

On the base size for the symmetric group acting on subsets

Zoltán Halasi*

Abstract

Let k, n be natural numbers with $k \leq n/2$ and let $X_{n,k}$ denote the set of k -element subsets of $\{1, 2, \dots, n\}$. The symmetric group S_n acts in a natural way on the set $X_{n,k}$. Motivated by the question of Robert Guralnick, we investigate the size of a minimal base for this action. We give constructions providing a minimal base if $n = 2k$ or if $n \geq k^2$. We also describe a general process providing a base of size at most c times bigger than the size of a minimal base for some universal constant c .

1 Introduction

Let G be a finite permutation group acting on the finite set Ω . A subset $\{\omega_1, \omega_2, \dots, \omega_l\} \in \Omega$ is called a base for G , if its point-wise stabilizer in G is trivial. The minimal base size for G is the minimal number $b(G)$ such that a base of size $b(G)$ exists. Since any element of G is determined by the images of the base elements, it follows that $|G| \leq |\Omega|^{b(G)}$. Taking logarithm, one get the lower bound $b(G) \geq \frac{\ln |G|}{\ln |\Omega|}$. On the other hand, a conjecture of L. Pyber asserts that for a primitive permutation group G acting on Ω the upper bound $b(G) \leq c \cdot \frac{\ln |G|}{\ln |\Omega|}$ holds with some universal constant $c > 1$. In this paper we try to find the minimal base size for the symmetric group acting on k -sets. Although Pyber's conjecture is solved in this case [4] (see also [1, Proposition 2.6]), for computational reasons it is important to find a specific base for a permutation group in size as near to the minimal base size as possible.

Now, let S_n be the symmetric group acting on the set $\Omega_n = \{1, 2, \dots, n\}$. Then for any $k \leq n$ one can define an induced action of S_n on the set of k -elements subsets $X_{n,k} = \{A \subseteq \Omega_n \mid |A| = k\}$. The action of S_n on $X_{n,k}$ is clearly isomorphic to its action on $X_{n,n-k}$, therefore, we shall assume in the following that $k \leq n/2$. We will denote the minimal base size for this action by $f(n, k)$. If $\mathcal{A} = \{A_1, A_2, \dots, A_l\} \subseteq X_{n,k}$ is any set of k -element subsets of Ω_n , and $x \in \Omega_n$, then we define the neighborhood of x as $N_{\mathcal{A}}(x) = \{A_i \in \mathcal{A} \mid x \in A_i\}$. It is clear that $\mathcal{A} \subseteq X_{n,k}$ is a base for S_n if and only if $N_{\mathcal{A}}(x) \neq N_{\mathcal{A}}(y)$ for any $x, y \in \Omega$, $x \neq y$.

In the following section we confirm some monotonic properties of the function $f(n, k)$. In Section 3 we investigate the cases when k is large or small compared to n , namely, if $k = n/2$ or if $k^2 \leq n$. In these cases we give the precise value

*Research supported by Hungarian National Research Fund (OTKA) under grant number NK72523.

of $f(n, k)$ and we also construct a base of minimal size. Finally, in Section 4 we show a general construction providing a base not very far from being a minimal base, which provides the same base as our former constructions in case of $k = n/2$ or $k^2 = n$, and which is asymptotically the best possible in several other cases as well.

Some related results have been obtained by other authors. The lower bound $f(n, k) \geq \lceil \frac{2n-2}{k+1} \rceil$ in Theorem 3.2 appears in the unpublished Ph.D. thesis of T. Maund [2]. On the other hand a general upper bound was established by C. Benbenishty in her (also unpublished) Ph.D. thesis [4]. However, compared to ours, her upper bound is not asymptotically the best.

2 Monotonic properties of $f(n, k)$

For a fixed n and $k \leq n/2$ let us consider the (intransitive) action of S_n on the set $Y_{n,k} = \{B \subseteq \Omega_n \mid |B| \leq k\}$ and let $g(n, k)$ denote the minimal base size for this action. For a subset $\mathcal{B} \subseteq Y_{n,k}$ and for an $x \in \Omega_n$ let $N_{\mathcal{B}}(x) = \{B \in \mathcal{B} \mid x \in B\}$ be the neighborhood of x .

Theorem 2.1. *For every pair of natural numbers n, k with $k \leq n/2$ we have $f(n, k) = g(n, k)$.*

Proof. Of course, $f(n, k) \geq g(n, k)$. To prove that $g(n, k) \geq f(n, k)$ let $l = g(n, k)$ and $\mathcal{B} = \{B_1, B_2, \dots, B_l\} \subseteq Y_{n,k}$ be a minimal base for S_n such that $|B_i| \leq k$ for each $1 \leq i \leq l$ and $w(B_1, B_2, \dots, B_l) = \sum_{i=1}^l |B_i|$ is as large as possible. We shall prove that $|B_i| = k$ for each $1 \leq i \leq l$. Assuming that $|B_s| < k$ for some $1 \leq s \leq l$ let $x \in \overline{B_s} = \Omega \setminus B_s$. Then

$$w(B_1, \dots, B_{s-1}, B_s \cup \{x\}, B_{s+1}, \dots, B_l) > w(B_1, B_2, \dots, B_l),$$

hence $\{B_1, \dots, B_{s-1}, B_s \cup \{x\}, B_{s+1}, \dots, B_l\} \subseteq Y_{n,k}$ is not a base for G . It follows that there exists a $y = y(x) \in B_s$ such that

$$\begin{aligned} N_{\mathcal{B}}(y) &= \{B_i \mid 1 \leq i \leq l, y \in B_i\} \\ &= \{B_i \mid 1 \leq i \leq l, x \in B_i\} \cup \{B_s\} = N_{\mathcal{B}}(x) \cup \{B_s\}. \end{aligned}$$

Such a $y(x)$ must be unique: If $y_1(x) \neq y_2(x)$ would be two elements with the above properties for some $x \in \overline{B_s}$, then $N_{\mathcal{B}}(y_1) = N_{\mathcal{B}}(y_2)$ contradicting the assumption that $\mathcal{B} \subseteq Y_{n,k}$ is a base for S_n . Similarly, if $y(x_1) = y(x_2)$ for some $x_1, x_2 \in \overline{B_s}$, then $x_1 = x_2$ holds. It follows that $y : \overline{B_s} \rightarrow B_s$, $x \rightarrow y(x)$ is an injective function, hence $n - |B_s| = |\overline{B_s}| \leq |B_s|$, and $n \leq 2|B_s| < 2k$, a contradiction. \square

Remark. The above proof actually gives us an algorithm which can be used to complete a (minimal) base for S_n in $Y_{n,k}$ to a (minimal) base for S_n in $X_{n,k}$.

Corollary 2.2. *The function $f(n, k)$ is monotonic increasing in its first variable, and it is monotonic decreasing in its second variable, that is*

1. For every k and $n_1 > n_2 \geq 2k$ we have $f(n_1, k) \geq f(n_2, k)$.
2. For every n and $k_1 < k_2 \leq n/2$ we have $f(n, k_1) \geq f(n, k_2)$.

Proof. To prove 1 it is enough to confirm that $f(n+1, k) \geq f(n, k)$ for every $k, n \in \mathbb{N}, n \geq 2k$. Using the definition of $l = f(n+1, k)$ we can choose subsets $A_1, A_2, \dots, A_l \subseteq \{1, 2, \dots, n+1\}$ such that $|A_i| = k$ for each $1 \leq i \leq l$, and $\mathcal{A} = \{A_1, A_2, \dots, A_l\}$ is a base for S_{n+1} acting on the set

$$X_{n+1, k} = \{A \subseteq \{1, 2, \dots, n+1\} \mid |A| = k\}.$$

Then the set $\mathcal{B} = \{B_i = A_i \setminus \{n+1\} \mid 1 \leq i \leq l\} \subseteq Y_{n, k}$ is a base for S_n . Using Theorem 2.1 and the definition of $g(n, k)$ we get

$$f(n, k) = g(n, k) \leq l = f(n+1, k).$$

If $k_1 < k_2 \leq n/2$ then $Y_{n, k_1} \subseteq Y_{n, k_2}$, so $g(n, k_1) \geq g(n, k_2)$. Furthermore, $f(n, k_1) = g(n, k_1)$ and $f(n, k_2) = g(n, k_2)$ by Theorem 2.1, and 2 holds. \square

3 Two Examples

In this section we handle two cases and we give the exact value of $f(n, k)$. In both of these cases we provide a general lower bound to $f(n, k)$, which is equal to $f(n, k)$ only if the ratio of n and k is suitable.

Theorem 3.1. *For any n, k with $n \geq 2k$ we have $f(n, k) \geq \lceil \log_2 n \rceil$. If $n = 2k$, then $f(n, k) = \lceil \log_2 n \rceil$.*

Proof. If $\mathcal{A} = \{A_1, A_2, \dots, A_l\} \subseteq X_{n, k}$ is a base for S_n , then the neighborhood function $N_{\mathcal{A}} : \Omega_n \rightarrow \mathcal{P}(\mathcal{A})$ is injective. Hence $n = |\Omega_n| \leq |\mathcal{P}(\mathcal{A})| = 2^l$, which proves $f(n, k) \geq \log_2 n$. Since $f(n, k)$ is an integer, we get $f(n, k) \geq \lceil \log_2 n \rceil$. Assuming that $n = 2k$ let $l = \lceil \log_2 n \rceil$. For any $x \in \Omega_n$ we define $\varphi(x)$ as the binary form of $x - 1$, completed by zeros in the front, if necessary, such that $\varphi(x)$ has exactly l digits. For every $1 \leq i \leq l$ let $\varphi(x)_i$ be the value of the i -th digit of $\varphi(x)$. Finally, for each $1 \leq i \leq l$ let $A_i = \{x \in \Omega_n \mid \varphi(x)_i = 1\}$. It is easy to see that $\mathcal{A} = \{A_1, A_2, \dots, A_l\} \subseteq X_{n, k}$ is a base for S_n acting on $Y_{n, k}$, hence $g(n, k) \leq l$. Using Theorem 2.1 we get $f(n, k) \leq \lceil \log_2 n \rceil$. \square

Theorem 3.2. *For any n, k with $n \geq 2k$ we have $f(n, k) \geq \left\lceil \frac{2n-2}{k+1} \right\rceil$. If $n \geq k^2$, then $f(n, k) = \left\lceil \frac{2n-2}{k+1} \right\rceil$.*

Proof. Let us assume that $\mathcal{A} = \{A_1, A_2, \dots, A_l\} \subseteq X_{n, k}$ is a base for S_n . For any $x \in \Omega_n$ let the degree of x be defined as $\deg(x) = |N_{\mathcal{A}}(x)|$. Then $\sum_{x \in \Omega_n} \deg(x) = lk$. It is clear that there is at most one element of Ω_n of degree 0 and there are at most l elements of Ω_n of degree 1. So, $lk \geq 0 \cdot 1 + 1 \cdot l + 2 \cdot (n - l - 1)$. It follows that $l \geq \frac{2n-2}{k+1}$. As l is an integer, the first part of the theorem follows. To prove the second part of the theorem, let $n \geq k^2$. Then $l = \left\lceil \frac{2n-2}{k+1} \right\rceil$ if and only if

$$\frac{(l-1)(k+1)+2}{2} < n \leq \frac{l(k+1)+2}{2}.$$

We have to prove that if these inequalities hold for some $n, k, l \in \mathbb{N}$, then $f(n, k) \leq l$. Using the monotonic increasing property of $f(n, k)$ in its first coordinate by Corollary 2.2, it is enough to find a base of size l in $X_{n, k}$ in case

of $n = \lfloor \frac{l(k+1)+2}{2} \rfloor$. In the following we provide a base $A_1, A_2, \dots, A_l \subseteq X_{n,k}$ for such k, l and n .

First let $l = 2d$ be even, so $n = d(k+1) + 1$. Let $\Omega_n = U \cup V \cup W \cup \{n\}$ be a decomposition of Ω_n into disjoint subsets, where the elements of the subsets are indexed as $U = \{u_{ij} \mid 1 \leq i \leq k-1, 1 \leq j \leq d\}$, $V = \{v_1, v_2, \dots, v_d\}$, $W = \{w_1, w_2, \dots, w_d\}$. Let the subsets $A_1, A_2, \dots, A_d, B_1, B_2, \dots, B_d \subseteq X_{n,k}$ be defined as

$$\begin{aligned} A_t &= \{u_{it} \mid 1 \leq i \leq k-1\} \cup \{v_t\} \quad \text{for } 1 \leq t \leq d, \\ B_t &= \{u_{ij} \mid j - i + 1 \equiv t \pmod{d}\} \cup \{w_t\} \quad \text{for } 1 \leq t \leq d. \end{aligned}$$

Then n is the only element of degree zero, $V \cup W$ consists of the elements of degree 1, and U consists of the elements of degree 2. Furthermore, the neighborhood of every element of U is of the form $\{A_t, B_s\}$ and $|A_t \cap B_s| \leq 1$ for each pair A_t, B_s (here we used that $d \geq k-1$, which follows from the assumption $n \geq k^2$). Hence the set $\mathcal{A}_1 = \{A_1, A_2, \dots, A_d, B_1, B_2, \dots, B_d\}$ has the property that $N_{\mathcal{A}_1}(x) \neq N_{\mathcal{A}_1}(y)$ if $x \neq y \in \Omega_n$.

Now let $l = 2d+1$ be odd, so $n = d(k+1) + \lfloor \frac{k+1}{2} \rfloor + 1$. In this case let $\Omega_n = U \cup V \cup W \cup \{n\} \cup S$, where the elements of U, V and W are indexed in the same way as in the previous case and $S = \{s_i \mid 1 \leq i \leq \lfloor \frac{k+1}{2} \rfloor\}$. We start with the same subsets $A_1, A_2, \dots, A_d, B_1, \dots, B_d \subseteq U \cup V \cup W$ defined in the previous case. Using that $d \geq k-1$, we modify A_t for $1 \leq t \leq 2\lfloor \frac{k-1}{2} \rfloor$: Let

$$A'_t = A_t \setminus \{u_{1t}\} \cup \{s_r\} \quad \text{for } 1 \leq r \leq \left\lfloor \frac{k-1}{2} \right\rfloor, \quad t = 2r-1, \text{ or } t = 2r.$$

Furthermore, let $Z = \{u_{11}, u_{12}, \dots, u_{1,k-1}, s_{\lfloor \frac{k+1}{2} \rfloor}\}$. It can easily be shown that the set

$$\mathcal{A}_2 = \left\{ A'_t, 1 \leq t \leq 2 \left\lfloor \frac{k-1}{2} \right\rfloor, A_t, 2 \left\lfloor \frac{k-1}{2} \right\rfloor < t \leq d, B_t, 1 \leq t \leq d, Z \right\}$$

has the property that $N_{\mathcal{A}_2}(x) \neq N_{\mathcal{A}_2}(y)$ if $x \neq y \in \Omega_n$. \square

4 General algorithm

In the last section we saw two constructions, which gave a base in $X_{n,k}$ of minimal size depending on the ratio of n and k . Interestingly, these two cases are rather extreme, and the general case is somewhere between these two cases. In this section we try to fill the gap between the results of the previous section and provide a general construction which always works. In some cases it provides the same constructions given in the last section, but in general it does not provide a base of minimal size. For simplicity, we search for a base in $Y_{n,k}$, since such a base can be completed to a base in $X_{n,k}$ by our Remark following Theorem 2.1.

Algorithm 4.1. *For a fixed n and k with $k \leq n/2$ we construct a base $\mathcal{A} = \{A_1, A_2, \dots, A_l\} \subseteq Y_{n,k}$. The construction consists of steps. In each step we choose $\lceil \frac{n}{k} \rceil - 1$ pairwise disjoint subsets of Ω_n in the following way: Let us assume that we have already chosen i times such a set of subsets, so we have a set of subsets $\mathcal{A}_i = \{A_1, A_2, \dots, A_{l_i}\} \subseteq Y_{n,k}$ with $l_i = i(\lceil n/k \rceil - 1)$. In the $i+1$ -th step we define an equivalence relation \sim_i on Ω_n as $x \sim_i y \iff N_{\mathcal{A}_i}(x) =$*

$N_{\mathcal{A}_i}(y)$. Then each equivalence class consists of a single element if and only if $\mathcal{A}_i \subseteq Y_{n,k}$ is a base for S_n . In this case $\mathcal{A} := \mathcal{A}_i$ is a base of size $i(\lceil n/k \rceil - 1)$. Otherwise, we reorder the elements of Ω_n such that we move equivalent elements side by side. More precisely, let $E_1, E_2, \dots, E_r \subseteq \Omega_n$ be the equivalence classes with respect to the equivalence relation \sim_i and let $\sigma \in S_n$ be a permutation of Ω_n such that

$$\sigma(E_s) = \{\sigma(x) \mid x \in E_s\} = \left\{ y \in \Omega_n \mid \sum_{j=1}^{s-1} |E_j| < y \leq \sum_{j=1}^s |E_j| \right\} \text{ for } 1 \leq s \leq r.$$

Now we define pairwise disjoint subsets $A_{l_i+1}, A_{l_i+2}, \dots, A_{l_i+1} \subseteq Y_{n,k}$ as follows. Let

$$A_{l_i+s} = \{x \in \Omega_n \mid \sigma(x) \equiv s \pmod{\lceil n/k \rceil}\} \text{ for } 1 \leq s \leq \lceil n/k \rceil - 1.$$

Since $k \cdot \lceil n/k \rceil \geq n$, each of these sets has size at most k . Finally, let

$$\mathcal{A}_{i+1} := \mathcal{A}_i \cup \{A_{l_i+1}, A_{l_i+2}, \dots, A_{l_i+1}\} \subseteq Y_{n,k}.$$

Theorem 4.2. *The above algorithm stops after $t = \lceil \log_{\lceil n/k \rceil}(n) \rceil$ steps, so $\mathcal{A} := \mathcal{A}_t \subseteq Y_{n,k}$ is a base of size $\lceil \log_{\lceil n/k \rceil}(n) \rceil \cdot (\lceil n/k \rceil - 1)$.*

Proof. We use the notations of Algorithm 4.1. Let us assume that we did t steps until we reached the trivial equivalence. We define the numbers c_1, c_2, \dots, c_t such that for each $1 \leq j \leq t$ let c_j be the maximum of the sizes of equivalence classes with respect to the relation \sim_j . Let us assume that we did i steps, so we have an equivalence relation \sim_i and a set of equivalence classes E_1, E_2, \dots, E_r . After the $i+1$ -th step, we choose additional disjoint subsets A_{l_i+s} , $1 \leq s < \lceil n/k \rceil$ defined above. Let us define the subsets B_s , $1 \leq s \leq \lceil n/k \rceil$ as

$$B_s = \begin{cases} A_{l_i+s} & \text{for } 1 \leq s < \lceil n/k \rceil; \\ \Omega_n \setminus (B_1 \cup \dots \cup B_{\lceil n/k \rceil - 1}) & \text{for } s = \lceil n/k \rceil. \end{cases}$$

Then each equivalence class with respect to the equivalence relation \sim_{i+1} is of the form $E_j \cap B_s$ for some $1 \leq j \leq r$, $1 \leq s \leq \lceil n/k \rceil$. Let us choose numbers j and s such that $c_{i+1} = |E_j \cap B_s|$. Using the definition of the subset B_s it follows that there are elements $x_1, x_2, \dots, x_{c_{i+1}} \in E_j$ and a permutation $\sigma \in S_n$ such that $\sigma(x_1), \sigma(x_2), \dots, \sigma(x_{c_{i+1}})$ are different elements of Ω_n such that all of them are congruent to s modulo $\lceil n/k \rceil$. It follows that the diameter of the set $\{\sigma(x_1), \sigma(x_2), \dots, \sigma(x_{c_{i+1}})\}$, that is, the distance between its smallest and its largest element, is at least $(c_{i+1} - 1)\lceil n/k \rceil$. Using that the reordering σ moved the elements of E_j side by side, it follows that

$$(c_{i+1} - 1)\lceil n/k \rceil + 1 \leq |\sigma(E_j)| = |E_j| \leq c_i, \text{ hence } c_{i+1} \leq \frac{c_i}{\lceil n/k \rceil} + 1 - \frac{1}{\lceil n/k \rceil}.$$

Starting with $c_0 = n$ (in the beginning the whole Ω_n is one equivalence class) we get

$$\begin{aligned} c_t &\leq \frac{1}{\lceil n/k \rceil} \left(\dots \left(\frac{1}{\lceil n/k \rceil} n + 1 - \frac{1}{\lceil n/k \rceil} \right) \dots \right) + 1 - \frac{1}{\lceil n/k \rceil} \\ &= \frac{n}{\lceil n/k \rceil^t} + \left(1 - \frac{1}{\lceil n/k \rceil} \right) \sum_{j=0}^{t-1} \frac{1}{\lceil n/k \rceil^j} < \frac{n}{\lceil n/k \rceil^t} + 1. \end{aligned}$$

Since c_t is an integer, we get the trivial equivalence if $c_t < 2$. By using the above inequality, \sim_t is the trivial equivalence if $\frac{n}{\lceil n/k \rceil^t} \leq 1$, which is equivalent to the lower bound $\log_{\lceil n/k \rceil}(n) \leq t$. Therefore, $t = \lceil \log_{\lceil n/k \rceil}(n) \rceil$ steps are enough, which proves the theorem. \square

Corollary 4.3. *For any $n, k \in \mathbb{N}$ with $k \leq n/2$ we have*

$$f(n, k) \leq \lceil \log_{\lceil n/k \rceil}(n) \rceil (\lceil n/k \rceil - 1).$$

Remarks. It is easy to check that in some cases the previous general algorithm provides a base of minimal size, namely, if $n = 2k$ or if $n = k^2$. It is even true that in these cases the base given by the general algorithm is isomorphic to the base given in Section 3, where “isomorphic” means that there is a permutation of Ω_n providing a bijection between the two bases.

On the other hand, if n is bigger than k^2 , say, $n = k^2 + k(k+1)m$, then the minimal base size can be arbitrarily smaller than the upper bound given by the above algorithm. In this case

$$\lceil \log_{\lceil n/k \rceil}(n) \rceil (\lceil n/k \rceil - 1) - f(n, k) = 2(k + (k+1)m - 1) - 2(k - 1 + km) = 2m.$$

We close this paper by giving a lower bound to $f(n, k)$ which shows that Algorithm 4.1 provides a base size at most constant times bigger than the minimal base size.

Theorem 4.4. *For any n, k with $n \geq 2k$ we have*

$$\lceil \log_{\lceil n/k \rceil}(n) \rceil (\lceil n/k \rceil - 1) \leq \left(1 + \frac{1}{\ln(2)} + o(1)\right) \cdot f(n, k) \quad \text{as } n \rightarrow \infty.$$

Proof. As we mentioned in the Introduction, if a finite group G acts on the finite set Ω then for the minimal base size $b(G) \geq \frac{\ln|G|}{\ln|\Omega|}$ holds. Using this lower bound and the inequality $n! \geq \left(\frac{n}{e}\right)^n$ we get

$$f(n, k) \geq \frac{\ln(n!)}{\ln \binom{n}{k}} \geq \frac{n \ln(n) - n}{k \ln(n) - \ln(k!)} \geq \frac{n \ln(n) - n}{k \ln(n) - k \ln(k) + k} = \frac{n}{k} \cdot \frac{\ln(n) - 1}{\ln(n/k) + 1}.$$

It follows that

$$\begin{aligned} \frac{\lceil \log_{\lceil n/k \rceil}(n) \rceil (\lceil n/k \rceil - 1)}{f(n, k)} &\leq \frac{(\log_{n/k}(n) + 1)(\ln(n/k) + 1)}{\ln(n) - 1} \\ &= \frac{\ln(n) + 1 + \ln(n/k) + \frac{\ln(n)}{\ln(n/k)}}{\ln(n) - 1} = 1 + o(1) + \frac{1}{\ln(n)} \left(\ln(n/k) + \frac{\ln(n)}{\ln(n/k)} \right). \end{aligned}$$

Choosing $a = \ln(n)$, $x = \ln(n/k)$ we get an upper bound for this last expression by finding the maximum of the function $h(x) = x + \frac{a}{x}$, $\ln(2) \leq x \leq a$. Using standard calculus, we get that $h(x)$ has maximum at $x = \ln(2)$, hence

$$\frac{\lceil \log_{\lceil n/k \rceil}(n) \rceil (\lceil n/k \rceil - 1)}{f(n, k)} \leq 1 + \frac{1}{\ln(2)} + o(1) \approx 2.44 + o(1).$$

\square

Remarks. In fact, the above proof also shows that Pyber’s conjecture holds for the symmetric group acting on k -sets with $c \approx 2.44 + o(1)$. Moreover, if we choose a sequence of (n, k) -s such that both $\log_{n/k}(n) \rightarrow \infty$ and $n/k \rightarrow \infty$, then our upper bound is asymptotically equal to $f(n, k)$.

For some n and k it is possible that after some steps a resulting equivalence class contains a single element. Such elements can clearly be ejected, and in further steps we need only deal with the remaining elements.

The base given in Algorithm 4.1 has the property that it is a union of “almost partitions”, where by an almost partition we mean a set of pairwise disjoint subsets $A_1, A_2, \dots, A_l \subseteq \Omega_n$, each of size k , such that $|\Omega_n \setminus (\cup_i A_i)| < k$. If we restrict our attention to bases in $X_{n,k}$ which are unions of almost partitions, then it is easy to see that the base given by our algorithm is minimal among these bases.

Note: After the first version of this paper was finished we were informed that Cáceres et al. [3] obtained independently results similar to our Theorem 3.2 (see also [1]).

References

- [1] R. F. Bailey and P. J. Cameron, Base size, metric dimension and other invariants of groups and graphs, *Bull. Lond. Math. Soc.* **43** (2011), 209–242.
- [2] T. Maund, Bases for permutation group, Ph.D. thesis, University of Oxford, 1989.
- [3] J. Cáceres, D. Garijo, A. González, A. Márquez, and M.L. Puertas, Hypergraphs for computing Determining Sets for Kneser Graphs, preprint.
- [4] C. Benbenishty, On actions of primitive groups, Ph.D. thesis, Hebrew University of Jerusalem, 2005.

Zoltán Halasi
Institute of Mathematics
University of Debrecen
P. O. Box 12
H-4010 Debrecen
Hungary
e-mail: zhalasi@renyi.hu