BROKEN BRACELETS, MOLIEN SERIES, PARAFFIN WAX AND AN ELLIPTIC CURVE OF CONDUCTOR 48

TEWODROS AMDEBERHAN, MAHİR BİLEN CAN, AND VICTOR H. MOLL

ABSTRACT. Certain enumeration questions arising from the study of binary necklaces are solved. Applications and interpretations are provided.

1. INTRODUCTION

A jeweler is asked to design a necklace consisting of a chain with n placements for k pieces of diamond. The client ask for one group of r diamonds to be placed next to each other and the remaining diamonds are to be isolated, that is, each one is mounted so that the two adjacent places are left empty. These special diamonds are called the *medallion* of the necklace. Figure 1 shows a necklace of length 20, with a medallion of length 5 and four extra diamonds.

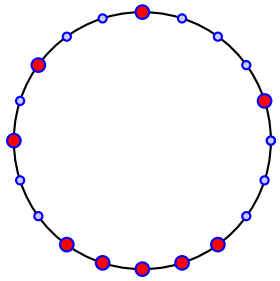


FIGURE 1. A necklace with a medallion.

FIGURE 2. A configuration.

Date: October 10, 2010.

2000 *Mathematics Subject Classification.* Primary 05A15, 05E10, Secondary 06A07, 06F05, 20M32.

Key words and phrases. necklaces, elliptic curves, Molien series, zeros of polynomials.

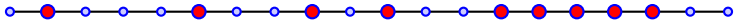


FIGURE 3. A forbidden configuration.

A *configuration* is a broken necklace resulting from one of the $r+1$ cuts to the left, right or in between the medallion. Figure 2 shows a configuration and Figure 3 depicts a forbidden cut.

Label n vertices as $\{1,\ 2, \cdots, n-1,\ n\}$. The *neighbors* of the vertex i are $i-1$ and $i+1$ for $2 \leq i \leq n-1$; the single vertex 2 for $i=1$ and the single vertex n for $i=n-1$. Configurations consist of a linear array of n vertices, k of which are *marked* or *painted red*. The marked vertices are either *isolated*, that is, its neighbors are not marked or *connected*, that is, the sequence of vertices $\{i, i+1, i+2, \cdots, j\}$ are all marked. In the latter case, it must be the case that $i=1$ or $j=n$; that is, connected marked vertices contain 1 or n.

Question 1. Determine the number $Z_k(n)$ of configurations up to symmetry.

The problem above, sans restriction, may be interpreted as a *binary necklace*: a periodic chain made of two kinds of beads. The classical result on counting all binary necklaces with n beads is given by MacMahon formula

$$N(n) = \frac{1}{n}\sum_{d|n} \varphi(d) 2^{n/d}, \tag{1.1}$$

where the summation runs through all divisors d of n, and $\varphi(d)$ is the *Euler totient* function counting the numbers $1,\ 2, \ldots,\ d$ relatively prime to d.

A simple parity distinction in n surprisingly isolates *allowed* from *forbidden* necklaces in supersymmetry [5]. The restrictions arise from Pauli exclusion principle, a result of anti-symmetry of planar states. In this context, a necklace is called forbidden if and only if it has $\mathbb{Z}_k$ symmetry for k even and F/k is odd. Here, F is the number of fermionic quanta. The statement in [5] is that the number of allowed and forbidden necklaces is given, respectively, by

$$N_{allowed}(n) = \frac{1}{n}\sum_{\substack{d|n \\ d \text{ odd}}} \varphi(d) 2^{n/d}, \tag{1.2}$$

and

$$N_{forbidden}(n) = \frac{1}{n}\sum_{\substack{d|n \\ d \text{ even}}} \varphi(d) 2^{n/d}. \tag{1.3}$$

This enumeration under Pauli principle is closely related to our initial question of the forbidden necklace problem.

2. The number of configurations

In this section the counting problem from the Introduction is rephrased and solved. The current format as well as the original formulation will be used interchangeably:

determine the number $Z_k(n)$ of painting k points in red from a linear array of n of them, with the condition that consecutive red points can only appear at the beginning or at end of the array. Moreover, arrays that are reflections of each other should be counted only once.

In order to determine the number of configurations $Z_k(n)$ it is convenient to begin with a simpler count.

Proposition 2.1. Let $f_k(n)$ be the number of arrangements of n vertices with k marked vertices, no consecutive marked ones where reflections are not identified. Then

$$f_k(n) = \binom{n-k+1}{k}. \tag{2.1}$$

Proof. Each such arrangement can be obtained by placing the k marked vertices and choosing $k-1$ places to separate them. The count is obtained by eliminating the separating spaces. □

Reduced configurations. The next step is to count those configurations obtained by cutting the necklace exactly on one side of the medallion. These produce linear arrays where clustered vertices appear either at the beginning or at the end of the array. Invoking symmetry, only those with the medallion at the left will be considered. Let $\beta_k(n)$ be the number of such arrays.

Theorem 2.8 provides an expression for the function $\beta_k(n)$ and Theorem 2.16 provides a formula for $Z_k(n)$.

Definition 2.1. Let $g_k(n)$ be the number of arrangements of n vertices with k marked points, no two being consecutively marked and identifying symmetric pairs.

Example 2.2. A numerical reinterpretation of $g_k(n)$ is given here. Take for example $n = 4$ and $k = 2$. From the pairs {12, 13, 14, 23, 24, 34} eliminate {12, 23, 34} for being consecutive somewhere. This leaves {13, 14, 24}. The pairs are now considered modulo 5, so that 24 is identified with 13 (the same as 31). The final allowed list is {13, 14} showing that $g_2(4) = 2$.

Theorem 2.3. The function $\beta_k(n)$ satisfies

$$\beta_k(n) = g_k(n) + \sum_{r=2}^{k} f_{k-r}(n-r-1). \tag{2.2}$$

Proof. Separate the different configurations into two groups: those with no consecutive marked points and those with at least two consecutive ones that are marked. The first type is counted by $g_k(n)$. Observe that if a certain arrangement has two or more adjacent marked vertices, then the remaining marked ones have no restrictions due to symmetry. In other words, reflection only imposes limitations if the configuration has no adjacent marked vertices in it.

The number of possible consecutive marked points is given by the size of the medallion. If this size is r, with $2 \leq r \leq k$, then drop $r+1$ places from the configuration (r for the medallion and one more at the right-end of it). This leaves a total of $n-r+1$ spaces where to place $k-r$ marked vertices. □

The next step is the enumeration of $g_k(n)$. This group is divided into three disjoint subclasses, those with (1) both ends are marked, (2) both ends are unmarked and (3) only the left end is marked. In the first class drop the vertices at positions 1, 2, $n-1$ and n and observe that the remaining $n-4$ vertices have $k-2$ marked ones and no further restrictions. Therefore there are $g_{k-2}(n-4)$ such arrangements. Similarly, the class (2) has $g_k(n-2)$ elements. Finally, in class (3), drop the first two vertices and the last one that is not marked. The remaining $n-3$ vertices have no symmetry restriction. The latter are counted by $f_{k-1}(n-3) = \binom{n-k-1}{k-1}$ such arrangements. This gives the relation

$$g_k(n) = g_k(n-2) + g_{k-2}(n-4) + \binom{n-k-1}{k-1}. \tag{2.3}$$

Theorem 2.4. Let $n = m+2k-1$ and define $\bar{g}_k(m) := g_k(m+2k-1)$. Then $\bar{g}_k$ satisfies

$$\bar{g}_k(m) = \bar{g}_{k-2}(m) + \bar{g}_k(m-2) + \binom{m+k-2}{k-1}. \tag{2.4}$$

Proof. Observe that any valid arrangement counted by $g_k(n)$ must satisfy $n \geq 2k-1$. The rest is elementary. □

The next result was obtained from experimental data generated by (2.4).

Example 2.5. The function $\bar{g}_k(m)$ is computed for $0 \leq m \leq 3$:

$$\bar{g}_k(0) = 1,\ \bar{g}_k(1) = \left\lfloor \frac{k+2}{2} \right\rfloor,\ \bar{g}_k(2) = \left\lfloor \frac{(k+2)^2}{4} \right\rfloor \tag{2.5}$$

and

$$\bar{g}_k(3) = \sum_{j=0}^{k} (-1)^{k-j} \left\{ \sum_{i=0}^{j} \left\lfloor \frac{j+2}{2} \right\rfloor + \binom{j+1}{2} \right\}. \tag{2.6}$$

Definition 2.6. The relation (2.4) attains a cleaner form by introducing the *necklace binomial coefficients*

$$\binom{t}{k}_{\mathfrak{N}} := \begin{cases} g_k(t+k-1) & \text{for } 0 \le k \le t \\ 0 & \text{otherwise.} \end{cases} \tag{2.7}$$

The next result is a restatement of Theorem 2.4.

Corollary 2.7. The necklace binomial coefficient satisfies the Pascal-type relation

$$\binom{t}{k}_{\mathfrak{N}} = \binom{t-2}{k-2}_{\mathfrak{N}} + \binom{t-2}{k-1} + \binom{t-2}{k}_{\mathfrak{N}}. \tag{2.8}$$

The evaluation of the necklace binomial coefficients is now easy to guess and establish using (2.8).

Theorem 2.8. For $0 \le k \le t$, it holds that

$$\binom{t}{k}_{\mathfrak{N}} = \frac{1}{2}\begin{cases} \binom{t}{k} & \text{for } t \text{ even and } k \text{ odd,} \\ \binom{t}{k} + \binom{\lfloor t/2 \rfloor}{\lfloor k/2 \rfloor} & \text{elsewhere.} \end{cases} \tag{2.9}$$

Moreover,

$$\beta_k(t) = \binom{t-k+1}{k}_{\mathfrak{N}} + \sum_{r=2}^{k} \binom{t-k}{r-2}. \tag{2.10}$$

Table 2 shows the values of the necklace coefficients:

t/k	0	1	2	3	4	5	6	7	8	9	10
1	1	1									
2	1	1	1								
3	1	2	2	1							
4	1	2	4	1	1						
5	1	3	6	6	3	1					
6	1	3	9	10	9	3	1				
7	1	4	12	19	19	12	4	1			
8	1	4	16	28	38	28	16	4	1		
9	1	5	20	44	66	66	44	20	5	1	
10	1	5	25	60	110	126	110	60	25	5	1

A series of elementary consequences of (2.9) are presented next.

Corollary 2.9. The row-sum identity

$$\sum_{k=0}^{t} \binom{t}{k}_{\mathfrak{N}} = 2^{t-1} + 2^{\lfloor (t-1)/2 \rfloor} \tag{2.11}$$

holds.

The next statements employ the *Fibonacci numbers* F_n, defined by the relation $F_n = F_{n-1} + F_{n-2}$ with initial conditions $F_0 = F_1 = 1$ and the *Lucas numbers* L_n defined by the same recurrence and with initial conditions $L_0 = 2$, $L_1 = 1$.

Corollary 2.10. Let F_n and L_n as above. Denote $\tilde{t} := \lfloor t/2 \rfloor + 2 + (-1)^{t+1}$. Then

$$\sum_{k=0}^{t} \beta_k(t) = \frac{1}{2}(L_{t+2} + F_{\tilde{t}}) - 1. \tag{2.12}$$

Corollary 2.11. The generating functions

$$\sum_{k=0}^{t} \binom{t}{k}_{\mathfrak{R}} y^k = \frac{1}{2}(1+y)^t + \frac{1}{2}(1+y^2)^{t/2}(1+y)^{t \bmod 2}, \tag{2.13}$$

$$\sum_{t\geq 0} \binom{t}{k}_{\mathfrak{R}} x^t = \frac{(1+x)^{\lfloor (k+1)/2 \rfloor} + (1-x)^{\lfloor (k+1)/2 \rfloor}}{2(1-x)^{\lceil (k+1)/2 \rceil}(1-x^2)^{\lfloor (k+1)/2 \rfloor}}, \tag{2.14}$$

and

$$\sum_{t,k\geq 0} \binom{t}{k}_{\mathfrak{R}} x^t y^k = \frac{1}{2(1-x-y)} + \frac{2+x}{2(1-x^2-y)}, \tag{2.15}$$

hold.

Corollary 2.12. The necklace binomial coefficients are symmetric, that is,

$$\binom{t}{k}_{\mathfrak{R}} = \binom{t}{t-k}_{\mathfrak{R}} \tag{2.16}$$

for $0 \leq k \leq t$.

Corollary 2.13. The function $\bar{g}$ is symmetric; that is,

$$\bar{g}_k(m) = \bar{g}_m(k). \tag{2.17}$$

Proof. This is a restatement of (2.16). An alternative proof of the symmetry (2.17) is obtained from the recurrence (2.4). Simply express it in two different forms

$$\begin{aligned} \bar{g}_k(m) - \bar{g}_{k-2}(m) &= \bar{g}_k(m-2) + \binom{m+k-2}{k-1}, \\ \bar{g}_k(m) - \bar{g}_k(m-2) &= \bar{g}_{k-2}(m) + \binom{m+k-2}{k-1}. \end{aligned} \tag{2.18}$$

The result now follows by induction and the symmetry of the binomial coefficients. □

The next theorem provides a combinatorial proof of the symmetry rule (2.17).

Theorem 2.14. The symmetry $\bar{g}_k(m) = \bar{g}_m(k)$ holds.

Proof. The assertion amounts to $g_k(m + 2k - 1) = g_m(k + 2m - 1)$. Take a linear array of n nodes and its 2-coloring (red r or white w). By definition, $g_k(n)$ enumerates all possible ways of coloring k nodes in red with the rule: (1) no two reds are consecutive; (2) two such arrays are equivalent if they relate by reflection. According to (1), it must be that the first $k - 1$ reds are each followed by white. Thus, any selection of k reds can be interpreted as choosing the $(k-1)$ pairs rw and a free r. For each pair rw, trim-off the w as well as its sitting node. That means, when $n = m + 2k - 1$ then the number of nodes reduces to $m + k$ and hence $g_k(m + 2k - 1)$ induces an equivalent counting of $(m + k)$-nodes of which k are red (note: rule (1) is absent but rule (2) stays). Similarly, $g_m(k + 2m - 1)$ tantamount to the counting of $(m + k)$-nodes of which m are white. But, it is obvious that coloring k nodes red on an $(m + k)$-array is equivalent to the coloring of m nodes in white. This gives the required bijection. The proof is complete. □

Example 2.15. This example demonstrates the above proof; i.e. $g_k(m+2k-1) = g_m(k + 2m - 1)$. Take $m = 2$ and $k = 3$. Then, $g_3(7)$ and $g_2(6)$ count respectively the cardinality of sets

$$A := \{rwrwrww, rwrwwrw, rwrwwwr, rwwrwrw, rwwrwwr, wrwrwrw\}$$

and

$$B : \{rwrwww, rwwrww, wrwrww, rwwwrw, wrrrrw, rwwwwr\}.$$

The set B after color-swapping turns to

$$B_1 := \{wrwrrr, wrrwrr, rwrwrr, wrrrwr, rwrrwr, wrrrrw\}.$$

The two sets A and B_1 are now mapped (w-trimmed and r-trimmed, respectively) to

$$A_1 := \{rrrww, rrwrw, rrwwr, rwrrw, rwrwr, wrrrw\},$$

and

$$B_{11} := \{wwrrr, wrwrr, rrwrr, wrrwr, rwrwr, wrrrw\}.$$

The bijection between A_1 and B_{11} is clearly exposed; that is, reflect B_{11} to get the set

$$B_{111} := \{rrrww, rrwrw, rrwrr, rwrrw, rwrwr, wrrrw\}.$$

The full counting solution to the configuration problem is presented next.

Theorem 2.16. The total number $Z_k(t)$ of possible linear configurations of k diamonds (with or without a medallion) on t nodes is given by

$$Z_k(t) = \sum_{j\geq 0} \binom{t-k-1}{k-2j}_{\mathfrak{R}} + \sum_{j\geq 0} \left\lfloor \frac{j+1}{2} \right\rfloor \binom{t-k-1}{k-j}.$$

Proof. Catalog the diamonds according to whether they are: (1) an equal number of clusters; (2) unequal number of clustered diamonds on the two end-nodes. However many are remaining to be mounted in the interior, case (1) is affected by the reflection but those in case (2) are not. It follows that the first case is enumerated by the function $g_k(t)$ (equivalently, by necklace binomials) while the function $f_k(t)$ is the right choice for the second category. The details are omitted. □

The necklace coefficients are given as Entry A005994 in Neil Sloane Encyclopedia of Integer Sequences. The reader will find there information on the connection between $\binom{t}{k}_{\mathfrak{R}}$ and the so-called *paraffin numbers*. The chemist S. M. Losanitsch studied in [4] the so-called *alkane numbers* (called here the necklace numbers) in his investigation of symmetries manifested by rows of paraffin (hydrocarbons). In the molecule of an *alkane* (also known as a paraffin), for n carbon atoms there are $2n + 2$ hydrogen atoms (i.e. the form C_nH_{2n+2}). Each carbon atom C is linked to four other atoms (either C of H); each hydrogen atom is joined to one carbon atom. The figures in the Appendix show all possible alkane bonds for $1 \leq n \leq 5$. There are 1, 1, 1, 2, 3 possible alignments, respectively.

A geometric interpretation. Given a finite group G, it is a classical problem to find the generators of the ring of polynomial invariants under the action of G. The *Molien series* $M(z; G)$ is the generating function that counts the number of linearly independent homogeneous polynomials of a given total degree d that are invariants for G. It is given by

$$M(z;G) = \frac{1}{|G|} \sum_{g\in G} \frac{1}{\det(I - zg)} = \sum_{i=0}^{\infty} b_i z^i. \tag{2.19}$$

Thus, the coefficients b_i record the number of linearly independent polynomials of total degree i.

Now assume $k = 2m - 1$. Then (2.14) becomes

$$\sum_{i\geq 0} \binom{i+2m-1}{2m-1}_{\mathfrak{R}} z^i = \frac{1}{2}\frac{1}{(1-z)^{2m}} + \frac{1}{2}\frac{1}{(1-z^2)^m}. \tag{2.20}$$

This is recognized as

$$\frac{1}{2}\frac{1}{(1-z)^{2m}} + \frac{1}{2}\frac{1}{(1-z^2)^m} = \frac{1}{|G|} \sum_{g\in G} \frac{1}{\det(\mathbf{1}_{2m} - zg)}, \tag{2.21}$$

where G is the symmetric group S_2 and the summation runs through the $2m$-dimensional group representation of the elements g in $GL_{2m}(\mathbb{C})$. The argument below shows that the series is indeed a Molien series for the ring of invariants under the action of S_2. More specifically, the ring of invariants under consideration is $\mathbb{C}[X;Y]^{\sim_2}$ where $X=(x_1,\ldots,x_m)$ and $Y=(y_1,\ldots,y_m)$. The action is given by $x_l \mapsto y_l$ for $l=1,\ldots,n$.

Let σ be the matrix $\sigma=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ and let π be the tensor product $\pi=\sigma\otimes\mathbf{1}_m$ resulting in a $2m\times 2m$ matrix which has four blocks of size $m\times m$ with the off-diagonal blocks being the identity matrix and the diagonals blocks being zero. The matrix group generated by π in GL_{2m} is S_2. Consequently,

$$\det(\mathbf{1}_{2m}-z\pi^2)=\det(\mathbf{1}_{2m}-z\mathbf{1}_{2m})=(1-z)^{2m} \tag{2.22}$$

and $\det(\mathbf{1}_{2m}-z\pi)=\det(\rho\otimes\mathbf{1}_{2m})$, with $\rho=\begin{pmatrix}1 & -z\\ -z & 1\end{pmatrix}$. Since $\det(A\otimes B)=\det(A)^m\det(B)^m$, it must be that $\det(\mathbf{1}_{2m}-z\pi)=(1-z^2)^m$.

These observations are summarized in the next statement.

Theorem 2.17. Consider the action of $\mathbb{Z}_2$ on $\mathbb{C}[x_1,\cdots,x_m,y_1,\cdots,y_m]$ given by $x_l\mapsto y_l$. Then, the number of linearly independent invariant polynomials of total degree i is given by the necklace binomial coefficient $\binom{i+2m-1}{2m-1}_{\mathfrak{N}}$.

3. The necklace polynomials

In this section we discuss properties of the *necklace polynomials* defined by

$$N_t(y)=\sum_{k=0}^{t}\binom{t}{k}_{\mathfrak{N}}y^k. \tag{3.1}$$

Theorem 3.1. The necklace polynomial is given by

$$N_t(y)=\frac{1}{2}(1+y)^t+\frac{1}{2}(1+y^2)^{\lfloor t/2\rfloor}(1+y)^{t \bmod 2}. \tag{3.2}$$

Proof. Use the binomial expansion and compare with (2.9). □

Example 3.2. The first few values of $N_t(y)$ are given by

$$\begin{aligned}
N_1(y) &= 1+y \\
N_2(y) &= 1+y+y^2 \\
N_3(y) &= N_1(y)N_2(y) \\
N_4(y) &= 1+2y+4y^2+2y^3+y^4 \\
N_5(y) &= N_1(y)N_4(y) \\
N_6(y) &= N_2(y)(1+2y+6y^2+2y^3+y^4) \\
N_7(y) &= N_1(y)N_2(y)(1+2y+6y^2+2y^3+y^4) \\
N_8(y) &= 1+4y+16y^2+28y^3+38y^4+28y^5+16y^6+4y^7+y^8.
\end{aligned}$$

The sequence of necklace polynomials have some interesting divisibility properties. The results presented below began with the empirical observation that, for t odd, $N_t(y) = N_1(t)N_{t-1}(y)$.

Corollary 3.3. Let $j \in \mathbb{N}$ and $t \in \mathbb{N}$. Then $N_j(y)$ divides $N_{(2t-1)j}(y)$.

Proof. This is a direct consequence of the explicit formula given in Theorem 3.1. □

Problem 3.4. Prove that $N_{2^j}(y)$ is irreducible.

Many polynomials appearing in Combinatorics are *unimodal*; that is, there is an index n^* such that the coefficients increase up to n^* and decrease from that point on. A stronger property is that of *logconcavity*: the polynomial $P(x) = \sum_{k=0}^{n} a_k x^k$ is logconcave if $a_k^2 - a_{k-1}a_{k+1} \geq 0$ for $1 \leq k \leq n-1$. The reader is referred to [2, 7] for surveys on these issues.

The explicit expression (2.9) gives an elementary proof of the next statement.

Theorem 3.5. The necklace binomial coefficients are unimodal.

Proof. The inequality

$$\binom{t}{k}_{\mathfrak{N}} \leq \binom{t}{k+1}_{\mathfrak{N}} \tag{3.3}$$

for $0 \leq k \leq \lfloor t/2 \rfloor$ and the symmetry of the necklace binomial coefficients, established in Theorem 2.12, give the result. □

Theorem 3.6. The polynomial $N_t(y)$ is logconcave.

Proof. Use (2.9) and separate cases according to the parity of t and k. □

Problem 3.7. Let $\mathfrak{Q}\{a_n\} := \{a_n^2 - a_{n-1}a_{n+1}\}$ be an operator defined on nonnegative sequences. Therefore, a polynomial $P(x)$ is logconcave if $\mathfrak{Q}$ maps

its coefficients into a nonnegative sequence. The polynomial P is called k-logconcave if $\mathfrak{L}^{(j)}(P)$ is nonnegative for $0 \leq j \leq k$. A sequence is called *infinitely logconcave* if it is k-logconcave for every $k \in \mathbb{N}$.

A recent result of P. Brändén [1] proves that if a polynomial P has only real and negative zeros, then the sequence of its coefficients is infinitely logconcave. The sequence of binomial coefficients satisfies this property.

The question proposed here is to prove that $N_t(y)$ is infinitely logconcave.

There is a well-established connection between unimodality questions and the location of the zeros of a polynomial. For example, a polynomial with all its zeros real and negative is logconcave [8]. This motivated the computation of the zeros of $N_t(y)$. Figure 4 shows the zeros of $N_{100}(y)$.

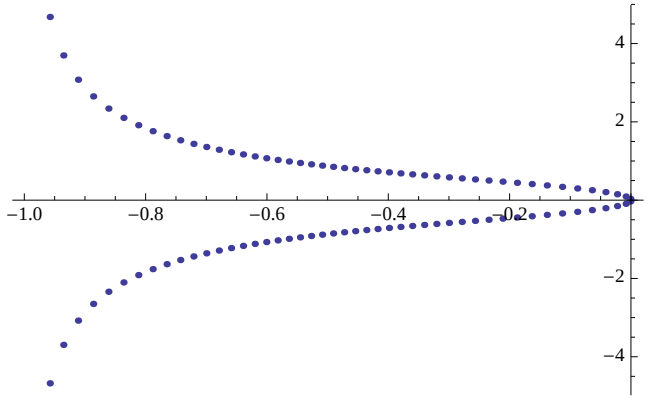


FIGURE 4. The zeros of the necklace polynomial $N_{100}(y)$.

Theorem 3.8. Let $y = a+ib$ be a root of the necklace polynomial $N_t(y) = 0$. For $a \neq -1$, define the new coordinates $u = 1/(1+a)$ and $v = b/(1+a)$. Then (u, v) is on the elliptic curve $v^2 = u^3 - 2u^2 + 2u - 1$.

Proof. Any zero of $N_t(y)$ satisfies

$$(1+y)^t = -\begin{cases} (1+y^2)^{t/2} & \text{if } t \text{ is even} \\ (1+y^2)^{(t-1)/2}(1+y) & \text{if } t \text{ is odd.} \end{cases} \tag{3.4}$$

Taking the complex modulus produces $|1+y|^4 = |1+y^2|^2$. In terms of $y = a + ib$ this equation becomes

$$b^2 = -\frac{a(a^2+a+1)}{1+a}. \tag{3.5}$$

The transformation $1+a=1/u$ and $b=v/u$ leads to equation

$$v^2 = u^3 - 2u^2 + 2u - 1 = (u-1)(u^2-u+1), \tag{3.6}$$

as claimed. □

Note 3.9. The collection of points on an elliptic curve $\mathfrak{E}$, such as (3.6), has been the subject of research since the 18th century. The general equation of such a curve is written as

$$y^2 + a_1 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{3.7}$$

and if $x, y \in P(\mathbb{C}^2)$, the complex projective space, then $\mathfrak{E}$ is a torus. The addition of this torus is expressed on the cubic in a geometric form: to add P_1 and P_2, form the line joining them and define $P_3 := P_1 \oplus P_2$ as the reflection of the third point of intersection of this line with the cubic curve. This addition rule is expressed in coordinate form: the general formula given in [6]. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. Define

$$\lambda = \begin{cases} \frac{y_2-y_1}{x_2-x_1} & \text{if } x_2 \neq x_1 \\ \frac{3x_1^2-4x_1+2}{2y_1} & \text{if } x_2 = x_1, \end{cases} \quad \text{and} \quad \nu = \begin{cases} \frac{y_1x_2-y_2x_1}{x_2-x_1} & \text{if } x_2 \neq x_1 \\ \frac{-x_1^3+2x_1-2}{2y_1} & \text{if } x_2 = x_1. \end{cases}$$

The $P_3 = (x_3, y_3)$ is given by

$$x_3 = \lambda^2 + 2 - x_1 - x_2 \text{ and } y_3 = -\lambda x_3 - \nu.$$

Aside from the point $P_0 = (1, 0)$, the table below shows a collection of points on the curve $\mathfrak{E}$ obtained using Mathematica. The notation

$$\gamma = \sqrt{3+2\sqrt{3}},\ \delta = \sqrt{\sqrt{5}-2},\ \tau = \sqrt{24+14\sqrt{3}},\ \sigma = 2\sqrt{2(11+5\sqrt{5})},$$
$$\omega_1 = 2+\sqrt{3},\ \omega_2 = 2(3+\sqrt{5}),\ \omega_3 = 3+2\sqrt{3}$$

is employed.

The notation *necklace point* refers to a point (u, v) on the elliptic curve $\mathfrak{E}$ that is produced by the zero $y = a + ib$ of a necklace polynomial via the transformation $1 + a = 1/u$ and $b = v/u$. The addition of two necklace points sometimes yields another one. For instance, $P_1 \oplus P_1 = P_0$ and $2P_3 := P_3 \oplus P_3 = P_2$. On the other hand, the set of necklace points is not closed under addition:

$$P_1 \oplus P_7 = \frac{1}{2}\left(7 + 3\sqrt{5} + \sqrt{66+30\sqrt{5}}\right) - \frac{I}{2}\left(21 + 9\sqrt{5} + \sqrt{30(29+13\sqrt{5})}\right).$$

The minimal polynomial for this number is $y^8 - 28y^7 + 1948y^6 - 5236y^5 + 4858y^4 - 3988y^3 + 7156y^2 - 6040y + 2245$. This polynomial does not divide a $N_t(y)$ for $1 \leq t \leq 1000$. It is conjectured that it never does.

Name	u	v	Root of $N_t(y) = 0$
P_1	2	$-\sqrt{3}$	2
P_2	2	$+\sqrt{3}$	2
P_3	$\omega_1 - \gamma$	$\omega_3 - \tau$	6
P_4	$\omega_1 - \gamma$	$-\omega_3 + \tau$	6
P_5	$\omega_1 + \gamma$	$-\omega_3 - \tau$	6
P_6	$\omega_1 + \gamma$	$\omega_3 + \tau$	6
P_7	$(1+\delta)\omega_2$	$\omega_2 + \sigma$	4
P_8	$(1+\delta)\omega_2$	$-(\omega_2 + \sigma)$	4
P_9	$(1-\delta)\omega_2$	$\omega_2 - \sigma$	4
P_{10}	$(1-\delta)\omega_2$	$-(\omega_2 - \sigma)$	4

TABLE 1. Some points on the elliptic curve $\mathfrak{E}$.

Note 3.10. Equation (3.5) shows that any root of $N_t(y)$ must satisfy $-1 \leq \operatorname{Re} y \leq 0$. Observe that $y = 0$ is never a root.

Note 3.11. The change of variables $u \mapsto u + 1$ transforms the curve $\mathfrak{E}$ into the form $v^2 = u^3 + u^2 + u$. This curve appears as $48a4$ in Cremona's table of elliptic curves, available at

`http://www.ma.utexas.edu/users/tornaria/cnt/cremona.html?conductor=48`

The discriminant of the cubic is negative. Therefore the curve has a single real component. This is seen in Figure 4.

Problem 3.12. The zeros of the polynomial $N_t(y)$ are algebraic numbers lying on the elliptic curve (3.5). The points on that curve with algebraic coordinates form a subgroup $\mathcal{A}$ under the addition described above. The question is to characterize in $\mathcal{A}$ the set coming from necklace points.

4. NECKALCES AND THEIR PROGENY

This section explores the enumeration of certain special necklaces and their generating functions. The latter is applied to the computation of some Molien series. A *circuit graph* is a graph consisting of n vertices placed on a circle with some of them colored by red.

Proposition 4.1. The total number of n-bead (circular) binary necklaces on which a red-red string is forbidden is given by

$$W(n) = \frac{1}{n} \sum_{d|n} \varphi\left(\frac{n}{d}\right) L_d. \tag{4.1}$$

Proof. A standard application of Burnside's lemma. □

Example 4.2. For $n = p$ prime, formula (4.1) gives

$$W(p) = \frac{(p-1) + L_p}{p}. \tag{4.2}$$

It follows that $L_p \equiv 1 \bmod p$. Similarly, for $n = p^2$, (4.1) gives

$$p^2 W(p^2) = L_{p^2} + (p-1)L_p + p(p-1). \tag{4.3}$$

It follows that

$$L_{p^2} \equiv L_p + 1 \bmod p^2. \tag{4.4}$$

These are well-known results [3].

A more distinguishing count is provided by defining $W_k(n)$ to be the number of n-bead (circular) binary necklaces on which a red-red string is forbidden, consisting of exactly k red beads. In order to accomodate the possibility that $k = 0$, we define $W_0(n) := 1$ (this is justifiable since $W_0(n) = \frac{1}{n}\sum_{d|n} \varphi(d) = 1)$.

Theorem 4.3. The function $W_k(n)$ is given by

$$W_k(n) = \frac{1}{n-k} \sum_{d|n,k} \varphi(d) \binom{\frac{n}{d} - \frac{k}{d}}{\frac{k}{d}}. \tag{4.5}$$

Proof. It follows directly from Burnside's lemma. □

Corollary 4.4. The identity

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \frac{1}{n-k} \sum_{d|n,k} \varphi(d) \binom{\frac{n}{d} - \frac{k}{d}}{\frac{k}{d}} = \frac{1}{n} \sum_{d|n} \varphi(d) L_{n/d} \tag{4.6}$$

holds.

Proof. The assertion follows from the combinatorial identity

$$\sum_{k \geq 0} W_k(n) = W(n). \tag{4.7}$$

□

Theorem 4.5. For $n \in \mathbb{N}$ define

$$V_d(x) = \left(\frac{1 - \sqrt{1+4x}}{2} \right)^d + \left(\frac{1 + \sqrt{1+4x}}{2} \right)^d. \tag{4.8}$$

Then the row-sum generating function of $W_k(n)$ is given by

$$F_n(x) := \sum_{k=0}^{\lfloor n/2 \rfloor} W_k(n) x^k = \frac{1}{n} \sum_{d|n} \varphi\left(\frac{n}{d}\right) V_d\left(x^{n/d}\right). \tag{4.9}$$

Proof. The proof is based on the identity

$$\frac{1}{m}V_m(x) = \sum_{k=0}^{\lfloor m/2 \rfloor} \frac{1}{m-k}\binom{m-k}{k}x^k, \tag{4.10}$$

which is easy to verify. This is applied to

$$\begin{aligned}\sum_{k=0}^{\lfloor n/2 \rfloor} W_k(n)x^k &= \sum_{d|n}\varphi(d)\sum_{k\geq 0}\frac{1}{n-dk}\binom{\frac{n}{d}-k}{k}x^{dk} \\ &= \sum_{d|n}\frac{\varphi(d)}{d}\sum_{k\geq 0}\frac{1}{\frac{n}{d}-k}\binom{\frac{n}{d}-k}{k}x^{dk}.\end{aligned}$$

The result follows from here. □

Example 4.6. For p prime, the polynomial $F_p(x)$, defined in (4.9), is given by

$$\begin{aligned}F_p(x) &= \sum_{k=0}^{\lfloor p/2 \rfloor}\frac{1}{p-k}\binom{p-k}{k}x^k \\ &= \frac{(p-1)2^p(1-\sqrt{1+4x})^p + (1+\sqrt{1+4x})^p}{p\cdot 2^p}.\end{aligned}$$

Example 4.7. Put $n = 3k+1$ in (4.3) to obtain $W_k(3k+1) = \frac{1}{2k+1}\binom{2k+1}{k}$, the Catalan numbers.

Example 4.8. For $n \in \mathbb{N}$, and with L_n denoting the Lucas number,

$$\sum_{k=0}^{\lfloor n/2 \rfloor}\frac{1}{n-k}\binom{n-k}{k} = \frac{1}{n}L_n. \tag{4.11}$$

This is obtained from setting $x = 1$ in (4.9).

Theorem 4.9. The ordinary generating function for the diagonals of $W_k(n)$ is given by

$$\sum_{n\geq k} W_k(n)x^n = \frac{1}{k}\sum_{d|k}\frac{\varphi(d)x^{2k}}{(1-x^d)^{k/d}}. \tag{4.12}$$

In its lowest terms, the denominator of this rational function takes the form

$$\prod_{d|k}(1-x^d)^{\varphi(k/d)} = \prod_{d|k}\Phi_d(x)^{k/d}, \tag{4.13}$$

where $\Phi_d(x)$ is the d-th cyclotomic polynomial given in terms of the Mobius μ-function as $\Phi_d(x) = \prod_{c|d}(1-x^{d/c})^{\mu(x)}$.

Proof. The result follows from the Taylor series expansion

$$\frac{x^{2m}}{m(1-x)^m} = \sum_{j\geq m} \frac{1}{j-m}\binom{j-m}{m}x^j. \tag{4.14}$$

□

A geometric interpretation. The above generating function $\sum_{n\geq k} W_k(n)x^n$ is the Molien series $W(x;\mathbb{Z}_k)$ for the ring of invariants $\mathbb{C}[X]^{\mathbb{Z}_k}$ where $X = (x_1,\ldots,x_k)$. In this case, the group $\mathbb{Z}_k$ is identified with its k-dimensional group representation in $GL_k(\mathbb{C})$. More concretely, $\mathbb{Z}_k \cong \langle \mathbf{e}_k\rangle$ where $\mathbf{e}_k$ is the $k\times k$ permutation matrix such that $\mathbf{e}[i,j] = 1$ if $j = i+1$; $\mathbf{e}[k,1] = 1$ and $\mathbf{e}[i,j] = 0$, otherwise. Let $RP(d)$ be the set of positive integers less than d and relatively prime to d. Partition the integer interval $[k]$ into the disjoint union

$$[k] = \{1,\,2,\,\ldots,\,k\} = \bigcup_{d|k} \frac{k}{d}\,RP(d). \tag{4.15}$$

This relation is reminiscent of the well-known identity $k = \sum_{d|k}\varphi(d)$. Then,

$$\begin{aligned}
W(x;\mathbb{Z}_k) &= \frac{1}{|\mathbb{Z}_k|}\sum_{j=1}^{k}\frac{1}{\det(\mathbf{1}_k - x\mathbf{e}_k^j)} \\
&= \frac{1}{k}\sum_{d|k}\frac{\varphi(d)}{\det(\mathbf{1}_k - x\mathbf{e}_k^{k/d})} \\
&= \frac{1}{k}\sum_{d|k}\frac{\varphi(d)}{\det((\mathbf{1}_d - x\mathbf{e}_d)\otimes \mathbf{1}_{k/d})} \\
&= \frac{1}{k}\sum_{d|k}\frac{\varphi(d)}{\det((\mathbf{1}_d - x\mathbf{e}_d)^{k/d}} \\
&= \frac{1}{k}\sum_{d|k}\frac{\varphi(d)}{(1-x^d)^{k/d}}.
\end{aligned}$$

These findings are stated in the next result.

Proposition 4.10. The number of linearly independent homogeneous polynomials, of total degree n, for the ring of invariants $\mathbb{C}[X]^{\mathbb{Z}_k}$ equals

$$\frac{1}{n+k}\sum_{d|n,k}\varphi(d)\binom{\frac{n}{d}+\frac{k}{d}}{\frac{k}{d}}.$$

5. A SAMPLE OF THE COMPUTATION OF ZEROS

Motivated by the interesting properties of the zeros of necklace polynomials, this section presents some computational graphics showing the zeros of the polynomials $F_n(x)$. Figure 5 shows the location of the roots of $F_{1000}(x)$.

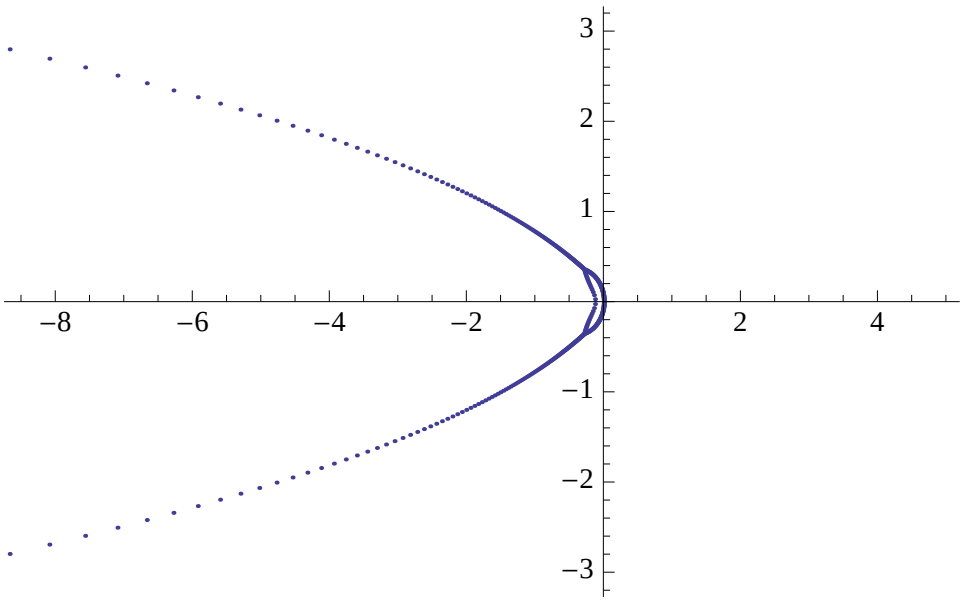


FIGURE 5. The zeros of $F_{1000}(x)$.

The next four figures show a selection of regions from the set of the roots of all the polynomials $F_n(x)$ for $3 \leq n \leq 1000$. The caption indicates the range depicted.

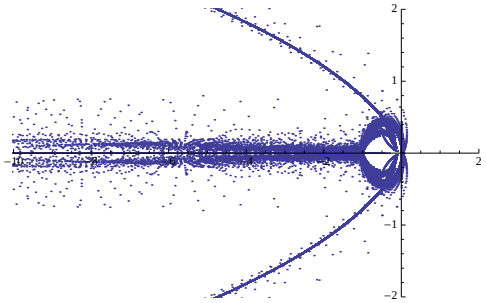


FIGURE 6. $[-10, 2] \times [-2, 2]$.

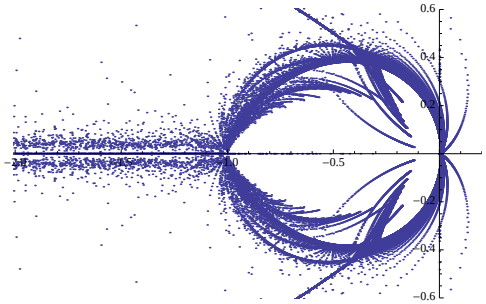


FIGURE 7. $[-2, 0.2] \times [-0.6, 0.6]$.

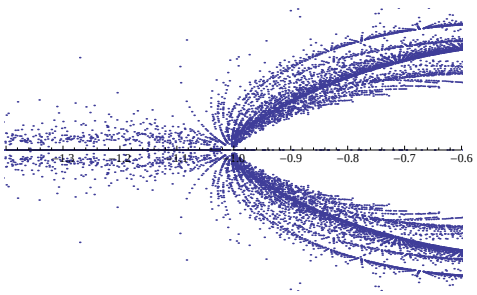


FIGURE 8. $[-1.4, -0.6] \times [-0.5, 0.5]$.

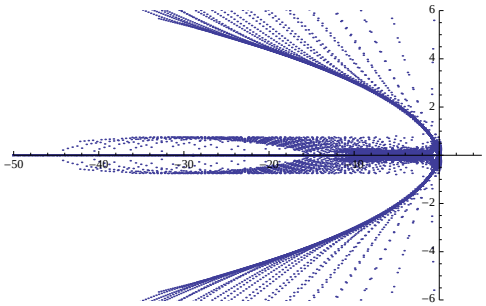


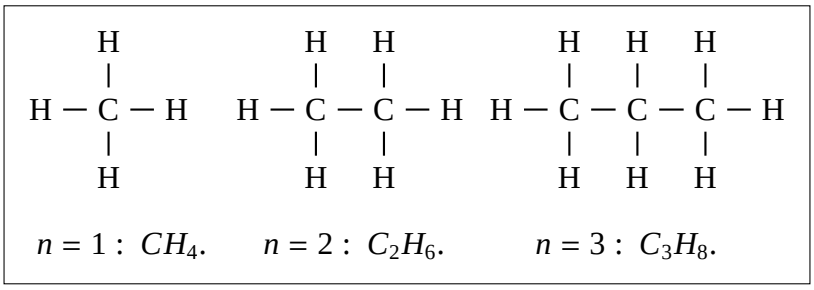
FIGURE 9. $[-50, 5] \times [-6, 6]$.

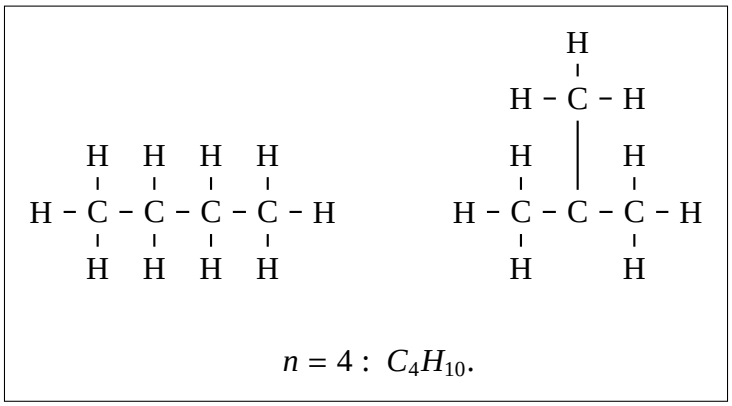
The interesting structure depicted in figures 6 to 9 will be explored in future work.

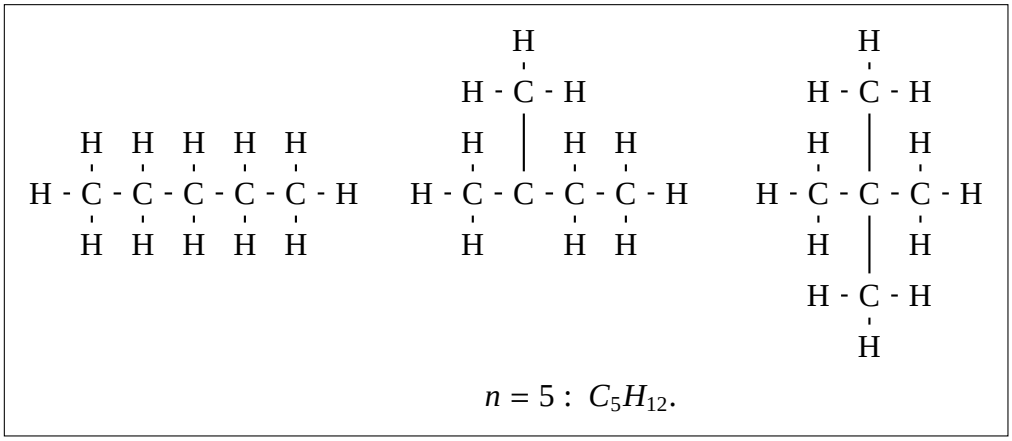
Acknowledgments. The authors wish to thank J. Silverman for providing information on the elliptic curve mentioned in the title. The third author was partially funded by NSF-DMS 0070567.

Appendix A. Rows of paraffin

The figures show all possible alkane bonds (paraffin) C_nH_{2n+2} for $n = 1, 2, 3, 4, 5$.







REFERENCES

[1] P. Brändén. Iterated sequences and the geometry of zeros. ArXiV: Math.CO/0909.1927, 2010.
[2] F. Brenti. Log-concave and unimodal sequences in Algebra, Combinatorics and Geometry: an update. *Contemporary Mathematics*, 178:71–89, 1994.
[3] G. H. Hardy, E. M. Wright; revised by D. R. Heath-Brown, and J. Silverman. *An Introduction to the Theory of Numbers*. Oxford University Press, 6th edition, 2008.
[4] S. M. Losanitsch. Die Isomerie-Arten bei den Homologen der Paraffin-Reihe. *Chem. Ber.*, 30:1917–1926, 1897.
[5] E. Onofri, G. Veneziano, and J. Wosiek. Supersymmetry and Combinatorics. ArXiV: math-ph/0603082, 2010.
[6] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer Verlag, New York, first edition, 1986.
[7] R. Stanley. Log-concave and unimodal sequences in Algebra, Combinatorics and Geometry. graph theory and its applications: East and West (Jinan, 1986). *Ann. New York Acad. Sci.*, 576:500–535, 1989.
[8] H. S. Wilf. *generatingfunctionology*. Academic Press, 1st edition, 1990.

DEPARTMENT OF MATHEMATICS, TULANE UNIVERSITY, NEW ORLEANS, LA 70118
E-mail address: tamdeber@tulane.edu

DEPARTMENT OF MATHEMATICS, TULANE UNIVERSITY, NEW ORLEANS, LA 70118
E-mail address: mcan@tulane.edu

DEPARTMENT OF MATHEMATICS, TULANE UNIVERSITY, NEW ORLEANS, LA 70118
E-mail address: vhm@math.tulane.edu