$$\begin{aligned}
\text{No of distinct necklaces} &= \sum_{t \in S} \frac{1}{|[t]|} \\
&= \sum_{t \in S} \frac{|N_t|}{|N|} \\
&= \frac{1}{2n} \sum_{t \in S} \sum_{\eta \in N} \chi_{\eta,t} \\
&= \frac{1}{2n} \sum_{\eta \in N} \sum_{t \in S} \chi_{\eta,t} \\
&= \frac{1}{2n} \sum_{\eta \in N} |F_\eta|
\end{aligned}$$

Counting Necklaces

- $|F_\psi| = 2^{(n+1)/2}$ if n is odd, $2^{(n+2)/2}$ otherwise.
- $|F_\phi| = 2$.
- In general, $|F_{\phi^i}| = 2^{\gcd(i,n)}$.
- And $|F_{\psi\circ\phi^i}| = 2^{(n+1)/2}$ if n is odd, $2^{(n+2)/2}$ otherwise since $\psi \circ \phi^i \circ \psi \circ \phi^i = e$.
- Therefore,

$$\text{No of distinct necklaces} = \frac{1}{2n}\left(n2^{\lfloor (n+2)/2 \rfloor} + \sum_{i=0}^{n-1} 2^{\gcd(i,n)}\right).$$

Polya's Counting Theorem

- The proof can be extended to more general settings.
- Let S be a finite set and G be a finite group acting on S in the following way: for every $g \in G$, $g : S \mapsto S$.
- G divides S into equivalence classes.
- Let $F_g = \{t \mid g(t) = t\}$.

Theorem

Let S be a finite set and G be a finite group acting on S. Then number of equivalence classes of S induced by G equals $\frac{1}{|G|} \sum_{g \in G} |F_g|$.