

# Cardinal Invariants Related to Permutation Groups

Bart Kastermans

*Department of Mathematics, Sun Yat-Sen University, Guangzhou, 510275, P. R. China and Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA*

Yi Zhang

*Department of Mathematics, Sun Yat-Sen University, Guangzhou, 510275, P. R. China*

---

## Abstract

We consider the possible cardinalities of the following three cardinal invariants which are related to the permutation group on the set of natural numbers:

$\mathfrak{a}_g$  := the least cardinal number of maximal cofinitary permutation groups;

$\mathfrak{a}_p$  := the least cardinal number of maximal almost disjoint permutation families;

$c(\text{Sym}(\mathbb{N}))$  := the cofinality of the permutation group on the set of natural numbers.

We show that it is consistent with ZFC that  $\mathfrak{a}_p = \mathfrak{a}_g < c(\text{Sym}(\mathbb{N})) = \aleph_2$ ; in fact we show that in the Miller model  $\mathfrak{a}_p = \mathfrak{a}_g = \aleph_1 < \aleph_2 = c(\text{Sym}(\mathbb{N}))$ .

---

## 1 Introduction

Let  $\text{Sym}(\mathbb{N})$  be the group of bijections from the natural numbers to the natural numbers. A permutation  $g \in \text{Sym}(\mathbb{N})$  is *cofinitary* if and only if  $g$  is the identity or has only finitely many fixed points. A group  $H \leq \text{Sym}(\mathbb{N})$  is *cofinitary* if and only if all its members are cofinitary. See [C], a survey paper by P. Cameron, for a discussion of different aspects of cofinitary groups. Since the union of a chain of cofinitary permutation groups is cofinitary,

---

*Email addresses:* [bart@kastermans.nl](mailto:bart@kastermans.nl) (Bart Kastermans), [yizhang@umich.edu](mailto:yizhang@umich.edu) (Yi Zhang).

<sup>1</sup> Partially supported by a fellowship from Sun Yat-Sen University.

<sup>2</sup> Partially supported by CNSF 10471158 and China-France-Russia mathematics collaboration grant 34000-3275100.

Zorn's Lemma implies that maximal cofinitary groups do exist, and indeed any cofinitary group is contained in a maximal one. The following theorem was proved by Adeleke [A] and Truss [T].

**Theorem 1** *If  $H \leq \text{Sym}(\mathbb{N})$  is a maximal cofinitary group, then  $H$  is not countable.*

Also, P. Neumann proved the following result (see, e.g. [C, Proposition 10.4]).

**Theorem 2** *There exists a cofinitary group of cardinality  $2^{\aleph_0}$ .*

Thus, P. Cameron (in [C]) asked the following question.

**Question 3** *If the continuum hypothesis (CH) fails, is it possible that there exists a maximal cofinitary group  $H$  such that  $|H| < 2^{\aleph_0}$ ?*

Here *maximal* is with respect to inclusion (a maximal cofinitary group is a cofinitary group not properly contained in another cofinitary group). In [Z], this question was answered by proving the following results.

**Theorem 4** *Martin's Axiom (MA) implies that, if  $H \leq \text{Sym}(\mathbb{N})$  is a maximal cofinitary group, then  $H$  has cardinality  $2^{\aleph_0}$ .*

**Theorem 5** *Let  $M \models \text{ZFC} + \neg\text{CH}$ . Let  $\kappa \in M$  be a cardinal such that  $\aleph_1 \leq \kappa < 2^{\aleph_0} = \lambda$ . Then there exists a countable chain condition notion of forcing  $\mathbb{P}$  such that the following statements hold in  $M^{\mathbb{P}}$ :*

- (1)  $2^{\aleph_0} = \lambda$ ;
- (2) *there exists a maximal cofinitary group  $H \leq \text{Sym}(\mathbb{N})$  of cardinality  $\kappa$ .*

Hence the following cardinal number is non-trivial:

$$\mathfrak{a}_g := \min\{|H| : H \leq \text{Sym}(\mathbb{N}) \text{ is a maximal cofinitary group}\}$$

Two permutations  $f, g \in \text{Sym}(\mathbb{N})$  are *almost disjoint* if and only if  $|f \cap g| < \aleph_0$ , i.e. the set  $\{n \in \mathbb{N} : f(n) = g(n)\}$  is finite. A family  $\mathcal{A} \subseteq \text{Sym}(\mathbb{N})$  is *almost disjoint* iff every two distinct members of  $\mathcal{A}$  are almost disjoint. It is easily seen that  $G \leq \text{Sym}(\mathbb{N})$  is cofinitary iff  $G$  is both an almost disjoint set of permutations and a group. We can prove the corresponding results to Theorem 4 and Theorem 5 for maximal almost disjoint families in  $\text{Sym}(\mathbb{N})$ . S. Thomas suggested a cardinal invariant as follows (e.g. [Z1] or [Z2]).

$$\mathfrak{a}_p := \min\{|\mathcal{A}| : \mathcal{A} \subseteq \text{Sym}(\mathbb{N}) \text{ is a maximal almost disjoint family}\}$$

Suppose that  $H$  is a group that is not finitely generated. Then  $H$  can be expressed as the union of a chain of proper subgroups. The cofinality of  $H$ , written  $c(H)$ , is defined to be the least  $\lambda$  such that  $H$  can be expressed as the union of a chain of  $\lambda$  proper subgroups. The following result was proved by H. D. Macpherson and P. Neumann in [MN].

**Theorem 6** *If  $\kappa$  is an infinite cardinal, then  $c(\text{Sym}(\kappa)) > \kappa$ .*

Upon learning of Theorem 6, A. Mekler and S. Thomas independently pointed out the following easy observation (see, e.g. [ST]).

**Theorem 7** *Suppose that  $M \models \kappa^\omega = \kappa > \aleph_1$ . Let  $\mathbb{P} = \text{Fn}(\kappa, 2)$  be the partial order of finite partial functions from  $\kappa$  to 2. Then  $M^\mathbb{P} \models c(\text{Sym}(\mathbb{N})) = \aleph_1 < 2^\omega = \kappa$ .*

Although it can be proved that MA implies  $c(\text{Sym}(\mathbb{N})) = 2^\omega$  (see, e.g. [ST]), some results indicate that  $c(\text{Sym}(\mathbb{N}))$  is rather small among the cardinal invariants. We give two examples:

(I) If we let  $\mathfrak{d}$  be the dominating number (the minimum cardinality of a dominating family in  ${}^\mathbb{N}\mathbb{N}$ ), then we know that:

**Theorem 8**  $c(\text{Sym}(\mathbb{N})) \leq \mathfrak{d}$ .

For a proof of this see [ST].

(II) A notion of forcing  $\mathbb{P}$  is Suslin if and only if  $\mathbb{P}$  is a  $\Sigma_1^1$  subset of  $\mathbb{R}$  and both  $\leq_\mathbb{P}$  and  $\perp_\mathbb{P}$  are  $\Sigma_1^1$  subsets of  $\mathbb{R} \times \mathbb{R}$ , where  $\mathbb{R}$  denotes the reals. The following result can be proved (see, e.g. [Z2]).

**Theorem 9** *Let  $M \models \text{ZFC} + \text{GCH}$ . Let  $\mathbb{P}$  be a Suslin c.c.c. notion of forcing which adjoins reals and let  $\mathbb{Q}$  be the  $\aleph_2$  length finite support iteration of  $\mathbb{P}$ . Then  $M^\mathbb{Q} \models c(\text{Sym}(\mathbb{N})) = \aleph_1$ .*

On the other hand, we can prove in ZFC the following theorem (see, e.g. [BSZ]).

**Theorem 10**  $\text{Non}(\mathcal{M}) \leq \mathfrak{a}_p, \mathfrak{a}_g$ , where  $\text{Non}(\mathcal{M})$  is the size of the smallest non-meager set of reals.

As a corollary of Theorems 9 and 10, we know the following.

**Corollary 11** *It is consistent with ZFC that  $c(\text{Sym}(\mathbb{N})) = \aleph_1 < \mathfrak{a}_p = \mathfrak{a}_g = 2^\omega = \aleph_2$ .*

**PROOF.** Iteratively add  $\aleph_2$  random reals with finite support to a ground model  $M \models \text{ZFC} + \text{GCH}$ .

The obvious question left to answer is whether we can prove  $c(\text{Sym}(\mathbb{N})) \leq \mathfrak{a}_p, \mathfrak{a}_g$ . In the second section, we will give a negative answer to this question, namely we will show that it is consistent with ZFC that  $\mathfrak{a}_p = \mathfrak{a}_g < c(\text{Sym}(\mathbb{N}))$ .

In the third section, we will state several open problems in this area.

## 2 The Theorems

In [MHD], Justin Moore, Michael Hrušák and Mirna Džamonja introduced weakenings of the diamond principle related to cardinal characteristics. We'll first study the effect of one of these weakenings of the diamond principle on families related to the symmetry group of the natural numbers.

**Definition 12**  ${}^{\mathbb{N}}\mathbb{N}$  is the Baire space, the space of all functions from the natural numbers,  $\mathbb{N}$ , to the natural numbers.  $=$  is the relation on Baire space of infinite equality, i.e. for  $f, g \in {}^{\mathbb{N}}\mathbb{N}$  we have  $f = g$  iff  $\{n \in \mathbb{N} : f(n) = g(n)\}$  is infinite.

A function  $F : {}^{<\omega_1}2 \rightarrow {}^{\mathbb{N}}\mathbb{N}$  is a Borel function iff for all  $\delta < \omega_1$  the function  $F \upharpoonright \delta : \delta 2 \rightarrow {}^{\mathbb{N}}\mathbb{N}$  is Borel.

$\diamond({}^{\mathbb{N}}\mathbb{N}, =)$  is the following guessing principle:

For every Borel function  $F : {}^{<\omega_1}2 \rightarrow {}^{\mathbb{N}}\mathbb{N}$  there is a function  $G : \omega_1 \rightarrow {}^{\mathbb{N}}\mathbb{N}$  such that for every  $f : \omega_1 \rightarrow 2$  the set

$$\{\delta < \omega_1 : F(f \upharpoonright \delta) = G(\delta)\}$$

is stationary.

A  $G$  related to  $F$  in this way is called a  $\diamond({}^{\mathbb{N}}\mathbb{N}, =)$ -sequence for  $F$ .

We will study the effect of this  $\diamond$ -principle on the cardinal invariants  $\mathfrak{a}_p$  and  $\mathfrak{a}_g$ .

**Theorem 13**  $\diamond({}^{\mathbb{N}}\mathbb{N}, =)$  implies  $\mathfrak{a}_p = \aleph_1$ .

**PROOF.** We will define a map  $F$  such that the  $\diamond({}^{\mathbb{N}}\mathbb{N}, =)$ -sequence for it will help us build a sequence of permutations  $\langle p_\alpha : \alpha < \delta \rangle$  which will be a maximal almost disjoint family of permutations of  $\mathbb{N}$ .

To define  $F : {}^{<\omega_1}2 \rightarrow {}^{\mathbb{N}}\mathbb{N}$ , by coding we let its domain be the set of pairs  $(\langle p_\alpha : \alpha < \delta \rangle, p)$  with  $\{p_\alpha : \alpha < \delta\} \cup \{p\}$  a family of permutations. This coding works on a club  $C \subseteq \omega_1$ , which is enough. Outside this club we let  $F$  be any constant map. Also by coding we let its range be  ${}^{\mathbb{N}}(\mathbb{N} \cup {}^{<\omega}(\mathbb{N} \times \mathbb{N}))$ . We also fix for every  $\delta < \omega_1$  a bijection  $e_\delta : \mathbb{N} \rightarrow \delta$ .

If  $\{p_\alpha : \alpha < \delta\} \cup \{p\}$  is not almost disjoint, we define  $F(\langle p_\alpha : \alpha < \delta \rangle, p)(n) = n$ . Otherwise, we define  $F(\langle p_\alpha : \alpha < \delta \rangle, p)(n)$  to be  $((k_0, p(k_0)), (k_1, p(k_1)), \dots, (k_{6n}, p(k_{6n})))$  with

- $k_0$  the least number such that  $p(k_0) \notin \{p_{e_\delta(j)}(k_0) : j \leq n\}$ ,
- and  $k_{i+1}$  the least number strictly bigger than  $k_i$  such that  $p(k_{i+1}) \notin \{p_{e_\delta(j)}(k_{i+1}) : j \leq n\}$ .

Since the family is almost disjoint, these  $k_i$  exist.

For any  $\delta < \omega_1$  the function  $F$  restricted to those  $(\langle p_\alpha : \alpha < \delta \rangle, p)$  for which  $\{p_\alpha : \alpha < \delta\} \cup \{p\}$  is an almost disjoint family is continuous. Since for fixed  $\delta$  the set of  $(\langle p_\alpha : \alpha < \delta \rangle, p)$  for which  $\{p_\alpha : \alpha < \delta\} \cup \{p\}$  is an almost disjoint family is a Borel set, this shows that  $F$  is a Borel function.

Let  $G : \omega_1 \rightarrow {}^{\mathbb{N}}\mathbb{N}$  be a  $\diamond({}^{\mathbb{N}}\mathbb{N}, =)$ -sequence for this  $F$ . We define  $G(\delta)(n)$  to be a *valid guess* for  $\langle p_\alpha : \alpha < \delta \rangle$ , a family of almost disjoint permutations, iff

- $G(\delta)(n) = ((k_0, o_0), (k_1, o_1), \dots, (k_{6n}, o_{6n}))$  for some  $k_i, o_i \in \mathbb{N}$ ,
- all  $k_i$  are distinct, and
- all  $o_i$  are distinct and  $o_i \notin \{p_{e_\delta(j)}(k_i) : j \leq n\}$ .

Note that for any  $\delta < \omega_1$ ,  $n \in \mathbb{N}$ , and any permutation almost disjoint from all  $p_\alpha$ , if  $F(\langle p_\alpha : \alpha < \delta \rangle, p)(n) = G(\delta)(n)$  then  $G(\delta)(n)$  is a valid guess for  $\langle p_\alpha : \alpha < \delta \rangle$ .

Now we use  $G$  to construct  $\langle p_\alpha : \alpha < \omega_1 \rangle$  recursively. So suppose  $\langle p_\alpha : \alpha < \delta \rangle$  have been defined. Then define  $p_\delta$  recursively,  $p_\delta := \bigcup_s {}_{\mathbb{N}}p_{\delta,s}$  where

- (P1)  $p_{\delta,0} := \emptyset$ ,
- (P2)  $p_{\delta,s+1} := p_{\delta,s}$  if  $G(\delta)(s)$  is not a valid guess for  $\langle p_\alpha : \alpha < \delta \rangle$ ,
- (P3)  $p_{\delta,s+1} := p_{\delta,s} \cup \{(k_i, o_i)\}$  if  $G(\delta)(s) = ((k_0, o_0), (k_1, o_1), \dots, (k_{6s}, o_{6s}))$  is a valid guess for  $\langle p_\alpha : \alpha < \delta \rangle$  and  $i$  is least such that  $k_i \notin \text{dom}(p_{\delta,s})$  and  $o_i \notin \text{ran}(p_{\delta,s})$ ,
- (P4)  $p_{\delta,s+1} := p_{\delta,s+1} \cup \{(a, b)\}$  where  $a$  is the least number not in  $\text{dom}(p_{\delta,s+1})$  and  $b$  is the least number not in  $\text{ran}(p_{\delta,s+1})$  and not in  $\{p_{e_\delta(j)}(a) : j \leq s\}$ , and
- (P5)  $p_{\delta,s+1} := p_{\delta,s+1} \cup \{(c, d)\}$  where  $d$  is the least number not in  $\text{ran}(p_{\delta,s+1})$  and  $c$  is the least number not in  $\text{dom}(p_{\delta,s+1})$  and not in  $\{p_{e_\delta(j)}^{-1}(d) : j \leq s\}$ .

Note that  $|p_{\delta,s}|$  is at most  $3s$ . This means we can do step P3, as the requirement  $k_i \notin \text{dom}(p_{\delta,s})$  excludes at most  $3s$  pairs in  $G(\delta)(s)$ ,  $o_i \notin \text{ran}(p_{\delta,s})$  excludes at most another  $3s$  pairs in  $G(\delta)(s)$ , and  $G(\delta)(s)$  has  $6s + 1$  pairs, always leaving at least one pair.

Now  $p_\delta$  is a permutation almost disjoint from all  $p_\alpha$ ,  $\alpha < \delta$ . This completes the construction of  $\langle p_\alpha : \alpha < \omega_1 \rangle$ .

It remains to see that this almost disjoint family of permutations is maximal. We do this by contradiction; suppose, therefore, that there is a permutation  $p$  almost disjoint from all  $p_\alpha$ ,  $\alpha < \omega_1$ . Then the set

$$\{\delta < \omega_1 : F(\langle p_\alpha : \alpha < \delta \rangle, p) = G(\delta)\}$$

is stationary. Remember that we use a coding for the inputs of the function  $F$ , and note that, if this coding is reasonable, the sequence  $\delta \mapsto (\langle p_\alpha : \alpha < \delta \rangle, p)$  determines a path  $f : \omega_1 \rightarrow 2$  in the tree  ${}^{<\omega_1}2$ .

Now let  $\delta$  be a member of this set (and the club  $C$ , the club where our coding for inputs works). Then  $F(\langle p_\alpha : \alpha < \delta \rangle, p) = G(\delta)$ , which means there are infinitely many  $n$  such that  $G(\delta)(n)$  is a valid guess for  $\langle p_\alpha : \alpha < \delta \rangle$ , and all the pairs in  $G(\delta)(n)$  belong to  $p$ . So we hit  $p$  infinitely often with  $p_\delta$ , which is a contradiction.

For our next result we will use some results from [GZ] by Su Gao and Yi Zhang (the definitions of  $W_G$  and good extensions and Lemmas 17 and 18 are theirs).

We start by noting that  $H \leq \text{Sym}(\mathbb{N})$  is a cofinitary group if it is a group and all nonidentity members are almost disjoint from the identity. This is equivalent to  $H$  being a group and an almost disjoint family  $(g, h \in \text{Sym}(\mathbb{N}))$  are almost disjoint iff  $gh^{-1}$  is almost disjoint from the identity).

**Definition 14** For  $H \subseteq \text{Sym}(\mathbb{N})$  and  $x$  a variable, let  $W_H$  be the set of words of the form

$$w = w(x) = g_0 x^{k_0} g_1 \cdots x^{k_l} g_{l+1},$$

where  $g_i \in H$ ,  $g_i \neq \text{Id}$  for  $0 < i \leq l$ , and  $k_i \in \mathbb{Z} \setminus \{0\}$ .

For  $w \in W_H$ , we define  $\#_x(w) = \sum_{i=0}^l |k_i|$ , the number of occurrences of  $x$  in  $w$ , and  $\text{lh}(w) = \sum_{i=0}^l |k_i| + l + 2$ , the length of the word. We also define  $w_i$  to be the  $i^{\text{th}}$  letter in  $w$  counted from the right (if  $w = g_0 x^2 g_1$ , then  $w_0 = g_1$ ,  $w_1 = x$ ,  $w_2 = x$ , and  $w_4 = w_{\text{lh}(w)} = g_0$ ).

For  $p : \mathbb{N} \rightarrow \mathbb{N}$  a partial function,  $w(x) \in W_H$  and  $n \in \mathbb{N}$ , we define the evaluation path for  $n$  in  $w(p)$  to be the sequence  $\langle l_i \in \mathbb{N} : i \leq j \rangle$ , with  $l_0 := n$ ,  $l_{i+1} := w_i(p)(l_i)$  and  $w_j(p)(l_j)$  not defined or  $j = \text{lh}(w)$  (if  $w(p)(l)$  is defined).

The pairs  $(l_i, l_{i+1})$  of  $p$  are the pairs of  $p$  used in this evaluation. For a general function  $f$  (possibly partial) we call  $(n, f(n))$  a pair from  $f$ .

For  $w \in W_H$  and finite one-to-one functions  $p, q$  such that  $p \subseteq q$  we say that  $q$  is a good extension of  $p$  with respect to  $w$  if the following condition is satisfied:

if for some  $l \in \mathbb{N}$

$$w(p)(l) \text{ is undefined and } w(q)(l) = l,$$

then there are subwords  $u$  and  $z$  of  $w$  and  $n \in \mathbb{N}$  such that

$$\begin{aligned} w &= uzu^{-1} \text{ without cancelation,} \\ u^{-1}(q)(l) &= n, \text{ and } z(p)(n) = n. \end{aligned}$$

In the same context we call  $q$  a very good extension of  $p$  with respect to  $w$  if  $w(q)$  has no more fixed points than  $w(p)$ .

Note that a very good extension is a good extension.

The usefulness of good extensions comes from the following: Let  $H$  be a countable cofinitary group and  $\langle w_n : n \in \mathbb{N} \rangle$  an enumeration of  $W_H$ . Then if  $g = \bigcup_s \mathbb{N} g_s$  with all  $g_s$  finite injective functions such that  $g$  is a bijection and  $g_{s+1}$  is a good extension of  $g_s$  with respect to the words  $w_0, \dots, w_s$ , then the group  $\langle H, g \rangle$ , the group generated by  $H$  and  $g$ , is also cofinitary.

We see this from the following facts:

- For every  $h \in \langle H, g \rangle$  there is a  $w \in W_H$  such that  $h = w(g)$ .
- For every  $w \in W_H$  the bijection  $w(g)$  is cofinitary.

The first fact is immediate, and the second follows from the fact that  $w = w_s$  for some  $s \in \mathbb{N}$ . Then from  $g_s$  on we only take good extensions with respect to  $w$ . This means that  $w(g)$  ends up with only the fixed points that it is forced to have by what  $g_s$  is, and of those there are only finitely many.

The following two lemmas show that we can construct a function  $F$  similar to the  $F$  in the proof of Theorem 13 but for maximal cofinitary groups.

**Lemma 15** *Let  $H$  be a cofinitary group,  $f \in \text{Sym}(\mathbb{N}) \setminus H$  such that  $\langle H, f \rangle$  is a cofinitary group and  $w \in W_H$ . Then for every  $k \in \mathbb{N}$  there exists a finite set  $S$  of pairs from  $f$  such that for every finite injective map  $p$  with  $|p|$  less than  $k$  there exists a pair  $(a, b)$  in  $S$  such that  $p \cup \{(a, b)\}$  is a very good extension of  $p$  with respect to  $w$ .*

**PROOF.** First we will find an infinite subset  $f'$  of  $f$  such that  $w(f')$  has no fixed points, then we'll show that a big enough finite subset of  $f'$  exists. The first step ensures that we don't have to worry about fixed points caused by pairs from  $f'$  alone. The second part is done by counting how many pairs from  $f'$  could combine with pairs from  $p$  to cause a fixed point.

Obtaining  $f'$  from  $f$  is done differently depending on whether  $w(f)$  is the identity or not.

If  $w(f)$  is not the identity, then it has only finitely many fixed points. Let  $f'$  be equal to  $f$  with for each of those finitely many fixed points one pair from  $f$  used in the evaluation path of that fixed point removed. We have ensured that  $w(f')$  has no fixed points.

If  $w(f)$  is the identity, then we know there is more than one occurrence of  $x$  in  $w(x)$  (since  $f \notin H$ ). So either there is an occurrence of  $x^2$  or  $x^{-2}$ , or there is a subword of the form  $x^{\epsilon_0} g x^{\epsilon_1}$ , with  $\epsilon_i \in \{-1, +1\}$  and  $g \in H$ . In either case there are only finitely many evaluation paths of  $w(f)$  that use the same pair from  $f$  in both these selected occurrences of  $x$  (use that  $f$  has only finitely many fixed points for the first case, and that  $f \notin H$  for the second case). Remove these finitely many pairs from  $f$  to obtain  $f'$ .

Now we have to find an infinite subset  $f''$  of  $f'$  such that  $w(f'')$  is nowhere defined (which in this case is equivalent to not having fixed points).

We do this by wellordering  $\mathbb{N} \times \mathbb{N}$  and recursively doing the following: Take the least pair  $(a, b)$  of  $f'$  and add it to  $f''$ . Then remove from  $f'$  this pair  $(a, b)$  and all finitely many pairs (actually at most 2) which are used in an evaluation path in one of the selected occurrences of  $x$  where  $(a, b)$  is used in the other selected occurrence of  $x$ .

We end up with an infinite  $f''$  such that  $w(f'')$  is indeed nowhere defined.

Now we examine for a given  $p$ , an injective map with  $|p| = l \leq k$ , how many pairs  $(a, b)$  of  $f$  can have that  $p \cup \{(a, b)\}$  is not a very good extension of  $p$  for  $w$ .

First there are at most  $2l$  pairs  $(a, b)$  from  $f$  that have  $a \in \text{dom}(p)$  or  $b \in \text{ran}(p)$ . Remove these from  $f$  to obtain  $\tilde{f}$ . Now we look at  $w(p \cup \tilde{f})$ ; any fixed point of  $w(p \cup \tilde{f})$  that was not a fixed point of  $w(p)$  has an evaluation path where both pairs from  $p$  and from  $\tilde{f}$  are used. If we remove one pair from  $\tilde{f}$  for each of those evaluation paths to obtain  $\hat{f}$  the partial permutation  $w(p \cup \hat{f})$  will only have fixed points that  $w(p)$  already had.

So we only have to find an upper bound for the number of evaluation paths using both pairs from  $p$  and  $\tilde{f}$ . This upper bound is attained if for each occurrence of  $x$  in  $w$  and any pair of  $p$ , it gets to be completed to an evaluation path with all pairs from  $\tilde{f}$ . This gives us  $|p| \cdot \#_x(w)$  as an upper bound.

So in total at most  $2l + l \cdot \#_x(w)$  pairs  $(a, b)$  of  $f$  are such that  $p \cup \{(a, b)\}$  is not a very good extension of  $p$  with respect to  $w$ .

This means that if we take  $S$  to consist of  $2k + k \cdot \#_x(w) + 1$  pairs of  $f$  we have a set as desired.

We need and easily get the following stronger lemma.

**Lemma 16** *Let  $H$  be a cofinitary group,  $f \in \text{Sym}(\mathbb{N}) \setminus H$  such that  $\langle H, f \rangle$  is a cofinitary group and  $w_0, \dots, w_n \in W_H$ . Then for every  $k \in \mathbb{N}$  there exists a finite set  $S$  of pairs from  $f$  such that for every injective map  $p$  with  $|p|$  less than  $k$  there exists a pair  $(a, b) \in S$  such that  $p \cup \{(a, b)\}$  is a very good extension of  $p$  for all the words  $w_0, \dots, w_n$ .*

**PROOF.** By applying the method used in the first half of the proof of the last lemma  $n + 1$  times we can find an infinite  $f' \subseteq f$  such that none of  $w_0(f'), \dots, w_n(f')$  have fixed points. Then using the method in the second half of the proof of the last lemma also  $n + 1$  times we can find how big a subset  $S$  of  $f'$  we have to choose.

We use the following two lemmas from [GZ] to make sure the permutation we construct later will be a bijection (these lemmas give us a method of getting a full domain and full range). The first lemma allows us to extend the domain of a finite partial injective function by any number.

**Lemma 17 (Domain Extension)** *Let  $H$  be a cofinitary group,  $w_0, \dots, w_n \in W_H$ ,  $p$  a finite injective function and  $i \notin \text{dom}(p)$ . Then for all but finitely many  $m \in \mathbb{N}$  the function  $p \cup \{(i, m)\}$  is a good extension of  $p$  with respect to all words  $w_0, \dots, w_n$ .*

And the second lemma allows us to extend the range of a finite partial injective function by any number.



**Lemma 18 (Range Extension)** *Let  $H$  be a cofinitary group,  $w_0, \dots, w_n \in W_H$ ,  $p$  a finite injective function and  $i \notin \text{ran}(p)$ . Then for all but finitely many  $k \in \mathbb{N}$  the function  $p \cup \{(k, i)\}$  is a good extension of  $p$  with respect to all words  $w_0, \dots, w_n$ .*

Now we are ready to state and prove the second theorem.

**Theorem 19**  $\diamond(\mathbb{N}\mathbb{N}, =)$  implies  $\mathfrak{a}_g = \aleph_1$ .

**PROOF.** We use the same strategy as in the proof of the previous theorem: we define a function  $F$  whose  $\diamond(\mathbb{N}\mathbb{N}, =)$ -sequence helps us build a maximal cofinitary group  $\langle \{g_\alpha : \alpha < \omega_1\} \rangle$ .

By coding we let its domain be the set of pairs  $(\langle g_\alpha : \alpha < \delta \rangle, g)$  with  $\delta < \omega_1$  and  $\{g_\alpha : \alpha < \delta\} \cup \{g\}$  a family of permutations. This coding works on a club  $C \subseteq \omega_1$ , which is enough. Also by coding we let its range be  ${}^{\mathbb{N}}(\mathbb{N} \cup {}^{<\omega}(\mathbb{N} \times \mathbb{N}))$ . We also fix for every  $\delta < \omega_1$  a bijection  $e_\delta : \mathbb{N} \rightarrow \delta$ .

For  $\langle g_\alpha : \alpha < \delta \rangle$  a sequence of permutations we let  $n \mapsto \tilde{w}_n$  be an enumeration of  $W_{\{g_\alpha : \alpha < \delta\}}$ .

Now we can define  $F$ . On the levels  $\delta < \omega_1$  where the chosen coding for the input does not work, define  $F$  to be any constant map. On the levels where the coding does work, define  $F(\langle g_\alpha : \alpha < \delta \rangle, g)(n)$  to be either  $m$ , the least code for  $((k_0, g(k_0)), (k_1, g(k_1)), \dots, (k_N, g(k_N)))$  such that for every injective partial map  $p : \mathbb{N} \rightarrow \mathbb{N}$  with  $|p| \leq 3n$  there is a pair  $(k_i, g(k_i))$  coded in  $m$  such that  $p \cup \{(k_i, g(k_i))\}$  is a very good extension of  $p$  with respect to all words  $\tilde{w}_0, \dots, \tilde{w}_n$ , or 0 if such a code does not exist.

Note that by Lemma 16 if  $\{g_\alpha : \alpha < \delta\} \cup \{g\}$  generates a cofinitary group and  $g \notin \langle \{g_\alpha : \alpha < \delta\} \rangle$  then there is such a code  $m$ . Also note that the function  $F$  is Borel.

Let  $G : \omega_1 \rightarrow {}^{\mathbb{N}}\mathbb{N}$  be a  $\diamond(\mathbb{N}\mathbb{N}, =)$ -sequence for this  $F$ . We define  $G(\delta)(n)$  to be a *valid guess* for  $\langle g_\alpha : \alpha < \delta \rangle$ , a family of permutations that generates a cofinitary group, iff

- $G(\delta)(n) = ((k_0, o_0), (k_1, o_1), \dots, (k_N, o_N))$  for some  $k_i, o_i \in \mathbb{N}$  and  $N \in \mathbb{N}$ ,
- all  $k_i$  are distinct,
- all  $o_i$  are distinct, and
- for every partial injective map  $p : \mathbb{N} \rightarrow \mathbb{N}$  with  $|p| \leq 3n$  there is a pair  $(k_i, o_i)$  such that  $p \cup \{(k_i, o_i)\}$  is a very good extension of  $p$  with respect to all words  $\tilde{w}_0, \dots, \tilde{w}_n$ .

Note that for any  $\delta < \omega_1$ ,  $n \in \mathbb{N}$ , and any permutation such that  $g \notin \langle \{g_\alpha : \alpha < \delta\} \rangle$  and  $\langle \{g_\alpha : \alpha < \delta\} \cup \{g\} \rangle$  is cofinitary, if  $F(\langle g_\alpha : \alpha < \delta \rangle, g)(n) = G(\delta)(n)$  then  $G(\delta)(n)$  is a valid guess for  $\langle g_\alpha : \alpha < \delta \rangle$ .

Now we use  $G$  to recursively construct  $\langle g_\alpha : \alpha < \omega_1 \rangle$ , a sequence of permutations such that  $\langle \{g_\alpha : \alpha < \delta\} \rangle$  is a maximal cofinitary group. So suppose  $\langle g_\alpha : \alpha < \delta \rangle$  have been constructed. Then construct  $g_\delta := \bigcup_{s \in \mathbb{N}} g_{\delta, s}$  recursively by:

- (P1)  $g_{\delta,0} := \emptyset$ ,
- (P2)  $g_{\delta,s+1} := g_{\delta,s}$  if  $G(\delta)(s)$  is not a valid guess for  $\langle g_\alpha : \alpha < \delta \rangle$ ,
- (P3)  $g_{\delta,s+1} := g_{\delta,s} \cup \{(k_i, o_i)\}$  if  $G(\delta)(s) = ((k_0, o_0), \dots, (k_N, o_N))$  is a valid guess for  $\langle g_\alpha : \alpha < \delta \rangle$  and  $i$  is least such that  $p \cup \{(k_i, o_i)\}$  is a very good extension of  $p$  for all words  $\tilde{w}_0, \dots, \tilde{w}_n$ ,
- (P4)  $g_{\delta,s+1} := g_{\delta,s+1} \cup \{(a, b)\}$  where  $a$  is the least number not in  $\text{dom}(g_{\delta,s+1})$  and  $b$  is the least number such that  $g_{\delta,s+1} \cup \{(a, b)\}$  is a good extension of  $g_{\delta,s+1}$  for all words  $\tilde{w}_0, \dots, \tilde{w}_n$  (this  $b$  exists by Lemma 17 (The Domain Extension Lemma)), and
- (P5)  $g_{\delta,s+1} := g_{\delta,s+1} \cup \{(c, d)\}$  where  $d$  is the least number not in  $\text{ran}(g_{\delta,s+1})$  and  $c$  is the least number such that  $g_{\delta,s+1} \cup \{(c, d)\}$  is a good extension of  $g_{\delta,s+1}$  with respect to all words  $\tilde{w}_0, \dots, \tilde{w}_n$  (this  $c$  exists by Lemma 18 (The Range Extension Lemma)).

Note that  $|g_{\delta,s}|$  is at most  $3s$  which means we can always perform step P3 when applicable.

Now  $g_\delta$  is a permutation such that  $\{g_\alpha : \alpha < \delta\} \cup \{g_\delta\}$  generates a cofinitary group; completing the construction of  $\langle g_\alpha : \alpha < \delta \rangle$ .

It remains to see that this group is *maximal* cofinitary. We do this by contradiction; suppose, therefore, that there is a  $g \in \text{Sym}(\mathbb{N})$  such that  $g \notin \langle \{g_\alpha : \alpha < \omega_1\} \rangle$  and that  $\langle \{g_\alpha : \alpha < \omega_1\}, g \rangle$  is a cofinitary group. Then the set

$$\{\delta < \omega_1 : F(\langle g_\alpha : \alpha < \delta \rangle, g) = G(\delta)\}$$

is stationary. Remember that we use a coding for the inputs of the function  $F$ , and note that, if this coding is reasonable, the sequence  $\delta \mapsto (\langle g_\alpha : \alpha < \delta \rangle, g)$  determines a path  $f : \omega_1 \rightarrow 2$  in the tree  ${}^{<\omega_1}2$ . Now let  $\delta$  be a member of this set (and the club  $C$ , the club where our coding for inputs works). Then  $F(\langle g_\alpha : \alpha < \delta \rangle, g) = G(\delta)$ , which means that for infinitely many  $n$  the value  $G(\delta)(n)$  is a valid guess for  $\langle g_\alpha : \alpha < \delta \rangle$  and all pairs in  $G(\delta)(n)$  belong to  $g$ . This means we hit  $g$  infinitely often with  $g_\delta$ , which is a contradiction.

Combining Theorem 13 and Theorem 19 with

**Theorem 20**  $\diamond({}^{\mathbb{N}}\mathbb{N}, =)$  is true in the Miller model.

which is from [MHD], we see that  $\mathfrak{a}_p = \mathfrak{a}_g = \aleph_1$  in the Miller model.

Then with  $\mathfrak{g} \leq \text{cof}(\text{sym}(N))$ . from [BL], and the fact that the cardinal  $\mathfrak{g}$  is  $\aleph_2$  in the Miller model, from [B] we see, as announced in the introduction, that

**Theorem 21** In the Miller model  $\mathfrak{a}_p = \mathfrak{a}_g = \aleph_1 < \aleph_2 = c(\text{Sym}(\mathbb{N}))$ .

### 3 Questions

We will finish this article with some questions related to the cardinal invariants  $\mathfrak{a}_p$  and  $\mathfrak{a}_g$ . For the first question, other than its intrinsic interest, a positive answer would have as likely consequence many more theorems as proved in this article (consistency of  $\mathfrak{a}_p, \mathfrak{a}_g$  less than other invariants).

**Question 22 (Veličković)** *Is there a natural cardinal invariant (other than  $\mathfrak{c}$ ) that is an upper bound for  $\mathfrak{a}_p$  and  $\mathfrak{a}_g$ ?*

For the second question we know that it is consistent that there exists a maximal cofinitary group  $G$  and an almost disjoint family  $A$  such that  $G \subseteq A$  and  $|G| < |A|$ . For this see [Z3]. However the following question is still open.

**Question 23** *Is it consistent with ZFC that  $\mathfrak{a}_p$  and  $\mathfrak{a}_g$  are different?*

Our third question is about relating cardinal invariant in Baire space to those in Cantor space. We are especially interested in the relation to

$$\mathfrak{a} := \min\{|A| : A \subseteq \mathcal{P}(\mathbb{N}) \text{ is an infinite maximal almost disjoint family}\}.$$

**Question 24** *Is  $\mathfrak{a} \leq \mathfrak{a}_p, \mathfrak{a}_g$ ?*

Jörg Brendle has conjectured a positive answer to this question.

We have noticed that, in all constructions and forcing results so far, both  $\mathfrak{a}_p$  and  $\mathfrak{a}_g$  are regular. We are not aware of anything indicating that this should be so. This leads to the following question.

**Question 25** *Is it consistent that  $\mathfrak{a}_p$  or  $\mathfrak{a}_g$  is singular?*

### 4 Acknowledgements

We thank Andreas Blass for comments on an earlier version of this paper.

### References

- [A] S. A. Adeleke, *Embeddings of Infinite Permutation Groups in Sharp, Highly Transitive, and Homogeneous Groups*, Proc. Edinburgh Math. Soc. ,**31** (1981), pp. 169–178.
- [B] A. Blass, *Applications of Superperfect Forcing and its Relatives*, appears in *Set Theory and its Applications*, Lecture Notes in Mathematics, **1401** (1989), pp. 18–40, edited by J. Steprāns and S. Watson.

- [BL] J. Brendle, M. Losada, *The Cofinality of the infinite Symmetric Group and Groupwise Density*, Journal of Symbolic Logic, **68** (2003), pp. 1354–1361.
- [BSZ] J. Brendle, O. Spinas and Y. Zhang, *Uniformity of the Meager Ideal and Maximal Cofinitary Groups*, J. of Algebra, **232** (2000), pp. 209–225.
- [C] P. J. Cameron, *Cofinitary Permutation Groups*, Bull. London Math. Soc., **28** (1996), pp. 113–140.
- [MN] H. D. Macpherson and P. M. Neumann, *Subgroups of Infinite Symmetric Groups*, J. of London Math. Soc (2), **42** (1990), pp. 64–84.
- [MHD] J. Moore, M. Hrušák, M. Džamonja, *Parameterized  $\diamond$  Principles*, Transactions of the American Mathematical Society, **356** (2004), pp. 2281–2306.
- [GZ] S. Gao, Y. Zhang, *Definable Sets of Generators in Maximal Cofinitary Groups*, preprint, 2003.
- [ST] J. D. Sharp and S. Thomas, *Uniformization Problems and the Cofinality of the Infinite Symmetric Groups*, Notre Dame J. Formal Logic, **35** (1994), pp. 328–345.
- [T] J. K. Truss, *Embeddings of Infinite Permutation Groups*, Proceedings of Groups, St. Andrews, 1985, London Math. Soc. Lecture Note Series **121** (ed. E.F. Robertson and Breach, 1997), pp. 101–120.
- [Z] Y. Zhang, *Maximal Cofinitary Groups*, Arch. Math. Logic, **39** (2000), pp. 41–52.
- [Z1] Y. Zhang, *A Class of MAD Families*, J. of Symbolic Logic, **64** (1999) pp. 737–746.
- [Z2] Y. Zhang, *Permutation Groups and Covering Properties*, J. of London Math. Soc. (2), **63** (2001), pp. 1–15.
- [Z3] Y. Zhang, *Adjoining Cofinitary Permutations*, The Journal of Symbolic Logic, **64** (1999), pp. 1803–1810.