CARDINALITY OF BALLS IN PERMUTATION SPACES

LIVIU P. DINU AND CATALIN ZARA

Abstract. For a right invariant distance on a permutation space $S_n$ we give a sufficient condition for the cardinality of a ball of radius $R$ to grow polynomially in $n$ for fixed $R$. For the distance $\ell_1$ we show that for an integer $k$ the cardinality of a sphere of radius $2k$ in $S_n$ (for $n \geq k$) is a polynomial of degree $k$ in $n$ and determine the high degree terms of this polynomial.

Contents

1. Introduction 1
2. Split Types 3
3. Polynomial Growth 5
4. Polynomial Growth for $\ell_p$ 6
5. High Degree Terms 8
6. Spheres of Small Radius 12
References 13

1. Introduction

Let $S_\infty$ be the group of permutations of $\mathbb{N} = \{1, 2, \ldots, n, \ldots\}$ that fix all but finitely many entries. For each positive integer $n$ the group $S_n$ of permutations of $[n] = \{1, 2, \ldots, n\}$ can be naturally identified with the subgroup of $S_\infty$ containing the permutations that fix all the entries greater than $n$. With these identifications $S_n \subset S_m \subset S_\infty$ for all $0 < n < m$. Let $D: S_\infty \times S_\infty \to [0, \infty)$ be a metric on $S_\infty$ for which right multiplications are isometries:

$$D(uw, vw) = D(u, v)$$

for all $u, v, w \in S_\infty$. Such metrics are called right invariant; several examples are discussed in the survey [DH98]. Since permutations in $S_\infty$ fix all but finitely many entries, the following right invariant metrics are well-defined on $S_\infty$:

- The Hamming distance $H$, counting the number of disagreements,

$$H(u, v) = \# \{ i \geq 1 \mid u(i) \neq v(i) \}.$$  

- For $p \geq 1$, the $\ell_p$ distance

$$\ell_p(u, v) = \left( \sum_{i \geq 1} |u(i) - v(i)|^p \right)^{1/p}. $$
in particular
\[ \ell_1(u, v) = \sum_{i \geq 1} |u(i) - v(i)|. \]

- The \( \ell_\infty \) distance
\[ \ell_\infty(u, v) = \max_{i \geq 1} |u(i) - v(i)|. \]

- The Cayley distance \( T \), with \( T(u, v) \) defined as the minimal number of transpositions needed to transform \( u \) into \( v \).

- The Kendall distance \( I \), with \( I(u, v) \) defined as the minimal number of transpositions of adjacent entries needed to transform \( u \) into \( v \).

The restriction of a right invariant metric \( D \) to \( S_n \) is a right invariant metric on \( S_n \) and an immediate consequence of right invariance is that the cardinality of spheres and of balls depends only on the radius and is independent of the center. For a permutation \( u \) we define \( D(u) = D(\text{id}, u) \), where \( \text{id} \) is the identity permutation. For \( R > 0 \), let
\[ B_D(R) = \{ u \in S_\infty \mid D(u) \leq R \} \]
be the closed ball of radius \( R \) centered at \( \text{id} \) and
\[ S_D(R) = \{ u \in S_\infty \mid D(u) = R \} \]
the sphere of radius \( R \) centered at \( \text{id} \). There are at most countably many values of \( R \) for which the sphere \( S_D(R) \) is not empty.

For \( n \geq 1 \), let
\[ B_{D,n}(R) = B_D(R) \cap S_n = \{ u \in S_n \mid D(u) \leq R \} \]
and
\[ S_{D,n}(R) = S_D(R) \cap S_n = \{ u \in S_n \mid D(u) = R \} \]
be the corresponding ball and sphere in \( S_n \), and
\[ V_{D,n}(R) = \# B_{D,n}(R) \quad \text{and} \quad A_{D,n}(R) = \# S_{D,n}(R) \]
the cardinalities of a ball and the sphere of radius \( R \) in \( S_n \).

Formulas for \( V_{D,n}(R) \) and \( A_{D,n}(R) \) (approximate or exact) are known for several of the metrics mentioned above. For the Kendall distance \( I \), the cardinality of the sphere \( S_{I,n}(k) \) is polynomial of degree \( k \) in \( n \) (see [Knu73, p. 15]). For the Hamming distance \( H \), the cardinality of the sphere \( S_{H,n}(k) \) is also polynomial of degree \( k \) in \( n \); more precisely
\[ A_{H,n}(k) = \left\lfloor \frac{k!}{e} \right\rfloor \binom{n}{k}, \]

since \( \left\lfloor \frac{k!}{e} \right\rfloor \) is the number of permutations in \( S_k \) with no fixed points.

For both metrics \( I \) and \( H \), the cardinality of a ball of fixed radius \( k \) is also a polynomial of degree \( k \) in \( n \). However, for the \( \ell_\infty \) metric, the situation is different. A consequence of [Sta97, Proposition 4.7.8] is that for fixed \( k \), the cardinality of a ball of \( \ell_\infty \)-radius \( k \) in \( S_n \) satisfies a linear recurrence in \( n \). A lower bound, exponential in \( n \), is given in [Klo11].

In this article we give a sufficient condition for the cardinality of a ball of radius \( R \) in \( S_n \) to grow polynomially in \( n \) for fixed \( R \). The condition is satisfied by the Kendall distance \( I \) and by the metrics \( \ell_p \) with \( p \geq 1 \), but not by \( \ell_\infty \) or by the Hamming distance \( H \).
For the metric $\ell_1$ we show that for an integer $k$, $A_{\ell_1,n}(2k)$ is a polynomial $P_k(n)$ of degree $k$ in $n$ (for $n \geq k$) and give explicit formulas for high degree terms of this polynomial. A direct consequence of the polynomial growth is that, if we randomly pick a permutation in a closed ball of radius $2^k$ then, with probability converging to 1 as $n \to \infty$, the permutation is on the sphere of radius $2^k$ with the same center:

$$\lim_{n \to \infty} P\left(\ell_1(u) = 2k | \ell_1(u) \leq 2k\right) = 1 .$$

In Section 2 we introduce the split types, one of the main tools used to prove our results. In Section 3 we formulate and prove the sufficient conditions for the cardinalities of balls and of spheres to grow polynomially, and in Section 4 we apply these conditions to the metrics $\ell_p$. In Section 5 we compute high degree terms of the polynomials $P_k(n) = A_{\ell_1,n}(k)$. Exact formulas for $\ell_1$-spheres of small radii are given in Section 6.

2. Split Types

We use the one-line notation for permutations: a permutation $\pi \in S_m$ is denoted by $\pi = (\pi(1) \pi(2) \ldots \pi(m))$.

**Definition 2.1.** If $\pi \in S_m$ and $\sigma \in S_n$, the concatenation $\pi + \sigma$ is the permutation $\pi + \sigma = (\pi(1) \ldots \pi(m) (m + \sigma(1)) \ldots (m + \sigma(n))) \in S_{m+n}$.

For example, $(321) + (21) = (32154)$.

Concatenation is associative (but not commutative) so we can define the concatenation of any finite number of permutations. For example,

$$(1) + (321) + (12) + (21) = (1432) + (1243) = (14325687).$$

**Definition 2.2.** A permutation that cannot be written as a concatenation of permutations of lower order is called connected. A permutation that can be written as a concatenation of permutations of lower order is called disconnected. The unique decomposition of a permutation as a concatenation of connected permutations is called the split decomposition of that permutation.  

For example, $(1432) = (1) + (321)$ is disconnected, but $(321)$ is connected.

An easy way to determine the split decomposition is to identify the cuts: a permutation $\pi \in S_n$ has a cut at $1 \leq i < n$ if $\pi(j) \leq i$ for all $j \leq i$ and $\pi(j) > i$ for all $j > i$. If $1 \leq i_1 < i_2 < \ldots < i_q < n$ are the cuts of $\pi$, then the slices $\pi_0 = \pi([1, i_1])$, $\pi_1 = \pi([i_1, i_2])$, $\ldots$, $\pi_q = \pi([i_q, n])$ correspond to the permutations in the split decomposition of $\pi$. For example, for $\pi = (1432576) \in S_7$ the splits are at 1, 4, and 5 and the split decomposition is

$$(1432576) = (1) + (321) + (1) + (21).$$

**Definition 2.3.** The split type of a permutation is the permutation obtained by concatenating the nontrivial permutations of its split decomposition.

For example, the split type of $(14325687) = (1) + (321) + (1) + (21) \in S_8$ is $(321) + (21) = (32154) \in S_5$.

---

1The connected parts of the split decomposition correspond to the components of the cycle diagram defined in [Eli11].
The necessary and sufficient condition that a permutation \( \sigma \) be a split type is that the connected parts in the split decomposition of \( \sigma \) be non-trivial permutations. Let \( S'_\infty \) be the set of split types and \( S'_m \), the subset of split types in \( S_m \). If \( \sigma \in S'_\infty \), we define \( q(\sigma) \) to be the number of connected parts, and \( m(\sigma) \) to be the smallest \( m \) such that \( \sigma \in S_m \). Equivalently, \( m(\sigma) \) is the unique value of \( m \) such that \( \sigma \in S'_m \).

For example, if \( \sigma = (32154) \), then \( q(\sigma) = 2 \) and \( m(\sigma) = 5 \). We have \( m(\sigma) \geq 2q(\sigma) \), or, equivalently,

\[ q(\sigma) \leq m(\sigma) - q(\sigma), \]

with equality only for \( \sigma = (21) + (21) + \cdots + (21) \).

**Lemma 2.4.** Let \( \sigma \in S'_\infty \) be a split type. The number of permutations \( \pi \in S_n \) of split type \( \sigma \) is

\[ M(n, \sigma) = \left[ \frac{n + q(\sigma) - m(\sigma)}{q(\sigma)} \right], \]

where \( \left[ \frac{j}{i} \right] \) is the binomial coefficient \( \left( \frac{j}{i} \right) \) if \( 0 \leq i \leq j \) and 0 otherwise.2

**Proof.** Let \( \pi \in S_n \) of split type \( \sigma = \sigma_1 + \cdots + \sigma_q \in S_m \). We mark the leftmost position of each of the images in \( \pi \) of the parts \( \sigma_1, \ldots, \sigma_q \), delete the other \( m - q \) positions of those images, and then compress the result, translating the markings. The marked values form a \( q \)-element subset of \([n+q-m]\). For example, for the permutation \( \pi = (1432576) \) of split type \( \sigma = (321) + (21) \), the image of \( \sigma \) in \( \pi \) is on positions 2, 3, 4 and 6. We keep and mark (in bold) 2 and 6 and delete 3, 4, and 7. The result is the set \( \{1, 2, 5, 6\} \), which is compressed to \( \{1, 2, 3, 4\} \), corresponding to the subset \( \{2, 4\} \) of \([4]\).

We have therefore associated a \( q \)-element subset of \([n+q-m]\) to each permutation \( \pi \in S_n \) of split type \( \sigma \), and this map is clearly injective. It is also surjective, because the process is reversible: each \( q \)-element subset of \([n+q-m]\) can be expanded to a unique permutation in \( S_n \) of split type \( \sigma \). For example, if \( \sigma = (321) + (21) \), then the subset \( \{1, 3\} \) of \([4]\) comes from \( \{1, 2, 3, 4\} \), which is the result of compressing \( \{1, 4, 5, 7\} \). That comes from the permutation \((3214657)\).

Hence the number of permutations in \( S_n \) of split type \( \sigma = \sigma_1 + \cdots + \sigma_q \in S_m \) is the same as the number of \( q \)-element subsets of \([n+q-m]\).

**Remark 2.5.** For \( n \geq m(\sigma) - q(\sigma) \), \( M(n, \sigma) \) is a polynomial of degree \( q(\sigma) \) in \( n \).

For all distances \( D = H, T, I, \ell_p, \ell_\infty \), the split type determines the distance to the identity: if a permutation \( u \in S_n \) has split type \( \sigma \in S_m \), then

\[ D(u) = D(\sigma). \]

**Definition 2.6.** A distance \( D \) on \( S_\infty \) is called a split type distance if \( D(u) = D(v) \) for any two permutations \( u \) and \( v \) having the same split type.

Moreover, if \( D = I, \ell_1 \), then \( D(u + v) = D(u) + D(v) \) for all \( u, v \).

**Definition 2.7.** A distance \( D \) on \( S_\infty \) is called an additive if \( D(u + v) = D(u) + D(v) \).

Any additive distance is a split type distance.

---

2If \( i < 0 < j \), then the binomial coefficient \( \left( \frac{j}{i} \right) \) is \( i(i-1) \ldots (i-j+1)/j! = (-1)^i \left( \frac{i-1}{j} \right) \) and is not zero. However, \( \left[ \frac{j}{i} \right] = 0 \).
3. Polynomial Growth

We can now formulate and prove our sufficient condition for a polynomial growth of $V_{D,n}(R)$, the cardinality of a $D$-ball of radius $R$ in $S_n$.

**Theorem 3.1.** Let $D$ be a right invariant split type distance on $S_\infty$ and $R > 0$. Suppose there exists an integer $N(R)$ such that $m(\sigma) - q(\sigma) \leq N(R)$ for every split type $\sigma$ with $D(\sigma) \leq R$. Then there exists a polynomial $P$ of degree at most $N(R)$ such that $V_{D,n}(R) = P(n)$ for all $n \geq N(R)$.

**Proof.** If $\sigma$ is a split type with $D(\sigma) \leq R$, then $q(\sigma) \leq m(\sigma) - q(\sigma) \leq N(R)$ and $m(\sigma) \leq N(R) + q(\sigma) \leq 2N(R)$. Then

$$V_{D,n}(R) = \sum_{\sigma \in S_m} \sum_{D(\sigma) \leq R} \left[n + q(\sigma) - m(\sigma)\right] = \sum_{m \leq 2N(R)} \sum_{\sigma \in S_m} \left[n + q(\sigma) - m\right].$$

Let $\alpha_D(R, m, q)$ be the number of split types $\sigma \in S_m$ with $q(\sigma) = q$ and $D(\sigma) \leq R$. Then

$$V_{D,n}(R) = \sum_{q=1}^{N(R)} \sum_{m=2q}^{q+N(R)} \alpha_D(R, m, q) \left[\frac{n + q - m}{q}\right]$$

and for $n \geq N(R)$,

$$V_{D,n}(R) = \sum_{q=1}^{N(R)} \sum_{m=2q}^{q+N(R)} \alpha_D(R, m, q) \left(n + q - m\right) \left[\frac{1}{q}\right]$$

is a polynomial in $n$ of degree at most $N(R)$. \hfill \Box

A completely similar argument proves the following condition for a polynomial growth of the cardinality of a sphere.

**Theorem 3.2.** Let $D$ be a right invariant split type distance on $S_\infty$ and $R > 0$. Suppose there exists an integer $N(R)$ such that $m(\sigma) - q(\sigma) \leq N(R)$ for every split type $\sigma$ with $D(\sigma) = R$. Let $\beta_D(R, m, q)$ be the number of split types $\sigma \in S_m$ such that $D(\sigma) = R$ and $q(\sigma) = q$. Then

$$A_{D,n}(R) = \sum_{q=1}^{N(R)} \sum_{m=2q}^{q+N(R)} \beta_D(R, m, q) \left[\frac{n + q - m}{q}\right]$$

and for $n \geq N(R)$,

$$A_{D,n}(R) = \sum_{q=1}^{N(R)} \sum_{m=2q}^{q+N(R)} \beta_D(R, m, q) \left(n + q - m\right) \left[\frac{1}{q}\right] \tag{3.1}$$

is a polynomial in $n$ of degree at most $N(R)$.

To determine the coefficient $\beta_D(R, m, q)$ by brute force, one would need to consider all permutations in $S_{2N(R)}$. The situation is better for additive distances.

**Definition 3.3.** Let $k$ be a positive integer. By a composition of $k$ we mean an expression of $k$ as an ordered sum of positive integers, and by a $q$-composition we mean a composition that has exactly $q$ terms. (See [Sta97].)
It is easy to see that the number of $q$-compositions of $k$ is $\binom{k-1}{q-1}$: a $q$-composition of $k$ is a way to break an array of $k$ blocks into $q$ non empty parts. The first part must start at 1, but the remaining $q-1$ parts can start at any $q-1$ places in the remaining $k-1$ blocks.

**Proposition 3.4.** Let $D: S_\infty \to \mathbb{N} \cup \{0\}$ be an additive right invariant distance on $S_\infty$. Then

\[
(3.2) \quad \beta_D(k, m, q) = \sum_{(k_1, \ldots, k_q)} \sum_{(m_1, \ldots, m_q)} \prod_{i=1}^{q} \beta_D(k_i, m_i, 1),
\]

where the sums are over of $q$–compositions $(k_1, \ldots, k_q)$ of $k$ and $q$–compositions $(m_1, \ldots, m_q)$ of $m$.

If the metric $D$ is additive, then all the coefficients $\beta_D(k, m, q)$ can be computed from $\beta(k', m', 1)$ for all $k' \leq k$ and $m' \leq m$, and that can be done inside $S_{k+1}$.

4. Polynomial Growth for $\ell_p$

In this section we prove that the metrics $\ell_p$ for $p \geq 1$ and the Kendall metric $I$ satisfy the condition of Theorems 3.1 and 3.2, hence the spheres and the balls grow polynomially in $n$ for a fixed radius.

**Proposition 4.1.** If $\sigma$ is a split type and $\ell_p(\sigma) \leq R$, then

\[
m(\sigma) - q(\sigma) \leq \frac{1}{2} R^p.
\]

Proof. If $\ell_p(\sigma) \leq R$, then

\[
\ell_1(\sigma) \leq \ell_p(\sigma)^p \leq R^p,
\]

and therefore it suffices to prove the statement for the case $p = 1$.

Suppose that $\sigma \in S_m$ is a split type with split decomposition $\sigma = \sigma_1 + \cdots + \sigma_q$ and such that $\ell_1(\sigma) \leq r$. We need to show that $m - q \leq r/2$. It suffices to prove that for every connected split type $\sigma$ we have

\[
(4.1) \quad m(\sigma) - 1 \leq \frac{1}{2} \ell_1(\sigma).
\]

We prove (4.1) by induction on the number of cycles of $\sigma$.

Suppose $\sigma$ is a cycle $c: i_1 = 1 \rightarrow i_2 \rightarrow \cdots \rightarrow i_t = m \rightarrow \cdots \rightarrow i_s$. Then

\[
\ell_1(\sigma) = (|i_1 - i_2| + \cdots + |i_{t-1} - i_t|) + (|i_t - i_{t+1}| + \cdots + |i_s - i_1|) \geq 2(i_t - i_1) = 2(m - 1),
\]

and that implies (4.1). The equality occurs if and only if the cycle $c$ is monotone,

\[
i = i_1 < i_2 < \cdots < i_{t-1} < i_t = m > i_{t+1} > \cdots > i_s > i_1 = 1,
\]

i.e. the values occurring in $c$ between $i_1 = 1$ and $i_t = m$ appear in increasing order, and the values from $i_t = m$ to $i_1 = 1$ appear in decreasing order.

Suppose now that (4.1) is valid for all connected permutations with at most $r$ cycles, and let $\sigma$ be a connected permutation with $r+1$ cycles $c_1, \ldots, c_{r+1}$, ordered in increasing order of their minimal elements. Let $a = \min(c_{r+1})$, $b = \max(c_{r+1})$, and $\sigma' = (c_1, \ldots, c_r)$, $a' = \min\{i \mid \sigma'(i) \neq i\}$, $b' = \max\{i \mid \sigma'(i) \neq i\}$. Then $m = \max(b, b') > \min(b, b') > \max(a, a') > \min(a, a') = 1$. Moreover, the split type of $\sigma'$ is a connected permutation in $S_{m'}$, where $m' = b' - a' + 1$. 

Using the induction hypothesis we obtain
\[ \ell_1(\sigma) = \ell_1(\sigma') + \ell_1(\varepsilon_{r+1}) \geq 2(m' - 1) + 2(b - a) >
\]
\[ > 2(\max(b, b') - \min(a, a')) = 2(m - 1), \]
so the inequality (5.1) follows by induction. \(\square\)

Theorem 3.1 implies that the cardinality \(V_{\ell_p,n}(R)\) of a ball of fixed radius \(R\) with respect to the distance \(\ell_p\) grows polynomially in \(n\), with the degree of the polynomial not exceeding \(R^p/2\). For the distance \(\ell_1\) we can be more precise.

**Theorem 4.2.** Let \(k\) be a positive integer. For \(n \geq k\), we have
\[
A_{\ell_1,n}(2k) = \binom{n-k}{k} + \text{positive terms of degree at most } k - 1,
\]
\[
V_{\ell_1,n}(2k) = \binom{n-k}{k} + \text{positive terms of degree at most } k - 1.
\]

**Proof.** If \(\sigma\) is a split type with \(\ell_1(\sigma) = 2k\), then \(q(\sigma) \leq m(\sigma) - q(\sigma) \leq k\). The split type \(\sigma = (21) + \cdots + (21)\) is the only one with \(k\) parts, and \(m(\sigma) = 2k\). Therefore \(\beta_{\ell_1}(2k, m, k) = 1\) if \(m = 2k\) and 0 otherwise. Theorem 3.1 implies the formula for \(A_{\ell_1,n}(2k)\), and the formula for \(V_{\ell_1,n}(2k)\) is an immediate consequence. \(\square\)

In the rest of this section we discuss results related to other distances.

**Remark 4.3.** If \(I\) is the Kendall metric, then \(A_{I,n}(k)\) is a polynomial of degree \(k\) in \(n\) for \(n \geq k\) (see [Knu73] p. 15, where an exact formula is also given). We use our result on \(\ell_1\) to give an alternative proof of this result. By [DG77] Theorem 2 we know that \(\ell_1(u) \leq 2I(u)\), and therefore
\[
S_{I,n}(k) \subset B_{I,n}(k) \subset B_{\ell_1,n}(2k).
\]
As a consequence, both \(A_{I,n}(k)\) and \(V_{I,n}(k)\) grow at most polynomially of degree \(k\) in \(n\). If \(\sigma\) is a split type and \(I(\sigma) \leq k\), then Proposition 4.1 implies \(m(\sigma) - q(\sigma) \leq k\); therefore \(q(\sigma) \leq k\) and the polynomial growth formula (5.1) is valid for \(n \geq k\). There exists exactly one split type \(\sigma\) with \(I(\sigma) = k\) and \(q(\sigma) = k\). This is the split type \(\sigma = (21) + (21) + \cdots + (21)\), with \(k\) terms in the concatenation, and \(m(\sigma) = 2k\). Hence \(\beta_{I}(k, m, k) = 1\) if \(m = 2k\) and 0 otherwise. Therefore for \(n \geq k\),
\[
A_{I,n}(k) = \binom{n-k}{k} + \text{positive terms of degree at most } k - 1,
\]
\[
V_{I,n}(k) = \binom{n-k}{k} + \text{positive terms of degree at most } k - 1.
\]
Hence \(A_{I,n}(k) \approx A_{\ell_1,n}(2k)\) and \(V_{I,n}(k) \approx V_{\ell_1,n}(2k)\) up to terms of degree \(k-1\), and therefore the relative errors converge to 0 as \(n\) goes to \(\infty\).

Even though Equation (5.1) does not seem to give a general formula for \(A_{I,n}(k)\) as in [Knu73], it has the advantage that the formulas it generates are **positive**: they express \(A_{I,n}(k)\) as a sum of positive terms, consistent with the fact that \(A_{I,n}(k)\) counts permutations with certain properties.

**Remark 4.4.** The cardinalities of \(\ell_\infty\)-balls of fixed radii satisfy linear recurrences in \(n\) ([Sta97 Prop. 4.7.8], [Ku02]). They grow at least exponentially in \(n\) and an exponential lower bound is also given in [Klos11]. Note that the \(\ell_\infty\) distance does
not satisfy the conditions of Theorems \[5.1\] and \[5.2\] if \(\sigma_r\) is the concatenation of \(r\) copies of (21), then \(\ell_\infty(\sigma_r) = 1\) but \(m(\sigma_r) - q(\sigma_r) = r \rightarrow \infty\) as \(r \rightarrow \infty\).

**Remark 4.5.** The Hamming distance shows that the condition is not necessary. Cardinalities of spheres and balls of fixed radii grow polynomially, but for every \(r\), the transposition \(\sigma\) that swaps 1 and \(r\) is a split type in \(S_r\) and \(H(\sigma_r) = 2\), even though \(m(\sigma_r) - q(\sigma_r) = r - 1 \rightarrow \infty\) as \(r \rightarrow \infty\). What remains true, however, is that an eventual polynomial growth implies a bound on the number of parts of a split type: let \(d(R)\) be the degree of \(P\). The terms of highest degree in \(5.1\) are not cancelled, hence that highest degree cannot exceed \(d(R)\). Therefore \(q(\sigma) \leq d(R)\) for all split types \(\sigma\) with \(D(\sigma) \leq R\).

5. **HIGH DEGREE TERMS**

In the remaining sections of this paper we focus on the cardinality of spheres for the distance \(D = \ell_1\), namely on \(A_{\ell_1,n}(2k) = A_n(2k)\). For \(n \geq k\), this number is given by the \(k\)-th-degree polynomial

\[
P_k(n) = \sum_{q=1}^{k} \sum_{m=2q}^{q+k} \beta(2k, m, q) \binom{n + q - m}{q} = \binom{n - k}{k} + \text{lower degree terms}.
\]

In this section we determine high degree terms of this polynomial.

Maximal distances in \(S_n\) and cardinalities of spheres of maximal radius have been determined in [DG77]. Their results imply the following.

**Lemma 5.1.** If \(m = 2r\) is even, then \(\beta(2k, 2r, q) = 0\) if \(k > r^2\) and

\[
\beta(2r^2, 2r, q) = \begin{cases} (r!)^2, & \text{if } q = 1 \\ 0, & \text{otherwise.} \end{cases}
\]

If \(m = 2r + 1\) is odd, then \(\beta(2k, 2r + 1, q) = 0\) if \(k > r^2 + r\) and

\[
\beta(2r^2 + 2r, 2r + 1, q) = \begin{cases} (2r + 1)(r!)^2, & \text{if } q = 1 \\ 0, & \text{otherwise.} \end{cases}
\]

**Proof.** If \(m = 2r\) is even, then the maximal distance \(2k = 2r^2 + 2r\) is achieved by permutations \(\sigma \in S_{2r}\) with the property that \(\sigma(i) > r\) for all \(i \leq r\), and there are \((r!)^2\) such permutations. All of them are connected, because the cycle containing 1 must coincide or overlap with the cycle containing \(m = 2r\), hence all of them are split types with \(q = 1\).

If \(m = 2r + 1\) is odd, then the maximal distance is attained for permutations \(\sigma \in S_{2r+1}\) with the property that \(\sigma(i) > r\) for \(i \leq r\) and \(\sigma(i) \leq r\) for \(i > r\). There are \((2r + 1)(r!)^2\) such permutations. All of them are connected, because the cycle containing 1 must coincide or overlap with the cycle containing \(m = 2r + 1\), hence they are all split types with \(q = 1\).

\[
\begin{array}{c|cccccccc}
\hline
m & 2 & 3 & 4 & 5 & 6 & 7 \\
2k & 2 & 4 & 8 & 12 & 18 & 24 \\
\hline
\end{array}
\]

For small \(m\) the maximal \(\ell_1\)-distances in \(S_m\) are given below.

**Therefore:**

- If \(k \leq 3\) and \(\beta(2k, m, 1) \neq 0\), then \(m = k + 1\).
- If \(k \leq 5\) and \(\beta(2k, m, 1) \neq 0\), then \(m \geq k\).
- If \(k \leq 7\) and \(\beta(2k, m, 1) \neq 0\), then \(m \geq k - 1\).
Lemma 5.2. If \( k \leq 8 \) and \( \beta(2k, m, 1) \neq 0 \), then \( m \geq k - 2 \).

If \( k \leq 9 \) and \( \beta(2k, m, 1) \neq 0 \), then \( m \geq k - 3 \).

These simple observations allow us to prove the following result.

**Lemma 5.3.** If \( q \geq k - 8 \) and \( \beta(2k, m, q) \neq 0 \), then:

- either \( m \geq k + q - 3 \), or
- \( q = k - 8, m = 2k - 12 \). Then \( \beta(2k, 2k - 12, k - 8) = 36(k - 8) \), and \( k \geq 9 \).

**Proof.** By Equation (3.2) we have

\[
\beta(2k, m, q) = \sum_{(k_1, \ldots, k_q)} \sum_{(m_1, \ldots, m_q)} \prod_{i=1}^{q} \beta(2k_i, m_i, 1)
\]

with sums over \( q \)-compositions of \( k \) and \( m \), respectively. Then \( \beta(2k, m, q) \neq 0 \) implies that for at least one pair of compositions, all the terms \( \beta(2k_i, m_i, 1) \) are non-zero. Suppose \((k_1, \ldots, k_q)\) and \((m_1, \ldots, m_q)\) are compositions of \( k \) and \( m \) respectively such that \( \beta(2k_i, m_i, 1) \neq 0 \) for all \( i = 1, \ldots, q \). Without loss of generality we can assume \( k_1 \geq k_2 \geq \cdots \geq k_q \). Then

\[
k = k_1 + \cdots + k_q \geq 1 + k_2 + k_3 + (q - 3) \geq k_1 + k_2 + k_3 + k - 11,
\]

so \( k_1 + k_2 + k_3 \leq 11 \). Similarly \( k_1 + k_2 \leq 10 \) and \( k_1 \leq 9 \). Hence at most two parts of the composition have \( k_i \geq 4 \), at most one part has \( k_i \geq 6 \), and no part exceeds 9. This shows that only the following situations are possible:

- \( k_1 \leq 3 \). No part is above 3, hence \( m_i = k_i + 1 \) for all \( q \) parts, so \( m = k + q \).
- \( k_2 \leq 3 \leq k_1 \leq 8 \). Only one part is above 3, and that part is under 8. Then \( m = m_i = k_i + 1 \) for all but at most one part, and \( m_1 \geq k_1 - 2 \) for the last part. In this case we have \( m \geq k + q - 3 \).
- \( k_2 \leq 3 < k_1 \leq 9 \). Only one part is above 3, and that part is of length 9. Then \( q = k - 8, k_2 = \cdots = k_q = 1 \), \( m_2 = \cdots = m_q = 2 \) and \( 6 \leq m_1 \leq 10 \), so \( m = m_1 + 2(q - 1) = m_1 + 2k - 18 \). The only case when \( m < k + q - 3 = 2k - 11 \) is when \( m_1 = 6 \), and then \( m = 2k - 12 \). Then the \( q \)-compositions of \( k \) and \( m \) are \((9, 1, \ldots, 1)\) and \((6, 2, \ldots, 2)\), respectively. There are \( q = k - 8 \) possible places for the part of \( k \) of length 9, \( \beta(18, 6, 1) = 36 \), and \( \beta(2, 2, 1) = 1 \), hence \( \beta(2k, 2k - 12, k - 8) = 36(k - 8) \).
- \( k_3 \leq 3 < k_2 = 4 \leq k_1 = 6 \). Only two parts are above 3: one is \( k_1 = 6 \) and the other is \( k_2 = 4 \). Then \( m_i = k_i + 1 \) for all but at most two parts, and for those two parts \( m_2 \geq k_2 \) and \( m_1 \geq k_1 - 1 \). In this case we have \( m \geq k + q - 3 \).
- \( k_3 \leq 3 < k_2 \leq k_1 \leq 5 \). Then \( m_1 \geq k_1, m_2 \geq k_2 \), and \( m_i \geq k_i + 1 \) for all other parts, hence \( m \geq k + q - 2 \).

Therefore the only case when \( m < k + q - 3 \) is when \( q = k - 8 \) and \( m = 2k - 12 \). In that situation, \( \beta(2k, 2k - 12, k - 8) = 36(k - 8) \), hence we must have \( k \geq 9 \). \( \square \)

The following estimate is an immediate consequence of Lemma 5.2.

**Lemma 5.3.** The \( k^{th} \)-degree polynomial

\[
Q_k(n) = \sum_{q=1}^{k} \sum_{m=k+q-3}^{k+q} \beta(2k, m, q) \binom{n - m + q}{q} + 36(k - 8) \binom{n - k + 4}{k - 8}
\]

agrees with \( P_k \) on terms of degree \( k - 8 \) and higher. Moreover \( P_k = Q_k \) for \( k \leq 9 \).
To determine $Q_k$ we need to determine $\beta(2k,m,q)$ for $m = k + q, \ldots, k + q - 3$.

**Lemma 5.4.** If $\sigma \in S_m$ is a connected split type and $\ell_1(\sigma) = 2k$, then $\sigma$ has at most $k + 2 - m$ cycles.

**Proof.** Let $c_1, \ldots, c_t$ be the cycles in $\sigma$, with $t \geq 1$. Let $[i_1, j_1], \ldots, [i_t, j_t]$ be the ranges of those cycles, such that $1 = i_1 < i_2 < \cdots < i_t$. Let $[j'_1, \ldots, j'_t]$ be the right endpoints of those ranges, sorted in increasing order: $\{j'_1, \ldots, j'_t\} = \{j_1, \ldots, j_t\}$ and $j'_1 < j'_2 < \cdots < j'_t = m$. Since $\sigma$ is connected, its cycles are linked, hence $j'_s > i_{s+1}$ for all $s = 1, \ldots, t-1$. Then

$$2k = \ell_1(\sigma) = \ell_1(c_1) + \cdots + \ell_1(c_t) \geq 2(j_1 - i_1) + \cdots + 2(j_t - i_t) = (5.2) \quad 2(m - 1) + 2(j'_1 - i_1) + \cdots + 2(j'_{t-1} - i_t) \geq 2(m - 1) + 2(t - 1) = 2(m + t - 2).$$

Hence $\sigma$ can’t have more than $t_0 = k + 2 - m$ cycles. \hfill \Box

Let $t$ be the number of cycles of a connected split type $\sigma \in S_m$. The excess of $\ell_1(\sigma)$ over the minimum $2(m + t - 2)$ occurs from two sources, corresponding to the inequalities in the first two lines of (5.2):

1. cycles of $\sigma$ are not monotone, i.e. values that occur in the part from $i_s$ to $j_s$ are not in increasing order, or values that occur in the part from $j_s$ to $i_s$ are not in decreasing order.
2. cycles of $\sigma$ are not minimally linked, i.e. $j'_s - i_{s+1} > 1$ for some endpoints;

For example, the cycle $c = (1, 4, 2, 3, 6, 5, 10, 8, 9)$ has the blocks $4 \to 2 \to 3$ and $6 \to 5$ in the part from 1 to 10 but not in increasing order, and the block $8 \to 9$ in the part from 10 to 1 but not in decreasing order.

We can now compute the coefficients $\beta(2k,m,q)$ for $m = k + q, \ldots, k + q - 3$.

**Lemma 5.5.** The coefficients $\beta(2k,m,q)$ for $m = k + q, \ldots, k + q - 3$ are

$$\beta(2k,k + q, q) = \binom{k-1}{q-1} 3^{k-q} \quad (5.3)$$

for all $1 \leq q \leq k$;

$$\beta(2k,k+q-1, q) = 4(k-3) \binom{k-4}{q-1} 3^{k-q-3} \quad (5.4)$$

if $1 \leq q \leq k-3$, and 0 otherwise;

$$\beta(2k,k+q-2, q) = 4(k-5) \binom{k-7}{q-1} + 15 \binom{k-6}{q-1} 3^{k-q-6} \quad (5.5)$$

if $1 \leq q \leq k-5$, and 0 otherwise;

$$\beta(2k,k+q-3, q) = 4(k-7) \binom{k-8}{q-1} (8(k-q)^2 + 60(k-q) - 137) 3^{k-q-10} \quad (5.6)$$

if $1 \leq q \leq k-7$, and 0 otherwise.

**Proof.** To prove (5.3) we start with $q = 1$ and determine $\beta(2k,k+1,1)$ for $k \geq 1$. If $\sigma \in S_{k+1}$ is a connected split type counted by $\beta(2k,k+1,1)$, then by Lemma 5.4 $\sigma$ must be a cycle, and by the proof of Proposition 4.1 this cycle must be monotone: the values between 1 and $k+1$ must occur in increasing order, and the values between $k+1$ and 1 in decreasing order. For each of the $k-1$ values $2, 3, \ldots, k$ we
have three possibilities: the value appears on the part from 1 to \( k + 1 \), on the part from \( k + 1 \) to 1, or doesn’t appear at all in the cycle. The choices are independent and each set of choices completely determines the permutation \( \sigma \). Therefore

\[
\beta(2k, k + 1, 1) = 3^{k-1}.
\]

If \((k_1, \ldots, k_q)\) and \((m_1, \ldots, m_q)\) are \( q \)-compositions that appear in the sum (3.2) and \( m = k + q \), then \( m_i = k_i + 1 \) for all \( i = 1, \ldots, q \) and therefore

\[
\beta(2k, k + q, q) = \sum_{(k_1, \ldots, k_q)} \prod_{i=1}^{q} \beta(2k, k_i + 1, 1) = \sum_{(k_1, \ldots, k_q)} \prod_{i=1}^{q} 3^{k_i-1} = 3^{k-q} \sum_{(k_1, \ldots, k_q)} \prod_{i=1}^{q} \frac{k}{k_i - 1} = 3^{k-q} \left( \begin{array}{c} k-1 \\ q-1 \end{array} \right).
\]

To prove the formula (5.3) we consider first the case \( q = 1 \) and prove that

\[
\beta(2k, k, 1) = 4(k - 3)3^{k-4}.
\]

If \( \sigma \in S_k \) is a split type such that \( \ell_1(\sigma) = 2k \), then \( \sigma \) can have at most 2 cycles.

If \( \sigma \) has two cycles \( c_1 \) and \( c_2 \), then they have to overlap, so \( \text{range}(c_1) = [1, j] \) and \( \text{range}(c_2) = [i, k] \), or \( \text{range}(c_1) = [i, k] \) and \( \text{range}(c_2) = [i, j] \), with \( i < j \). Since

\[
2k = \ell_1(\sigma) = \ell_1(c_1) + \ell_1(c_2) \geq 2k + 2(j - i - 1) = 2k,
\]

we must have \( j = i + 1 \) and the cycles have to be monotone. In both cases there are \( k-3 \) ways of choosing the pair \((i, i+1)\). For each choice, for each of the remaining \( k-4 \) values, the cycle it belongs to, if any, is determined. There are three possibilities for each of the remaining \( k-4 \) values: to be on the ascending part of the cycle, on the descending part, or to not be in the cycle at all. Consequently, there are \( 2(k-3)3^{k-4} \) split types with two cycles.

If \( \sigma \) has only one cycle \( c \), the only way to increase \( \ell_1 \) by exactly 2 over the minimum \( 2(k-1) \) is to have two adjacent values occurring in the opposite order to the ascending/descending part they belong to: \( 1 \rightarrow i+1 \rightarrow i \rightarrow k \) or \( k \rightarrow i \rightarrow i+1 \rightarrow 1 \). In each of the two cases there are \( k-3 \) ways of choosing the pair \((i, i+1)\), and for each choice, there are three possibilities for each of the remaining \( k-4 \) values. Hence the number of split types \( \sigma \in S_k \) consisting of one cycle such that \( \ell_1(\sigma) = 2k \) is \( 2(k-3)3^{k-4} \).

Therefore

\[
\beta(2k, k, 1) = 2(2k-3)3^{k-4} + 2(k-3)3^{k-4} = 4(k-3)3^{k-4},
\]

hence (5.7). In particular, for \( \beta(2k, k, 1) \) to be positive, we must have \( k \geq 4 \).

Let \((k_1, k_2, \ldots, k_q)\) be a composition of \( k \). If a composition \((m_1, \ldots, m_q)\) of \( m = k+q-1 \) contributes to \( \beta(2k, k+q-1, q) \), then \( m_i \leq k_i + 1 \) for all \( i = 1, \ldots, q \), which implies

\[
k + q - 1 = m = m_1 + \cdots + m_q \leq (k_1 + 1) + \cdots + (k_q + 1) = k + q.
\]

This can only happen is if \( m_i = k_i + 1 \) for \( q-1 \) values of \( i \) and \( m_{i_0} = k_{i_0} \) for exactly one value \( i_0 \). But for \( \beta(2k_{i_0}, k_{i_0}, 1) \) to be nonzero, we must have \( k_{i_0} \geq 4 \), hence one of the parts of the composition of \( k \) must be of order at least 4, which implies \( q \leq k-3 \).

We determine all the pairs \((k_1, \ldots, k_q), (m_1, \ldots, m_q)\) of compositions of \( k \) and \( m = q + k - 1 \) that give nonzero contributions to \( \beta(2k, k+q-1, q) \) by deciding beforehand which index \( i \) corresponds to the term with \( m_i = k_i \). Select an index
1 \leq i_0 \leq q. Let \((k_1, \ldots, k_q), (m_1, \ldots, m_q)\) be a pair of partitions with a nonzero contribution such that \(m_i = k_i\). Then \(m_i = k_i\) for all \(i \neq i_0\), hence the partition \((m_1, \ldots, m_q)\) is completely determined by the pair \([(k_1, \ldots, k_q), i_0]\). Let \(k_i' = k_i\) for all \(i \neq i_0\) and \(k_i' = k_i - 3 \geq 1\). Then \((k_1', \ldots, k_q')\) is a composition of \(k - 3\). The process is reversible, hence the pairs \([(k_1, \ldots, k_q), (m_1, \ldots, m_q)]\) are indexed by pairs \([(k_1', \ldots, k_q'), i_0]\) consisting of a partition of \(k - 3\) into positive parts and an index \(1 \leq i_0 \leq q\). The contribution of such a pair is

\[
\beta(2k_1, \alpha_1 + 1, 1) \cdots \beta(2k_i, \alpha_i, 1) \cdots \beta(2k_q, \alpha_q + 1, 1) = 4k_i' 3^{k-q-3}.
\]

The contribution of all pairs from the same composition of \(k - 3\) is then

\[
4(k_1' + \cdots + k_q') 3^{k-q-3} = 4(k - 3) 3^{k-q-3},
\]

and there are \(\binom{k-4}{q-1}\) such compositions, hence (5.7).

The proofs of (5.5) and (5.6) are similar but the bookkeeping is more elaborate.

\[\square\]

**Remark 5.6.** The polynomial

\[
R_k(n) = \sum_{q=1}^{k} \beta(2k_q, k + q, q) \binom{n-k}{q} = \sum_{q=1}^{k} \binom{k-1}{q-1} 3^{k-q} \binom{n-k}{q}
\]

agrees with \(P_k\) on terms of degree \(k-2\) and higher and is exact for \(k \leq 3\). The generating function of \(R_k\) is

\[
f_k(X) = \sum_{n \geq 0} R_k(n) X^n = \frac{X^{k+1}(2X - 3)^{k-1}}{(X - 1)^{k+1}}.
\]

### 6. Spheres of Small Radius

Combining Lemmas 5.3 and 5.5 we obtain formulas for \(P_k(n)\) for \(k \leq \min(9, n)\). The polynomials for \(k \leq 6\) are:

\[
P_1(n) = \binom{n-1}{1} = n - 1
\]

\[
P_2(n) = \binom{n-2}{2} + 3 \binom{n-2}{1} = \frac{1}{2} (n^2 + n - 6)
\]

\[
P_3(n) = \binom{n-3}{3} + 6 \binom{n-3}{2} + 9 \binom{n-3}{1} = \frac{1}{6} (n^3 + 6n^2 - 25n - 6)
\]

\[
P_4(n) = \binom{n-4}{4} + 9 \binom{n-4}{3} + 27 \binom{n-4}{2} + 27 \binom{n-4}{1} + 4 \binom{n-3}{1}
\]

\[
P_5(n) = \binom{n-5}{5} + 12 \binom{n-5}{4} + 54 \binom{n-5}{3} + 108 \binom{n-5}{2} + 81 \binom{n-5}{1} +
\]

\[+ 8 \binom{n-4}{2} + 24 \binom{n-4}{1}
\]

\[
P_6(n) = \binom{n-6}{6} + 15 \binom{n-6}{5} + 90 \binom{n-6}{4} + 270 \binom{n-6}{3} + 405 \binom{n-6}{2} +
\]

\[+ 243 \binom{n-6}{1} + 12 \binom{n-5}{3} + 240 \binom{n-5}{2} + 108 \binom{n-5}{1} + 20 \binom{n-4}{1}.
\]
We can use the expressions above to compute the cardinality of spheres of radius $2k$ in $S_n$ for $k \leq 6$ and for all $n \geq 2$, not just for $n \geq k$. All we have to do is replace the binomial coefficient $\binom{x}{y}$ by 0 if $a < 0$. Nothing interesting occurs for $k \leq 5$: $A_{\ell_1,2k}(n) = P_k(n)$ if $n \geq k$ and $A_{\ell_1,2k}(n) = 0$, if $n < k$. But when $k = 6$, then $A_{\ell_1,12}(n) = P_6(n)$ for $n \geq 6$, and $A_{\ell_1,12}(n) = 0$ only for $n \leq 4$. For $n = 5$,

$$A_{\ell_1,12}(5) = \# \{ u \in S_5 \mid \ell_1(u) = 12 \} = 20$$

is computed from the expression for $P_6(5)$ by ignoring all but the last term.

References

[DG77] Persi Diaconis and R. L. Graham. Spearman’s footrule as a measure of disarray. *J. Roy. Statist. Soc. Ser. B*, 39(2):262–268, 1977.

[DH98] Michel Deza and Tayuan Huang. Metrics on permutations, a survey. *J. Combin. Inform. System Sci.*, 23(1-4):173–185, 1998.

[Eli11] Sergi Elizalde. The X-class and almost-increasing permutations. *Ann. Comb.*, 15(1):51–68, 2011.

[Klo11] Torleiv Kløve. Lower bounds on the size of spheres of permutations under the Chebychev distance. *Des. Codes Cryptogr.*, 59(1-3):183–191, 2011.

[Knu73] Donald E. Knuth. *The art of computer programming. Volume 3*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1973. Sorting and searching, Addison-Wesley Series in Computer Science and Information Processing.

[KS02] O. Krafft and M. Schaefer. On the number of permutations within a given distance. *Fibonacci Quart.*, 40(5):429–434, 2002.

[Sta97] Richard P. Stanley. *Enumerative combinatorics. Vol. 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997.