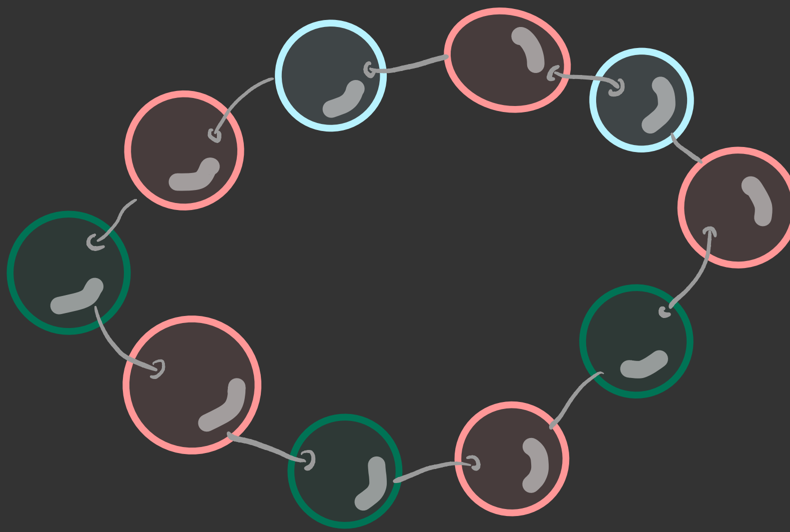
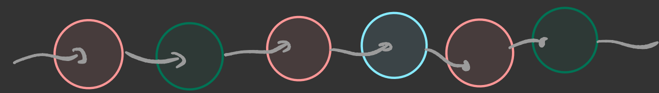
Computing the number of cyclic sequences



Definition: Let A be a set. A *linear sequence* of length n in alphabet A is an element of A^n:

$$a = (a_1, \dots, a_n), \quad a_k \in A \quad \text{for } k = 1, \dots, n.$$



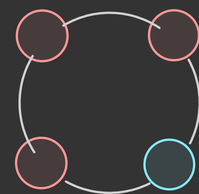
The number of linear sequences of lenth n in an alphabet of size r is r^n.

Consider the following equivalence relation on the set of linear sequences:

$$(a_1, \dots, a_n) \sim (a_2, a_3, \dots, a_n, a_1)$$

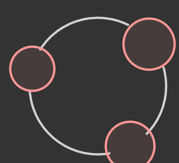
Two linear sequences are equivalent if one of them can be obtained from another by a cyclic shift.

Example:

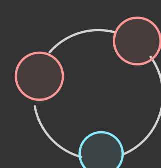


Definition: A *cyclic sequence* of length n in alphabet $\mathcal{A}$ is an equivalence class of linear sequences with respect to the relation $\sim$.

Example: There are 8 linear sequences of lenth 3 in alphabet $\{a, b\}$ and only 4 cyclic sequences



aaa



aab
aba
baa

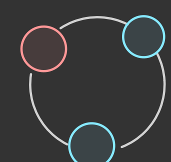
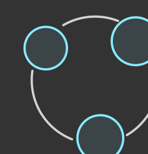


abb
bab
bba



bbb

Proposition: The number $T(n,r)$ of cyclic sequences of length n on an alphabet of size r is

$$T(n,r) = \frac{1}{n} \sum_{d \mid n} \phi(n/d)\, r^d$$

Here $\phi(\cdot)$ is the Euler's totient function.

Proof:

Definition: A *period* of a cyclic sequence $(a_1, \dots, a_n)$ is a minimal number $k \in \{1, 2, \dots, n\}$ such that

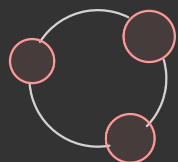
$$(a_1, a_2, \dots, a_n) = (a_{1+k}, a_{2+k}, \dots\, a_1, a_2, \dots, a_k)$$

are equal as linear sequences.

Exercise: The period of a sequence is a divisor of the sequences length.

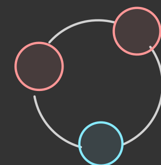
Let $M(d,r)$ be the number of cyclic sequences of length d and period exactly d

Example:



aaa

Period 1



aab
aba
baa

Period 3

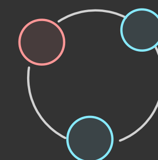
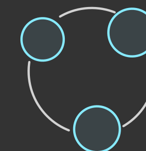


abb
bab
bba

Period 3



bbb

Period 1

$T(3,2) = 4$ $\qquad$ $M(3,2) = 2$

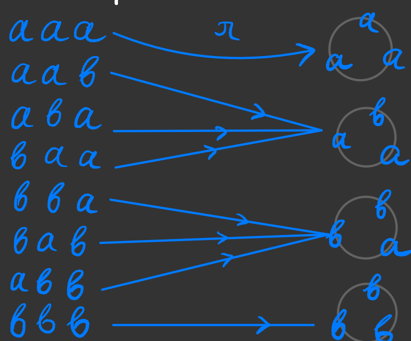
The following identity holds:

$$r^n = \sum_{d \mid n} d \cdot M(d,r)$$

$$\left\{ \begin{array}{l} \text{linear sequences} \\ \text{of lenth } n \\ \text{in alphabet } [r] \end{array} \right\} \xrightarrow[\substack{\text{projection} \\ \text{into} \\ \text{equivalence} \\ \text{class}}]{\pi} \left\{ \begin{array}{l} \text{Cyclic sequences} \\ \text{of lenth } n \\ \text{in alphabet } [r] \end{array} \right\}$$

$$= \bigsqcup_{d|n} \left\{ \begin{array}{l} \text{Cyclic sequences} \\ \text{of lenth } n \\ \text{and period } d \\ \text{in alphabet } [r] \end{array} \right\}$$

Example:



The number of preimages of a cyclic sequence under the map π is d, the period of the sequence.

Therefore $$|\mathcal{L}(n,r)| = \sum_{d|n} d \cdot |\mathcal{M}(d,r)|$$

$\mathcal{L}(n,r)$: set of linear sequences

$\mathcal{M}(d,r)$: set of cyclic sequences of lenth d and period d.

This proves the claim.

Starting with the identity

$$r^n = \sum_{d \mid n} d \cdot M(d,r)$$

we apply the Möbius inversion formula and obtain

$$\mu(d)\, r^{n/d}$$

$$n \cdot M(n,r) = \sum_{d \mid n} \mu(d/n)\, r^d \qquad (1)$$

Each cyclic sequence has well defined period d and it corresponds to the unique cyclic sequence of lenth d and period d.

$$(a_1, .., a_d, a_1 \ldots a_d, \ldots, a_1, \ldots, a_d) \sim (a_1, \ldots, a_d)$$

Thus $$T(n,r) = \sum_{d \mid n} M(d,r). \qquad (2)$$

Now we substitute (1) into (2):

$$T(n,r) = \sum_{d|n} M(d,r)$$

$$= \sum_{d|n} \frac{1}{d} \sum_{d'|d} \mu(d/d') r^{d'} =$$

we introduce the new summation variable $d'' = \frac{d}{d'}$

$$= \sum_{d'|n} \Big(\sum_{d''|\frac{n}{d'}} \frac{1}{d' \cdot d''} \mu(d'') \Big) \cdot r^{d'}$$

Now it remains to compute the sum:

$$\sum_{d''|\frac{n}{d'}} \frac{1}{d''} \mu(d'')$$

Exercise: Show that for $n \in \mathbb{Z}_{\geq 1}$, $\sum_{d|n} \frac{1}{d} \mu(d) = \frac{\varphi(n)}{n}$

Using this exercise we compute

$$T(n,r) = \sum_{d' \mid n} \frac{\varphi(n/d')}{n} \cdot r^{d'}$$

This finishes the proof. $\blacksquare$

There is another method to compute the number of cyclic sequences using the Burnside's lemma.