Journal of Integer Sequences, Vol. 29 (2026),
Article 26.4.6

Necklaces over a Group with Identity Product

Darij Grinberg and Peter Mao
Department of Mathematics
Drexel University
Korman Center, Room 291
15 S. 33rd Street
Philadelphia PA, 19104
USA
darijgrinberg@gmail.com
pm929@drexel.edu

Abstract

We address two variants of the classical necklace counting problem from enumerative combinatorics. In both cases, we fix a finite group $\mathcal{G}$ and a positive integer n. In the first variant, we count the "identity-product n-necklaces"—that is, the orbits of n-tuples $(a_1, a_2, \ldots, a_n) \in \mathcal{G}^n$ that satisfy $a_1 a_2 \cdots a_n = 1$ under cyclic rotation. In the second, we count the orbits of all n-tuples $(a_1, a_2, \ldots, a_n) \in \mathcal{G}^n$ under cyclic rotation and left multiplication (i.e., the operation of $\mathcal{G}$ on $\mathcal{G}^n$ given by $h \cdot (a_1, a_2, \ldots, a_n) = (ha_1, ha_2, \ldots, ha_n)$). We prove bijectively that both answers are the same, and express them as a sum over divisors of n.

Consequently, we generalize the first problem to n-necklaces whose product of entries lies in a given subset of $\mathcal{G}$ (closed under conjugation), and we connect a particular case to the enumeration of irreducible polynomials over a finite field with given degree and second-highest coefficient 0.

1 Introduction

Necklaces are combinatorial objects situated on the spectrum between ordered selections (tuples) and unordered selections (multisets) of elements from a set. Formally, they are defined as orbits (i.e., equivalence classes) of n-tuples under cyclic rotation. They can be

visualized as labellings (or colorings) of a circular necklace, where we understand that the necklace can be rotated at will (but not turned over) without changing the object.

Counting necklaces is a classical problem in enumerative combinatorics (see, e.g., [3, §3, Example 3 (b)], [15, Chapter 7], [10, §5.5]). A well-known formula due to Moreau [17] says that the number of n-necklaces (i.e., rotation classes of n-tuples) over a size-q set A is

$$\frac{1}{n}\sum_{d|n}\phi\left(d\right)q^{n/d}, \tag{1}$$

where the sum runs over all positive divisors d of n, and where ϕ denotes the Euler totient function (see Definition 4 below). This surprisingly simple formula is a starting point for several deeper developments, including the theory of necklace polynomials [12, §17.3]. The fact that (1) is an integer (obvious from its combinatorial meaning) itself has some uses in number theory (yielding, e.g., Fermat's Little Theorem when n is prime). The expression (1) also counts irreducible monic polynomials of degree dividing n over the finite field $\mathbb{F}_q$ when q is a prime power, and this can be proved using a bijection between necklaces and irreducible polynomials [20, §7.6.2]. There is also a bijection between words and multisets of necklaces [8, §3] with far-reaching applications to symmetric functions, free Lie algebras and permutation enumeration. Further afield, the Burrows–Wheeler transform (transforming words into necklaces) is used for data compression in software such as `bzip2` [1, §2.3].

In this paper, we count what we call *identity-product necklaces*, i.e., necklaces where instead of colored beads we have elements of a finite group $\mathcal{G}$ which multiply to the identity. This is an orbit-counting problem for a certain action of the cyclic group C_n, which (by a well-known technique) can be reduced to counting identity-product tuples which are fixed under different cyclic rotations. We thus obtain a "sum over divisors" formula similar to (1) but involving the sizes of the group and of its torsion subgroups (Theorem 5). Once again, the integrality of the result is not evident from the formula, and thus gives rise to nontrivial congruences between sizes of torsion subgroups modulo the length of the necklaces being counted.

After proving our main formula, we count the *aperiodic* identity-product necklaces (i.e., the ones that have no nontrivial rotational symmetries) as well (Theorem 16). As expected from classical necklace-counting, the sum is the same but for the replacement of the Euler totient function ϕ by the Möbius function μ.

The number of identity-product n-necklaces over a group $\mathcal{G}$ furthermore equals the number of "homogeneous n-necklaces" over $\mathcal{G}$, that is, orbits of n-tuples of elements of $\mathcal{G}$ under the action of the direct product $C_n \times \mathcal{G}$ (where C_n acts by cyclic rotation and $\mathcal{G}$ acts by left multiplication on each entry). We prove this bijectively (Theorem 19), thus obtaining a formula for the latter number as well.

In Section 8, we extend some of our enumerative results to the more general notion of *K-product necklaces*, in which the product of the entries is required to belong to a given conjugacy-invariant subset K of the group.

Just like Moreau's original necklaces, our identity-product necklaces can be connected to irreducible polynomials over finite fields. In Section 9, we take up this connection and prove

some enumerative results about conjugacy classes in finite field extensions and irreducible polynomials.

In Section 10, we relate our enumerations to three integer sequences from the Online Encyclopedia of Integer Sequences. In the short final Section 11, we suggest two venues for further research.

2 Definitions

Fix a finite group $\mathcal{G}$ with binary operation $\cdot$ and identity element 1.

Definition 1. For any nonnegative integer n, we let $\mathcal{G}_1^n$ be the set of all *identity-product n-tuples*, defined by

$$\mathcal{G}_1^n := \{a = (a_1, a_2, \ldots, a_n) \in \mathcal{G}^n : a_1 a_2 a_3 \cdots a_n = 1\}.$$

Definition 2. For any integer n, let us define the number $[\mathcal{G} \div n]$ to be

$$[\mathcal{G} \div n] := |\{a \in \mathcal{G} : a^n = 1\}|.$$

This is the number of elements in $\mathcal{G}$ whose order divides n.

Definition 3. Let n be a positive integer. Then the n-element cyclic group

$$C_n = \left\{1, g, g^2, \ldots, g^{n-1}\right\}$$

acts on $\mathcal{G}^n$ by cyclic rotation:

$$g\,(a_1, a_2, \ldots, a_n) = (a_n, a_1, a_2, \ldots, a_{n-1}).$$

To see that the subset $\mathcal{G}_1^n$ of $\mathcal{G}^n$ is preserved by this action, we observe that the equation

$$a_1 a_2 a_3 \cdots a_{n-1} a_n = 1$$

implies that a_n is the inverse of $a_1 a_2 a_3 \cdots a_{n-1}$, and thus

$$a_n a_1 a_2 a_3 \cdots a_{n-1} = 1.$$

Therefore, if $a = (a_1, a_2, a_3, \ldots, a_n)$ was an identity-product n-tuple, then ga will be also. Hence $\mathcal{G}_1^n$ is preserved by the action of C_n and thus itself becomes a C_n-set. The orbits of this action of C_n on $\mathcal{G}_1^n$ (that is, the elements of the quotient $\mathcal{G}_1^n / C_n$) are called the *identity-product n-necklaces*.

Definition 4. Let n be a positive integer. We define the *Euler totient* $\phi(n)$ to be the number of integers $i \in \{1, 2, \ldots, n\}$ that are coprime to n.

3 Main theorem I: Identity-product n-necklaces

Our first main result is a formula for the number of identity-product n-necklaces for any finite group $\mathcal{G}$:

Theorem 5. *Let n be a positive integer. The number $|\mathcal{G}_1^n/C_n|$ of identity-product n-necklaces is*

$$|\mathcal{G}_1^n/C_n| = \frac{1}{n}\sum_{d|n}\phi\left(\frac{n}{d}\right)\left[\mathcal{G} \div \frac{n}{d}\right]|\mathcal{G}|^{d-1}.$$

Here, as usual, the summation sign means a sum over all positive divisors d of n.

We can make this more explicit if $\mathcal{G}$ is abelian. Recall the cyclic groups C_k of order k, defined for all positive integers k. The structure theorem for finite abelian groups says that each abelian group is isomorphic to a direct product of such cyclic groups. If $\mathcal{G}$ is an abelian group written in such a form, then the above formula reduces to the following:

Corollary 6. *Assume that*

$$\mathcal{G} = \prod_{i=1}^{m} C_{k_i} \qquad (\text{a direct product of cyclic groups})$$

for some positive integers $k_1, k_2, \ldots, k_m$. Then the number $|\mathcal{G}_1^n/C_n|$ of identity-product n-necklaces is

$$|\mathcal{G}_1^n/C_n| = \frac{1}{n}\sum_{d|n}\phi\left(\frac{n}{d}\right)\prod_{i=1}^{m}\left(\gcd\left(k_i, \frac{n}{d}\right)k_i^{d-1}\right).$$

4 Lemmas

Our proofs of the above claims are based on a common set of lemmas. We use the *orbit-counting lemma* (by historic accident also known as the *Burnside lemma*; see [24] or [11, Theorem 6.2.5] for a proof):

Lemma 7. *Let G be a finite group acting on a finite set X. Then the number $|X/G|$ of orbits is*

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|\{x \in X : g \cdot x = x\}|.$$

We also need a basic theorem due to Gauss [21, Theorem 2.40]:

Lemma 8. *For any positive integer n, we have*

$$\sum_{d|n}\phi(d) = n.$$

A useful consequence thereof is the following:

Lemma 9. *Let f and g be two functions from $\{1,2,3,\ldots\}$ to $\mathbb{Q}$. Assume that*

$$g(k) = \sum_{d|k} f(d) \qquad \text{for each } k \geq 1. \tag{2}$$

Then

$$\sum_{d|k} \frac{k}{d} f(d) = \sum_{d|k} \phi\left(\frac{k}{d}\right) g(d) \qquad \text{for each } k \geq 1. \tag{3}$$

We shall prove this lemma using the following classical notion:

Definition 10. Let f and g be two functions from $\{1,2,3,\ldots\}$ to $\mathbb{Q}$. We define the *Dirichlet convolution* $f * g$ to be the function from $\{1,2,3,\ldots\}$ to $\mathbb{Q}$ given by

$$(f * g)(k) = \sum_{d|k} f(d)\, g\left(\frac{k}{d}\right).$$

The Dirichlet convolution operation $*$ is known to be commutative and associative (see, e.g., [21, §2.9]). Furthermore, Lemma 8 can be restated as

$$\phi * \underline{1} = \mathrm{id}, \tag{4}$$

where $\underline{1}$ denotes the constant function that sends all positive integers to 1 (because every integer $n > 0$ satisfies $(\phi * \underline{1})(n) = \sum_{d|n} \phi(d)\underline{1}(\frac{n}{d}) = \sum_{d|n} \phi(d)$ and $\mathrm{id}(n) = n$).

Proof of Lemma 9. We note that the assumption (2) is the written out form of the statement

$$g = f * \underline{1} \tag{5}$$

where $\underline{1}$ is the constant function which maps all positive integers to 1. We can also rewrite the conclusion (3) as

$$\sum_{d|k} f(d)\frac{k}{d} = \sum_{d|k} g(d)\, \phi\left(\frac{k}{d}\right), \tag{6}$$

or, equivalently,

$$(f * \mathrm{id})(k) = (g * \phi)(k). \tag{7}$$

To prove this, we observe that

$$\begin{aligned}
g * \phi &= (f * \underline{1}) * \phi && \text{(by (5))} \\
&= f * (\underline{1} * \phi) && \text{(by associativity of the Dirichlet convolution)} \\
&= f * (\phi * \underline{1}) && \text{(by commutativity of the Dirichlet convolution)} \\
&= f * \mathrm{id} && \text{(by (4))}
\end{aligned}$$

and therefore $f * \mathrm{id} = g * \phi$. □

The following lemma is a classical property of greatest common divisors:

Lemma 11. *Let a, b and c be three integers, where a and b are not both 0. Then $a \mid bc$ holds if and only if $\dfrac{a}{\gcd(a,b)} \mid c$.*

Proof. The "if" part is easy (since multiplying the divisibility $\dfrac{a}{\gcd(a,b)} \mid c$ with the obvious divisibility $\gcd(a,b) \mid b$ yields $a \mid bc$). It remains to prove the "only if" part. So let us assume that $a \mid bc$, and try to prove that $\dfrac{a}{\gcd(a,b)} \mid c$.

Let $g = \gcd(a,b)$. Thus, we can write a and b as $a = ga'$ and $b = gb'$ for two coprime integers a' and b'. Consider these a' and b'. Thus, $a \mid bc$ rewrites as $ga' \mid gb'c$. Cancelling g (which is nonzero, since a and b are not both 0), we thus obtain $a' \mid b'c$. Since a' is coprime to b', we can cancel b' from this divisibility (by [21, Theorem 1.9]), and obtain $a' \mid c$. In other words, $\dfrac{a}{\gcd(a,b)} \mid c$ (since $a' = \dfrac{a}{g} = \dfrac{a}{\gcd(a,b)}$), which completes our proof. □

Lemma 12. *Let a and b be two positive integers. Then $[C_a \div b] = \gcd(a,b)$.*

Proof. Set $g = \gcd(a,b)$ and $a' = a/g$, so that $a = ga'$. We write $\overline{c}$ for the residue class of an integer c modulo a. This remainder belongs to the finite ring $\mathbb{Z}/a\mathbb{Z}$.

Now, by the definition of $[C_a \div b]$, we have

$$\begin{aligned}[C_a \div b] &= \left|\left\{h \in C_a : h^b = 1\right\}\right| \\ &= \left|\left\{x \in \mathbb{Z}/a\mathbb{Z} : bx = \overline{0}\right\}\right|\end{aligned}$$

(since C_a is the additive abelian group $\mathbb{Z}/a\mathbb{Z}$, rewritten multiplicatively). Hence,

$$\begin{aligned}[C_a \div b] &= \left|\left\{x \in \mathbb{Z}/a\mathbb{Z} : bx = \overline{0}\right\}\right| \\ &= \left|\left\{c \in \{0,1,\ldots,a-1\} : b\overline{c} = \overline{0}\right\}\right| \qquad (8)\end{aligned}$$

(since the elements of $\mathbb{Z}/a\mathbb{Z}$ are precisely the elements $\overline{c}$ with $c \in \{0,1,\ldots,a-1\}$). However, for any $c \in \{0,1,\ldots,a-1\}$, we have the chain of equivalences

$$\begin{aligned}\left(b\overline{c} = \overline{0}\right) &\iff (bc \equiv 0 \mod a) \iff (a \mid bc) \\ &\iff \left(\frac{a}{\gcd(a,b)} \mid c\right) \qquad \text{(by Lemma 11)} \\ &\iff \left(\frac{ga'}{g} \mid c\right) \qquad \text{(since } a = ga' \text{ and } \gcd(a,b) = g\text{)} \\ &\iff (a' \mid c)\,.\end{aligned}$$

Thus, we can rewrite (8) as

$$\begin{aligned}[C_a \div b] &= |\{c \in \{0,1,\ldots,a-1\} : a' \mid c\}| \\ &= |\{c \in \{0,1,\ldots,ga'-1\} : a' \mid c\}| \qquad \text{(since } a = ga'\text{)} \\ &= |\{\text{the multiples of } a' \text{ between 0 (inclusive) and } ga' \text{ (exclusive)}\}| \\ &= |\{0a', 1a', 2a', \ldots, (g-1)\,a'\}| = g = \gcd(a,b)\,.\end{aligned}$$

□

5 Proofs

We now come to the proofs of Theorem 5 and Corollary 6.

Proof of Theorem 5. A *period* of an n-tuple $a = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ means a positive integer $k \in \{1, 2, 3, \ldots\}$ such that $g^k \cdot a = a$. Clearly, n is a period of each n-tuple. Thus, each n-tuple a has a smallest period. This smallest period must furthermore divide n (because if it does not, then the remainder of n upon division by this smallest period will be an even smaller period of a, which is a contradiction).

Next, we define P_k to be the set of all identity-product tuples in $\mathcal{G}_1^n$ which have smallest period k:

$$P_k := \left\{ a \in \mathcal{G}_1^n : g^k \cdot a = a, \text{ but } g^l \cdot a \neq a \text{ for all } 0 < l < k \right\}. \tag{9}$$

Finally, we define A_k to be the set of all identity-product tuples with period k:

$$A_k := \left\{ a \in \mathcal{G}_1^n : g^k \cdot a = a \right\}. \tag{10}$$

Lemma 13. *For any $k \mid n$, we have*

$$|A_k| = \left[\mathcal{G} \div \frac{n}{k} \right] |\mathcal{G}|^{k-1}. \tag{11}$$

Proof of Lemma 13. By definition, A_k is the set of identity-product tuples fixed by g^k. This implies that if we denote the first k entries of $a \in A_k$ by $\alpha_1, \alpha_2, \ldots, \alpha_k$, then

$$\begin{aligned}
a &= (\alpha_1, \alpha_2, \ldots, \alpha_k, \underbrace{*, \ldots, *}_{(n-k) \text{ entries}}) \\
&= g^k (\alpha_1, \alpha_2, \ldots, \alpha_k, \underbrace{*, \ldots, *}_{(n-k) \text{ entries}}) \\
&= (\underbrace{*, \ldots, *}_{k \text{ entries}}, \alpha_1, \alpha_2, \ldots, \alpha_k, \underbrace{*, \ldots, *}_{(n-2k) \text{ entries}}) \\
&= g^k (\underbrace{*, \ldots, *}_{k \text{ entries}}, \alpha_1, \alpha_2, \ldots, \alpha_k, \underbrace{*, \ldots, *}_{(n-2k) \text{ entries}}) \\
&\quad \vdots \\
&= (\underbrace{*, \ldots, *}_{(n-k) \text{ entries}}, \alpha_1, \alpha_2, \ldots, \alpha_k).
\end{aligned}$$

Comparing every other line entrywise, we conclude that

$$a = (\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_1, \alpha_2, \ldots, \alpha_k, \ldots, \alpha_1, \alpha_2, \ldots, \alpha_k).$$

This means that the whole identity-product tuple $a \in A_k$ is determined by $\alpha_1, \alpha_2, \ldots, \alpha_k$. Moreover, these k elements $\alpha_1, \alpha_2, \ldots, \alpha_k$ must satisfy

$$(\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_k)^{n/k} = 1$$

(in order for the product of the entries of a to be 1). We can thus construct such a tuple a by first choosing the $k-1$ entries $\alpha_1, \alpha_2, \ldots, \alpha_{k-1}$ arbitrarily (there are $|\mathcal{G}|^{k-1}$ many options for this), and then choosing the product $\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_k$ to be any element $a \in \mathcal{G}$ that satisfies $a^{n/k} = 1$ (there are $\left[\mathcal{G} \div \frac{n}{k}\right]$ many such elements); this uniquely determines α_k and therefore the entire tuple a. So the total number of such n-tuples $a \in A_k$ is $|\mathcal{G}|^{k-1} \cdot \left[\mathcal{G} \div \frac{n}{k}\right]$. This proves Lemma 13. □

Lemma 14. *For any positive integer k, we have*

$$|A_k| = \sum_{d \mid k} |P_d| \,. \tag{12}$$

Proof of Lemma 14. Each $a \in A_k$ has some smallest period d, and this d must divide k (since otherwise, the remainder of k upon division by d would be an even smaller period of a). In other words, each $a \in A_k$ belongs to P_d for some $d \mid k$, and this d is obviously unique. Thus,

$$A_k \subseteq \bigsqcup_{d \mid k} P_d. \tag{13}$$

Conversely, if $p \in P_d$ for some $d \mid k$, then the tuple p has smallest period d and thus has period k (since k is a multiple of d), so that p belongs to A_k. Thus,

$$\bigsqcup_{d \mid k} P_d \subseteq A_k.$$

Combined with (13), this leads to

$$A_k = \bigsqcup_{d \mid k} P_d. \tag{14}$$

Hence,

$$|A_k| = \left| \bigsqcup_{d \mid k} P_d \right| = \sum_{d \mid k} |P_d| \,.$$

This proves Lemma 14. □

Now Lemma 7 (applied to $G = C_n$ and $X = \mathcal{G}_1^n$) yields

$$\begin{aligned} |\mathcal{G}_1^n / C_n| &= \frac{1}{|C_n|} \sum_{h \in C_n} |\{a \in \mathcal{G}_1^n : h \cdot a = a\}| \\ &= \frac{1}{n} \sum_{k=1}^{n} \left|\left\{a \in \mathcal{G}_1^n : g^k \cdot a = a\right\}\right| \end{aligned}$$

(since C_n consists of the n elements $g^1, g^2, \ldots, g^n$). Since each $k \in \{1, 2, \ldots, n\}$ satisfies

$$\left|\left\{a \in \mathcal{G}_1^n : g^k \cdot a = a\right\}\right| = |A_k| = \sum_{d|k} |P_d| \qquad \text{(by Lemma 14)},$$

we can rewrite this as

$$|\mathcal{G}_1^n / C_n| = \frac{1}{n} \sum_{k=1}^{n} \sum_{d|k} |P_d|.$$

Since the smallest period of an n-tuple must divide n, we have $|P_d| = 0$ whenever $d \nmid n$. This gives us

$$\frac{1}{n} \sum_{k=1}^{n} \sum_{d|k} |P_d| = \frac{1}{n} \sum_{k=1}^{n} \sum_{\substack{d|k; \\ d|n}} |P_d|.$$

Now we switch the order of the summations:

$$\frac{1}{n} \sum_{k=1}^{n} \sum_{\substack{d|k; \\ d|n}} |P_d| = \frac{1}{n} \sum_{d|n} \sum_{\substack{k \in [1,n]; \\ d|k}} |P_d|.$$

Then we note that there are $\frac{n}{d}$ equal terms in the inner sum since $d \mid k$ is equivalent to k being a multiple of d, so

$$\frac{1}{n} \sum_{d|n} \sum_{\substack{k \in [1,n]; \\ d|k}} |P_d| = \frac{1}{n} \sum_{d|n} \frac{n}{d} |P_d| = \sum_{d|n} \frac{|P_d|}{d}.$$

Combining the previous five equalities, we obtain

$$|\mathcal{G}_1^n / C_n| = \sum_{d|n} \frac{|P_d|}{d}. \tag{15}$$

Let us define two functions f and g from $\{1, 2, 3, \ldots\}$ to $\mathbb{Z}$ by

$$f(k) = |P_k|; \tag{16}$$
$$g(k) = |A_k|. \tag{17}$$

Then the assumption of Lemma 9 is satisfied because of Lemma 14. Hence, the former lemma yields

$$\sum_{d|n} \frac{n}{d} f(d) = \sum_{d|n} \phi\left(\frac{n}{d}\right) g(d).$$

In view of our definitions of f and g and dividing both sides by n, we can rewrite this as

$$\sum_{d|n} \frac{|P_d|}{d} = \frac{1}{n} \sum_{d|n} \phi\left(\frac{n}{d}\right) |A_d| \,.$$

Using (15) for the left hand side and Lemma 13 for the right hand side, we can further rewrite this as

$$|\mathcal{G}_1^n / C_n| = \frac{1}{n} \sum_{d|n} \phi\left(\frac{n}{d}\right) \left[\mathcal{G} \div \frac{n}{d}\right] |\mathcal{G}|^{d-1} \,.$$

This proves Theorem 5. □

Proof of Corollary 6. To begin with, since

$$\mathcal{G} = \prod_{i=1}^{m} C_{k_i}, \tag{18}$$

we can compute the size

$$|\mathcal{G}| = \left|\prod_{i=1}^{m} C_{k_i}\right| = \prod_{i=1}^{m} |C_{k_i}| = \prod_{i=1}^{m} k_i. \tag{19}$$

Now we need to compute $\left[\mathcal{G} \div \frac{n}{d}\right]$ for each $d \mid n$. Any finite groups $H_1, H_2, \ldots, H_m$ and any integer k satisfy

$$\left[\prod_{i=1}^{m} H_i \div k\right] = \prod_{i=1}^{m} \left[H_i \div k\right],$$

since k-th powers in a direct product are taken entrywise. Thus, from (18), we obtain

$$\left[\mathcal{G} \div \frac{n}{d}\right] = \prod_{i=1}^{m} \left[C_{k_i} \div \frac{n}{d}\right] = \prod_{i=1}^{m} \gcd\left(k_i, \frac{n}{d}\right) \tag{20}$$

(where we used Lemma 12 in the last step). The claim of Theorem 5 thus becomes

$$\begin{aligned}
|\mathcal{G}_1^n / C_n| &= \frac{1}{n} \sum_{d|n} \phi\left(\frac{n}{d}\right) \left[\mathcal{G} \div \frac{n}{d}\right] |\mathcal{G}|^{d-1} \\
&= \frac{1}{n} \sum_{d|n} \phi\left(\frac{n}{d}\right) \left(\prod_{i=1}^{m} \gcd\left(k_i, \frac{n}{d}\right)\right) \left(\prod_{i=1}^{m} k_i\right)^{d-1} \qquad \text{(by (19) and (20))} \\
&= \frac{1}{n} \sum_{d|n} \phi\left(\frac{n}{d}\right) \prod_{i=1}^{m} \left(\gcd\left(k_i, \frac{n}{d}\right) k_i^{d-1}\right).
\end{aligned}$$

□

6 Main theorem II: Aperiodic necklaces

After having computed the total number of identity-product n-necklaces for a given finite group $\mathcal{G}$, we can further restrict ourselves to just those necklaces which are aperiodic.

We declare an identity-product n-necklace N to be *aperiodic* if it contains n distinct n-tuples. In other words, a necklace $N = \{a, g \cdot a, g^2 \cdot a, \ldots, g^{n-1} \cdot a\} \subseteq \mathcal{G}_1^n$ is aperiodic if and only if no two of the tuples $a, g \cdot a, g^2 \cdot a, \ldots, g^{n-1} \cdot a$ are equal. This latter condition is equivalent to $a \in P_n$, where we use the notation P_k introduced in (9) (since $g^n \cdot a = a$ holds automatically). Thus, each aperiodic necklace in $\mathcal{G}_1^n$ contains n distinct tuples in P_n, and each tuple in P_n is contained in a unique aperiodic necklace in $\mathcal{G}_1^n$. Hence, the number of aperiodic necklaces in $\mathcal{G}_1^n$ is $\dfrac{|P_n|}{n}$.

Therefore, it suffices to compute $|P_n|$. To compute it, we need another number-theoretic function instead of the Euler totient function:

Definition 15. We define the Möbius function $\mu : \{1, 2, 3, \ldots\} \to \mathbb{Z}$ by

$$\mu(n) = \begin{cases} (-1)^m, & \text{if } n \text{ is a product of } m \text{ distinct primes;} \\ 0, & \text{otherwise.} \end{cases}$$

Theorem 16. *Let n be a positive integer. The number $\frac{|P_n|}{n}$ of aperiodic identity-product n-necklaces is*

$$\frac{|P_n|}{n} = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) \left[\mathcal{G} \div \frac{n}{d}\right] |\mathcal{G}|^{d-1}.$$

Our proof of this theorem relies on the *Möbius inversion formula*, a classical result in elementary number theory (see, e.g., [21, Theorem 2.39 and the paragraph that follows]):

Lemma 17. *Let f and g be two functions from $\{1, 2, 3, \ldots\}$ to $\mathbb{Q}$. Assume that*

$$g(k) = \sum_{d|k} f(d) \qquad \text{for each } k \geq 1.$$

Then

$$f(k) = \sum_{d|k} \mu(d) g\left(\frac{k}{d}\right) \qquad \text{for each } k \geq 1.$$

Proof of Theorem 16. Let us define two functions f and g from $\{1, 2, 3, \ldots\}$ to $\mathbb{Z}$ by

$$f(k) = |P_k|, \tag{21}$$
$$g(k) = |A_k|. \tag{22}$$

Then the assumption of Lemma 17 is satisfied because of Lemma 14. Hence, Lemma 17 yields

$$|P_k| = \sum_{d|k} \mu(d) \left| A_{\frac{k}{d}} \right| \tag{23}$$

for all $k \geq 1$. Dividing both sides by n and setting $k = n$, this becomes

$$\frac{|P_n|}{n} = \frac{1}{n} \sum_{d|n} \mu(d) \left| A_{\frac{n}{d}} \right| .$$

We can substitute d for $\frac{n}{d}$ in the sum on the right, since the map $d \mapsto \frac{n}{d}$ is a bijection from the set of positive divisors of n to itself. This yields

$$\frac{|P_n|}{n} = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) |A_d| . \tag{24}$$

Finally, we use Lemma 13 to rewrite this as

$$\frac{|P_n|}{n} = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) \left[\mathcal{G} \div \frac{n}{d}\right] |\mathcal{G}|^{d-1} \tag{25}$$

which concludes the proof. □

On top of the special case of aperiodic necklaces, let us consider the case of identity-product n-necklaces with smallest period k. Here we declare an n-necklace N to have *smallest period* k when $|N| = k$. Equivalently, an n-necklace $N = \{a, g \cdot a, g^2 \cdot a, \ldots, g^{n-1} \cdot a\} \subseteq \mathcal{G}_1^n$ has smallest period k if and only if the n-tuple a has smallest period k. This is because if k is the smallest period of an n-tuple a, then the first k of the n-tuples $a, g \cdot a, g^2 \cdot a, \ldots, g^{n-1} \cdot a$ are distinct, while all following tuples are repetitions of them. Thus, each identity-product n-necklace with smallest period k contains k distinct tuples in P_k. Hence, the number of these necklaces is $\frac{|P_k|}{k}$.

Corollary 18. *Let n and k be positive integers with $k \mid n$. The number $\frac{|P_k|}{k}$ of identity-product n-necklaces with smallest period k is*

$$\frac{|P_k|}{k} = \frac{1}{k} \sum_{d|k} \mu\left(\frac{k}{d}\right) \left[\mathcal{G} \div \frac{n}{d}\right] |\mathcal{G}|^{d-1} .$$

Proof. Recall that in the proof of Theorem 16, we proved the general equation (23). That is,

$$|P_k| = \sum_{d|k} \mu(d) \left| A_{\frac{k}{d}} \right| .$$

By bijective substitution of d with $\frac{k}{d}$ on the positive divisors of k to themselves, this can be turned into

$$|P_k| = \sum_{d|k} \mu\left(\frac{k}{d}\right) |A_d| .$$

We can rewrite the right hand side using Lemma 13, applied to d instead of k (since $d \mid k \mid n$). The above equality thus takes the form

$$|P_k| = \sum_{d|k} \mu\left(\frac{k}{d}\right) \left[\mathcal{G} \div \frac{n}{d}\right] |\mathcal{G}|^{d-1} . \tag{26}$$

Now, dividing both sides by k, we obtain

$$\frac{|P_k|}{k} = \frac{1}{k} \sum_{d|k} \mu\left(\frac{k}{d}\right) \left[\mathcal{G} \div \frac{n}{d}\right] |\mathcal{G}|^{d-1} . \tag{27}$$

□

7 Main theorem III: Homogeneous necklaces

An interesting variant of necklaces was proposed by Gilbert and Riordan [9]. They count n-tuples of elements of the cyclic group C_q (which they write additively, as $\mathbb{Z}/q$), but identifying each n-tuple not only with its cyclic rotations, but also with all the other n-tuples that can be obtained by multiplying all its entries by the same element of C_q. For instance, for $q = 3$ and $n = 3$, each n-tuple $(a, b, c) \in C_q^n = C_3^3$ thus ends up in a single equivalence class with (b, c, a), (c, a, b), (ga, gb, gc), (gb, gc, ga), (gc, ga, gb), (g^2a, g^2b, g^2c), (g^2b, g^2c, g^2a) and (g^2c, g^2a, g^2b). Such equivalence classes can be called "homogeneous necklaces". They were first considered for $q = 2$ by Fine [6], motivated by psychometric experiments.

The "homogeneous necklaces" can also be generalized to an arbitrary finite group $\mathcal{G}$ instead of C_q. Rather than introduce custom terminology for them, we shall define them as the orbits of a group action:

As before, $\mathcal{G}$ is a finite group. We also fix a positive integer n. Consider the cyclic group $C_n = \{g^0, g^1, \ldots, g^{n-1}\}$ with generator g.

We recall that the cyclic group C_n acts (from the left) on $\mathcal{G}^n$ by rotating n-tuples: If $i \in \mathbb{Z}$, then the element $g^i \in C_n$ acts on an n-tuple by rotating this n-tuple i steps to the right.

The group $\mathcal{G}$ also acts from the left on $\mathcal{G}^n$, by the rule

$$h \cdot (a_1, a_2, \ldots, a_n) = (ha_1,\ ha_2,\ \ldots,\ ha_n)$$
$$\text{for all } h \in \mathcal{G} \text{ and } (a_1, a_2, \ldots, a_n) \in \mathcal{G}^n.$$

Thus, an element $h \in \mathcal{G}$ acts on an n-tuple $a \in \mathcal{G}^n$ by multiplying all entries of a by h from the left.

The two actions (of C_n and of $\mathcal{G}$) on $\mathcal{G}^n$ commute, meaning that

$$g^i \cdot (h \cdot a) = h \cdot \left(g^i \cdot a\right) \qquad \text{for all } g^i \in C_n \text{ and } h \in \mathcal{G} \text{ and } a \in \mathcal{G}^n.$$

(This is intuitively obvious: Multiplying all entries of a by h can be done either before or after a cyclic rotation; the outcome will be the same.)

This commutativity allows us to combine the actions of C_n and of $\mathcal{G}$ into a single action of the direct product $C_n \times \mathcal{G}$ on $\mathcal{G}^n$. Explicitly, the group $C_n \times \mathcal{G}$ acts from the left on $\mathcal{G}^n$ by the rule

$$\left(g^i, h\right) \cdot a = g^i \cdot (h \cdot a) = h \cdot \left(g^i \cdot a\right)$$
$$\text{for all } g^i \in C_n \text{ and } h \in \mathcal{G} \text{ and } a \in \mathcal{G}^n.$$

Thus, a pair (g^i, h) acts on an n-tuple $a \in \mathcal{G}^n$ by rotating the n-tuple i steps to the right and multiplying each entry by h from the left. The orbits of this action can be called the "homogeneous n-necklaces", though we shall just refer to them as orbits. Now, we claim the following:

Theorem 19. *The number $\left|\mathcal{G}^n / \left(C_n \times \mathcal{G}\right)\right|$ of all orbits of the action of $C_n \times \mathcal{G}$ on $\mathcal{G}^n$ equals the number $\left|\mathcal{G}_1^n / C_n\right|$ of all identity-product n-necklaces. Thus,*

$$\left|\mathcal{G}^n / \left(C_n \times \mathcal{G}\right)\right| = \left|\mathcal{G}_1^n / C_n\right| = \frac{1}{n} \sum_{d \mid n} \phi\left(\frac{n}{d}\right) \left[\mathcal{G} \div \frac{n}{d}\right] |\mathcal{G}|^{d-1}.$$

This is implicitly claimed in the OEIS (On-Line Encyclopedia of Integer Sequences) entry for sequence A000013 for the case $\mathcal{G} = C_2$ (see also https://math.stackexchange.com/questions/3249602), but the general case appears new. We prove the general case bijectively:

Proof of Theorem 19. If i is any integer, then the residue class of i modulo n will be denoted by $\overline{i}$. For instance, $\overline{n} = \overline{0}$.

If $a \in \mathcal{G}^n$ is an n-tuple, then the i-th entry of a (for any given $i \in \{1, 2, \ldots, n\}$) will be denoted by $a_{\overline{i}}$ (so that $a = \left(a_{\overline{1}}, a_{\overline{2}}, \ldots, a_{\overline{n}}\right)$ and $a_{\overline{0}} = a_{\overline{n}}$ and $a_{\overline{n+1}} = a_{\overline{1}}$). Thus, the entries of our n-tuples are now indexed by elements of $\mathbb{Z}/n$. If $a \in \mathcal{G}^n$ is an n-tuple, then a_r is hence defined for any residue class $r \in \mathbb{Z}/n$.

Note that the action of C_n on $\mathcal{G}^n$ can thus be described by the equality

$$\left(g^i \cdot a\right)_{\overline{j}} = a_{\overline{j-i}} \tag{28}$$

for all $g^i \in C_n$ (that is, all $i \in \mathbb{Z}$), all $a \in \mathcal{G}^n$ and all $j \in \mathbb{Z}$.

Likewise, the action of $\mathcal{G}$ on $\mathcal{G}^n$ can be described by the equality

$$(h \cdot a)_{\overline{j}} = h a_{\overline{j}} \tag{29}$$

for all $h \in \mathcal{G}$, all $a \in \mathcal{G}^n$ and all $j \in \mathbb{Z}$.

Hence, for all $g^i \in C_n$, all $h \in \mathcal{G}$, all $a \in \mathcal{G}^n$ and all $j \in \mathbb{Z}$, we have

$$\begin{aligned}\left(\left(g^i, h\right) \cdot a\right)_{\overline{j}} &= \left(g^i \cdot (h \cdot a)\right)_{\overline{j}} \qquad \left(\text{since } \left(g^i, h\right) \cdot a = g^i \cdot (h \cdot a)\right) \\ &= (h \cdot a)_{\overline{j-i}} \qquad (\text{by (28), applied to } h \cdot a \text{ instead of } a) \\ &= h a_{\overline{j-i}} \end{aligned} \tag{30}$$

(by (30), applied to $j - i$ instead of j).

If $a \in \mathcal{G}^n$ is any n-tuple, then

$$\left(a_{\overline{0}}^{-1} a_{\overline{1}},\ a_{\overline{1}}^{-1} a_{\overline{2}},\ a_{\overline{2}}^{-1} a_{\overline{3}},\ \ldots,\ a_{\overline{n-1}}^{-1} a_{\overline{n}}\right) \in \mathcal{G}_1^n,$$

since

$$\begin{aligned} a_{\overline{0}}^{-1} a_{\overline{1}} \cdot a_{\overline{1}}^{-1} a_{\overline{2}} \cdot a_{\overline{2}}^{-1} a_{\overline{3}} \cdot \cdots \cdot a_{\overline{n-1}}^{-1} a_{\overline{n}} &= a_{\overline{0}}^{-1} a_{\overline{n}} \qquad (\text{by the telescope principle}) \\ &= 1 \qquad \left(\text{since } a_{\overline{n}} = a_{\overline{0}} \ (\text{since } \overline{n} = \overline{0})\right). \end{aligned}$$

Thus, we can define a map

$$\begin{aligned} \Delta : \mathcal{G}^n &\to \mathcal{G}_1^n, \\ a &\mapsto \left(a_{\overline{0}}^{-1} a_{\overline{1}},\ a_{\overline{1}}^{-1} a_{\overline{2}},\ a_{\overline{2}}^{-1} a_{\overline{3}},\ \ldots,\ a_{\overline{n-1}}^{-1} a_{\overline{n}}\right). \end{aligned}$$

This map Δ satisfies the equality

$$\left(\Delta\left(a\right)\right)_{\overline{j}} = a_{\overline{j-1}}^{-1} a_{\overline{j}} \tag{31}$$

for all $a \in \mathcal{G}^n$ and $j \in \mathbb{Z}$.

Proof of (31). Let $a \in \mathcal{G}^n$. The definition of Δ shows that

$$\Delta\left(a\right) = \left(a_{\overline{0}}^{-1} a_{\overline{1}},\ a_{\overline{1}}^{-1} a_{\overline{2}},\ a_{\overline{2}}^{-1} a_{\overline{3}},\ \ldots,\ a_{\overline{n-1}}^{-1} a_{\overline{n}}\right).$$

Hence, the equality $\left(\Delta\left(a\right)\right)_{\overline{j}} = a_{\overline{j-1}}^{-1} a_{\overline{j}}$ holds for each $j \in \{1, 2, \ldots, n\}$. But both sides of this equality—considered as functions of j—are periodic with a period of n (since $\overline{j}$ and $\overline{j-1}$ are periodic with a period of n). Therefore, having shown that this equality holds for all $j \in \{1, 2, \ldots, n\}$, we automatically conclude that it must hold for all $j \in \mathbb{Z}$. This proves (31). $\square$

Next we claim the following property of Δ:

> *Claim 1:* If two n-tuples $a \in \mathcal{G}^n$ and $b \in \mathcal{G}^n$ belong to the same $C_n \times \mathcal{G}$-orbit, then their images $\Delta\left(a\right)$ and $\Delta\left(b\right)$ belong to the same C_n-orbit.

Proof of Claim 1. Let $a \in \mathcal{G}^n$ and $b \in \mathcal{G}^n$ belong to the same $C_n \times \mathcal{G}$-orbit. Thus, $b = (g^i, h) \cdot a$ for some $g^i \in C_n$ and $h \in \mathcal{G}$. Consider these g^i and h. Thus, for each $j \in \mathbb{Z}$, we have

$$b_{\overline{j}} = \left(\left(g^i, h\right) \cdot a\right)_{\overline{j}} = h a_{\overline{j-i}} \qquad \text{(by (30))}$$

and

$$b_{\overline{j-1}} = h a_{\overline{j-1-i}} \qquad \text{(similarly)}$$

and

$$\begin{aligned}
\left(\Delta\left(b\right)\right)_{\overline{j}} &= b_{\overline{j-1}}^{-1} b_{\overline{j}} \qquad \text{(by (31), applied to } b \text{ instead of } a\text{)} \\
&= \left(h a_{\overline{j-1-i}}\right)^{-1} \left(h a_{\overline{j-i}}\right) \qquad \left(\text{since } b_{\overline{j}} = h a_{\overline{j-i}} \text{ and } b_{\overline{j-1}} = h a_{\overline{j-1-i}}\right) \\
&= \underbrace{a_{\overline{j-1-i}}^{-1}}_{= a_{\overline{j-i-1}}^{-1}} \underbrace{h^{-1} h}_{=1} a_{\overline{j-i}} = a_{\overline{j-i-1}}^{-1} a_{\overline{j-i}}. \qquad (32)
\end{aligned}$$

However, for each $j \in \mathbb{Z}$, we have

$$\begin{aligned}
\left(g^i \cdot \Delta\left(a\right)\right)_{\overline{j}} &= \left(\Delta\left(a\right)\right)_{\overline{j-i}} \qquad \text{(by (28), applied to } \Delta\left(a\right) \text{ instead of } a\text{)} \\
&= a_{\overline{j-i-1}}^{-1} a_{\overline{j-i}} \qquad \text{(by (31), applied to } j-i \text{ instead of } j\text{)}.
\end{aligned}$$

Comparing this with (32), we obtain

$$\left(\Delta\left(b\right)\right)_{\overline{j}} = \left(g^i \cdot \Delta\left(a\right)\right)_{\overline{j}} \qquad \text{for each } j \in \mathbb{Z}.$$

In other words, each entry of $\Delta\left(b\right)$ equals the corresponding entry of $g^i \cdot \Delta\left(a\right)$. Hence, $\Delta\left(b\right) = g^i \cdot \Delta\left(a\right)$. This shows that $\Delta\left(a\right)$ and $\Delta\left(b\right)$ belong to the same C_n-orbit. Claim 1 is thus proved. $\square$

Next, we define a map

$$\begin{aligned}
\Gamma : \mathcal{G}_1^n &\to \mathcal{G}^n, \\
a &\mapsto \left(a_{\overline{1}},\ a_{\overline{1}} a_{\overline{2}},\ a_{\overline{1}} a_{\overline{2}} a_{\overline{3}},\ \ldots,\ a_{\overline{1}} a_{\overline{2}} \cdots a_{\overline{n}}\right).
\end{aligned}$$

Thus, this map Γ is given by the rule

$$\left(\Gamma\left(a\right)\right)_{\overline{j}} = a_{\overline{1}} a_{\overline{2}} \cdots a_{\overline{j}} \qquad (33)$$

for all $a \in \mathcal{G}^n$ and $j \in \{1, 2, \ldots, n\}$. When a is an identity-product n-tuple, we can extend this rule a bit further: For any $a \in \mathcal{G}_1^n$, we have

$$\left(\Gamma\left(a\right)\right)_{\overline{j}} = a_{\overline{1}} a_{\overline{2}} \cdots a_{\overline{j}} \qquad \text{for all } j \in \{0, 1, \ldots, n\}. \qquad (34)$$

Proof of (34). Let $a \in \mathcal{G}_1^n$. Let $j \in \{0, 1, \ldots, n\}$. We must prove (34). If $j \neq 0$, then $j \in \{1, 2, \ldots, n\}$, and thus (34) follows directly from (33) in this case. Thus, it remains to prove (34) for $j = 0$. In other words, it remains to prove that $(\Gamma(a))_{\overline{0}} = a_{\overline{1}} a_{\overline{2}} \cdots a_{\overline{0}}$. Since the empty product $a_{\overline{1}} a_{\overline{2}} \cdots a_{\overline{0}}$ is 1 by definition, this means proving that $(\Gamma(a))_{\overline{0}} = 1$. But this is easy: We have $\overline{0} = \overline{n}$, so that $(\Gamma(a))_{\overline{0}} = (\Gamma(a))_{\overline{n}} = a_{\overline{1}} a_{\overline{2}} \cdots a_{\overline{n}}$ (by (33)). But $(a_{\overline{1}}, a_{\overline{2}}, \ldots, a_{\overline{n}}) = a \in \mathcal{G}_1^n$, and thus $a_{\overline{1}} a_{\overline{2}} \cdots a_{\overline{n}} = 1$ (by the definition of $\mathcal{G}_1^n$). Hence, $(\Gamma(a))_{\overline{0}} = a_{\overline{1}} a_{\overline{2}} \cdots a_{\overline{n}} = 1$, just as we desired to prove. Thus the proof of (34) is complete. $\square$

Next, let us prove an analogue of Claim 1 for the map Γ:

> *Claim 2:* If two n-tuples $a \in \mathcal{G}_1^n$ and $b \in \mathcal{G}_1^n$ belong to the same C_n-orbit, then their images $\Gamma(a)$ and $\Gamma(b)$ belong to the same $C_n \times \mathcal{G}$-orbit.

Proof of Claim 2. We define a binary relation $\sim$ on the set $\mathcal{G}^n$ by

$$(u \sim v) \iff (u \text{ and } v \text{ belong to the same } C_n \times \mathcal{G}\text{-orbit}).$$

Clearly, this relation $\sim$ is an equivalence relation.

Now let us show that every $a \in \mathcal{G}_1^n$ satisfies

$$\Gamma(a) \sim \Gamma(g \cdot a). \tag{35}$$

Indeed, fix $a \in \mathcal{G}_1^n$. We shall show that $\Gamma(g \cdot a) = (g^1, a_{\overline{n}}) \cdot \Gamma(a)$ (where the pair $(g^1, a_{\overline{n}}) \in C_n \times \mathcal{G}$ acts on $\Gamma(a)$ via the $C_n \times \mathcal{G}$-action on $\mathcal{G}^n$ defined above).

First we observe that $g \cdot a = (a_{\overline{n}}, a_{\overline{1}}, a_{\overline{2}}, \ldots, a_{\overline{n-1}})$ by the definition of the C_n-action on $\mathcal{G}^n$. Thus, $(g \cdot a)_{\overline{1}} = a_{\overline{n}}$ and

$$(g \cdot a)_{\overline{i}} = a_{\overline{i-1}} \qquad \text{for each } i \in \mathbb{Z}. \tag{36}$$

Now, let $k \in \{1, 2, \ldots, n\}$. Then (33) (applied to $g \cdot a$ and k instead of a and j) shows that

$$\begin{aligned}
(\Gamma(g \cdot a))_{\overline{k}} &= (g \cdot a)_{\overline{1}} (g \cdot a)_{\overline{2}} \cdots (g \cdot a)_{\overline{k}} \\
&= \underbrace{(g \cdot a)_{\overline{1}}}_{= a_{\overline{n}}} \cdot \underbrace{(g \cdot a)_{\overline{2}}}_{\substack{= a_{\overline{1}} \\ \text{(by (36))}}} \underbrace{(g \cdot a)_{\overline{3}}}_{\substack{= a_{\overline{2}} \\ \text{(by (36))}}} \cdots \underbrace{(g \cdot a)_{\overline{k}}}_{\substack{= a_{\overline{k-1}} \\ \text{(by (36))}}} \\
&= a_{\overline{n}} \cdot a_{\overline{1}} a_{\overline{2}} \cdots a_{\overline{k-1}}.
\end{aligned} \tag{37}$$

On the other hand, from $k \in \{1, 2, \ldots, n\}$, we obtain $k - 1 \in \{0, 1, \ldots, n\}$. Hence, (34) (applied to $j = k - 1$) yields $(\Gamma(a))_{\overline{k-1}} = a_{\overline{1}} a_{\overline{2}} \cdots a_{\overline{k-1}}$. But (30) (applied to 1, $a_{\overline{n}}$, $\Gamma(a)$ and k instead of i, h, a and j) yields

$$\left(\left(g^1, a_{\overline{n}}\right) \cdot \Gamma(a)\right)_{\overline{k}} = a_{\overline{n}} \cdot \underbrace{(\Gamma(a))_{\overline{k-1}}}_{= a_{\overline{1}} a_{\overline{2}} \cdots a_{\overline{k-1}}} = a_{\overline{n}} \cdot a_{\overline{1}} a_{\overline{2}} \cdots a_{\overline{k-1}}.$$

Comparing this with (37), we see that

$$\left(\Gamma\left(g\cdot a\right)\right)_{\overline{k}} = \left(\left(g^1, a_{\overline{n}}\right)\cdot\Gamma\left(a\right)\right)_{\overline{k}}.$$

Forget that we fixed k. We thus have shown that $\left(\Gamma\left(g\cdot a\right)\right)_{\overline{k}} = \left(\left(g^1, a_{\overline{n}}\right)\cdot\Gamma\left(a\right)\right)_{\overline{k}}$ for each $k\in\{1,2,\ldots,n\}$. In other words, each entry of the n-tuple $\Gamma\left(g\cdot a\right)$ equals the corresponding entry of $\left(g^1, a_{\overline{n}}\right)\cdot\Gamma\left(a\right)$. Hence,

$$\Gamma\left(g\cdot a\right) = \left(g^1, a_{\overline{n}}\right)\cdot\Gamma\left(a\right).$$

Thus, the two n-tuples $\Gamma\left(a\right)$ and $\Gamma\left(g\cdot a\right)$ belong to the same $C_n\times\mathcal{G}$-orbit. By the definition of the relation $\sim$, this means that $\Gamma\left(a\right)\sim\Gamma\left(g\cdot a\right)$. Thus, (35) is proved.

Now, let $a\in\mathcal{G}_1^n$ and $b\in\mathcal{G}_1^n$ be two n-tuples that belong to the same C_n-orbit. We must prove that their images $\Gamma\left(a\right)$ and $\Gamma\left(b\right)$ belong to the same $C_n\times\mathcal{G}$-orbit. In other words, we must prove that $\Gamma\left(a\right)\sim\Gamma\left(b\right)$.

We have assumed that a and b belong to the same C_n-orbit. In other words, $a=\gamma\cdot b$ for some $\gamma\in C_n$. Consider this γ. Thus, $\gamma\in C_n = \{g^0, g^1, \ldots, g^{n-1}\}$. In other words, $\gamma = g^i$ for some $i\in\{0,1,\ldots,n-1\}$. Consider this i. Now, for each $k\in\mathbb{N}$, we have

$$\Gamma\left(g^k\cdot b\right)\sim\Gamma\left(g^{k+1}\cdot b\right) \tag{38}$$

(since (35) (applied to $g^k\cdot b$ instead of a) yields $\Gamma\left(g^k\cdot b\right)\sim\Gamma\left(\underbrace{g\cdot g^k}_{=g^{k+1}}\cdot b\right) = \Gamma\left(g^{k+1}\cdot b\right)$).

Hence, we obtain a chain of relations

$$\Gamma\left(g^0\cdot b\right)\sim\Gamma\left(g^1\cdot b\right)\sim\Gamma\left(g^2\cdot b\right)\sim\cdots.$$

Since $\sim$ is an equivalence relation, this yields $\Gamma\left(g^i\cdot b\right)\sim\Gamma\left(g^0\cdot b\right)$ in particular. In view of $g^i=\gamma$ and $g^0=1$, we can rewrite this as $\Gamma\left(\gamma\cdot b\right)\sim\Gamma\left(1\cdot b\right)$. In other words, $\Gamma\left(a\right)\sim\Gamma\left(b\right)$ (since $a=\gamma\cdot b$ and $b=1\cdot b$). Hence, Claim 2 is proved. □

Now, the map

$$\begin{aligned}\overline{\Delta}: \mathcal{G}^n/\left(C_n\times\mathcal{G}\right) &\to \mathcal{G}_1^n/C_n,\\ \left(C_n\times\mathcal{G}\text{-orbit of } a\right) &\mapsto \left(C_n\text{-orbit of } \Delta\left(a\right)\right)\end{aligned}$$

is well-defined (by Claim 1), and so is the map

$$\begin{aligned}\overline{\Gamma}: \mathcal{G}_1^n/C_n &\to \mathcal{G}^n/\left(C_n\times\mathcal{G}\right),\\ \left(C_n\text{-orbit of } a\right) &\mapsto \left(C_n\times\mathcal{G}\text{-orbit of } \Gamma\left(a\right)\right)\end{aligned}$$

(by Claim 2). We shall now prove that these two maps $\overline{\Delta}$ and $\overline{\Gamma}$ are mutually inverse. We do this through two claims:

Claim 3: We have $\overline{\Gamma} \circ \overline{\Delta} = \mathrm{id}$.

Proof of Claim 3. Let $x \in \mathcal{G}^n / (C_n \times \mathcal{G})$ be arbitrary. Thus, x is the $C_n \times \mathcal{G}$-orbit of some $a \in \mathcal{G}^n$. Consider this a. Thus, the definition of $\overline{\Delta}$ shows that $\overline{\Delta}(x)$ is the C_n-orbit of $\Delta(a)$. Hence, the definition of $\overline{\Gamma}$ shows that $\overline{\Gamma}\left(\overline{\Delta}(x)\right)$ is the $C_n \times \mathcal{G}$-orbit of $\Gamma(\Delta(a))$. We shall now show that $\Gamma(\Delta(a))$ and a belong to the same $C_n \times \mathcal{G}$-orbit. More specifically, we shall show that $\Gamma(\Delta(a)) = \left(g^0, a_{\overline{0}}^{-1}\right) \cdot a$, where the pair $\left(g^0, a_{\overline{0}}^{-1}\right) \in C_n \times \mathcal{G}$ acts on a via the $C_n \times \mathcal{G}$-action on $\mathcal{G}^n$.

For each $k \in \{1, 2, \ldots, n\}$, we have

$$\begin{aligned}
(\Gamma(\Delta(a)))_{\overline{k}} &= \underbrace{(\Delta(a))_{\overline{1}}}_{\substack{=a_{\overline{0}}^{-1} a_{\overline{1}} \\ \text{(by (31))}}} \cdot \underbrace{(\Delta(a))_{\overline{2}}}_{\substack{=a_{\overline{1}}^{-1} a_{\overline{2}} \\ \text{(by (31))}}} \cdot \cdots \cdot \underbrace{(\Delta(a))_{\overline{k}}}_{\substack{=a_{\overline{k-1}}^{-1} a_{\overline{k}} \\ \text{(by (31))}}} \\
&\qquad \text{(by (33), applied to } \Delta(a) \text{ and } k \text{ instead of } a \text{ and } j\text{)} \\
&= a_{\overline{0}}^{-1} a_{\overline{1}} \cdot a_{\overline{1}}^{-1} a_{\overline{2}} \cdot \cdots \cdot a_{\overline{k-1}}^{-1} a_{\overline{k}} \\
&= a_{\overline{0}}^{-1} a_{\overline{k}} \qquad \text{(by the telescope principle)}
\end{aligned}$$

and

$$\begin{aligned}
\left(\left(g^0, a_{\overline{0}}^{-1}\right) \cdot a\right)_{\overline{k}} &= a_{\overline{0}}^{-1} a_{\overline{k-0}} \qquad \left(\text{by (30), applied to } i = 0 \text{ and } h = a_{\overline{0}}^{-1} \text{ and } j = k\right) \\
&= a_{\overline{0}}^{-1} a_{\overline{k}} \qquad (\text{since } k - 0 = k).
\end{aligned}$$

Comparing these two equalities, we see that

$$(\Gamma(\Delta(a)))_{\overline{k}} = \left(\left(g^0, a_{\overline{0}}^{-1}\right) \cdot a\right)_{\overline{k}} \qquad \text{for each } k \in \{1, 2, \ldots, n\}.$$

In other words, each entry of the n-tuple $\Gamma(\Delta(a))$ equals the corresponding entry of $\left(g^0, a_{\overline{0}}^{-1}\right) \cdot a$. Hence, $\Gamma(\Delta(a)) = \left(g^0, a_{\overline{0}}^{-1}\right) \cdot a$. Therefore, $\Gamma(\Delta(a))$ and a belong to the same $C_n \times \mathcal{G}$-orbit. In other words, the $C_n \times \mathcal{G}$-orbit of $\Gamma(\Delta(a))$ is precisely the $C_n \times \mathcal{G}$-orbit of a. In other words, $\overline{\Gamma}\left(\overline{\Delta}(x)\right) = x$ (since $\overline{\Gamma}\left(\overline{\Delta}(x)\right)$ is the $C_n \times \mathcal{G}$-orbit of $\Gamma(\Delta(a))$, whereas x is the $C_n \times \mathcal{G}$-orbit of a).

Forget that we fixed x. We thus have shown that $\overline{\Gamma}\left(\overline{\Delta}(x)\right) = x$ for each $x \in \mathcal{G}^n / (C_n \times \mathcal{G})$. In other words, $\overline{\Gamma} \circ \overline{\Delta} = \mathrm{id}$. This proves Claim 3. $\square$

Claim 4: We have $\overline{\Delta} \circ \overline{\Gamma} = \mathrm{id}$.

Proof of Claim 4. Let $x \in \mathcal{G}_1^n / C_n$ be arbitrary. Thus, x is the C_n-orbit of some $a \in \mathcal{G}_1^n$. Consider this a. Hence, the definition of $\overline{\Gamma}$ shows that $\overline{\Gamma}(x)$ is the $C_n \times \mathcal{G}$-orbit of $\Gamma(a)$. Therefore, the definition of $\overline{\Delta}$ shows that $\overline{\Delta}\left(\overline{\Gamma}(x)\right)$ is the C_n-orbit of $\Delta(\Gamma(a))$. We shall now show that $\Delta(\Gamma(a)) = a$.

Let $k \in \{1, 2, \ldots, n\}$. Then (31) (applied to $\Gamma(a)$ and k instead of a and j) yields

$$\begin{aligned}
(\Delta(\Gamma(a)))_{\overline{k}} &= (\Gamma(a))_{\overline{k-1}}^{-1} \cdot (\Gamma(a))_{\overline{k}} \\
&= \left(a_{\overline{1}} a_{\overline{2}} \cdots a_{\overline{k-1}}\right)^{-1} \cdot \left(a_{\overline{1}} a_{\overline{2}} \cdots a_{\overline{k}}\right)
\end{aligned}$$

(since (34) shows that $(\Gamma(a))_{\overline{k}} = a_{\overline{1}}a_{\overline{2}}\cdots a_{\overline{k}}$ and $(\Gamma(a))_{\overline{k-1}} = a_{\overline{1}}a_{\overline{2}}\cdots a_{\overline{k-1}}$ (because $k-1 \in \{0,1,\ldots,n\}$)). Thus,

$$\begin{aligned}(\Delta(\Gamma(a)))_{\overline{k}} &= \left(a_{\overline{1}}a_{\overline{2}}\cdots a_{\overline{k-1}}\right)^{-1} \cdot \left(a_{\overline{1}}a_{\overline{2}}\cdots a_{\overline{k}}\right) \\ &= a_{\overline{k}} \qquad \left(\text{since } a_{\overline{1}}a_{\overline{2}}\cdots a_{\overline{k}} = \left(a_{\overline{1}}a_{\overline{2}}\cdots a_{\overline{k-1}}\right)\cdot a_{\overline{k}}\right).\end{aligned}$$

Forget that we fixed k. We have thus shown that $(\Delta(\Gamma(a)))_{\overline{k}} = a_{\overline{k}}$ for each $k \in \{1,2,\ldots,n\}$. In other words, each entry of the n-tuple $\Delta(\Gamma(a))$ equals the corresponding entry of a. Hence, $\Delta(\Gamma(a)) = a$. Therefore, $\overline{\Delta}\left(\overline{\Gamma}(x)\right) = x$ (since $\overline{\Delta}\left(\overline{\Gamma}(x)\right)$ is the C_n-orbit of $\Delta(\Gamma(a))$, whereas x is the C_n-orbit of a).

Forget that we fixed x. We thus have shown that $\overline{\Delta}\left(\overline{\Gamma}(x)\right) = x$ for each $x \in \mathcal{G}_1^n/C_n$. In other words, $\overline{\Delta} \circ \overline{\Gamma} = \mathrm{id}$. This proves Claim 4. □

Combining Claim 3 with Claim 4, we see that the maps $\overline{\Delta}$ and $\overline{\Gamma}$ are mutually inverse. In particular, $\overline{\Delta} : \mathcal{G}^n/(C_n \times \mathcal{G}) \to \mathcal{G}_1^n/C_n$ is an invertible map, i.e., a bijection. Hence, by the bijection principle, we have

$$\left|\mathcal{G}^n/(C_n \times \mathcal{G})\right| = \left|\mathcal{G}_1^n/C_n\right| = \frac{1}{n}\sum_{d|n}\phi\left(\frac{n}{d}\right)\left[\mathcal{G} \div \frac{n}{d}\right]|\mathcal{G}|^{d-1}$$

(by Theorem 5). This proves Theorem 19. □

8 K-product necklaces

We can extend the definition we gave earlier for identity-product necklaces to be more general than dealing with only the case of the identity.

For this entire section, we fix a subset K of $\mathcal{G}$ that is closed under conjugation (i.e., satisfies $gkg^{-1} \in K$ for all $g \in \mathcal{G}$ and $k \in K$). Equivalently, K shall be a union of conjugacy classes of $\mathcal{G}$. Examples of such subsets K are single conjugacy classes, normal subgroups, complements of normal subgroups, singleton subsets $\{h\}$ where h lies in the center of $\mathcal{G}$, and the whole group $\mathcal{G}$.

Definition 20. For any nonnegative integer n, we let $\mathcal{G}_K^n$ be the set of all *K-product n-tuples*, defined by

$$\mathcal{G}_K^n := \{a = (a_1, a_2, \ldots, a_n) \in \mathcal{G}^n : a_1a_2a_3\cdots a_n \in K\}.$$

The cyclic group C_n acts on $\mathcal{G}^n$ by cyclic rotation, as we know. We claim that the subset $\mathcal{G}_K^n$ is preserved under this action also. That is, for any K-product n-tuple $(a_1, a_2, \ldots, a_n)$, its cyclic rotation $(a_n, a_1, a_2, \ldots, a_{n-1})$ is again a K-product n-tuple, since its product

$$a_na_1a_2\cdots a_{n-1} = a_n \underbrace{a_1a_2\cdots a_{n-1}a_n}_{\in K} a_n^{-1} \in a_nKa_n^{-1} \subseteq K$$

(since K is closed under conjugation). Thus $\mathcal{G}_K^n$ is a C_n-set. In a similar fashion as with identity-product necklaces, orbits of this action of C_n on $\mathcal{G}_K^n$ will be called *K-product n-necklaces*.

Definition 21. For any integer n, let us define the number $[\mathcal{G} \div K \div n]$ to be

$$[\mathcal{G} \div K \div n] := |\{a \in \mathcal{G} : a^n \in K\}| .$$

This generalizes $[\mathcal{G} \div n]$, since $[\mathcal{G} \div n] = [\mathcal{G} \div \{1\} \div n]$.

With this generalization to K-product n-necklaces, we get an analogue to Theorem 5:

Theorem 22. *Let n be a positive integer. The number $|\mathcal{G}_K^n/C_n|$ of K-product n-necklaces is*

$$|\mathcal{G}_K^n/C_n| = \frac{1}{n} \sum_{d|n} \phi\left(\frac{n}{d}\right) [\mathcal{G} \div K \div n] \, |\mathcal{G}|^{d-1} .$$

The proof of this analogue of Theorem 5 is the same except for the following changes: replace all $\mathcal{G}_1$ by $\mathcal{G}_K$ and replace all $[\mathcal{G} \div n]$ by $[\mathcal{G} \div K \div n]$.

For example, the analogous versions of the definitions of P_k and A_k as well as Lemma 13 are, respectively

$$P_k := \left\{a \in \mathcal{G}_K^n : g^k \cdot a = a, \text{ but } g^l \cdot a \neq a \text{ for all } 0 < l < k\right\} . \tag{39}$$

$$A_k := \left\{a \in \mathcal{G}_K^n : g^k \cdot a = a\right\} . \tag{40}$$

Lemma 23. *For any $k \mid n$, we have*

$$|A_k| = \left[\mathcal{G} \div K \div \frac{n}{k}\right] |\mathcal{G}|^{k-1} . \tag{41}$$

This generalization also subsumes the classical formula (1). Indeed, if we take $\mathcal{G} = C_q$ and $K = \mathcal{G}$, then Theorem 22 recovers the count of n-necklaces over a size-q set.

With the same replacement of all mentions of $\mathcal{G}_1$ and $[\mathcal{G} \div n]$ with their K-product analogues, we can also obtain an analogous K-product version of Theorem 16 which counts the number of aperiodic K-product n-necklaces:

Theorem 24. *Let n be a positive integer. The number $\frac{|P_n|}{n}$ of aperiodic K-product n-necklaces is*

$$\frac{|P_n|}{n} = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) \left[\mathcal{G} \div K \div \frac{n}{d}\right] |\mathcal{G}|^{d-1} .$$

We leave it as an open question as to whether or not the bijection between identity-product necklaces and homogeneous necklaces has some analogue in the K-product setting as well.

9 Irreducible polynomials

As we briefly mentioned in the introduction, aperiodic necklaces over a size-q set are related to irreducible degree-n polynomials over the finite field $\mathbb{F}_q$ when q is a prime power. This relation can be restricted to aperiodic identity-product n-necklaces (over the additive group of $\mathbb{F}_q$, so the identity is actually 0) on the one hand, and to the irreducible degree-n polynomials with second-highest coefficient 0 on the other. We shall now elaborate on this.

9.1 Reminders on finite fields and their Galois groups

Let q be a prime power. Let K/F be a degree-n field extension, where F is the finite field with q elements. Thus, K is a finite field with q^n elements. Note that K/F is a Galois extension (like any extension of finite fields).

It is well-known that the map

$$\begin{aligned} \mathbf{F} : K &\to K, \\ x &\mapsto x^q \end{aligned}$$

is an F-algebra automorphism of K. This is called the *Frobenius automorphism over* $\mathbb{F}_q$, and generates the Galois group of the field extension K/F. Its k-th power $\mathbf{F}^k$ sends each $x \in K$ to x^{q^k}. In particular, its n-th power $\mathbf{F}^n$ is the identity map, since each $x \in K$ satisfies $x^{q^n} = x^{|K|} = x$. Thus, the Galois group $\mathrm{Gal}(K/F)$ consists of the n distinct automorphisms $\mathbf{F}^0, \mathbf{F}^1, \ldots, \mathbf{F}^{n-1}$.

A significant role in Galois theory is played by the trace:

Definition 25. The *trace map* is the linear map $\mathrm{tr} : K \to K$ defined by

$$\mathrm{tr} := \mathbf{F}^0 + \mathbf{F}^1 + \cdots + \mathbf{F}^{n-1}. \tag{42}$$

The *trace* of an element $x \in K$ is defined to be the image $\mathrm{tr}(x)$ of x under this map. Explicitly,

$$\begin{aligned} \mathrm{tr}(x) &= x + \mathbf{F}x + \mathbf{F}^2 x + \cdots + \mathbf{F}^{n-1} x \qquad (43) \\ &= x + x^q + x^{q^2} + \cdots + x^{q^{n-1}}. \qquad (44) \end{aligned}$$

Notably, $\mathrm{tr} \circ \mathbf{F} = \mathrm{tr}$, since right-multiplication by $\mathbf{F}$ merely cyclically permutes the addends on the right hand side of (42) (since $\mathbf{F}^n = \mathrm{id} = \mathbf{F}^0$) but does not affect the sum as a whole. Similarly, $\mathbf{F} \circ \mathrm{tr} = \mathrm{tr}$. The latter equality shows that each $x \in K$ satisfies $\mathbf{F}(\mathrm{tr}(x)) = \mathrm{tr}(x)$, and thus $\mathrm{tr}(x)$ is fixed by the Galois group $\mathrm{Gal}(K/F)$ (since all elements of $\mathrm{Gal}(K/F)$ are powers of $\mathbf{F}$). Since K/F is a Galois extension, this shows that

$$\mathrm{tr}(x) \in F \qquad \text{for all } x \in K. \tag{45}$$

Definition 26. We say that two elements of K are *conjugate* if they have the same minimal polynomial over F. Equivalently, two elements $x, y \in K$ are conjugate if $x = A(y)$ for some $A \in \mathrm{Gal}(K/F)$.

If x and y are two conjugate elements of K, then their traces are equal: $\mathrm{tr}(x) = \mathrm{tr}(y)$. Indeed, from $\mathrm{tr} \circ \mathbf{F} = \mathrm{tr}$, we obtain

$$\mathrm{tr} \circ \mathbf{F}^k = \mathrm{tr} \qquad \text{for all } k \in \mathbb{Z}. \tag{46}$$

But this means that $\mathrm{tr} \circ A = \mathrm{tr}$ for each $A \in \mathrm{Gal}(K/F)$ (since all elements of $\mathrm{Gal}(K/F)$ are powers of $\mathbf{F}$). Hence, if $x = A(y)$ for some $A \in \mathrm{Gal}(K/F)$, then $\mathrm{tr}(x) = \mathrm{tr}(A(y)) = (\mathrm{tr} \circ A)(y) = \mathrm{tr}(y)$.

Hence, we define the trace of an entire conjugacy class to be the trace of any of its elements.

9.2 Normal bases and the bijection Φ

A *normal basis* of K (over F) means a basis of K as an F-vector space that has the form $\left(\theta^{q^0}, \theta^{q^1}, \ldots, \theta^{q^{n-1}}\right)$, where $\theta \in K$. A classical fact (the normal basis theorem for finite fields) says:

Theorem 27. *There exists a normal basis of K over F.*

Proofs of this theorem can be found in [14, Theorem 2.35], [18, Appendix B], [13, Theorem 1.15], [7, Corollary 2.4.6] and various other texts on finite fields. It is in fact a particular case of the normal basis theorem for arbitrary Galois extensions, which appears (e.g.) in [16, Theorem 5.18], [4] etc.

Henceforth, we fix a normal basis $\left(\theta^{q^0}, \theta^{q^1}, \ldots, \theta^{q^{n-1}}\right)$ of K over F.

Following [20, Section 7.6.2], we introduce the map

$$\begin{aligned} \Phi : F^n &\to K, \\ (a_0, a_1, \ldots, a_{n-1}) &\mapsto a_0\theta^{q^0} + a_1\theta^{q^1} + \cdots + a_{n-1}\theta^{q^{n-1}}. \end{aligned}$$

This is a bijection, since $\left(\theta^{q^0}, \theta^{q^1}, \ldots, \theta^{q^{n-1}}\right)$ is a basis of K over F. Note that $\mathbf{F}^n(\theta) = \theta$, since $\mathbf{F}^n = \mathrm{id}$.

Recall that the cyclic group C_n acts on the set F^n by cyclically rotating n-tuples. We also let C_n act on the set K by having the generator g act as the Frobenius automorphism $\mathbf{F}$. This is a well-defined group action, since $\mathbf{F}^n = \mathrm{id}$. Now we claim the following:

Lemma 28. *The bijection Φ is an isomorphism of C_n-sets.*

Proof. We must prove that Φ is C_n-equivariant (since we already know Φ to be a bijection). Thus, need to show that $\Phi(h \cdot a) = h \cdot \Phi(a)$ for any $a \in F^n$ and any $h \in C_n$. Since the

group C_n is generated by g, it suffices to show this for $h = g$. So we must prove that $\Phi(g \cdot a) = g \cdot \Phi(a)$ for any $a \in F^n$.

Consider the standard basis $(e_0, e_1, \ldots, e_{n-1})$ of the F-vector space F^n, where e_i is the n-tuple $(0, 0, \ldots, 0, 1, 0, 0, \ldots, 0)$ with i many 0's preceding the entry 1. We also set $e_n := e_0$. The C_n-action on F^n then satisfies $g \cdot e_i = e_{i+1}$ for each $i \in \{0, 1, \ldots, n-1\}$.

We must prove that $\Phi(g \cdot a) = g \cdot \Phi(a)$ for any $a \in F^n$. Since Φ is F-linear, it suffices to prove this for all basis vectors $a = e_i$ with $i \in \{0, 1, \ldots, n-1\}$. That is, we must show that $\Phi(g \cdot e_i) = g \cdot \Phi(e_i)$ for all $i \in \{0, 1, \ldots, n-1\}$.

Fix $i \in \{0, 1, \ldots, n-1\}$. Then $g \cdot e_i = e_{i+1}$ as we saw above. Hence, $\Phi(g \cdot e_i) = \Phi(e_{i+1})$. But the definition of Φ yields $\Phi(e_i) = \theta^{q^i} = \mathbf{F}^i(\theta)$, so that

$$g \cdot \Phi(e_i) = g \cdot \mathbf{F}^i(\theta) = \mathbf{F}\left(\mathbf{F}^i(\theta)\right) = \mathbf{F}^{i+1}(\theta). \tag{47}$$

Moreover, we claim that $\Phi(e_{i+1}) = \mathbf{F}^{i+1}(\theta)$. Indeed, if $i+1 < n$, then this follows from the definition of Φ (similarly to $\Phi(e_i) = \mathbf{F}^i(\theta)$), whereas in the case $i+1 = n$, it follows from $\Phi(e_n) = \Phi(e_0) = \theta^{q^0} = \theta = \mathbf{F}^n(\theta)$. Thus, $\Phi(g \cdot e_i) = \Phi(e_{i+1}) = \mathbf{F}^{i+1}(\theta)$. Comparing this with (47), we obtain $\Phi(g \cdot e_i) = g \cdot \Phi(e_i)$ as desired. □

Corollary 29. *Two n-tuples in F^n lie in the same C_n-orbit if and only if their images under Φ are conjugate elements.*

Proof. Let x and y be two n-tuples in F^n. By Lemma 28, these tuples x and y lie in the same C_n-orbit if and only if their images $\Phi(x)$ and $\Phi(y)$ lie in the same C_n-orbit. But the C_n-orbits on K are just the orbits of the Galois group $\mathrm{Gal}(K/F)$, since C_n acts on K by having g act as the generator $\mathbf{F}$ of $\mathrm{Gal}(K/F)$. So x and y lie in the same C_n-orbit if and only if their images $\Phi(x)$ and $\Phi(y)$ lie in the same orbit of $\mathrm{Gal}(K/F)$, that is, are conjugate. □

Thus, Φ gives rise to a bijection from F^n/C_n (that is, n-necklaces over F) to the set of conjugacy classes of elements of K over F. We denote this bijection by $\hat{\Phi}$.

9.3 Zero-sum necklaces and zero-trace conjugacy classes

We say that an n-tuple $a = (a_1, a_2, \ldots, a_n) \in F^n$ is *zero-sum* if $a_1 + a_2 + \cdots + a_n = 0$ in F. The zero-sum n-tuples are just the identity-product n-tuples for the abelian group $(F, +, 0)$. We denote the set of those zero-sum n-tuples as F_0^n.

We say that a given n-necklace $\mathbf{a} \in F^n/C_n$ is *zero-sum* if its representatives $a = (a_1, a_2, \ldots, a_n) \in \mathbf{a}$ are zero-sum n-tuples (i.e., satisfy $a_1 + a_2 + \cdots + a_n = 0$ in F). This condition clearly does not depend on the choice of the representative, since cyclic rotation of an n-tuple does not change the sum of its entries. The zero-sum n-necklaces are just the n-identity-product necklaces for the abelian group $(F, +, 0)$. Therefore, their set is F_0^n/C_n.

Theorem 30. *A necklace $\mathbf{a} \in F^n/C_n$ is zero-sum if and only if the corresponding conjugacy class $\hat{\Phi}(\mathbf{a})$ has trace 0.*

Proof of Theorem 30. Let us first note that (44) yields $\operatorname{tr}(\theta) = \theta + \theta^q + \theta^{q^2} + \cdots + \theta^{q^{n-1}} \neq 0$, since $\left(\theta, \theta^q, \theta^{q^2}, \ldots, \theta^{q^{n-1}}\right) = \left(\theta^{q^0}, \theta^{q^1}, \ldots, \theta^{q^{n-1}}\right)$ is a basis of K over F.

Fix a necklace $\mathbf{a}$, and let $a = (a_0, a_1, \ldots, a_{n-1})$ be a representative (i.e., one of the tuples in $\mathbf{a}$). Thus, $\hat{\Phi}(\mathbf{a})$ is the conjugacy class of

$$\begin{aligned}\Phi(a) &= \Phi(a_0, a_1, \ldots, a_{n-1}) = a_0\theta^{q^0} + a_1\theta^{q^1} + \cdots + a_{n-1}\theta^{q^{n-1}} \\ &= \sum_{k=0}^{n-1} a_k \theta^{q^k} = \sum_{k=0}^{n-1} a_k \mathbf{F}^k(\theta).\end{aligned}$$

Hence, we can compute the trace of $\hat{\Phi}(\mathbf{a})$ as follows:

$$\begin{aligned}\operatorname{tr}(\hat{\Phi}(\mathbf{a})) &= \operatorname{tr}\left(\sum_{k=0}^{n-1} a_k \mathbf{F}^k(\theta)\right) \\ &= \sum_{k=0}^{n-1} a_k \operatorname{tr}\left(\mathbf{F}^k(\theta)\right) \qquad \text{(since tr is } F\text{-linear)} \\ &= \sum_{k=0}^{n-1} a_k \left(\operatorname{tr} \circ \mathbf{F}^k\right)(\theta) \\ &= \sum_{k=0}^{n-1} a_k \operatorname{tr}(\theta) \qquad \text{(by (46))} \\ &= (a_0 + a_1 + \cdots + a_{n-1}) \operatorname{tr}(\theta).\end{aligned}$$

Thus, $\operatorname{tr}(\hat{\Phi}(\mathbf{a})) = 0$ if and only if $a_0 + a_1 + \cdots + a_{n-1} = 0$ (since $\operatorname{tr}(\theta) \neq 0$). In other words, $\hat{\Phi}(\mathbf{a})$ has trace 0 if and only if $\mathbf{a}$ is a zero-sum necklace. □

Corollary 31. *The number of conjugacy classes of elements of K over F with trace 0 is equal to $|F_0^n/C_n|$.*

Proof. Theorem 30 shows that the bijection $\hat{\Phi}$ restricts to a bijection from the set F_0^n/C_n of zero-sum n-necklaces to the set of conjugacy classes of elements of K over F with trace 0. Thus, the two sets are equinumerous. □

Thus, we can use Theorem 5 to count the conjugacy classes with trace 0.

We shall next restrict ourselves to zero-sum n-tuples and n-necklaces with certain periodicity properties. We recall the notions of "aperiodic" and "smallest period" we introduced in Section 6. We define P_n to be the set of all zero-sum n-tuples in F_0^n whose smallest period is n. This is a particular case of the definition of P_k in (9), applied to the group $(F, +, 0)$ as $\mathcal{G}$.

Proposition 32. *The number of size-n conjugacy classes of elements of K with trace 0 is equal to the number of aperiodic zero-sum n-necklaces.*

Proof. Since $\Phi : F^n \to K$ is a bijection, it preserves the size of any subset of F^n. Thus, the size of an n-necklace $\mathbf{a}$ as a set must be equal to the size of the conjugacy class $\hat{\Phi}(\mathbf{a})$. In particular, the n-necklaces with size n as sets are bijectively mapped by $\hat{\Phi}$ to the size-n conjugacy classes. But the former necklaces are precisely the aperiodic n-necklaces. Thus, by restricting $\hat{\Phi}$ to these necklaces, we obtain a bijection from the aperiodic n-necklaces to the size-n conjugacy classes.

Restricting this bijection further to the zero-sum aperiodic n-necklaces, we obtain precisely the size-n conjugacy classes with trace 0 as their images because of Theorem 30. □

By Theorem 16, the number of aperiodic zero-sum n-necklaces is $\frac{|P_n|}{n}$.

Corollary 33. *There are $|P_n|$ elements in K that belong to size-n conjugacy classes.*

Proof. By Proposition 32, the number of size-n conjugacy classes in K is the number of aperiodic zero-sum n-necklaces; but this number is $\frac{|P_n|}{n}$ by Theorem 16. Since these classes are disjoint and have size n each, they contain a total of $\frac{|P_n|}{n} \cdot n = |P_n|$ many elements. □

9.4 The viewpoint of irreducible polynomials

Proposition 32 leads to an enumerative result about irreducible polynomials over F. To obtain it, we need a lemma that connects the trace of an element of K with its minimal polynomial:

Lemma 34. *Let $z \in K$ be an element whose minimal polynomial over F has degree n. Then the second-highest coefficient of this polynomial is $-\operatorname{tr}(z)$.*

This is a special case where the minimal polynomial is degree n of [16, Corollary 5.45] or of [5, Section 14.2, Exercise 18 (d)].

Corollary 35. *The number of monic irreducible polynomials of degree n over F with second-highest coefficient equal to 0 is equal to the number of aperiodic zero-sum n-necklaces over F.*

Proof. Starting from Proposition 32, we know that the number of aperiodic zero-sum n-necklaces over F is equal to the number of size-n conjugacy classes with trace 0.

Each monic irreducible polynomial f of degree n over F has n distinct zeroes in K (since F is a perfect field and K is its only degree-n extension up to isomorphism). These n zeroes form a conjugacy class, and f is their minimal polynomial.

Thus, we can define a map

$$\begin{aligned}\sigma : &\{\text{monic irreducible polynomials of degree } n \text{ over } F\} \\ &\to \{\text{size-}n \text{ conjugacy classes on } K\}\end{aligned}$$

that sends a polynomial to the conjugacy class consisting of its n zeroes in K. The inverse σ^{-1} of this map sends

$$\{z_1, z_2, \ldots, z_n\} \mapsto (x - z_1)(x - z_2) \cdots (x - z_n).$$

Thus σ is a bijection.

Via σ^{-1}, each size-n conjugacy class with trace 0 corresponds to a monic irreducible degree-n polynomial over F, and by Lemma 34 that polynomial must have second-highest coefficient 0. Thus the number of monic irreducible polynomials of degree n over F with second-highest coefficient equal to 0 is equal to the number of size-n conjugacy classes on K; but the latter number is in turn equal to the number of aperiodic zero-sum n-necklaces over F. □

Combining Corollary 35 with the explicit formula in Theorem 16 for the number of aperiodic zero-sum n-necklaces over F, we obtain a formula for the number of monic irreducible polynomials of degree n over F with second-highest coefficient equal to 0; this recovers [25, Corollary 2.8].

10 Sequences

The numbers $|\mathcal{G}_1^n/C_n|$ computed in Theorem 5 give rise to several integer sequences, some of which are present in the OEIS (Online Encyclopedia of Integer Sequences, [19]). The simplest way to obtain a sequence is to fix the group $\mathcal{G}$ and to vary n.

Setting the group $\mathcal{G}$ to be the cyclic group C_2, and varying the length n of the necklaces being counted, we obtain the OEIS sequence A000013, which counts the equivalence classes of n-bead binary necklaces with beads of 2 colors with respect to swapping all colors (the equivalence follows from Theorem 19):

$$|(C_2)_1^n/C_n| = \frac{1}{n} \sum_{d|n} \phi\left(\frac{n}{d}\right) \gcd\left(2, \frac{n}{d}\right) 2^{d-1}.$$

See Table 1 for the first few values.

n	1	2	3	4	5	6	7	8	9
$\lvert(C_2)_1^n/C_n\rvert$	1	2	2	4	4	8	10	20	30

Table 1: The numbers $|(C_2)_1^n/C_n|$ for $n \leq 9$.

These numbers $|(C_2)_1^n/C_n|$ appear under the name of $S(n-1)$ in [22].

We can also vary n and $\mathcal{G}$ in lockstep. For instance, we can let $\mathcal{G}$ be the cyclic group C_n and count identity-product n-necklaces. This gives us the OEIS sequence A130293, which

counts the number of necklaces of n colors up to cyclic permutation (again by Theorem 19):

$$\begin{aligned}|(C_n)_1^n/C_n| &= \frac{1}{n}\sum_{d|n}\phi\left(\frac{n}{d}\right)\gcd\left(n,\frac{n}{d}\right)n^{d-1}\\ &= \frac{1}{n}\sum_{d|n}\phi\left(\frac{n}{d}\right)\left(\frac{n}{d}\right)n^{d-1} \qquad \left(\text{since } \gcd\left(n,\frac{n}{d}\right)=\frac{n}{d}\right)\\ &= \sum_{d|n}\phi\left(\frac{n}{d}\right)\frac{n^{d-1}}{d}.\end{aligned}$$

See Table 2.

n	1	2	3	4	5	6	7	8	9
$\lvert(C_n)_1^n/C_n\rvert$	1	2	5	20	129	1316	16813	262284	4783029

Table 2: The numbers $|(C_n)_1^n/C_n|$ for $n \leq 9$.

Alternatively, letting $\mathcal{G}$ be the cyclic group C_{n+1} and again counting identity-product n-necklaces, we obtain the integer sequence A121774. This counts the number of n-bead necklaces with $n+1$ colors divided by $n+1$:

$$\begin{aligned}|(C_{n+1})_1^n/C_n| &= \frac{1}{n}\sum_{d|n}\phi\left(\frac{n}{d}\right)\underbrace{\gcd\left(n+1,\frac{n}{d}\right)}_{\substack{=1\\ \text{(since } n+1 \text{ is coprime to } n\text{)}}}(n+1)^{d-1}\\ &= \frac{1}{n}\sum_{d|n}\phi\left(\frac{n}{d}\right)(n+1)^{d-1}.\end{aligned}$$

See Table 3.

n	1	2	3	4	5	6	7	8	9
$\lvert(C_{n+1})_1^n/C_n\rvert$	1	2	6	33	260	2812	37450	597965	11111134

Table 3: The numbers $|(C_{n+1})_1^n/C_n|$ for $n \leq 9$.

A similar simplified formula can be obtained for $|\mathcal{G}_1^n/C_n|$ whenever the size $|\mathcal{G}|$ of $\mathcal{G}$ is coprime to n; but the result (which equals the number of n-bead necklaces with $|\mathcal{G}|$ colors divided by $|\mathcal{G}|$) can also be proved by a simple direct bijection, which we invite the reader to find.

11 Further directions

A variation on the set-up of the problem is to change the group acting on $\mathcal{G}_1^n$. A natural candidate for this is the dihedral group D_n, since $\mathcal{G}_1^n$ is already closed under the reflection r defined by

$$r \cdot (a_1, \ldots, a_n) := (a_n^{-1}, \ldots, a_1^{-1}).$$

Here, again, we can ask for the number of orbits, noticing that the analogous necklaces on non-group alphabets are known as *bracelets* and have been counted long ago [26]. When $\mathcal{G}$ is abelian, we can also have the symmetric group S_n (or a subgroup thereof) act on $\mathcal{G}_1^n$ by permuting the entries.[1]

Generalizing in a different direction but in a similar vein, we can consider n-tuples of matrices whose product has a given trace:

Definition 36. Let R be a commutative ring. Consider n-tuples of $m \times m$-matrices over R. We define the set of *h-trace-product n-tuples* ${}^h\mathcal{M}_m^n$ to be

$${}^h\mathcal{M}_m^n := \{A = (A_1, A_2, \ldots, A_n) : \operatorname{tr}(A_1 A_2 \cdots A_n) = h\}.$$

Since $\operatorname{tr}(AB) = \operatorname{tr}(BA)$, this set ${}^h\mathcal{M}_m^n$ is a C_n-set and therefore we can attempt to count the number of orbits $\left|{}^h\mathcal{M}_m^n / C_n\right|$ when R is finite.

References

[1] Donald Adjeroh, Tim Bell, and Amar Mukherjee, *The Burrows-Wheeler Transform: Data Compression, Suffix Arrays, and Pattern Matching*, Springer, 2008. https://doi.org/10.1007/978-0-387-78909-5.

[2] Daniel M. Baczkowski and Dursun A. Bulutoglu, Decimation classes of nonnegative integer vectors using multisets. Arxiv preprint, arXiv:2310.00403 [math.CO], 2023. Available at https://arxiv.org/abs/2310.00403.

[3] E. A. Bender and J. R. Goldman, On the applications of Möbius inversion in combinatorial analysis, *Amer. Math. Monthly* **82** (1975), 789–803.

[4] Dieter Blessenohl, On the normal basis theorem, *Note Mat.* **27** (2007), 5–10.

[5] D. S. Dummit and R. M. Foote, *Abstract Algebra*, John Wiley and Sons, Inc., 3rd edition, 2003.

[6] N. J. Fine, Classes of periodic sequences, *Illinois J. Math.* **2** (1958), 285–302.

[1] Cf. also the notion of *decimation classes* considered in [23] and [2].

[7] Shuhong Gao, *Normal Bases over Finite Fields*, PhD thesis, University of Waterloo, 1993. Available at https://www.math.clemson.edu/~sgao/papers/thesis.pdf.

[8] Ira M. Gessel and Christophe Reutenauer, Counting permutations with given cycle structure and descent set, *J. Combin. Theory Ser. A* **64** (1993), 189–215.

[9] E. N. Gilbert and John Riordan, Symmetry types of periodic sequences, *Illinois J. Math.* **5** (1961), 657–665.

[10] Solomon W. Golomb and Andy Liu, *Solomon Golomb's Course on Undergraduate Combinatorics*, Springer, 2021.

[11] David Guichard, An introduction to combinatorics and graph theory, 2025-01-04. Available at https://www.whitman.edu/mathematics/cgt_online/cgt.pdf.

[12] Michiel Hazewinkel, Witt vectors. I. In *Handbook of Algebra*, Vol. 6, pp. 319–472. Elsevier/North-Holland, 2009. https://doi.org/10.1016/S1570-7954(08)00207-6.

[13] Xiang-dong Hou, *Lectures on Finite Fields*, Vol. 190 of *Graduate Studies in Mathematics*, American Mathematical Society, 2018.

[14] Rudolf Lidl and Harald Niederreiter, *Finite Fields*, Vol. 20 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, second edition, 1997.

[15] Nicholas A. Loehr, *Combinatorics*, Discrete Mathematics and its Applications, Chapman and Hall/CRC, second edition, 2017. https://doi.org/10.1201/9781315153360.

[16] J. S. Milne, *Fields and Galois Theory*, Kea Books, 2022. Version 5.10 available at https://www.jmilne.org/math/CourseNotes/ft.html.

[17] C. Moreau, Sur les permutations circulaires distinctes, *Nouv. Ann.* **11** (1872), 309–314.

[18] Timothy Murphy, Finite fields, 2007. Available at https://www.maths.tcd.ie/pub/Maths/Courseware/FiniteFields/GF.pdf.

[19] OEIS Foundation Inc., The On-Line Encyclopedia of Integer Sequences, 2024. Published electronically at https://oeis.org.

[20] Christophe Reutenauer, *Free Lie Algebras*, Vol. 7 of *London Mathematical Society Monographs, New Series*, Oxford Science Publications, 1993.

[21] Victor Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, 2005.

[22] N. J. A. Sloane, On single-deletion-correcting codes. In *Codes and Designs*, Vol. 10 of *Ohio State Univ. Math. Res. Inst. Publ.*, pp. 273–291. De Gruyter, 2002. Newer version at http://neilsloane.com/doc/dijen.pdf.

[23] Jonathan S. Turner, Dursun A. Bulutoglu, Daniel Baczkowski, and Andrew J. Geyer, Counting the decimation classes of binary vectors with relatively prime length and density, *J. Algebraic Combin.* **55** (2022), 61–87.

[24] Vince Vatter, A probabilistic proof of a lemma that is not Burnside's, *Amer. Math. Monthly* **127** (2020), 63.

[25] Joseph L. Yucas, Irreducible polynomials over finite fields with prescribed trace/prescribed constant term, *Finite Fields Appl.* **12** (2006), 211–221.

[26] Yevhen Zelenyuk and Yuliya Zelenyuk, Counting symmetric bracelets, *Bull. Aust. Math. Soc.* **89** (2014), 431–436.

2020 *Mathematics Subject Classification*: Primary 05E18; Secondary 05A15, 11T06.
Keywords: Finite group, necklace, enumerative combinatorics, counting, Euler totient function, Möbius function, orbit, group action, Pólya enumeration, Burnside lemma, finite field, irreducible polynomial, Galois field, Galois theory.

(Concerned with sequences A000013, A081720, A121774, and A130293.)

Received May 28 2024; revised version received December 23 2025. Published in *Journal of Integer Sequences*, August 3 2026.

Return to Journal of Integer Sequences home page.