Proof of some conjectures related to the enumeration of magic series of arbitrary dimensions

Let $x \geq 0$ and $m > 0$ be integers, and let $N(x,m)$ be the number of partitions of $\lfloor m(x+1)/2 \rfloor$ into m distinct positive integers each less than or equal to x. We use the notation $\lfloor a \rfloor$ to represent the largest integer which is less than or equal to a ($a \in \mathbb{R}$).

More formally, $N(x,m)$ is the number of solutions $(z_1, \dots, z_m) \in \mathbb{Z}^m$ of the system

$$\begin{cases} 1 \leq z_1 < z_2 < \cdots < z_m \leq x \\ z_1 + z_2 + \cdots + z_m = \lfloor m(x+1)/2 \rfloor \end{cases}$$

Obviously, if $x < m$ then $N(x,m) = 0$, so from now on we will assume that $x \geq m$.

Note by the way that the value of $N(x,m)$ would not change if we would count the partitions of $\lceil m(x+1)/2 \rceil$ instead, where $\lceil a \rceil$ represents the smallest integer which is greater than or equal to a ($a \in \mathbb{R}$). This can be proved by considering the "complement" in the Ferrer diagram of the partitions. Since we do not need this result here, we'll just leave it at that.

The form $N(x,m)$ is related to the enumeration of magic series of arbitrary dimensions, because, as can easily be verified, the number of magic series of dimension n and order m is equal to $N(m^n, m)$. See for example http://www.trump.de/magic-squares/magic-series/hyper.htm.

First we will prove, at least for the case that m is even, that $N(x,m)$ is a quasi-polynomial of degree $m-1$ in x, and that its coefficient N_{m-1} of degree $m-1$ is given by

$$N_{m-1} = \frac{f(m)}{2^{m-1}(m-1)!^2}$$

where $f(m)$ is the m-th term in the sequence defined in OEIS A099765. The proof will be based on geometric concepts. It will give a geometric interpretation of all the terms and factors appearing in the expanded formula obtained by substituting the above occurrence of $f(m)$ by the explicit summation formula given in OEIS A099765. This is our main result.

Next, we will also prove that, for the case that m is even and $m \geq 4$, the period $L(m)$ of the quasi-polynomial $N(x,m)$ in x is a divisor of $\ell(m-1)$, where $\ell(n)$ is the n-th term in the sequence defined in OEIS A003418, so $\ell(n)$ is the least common multiple of the numbers in $[n] = \{1,2,\dots,n\}$.

Finally we will prove, again assuming that m is even, that the coefficient N_{m-2} of degree $m-2$ of the quasi-polynomial $N(x,m)$ is given by

$$N_{m-2} = -\frac{(m-1)^2 N_{m-1}}{2} = -\frac{f(m)}{2^m (m-2)!^2}$$

Note that this explains why, after the substitution $u = (x - (m-1)/2)/2$ as in http://www.trump.de/magic-squares/magic-series/formulae.htm, the coefficient of u^{m-2} is 0.

All of the above seems to be true if m is odd as well, but adaptations of the current proof would certainly be necessary. It seems that only some minor modifications are sufficient to prove the case where both m and x are odd (admittedly, I have not yet written this out). Actually this case is all we need if we are only interested in the application to magic series: the number of magic series of dimension n and order m is equal to $N(m^n, m)$, and obviously $x = m^n$ is odd if m is odd.

Let's start with the first part of the proof. First, we perform the following substitution of variables:

$$y_k = z_k - k, k = 1, \ldots, m$$

The original system then becomes

$$\begin{cases} 0 \le y_1 \le y_2 \le \cdots \le y_m \le x - m \\ y_1 + y_2 + \cdots + y_m + (1 + 2 + \cdots + m) = \lfloor m(x+1)/2 \rfloor \end{cases}$$

The last equation is equivalent to

$$y_1 + y_2 + \cdots + y_m = \lfloor m(x+1)/2 \rfloor - m(m+1)/2 = \lfloor m(x-m)/2 \rfloor$$

There is a 1-to-1 correspondence between the solutions of this system and the solutions of the original system, so $N(x, m)$ is also the number of solutions $(y_1, \ldots, y_m) \in \mathbb{Z}^m$ of the new system

$$\begin{cases} 0 \le y_1 \le y_2 \le \cdots \le y_m \le x - m \\ y_1 + y_2 + \cdots + y_m = \lfloor m(x-m)/2 \rfloor \end{cases}$$

This, by the way, proves that $N(x, m) = T(m, x - m)$, where $T(n, k)$ is the (symmetric) table defined in OEIS A067059.

We will now continue to work with the system in the y-variables. An alternative approach would be to work with the initial system in the z-variables, and to make use of Ehrhart-Macdonald reciprocity (which, by the way, we will use later in order to determine a formula for N_{m-2}).

From now on, we assume that m is fixed in advance and even.

Using the last equation to eliminate y_m from the system, we obtain the reduced system

$$\begin{cases} 0 \le y_1 \le y_2 \le \cdots \le y_{m-1} \\ y_1 + y_2 + \cdots + 2y_{m-1} \le m(x-m)/2 \\ y_1 + y_2 + \ldots + y_{m-1} \ge (m-2)(x-m)/2 \end{cases}$$

Subtracting the last two inequalities results in $y_{m-1} \le x - m$, which reconfirms that the solution space is bounded.

We will now make use of the following theorem (Ehrhart):

- let A be an integer $N \times M$ matrix, let $a = (a_1, \ldots, a_N)$ be an integer vector, and let $t \ge 0$ be an integer parameter;
- let $y_1, \ldots, y_M$, be M variables and $y = (y_1, \ldots, y_M)$;
- consider the system $Ay \le at$ of N inequalities in the M variables $y_1, \ldots, y_M$, and suppose that the solution space is bounded;

- let $q(t)$ be the (finite) number of solutions $y = (y_1, \dots, y_M) \in \mathbb{Z}^M$ of this system;
- let P be the (rational) polytope of all points y in $\mathbb{R}^M$ satisfying $Ay \leq a$ (the above system with $t = 1$); this also means that $t \cdot P$ is the "dilated" polytope of all points y in $\mathbb{R}^M$ satisfying the original system $Ay \leq at$.

Then the theorem states that

- $q(t)$ is a quasi-polynomial of degree M in t, called the Ehrhart quasi-polynomial of P;
- the coefficient of degree M of $q(t)$ is equal to the volume of P;
- the period of the quasi-polynomial is a divisor of the least common multiple of the denominators appearing in the coordinates of the vertices of P (all vertices of P have rational coordinates).

The statement about the period implies that if all vertices of P have integer coordinates, $q(t)$ is an ordinary polynomial, which is then called the Ehrhart polynomial of P.

We refer to the Wikipedia page http://en.wikipedia.org/wiki/Ehrhart_polynomial for some basic definitions and known properties about Ehrhart polynomials and quasi-polynomials, including Ehrhart-Macdonald reciprocity.

Our last system in the y-variables is of the required form to apply the theorem, with $M = m - 1$ and $t = x - m$, and we have $N(x, m) = q(x - m)$.

[Open question: are there perhaps more general versions of this theorem which would allow us also to deal with the case where m is odd? Maybe this is trivial, but maybe it is not…]

We want to find a formula for the coefficient N_{m-1} of x^{m-1} in $N(x, m)$. With $M = m - 1$ and $t = x - m$ as before, we have $N(x, m) = q(x - m) = q(t)$, which shows that N_{m-1} is equal to the coefficient of q^{m-1} in $q(t)$.

So our next goal is to find the volume V of the $(m - 1)$-dimensional rational polytope P defined by

$$\begin{cases} 0 \leq y_1 \leq y_2 \leq \cdots \leq y_{m-1} \\ y_1 + y_2 + \cdots + 2y_{m-1} \leq m/2 \\ y_1 + y_2 + \cdots + y_{m-1} \geq (m-2)/2 \end{cases}$$

setting $t = 1$ as required in the theorem.

If we reintroduce variable y_m such that $y_1 + y_2 + \cdots + y_m = m/2$, we see that in m-space this polytope is the orthogonal projection of the $(m - 1)$-dimensional polytope defined by

$$\begin{cases} 0 \leq y_1 \leq y_2 \leq \cdots \leq y_m \leq 1 \\ y_1 + y_2 + \cdots + y_m = m/2 \end{cases}$$

onto the hyperplane $y_m = 0$. From now on, by "projection" we always mean: the orthogonal projection onto the hyperplane $y_m = 0$.

Next we consider the $m!$ polytopes obtained by replacing the set of inequalities $y_1 \leq y_2 \leq \cdots \leq y_m$ by the set of inequalities obtained by permuting the order of the variables, in all $m!$ possible ways. These $m!$ polytopes have disjoint interiors. Their projections also have disjoint interiors, and, because of the symmetry, they all have the same volume V.

Now let P' be the projection of the more symmetric (and thus simpler) polytope defined by

$$\begin{cases} 0 \leq y_1, y_2, \dots, y_m \leq 1 \\ y_1 + y_2 + \cdots + y_m = m/2 \end{cases}$$

and let V' be its volume. P' is the union of the $m!$ projected polytopes. Since the $m!$ projected polytopes have disjoint interiors, and since they all have the same volume V, we have $V = V'/m!$.

We will now study the related parametric polytope $P(S)$ defined by

$$\begin{cases} 0 \leq y_1, y_2, \dots, y_m \leq 1 \\ y_1 + y_2 + \cdots + y_m \leq S \end{cases}$$

with $S \in \mathbb{R}$. Note that $P(S)$ is empty if $S \leq 0$ or $S \geq m$, so the interesting case is $0 \leq S \leq m$. From now on we always assume that $0 \leq S \leq m$.

Let $F(S)$ be the face of $P(S)$ lying in the bounding hyperplane $y_1 + y_2 + \cdots + y_m = S$, and let $F^*(S)$ be its projection.

We will use the notation vol_k to denote volumes in an affine space of dimension k, so vol_1 means *length*, vol_2 means *area*, and so on for higher dimension. This distinction may actually be overkill as the context should make clear which "volume" is intended in each case.

We can now restate the above definitions of P' and V' as follows:

$$P' = F^*(m/2)$$
$$V' = vol_{m-1}(P') = vol_{m-1}(F^*(m/2))$$

Summarizing, we found that the coefficient of degree $m-1$ of $N(x, m)$ in x (m even) is equal to

$$V = V'/m! = vol_{m-1}(F^*(m/2))/m!$$

Note that, because of the orientation of the face $F(S)$,

$$vol_{m-1}(F^*(S)) = \frac{d vol_m(P(S))}{dS}$$

Next, we will try to find a formula for the (parametric) volume of $P(S)$ valid for $0 \leq S \leq m$.

Consider the dilated unit m-simplex $H(S)$ defined by

$$\begin{cases} 0 \leq y_1, y_2, \dots, y_m \\ y_1 + y_2 + \cdots + y_m \leq S \end{cases}$$

It has one vertex in the origin, and m vertices on the bounding hyperplane $y_1 + y_2 + \cdots + y_m = S$, each lying on one of the coordinate axes, at a distance S from the origin.

For each subset $I \subseteq [m] = \{1, \dots, m\}$, let $I^* = [m] \backslash I$, and let $H_S(I)$ be the polytope defined by

$$\begin{cases} 0 \leq y_1, y_2, \dots, y_m \\ y_1 + y_2 + \cdots + y_m \leq S \\ \forall k \in I: y[k] \leq 1 \\ \forall k \in I^*: y[k] \geq 1 \end{cases}$$

Note that some of the $H_S(I)$ may be empty, and that $H_S([m]) = P(S)$.

Let $G(S)$ be the set of all such polytopes for the given values of m and S, so

$$G(S) = \{ H_S(I) \mid I \subseteq [m] \}$$

All the polytopes in $G(S)$ have disjoint interiors, and their union is the simplex $H(S)$. So the volume of $H(S)$ is equal to the sum of the volumes of all the polytopes in $G(S)$.

Let $f_S(I) = vol_m(H_S(I))$ and $g_S(I) = \sum_{J \subseteq I} f_S(J)$.

In particular, we have $f_S([m]) = vol_m(P(S))$ and $g_S([m]) = vol_m(H(S))$.

Our next goal is to find an expression for $g_S(I)$, and then to derive an expression for $vol_m(P(S)) = f_S([m])$ using the Möbius inversion theorem for the poset of subsets of $[m]$, see for example http://www.sfu.ca/~mdevos/notes/comb_struct/mobius.pdf, theorem 6.2.

Because of the symmetry, it is clear that $g_S(I)$, only depends on the *cardinality* of I (the actual numbers in I are of no importance).

So let's assume, without loss of generality, that $I = [i]$, $0 \leq i \leq m$ (assuming $[0] = \phi$), so $|I| = i$.

Going back to the above definitions we see that $g_S(I)$ is the volume of the polytope defined by

$$\begin{cases} 0 \leq y_1, y_2, \dots, y_m \\ y_1 + y_2 + \cdots + y_m \leq S \\ \forall k \in [i]^*: y[k] \geq 1 \end{cases}$$

If $S \leq m - i$ this polytope is empty, and its volume is 0. If $S \geq m - i$, this polytope is a dilated unit m-simplex with one vertex in the point $a = (a_1, \dots, a_m)$, with

$$a_1 = \cdots = a_i = 0, a_{i+1} = \cdots = a_m = 1$$

and with m vertices on the bounding hyperplane $y_1 + y_2 + \cdots + y_m = S$. These m vertices are at the intersection of an edge through a and parallel to one of the m coordinate axes.

Suppose that the edge parallel to axis y_k $(1 \leq k \leq m)$ connects vertices a and b, then

- $b_j = a_j, j \in \{k\}^* = [m]\backslash\{k\}$
- $b_k = S - \sum_{j \in \{k\}^*} b_j$, because b lies on the bounding hyperplane $y_1 + y_2 + \cdots + y_m = S$
- the length $|a - b|$ of the edge between a and b is $b_k - a_k$.

If $k \leq i$ then $a_k = 0$, and the sum $\sum_{j \in \{k\}^*} b_j$ contains $i - 1$ terms b_j which are equal to 0, and $m - i$ terms b_j which are equal to 1. So $b_k = S - (m - i)$, and $|a - b| = b_k - a_k = S - (m - i) - 0 = S - (m - i)$.

If $k > i$ then $a_k = 1$, and the sum $\sum_{j \in \{k\}^*} b_j$ contains i terms b_j which are equal to 0, and $m - i - 1$ terms b_j which are equal to 1. So $b_k = S - (m - i - 1)$, and again $|a - b| = b_k - a_k = S - (m - i - 1) - 1 = S - (m - i)$.

So in any case, the volume of this simplex $g_S(I)$ is always equal to $(S - (m - i))^m / m!$.

Conclusion, with $i = |I|$: $g_S(I) = (S - (m - i))^m / m!$ if $S \geq m - i$, and $g_S(I) = 0$ if $S \leq m - i$.

Next, we will apply a special case of the Möbius inversion theorem. The Möbius inversion theorem for the poset of subsets of $[m]$ states that

- if two functions f and g from the poset of subsets of $[m]$ to $\mathbb{R}$ (or $\mathbb{C}$) are defined such that $\forall I \subseteq [m]: g(I) = \sum_{J \subseteq I} f(J)$,
- then $\forall I \subseteq [m]: f(I) = \sum_{J \subseteq I} (-1)^{|I|-|J|} g(J)$

We can apply this theorem to our functions $f_S(I)$ and $g_S(I)$, assuming S is fixed in advance:

$$\forall I \subseteq [m]: f_S(I) = \sum_{J \subseteq I} (-1)^{|I|-|J|} g_S(J)$$

and consequently, for $I = [m]$:

$$f_S([m]) = \sum_{J \subseteq [m]} (-1)^{m-|J|} g_S(J)$$

Now in this sum all the $g_S(J)$ are 0, except the ones with $S \geq m - |J|$, so $|J| \geq m - S$, and we have

$$f_S([m]) = \sum_{\substack{J \subseteq [m] \\ |J| \geq m-S}} (-1)^{m-|J|} g_S(J) = \sum_{j=m-\lfloor S \rfloor}^{m} (-1)^{m-j} \sum_{\substack{J \subseteq [m] \\ |J| = j}} g_S(J)$$

The value of $g_S(J)$ is the same for all J with the same cardinality $|J|=j$, so all terms in the inner sum are identical. The number of terms in the inner sum is equal to the number of subsets of $[m]$ with cardinality j, $\binom{m}{j}$. So we have

$$f_S([m]) = \sum_{j=m-\lfloor S \rfloor}^{m} (-1)^{m-j} \binom{m}{j} \frac{(S - (m - j))^m}{m!} = \frac{1}{m!} \sum_{k=0}^{\lfloor S \rfloor} (-1)^k \binom{m}{k} (S - k)^m$$

In the last step we replaced the free variable j by k, with $k = m - j$.

Now we can combine this result with the results we found earlier:

$$vol_m(P(S)) = f_S([m]) = \frac{1}{m!} \sum_{k=0}^{\lfloor S \rfloor} (-1)^k \binom{m}{k} (S - k)^m$$

$$vol_{m-1}(F^*(S)) = \frac{dvol_m(P(S))}{dS} = \frac{1}{(m-1)!} \sum_{k=0}^{\lfloor S \rfloor} (-1)^k \binom{m}{k} (S - k)^{m-1}$$

Note that the variable S appears in the upper bound of the summations, so we have to be careful when taking the above derivative. If S is not an integer, it is always possible to define an environment of S in which the upper bound $\lfloor S \rfloor$ of the summations remains constant, so we can just take the derivative of the summand. If S is an integer, this is also true when taking the right derivative. When taking the left derivative however, this is only true if we first change the upper bounds to $\lceil S \rceil - 1$. This change in the *formulas* does not actually change the *functions* $vol_m(P(S))$ and $vol_{m-1}(F^*(S))$. This can be seen as follows. Clearly, $\lceil S \rceil - 1 = \lfloor S \rfloor$, except when S is an integer. But even when S is an integer, the upper bounds can still be replaced with $\lceil S \rceil - 1$ $(= S - 1 = \lfloor S \rfloor - 1)$ without changing the functions, because the last term ($k = \lfloor S \rfloor = S$) is then equal to 0 (in both summations), and can be dropped. So both one-sided derivatives are the same, and thus equal to the (two-sided) derivative.

Finally,

$$V = vol_{m-1}(F^*(m/2))/m! = \frac{1}{2^{m-1}m(m-1)!^2}\sum_{k=0}^{m/2}(-1)^k\binom{m}{k}(m-2k)^{m-1}$$

Now, is n is even, the n-th term in the sequence defined in OEIS A099765 is

$$f(n) = \frac{1}{n}\sum_{k=0}^{n/2}(-1)^k\binom{n}{k}(n-2k)^{n-1}$$

Comparing this with our expression for V, we see that

$$V = \frac{f(m)}{2^{m-1}(m-1)!^2}$$

In other words, if m is even, then the coefficient N_{m-1} of x^{m-1} in $N(x,m)$ is given by

$$N_{m-1} = \frac{f(m)}{2^{m-1}(m-1)!^2}$$

This is the main result we wanted to prove, and agrees with the results found by Walter Trump ($m \leq 12$).

Next, let's proceed to the second part, and focus our attention to the *period* $L(m)$ of the quasi-polynomial $N(x,m)$ in x. We want to prove that if m is even and $m \geq 4$, $L(m)$ must be a divisor of $\ell(m-1)$, where $\ell(n)$ is the least common multiple of the numbers in $[n]$.

We consider again the $(m-1)$-dimensional rational polytope P defined by

$$\begin{cases} 0 \leq y_1 \leq y_2 \leq \cdots \leq y_{m-1} \\ y_1 + y_2 + \cdots + 2y_{m-1} \leq m/2 \\ y_1 + y_2 + \cdots + y_{m-1} \geq (m-2)/2 \end{cases}$$

which we defined earlier in the context of the application of Ehrhart's theorem.

So far we did not use the last part of the theorem, which states that the period of the quasi-polynomial is a divisor of the least common multiple of the denominators appearing in the coordinates of the vertices of P (all vertices of the polytope have rational coordinates).

Now the question is: what are (the denominators appearing in) the coordinates of the vertices of P?

Since P is an $(m-1)$-dimensional polytope, each vertex is at the intersection of $m-1$ faces of P, and its coordinates can be found by solving the set of equations of $m-1$ of the bounding hyperplanes.

The problems will become easier after performing the following linear transformation, which, although it deforms the polytope, preserves vertices and faces:

$$\begin{aligned} y_1' &= y_1 \\ y_k' &= y_k - y_{k-1}\ (k = 1, \dots, m-1) \end{aligned}$$

We also have $y_1 = y_1'$ and $y_k = y_1' + y_2' + \cdots + y_k'$ $(k = 1, \dots, m-1)$, so it is clear that for any vertex, the denominators appearing in the y_j $(j = 1, \dots, m)$ are divisors of the least common multiple of the denominators appearing in the y_j'. We will prove that the denominators appearing in the y_j' of all the vertices are divisors of $\ell(m-1)$. From this it follows that the least common multiple of the denominators appearing in the y_j, over all the vertices, is a divisor of $\ell(m-1)$ as well, and consequently that $L(m)$ is a divisor of $\ell(m-1)$.

So using $y_k = y_1' + y_2' + \cdots + y_k'$ $(k = 1, \dots, m-1)$, we can rewrite the system as

$$\begin{cases} 0 \le y_1', y_2', \dots, y_{m-1}' \\ m y_1' + (m-1) y_2' + \cdots + 2 y_{m-1}' \le m/2 \\ (m-1) y_1' + (m-2) y_2' + \cdots + y_{m-1}' \ge (m-2)/2 \end{cases}$$

To obtain a vertex (any of them), we must select $m-1$ of these inequalities, which means that we must drop 2 of the $m+1$ equations, replace inequalities by equalities, and solve the resulting linear system of $m-1$ equations. Note that not every selection would results in a vertex, because the point of intersection may fall outside P. If we replace the inequalities by equalities in advance, we just have to select $m-1$ equations from the following list of $m+1$ equations (the first line $[A]$ represets $m-1$ equations):

$$\begin{aligned} y_k' &= 0\ (k = 1, \dots, m-1) && [A] \\ m y_1' + (m-1) y_2' + \cdots + 2 y_{m-1}' &= m/2 && [B] \\ (m-1) y_1' + (m-2) y_2' + \cdots + y_{m-1}' &= (m-2)/2 && [C] \end{aligned}$$

If we select the $m-1$ equations $[A]$, the solution is the origin, which is not a vertex (because of our assumption $m \ge 4$).

Next, for those vertices where the two equations $[B]$ and $[C]$ are both selected, equation $[B]$ can be subtracted from $[A]$. Assuming that we drop the two equations $y_i' = 0$ and $y_j' = 0$ (with $i, j \in [m-1]$), this results in the system

$$\begin{cases} \forall k \in [m-1] \backslash \{i, j\}: y_k' = 0 \\ y_1' + y_2' + \cdots + y_{m-1}' = 1 \\ (m-1) y_1' + (m-2) y_2' + \cdots + y_{m-1}' = (m-2)/2 \end{cases}$$

After eliminating the variables appearing in the equations $y_k' = 0$, we arrive at the reduced system

$$\begin{cases} y_i' + y_j' = 1 \\ (m-i) y_i' + (m-j) y_j' = (m-2)/2 \end{cases}$$

The determinant of this linear system is $(m-j)-(m-i)=i-j$. The denominators appearing in the coordinates y_i' and y_j' are divisors of the absolute value of the determinant $|i-j| \leq m-1$, and as a consequence are also divisors of $\ell(m-1)$. The other coordinates are all 0, so there are no other denominators.

Next, for those vertices where equation $[A]$ is selected, and equation $[B]$ is not selected, and assuming that we drop the equation $y_i' = 0$ (with $i \in [m-1]$), we arrive at the system

$$\begin{cases} \forall k \in [m-1]\backslash\{i\}: y_k' = 0 \\ my_1' + (m-1)y_2' + \cdots + 2y_{m-1}' = m/2 \end{cases}$$

After eliminating the variables appearing in the equations $y_k' = 0$, we are left with a single equation

$$(m-i+1)y_i' = m/2$$

If $i = 1$ then $y_i' = (m/2)/m = 1/2$, and because $m \geq 4$ the denominator 2 is indeed a divisor of $\ell(m-1)$.

Otherwise we have $2 \leq i \leq m-1$, so $2 \leq m-i+1 \leq m-1$, and because the equation shows that the denominator appearing in y_i' is now a divisor of $m-i+1$, it will also be a divisor of $\ell(m-1)$. Again, the other coordinates are all 0, so there are no other denominators.

Finally, for those vertices where equation $[B]$ is selected, and equation $[A]$ is not selected, and assuming that we drop the equation $y_i' = 0$ (with $i \in [m-1]$), we arrive at the system

$$\begin{cases} \forall k \in [m-1]\backslash\{i\}: y_k' = 0 \\ (m-1)y_1' + (m-2)y_2' + \cdots + y_{m-1}' = (m-2)/2 \end{cases}$$

After eliminating the variables appearing in the equations $y_k' = 0$, we are now left with the single equation

$$(m-i)y_i' = (m-2)/2$$

The equation shows that the denominator appearing in y_i' is now a divisor of $m-i \in [m-1]$, so it will also be a divisor of $\ell(m-1)$. As before, the other coordinates are all 0, so there are no other denominators.

Conclusion: assuming that m is even and $m \geq 4$, we found that the denominators appearing in the y_j' of all the vertices are divisors of $\ell(m-1)$. So the least common multiple of the denominators appearing in the y_j, over all the vertices, is a divisor of $\ell(m-1)$ as well, and using Ehrhart's theorem we may conclude that $L(m)$ is also a divisor of $\ell(m-1)$.

Finally, let's proceed to the third part, and focus our attention to the *second* coefficient N_{m-2} of the quasi-polynomial $N(x,m)$ in x. Assuming that m is even, as before, we will prove that

$$N_{m-2} = -\frac{(m-1)^2 N_{m-1}}{2}$$

Consider the following two systems we have encountered before in a slightly different form:

$$\begin{cases} 0 \le y_1 \le y_2 \le \cdots \le y_m \le x - m \\ y_1 + y_2 + \cdots + y_m = m(x-m)/2 \end{cases}, \text{ and } \begin{cases} 0 < y_1 < y_2 < \cdots < y_m < x + 1 \\ y_1 + y_2 + \cdots + y_m = m(x+1)/2 \end{cases}$$

We already know that both systems have $N(x, m)$ solutions $(y_1, \dots, y_m) \in \mathbb{Z}^m$.

Now let R be the rational polytope defined by the system

$$\begin{cases} 0 \le y_1 \le y_2 \le \cdots \le y_m \le 1 \\ y_1 + y_2 + \cdots + y_m = m/2 \end{cases}$$

Then the solutions of the first system are the points $(y_1, \dots, y_m) \in \mathbb{Z}^m$ belonging to the rational polytope $R_{x-m} = (x - m) \cdot R$, and the solutions of the second system are the points $(y_1, \dots, y_m) \in \mathbb{Z}^m$ belonging to the *interior of* the rational polytope $R_{x+1} = (x + 1) \cdot R$.

Note, by the way, that the number of points $(y_1, \dots, y_m) \in \mathbb{Z}^m$ on the *boundary* ∂R_{x+1} of R_{x+1} is equal to $N(x + m + 1, m) - N(x, m)$, $x \ge m$. So we now know that this is also a quasi-polynomial in x, and we could easily derive a closed formula for the high order coefficient of this quasi-polynomial (the coefficient of x^{m-2}) from the known closed formulas for N_{m-1} and N_{m-2}.

Next, to continue our proof, let $r(t)$ be the Ehrhart quasi-polynomial of R. Then we have, looking at the first system,

$$N(x, m) = r(x - m)$$

For the second system we must count only the *interior* points $(y_1, \dots, y_m) \in \mathbb{Z}^m$ in R_{x+1}. According to the Ehrhart-Macdonald reciprocity theorem we know that

$$N(x, m) = (-1)^{m-1} r(-(x + 1))$$

Comparing both expressions for $N(x, m)$, we see that

$$r(x - m) = (-1)^{m-1} r(-(x + 1))$$

Now let $\mathrm{r}(t) = N_{m-1} t^{m-1} + A t^{m-2} + \cdots$, where the coefficient A is still unknown. We know that A is not a periodic number, but a constant which is completely determined by the faces of the polytope R, as mentioned on the same Wikipedia page about Ehrhart (quasi-)polynomials. We could use this fact to determine A geometrically, but this leads to rather lengthy calculations. I actually did this, as an exercise, for the simple case $m = 4$. The faces turn out to be the 5 faces of a pyramid with a quadrilateral base, and with identical adjusted “volumes” (areas), despite their quite different shapes. Note that the equation $y_1 + y_2 + \cdots + y_m = m/2$ reduces the dimension of the polytope by 1.

Next, if we substitute the general expression for $r(t)$ in the last equation, we find

$$N_{m-1}(x - m)^{m-1} + A(x - m)^{m-2} + \cdots = N_{m-1}(x + 1)^{m-1} - A(x + 1)^{m-2} + \cdots$$

The coefficient of x^{m-2} must be the same on both sides of the equation, so we have

$$N_{m-1}(m - 1)(-m) + A = N_{m-1}(m - 1) - A$$

Solving for A we get

$$A = \frac{(m^2-1)N_{m-1}}{2}$$

and consequently,

$$r(t) = N_{m-1}t^{m-1} + \frac{(m^2-1)N_{m-1}}{2}t^{m-2} + \cdots$$

$$\begin{aligned} N(x,m) = r(x-m) &= N_{m-1}(x-m)^{m-1} + \frac{(m^2-1)N_{m-1}}{2}(x-m)^{m-2} + \cdots \\ &= N_{m-1}x^{m-1} - N_{m-1}(m-1)mx^{m-2} + \frac{(m^2-1)N_{m-1}}{2}x^{m-2} + \cdots \end{aligned}$$

So the coefficient of x^{m-2} is

$$N_{m-2} = -N_{m-1}(m-1)m + \frac{(m^2-1)N_{m-1}}{2} = -\frac{(2m^2-2m-m^2+1)N_{m-1}}{2} = -\frac{(m-1)^2N_{m-1}}{2}$$

This explains why, after the substitution $u = (x-(m-1)/2)/2$, hence $x = 2u + (m-1)/2$, as in http://www.trump.de/magic-squares/magic-series/formulae.htm, the coefficient of u^{m-2} is always equal to 0. The proof is trivial of course: if we start from

$$N(x,m) = N_{m-1}x^{m-1} + N_{m-2}x^{m-2} + \cdots$$

and replace x by $2u + (m-1)/2$, we get

$$\begin{aligned} &N_{m-1}(2u+(m-1)/2)^{m-1} + N_{m-2}(2u+(m-1)/2)^{m-2} + \cdots \\ &\qquad = 2^{m-1}N_{m-1}u^{m-1} + 2^{m-3}(m-1)^2N_{m-1}u^{m-2} + 2^{m-2}N_{m-2}u^{m-2} + \cdots \end{aligned}$$

and the coefficient of u^{m-2} turns out to be

$$2^{m-3}(m-1)^2N_{m-1} + 2^{m-2}N_{m-2} = 2^{m-3}(m-1)^2N_{m-1} - 2^{m-2}\frac{(m-1)^2N_{m-1}}{2} = 0$$

In fact this is true for any substitution of the form $u = a(x-(m-1)/2)$, so we could just as well have left out the second denominator 2, i.e. take $a = 1$ instead of $a = 1/2$.

Dirk Kinnaes

2013-04-12