Necklaces and subset-sums: How can they be related?
Swee Hong Chan
Cornell University

\begin{align*}
\text{Necklace 1:} & \quad \{0\} \\
\text{Necklace 2:} & \quad \{2, 3\} \\
\text{Necklace 3:} & \quad \{1, 4\} \\
\text{Necklace 4:} & \quad \{0, 1, 4\}
\end{align*}
105. (a) [3–] Let \( n \in \mathbb{P} \), and let \( f(n) \) denote the number of subsets of \( \mathbb{Z}/n\mathbb{Z} \) (the integers modulo \( n \)) whose elements sum to 0 in \( \mathbb{Z}/n\mathbb{Z} \). For instance, \( f(4) = 4 \), corresponding to \( \emptyset, \{0\}, \{1, 3\}, \{0, 1, 3\} \). Show that

\[
f(n) = \frac{1}{n} \sum_{\substack{d \mid n \\text{odd}}} \phi(d) 2^{n/d},
\]

where \( \phi \) denotes Euler’s totient function.

(b) [5–] When \( n \) is odd, it can be shown using (a) (see Exercise 7.112) that \( f(n) \) is equal to the number of necklaces (up to cyclic rotation) with \( n \) beads, each bead colored black or white. Give a combinatorial proof. (This is easy if \( n \) is prime.)
Necklaces with two colors

Necklaces are rotationally invariant.
Subsets of $\mathbb{Z}_n$ that sums to 0 (modulo $n$)

Let $n = 5$.

Example:
- $\{0, 1, 4\}$; $0 + 1 + 4 = 5 = 0 \mod 5$.
- $\{1, 2, 3, 4\}$; $1 + 2 + 3 + 4 = 10 = 0 \mod 5$.

Non-example:
- $\{1, 3, 4\}$; $1 + 3 + 4 = 8 = 3 \mod 5$.
- $\{0, 1, 2, 3\}$; $0 + 1 + 2 + 3 = 6 = 1 \mod 5$. 
The theorem

Theorem (EC1, 1.105(a))

If \( n \) is odd, then:

\[
\text{\# of necklaces of length } n \text{ with two colors} = \text{\# of subsets of } \mathbb{Z}_n \text{ that sums to 0}.
\]

Proof in EC 1 uses orbit-counting theorem and generating function. Stanley then asked for a combinatorial proof.
The theorem

Theorem (EC1, 1.105(a))

If \( n \) is odd, then:

\[
\text{# of necklaces of length } n \text{ with two colors} = \text{# of subsets of } \mathbb{Z}_n \text{ that sums to 0}.
\]

We will give a combinatorial proof to this theorem.
Proof in EC1

**Orbit-counting theorem:** For a group $G$ acting on a set $X$,

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$  

For $G = \mathbb{Z}_n$ and $X =$ set of strings of length $n$ with two colors,

$$\# \text{ of necklaces of length } n \text{ with two colors} = \frac{1}{n} \sum_{d | n} 2^{n/d} \phi(d).$$

Euler's totient function.
For any complex $n$-th root of unity $\zeta := e^{2\pi i/n},$

$$(1 + \zeta)(1 + \zeta^2) \cdots (1 + \zeta^n) = c_0 + c_1\zeta + \cdots + c_{n-1}\zeta^{n-1}.$$ 

By summing over all $n$-th roots of unity,

$$\sum_{d|n \atop d \text{ odd}} 2^{n/d} \phi(d) = n \left( \text{\# of subsets of } \mathbb{Z}_n \text{ that sums to 0} \right).$$
Proof in EC1 (ctd)

If $n$ is odd, then:

$$\text{# of necklaces of length } n \text{ with two colors} = \text{# of subsets of } \mathbb{Z}_n \text{ that sums to 0},$$

and is equal to

$$\frac{1}{n} \sum_{d|n} 2^{n/d} \phi(d).$$

Questions unanswered by this proof:

- How are they related?
- Why odd $n$?
View necklaces as polynomials

The necklace

\[ \{1 + X^2, X + X^3, X^2 + X^4, X^3 + 1, X^4 + X\} \subset \mathbb{F}_2[X]/(X^5 - 1), \]

which is equal to:

\[ \{X^k(1 + X^2) \mid 0 \leq k < 5\}. \]
Facts that we will use

For odd $n$, fix a primitive $n$-th root of unity $\omega$ over $\mathbb{F}_2$. Write

$$C_i := \{s_i, 2s_i, \ldots, 2^{\ell_i - 1}s_i\} \subset \mathbb{Z}_n$$  \hspace{1cm} (cyclotomic coset)

$$P_i(X) := (X - \omega^{s_i})(X - \omega^{2s_i}) \cdots (X - \omega^{2^{\ell_i - 1}s_i}) \in \mathbb{F}_2[X].$$

Facts:

- $X^n - 1$ factors into irreducible polynomials $P_1(X) \cdots P_m(X)$;
- $(\mathbb{F}_2[X]/P_i(X))^\times$ is isomorphic to the cyclic group $\mathbb{Z}_{2^{\ell_i - 1}}$.

Example:

$$X^5 - 1 = (X + 1)(\underbrace{1 + X + X^2 + X^3 + X^4}_{P_1(X)}),$$

$$(\mathbb{F}_2[X]/P_1(X))^\times \simeq \mathbb{Z}_1; \quad (\mathbb{F}_2[X]/P_1(X))^\times \simeq \mathbb{Z}_{15}.$$
The bijection for $n = 5$

Necklaces divisible by $P_1(X)$ but not $P_2(X)$ ↔ Nonempty subsets of $\{1, 2, 3, 4\}$ that sums to 0.

\[ \{X^k(1 + X^2) \mid 0 \leq k < 5\} \]
An example of the bijection

\[ \{X^k(1 + X^2) \mid 0 \leq k < 5\}. \]

Take \(1 + X^3\) as the group generator of \((\mathbb{F}_2[X]/P_2(X))^{\times}\),

\[ \{(1 + X^3)^{9k}(1 + X^3)^4 \mid 0 \leq i < 5\} \mod P_2(X) \]

Viewing \((\mathbb{F}_2[X]/P_2(X))^{\times}\) as the group \(\mathbb{Z}_{15}\),

\[ \{9k + 4 \mid 0 \leq k < 5\} \subset \mathbb{Z}_{15}. \]

This gives us

\[ \{4, 13, 7, 1, 10\}. \]
An example of the bijection (ctd)

\[ \{ 4, 13, 7, 1, 10 \} . \]

Take the quotient and the remainder of division by 3:

\[ \{ 3 \cdot 1 + 1 , 3 \cdot 4 + 1 , 3 \cdot 2 + 1 , 3 \cdot 0 + 1 , 3 \cdot 3 + 1 \} \]

Exchange the quotient with the remainder, then change 3 to 5:

\[ \{ 5 \cdot 1 + 1 , 5 \cdot 1 + 4 , 5 \cdot 1 + 2 , 5 \cdot 1 + 0 , 5 \cdot 1 + 3 \} \]

This gives us:

\[ \{ 6, 9, 7, 5, 8 \} . \]

Take the unique subset of \{1, 2, 4, 8\} that sums to 5 mod 15:

\[ \{ 1, 4 \} . \]
The bijection for necklaces coprime only to $P_i(X)$

Input: Necklaces coprime only to $P_i(X) = (X - \omega^{s_i}) \ldots (X - \omega^{2^{\ell_i-1}s_i})$.
Output: Nonempty subset of $\{s_i, \ldots, 2^{\ell_i-1}s_i\}$ that sums to 0 mod $n$.

Algorithm:
(1) View necklace as subset of $(\mathbb{F}_2[X]/P_i(X))^\times = \mathbb{Z}_{2^{\ell_i-1}}$;
(2) Take the quotient and remainder of division by $\frac{(2^{\ell_i-1}) \gcd(s_i,n)}{n}$;
(3) Exchange quotient with remainder;
(4) Change $\frac{(2^{\ell_i-1}) \gcd(s_i,n)}{n}$ to $\frac{n}{\gcd(s_i,n)}$;
(5) Take the unique number that is divisible by $\frac{n}{\gcd(s_i,n)}$;
(6) Output is the unique nonempty subset of $\{s_i, \ldots, 2^{\ell_i-1}s_i\}$ that sums to the number.
How about other necklaces?

Input: A necklace of length \( n \) with two colors.
Output: Subsets of \( \mathbb{Z}_n \) that sums to 0 mod \( n \).

Algorithm:
(1) View necklaces as elements of \( \frac{\mathbb{F}_2[X]}{P_1(X)} \times \frac{\mathbb{F}_2[X]}{P_2(X)} \times \ldots \times \frac{\mathbb{F}_2[X]}{P_k(X)} \);
(2)-(5) Apply analogous steps to \( \mathbb{Z}_{2^{\ell_1}-1} \times \mathbb{Z}_{2^{\ell_2}-1} \times \ldots \times \mathbb{Z}_{2^{\ell_k}-1} \);
(6) Output is a subset of \( \mathbb{Z}_n \) viewed as \( C_1 \cup C_2 \cup \ldots \cup C_k \).
Conclusion

Theorem

If $n$ is odd, then:

$$\sum_{I \subseteq \{1, \ldots, m\}} \frac{\text{gcd}(n, (s_i)_{i \in I})}{n} \prod_{i \in I} (2^{\ell_i} - 1).$$

This formula is different from (EC1)'s $\frac{1}{n} \sum_{d \mid n} 2^{n/d} \phi(d)$.
Conclusion

Theorem

If \( n \) is odd, then:

\[
\text{\# of necklaces of length } n \text{ with two colors} = \text{\# of subsets of } \mathbb{Z}_n \text{ that sums to 0},
\]

and is equal to

\[
\sum_{I \subseteq \{1, \ldots, m\}} \frac{\gcd(n, (s_i)_{i \in I})}{n} \prod_{i \in I} (2^{\ell_i} - 1).
\]

Q: Why odd \( n \)?

- Reason 1: so \( \mathbb{F}_2[X]/P_1(X), \ldots, \mathbb{F}_2[X]/P_m(X) \) are finite fields;
- Reason 2: so \( C_1, \ldots, C_m \) form a partition of \( \mathbb{Z}_n \).
Conclusion

**Theorem**

*If $n$ is odd, then:*

$$\text{# of necklaces of length } n \text{ with two colors} = \text{# of subsets of } \mathbb{Z}_n \text{ that sums to 0},$$

*and is equal to*

$$\sum_{I \subseteq \{1, \ldots, m\}} \frac{\gcd(n, (s_i)_{i \in I})}{n} \prod_{i \in I} (2^{\ell_i} - 1).$$

**Q:** How are those two sets related?

**A:** They are both secretly a union of products of cyclic groups.
What is next?

Bijection that preserves the number of blue beads?

Possible leads to answering this mystery:

- Number of necklaces with $k$ blue beads is as an evaluation of an arithmetic Tutte Polynomial (Ardila-Castilo-Henley ’15).
- Also the number of components in a chamber of the coroot toric arrangement of type A (Aguiar, C. ’17).
Why stop at two colors?

**Theorem**

If $q$ and $n$ are coprime, then:

\[
\text{# of necklaces of length } n \text{ with } q \text{ colors} = \text{# of multi-subsets of } \mathbb{Z}_n \text{ with mult. } < q \text{ that sums to 0},
\]

and is equal to

\[
\sum_{I \subseteq \{1, \ldots, m\}} \frac{\gcd(n, (s_i)_{i \in I})}{n} \prod_{i \in I} (q^{\ell_i} - 1).
\]

The proof is bijective if $q$ is prime power.

Bijective proof for the rest of the values of $q$?
THANK YOU!

⇒ {4,13,7,1,10} ⇒ {6,9,7,5,8} ⇒ {1,4}

Email: sweehong@math.cornell.edu