COFINITARY GROUPS,
ALMOST DISJOINT AND DOMINATING FAMILIES

MICHAEL HRUŠÁK, JURIS STEPRANS, AND YI ZHANG

Abstract. In this paper we show that it is consistent with ZFC that the cardinality of every maximal cofinitary group of $Sym(\omega)$ is strictly greater than the cardinal numbers $\mathfrak{d}$ and $\mathfrak{a}$.

§1. Introduction. We say that two permutations $f, g \in Sym(\omega)$ are almost disjoint (a.d.) if $|f \cap g| < \omega$, that is, that $\{n \in \omega | f(n) = g(n)\}$ is finite. An a.d. permutation family $A \subseteq Sym(\omega)$ is a subset of $Sym(\omega)$ such that $|f \cap g| < \omega$, for any $f, g \in A$. A permutation $g \in Sym(\omega)$ is cofinitary if g has only finitely many fixed points. A group $G \leq Sym(\omega)$ is cofinitary if every non-identity element is cofinitary. It is easily seen that $G \leq Sym(\omega)$ is cofinitary if and only if G is both an almost disjoint family of permutations and a group. For a discussion of different aspects of cofinitary groups, the reader can consult the well-written survey paper by P. Cameron (see [3]). Since the union of a chain of cofinitary permutation groups is cofinitary, Zorn's Lemma implies that maximal cofinitary groups exist, and indeed any cofinitary group is contained in a maximal one. The following theorem was proved by Truss [9] and Adeleke [1].

THEOREM 1.1. *If $G \leq Sym(\omega)$ is a maximal cofinitary group, then G is not countable.*

Also, P. Neumann proved the following result.

THEOREM 1.2. *There exists a maximal cofinitary group of cardinality 2^{ω}.*

PROOF. See Proposition 10.4 and its proof in [3] for a detailed discussion.   ⊣

Thus P. Cameron (in [3]) asked the following question.

QUESTION 1.3. *If the Continuum Hypothesis (CH) fails, is it possible that there exists a maximal cofinitary group G such that $|G| < 2^{\omega}$?*

In [11] (or [13]), this question was answered by proving the following results.

THEOREM 1.4. *(MA) If $G \leq Sym(\omega)$ is a maximal cofinitary group, then G has cardinality 2^{ω}.*

THEOREM 1.5. *Let* $M \models (ZFC + \neg CH)$. *Let* $\kappa \in M$ *be a cardinal such that* $\omega_1 \leq \kappa < 2^\omega = \lambda$. *Then there exists a c.c.c. notion of forcing* $\mathbb{G}$ *such that the following statements holds in* $M^{\mathbb{G}}$.

(1) $2^\omega = \lambda$.
(2) *There exists a maximal cofinitary group* $G \leq Sym(\omega)$ *of cardinality* κ.

Hence we can consider the following cardinal number.

DEFINITION 1.6. *Let* $\mathfrak{a}_\mathfrak{g}$ *be the least* λ *such that there exists a maximal cofinitary group of cardinality* λ.

It would be interesting to compare $\mathfrak{a}_\mathfrak{g}$ with some other well-known cardinal invariants of the continuum (see [10]). For example, we consider the following cardinals,

(1) $\mathfrak{a}$ is the least λ such that there exists an infinite maximal almost disjoint family of $\wp(\omega)$ with the size λ; and
(2) $\mathfrak{d}$ is the least λ of a dominating family in $\langle {}^\omega\omega, \leq^* \rangle$ with size λ.

In [14], we proved the following result.

THEOREM 1.7. *Let* $M \models (ZFC + CH)$. *There is a maximal cofinitary group* $G \leq Sym(\omega)$ *of size* ω_1 *in* M *such that for any Cohen generic* H *over* M, G *remains a maximal cofinitary group in* $M[H]$.

It is an easy corollary of Theorem 1.7 that it is consistent with ZFC that $\mathfrak{a} = \mathfrak{a}_\mathfrak{g} = \omega_1 < \mathfrak{d} = 2^\omega$.

Notice that $\mathfrak{a}_\mathfrak{g}$ looks similar to $\mathfrak{a}$ and lots of well-known results about $\mathfrak{a}$ can also be proved for $\mathfrak{a}_\mathfrak{g}$ (see [11] and [13]). In this paper, we are interested in finding the difference between $\mathfrak{a}$ and $\mathfrak{a}_\mathfrak{g}$. We want to consider the following questions.

QUESTION 1.8. *Can we separate* $\mathfrak{a}$ *from* $\mathfrak{a}_\mathfrak{g}$?

QUESTION 1.9. *Is it consistent that* $\mathfrak{d} < \mathfrak{a}_\mathfrak{g}$?

Note. The consistency of $\mathfrak{d} < \mathfrak{a}$ is one of the main unsolved problems in the area of cardinal invariants of the continuum.

To answer these questions 1.8 and 1.9, we shall construct two different forcing models. In section 2, we sketch a proof of the consistency of $\mathfrak{a} = \omega_1 < \mathfrak{a}_\mathfrak{g} = \mathfrak{d} = \kappa = 2^\omega$, where κ can be any regular cardinal. In section 3, we give a detailed proof of the consistency of $\mathfrak{a} = \mathfrak{d} = \omega_1 < \mathfrak{a}_\mathfrak{g} = \omega_2 = 2^\omega$.

The set-theoretic notation used is standard (see either [5] or [4]). If $\mathbb{P}$ is a notion of forcing and $p, q \in \mathbb{P}$, then $q \leq p$ means that q is stronger than p. M (or, V) always denotes a countable transitive model of large enough fragment of ZFC.

§2. The consistency of $\mathfrak{a} < \mathfrak{a}_\mathfrak{g} = \mathfrak{d}$. In this section, we shall force with a c.c.c. partially ordered set $\mathbb{G}$, which is defined in Definition 2.1, over a ground model M such that $M \models (ZFC + GCH)$. We shall prove that it is consistent with ZFC that $\mathfrak{a} = \omega_1 < \mathfrak{a}_\mathfrak{g} = \mathfrak{d} = 2^\omega = \kappa$, where κ can be any regular cardinal such that $\kappa \geq \omega_2$.

We first define several concepts as follows:

Let $Fpf(\omega) = \{f \in Sym(\omega) \mid f \text{ is fixed point free}\}$.

We define that $f \sim g$ iff $|f \cap g| = \omega$.

Note. The relation $\sim$ is not an equivalence relation.

Let W consist of words $g_1 x^{n_1} g_2 ... g_t x^{n_t} g_{t+1}$ which actually involve x such that $g_l \in Fpf(\omega)$ except possibly $g_1 = id$ or $g_{t+1} = id$, here $id = \{\langle n, n \rangle \mid n \in \omega\}$. If $w(x) \in W$ and s is a 1–1 finite partial function from ω to ω, then $w(s)$ denotes the partial function obtained by substituting s for x in $w(x)$.

We say w_0 is an almost conjugate (a. c.) subword of w if $w = u_1 w_0 u_2$ with $u_1 \sim u_2^{-1}$, i.e., if

$$u_1 = f_1 x^{m_1} ... f_k x^{m_k} f_{k+1},$$

then

$$u_2 = (f'_{k+1})^{-1} x^{-m_k} (f'_k)^{-1} ... x^{-m_1} (f'_1)^{-1}.$$

Here $f_i \sim f'_i$ and $f_i \in Fpf(\omega)$ for each $i \in \{1, ..., k+1\}$ except possibly $f_1 = id$ or $f_{k+1} = id$.

We define a $c.c.c.$ partially ordered set:

DEFINITION 2.1. Define a partial order $\mathbb{G}$ which consists of all conditions of the form $\langle s, F \rangle$ such that

(1) s is a 1–1 finite partial function from ω to ω;
(2) F is a finite set of words from W.

We define $\langle s_2, F_2 \rangle \leq \langle s_1, F_1 \rangle$ iff

(a) $s_1 \subseteq s_2$ and $F_1 \subseteq F_2$;
(b) for every a. c.(reduced) subword w_0 of $w \in F_1$, the following holds: suppose that for any $\ell \in \omega$, if $w_0(s_1)(\ell) \uparrow$ and $w_0(s_2)(\ell) = \ell$, then there exists some $z \in W$ such that z is an a. c. subword of $w_0 = u_1 z u_2$ and the computation for $w_0(s_2)(\ell)$ has the following form,

$$\langle n_{11}, n_{12} \rangle \langle n_{21}, n_{11} \rangle ... \langle n_{k1}, n_{k-1,1} \rangle z(s_1) \langle n_{k-1,1}, n_{k1} \rangle ... \langle n_{11}, n_{21} \rangle \langle n_{12}, n_{11} \rangle (\ell) = \ell,$$

where $z(s_1)(n_{k1}) = n_{k1}$, $n_{12} = \ell$, and each $\langle n_j, n_{j'} \rangle$ is either in s_2 or g_i, $i = 1, ..., t+1$, and we use $\uparrow$ to denote the computation is undefined.

In $\mathbb{G}$, define

$$D_n = \{\langle s, F \rangle \in \mathbb{G} \mid n \in \text{dom}(s)\};$$

$$E_n = \{\langle s, F \rangle \in \mathbb{G} \mid n \in \text{rang}(s)\}.$$

By a very complicated argument, we can prove that D_n and E_n are dense in $\mathbb{G}$ for any $n \in \omega$ (for details see [14]). Thus by a standard density argument, we know that the following lemma holds.

LEMMA 2.2. *Assume $M \models ZFC$. Let G be any cofinitary group in M, and let H be $\mathbb{G}$–generic over M. Then $M[H]$ contains a permutation $g^\star \in Sym(\omega)$ such that $g^\star \notin G$ and $G * \langle g^\star \rangle$ is a cofinitary group.*

Let $M \models (ZFC + GCH)$. We proceed with a system of iterated forcing of length κ with finite support as follows:

Define $\mathbb{G}_\alpha$ for $\alpha < \kappa$ as follows:

(1) $\mathbb{G}_0 = \mathbb{G}^M$;
(2) $\mathbb{G}_{\alpha+1} = \mathbb{G}_\alpha * (\dot{\mathbb{G}})^{M^{\mathbb{G}_\alpha}}$, where $(\dot{\mathbb{G}})^{M^{\mathbb{G}_\alpha}}$ is a $\mathbb{G}_\alpha$ name such that

$$\Vdash_{\mathbb{G}_\alpha} (\dot{\mathbb{G}}^{M^{\mathbb{G}_\alpha}} = \mathbb{G}).$$

It is easy to see that $M[H_\kappa] \models \mathfrak{d} = \mathfrak{a}_\mathfrak{g} = 2^\omega = \kappa$.

The following lemma is crucial for proving that $\mathfrak{a} < \mathfrak{a}_\mathfrak{g}$. Define $w(x, \bar{y})$ to be a form of words, where $\bar{y} = \langle y_1, ..., y_n \rangle$ stands as variables which can be substituted for any n–tuple $\bar{g} = \langle g_1, ..., g_n \rangle$ of fixed point free permutations in $(Fpf(\omega))^n$.

LEMMA 2.3. *Suppose* $\Vdash_\mathbb{G} \tau \in \omega$, $s \in \omega^{<\omega}$ *is injective and* $\{w_1(x, \bar{y}), ..., w_t(x, \bar{y})\}$ *is a form of words. Then there exists an* $H \in [\omega]^{<\omega}$ *such that for any* $F \in [W]^{<\omega}$, *if* F *has the form*

$$\{w_1(x, \bar{y}), ..., w_t(x, \bar{y})\}$$

then

$$\exists p \leq \langle s, F \rangle (p \Vdash_\mathbb{G} \tau \in H).$$

PROOF. We prove the lemma by proving the following equivalent proposition.

Let $A = \{\langle t_n, F_n \rangle \in \mathbb{G} \mid n < \omega\}$ be an antichain which is maximal subject to the condition that $s \subseteq t_n$. Then there exists a $k < \omega$ such that for any $F = \{w_1(x, \bar{g}), ..., w_t(x, \bar{g})\} \in [W]^t$, there exists a $l < k$ such that $\langle s, F \rangle \parallel \langle t_l, F_l \rangle$; i.e., for each $F = \{w_1(x, \bar{g}), ..., w_t(x, \bar{g})\}$, there exists a $l < k$, such that for any a. c. subword $w_{i,0}$ in $w_i(x, \bar{g}) \in F$, for any $j_l \in \omega$, if

$$w_{i,0}(t_l, \bar{g})(j_l) = j_l \text{ and } w_{i,0}(s, \bar{g})(j_l) \uparrow,$$

then the condition 2.1–(b) holds.

Assume this is not the case. Then the following hypothesis $\mathscr{S}$ holds:

For any $l, k < \omega$ (with $l < k$), there is a $F = \{w_1(x, \bar{g}), ..., w_t(x, \bar{g})\}$ such that there exist some $w_{i,0}$ which is an a. c. subword of $w_i(x, \bar{g}) \in F$, and some $j_l \in \omega$ such that

$$w_{i,0}(t_l, \bar{g})(j_l) = j_l \text{ and } w_{i,0}(s, \bar{g})(j_l) \uparrow,$$

but for any subword z of $w_{i,0} = u_1 z u_2$, if z is an a. c. subword of $w_{i,0}$, then the computation of $w_{i,0}(t_l, \bar{g})(j_l)$ is not in the following form:

$$\langle n_{11}, n_{12} \rangle \langle n_{21}, n_{11} \rangle ... \langle n_{k1}, n_{k-1,1} \rangle z(s) \langle n_{k-1,1}, n_{k,1} \rangle ... \langle n_{11}, n_{21} \rangle \langle n_{12}, n_{11} \rangle (l),$$

where $z(s)(n_{k1}) = n_{k1}$, $n_{12} = l$ and each $\langle n_j, n_{j'} \rangle$ is either in t_l or in g_i.

We shall use the above hypothesis to construct a tree.

First, we define some terminology.

Let $w_{i,0}(x, \bar{g}) = g_{i_1} x^{k_{i_1}} g_{i_2} x^{k_{i_2}} ... x^{k_{i_{m_i}}} g_{i_{m_i+1}}$, where g_{i_j} may equal to g_{i_h}, when $j \neq h$. And let $\langle h_{i_j,1}, h_{i_j,2} \rangle \in g_{i_j}$ such that

(α) $\langle h_{i_1,1}, h_{i_1,2} \rangle t_l^{k_{i_1}} \langle h_{i_2,1}, h_{i_2,2} \rangle t_l^{k_{i_2}} ... t_l^{k_{i_{m_i}}} \langle h_{i_{m_i+1},1}, h_{i_{m_i+1},2} \rangle (j_l) = j_l.$

(β) $\langle h_{i_1,1}, h_{i_1,2} \rangle s^{k_{i_1}} \langle h_{i_2,1}, h_{i_2,2} \rangle s^{k_{i_2}} ... s^{k_{i_{m_i}}} \langle h_{i_{m_i+1},1}, h_{i_{m_i+1},2} \rangle (j_l) \uparrow .$

We define

$$\varepsilon_l = \max\{h_{i_j,o} \mid 1 \leq i \leq t, 1 \leq j \leq i_{m_i+1}, o = 1, \text{ or } 2\}.$$

for any $l < k$.

Let $T = \bigcup_{m<\omega} T_m$ be a naturally ordered tree such that $\bar{\psi} \in T_m$ iff

(1) $\bar{\psi}$ is an t–tuple of finite partial functions $\bar{\psi} = \{w_1(x, \bar{\phi}), ... w_t(x, \bar{\phi})\}$, where $\bar{\phi}$ is an n–tuple of fixed-point-free 1–1 finite functions of ω, and for any $\phi \in \bar{\phi}$,

$$\text{dom}(\phi) \subseteq \max\{\varepsilon_1, ..., \varepsilon_m\} + 1,$$

$$\text{rang}(\phi) \subseteq \max\{\varepsilon_1, ..., \varepsilon_m\} + 1;$$

(2) for any $l \leq m$, there exists some $w_i(x, \bar{\phi}) \in \bar{\psi}$, in which $w_{i,0}(x, \bar{\phi})$ is an conjugate subword of $w_i(x, \bar{\phi})$, and there exists some $j \in \omega$ such that

$$w_{i,0}(t_l, \bar{\phi})(j) = j, \text{ and}$$

$$w_{i,0}(s, \bar{\phi})(j) \uparrow, \text{ and}$$

for any z which is a conjugate subword of $w_{i,0}$, $w_{i,0}(t_l, \bar{\phi})(j)$ is not in the following form:

$$\langle n_{11}, n_{12}\rangle...\langle n_{k,1}, n_{k-1,1}\rangle z(s)\langle n_{k-1,1}, n_{k,1}\rangle...\langle n_{12}, n_{11}\rangle(j),$$

where $z(s)(n_{k,1}) = n_{k,1}$, $n_{12} = j$ and each $\langle n_j, n_{j'}\rangle$ is either in t_l or in ϕ_i.

It is easily seen that T_m is a nonempty finite set for all $m < \omega$.

CLAIM. *T is a well–defined ω–tree.*

PROOF OF THE CLAIM. Without loss of generality, we may assume that for any $l \leq m$, when we construct the tree in T_l, we make sure that whenever

(α') $\qquad \langle h^l_{i_1,1}, h^l_{i_1,2}\rangle t_l^{k_{i_1}} \langle h^l_{i_2,1}, h^l_{i_2,2}\rangle t_l^{k_{i_2}}...t_l^{k_{i_{m_i}}} \langle h^l_{i_{m_i}+1,1}, h^l_{i_{m_i}+1,2}\rangle(j_l) = j_l,$

(β') $\qquad \langle h^l_{i_1,1}, h^l_{i_1,2}\rangle s^{k_{i_1}} \langle h^l_{i_2,1}, h^l_{i_2,2}\rangle s^{k_{i_2}}...s^{k_{i_{m_i}}} \langle h^l_{i_{m_i}+1,1}, h^l_{i_{m_i}+1,2}\rangle(j_l) \uparrow,$

hold, then for each $h^l_{i_j,k}$ in (α') and (β'),

$$h^l_{i_j,k} \leq \varepsilon_l.$$

In the following, we will prove that, for any $m > 0$, if

$$\bar{\psi} = \{w_i(x, \bar{\phi}) \mid 1 \leq i \leq t\} \in T_m,$$

then there exists a $\bar{\psi}' = \{w_i(x, \bar{\phi}') \mid 1 \leq i \leq t\} \in T_{m-1}$ such that

$$\forall \phi \in \bar{\phi} \exists \phi' \in \bar{\phi}'(\phi' \subseteq \phi).$$

Given $w_i(x, \bar{\phi}) \in \bar{\psi}$, we define $w_i(x, \bar{\phi}')$ as follows: for any $\phi \in \bar{\phi}$, let

$$\phi'(k) = \phi(k), \text{ if } k \in \text{dom}(\phi) \cap (\max\{\varepsilon_1, ..., \varepsilon_{m-1}\} + 1);$$

$$\phi'(k) \text{ is undefined, otherwise.}$$

Let $\bar{\phi}' = \langle \phi'_1, ..., \phi'_n\rangle$. And let $\bar{\psi}' = \{w_1(x, \bar{\phi}'), ..., w_t(x, \bar{\phi}')\}$.

We prove that $\bar{\psi}'$ satisfies (1) and (2).

Obviously $\bar{\psi}'$ satisfies (1). For (2), if there exists a k such that $\varepsilon_m \leq \varepsilon_k$, then $\bar{\psi}'$ satisfies (2). (See Lemma 3, [12].) Assume otherwise, there is a $l < m$ such that, for any $w_i(x, \bar{\phi}') \in \bar{\psi}'$, if $w_{i,0}(x, \bar{\phi}') = \phi'_{i_1} x^{n_{i_1}} \phi'_{i_2} x^{n_{i_2}}...\phi'_{i_{m_i}} x^{n_{i_{m_i}}} \phi'_{i_{m_i}+1}$ is a conjugate subword of w_i, there is not any

$$\langle\langle h_{i_1,1}, h_{i_1,2}\rangle, ..., \langle h_{i_{m_i}+1,1}, h_{i_{m_i}+1,2}\rangle\rangle$$

such that (α) and (β), where each $h_{i,j} \leq \max\{\varepsilon_1, ..., \varepsilon_{m-1}\}$. This is a contradiction to the statement $\mathcal{S}$. Hence we proved that $\bar{\psi}'$ satisfies (2).

Therefore it is clear that $\bar{\psi}' \in T_{m-1}$. Then T is a well–defined ω–tree. $\quad\dashv$

By König's Lemma, there is an infinite branch

$$B = \{b_m \mid b_m \in T_m\}$$

through T, where $b_m = \{w_1(x, \bar\phi_m), ... w_t(x, \bar\phi_m)\}$ and $\bar\phi_m = \langle \phi_{m,1}, ..., \phi_{m,n} \rangle$.

Define

$$F' = \left\{ w_1\left(x, \langle \bigcup_{m \in \omega} \phi_{m,1}, ..., \bigcup_{m \in \omega} \phi_{m,n} \rangle\right), ..., w_t\left(x, \langle \bigcup_{m \in \omega} \phi_{m,1}, ..., \bigcup_{m \in \omega} \phi_{m,n} \rangle\right) \right\}.$$

Then F' is a set of partial words, where each

$$\phi_i = \bigcup_{m \in \omega} \phi_{m,i}$$

is a fixed point free 1–1 partial function of ω. Let

$$\bar\phi = \langle \phi_1, ..., \phi_n \rangle,$$

then for any $m \in \omega$, there exist some $w_i(x, \bar\phi) \in F'$, in which $w_{i,0}(x, \bar\phi)$ is some conjugate subword of $w_i(x, \bar\phi)$, and there exists some $j \in \omega$ such that

$$w_{i,0}(t_m, \bar\phi)(j) = j \text{ and } w_{i,0}(s, \bar\phi)(j) \uparrow,$$

but for any z which is conjugate subword of $w_{i,0} = uzu^{-1}$, there is no $n \in \omega$ such that $z(s)(n) = n$ with $u(t_m)(n) = j$.

CLAIM. *There exists a $F^* \in [W]^{<\omega}$ such that, for all $\langle t_m, F_m \rangle \in A$*

$$\langle s, F^* \rangle \not\Vdash \langle t_m, F_m \rangle.$$

PROOF OF THE CLAIM. We shall use F' to construct a F^*. For each $w_i(x, \bar\phi) \in F'$, we may assume that

$$w_i(x, \bar\phi) = \phi_{i_1} x^{k_{i_1}} \phi_{i_2} x^{k_{i_2}} ... x^{k_{i_{n_i}}} \phi_{i_{n_i+1}},$$

where each ϕ_{i_j} is a fixed point free 1–1 partial function of ω except possibly $\phi_{i_1} = id$ or $\phi_{i_{n_i+1}} = id$. We shall use ϕ_{i_j} to construct two permutations $f_{i_j}^1, f_{i_j}^2$ on ω as the follows.

If ϕ_{i_j} is a permutation on ω, let $f_{i_j}^1 = f_{i_j}^2 = \phi_{i_j}$. Otherwise, we will do the following:

We arrange all elements

$$r_{i_j}^1, r_{i_j}^2, r_{i_j}^3, ...$$

in $\mathrm{dom}(\phi_{i_j})$ in an increasing order, i.e.,

$$r_{i_j}^1 < r_{i_j}^2 < r_{i_j}^3, ...$$

We define

$$K_{i_j}^1 = \omega \smallsetminus \{\phi_{i_j}(r_{i_j}^{2n+1}) \mid n \in \omega \text{ and } r_{i_j}^{2n+1} \in \mathrm{dom}(\phi_{i_j})\}, \text{ and}$$

$$K_{i_j}^2 = \omega \smallsetminus \{\phi_{i_j}(r_{i_j}^{2n}) \mid n \in \omega \text{ and } r_{i_j}^{2n} \in \mathrm{dom}(\phi_{i_j})\}.$$

To define $f_{i_j}^1$, we assume $\{f_{i_j}^1(m) \mid m < k\}$ has been defined, where $0 \le k < \omega$. Now we define $f_{i_j}^1(k)$ as follows:

if $k = r_{i_j}^{2n+1}$ for some $n \in \omega$, let $f_{i_j}^1(k) = \phi_{i_j}(k)$;

otherwise, let $f_{i_j}^1(k) = $ the least $l \in K_{i_j}^1 \smallsetminus \{f_{i_j}^1(m) \mid m < k\}$ such that $l \ne k$.

To define $f_{i_j}^2$, we assume $\{f_{i_j}^2(m) \mid m < k\}$ has been defined.

if $k = r_{i_j}^{2n}$ for some $n \in \omega$, let $f_{i_j}^2(k) = \phi_{i_j}(k)$;

otherwise, let $f_{i_j}^2(k) =$ the least $l \in K_{i_j}^2 \setminus \{f_{i_j}^2(m) \mid m < k\}$ such that $l \neq k$. We define

$$w_{i,1} = f_{i_1}^1 x^{k_{i_1}} f_{i_2}^1 x^{k_{i_2}} \ldots f_{i_{n_i}}^1 x^{k_{i_{n_i}}} f_{i_{n_i+1}}^1$$

$$w_{i,2} = f_{i_1}^1 x^{k_{i_1}} f_{i_2}^1 x^{k_{i_2}} \ldots f_{i_{n_i}}^1 x^{k_{i_{n_i}}} f_{i_{n_i+1}}^2$$

$$\vdots$$

$$w_{i,2^{n_i+1}-1} = f_{i_1}^2 x^{k_{i_1}} f_{i_2}^2 x^{k_{i_2}} \ldots f_{i_{n_i}}^2 x^{k_{i_{n_i}}} f_{i_{n_i+1}}^1$$

$$w_{i,2^{(n_i+1)}} = f_{i_1}^2 x^{k_{i_1}} f_{i_2}^2 x^{k_{i_2}} \ldots f_{i_{n_i}}^2 x^{k_{i_{n_i}}} f_{i_{n_i+1}}^2.$$

Let $F^* = \{w_{i,j} \mid 1 \leq i \leq t$ and $1 \leq j \leq 2^{n_i+1}\}$. Obviously, $\langle s, F^* \rangle$ is a member of $\mathbb{G}$.

Next we shall prove that for any $m \in \omega$, there exists some $w(x, \bar{f}) \in F^*$, in which $w_0(x, \bar{f})$ is an a. c. subword of $w(x, \bar{f})$, and there exists some $j \in \omega$ such that

$$w_0(t_m, \bar{f})(j) = j \text{ and } w_0(s, \bar{f})(j) \uparrow,$$

but for any a. c. subword z in w_0, $w_0(t_m, \bar{f})(j)$ is not in the following form:

$$\langle n_{11}, n_{12} \rangle \ldots \langle n_{k,1}, n_{k-1,1} \rangle z(s) \langle n_{k-1,1}, n_{k,1} \rangle \ldots \langle n_{12}, n_{11} \rangle (j),$$

where $z(s)(n_{k,1}) = n_{k,1}$, $n_{12} = j$ and each $\langle n_j, n_{j'} \rangle$ is in either f_i or t_m. Hence $\langle s, F^* \rangle \not\Vdash \langle t_m, F_m \rangle$, for any $\langle t_m, F_m \rangle \in A$.

By the above tree argument, we know that, for any $m \in \omega$, there exists some $w_i(x, \bar{\phi}) \in F'$ in which $w_0(x, \bar{\phi})$ is a conjugate subword of $w_i(x, \bar{\phi})$ and there is some $j_m \in \omega$ such that

$$w_{i,0}(t_m, \bar{\phi})(j_m) = j_m,$$

$$w_{i,0}(s, \bar{\phi})(j_m) \uparrow, \text{ and}$$

there is no conjugate subword z in $w_0 = uzu^{-1}$ such that $z(s)(n) = n$ with $u(t_m)(n) = j_m$.

We may assume that

$$w_{i,0}(x, \bar{\phi}) = \phi_{i_1} x^{k_{i_1}} \phi_{i_2} x^{k_{i_2}} \ldots x^{k_{i_{m_i}}} \phi_{i_{m_i+1}},$$

where ϕ_{i_j} may equal to ϕ_{i_h} when $j \neq h$. As we did above, we used each ϕ_{i_j} to obtain $f_{i_j}^1$ and $f_{i_j}^2$. We know that $f_{i_j}^1$ preserves all $\langle r_{i_j}^{2n+1}, \phi_{i_j}(r_{i_j}^{2n+1}) \rangle \in \phi_{i_j}$; and $f_{i_j}^2$ preserves all $\langle r_{i_j}^{2n}, \phi_{i_j}(r_{i_j}^{2n}) \rangle \in \phi_{i_j}$. Also we know that

$$w_{i,0}(t_m, \bar{\phi})(j_m) = \phi_{i_1} t_m^{k_{i_1}} \phi_{i_2} \ldots t_m^{k_{i_{m_i}}} \phi_{i_{m_i+1}}(j_m) = j_m,$$

$$w_{i,0}(s, \bar{\phi})(j_m) \uparrow,$$

and there is no conjugate subword z in $w_0 = uzu^{-1}$ such that $z(s)(n) = n$ with $u(t_m)(n) = j_m$. Then, for each $j \in \{1, \ldots, m_i + 1\}$, there is a pair $\langle h_{i_j}, \phi_{i_j}(h_{i_j}) \rangle$ such that

$$\{\langle h_{i_1}, \phi_{i_1}(h_{i_1}) \rangle\} t_m^{k_{i_1}} \ldots t_m^{k_{i_{m_i}}} \{\langle h_{i_{m_i+1}}, \phi_{i_{m_i+1}}(h_{i_{m_i+1}}) \rangle\}(j_m) = j_m.$$

Since for any $j \in \{1, ..., m_i + 1\}$, h_{i_j} is either at an even or at an odd place of the sequence

$$r_{i_j}^1, r_{i_j}^2, r_{i_j}^3, ...$$

so by our construction of $w_{i,1}, ..., w_{i,2^{n_i}+1}$, there is a $w_{i,k}$, where $1 \le k \le 2^{(n_i+1)}$, such that there exists some $w_{i,k,0}$ which is an a. c. subword of $w_{i,k}$ and

$$w_{i,k,0}(t_m, \bar{f}_{i,k})(j_m) = j_m,$$

$$w_{i,k,0}(s, \bar{f}_{i,k})(j_m) \uparrow,$$

and for any a. c. subword z in $w_{i,k,0}$, $w_{i,k,0}(t_m, \bar{f}_{i,k})(j_m)$ is not in the following form:

$$\langle n_{11}, n_{12} \rangle ... \langle n_{k1}, n_{k,1} \rangle z(s) \langle n_{k-1,1}, n_{k,1} \rangle ... \langle n_{12}, n_{11} \rangle (j),$$

where $z(s)(n_{k,1}) = n_{k,1}$, $n_{12} = j$ and each $\langle n_j, n_{j'} \rangle$ is in either f_j or t_m.

Therefore, we have proved the claim.   ⊣

The claim, however, tells us that A is not a maximal antichain, which is a contradiction. Hence, the lemma is proved.   ⊣

By induction, we can prove Lemmas 2.4 and 2.5.

LEMMA 2.4. *For any $p \in \mathbb{G}_\kappa$, there exists some $q \le p$, such that for all $\alpha \in \mathrm{supt}(q)$, there exist some injective function $s_\alpha \in \omega^{<\omega}$ and some $n_\alpha, t_\alpha < \omega$ such that*

$$\Vdash_{\mathbb{G}_\alpha} (q(\alpha) = \langle s_\alpha, G \rangle \text{ for some } G \in [W]^{t_\alpha}$$

which has the form $\{w_1(x, \bar{y}), ..., w_{t_\alpha}(x, \bar{y})\}$),

where $\bar{y} = \langle y_1, ..., y_{n_\alpha} \rangle$ stands as variables which can be substituted for any n_α–tuple $\bar{g} = \langle g_1, ..., g_{n_\alpha} \rangle$ of fixed point free permutations in $(Fpf(\omega))^{n_\alpha}$.

We shall say that a condition $q \in \mathbb{G}_\kappa$ is canonical if it satisfies the conclusion of Lemma 2.4; and from now on we shall assume that all conditions in $\mathbb{G}_\kappa$ are canonical. (This is harmless since the canonical conditions are dense in $\mathbb{G}_\kappa$.) If $q \in \mathbb{G}_\kappa$, $\alpha \in \mathrm{supt}(q)$ and

$$\Vdash_{\mathbb{G}_\alpha} (q(\alpha) = \langle s_\alpha, G \rangle \text{ for some } G \in [W]^{t_\alpha}$$

which has the form $\{w_1(x, \bar{y}), ..., w_{t_\alpha}(x, \bar{y})\}$),

then we shall write $n_\alpha^q = n_\alpha$ and $s_\alpha^q = s_\alpha$.

LEMMA 2.5. *Suppose $\Vdash_{\mathbb{G}_\kappa} \tau \in \omega$, and given $F \in [\kappa]^{<\omega}$. For each $\alpha \in F$, we have $n_\alpha, t_\alpha \in \omega$, $s_\alpha \in \omega^{<\omega}$ injective, and $G_\alpha \in [W]^{t_\alpha}$ which has the form $\{w_1(x, \bar{y}), ..., w_{t_\alpha}(x, \bar{y})\}$, where $\bar{y} = \langle y_1, ..., y_{n_\alpha} \rangle$ stands as variables which can be substituted for any n_α–tuple $\bar{g} = \langle g_1, ..., g_{n_\alpha} \rangle$ of fixed point free permutations in $(Fpf(\omega))^{n_\alpha}$, then there exists a $H \in [\omega]^{<\omega}$ such that*

$$\forall q \in \mathbb{G}_\kappa((\mathrm{supt}(q) = F \wedge \forall \alpha \in F((G_\alpha^q \in [W]^{t_\alpha}$$

which has the same form as $G_\alpha) \wedge (s_\alpha^q = s_\alpha)) \to \exists p \le q(p \Vdash_{\mathbb{G}_\kappa} \tau \in H)).

Using Lemmas 2.4 and 2.5, we can prove the following:

LEMMA 2.6. *Let $M \models (ZFC + GCH)$. There is a m.a.d. family $\mathscr{F}$ in M such that for all $\alpha < \omega_1$ if H_α is $\mathbb{G}_\alpha$–generic over M, then $\mathscr{F}$ remains to be maximal in $M[H_\alpha]$.*

PROOF. The proof is similar to the one of Lemma 2.6 in [12].   ⊣

By absoluteness, we can prove the following lemma.

LEMMA 2.7. *The following statement holds for* $\mathbb{G}_\kappa$.

$$M[H_\kappa] \cap \omega^\omega = \bigcup \{M[H_\alpha] \cap \omega^\omega \mid \alpha < \omega_1, H_\alpha \in M[H_\kappa].$$
$$\text{and } H_\alpha \text{ is } \mathbb{G}_\alpha\text{-generic over } M\}.$$

PROOF. For a sketched proof, see [6] or [14].   ⊣

Together with Lemma 2.6, this shows that there exists a m.a.d. family $\mathscr{F}$ in M such that if H_κ is $\mathbb{G}_\kappa$-generic over M, $\mathscr{F}$ remains maximal in $M[H_\kappa]$.

Thus we can conclude this section with the following theorem.

THEOREM 2.8. *It is consistent with ZFC that* $\mathfrak{a} = \omega_1$ *and* $\mathfrak{d} = \mathfrak{a}_\mathfrak{g} = \kappa = 2^\omega$.

§3. **The consistency of** $\mathfrak{a} = \mathfrak{d} < \mathfrak{a}_\mathfrak{g}$. In this section, we give a detailed proof of the following theorem.

THEOREM 3.1. *It is consistent with ZFC that* $\mathfrak{a} = \mathfrak{d} = \omega_1$ *and* $\mathfrak{a}_\mathfrak{g} = 2^\omega = \omega_2$.

The model in which the above holds will be constructed using countable support iteration of proper ω-bounding forcing adding generically a permutation which can be adjoined to any ground model cofinitary group maintaining that the generated group would still be cofinitary. Finally we will show that there is a maximal almost disjoint family in the ground model indestructible by the iteration.

3.1. Combinatorics. We introduce the basic combinatorial tools used in the forcing construction. Let $k < n < m$ be positive integers and let $f : k \longrightarrow n$ be a one-to-one function. We shall use the following notation:

$$S(f, n, m) = \{g : n \longrightarrow m \mid f \subseteq g, g \text{ one-to-one}, k \subseteq \text{rang}(g)\}.$$

The set of cofinitary permutations in $Sym(\omega)$ will be denoted by $\mathbb{A}$. An $\mathbb{A}$-*word* is a finite sequence $w_0 w_1 \ldots w_{k-1}$, where $w_i \in \mathbb{A}$ or $w_i \in \{x, x^{-1}\}$. An $\mathbb{A}$-word $w = w_0 \ldots w_{j-1}$ is a *reduced* $\mathbb{A}$-word if

$w_i \neq id$ for all i
$w_i \in \mathbb{A} \Rightarrow w_{i+1} \notin \mathbb{A}$
$w_i = x \Rightarrow w_{i+1} \neq x^{-1}$
$w_i = x^{-1} \Rightarrow w_{i+1} \neq x$
$w_0 \neq w_{j-1}^{-1}$
$w_0 \in \mathbb{A}$ and $w_{j-1} \in \mathbb{A} \Rightarrow w_{j-1} \circ w_0 \in \mathbb{A}$.

If $w = w_0 \ldots w_{j-1}$ is a reduced $\mathbb{A}$-word, call j the *length* of w. If w is an $\mathbb{A}$-word, $B(w)$ denotes the set $\{h \in \mathbb{A} : \exists i \, w_i = h\}$. Let $w = w_0 \ldots w_{j-1}$ be a reduced $\mathbb{A}$-word. We shall call v a *(cyclical) subword* of w if for some $0 \leq l < k < j$ either $v = w_l \ldots w_k$ or $v = w_k \ldots w_{j-1} w_0 \ldots w_l$.

If $w = w_0 \ldots w_{j-1}$ is an $\mathbb{A}$-word, f a (partial) one-to-one function from ω to ω, we put

$$E(f, w) = w_0^f \circ \cdots \circ w_{j-1}^f$$

where

$$w_i^f = \begin{cases} w_i & \text{if } w_i \in \mathbb{A} \\ f & \text{if } w_i = x \\ f^{-1} & \text{if } w_i = x^{-1}. \end{cases}$$

$E(f, w)$ is a partial function and we denote by $Fix(f, w)$ the set of fixed points of $E(f, w)$.

DEFINITION 3.2. Let $k < n < m$ be positive integers and $f : k \longrightarrow n$ be a one-to-one function. For every $j \in \omega$ define a norm v_j on subsets of $S(f, n, m)$ as follows:

$v_j(X) \geq 0$ for every nonempty $X \subseteq S(f, n, m)$

$v_j(X) \geq 1$ if whenever w is a reduced $\mathbb{A}$-word of length less than j
                 such that $\forall h \in B(w) \; Fix(h) \subseteq k$ then
                 there is a $g \in X$ such that $Fix(f, w) = Fix(g, w)$

$v_j(X) \geq i + 1$ if whenever $X = A_0 \cup A_1$ then there is an $l \in \{0, 1\}$
                 such that $v_j(A_l) \geq i$

$v_j(X) = i$ if i is maximal such that $v_j(X) \geq i$.

The rest of this section is devoted solely to proving that we can always find sets of arbitrarily big norms. To that end we have to introduce yet another definition.

DEFINITION 3.3. Let $X \subseteq S(f, n, m)$, u, j integers. We will say that X is (u, j)-big if for every collection $\{w_l\}_{l=0}^{u-1}$ of reduced $\mathbb{A}$-words, each of them of length less than j and such that $\forall h \in B(w_l) \; Fix(h) \subseteq k$, there is a $g \in X$ such that $\forall l < u$ $Fix(f, w_l) = Fix(g, w_l)$.

LEMMA 3.4. Let $f : k \longrightarrow n$ be one-to-one, $k < n < m$, $u, j \in \omega$. If $X \subseteq S(f, n, m)$ is $(2^u, j)$-big then $v_j(X) \geq u$.

PROOF. We shall prove the claim by induction on u.

$u = 0$: Trivial.

$u = 1$: The definition of X being $(2, j)$-big immediately implies $v_j(X) \geq 1$.

$u = v + 1$: Let $X \subseteq S(f, n, m)$ be $(2^u, j)$-big. Assume that $v_j(X) < u$. Then there is a partition $X = A_0 \cup A_1$ such that $v_j(A_0) < v$ and $v_j(A_1) < v$. By our induction hypothesis there are two collections $W_0 = \{w_l^0\}_{l=1}^{2^v}$ and $W_1 = \{w_l^1\}_{l=1}^{2^v}$ of reduced $\mathbb{A}$-words with all fixed points in $\mathrm{dom}(f)$ such that there is no g in A_i, $i \in 2$, such that $Fix(f, w_l^i) = Fix(g, w_l^i)$ for all $l \in \{1 \ldots 2^v\}$. Then there would be no g in X such that $Fix(f, w) = Fix(g, w)$ for every $w \in \{w_l^i\}_{l=1 \ldots 2^v}^{i=0,1}$. That would contradict, however, the assumption that X was $(2^u, j)$-big. ⊣

LEMMA 3.5. Let $X \subseteq S(f, n, m)$, w a reduced $\mathbb{A}$-word of length less than j such that $\forall h \in B(w) \; Fix(h) \subseteq \mathrm{dom}(f)$. Then

$$v_j(\{g \in X : Fix(f, w) = Fix(g, w)\}) \geq v_j(X) - 1.$$

PROOF. For $v_j(X) \leq 1$ it is completely trivial.

If $v_j(X) > 1$ then either $v_j(\{g \in X : Fix(f, w) = Fix(g, w)\}) \geq v_j(X) - 1$ or $v_j(\{g \in X : Fix(f, w) \neq Fix(g, w)\}) \geq v_j(X) - 1$. The latter contradicts, however, the fact that $v_j(X) > 1$. ⊣

LEMMA 3.6. For every $k, j, u \in \omega$ there are $n, m \in \omega$, $k < n < m$ such that $S(f, n, m)$ is (u, j)-big for every one-to-one $f : k \longrightarrow n$.

PROOF. We have to show that there are $n, m \in \omega$ such that, given a collection of u-many words of length less than j such that fixed points of all permutations involved are contained in the domain of f, there is a $g \in S(f, n, m)$ not adding new fixed points. The argument is basically just a simple counting argument.

Let $f : k \longrightarrow n$ be a one-to-one function w a reduced $\mathbb{A}$-word of length less than j with all fixed points contained in k (we use this to abbreviate $\forall h \in B(w)$: $Fix(w) \subseteq k$) and let $d \neq r$ be a pair of integers such that $f \cup \{(d, r)\}$ is a one-to-one

function. We shall say that (d, r) is (f, w)-*good* if $Fix(f \cup \{(d, r)\}, w) = Fix(f, w)$. If a pair (d, r) is not (f, w)-good we shall say that it is (f, w)-*bad*.

CLAIM 1. *If (d, r) is (f, w)-bad then one of the following holds*:

(1) *There is a subword v of w such that $E(f, v)(d) = r$ or $E(f, v)(r) = d$*
(2) *There are subwords v_d, v_r of w such that $E(f, v_d)(d) = d$ or $E(f, v_r)(r) = r$.*

Let $w = w_0 \ldots w_{j-1}$. If (d, r) is (f, w)-bad then there is a

$$t \in Fix(f \cup \{(d, r)\}, w) \setminus Fix(f, w).$$

That is $E(f \cup \{(d, r)\}, w)(t) = t$ but $E(f, w)(t)$ is undefined. Let $l < j$ be maximal such that $E(f, w_0 \ldots w_{l-1})(t) = d$ or $E(f, w_0 \ldots w_{l-1})(t) = r$. Similarly, let $l' < j$ be minimal such that $E(f, w_{l'} \ldots w_{j-1})(t) = r$ or $E(f, w'_l \ldots w_{j-1})(t) = d$. Note that such l and l' have to exist since t is a new fixed point and for the same reason $l < l'$. Then one of the following holds:

(1) $E(f, w_{l'} \ldots w_{j-1} w_o \ldots w_{l-1})(d) = r$
(2) $E(f, w_{l'} \ldots w_{j-1} w_o \ldots w_{l-1})(r) = d$
(3) $E(f, w_{l'} \ldots w_{j-1} w_o \ldots w_{l-1})(d) = d$
(4) $E(f, w_{l'} \ldots w_{j-1} w_o \ldots w_{l-1})(r) = r$

If one of the first two clauses holds, we are done. So assume that either (3) or (4) holds. As the situation is symmetrical assume that (3) holds and let $v_d = w'_l \ldots w_{j-1} w_o \ldots w_{l-1}$. Note that the word $w_l \ldots w_{l'}$ is of the form $x w' x^{-1}$ by maximality (resp. minimality) of l and l'. Now consider the word w' and note that $E(f \cup \{(d, r)\}, w')(r) = r$. Let v be a subword of w' such that $E(f, v)(r) \in \{d, r\}$. It is easy to see that in any case this finishes the proof of the Claim.

CLAIM 2. *Given $j, f, d \notin \dom(f), w$ there are at most $k + 2^j$-many r such that (d, r) is (f, w)-bad and, similarly, for $r \notin \rang(f)$ there are at most $k + 2^j$-many d such that (d, r) is (f, w)-bad.*

This follows immediately from Claim 1, since there are at most 2^j-many subwords of w. We added k to the bound since we have to make sure that $f \cup \{(d, r)\}$ is a one-to-one function.

CLAIM 3. *Given $j, f, d \notin \dom(f)$ and $\{w_l\}_{l=1}^u$ a collection of reduced $\mathbb{A}$-words with all fixed points contained in the domain of f there are at most $k + u \cdot 2^j$-many r such that (d, r) is (f, w_l)-bad for some l and, similarly, for $r \notin \rang(f)$ there are at most $k + u \cdot 2^j$-many d such that (d, r) is (f, w_l)-bad for some l.*

Each word has at most 2^j-many subwords which could cause (d, r) to be bad and we have u-many words to deal with.

Notice that the bounds depend neither on f nor on the particular words involved but only on j, u and k. Therefore it is not difficult to find n and m ($n > k^2 \cdot u \cdot 2^j$ and $m > n^2 \cdot u \cdot 2^j$ should work) so that, given a family of u-many reduced $\mathbb{A}$-words, one can inductively extend f to a $g : n \longrightarrow m$ so that $k = \dom(f) \subseteq \rang(g)$ and $Fix(f, w) = Fix(g, w)$ for every w listed. To that end put $f_0 = f$. Having defined f_i find a pair (d_i, r_i) which is (f_i, w)-good for every w involved and such that $d < n$ and $r \in k \setminus \rang(f_i)$. Then put $f_{i+1} = f_i \cup \{(d_i, r_i)\}$ and continue until $k \subseteq \rang(f_i)$. Then proceed by finding (d_i, r_i) which is (f_i, w)-good for every w involved and such that $d < n$ and $r < m$. Then put $f_{i+1} = f_i \cup \{(d_i, r_i)\}$ and continue until $\dom(f_i) = n$. Then put $g = f_i$. Since we have not added any bad

pairs to f, g does not add any new fixed points and this is exactly what we wanted to prove.   ⊣

LEMMA 3.7. *There is a strictly increasing function $n : \omega \longrightarrow \omega$ such that*

$$v_i(S(f, n(i+1), n(i+2))) \geq i$$

for every $i \in \omega$ and every $f : n(i) \longrightarrow n(i+1)$.

PROOF. Construct n by induction using Lemma 3.6 and Lemma 3.4.   ⊣

3.2. Single step forcing. Let $n : \omega \longrightarrow \omega$ be as in Lemma 3.7. We shall define a forcing notion $\mathbb{P}$ as follows: $p \in \mathbb{P}$ if

(1) p is a finite branching tree of height ω
(2) $(\forall t \in p) \operatorname{dom}(t) \in \omega$
(3) $(\forall t \in p) \, t(0) : n(0) \longrightarrow n(1)$ and $t(i+1) \in S(t(i), n(i+1), n(i+2))$
(4) $(\forall j \in \omega) |\{t \in p : v_{|t|}(succ(t)) < j\}| < \omega$

where $succ_p(t) = \{t' \in p : t \subseteq t' \text{ and } \operatorname{dom}(t') = \operatorname{dom}(t) + 1\}$. As usual $p \leq p'$ if $p \subseteq p'$.

For $p \in \mathbb{P}$, $t \in p$ we put $\Theta_p(t) = v_{|t|}(succ_p(t))$. We shall call p a *k-tree with stem s* if

(1) $(\forall t \in p) \, t \subseteq s$ or $s \subseteq t$ and
(2) $(\forall t \in p) \, s \subseteq t \Rightarrow \Theta_p(t) \geq k$

If $n \in \omega$ and $p, p' \in \mathbb{P}$ we shall say that

$$p \leq_n p' \text{ if } \forall t \in p \; \Theta_{p'}(t) \leq n \Rightarrow succ_p(t) = succ_{p'}(t)$$
$$\Theta_{p'}(t) \geq n \Rightarrow \Theta_p(t) \geq n.$$

A partial order $\mathbb{P}$ satisfies *Axiom A* if there is a sequence $\{\leq_n : n \in \omega\}$ of orderings on $\mathbb{P}$ such that

(1) $p \leq_0 q$ if $p \leq q$ for every $p, q \in \mathbb{P}$
(2) $p \leq_{n+1} q \Rightarrow p \leq_n q$ for all $p, q \in \mathbb{P}$
(3) If $\{p_n : n \in \omega\}$ is such that $\forall n \; p_{n+1} \leq_n p_n$ then $\exists p \in \mathbb{P} \, \forall n \in \omega \; p \leq_n p_n$
(4) $\forall \mathscr{A}$ a maximal antichain in $\mathbb{P}$, $\forall p \in \mathbb{P}$ and $\forall n \in \omega \; \exists q \leq_n p$ such that $\{r \in \mathscr{A} : r \text{ is compatible with } q\}$ is countable.

A forcing $\mathbb{P}$ is *ω-bounding* if for every $\mathbb{P}$-name τ and every $p \in \mathbb{P}$ such that $p \Vdash \text{“}\tau \in \omega^\omega\text{”}$ there is a $q \leq p$ and there is a $g \in \omega^\omega$ such that $q \Vdash \text{“}\tau \leq g\text{”}$. It is well known that every forcing satisfying Axiom A is proper and that a countable support iteration of proper ω-bounding forcings is ω-bounding (see [7]).

LEMMA 3.8 (The Fusion Lemma). *Let $\{p_n : n \in \omega\}$ be such that $\forall n \in \omega \; p_{n+1} \leq_n p_n$. Then $p = \bigcap\{p_n : n \in \omega\} \in \mathbb{P}$ and $\forall n \in \omega \; p \leq_n p_n$.*

PROOF. Left to the reader.   ⊣

LEMMA 3.9. $\mathbb{P}$ *is a non-trivial ω-bounding forcing satisfying Axiom A.*

PROOF. The fact that $\mathbb{P}$ is a non-trivial forcing follows immediately from Lemma 3.7. For the rest of the proof we shall utilize the following:

CLAIM. *Let τ be a $\mathbb{P}$-name, $p \in \mathbb{P}$ such that $p \Vdash \text{“}\tau \in V\text{”}$ and $n \in \omega$. Then there is a $p' \leq_n p$ and F a finite set such that $p' \Vdash \text{“}\tau \in F\text{”}$.*

Using the Claim and Lemma 3.8 it is easy to see that $\mathbb{P}$ indeed satisfies Axiom A. The condition (4) even holds in a stronger sense since, for every antichain $\mathscr{A}$ and $p \in \mathbb{P}$ there is a $p' \leq_n p$ such that $\{q \in \mathscr{A} : q$ is compatible with $p'\}$ is finite.

To show that $\mathbb{P}$ is ω-bounding let τ and p be such that $p \Vdash$ "τ is a function from ω to ω". Construct a sequence $\{p_n : n \in \omega\}$ and a sequence $\{F_n : n \in \omega\}$ such that

(1) $p_0 \leq p$
(2) $p_{n+1} \leq_n p_n$ and
(3) $p_n \Vdash$ "$\tau(n) \in F_n$".

Let p be the fusion of the sequence and $g \in \omega^\omega$ is defined by $g(n) = \max(F_n \cap \omega)$. Then $p \Vdash$ "$\tau \leq g$".

PROOF OF THE CLAIM. Let p, n and τ be given. For $t \in p$ define a rank $r(t)$ as follows:

$$r(t) = 0 \text{ if } \exists n\text{-tree } q \leq p \text{ with stem } t \text{ such that}$$
$$\exists A_q \in V : q \Vdash \text{"}\tau = A_q\text{"}$$
$$r(t) = i + 1 \text{ if } r(t) \nleq i \text{ and}$$
$$v_{|t|}(\{s \in succ_p(t) : r(s) \leq i\}) \geq \Theta_p(t) - 1.$$

$\forall t \in p \, \exists i \in \omega : r(t) = i$: If not, then $\exists t \in p$ such that

$$v_{|t|}(\{s \in succ_p(t) : r(s) \text{ is not defined }\}) \geq \Theta_p(t) - 1.$$

By induction we can then construct a tree $p' \subseteq p$ such that $\forall s \in p'$

$$v_{|s|}(\{s' \in succ_p(s) : r(s') \text{ is not defined }\}) \geq \Theta_p(s) - 1$$

and

$$succ_{p'}(s) = \{s' \in succ_p(s) : r(s') \text{ is not defined }\}.$$

From the construction it is obvious that $p' \in \mathbb{P}$. This contradicts, however, the fact that the set

$$\{q \in \mathbb{P} : \exists A \in V \quad q \Vdash \text{"}\tau = A\text{"}\}$$

is dense in $\mathbb{P}$.

Fix $k \in \omega$ such that $\forall t \in p : |t| \geq k \Rightarrow \Theta_p(t) > n$. The fact that such a k exists follows immediately from the definition of $\mathbb{P}$. Define $p' \subseteq p$ as follows:

(1) $\forall t \in p : |t| \leq k \Rightarrow t \in p'$
(2) If $t \in p'$, $|t| \geq k$ and $r(t) = i > 0$ then

$$succ_{p'}(t) = \{s \in succ_p(t) : r(s) < i\}$$

(3) If $t \in p'$, $|t| \geq k$, $r(t) = 0$ and $r(t \upharpoonright dom(t) - 1) > 0$ then choose a $q_t \leq p$ an n-tree with stem t and an A_{q_t} such that $q_t \Vdash$ "$\tau = A_{q_t}$". Let $t \subseteq s$. Then $s \in p'$ if and only if $s \in q_t$.

Put $F = \{A_{q_t} : t \in p', t$ minimal such that $r(t) = 0\}$. F is a finite set since the tree p is finitely branching and r is well-founded. Obviously $p' \leq_n p$ and $p' \Vdash$ "$\tau \in F$. $\dashv$

$\dashv$

LEMMA 3.10. *Let G be a $\mathbb{P}$-generic filter. Let $\pi = \bigcup \bigcap G$. Then $\pi \in Sym(\omega)$ and for every ground model cofinitary group $\mathbb{G} \leq Sym(\omega)$, the group $\mathbb{G} * \langle \pi \rangle$ is cofinitary.*

PROOF. For every $n \in \omega$ is the set of $p \in \mathbb{P}$ with stem t such that $n \subseteq \operatorname{dom}(\bigcup t) \cap \operatorname{rang}(\bigcup t)$ dense. Therefore π is indeed a permutation.

If $\mathbb{G} * \langle \pi \rangle$ was not cofinitary then there would be a reduced $\mathbb{A}$-word w such that $B(w) \subseteq \mathbb{G}$ and $E(\pi, w)$ has infinitely many fixed points. Let j be greater than the length of w and such that $\forall h \in B(w) \; Fix(h) \subseteq j$. Using Lemma 3.1.4 it is easy to see that the set of p with stem s of length bigger than j such that

$$p \Vdash \text{``} Fix(\pi, w) = Fix(\bigcup s, w)\text{''}$$

is dense, which is a contradiction.   ⊣

3.3. Iteration. In this section we utilize ideas from [2] and [8]. The first three Lemmas are a reformulation of results from [2]. The main result of this section is Lemma 3.16.

We will call $Seq(\mathbb{P})$ the set of all finite sequences t such that $\operatorname{dom}(t) \in \omega$, $t(0) : n(0) \longrightarrow n(1)$ and $t(i+1) \in S(t(i), n(i+1), n(i+2))$. $Seq_n(\mathbb{P})$ will denote the set of sequences in $Seq(\mathbb{P})$ of length n. For $p \in \mathbb{P}$ and $s \in Seq(\mathbb{P})$ we let $p_s = \{t \in p : t \subseteq s \text{ or } s \subseteq t\}$. Notice that $p_s \in \mathbb{P}$ if and only if $s \in p$.

$\mathbb{P}_\alpha$ denotes a countable support iteration of $\mathbb{P}$ of length α. In order for this to be well defined notice that the conclusion of Lemma 3.7 is finitary, hence absolute. A version of the Fusion Lemma will be needed also for $\mathbb{P}_\alpha$. If $p, q \in \mathbb{P}_\alpha$, $n \in \omega$ and $F \in [\operatorname{dom}(q)]^{<\omega}$ we will write $p <_{F,n} q$ when $p \leq q$ and $\forall \beta \in F \; p \restriction \beta \Vdash \text{``} p(\beta) <_n q(\beta)\text{''}$.

LEMMA 3.11 (The Fusion Lemma). *Let* $\{(p_i, m_i, F_i) : i \in \omega\}$ *be such that* $p_i \in \mathbb{P}_\alpha$, $m_i \in \omega$, $m_i \nearrow \infty$, $F_i \subseteq F_{i+1}$, $\bigcup F_i = \bigcup \operatorname{dom}(p_i)$ *and* $p_{i+1} <_{F_i, m_i} p_i$ *for every* i. *Define* p *so that* $\operatorname{dom}(p) = \bigcup\{\operatorname{dom}(p_i) : i \in \omega\}$ *and* $\forall \beta \in \operatorname{dom}(p)$ $p(\beta) = \bigcap\{p_i(\beta) : \beta \in \operatorname{dom}(p_i)\}$. *Then* $p \in \mathbb{P}_\alpha$.

PROOF. Proof is an easy induction using Lemma 3.8.   ⊣

Let $p \in \mathbb{P}_\alpha$, $F \in [\operatorname{dom}(p)]^{<\omega}$ and $\sigma : F \longrightarrow Seq_n(\mathbb{P})$. We shall denote $p \restriction \sigma$ the function with the same domain as p such that

$$(p \restriction \sigma)(\beta) = \begin{cases} p(\beta) & \text{if } \beta \notin F \\ p(\beta)_{\sigma(\beta)} & \text{if } \beta \in F. \end{cases}$$

$p \restriction \sigma$ doesn't have to be a condition. We'll say that σ is *consistent with* p if $p \restriction \sigma \in \mathbb{P}_\alpha$ (i.e. if $\forall \beta \in F \; (p \restriction \sigma) \restriction \beta \Vdash \text{``} \sigma(\beta) \in p(\beta)\text{''}$). We shall say that p is (F, n)-*determined* provided that $\forall \sigma : F \longrightarrow Seq_n(\mathbb{P})$ either σ is consistent with p or $\exists \beta \in F$ s.t. $\sigma \restriction (F \cap \beta)$ is consistent with p and $(p \restriction \sigma) \restriction \beta \Vdash \text{``} \sigma(\beta) \notin p(\beta)\text{''}$.

LEMMA 3.12. *Let* $p \in \mathbb{P}_\alpha$, $F \in [\operatorname{dom}(p)]^{<\omega}$, $n \in \omega$ *and* $\sigma : F \longrightarrow Seq_n(\mathbb{P})$. *Then*:

(1) *If* $\max F < \beta < \alpha$ *then* $(p \restriction \sigma) \restriction \beta = (p \restriction \beta) \restriction \sigma$.
(2) p *is* $(\{0\}, n)$-*determined for every* $n \in \omega$.
(3) *If* $k \geq n$, $F \subseteq G$, $q <_{G,k} p$ *and* p *is* (F, n)-*determined then so is* q.
(4) *If* $\max F < \beta < \alpha$ *then* p *is* (F, n)-*determined if and only if* $p \restriction \beta$ *is* (F, n)-*determined.*
(5) *There is* $q \in \mathbb{P}_\alpha$, $q \leq p$ *such that* $q = q \restriction \tau$ *for some* $\tau : F \longrightarrow Seq_n(\mathbb{P})$.
(6) *If* p *is* (F, n)-*determined and* $q \leq p$ *then there is* $\tau : F \longrightarrow Seq_n(\mathbb{P})$ *such that* τ *is consistent with* p, *and* q *and* $p \restriction \tau$ *are compatible.*

PROOF. The only parts which are not completely obvious are (5) and (6) and (6) follows from (5), so all we have to prove is (5). Let $\beta_1, \ldots, \beta_k$ be an increasing enumeration of F. By induction on $i \leq k$ find q_i and $\sigma_i : \{\beta_1, \ldots, \beta_i\} \longrightarrow Seq_n(\mathbb{P})$ such that $p \geq q_0 \geq \cdots \geq q_k$ and $q_i \restriction \sigma_i = q_i$. Let $q_0 = p$ and $\sigma_0 = \emptyset$. Given q_i and σ_i find $q \leq q_i \restriction \beta_{i+1}$ and $s \in Seq_n(\mathbb{P})$ such that $q \Vdash$ "$s \in q_i(\beta_{i+1})$". Then let $\sigma_{i+1} = \sigma_i \cup (\beta_{i+1}, s)\}$ and

$$q_{i+1}(\beta) = \begin{cases} q(\beta) & \text{if} \quad \beta < \beta_{i+1} \\ q_i(\beta)_s & \text{if} \quad \beta = \beta_{i+1} \\ q_i(\beta) & \text{if} \quad \beta > \beta_{i+1}. \end{cases} \qquad \dashv$$

We shall say that $p \in \mathbb{P}_\alpha$ is *continuous* if $\forall F \in [\text{dom}(p)]^{<\omega} \ \forall n \in \omega \ \exists m \geq n$ $\exists G \in [\text{dom}(p)]^{<\omega} \ F \subseteq G$ so that p is (G, m)-determined. For $q \in \mathbb{P}$, $n, m \in \omega$ we shall say that m is an *n-bound* in q if $\forall t \in q \ |t| \geq m \Rightarrow \Theta_q(t) > n$. Let $q \in \mathbb{P}_\alpha$, F a finite subset of $\text{dom}(q)$ and $n \in \omega$ be given. Then we shall call an $m \in \omega$ an *(F, n)-bound* in q if $\forall \beta \in F \ q \restriction \beta \Vdash$ "m is an n-bound in $q(\beta)$".

LEMMA 3.13. *Let $p \in \mathbb{P}_\alpha$, $n \in \omega$ and $F \in [\text{dom}(p)]^{<\omega}$. There is a $q <_{F,n} p$ and an $m \in \omega$ such that q is (F, n)-determined and m is an (F, n)-bound in q.*

PROOF. We shall prove this by induction on α.

$\alpha = 1$: This is true since every $p \in \mathbb{P}_1$ is $(\{0\}, n)$-determined for every n and the existence of m follows immediately from the definition of $\mathbb{P}$.

$\alpha = \beta + 1$: We only have to consider the case when $\beta \in F$. There are $\mathbb{P}_\beta$-names $\dot{q}$ and $\dot{m}$ such that $p \restriction \beta \Vdash$ "$\dot{q} <_n p(\beta)$ and $\dot{m}$ is an n-bound in $\dot{q}$". By our inductive hypothesis there are q' and m' such that q' is $(F \setminus \{\beta\}, n)$-determined, $q' <_{F \setminus \{\beta\}, n} p \restriction \beta$ and m' is an $(F \setminus \{\beta\}, n)$-bound. For every σ consistent with q' let m_σ be such that $q' \restriction \sigma \Vdash$ "$\dot{m} = m_\sigma$". Then put $q = q'^\frown \dot{q}$ and

$$m = \max\{\{m'\} \cup \{m_\sigma : \sigma \text{ is compatible with } q'\} + 1.$$

α-limit: Choose β such that $\max F < \beta < \alpha$. Let $q' \in \mathbb{P}_\beta$, $m \in \omega$ be such that $q' <_{F,n} p \restriction \beta$, m is an (F, n)-bound in q' and q' is (F, n)-determined. Then put

$$q(\gamma) = \begin{cases} q'(\gamma) & \text{if } \gamma < \beta \\ p(\gamma) & \text{if } \gamma \geq \beta \end{cases}$$

It is left to the reader to check that this works. $\qquad \dashv$

LEMMA 3.14. *For every $p \in \mathbb{P}_\alpha$ there is a continuous $q \leq p$.*

PROOF. We shall construct q_n, m_n and F_n by induction so that

(1) $p_0 = p$, $n_o = 1$, $F_0 = \{\min(\text{dom}(p))\}$
(2) $p_{n+1} <_{F_n, m_n} p_n$
(3) p_{n+1} is (F_n, m_n)-determined
(4) m_{n+1} is an (F_n, m_n) bound in p_n
(5) $\bigcup\{F_n : n \in \omega\} = \bigcup\{\text{dom}(p_n) : n \in \omega\}$.

Let q be the fusion of this sequence. $\qquad \dashv$

We shall make use of the fact that every continuous condition q is fully described by a sequence $\{(F_i, m_i, \Sigma_i) : i \in \omega\}$ where F_i, m_i are as above and $\Sigma_i = \{\sigma : F_i \longrightarrow Seq_{m_i}(\mathbb{P})$ such that σ is consistent with $q\}$. The important property of this representation is that (informally) each condition is forced to

branch enough between levels m_i and m_{i+1}. This is being ensured by the fact that m_{i+1} is an (F_i, m_i)-bound in p. Notice that if $\{(F_i, m_i, \Sigma_i) : i \in \omega\}$ is a representation of a continuous q and $f \in \omega^\omega$ is a strictly increasing function, then $\{(F_{f(i)}, m_{f(i)}, \Sigma_{f(i)}) : i \in \omega\}$ also represents the same q.

LEMMA 3.15. *Let $q \leq p \in \mathbb{P}_\alpha$ be continuous. Then there is a representation $\{(F_i^q, m_i^q, \Sigma_i^q) : i \in \omega\}$ of q and a representation $\{(F_i^p, m_i^p, \Sigma_i^p) : i \in \omega\}$ of p such that*

$$\forall i \in \omega \quad F_i^q \cap \operatorname{dom}(p) \subseteq F_i^p \text{ and } m_i^q < m_i^p < m_{i+1}^q.$$

PROOF. Let $\{(\bar{F}_i^q, \bar{m}_i^q, \bar{\Sigma}_i^q) : i \in \omega\}$ and $\{(\bar{F}_i^p, \bar{m}_i^p, \bar{\Sigma}_i^p) : i \in \omega\}$ be representations of q and of p. We shall define new representations $\{(F_i^q, m_i^q, \Sigma_i^q) : i \in \omega\}$ and $\{(F_i^p, m_i^p, \Sigma_i^p) : i \in \omega\}$ of p and q using the previous remark. By induction define functions f and g. Put $g(0) = 0$ and having defined $g(i)$ let $f(i)$ be the least j such that $F_{g(i)}^q \cap \operatorname{dom}(p) \subseteq F_j^p$ and $m_{g(i)}^q < m_j^p$. Similarly having defined $f(i)$ let $g(i+1)$ be minimal j such that $m_{f(i)}^q < m_j^q$. Then the desired representations are $\{(\bar{F}_{g(i)}^q, \bar{m}_{g(i)}^q, \bar{\Sigma}_{g(i)}^q) : i \in \omega\}$ and $\{(\bar{F}_{f(i)}^p, \bar{m}_{f(i)}^p, \bar{\Sigma}_{f(i)}^p) : i \in \omega\}$. ⊣

Let a^* be a countable set of ordinals we define $\mathbb{P}_{a^*}$ as a countable support iteration of $\mathbb{P}$ with domain a^*. $\mathbb{P}_{a^*}$ is isomorphic to $\mathbb{P}_\delta$ where δ is the order type of a^*. Even though in general it is not obvious that every condition in $\mathbb{P}_{a^*}$ can be viewed as a condition in $\mathbb{P}_{\omega_2}$ it is obviously so for continuous ones. Since the set of continuous conditions is dense and closed under fusion we can (and will) from now on assume that **all conditions mentioned are continuous**.

LEMMA 3.16. *Let a^* be a countable subset of $\alpha < \omega_2$. Let $p^* \in \mathbb{P}_{a^*}$, $q \in \mathbb{P}_\alpha$ such that $q \leq p^*$. Then there is a $q^* \in \mathbb{P}_{a^*}$, $q^* \leq p^*$ such that if q is incompatible with an $r^* \in \mathbb{P}_{a^*}$ then q^* is incompatible with r^*.*

PROOF. Let $q \leq p^*$ be given (WLOG we can assume that $\operatorname{dom}(p) = a^*$) and let $\{(F_i^q, m_i^q, \Sigma_i^q) : i \in \omega\}$ and $\{(F_i^{p^*}, m_i^{p^*}, \Sigma_i^{p^*}) : i \in \omega\}$ be their representations as in Lemma 3.15. We shall define q^* via a representation by putting for every $i \in \omega$

$F_i^{q^*} = F_i^{p^*}$,
$m_i^{q^*} = m_i^{q^*}$ and
$\Sigma_i^{q^*} = \{\sigma \in \Sigma_i^{p^*} : \exists \tau \in \Sigma_{i+1}^q \forall \beta \in F_i^{q^*} \; \sigma(\beta) \subseteq \tau(\beta)\}$.

It is easy to see (using the fact that the representations were as in Lemma 3.15) that this indeed defines a representation of a condition. Another way of describing the same procedure is as a fusion of $p_i = \bigcup\{p \upharpoonright \tau : \tau \in \Sigma_{i+1}^q\}$. So $q^* \in \mathbb{P}_{a^*}$ and obviously $q^* \leq p^*$.

Let $r^* \in \mathbb{P}_{a^*}$ be compatible with q^*. Let $s^* \in \mathbb{P}_{a^*}$ be their common extension. Let $\{(F_i^q, m_i^q, \Sigma_i^q) : i \in \omega\}$ and $\{(F_i^{s^*}, m_i^{s^*}, \Sigma_i^{p^*}) : i \in \omega\}$ be representations of q and s^* such that for every $i \in \omega$ $F_i^{s^*} \subseteq F_i^q$ and $m_i^{s^*} < m_i^q < m_{i+1}^{s^*}$. As in Lemma 3.15 this is very easy to provide. Notice that here we are using possibly different representation of q than before. However, for notational simplicity, we denote it the same way. We shall define a common extension t of s^* and q by putting

$F_i^t = F_i^q$,
$m_i^t = m_i^q$ and
$\Sigma_i^t = \{\sigma \in \Sigma_i^q : \exists \tau \in \Sigma_{i+1}^{s^*} \forall \beta \in F_i^{s^*} \; \sigma(\beta) \subseteq \tau(\beta)\}$.

The condition t also has an alternative description using fusion. It should be obvious that $t \leq q, s^*$. That finishes the proof.   ⊣

3.4. Proof of the Main Theorem.

LEMMA 3.17. *[CH] For every proper ω-bounding forcing $\mathbb{P}$ with a dense subset of size $\aleph_1$ there is a $\mathbb{P}$-indestructible MAD family.*

PROOF. Using the properness of $\mathbb{P}$ and [CH] it is possible to construct a sequence $\{(p_\alpha, \tau_\alpha) : \alpha < \omega_1\}$, where $p_\alpha \in \mathbb{P}$, τ_α is a $\mathbb{P}$-name, so that if τ is a $\mathbb{P}$-name and $p \Vdash$ "$\tau \in [\omega]^\omega$" then there is an $\alpha \in \omega_1$ such that $p_\alpha \leq p$ and $p_\alpha \Vdash$ "$\tau = \tau_\alpha$". Having fixed such a sequence we shall construct the almost disjoint family $\mathscr{A} = \{A_\alpha : \alpha < \omega_1\}$ by induction.

Let $\{A_i : i \in \omega\}$ be a partition of ω into infinite sets. At stage α look at the pair (p_α, τ_α). If $p_\alpha \nVdash$ "$\forall \beta < \alpha |\tau_\alpha \cap A_\beta| < \omega$" then let A_α be any set almost disjoint from $\{A_\beta : \beta < \alpha\}$.

If $p_\alpha \Vdash$ "$\forall \beta < \alpha |\tau_\alpha \cap A_\beta| < \omega$" then enumerate $\{A_\beta : \beta < \alpha\}$ as $\{B_n : n \in \omega\}$ and let $C_0 = B_0$ and $C_{n+1} = B_{n+1} \setminus \bigcup \{B_i : i \leq n\}$. Let ρ be a name such that $p_\alpha \Vdash$ "$\rho \in \omega^\omega$ and $\forall m\, C_m \cap \tau_\alpha \subseteq \rho(m)$". (Let $\rho = \{(p, m, n) : p \leq p_\alpha \Rightarrow n = \min\{k : p \Vdash$ "$C_m \cap \tau_\alpha \subseteq k$"$\}\}$.) Since $\mathbb{P}$ is ω-bounding, there is an $f \in \omega^\omega$ and a $q \leq p_\alpha$ such that $q \Vdash$ "$\rho \leq f$". Put

$$A_\alpha = \bigcup_{m \in \omega} C_m \cap f(m).$$

To finish the proof it is sufficient to show that $\Vdash_\mathbb{P}$ "$\mathscr{A}$ is MAD". To that end assume the contrary, that is there is a $\mathbb{P}$-name for a real τ and a condition $p \in \mathbb{P}$ such that $p \Vdash$ "$\forall \alpha < \omega_1 : |\tau \cap A_\alpha| < \omega$". There is a β such that $p_\beta \leq p$ and $p_\beta \Vdash$ "$\tau = \tau_\beta$". Then, however, $p_\beta \Vdash$ "$\tau \subseteq A_\beta$" which is a contradiction.   ⊣

COROLLARY 3.18. *[CH] There is a $\mathbb{P}_{\omega_1}$-indestructible MAD family.*

PROOF. Even though $\mathbb{P}_{\omega_1}$ itself does not have cardinality ω_1 it has a dense subset of cardinality ω_1. Take for instance the set of continuous conditions.   ⊣

LEMMA 3.19. *[CH] Every $\mathbb{P}_{\omega_1}$-indestructible MAD family is $\mathbb{P}_{\omega_2}$-indestructible.*

PROOF. Let $\mathscr{A}$ be an $\mathbb{P}_{\omega_1}$-indestructible MAD family. Assume that there is a $\mathbb{P}_\alpha$-name τ for a real and a $p \in \mathbb{P}_\alpha$ such that $p \Vdash_{\mathbb{P}_\alpha}$ "$\forall A \in \mathscr{A} |\tau \cap A| < \omega$". Let N be an elementary submodel of $H(\omega_2)$ such that $p, \alpha, \tau, \mathscr{A} \in N$. Let

$$D_n = \{p : p \text{ decides whether } n \in \tau\}.$$

We assume all conditions involved to be continuous hence absolute. Let $a^* = \alpha \cap N$ an let $q^* \leq p$ be $(N, \mathbb{P}_\alpha)$-generic such that $q^* \in \mathbb{P}_{a^*}$. Then

(1) $\forall n \in \omega\, D_n \cap N$ is predense below q^* and $D_n \cap N \subseteq \mathbb{P}_{a^*}$
(2) There is a $\mathbb{P}_{a^*}$-name τ' such that $q^* \Vdash_{\mathbb{P}_\alpha}$ "$\tau = \tau'$".

Since $\mathscr{A}$ is $\mathbb{P}_{\omega_1}$-indestructible it is also $\mathbb{P}_{a^*}$-indestructible. Using this and the existential completeness of forcing

$$\exists r^* \in \mathbb{P}_{a^*} r^* \leq q^* \exists A \in \mathscr{A} r^* \Vdash_{\mathbb{P}_{a^*}} \text{"}|A \cap \tau| = \omega\text{"}.$$

However since $r^* \leq p$ and $p \Vdash_{\mathbb{P}_\alpha}$ "$\forall A \in \mathscr{A} |\tau \cap A| < \omega$"

$$\exists q \in \mathbb{P}_\alpha q \leq r^* \exists M \in \omega q \Vdash_{\mathbb{P}_\alpha} \text{"}\tau \cap A \subseteq M\text{"}$$

which means that q is incompatible with those elements of D_n for $n > M$, $n \in A$ which force $n \in \tau$. By Lemma 3.16 there is $s^* \in \mathbb{P}_{a^*}$, $s^* \leq r^*$ such that every $t^* \in \mathbb{P}_{a^*}$ incompatible with q is also incompatible with s^*. Therefore $s^* \Vdash_{\mathbb{P}_{a^*}}$ "$\tau \cap A \subseteq M$" which is contradictory to the fact that $r^* \Vdash_{\mathbb{P}_{a^*}}$ "$|A \cap \tau| = \omega$".   ⊣

THEOREM 3.20. *It is consistent with ZFC that* $\mathfrak{a} = \mathfrak{d} = \omega_1$ *and* $\mathfrak{a}_\mathfrak{g} = 2^\omega = \omega_2$.

PROOF. Let $V \models CH$ and let G be $\mathbb{P}_{\omega_2}$-generic over V. The proof of the fact that $2^\omega = \omega_2$ is standard and so is the proof of $\mathfrak{d} = \omega_1$ since $\mathbb{P}_{\omega_2}$ is ω-bounding. Corollary 3.18 and Lemma 3.19 give us $\mathfrak{a} = \omega_1$. So the only thing that still requires a little bit of an argument is the fact that $\mathfrak{a}_\mathfrak{g} = \omega_2$.

Assume on the contrary that there is a maximal cofinitary group $\mathbb{G}$ of $Sym(\omega)$ of size ω_1 in $V[G]$. Then this group would have to appear in $V[G_\alpha]$ for some $\alpha < \omega_2$. Let π_α be the generic permutation added by $\mathbb{Q}_\alpha[G_\alpha]$. Then by Lemma 3.10 the group $\mathbb{G} * \langle \pi_\alpha \rangle$ is cofinitary which contradicts our assumption of maximality of $\mathbb{G}$.   ⊣

REFERENCES

[1] S. A. ADELEKE, *Embeddings of infinite permutation groups in sharp, highly transitive, and homogeneous groups*, **Proceedings of Edinburgh Mathematical Society**, vol. 31 (1981), pp. 169–178.

[2] J. E. BAUMGARTNER and R. LAVER, *Iterated perfect–set forcing*, **Annals of Mathematical Logic**, vol. 17 (1979), pp. 271–288.

[3] P. J. CAMERON, *Cofinitary permutation groups*, **Bulletin of the London Mathematical Society**, vol. 28 (1996), pp. 113–140.

[4] T. JECH, *Set theory*, Academic Press, 1978.

[5] K. KUNEN, *Set theory. an introduction to independence proofs*, North-Holland, Amsterdam, 1980.

[6] A. MILLER, *Some properties of measure and category*, **Transactions of the American Mathematical Society**, vol. 266 (1981), no. 1, pp. 93–114.

[7] S. SHELAH, *Proper forcing*, Lecture Notes in Mathematics, vol. 940, Springer–Verlag, 1982.

[8] O. SPINAS and S. SHELAH, *The distributivity numbers of* $\wp(\omega)/fin$ *and its square*, (preprint).

[9] J. K. TRUSS, *Embeddings of infinite permutation groups*, **Proceedings of groups–St Andrews 1985** (E. F. Robertson and C. M. Cambell, editors), London Mathematical Society Lecture Note Series, vol. 121, Cambridge University Press, 1986, pp. 335–351.

[10] E. VAN DOUWEN, *The integers and topology*, **Handbook of set theoretic topology** (K. Kunen and J. Vaughan, editors), North-Holland, Amsterdam, 1984, pp. 111–167.

[11] Y. ZHANG, *Cofinitary groups and almost disjoint families*, **Ph.D. thesis**, Rutgers University, 1997.

[12] ———, *On a class of mad families*, this JOURNAL, vol. 64 (1999), no. 2, pp. 737–746.

[13] ———, *Maximal cofinitary groups*, **Archive of Mathematical Logic**, vol. 39 (2000), pp. 41–52.

[14] ———, *Permutation groups and covering properties*, **Journal of London Mathematical Society**, vol. 63 (2001), no. 2, pp. 1–15.

MATHEMATICS DEPARTMENT
YORK UNIVERSITY
4700 KEELE STREET
NORTH YORK, ONTARIO, CANADA, M3J 1P3
E-mail: yu50029@pascal.math.yorku.ca   *E-mail*: steprans@mathstat.yorku.ca

MATHEMATICS INSTITUTE
ACADEMIA SINICA, BEIJING, 100080, P. R. CHINA
Current address: Department of Mathematics and Computer Science, Istanbul Bilgi University, Kustepe, Istanbul, 80310, Turkey
E-mail: zhang@bilgi.edu.tr