Journal of Algebra **232,** 209–225 (2000)
doi:10.1006/jabr.2000.8396, available online at http://www.idealibrary.com on IDEAL®

Uniformity of the Meager Ideal and Maximal Cofinitary Groups

Jörg Brendle[1]

Graduate School of Science and Technology, Kobe University, Rokkodai 1-1, Nada, Kobe 657-8501, Japan
E-mail: brendle@pascal.seg.kobe-u.ac.jp

Otmar Spinas[2]

Mathematisches Seminar, Christian-Albrechts-Universität, 24098 Kiel, Germany
E-mail: spinas@math.uni-kiel.de

and

Yi Zhang[3]

Department of Mathematics and Computer Science, Istanbul Bilgi University, Inonu Cad. No. 28, Kustepe 80310, Sisli-Istanbul, Turkey; and Institute of Mathematics, Academic Sinica, Beijing 100080, People's Republic of China
E-mail: zhang@bilgi.edu.tr

Communicated by Peter M. Neumann

Received January 30, 1999

We prove that every maximal cofinitary group has size at least the cardinality of the smallest non-meager set of reals. We also provide a consistency result saying that the spectrum of possible cardinalities of maximal cofinitary groups may be quite arbitrary. © 2000 Academic Press

[1]Partially supported by Grants-in-Aid for Scientific Research (B)09440078 and (C)(2)10640118.

[2]Profil fellow of the Swiss National Science Foundation (Grant 2124-045702.95/1).

[3]Research partially supported by the Mathematics Research Institute, ETH, Switzerland. The author also thanks his friend Luca Bonatti for all kinds of help he offered.

0021-8693/00 $35.00

1. INTRODUCTION

Let ω denote the natural numbers. We say that a permutation $g \in \mathrm{Sym}(\omega)$ is *cofinitary* iff g has only finitely many fixed points. A group $G \leq \mathrm{Sym}(\omega)$ is *cofinitary* iff every non-identity element is cofinitary. Two permutations $f, g \in \mathrm{Sym}(\omega)$ are *almost disjoint* (a.d.) iff $|f \cap g| < \omega$. It is easily seen that $G \leq \mathrm{Sym}(\omega)$ is cofinitary iff G is both an almost disjoint set of permutations and a group. For a discussion of different aspects of cofinitary groups, the reader can consult the well-written survey paper by Cameron [C]. 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 in a maximal one. The following theorem was proved by Truss (see [T, T1] for details) and Adeleke [A].

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

Also, P. Neumann showed (see, e.g., [C, Proposition 10.4])

THEOREM 1.2. *There exists a maximal cofinitary group of cardinality $\mathfrak{c}$, the size of the continuum.*

This motivated Cameron [C] to ask

Question 1.3. If the continuum hypothesis (CH) fails, is it possible that there exists a maximal cofinitary group G such that $|G| < \mathfrak{c}$?

In [Z, Theorem 1.5], this problem was solved by:

THEOREM 1.4. *Assume that $\kappa \leq \lambda$ are uncountable cardinals with $cf(\lambda) > \omega$. Then it is consistent with ZFC that there exists a maximal cofinitary group $G \leq \mathrm{Sym}(\omega)$ such that $|G| = \kappa$ and $\mathfrak{c} = \lambda$.*

Here, ZFC denotes Zermelo–Fraenkel set theory with the axiom of choice (the standard axiom system for set theory), and by *consistency* we mean *relative consistency*; e.g., in the case of the above theorem, if ZFC is consistent, then so is ZFC + "there is a maximal cofinitary group of size $< \mathfrak{c}$." Such consistency results are always obtained by the method of forcing: starting with a ground model V which satisfies ZFC and (possibly) some other statements needed for the construction, one builds a larger model $V[F]$, called a generic extension, which satisfies ZFC as well as the statement one wants to show is consistent.

We shall considerably generalize this result in Section 3 of the present work by showing that the spectrum of possible cardinalities of maximal cofinitary groups may be quite arbitrary. The argument, however, is different: we use a product instead of an iteration.

During the past decades, a plethora of so-called *cardinal invariants of the continuum* (cardinals which are defined as the smallest size of a set of reals with certain combinatorial properties and which assume values between $\aleph_1$ and $\mathfrak{c}$) have been investigated, and it is natural to introduce one for the combinatorial phenomenon at hand as well.

DEFINITION 1.5. Let $\mathfrak{a}_{\mathfrak{g}}$ be the least λ such that there exists a maximal cofinitary group $G \leq \mathrm{Sym}(\omega)$ with $|G| = \lambda$.

Recently, quite a number of consistency results have been proved about $\mathfrak{a}_{\mathfrak{g}}$. For example, Zhang [Z1, Corollary 1.7] showed that $\mathfrak{a}_{\mathfrak{g}} = \aleph_1$ in the Cohen real model (the model obtained by adjoining at least $\aleph_2$ Cohen reals to a model of ZFC + CH) so that $\mathfrak{a}_{\mathfrak{g}} < \mathfrak{d} = \mathrm{cov}(\mathscr{M})$ is consistent.

Here, as is usual, we let ω^ω denote the set of functions from ω to ω, and define the *dominating number* $\mathfrak{d}$ to be the size of the least dominating (cofinal) family in $\langle \omega^\omega, \leq^* \rangle$ where $\leq^*$ denotes as usual the *eventual dominance order* on ω^ω given by $f \leq^* g$ iff $f(n) \leq g(n)$ for all but finitely many n. Similarly, the *unbounding number* $\mathfrak{b}$ is the minimal size of an unbounded subset of $\langle \omega^\omega, \leq^* \rangle$. Also $\mathrm{cov}(\mathscr{M})$ ($\mathrm{cov}(\mathscr{N})$, respectively) is the least λ such that there exists a family F of meager (null, resp.) sets such that $\bigcup F$ is the set of real numbers and $|F| = \lambda$. More on these (and other) cardinal invariants of the continuum can be found in [BJ, B, vD]. Further consistency results which have been obtained in the past will be mentioned in Section 2 of the present work for they also follow from the ZFC results presented there.

One can easily prove the result corresponding to Theorem 1.4 for maximal almost disjoint families in $\mathrm{Sym}(\omega)$. The related cardinal number was suggested by S. Thomas.

DEFINITION 1.6. Let $\mathfrak{a}_{\mathfrak{p}}$ be the least λ such that there exists a maximal almost disjoint family A in $\mathrm{Sym}(\omega)$ with $|A| = \lambda$.

Again one has $\mathfrak{a}_{\mathfrak{p}} = \aleph_1$ in the Cohen real model [Z1, Corollary 1.7].

Motivated by the mentioned consistency results concerning $\mathfrak{a}_{\mathfrak{p}}$ and $\mathfrak{a}_{\mathfrak{g}}$, S. Todorčević suggested the following question (see [Z, Z2, Question 4.6]).

Question 1.7. Can we find a lower bound for $\mathfrak{a}_{\mathfrak{g}}$ ($\mathfrak{a}_{\mathfrak{p}}$, respectively) which is also a cardinal invariant of the continuum? For example, can we prove that $\mathfrak{b} \leq \mathfrak{a}_{\mathfrak{g}}$ ($\mathfrak{b} \leq \mathfrak{a}_{\mathfrak{p}}$, resp.)?

Goldstern [G] subsequently observed

THEOREM 1.8. $\mathfrak{b} \leq \mathfrak{a}_{\mathfrak{p}}$.

By a much more complicated argument, O. Spinas and Y. Zhang obtained

THEOREM 1.9. $\mathfrak{b} \leq \mathfrak{a}_{\mathfrak{g}}$.

The proof of Theorem 1.9 uses a rather strong combinatorial lemma (Main Lemma 4.1) which might be useful for other purposes. Therefore, we give a brief sketch of the argument in Section 4 of our work.

After Y. Zhang announced Theorem 1.9 at the Logic Colloquim 1998 in Prague, Czech Republic, J. Brendle proved stronger results (Theorems 2.2 and 2.4) which subsume Theorems 1.8 and 1.9 and which are presented in detail in the next section.

2. non($\mathcal{M}$) IS A LOWER BOUND FOR $\mathfrak{a}_{\mathfrak{g}}$ AND $\mathfrak{a}_{\mathfrak{p}}$

Let $\omega^{<\omega}$ denote the set of finite sequences of natural numbers. $[\omega]^{<\omega}$ stands for the set of finite subsets of ω. For $h \in \omega^\omega$, a function $\phi: \omega \to [\omega]^{<\omega}$ with $|\phi(n)| \leq h(n)$ for all n is called an *h-slalom*. A function $\pi: \omega^{<\omega} \to \omega$ is said to be a *predictor*. If $h: \omega^{<\omega} \to \omega$, a function $\pi: \omega^{<\omega} \to [\omega]^{<\omega}$ with $|\pi(s)| \leq h(s)$ for all s is called an *h-slalom predictor*. The *uniformity* of the meager ideal non($\mathcal{M}$) is the size of the least non-meager set of reals. It is well known (and easy to see) that $\mathfrak{b} \leq$ non($\mathcal{M}$) (see, e.g., [BJ]).

THEOREM 2.1. *The following are equivalent for any cardinal* κ.

(i) non($\mathcal{M}$) $> \kappa$

(ii) *for all* $\mathcal{F} \subseteq \omega^\omega$ *of size* $\leq \kappa$ *there is* $g \in \omega^\omega$ *such that for all* $f \in \mathcal{F}$, $f(n) \neq g(n)$ *holds for almost all* n

(iii) *for all* $h \in \omega^\omega$ *and all families* Φ *of h-slaloms of size* $\leq \kappa$ *there is* $g \in \omega^\omega$ *such that for all* $\phi \in \Phi$, $g(n) \notin \phi(n)$ *for almost all* n

(iv) *for all families* Π *of predictors of size* $\leq \kappa$ *there is* $g \in \omega^\omega$ *such that for all* $\pi \in \Pi$, $g(n) \neq \pi(g \restriction n)$ *holds for almost all* n

(v) *for all* $h: \omega^{<\omega} \to \omega$ *and all families* Π *of h-slalom predictors of size* $\leq \kappa$ *there is* $g \in \omega^\omega$ *such that for all* $\pi \in \Pi$, $g(n) \notin \pi(g \restriction n)$ *holds for almost all* n

(vi) *any of* (ii) *through* (v) *with the additional stipulation that* g *be injective*.

Note. (i) to (iii) is the well-known Bartoszyński–Miller characterization of non($\mathcal{M}$) (see [BJ, 2.4.8]). That (iv) is equivalent to any of the preceding statements has been observed by Kada [K] and Scheepers [S]. See also [B, Sect. 10] for closely related results.

Partial proof. Since clearly (v) ⇒ (iv) ⇒ (ii) and since (vi) is a strengthening of the preceding ones, it suffices to prove (iii) ⇒ (v) with the additional stipulation that g be injective.

Let h and Π be given. Define $h'\colon \omega^{<\omega} \to \omega$ by $h'(s) = \max\{h(s), |s|\}$ where $|s|$ denotes the length (i.e., the domain) of the finite sequence s. Define an h'-slalom predictor ψ by $\psi(s) = \operatorname{ran}(s)$. Let $\Pi' = \Pi \cup \{\psi\}$. Identify $\omega^{<\omega}$ and ω. By (iii) there is a predictor $\rho\colon \omega^{<\omega} \to \omega$ such that for all $\pi \in \Pi'$, $\rho(s) \notin \pi(s)$ holds for almost all s. Since this is true for $\pi = \psi$, choosing $g(0)$ large enough and then defining recursively $g(n) = \rho(g \restriction n)$ for $n > 0$ will give us an injective g. It is clear that for all $\pi \in \Pi$, $g(n) = \rho(g \restriction n) \notin \pi(g \restriction n)$ for almost all n, as required. ∎

THEOREM 2.2. $\mathfrak{a}_{\mathfrak{p}} \geq \operatorname{non}(\mathscr{M})$. *In fact there are functions* $F_0\colon \operatorname{Sym}(\omega) \to \omega^{\omega}$, $F_1\colon \omega^{\omega} \to \operatorname{Sym}(\omega)$ *such that whenever* $A \subseteq \operatorname{Sym}(\omega)$, $f \in \omega^{\omega}$ *is injective with* $f(2n) \geq n$ *and* $f(2n+1) \geq n+1$ *for all n and eventually different from all members of* $F_0(A)$, *then* $F_1(f)$ *is eventually different from all members of* A.

Proof. We first argue that the second statement implies the first. Let $A \subseteq \operatorname{Sym}(\omega)$ be almost disjoint with $|A| < \operatorname{non}(\mathscr{M})$. Using the "injective version" of (iii) in Theorem 2.1, find an injective $f \in \omega^{\omega}$ which is eventually different from all members of $F_0(A)$ and satisfies $f(n) \geq n$ for almost all n. By changing f on finitely many values we may assume $f(n) \geq n$ for all n. Then $F_1(f)$ witnesses A is not maximal.

To prove the second statement, define F_0 by $F_0(x)(2n) = x(n)$ and $F_0(x)(2n+1) = x^{-1}(n)$ for all n (where $x \in \operatorname{Sym}(\omega)$). For injective $f \in \omega^{\omega}$ with $f(2n) \geq n$ and $f(2n+1) \geq n+1$ for all n define $F_1(f)$ recursively as follows: let $n \in \omega$ and assume $F_1(f)(k)$ and $F_1(f)^{-1}(k)$ have been defined for $k < n$. If $F_1(f)^{-1}(k) = n$ for some $k < n$, then clearly $F_1(f)(n) = k$. If not, then let $F_1(f)(n) = f(2n)$. If $F_1(f)(k) = n$ for some $k \leq n$, then clearly $F_1(f)^{-1}(n) = k$. If not, then let $F_1(f)^{-1}(n) = f(2n+1)$. It is easy to see that $F_1(f) \in \operatorname{Sym}(\omega)$. For other $f \in \omega^{\omega}$, let $F_1(f) = \mathrm{id}$.

Now let $x \in A$. Find n_0 such that $F_0(x)(n) \neq f(n)$ for all $n \geq 2n_0$. Then for all n with n, $F_1(f)(n) \geq n_0$, either

- $F_1(f)(n) = f(2n) \neq F_0(x)(2n) = x(n)$, or
- $F_1(f)(n) = k$ for some $k < n$ with $F_1(f)^{-1}(k) = n$. But since $k \geq n_0$ we must have $n = F_1(f)^{-1}(k) = f(2k+1) \neq F_0(x)(2k+1) = x^{-1}(k)$; that is, $x(n) \neq k = F_1(f)(n)$.

We are done in both cases. ∎

COROLLARY 2.3. *It is consistent that* $\mathfrak{a}_{\mathfrak{p}} > \max\{\mathfrak{a}, \mathfrak{d}\}$, *where* $\mathfrak{a}$ *is, as usual, the minimal size of an infinite maximal almost disjoint (mad) family in* $\wp(\omega)$ *(see, e.g.,* [vD]).

Proof. Add κ random reals to a model of CH where $\kappa \geq \aleph_2$. It is well known that $\operatorname{non}(\mathscr{M}) = \kappa$, and therefore $\mathfrak{a}_{\mathfrak{p}} = \kappa$ by the previous theorem, that $\mathfrak{d} = \aleph_1$, and that $\mathfrak{a} = \aleph_1$ in the resulting model. (See, e.g., [BJ, 7.6.8] for non($\mathscr{M}$) and $\mathfrak{d}$. A proof of $\mathfrak{a} = \aleph_1$, an adaption of Kunen's proof for the Cohen real model, can be found in [B, Sect. 11.4].) ∎

Note. The consistency of $\mathfrak{a}_{\mathfrak{p}} > \mathfrak{a}$ is already known. It was proved by Zhang [Z2, Theorem 3.6] by a finite support iteration of ccc p.o.'s. In his model one also has $\mathrm{cov}(\mathscr{N}) < \mathfrak{a}_{\mathfrak{p}}$ [Z1, Theorem 3.12]. Also note that we get, e.g., the consistency of $\mathfrak{a}_{\mathfrak{p}} > \max\{\mathfrak{d}, \mathrm{cov}(\mathscr{N})\}$ as a consequence of the well-known CON ($\mathrm{non}(\mathscr{M}) > \max\{\mathfrak{d}, \mathrm{cov}(\mathscr{N})\}$) (see [BJ, 7.6.6]).

THEOREM 2.4. $\mathfrak{a}_{\mathfrak{g}} \geq \mathrm{non}(\mathscr{M})$.

Proof. We shall again use the function F_1 defined in the previous proof—however, we will need it also for injective partial functions $s \in \omega^{<\omega}$ with $s(2n) \geq n$ for $2n < |s|$ and $s(2n+1) \geq n+1$ for $2n+1 < |s|$. Denote the set of such functions by S. $F_1(s)$ is defined by recursion as before. Clearly $F_1(s)$ is an injective finite partial function (not necessarily in $\omega^{<\omega}$). If H is any cofinitary group, a *word* $w(x)$ in variable x from H is an expression of the form

$$g_0 \cdot x^{m_0} \cdot g_1 \cdot \dots \cdot g_{l-1} \cdot x^{m_{l-1}} \cdot g_l$$

such that $g_i \in H$, $g_i \neq \mathrm{id}$ for $1 \leq i \leq l-1$, and $m_i \in \mathbb{Z} \setminus \{0\}$ for all i. The *length* of such a $w(x)$ is $\mathrm{lg}(w(x)) = |\{i \leq l; g_i \neq \mathrm{id}\}| + \Sigma_{i<l}|m_i|$. For a word $w(x)$, an injective finite partial function t (not necessarily in $\omega^{<\omega}$), we form the (possibly empty) injective finite partial function $w(t)$ in the usual manner. Also, if $g \in \mathrm{Sym}(\omega)$, we define $w(g) \in \mathrm{Sym}(\omega)$ as usual. Given a word $w(x)$, define a predictor $\pi_{w(x)}$ as follows. Assume $s \in S$ with $|s| = 2n + e$ where $e \in \{0, 1\}$. Put $\pi_{w(x)}(s) = w(F_1(s))(n)$ if $n \in \mathrm{dom}(w(F_1(s)))$. If $n \notin \mathrm{dom}(w(F_1(s)))$, the value of $\pi_{w(x)}(s)$ is irrelevant.

Now let H be a cofinitary group of size $< \mathrm{non}(\mathscr{M})$. We have to show that H is not maximal. By the "injective version" of (v) in Theorem 2.1, there is $f \in \omega^\omega$ injective with $f(2n) \geq n$, $f(2n+1) \geq n+1$ for all n and such that for all $\pi_{w(x)}$ with $w(x)$ being a word from H, $\pi_{w(x)}(f \restriction n) \neq f(n)$ holds for almost all n. Let $F_1(f)$ be as before. We claim that $G = \langle H, F_1(f)\rangle = H * \langle F_1(f)\rangle$ is a cofinitary group. Since all elements of G are of the form $w(F_1(f))$ where $w(x)$ is a word from H, it suffices to show that for all such words $w(x) \neq \mathrm{id}$ (that is, for all words of length at least one), $w(F_1(f))(n) \neq n$ holds for almost all n. This is done by induction on $\mathrm{lg}(w(x))$.

Basic step. $\mathrm{lg}(w(x)) = 1$. Then either $w(x) = g_0$ for $g_0 \in H \setminus \{\mathrm{id}\}$ in which case there is nothing to prove, or $w(x) = x$ or $w(x) = x^{-1}$. Since $\pi_1(f \restriction n) \neq f(n)$ for almost all n (where π_1 is the predictor associated with the word representing the identity), $F_1(f)(n) \neq n$ for almost all n as well.

Induction step. Assume $w(x) = g_0 \cdot x^{m_0} \cdot g_1 \cdot \cdots \cdot g_{l-1} \cdot x^{m_{l-1}} \cdot g_l$ is a word of length at least two and the claim has been proved for all shorter words. For $k < \sum_{i<l} |m_i|$ we define the *chopped word* $w_k(x)$ and the *inverse chopped word* $w_k^{-1}(x)$ basically by removing the kth occurrence of x, as follows. First let $j < l$ be such that $\sum_{i<j}|m_i| \le k < \sum_{i<j+1} |m_i|$ and assume $k = \sum_{i<j} |m_i| + k'$ with $0 \le k' < |m_j|$. Then $w_k(x)$ is the reduced word obtained from the word

$$x^{\operatorname{sgn}(m_j)(|m_j|-k'-1)} \cdot g_{j+1} \cdot x^{m_{j+1}} \cdot \cdots \cdot x^{m_{l-1}} \cdot g_l \cdot g_0 \cdot x^{m_0} \cdot \cdots \cdot g_j \cdot x^{\operatorname{sgn}(m_j)\cdot k'},$$

and $w_k^{-1}(x)$ is simply its inverse, i.e., the reduced word associated with

$$x^{-\operatorname{sgn}(m_j)\cdot k'} \cdot g_j^{-1} \cdot \cdots \cdot x^{-m_0} \cdot g_0^{-1} \cdot g_l^{-1} \cdot x^{-m_{l-1}} \cdot \cdots \cdot x^{-m_{j+1}} \cdot g_{j+1}^{-1} \cdot x^{-\operatorname{sgn}(m_j)(|m_j|-k'-1)}.$$

Now let n^* be so large that for all $n \ge n^*$ the following hold:

(i) the values

$$n, \left(F_1(f)^{\operatorname{sgn}(m_{l-1})} \cdot g_l\right)(n),$$
$$\left(F_1(f)^{\operatorname{sgn}(m_{l-1})\cdot 2} \cdot g_l\right)(n), \ldots, \left(F_1(f)^{m_{l-1}} \cdot g_l\right)(n), \ldots,$$
$$\left(F_1(f)^{m_0-\operatorname{sgn}(m_0)} \cdot g_1 \cdot \cdots \cdot g_{l-1} \cdot F_1(f)^{m_{l-1}} \cdot g_l\right)(n),$$

and—in case $g_l \neq \mathrm{id}$—also $g_l(n)$, and—in case $g_0 \neq \mathrm{id}$—also

$$\left(F_1(f)^{m_0} \cdot g_1 \cdot \cdots \cdot g_{l-1} \cdot F_1(f)^{m_{l-1}} \cdot g_l\right)(n),$$

are all distinct, as well as

(ii) for each $k < \sum_{i<l} |m_i|$ with $k = \sum_{i<j} |m_i| + k'$, if

$$n' = \left(F_1(f)^{-\operatorname{sgn}(m_j)\cdot k'} \cdot g_j^{-1} \cdot \cdots \cdot F_1(f)^{-m_0} \cdot g_0^{-1}\right)(n),$$

then $f(2n') \neq \pi_{w_k(x)}(f \restriction 2n')$ and $f(2n'+1) \neq \pi_{w_k(x)}(f \restriction (2n'+1))$, and also if

$$n' = \left(F_1(f)^{\operatorname{sgn}(m_j)(|m_j|-k'-1)} \cdot g_{j+1} \cdot \cdots \cdot F_1(f)^{m_{l-1}} \cdot g_l\right)(n),$$

then $f(2n') \neq \pi_{w_k^{-1}(x)}(f \restriction 2n')$ and $f(2n'+1) \neq \pi_{w_k^{-1}(x)}(f \restriction (2n'+1))$. By induction hypothesis, and since there are only finitely many k and for each k only finitely many n' for which (ii) can fail, it is clear that there is such an n^*. We claim that $w(F_1(f))(n) \neq n$ for each $n \ge n^*$.

Assume this were not the case and fix $n \geq n^*$ with $w(F_1(f))(n) = n$. For each $k < \Sigma_{i<l} |m_i|$ with $k = \Sigma_{i<j} |m_i| + k'$, let

$$n_k = \min\Big\{ \big(F_1(f)^{\operatorname{sgn}(m_j)(|m_j| - k' - 1)} \cdot \dots \cdot F_1(f)^{m_{l-1}} \cdot g_l \big)(n), \big(F_1(f)^{\operatorname{sgn}(m_j)(|m_j| - k')} \cdot \dots \cdot F_1(f)^{m_{l-1}} \cdot g_l \big)(n) \Big\}.$$

Now note that by (i), there can be at most two values k_0 and k_1 for k such that n_k is maximal; and if there are two they must be adjacent; i.e., $k_1 = k_0 + 1$ without loss. Let $j < l$ be such that this (these) maximal value(s) n_k occurs(s) at $k = \Sigma_{i<j} |m_i| + k'$ for some k'. We need to consider four cases.

Case 1. $m_j > 0$, and either there are $k_1 = k_0 + 1$ such that $n_{k_0} = n_{k_1}$ is maximal in which case we let $k = k_1$, or there is a unique k such that n_k is maximal and one has $n_k = (F_1(f)^{\operatorname{sgn}(m_j)(|m_j| - k')} \cdot \dots \cdot F_1(f)^{m_{l-1}} \cdot g_l)(n)$. Note that in the former case n_k must necessarily have the value $(F_1(f)^{\operatorname{sgn}(m_j)(|m_j| - k')} \cdot \dots \cdot F_1(f)^{m_{l-1}} \cdot g_l)(n)$. Also note that since we assume $w(F_1(f))(n) = n$ we additionally have $n_k = (F_1(f)^{-\operatorname{sgn}(m_j) \cdot k'} \cdot \dots \cdot F_1(f)^{-m_0} \cdot g_0^{-1})(n)$. Now,

$$\pi_{w_k(x)}(f \upharpoonright (2n_k + 1)) = w_k(F_1(f \upharpoonright (2n_k + 1)))(n_k)$$

because the right-hand side is indeed defined by maximality of n_k. By definition of n_k as a minimum, we must also have

$$f(2n_k + 1) = F_1(f)^{-1}(n_k).$$

And $w(F_1(f))(n) = n$ clearly entails

$$w_k(F_1(f \upharpoonright (2n_k + 1)))(n_k) = F_1(f)^{-1}(n_k).$$

However, by (ii), we get

$$\pi_{w_k(x)}(f \upharpoonright (2n_k + 1)) \neq f(2n_k + 1),$$

a contradiction.

Case 2. $m_j < 0$, and either there are $k_1 = k_0 + 1$ such that $n_{k_0} = n_{k_1}$ is maximal in which case we let $k = k_0$, or there is a unique k such that n_k is maximal and one has $n_k = (F_1(f)^{\operatorname{sgn}(m_j)(|m_j| - k' - 1)} \cdot \dots \cdot F_1(f)^{m_{l-1}} \cdot g_l)(n)$. In this case use $\pi_{w_k^{-1}(x)}(f \upharpoonright (2n_k + 1))$ to derive a contradiction.

Case 3. $m_j > 0$ and there is a unique k such that n_k is maximal and one has $n_k = (F_1(f)^{\operatorname{sgn}(m_j)(|m_j| - k' - 1)} \cdot \dots \cdot F_1(f)^{m_{l-1}} \cdot g_l)(n)$. Use $\pi_{\omega_k^{-1}(x)}(f \upharpoonright 2n_k)$.

Case 4. $m_j < 0$ and there is a unique k such that n_k is maximal and one has $n_k = (F_1(f)^{\mathrm{sgn}(m_j)(|m_j|-k')} \cdot \cdots \cdot F_1(f)^{m_{l-1}} \cdot g_l)(n)$. Use $\pi_{w_k(x)}(f \upharpoonright 2n_k)$.

These contradictions complete the proof of the Theorem. ∎

Using again the random real model, we deduce the following result which was proved by different methods by Hrusak et al. [HSZ].

COROLLARY 2.5. *It is consistent that* $\mathfrak{a}_{\mathfrak{g}} > \max\{\mathfrak{a}, \mathfrak{d}\}$.

From the well-known fact that Martin's axiom MA implies every non-meager set of reals has size $\mathfrak{c}$ we also infer

COROLLARY 2.6 [Z, Theorem 1.4]. MA *implies* $\mathfrak{a}_{\mathfrak{g}} = \mathfrak{c}$.

3. THE SPECTRUM OF CARDINALITIES OF MAXIMAL COFINITARY GROUPS

Let Spec(mcg), the *spectrum of cardinalities of maximal cofinitary groups*, denote the set of cardinals λ such that there is a maximal cofinitary group of size λ. So $\mathfrak{a}_{\mathfrak{g}}, \mathfrak{c} \in$ Spec(mcg), and Spec(mcg) is a subset of the interval $[\mathfrak{a}_{\mathfrak{g}}, \mathfrak{c}]$ of cardinals. What else can be said about it? In particular, the third author addressed the following question [Z, Question 4.3]:

Question 3.1. Is it consistent that there exists a maximal cofinitary group G such that $\mathfrak{a}_{\mathfrak{g}} < |G| < \mathfrak{c}$?

It turns out the answer is positive. In fact, by modifying the analogous argument for mad families due to Blass [B1, Theorem 9], one can show

THEOREM 3.2. *Let V be a model of ZFC and the generalized continuum hypothesis* (GCH). *In V, let C be a closed set of uncountable cardinals with $\aleph_1 \in C$, $\kappa \in C$ for $\aleph_1 \leq \kappa \leq |C|$, and $\lambda^+ \in C$ for $\lambda \in C$ with $cf(\lambda) = \omega$. Then there is a ccc p.o. $\mathbb{P}$ forcing $\mathfrak{c} = \max(C)$ and* Spec(mcg) $= C$. (*This means that the statements $\mathfrak{c} = \max(C)$ and* Spec(mcg) $= C$ *hold in the $\mathbb{P}$-generic extension $V[F]$ which is also a model of ZFC*.)

Proof. As mentioned already, the proof follows closely the one of [B1, Theorem 9]. However, since a maximal cofinitary group is combinatorially more complicated than a mad family, the definition of the p.o. $\mathbb{P}$ is more involved. Therefore, we provide its definition, sketch briefly its main properties, and refer to Blass' work for whatever can be taken over from his proof.

Fix $\kappa \in C$. For $A \subseteq \kappa$, an *(abstract) word w over A* is an expression of the form

$$x_{\alpha_0}^{n_0} \cdot \cdots \cdot x_{\alpha_k}^{n_k}$$

such that $\alpha_l \in A$, $\alpha_{l+1} \neq \alpha_l$, and $n_l \in \mathbb{Z} \setminus \{0\}$. A *subword* of w is any expression of the form

$$x_{\alpha_l}^{n'_l} \cdot x_{\alpha_{l+1}}^{n_{l+1}} \cdot \cdots \cdot x_{\alpha_{m-1}}^{n_{m-1}} \cdot x_{\alpha_m}^{n'_m},$$

where $0 \leq l \leq m \leq k$, $\operatorname{sgn}(n'_l) = \operatorname{sgn}(n_l)$, $\operatorname{sgn}(n'_m) = \operatorname{sgn}(n_m)$, $|n'_l| \leq |n_l|$, and $|n'_m| \leq |n_m|$. χ is a *good function over* A if: $\operatorname{dom}(\chi)$ is a finite set of words over A which is closed under subwords, $\operatorname{ran}(\chi) \subseteq \omega$, and if v is a subword of $w \in \operatorname{dom}(\chi)$, then $\chi(v) \leq \chi(w)$.

The partial order $\mathbb{P}_\kappa$ consists of all pairs (p, χ) such that

(i) p is a finite partial function with $\operatorname{dom}(p) \subseteq \kappa$

(ii) for any $\alpha \in \operatorname{dom}(p)$, $p(\alpha)$ is a finite injective partial function from ω to ω

(iii) χ is a good function over $\operatorname{dom}(p)$

(iv) for all $w \in \operatorname{dom}(\chi)$ and all $i \geq \chi(w)$, if the computation $w_p(i)$ converges, and if all intermediate values of the computation are $\geq \chi(w)$, then $w_p(i) \neq i$.

Here, for $w = x_{\alpha_0}^{n_0} \cdot \cdots \cdot x_{\alpha_k}^{n_k}$, we say *the computation* $w_p(i)$ *converges* (*to* j) and write $w_p(i)\downarrow j$ if

$$\left(p(\alpha_0)^{n_0} \cdot \cdots \cdot p(\alpha_k)^{n_k}\right)(i)$$

is defined (and equals j). Otherwise we say the computation *diverges* and write $w_p(i)\uparrow$. Any number of the form

$$\left(p(\alpha_l)^{n'_l} \cdot \cdots \cdot p(\alpha_k)^{n_k}\right)(i),$$

where $0 \leq l \leq k$, $\operatorname{sgn}(n'_l) = \operatorname{sgn}(n_l)$, and $|n'_l| \leq |n_l|$ is an *intermediate value*. The p.o. on $\mathbb{P}_\kappa$ is given by extension; i.e., $(p', \chi') \leq (p, \chi)$ iff $\operatorname{dom}(p') \supseteq \operatorname{dom}(p)$, $p'(\alpha) \supseteq p(\alpha)$ for all $\alpha \in \operatorname{dom}(p)$, and $\chi' \supseteq \chi$.

Let F be a $\mathbb{P}_\kappa$-generic filter over V. For $\alpha < \kappa$, let $g_{\kappa,\alpha} = \{\langle i, j\rangle; \exists (p, \chi) \in F(p(\alpha)(i) = j)\}$.

LEMMA 3.3. *Each $g_{\kappa,\alpha}$ is a surjective total function—and so $g_{\kappa,\alpha} \in \operatorname{Sym}(\omega)$.*

Proof. Fix α. It suffices to show that for each $j \in \omega$, the set $D_{\alpha,j} = \{(p, \chi) \in \mathbb{P}_\kappa;\ \alpha \in \operatorname{dom}(p) \text{ and } j \in \operatorname{dom}(p(\alpha)) \cap \operatorname{ran}(p(\alpha))\}$ is dense in $\mathbb{P}_\kappa$. To see this, fix $(p_0, \chi_0) \in \mathbb{P}_\kappa$. Without loss $\alpha \in \operatorname{dom}(p_0)$. Suppose $p_0(\alpha)(i) \neq j$ for all $i \in \operatorname{dom}(p_0(\alpha))$. Choose $i \notin \cup\{\operatorname{dom}(p_0(\beta)) \cup \operatorname{ran}(p_0(\beta));\ \beta \in \operatorname{dom}(p_0)\}$ and let $p_1(\alpha) = p_0(\alpha) \cup \{\langle i, j\rangle\}$, $p_1(\beta) = p_0(\beta)$ for $\beta \in \operatorname{dom}(p_0) \setminus \{\alpha\}$. Now choose $w \in \operatorname{dom}(\chi_0)$ and assume

$w_{p_0}(i')\uparrow$, $w_{p_1}(i')\downarrow i'$ for some i'. Then i and j must be intermediate values of the computation, but by its choice, i can only appear right at the beginning or at the end. So $i = i'$, and $w = x_\alpha^{n_0} \cdot x_{\alpha_1}^{n_1} \cdot \cdots \cdot x_{\alpha_{k-1}}^{n_{k-1}} \cdot x_\alpha^{n_k}$ with $n_k > 0$ and $n_0 < 0$. Hence $v_{p_0}(j)\downarrow j$ where $v = x_\alpha^{n_0+1} \cdot x_{\alpha_1}^{n_1} \cdot \cdots \cdot x_{\alpha_{k-1}}^{n_{k-1}} \cdot x_\alpha^{n_k - 1}$. Thus some intermediate value of the computation is $< \chi(v) \leq \chi(w)$. So (p_1, χ_0) is indeed a condition extending (p_0, χ_0) and $j \in \operatorname{ran}(p_1(\alpha))$.

Applying this argument once again, we easily extend $p_1(\alpha)$ to $p(\alpha)$ with $j \in \operatorname{dom}(p(\alpha))$ so that $(p, \chi_0) \leq (p_1, \chi_0)$ and $(p, \chi_0) \in D_{\alpha, j}$, as required. ∎

Put $G_\kappa = \langle g_{\kappa,\alpha};\ \alpha < \kappa \rangle$.

Lemma 3.4. *G_κ is a cofinitary group.*

Proof. By clause (iv) in the definition of $\mathbb{P}_\kappa$, it suffices to show that for each finite $A \subseteq \kappa$ and each abstract word w over A, $E_{A,w} = \{(p, \chi) \in \mathbb{P}_\kappa;\ A \subseteq \operatorname{dom}(p) \text{ and } w \in \operatorname{dom}(\chi)\}$ is dense. This, however, is simple: given $(p_0, \chi_0) \in \mathbb{P}_\kappa$ such that—without loss—$A \subseteq \operatorname{dom}(p_0)$, let $\operatorname{dom}(\chi) = \operatorname{dom}(\chi_0) \cup \{v; v \text{ is a subword of } w\}$ and put $\chi \restriction \operatorname{dom}(\chi_0) = \chi_0$, and $\chi(v) = \max\{\max(\operatorname{dom}(p_0(\alpha)) \cup \operatorname{ran}(p_0(\alpha))) + 1;\ \alpha \in \operatorname{dom}(p_0)\}$ for $v \in \operatorname{dom}(\chi) \setminus \operatorname{dom}(\chi_0)$. Then $(p_0, \chi) \in E_{A,w}$. ∎

Note that this also shows G_κ is a free subgroup of $\operatorname{Sym}(\omega)$ of rank κ. Now, let $\mathbb{P}$ be the finite support product of the $\mathbb{P}_\kappa$ for $\kappa \in C$. A standard Δ-system argument (compare [B1, Lemma 11]) shows:

Lemma 3.5. *$\mathbb{P}$ is ccc.*

Next, let F be $\mathbb{P}$-generic over V. In $V[F]$, we have:

Lemma 3.6. *For each $\kappa \in C$, G_κ is a maximal cofinitary group.*

Proof. Basically, this is like the argument for mad families [B1, Lemma 12] which goes back to Hechler. However, there are some tricky points, and we therefore provide the proof.

Fix $\kappa \in C$. Assume we had $\bar{p}_0 \in \mathbb{P}$ and a $\mathbb{P}$-name $\dot{g}$ for a permutation such that $\bar{p}_0 \Vdash$ "$\langle \dot{g}, \dot{G}_\kappa \rangle$ is cofinitary and $\dot{g} \notin \dot{G}_\kappa$." Given a condition $\bar{p} \in \mathbb{P}$, denote by $(p^{\bar{p}}, \chi^{\bar{p}}) \in \mathbb{P}_\kappa$ its κth coordinate. Let $I \subseteq \kappa$ be countable such that for each $i \in \omega$ there is a maximal antichain of conditions $\bar{p} \in \mathbb{P}$ deciding $\dot{g}(i)$ with $\operatorname{dom}(p^{\bar{p}}) \subseteq I$. Fix $\alpha \in \kappa \setminus I$. Find i_0 and $\bar{q}_0 \leq \bar{p}_0$ such that

$$\bar{q}_0 \Vdash \text{“}\dot{g}(i) \neq \dot{g}_{\kappa,\alpha}(i) \qquad \text{for all } i \geq i_0.\text{”} \tag{$\bigstar$}$$

Without loss $\operatorname{dom}(p^{\bar{q}_0}(\alpha)) \cup \operatorname{ran}(p^{\bar{q}_0}(\alpha)) \subseteq i_0$.

Next choose $i_2 \geq i_1 \geq i_0$ and $\bar{r}_0 \leq \bar{q}_0$ such that for all words $w \in \mathrm{dom}(\chi^{\bar{q}_0})$, either

$$\bar{r}_0 \Vdash \text{“}\dot{w}^{\alpha, \dot{g}} = \mathrm{id}\text{”} \tag{1}$$

or

$$\begin{aligned} \bar{r}_0 \Vdash \text{“}\dot{w}^{\alpha,\dot{g}}(i) \neq i \qquad &\text{for all } i \geq i_1, \dot{w}^{\alpha,\dot{g}}(i) \geq i_1, \\ \text{and} \qquad (\dot{w}^{\alpha,\dot{g}})^{-1}(i) \geq i_1 \qquad &\text{for all } i \geq i_2.\text{”} \end{aligned} \tag{2}$$

Here, for any $w \in \mathrm{dom}(\chi^{\bar{q}_0})$, $\dot{w}^{\alpha,\dot{g}}$ is the name (for an element of $\mathrm{Sym}(\omega)$) which is obtained by replacing each occurrence of x_α in w by $\dot{g}$ and each occurrence of x_β, $\beta \neq \alpha$, by $\dot{g}_{\kappa,\beta}$. It is clear that this can be done by our assumptions, and that for each $w \in \mathrm{dom}(\chi^{\bar{q}_0})$ which contains at most one occurrence of x_α, alternative (2) must hold. Fix any $i \geq i_2$ and $\bar{p}_1 \in \mathbb{P}$ with $\mathrm{dom}(p^{\bar{p}_1}) \subseteq I$ such that $\bar{p}_1$ decides $\dot{g}(i)$, say $\bar{p}_1 \Vdash$ “$\dot{g}(i) = j$,” and $\bar{p}_1$ is compatible with $\bar{r}_0$. Now define $\bar{q}_1$ as follows. On coordinates outside κ, $\bar{q}_1$ is any common extension of $\bar{r}_0$ and $\bar{p}_1$. Next, $\mathrm{dom}(p^{\bar{q}_1}) = \mathrm{dom}(p^{\bar{q}_0}) \cup \mathrm{dom}(p^{\bar{p}_1})$, $\chi^{\bar{q}_1} = \chi^{\bar{q}_0} \cup \chi^{\bar{p}_1}$, $p^{\bar{q}_1}(\beta) = p^{\bar{q}_0}(\beta) \cup p^{\bar{p}_1}(\beta)$ for $\beta \in \mathrm{dom}(p^{\bar{q}_1}) \setminus \{\alpha\}$ (this makes sense because $\bar{q}_0$ and $\bar{p}_1$ are compatible), and $p^{\bar{q}_1}(\alpha) = p^{\bar{q}_0}(\alpha) \cup \{\langle i, j\rangle\}$.

We need to check that $\bar{q}_1$ is a condition. There is no problem on coordinates outside κ, and the only thing we have to verify is clause (iv) in coordinate κ. This clearly holds for $w \in \mathrm{dom}(\chi^{\bar{p}_1})$ (since such words do not involve x_α), so assume $w \in \mathrm{dom}(\chi^{\bar{q}_0})$ is a counterexample to (iv) of minimal length. Thus $w_{p^{\bar{p}_1}}(i') \downarrow i'$ for some i' (with all intermediate values of the computation $\geq \chi^{\bar{q}_0}(\omega)$). Clearly x_α occurs in w and the computation must involve i and j as intermediate values. Since $\bar{p}_1$ and $\bar{r}_0$ are compatible, and by (1) and (2), all intermediate values, and, in particular, i', must be $\geq i_1$. This means that if x_α occurs more than once in w, then i and j occur at least twice as intermediate values, a contradiction to the minimality of w. Hence x_α occurs (exactly) once in w. As remarked above, this means case (2) holds for $\dot{w}^{\alpha,\dot{g}}$. So $\bar{r}_0 \Vdash$ “$\dot{w}^{\alpha,\dot{g}}(i') \neq i'$.” Since $\bar{p}_1$ and $\bar{r}_0$ are compatible, this contradicts $w_{p^{\bar{p}_1}}(i') \downarrow i'$, and the argument is complete.

Now we clearly have $\bar{q}_1 \leq \bar{p}_1$, so $\bar{q}_1 \Vdash$ “$\dot{g}(i) = j = \dot{g}_{\kappa,\alpha}(i)$.” Since $\bar{q}_1 \leq \bar{q}_0$, this contradicts (★) and concludes the proof of maximality. ∎

The argument that for $\kappa \notin C$, there is no maximal cofinitary group of size κ (and, in fact, κ, is not an $OD\mathbb{R}$-characteristic) can be taken over verbatim from Blass' work (see [B1, pp. 75–77]), for that proof uses only very general homogeneity properties of the p.o. involved (which are shared by our $\mathbb{P}$). ∎

4. FURTHER REMARKS AND PROBLEMS

As promised, we include the original argument for $\mathfrak{b} \leq \mathfrak{a}_{\mathfrak{g}}$ (Theorem 1.9) due to Spinas and Zhang.

Let $G \leq \mathrm{Sym}(\omega)$ be a cofinitary group of size less than $\mathfrak{b}$. We have to show that G is not maximal. Choose $d \in \omega^{\omega}$ strictly increasing and dominating the members of G. Without loss, we may assume $d(0) > 0$, and for any finite subset F of G there is k such that for all $i \geq k$, $\mathrm{ran}(d)$ has at most one value in common with $\{j; \min\{g(i); g \in F\} \leq j \leq \max\{g(i); g \in F\}\}$, and $d(i)$ is larger than $g_0(j)$ for any $g_0 \in F$ and any $j \leq \max\{g(i); g \in F\}$. It is easy to see there is such a d.

We define a permutation f of ω by induction as follows:

$$f(0) = d(0), \qquad f\big(d^2(0)\big) = 0.$$

In general, assume that $f(i)$ as well as $f^{-1}(i)$ have been defined for $i < n$.

Case 1. $n = f(i)$ for some $i < n$ (so $f^{-1}(n)$ is already defined). Let

$$f(n) = d\big(\max\{f(j); j < n\} \cup \{f^{-1}(j); j < n\}\big).$$

Case 2. $n = f^{-1}(i)$ for some $i < n$ (so $f(n)$ is already defined). Let

$$f^{-1}(n) = d\big(\max\{f(j); j < n\} \cup \{f^{-1}(j); j < n\}\big).$$

Case 3. $n \notin \{f(i), f^{-1}(i); i < n\}$. Define

$$f(n) = d\big(\max\{f(j); j < n\} \cup \{f^{-1}(j); j < n\}\big),$$
$$f^{-1}(n) = d\big(\max\{f(j); j \leq n\} \cup \{f^{-1}(j); j < n\}\big).$$

It is easy to see that f is a permutation. Let $O(f, i) = \{f^m(i); m \in \mathbb{Z}\}$ denote the *f-orbit* of i. Note that every orbit of f is infinite and that there are infinitely many f-orbits. Hence f has no fixed points. Let $\langle G, f\rangle$ be the group generated by G and f. We have to show that $\langle G, f\rangle$ is cofinitary. An arbitrary member of $\langle G, f\rangle$ looks like

$$w = g_n \cdot f^{m_{n-1}} \cdot \cdots \cdot f^{m_0} \cdot g_0, \qquad (*)$$

where $g_j \in G$, $m_j \in \mathbb{Z} \setminus \{0\}$ and $g_j \neq \mathrm{id}$ for $0 < j < n$. The following lemma on orbits is much stronger than what we need to complete the proof of Theorem 1.9.

MAIN LEMMA 4.1. *For every w as in $(*)$ with the property that at least one g_j is not* id, *there exists $k^* < \omega$ such that for every $i \geq k^*$ we have $w(i) \notin O(f,i)$.*

We first prove several auxiliary lemmata.

SUBLEMMA 4.2. *Given $g_0, g_1 \in G$ there is $k = k_0(g_0, g_1)$ such that for all $i \geq k$ and all $m \in \mathbb{Z} \setminus \{0\}$, if $f^m(i) \geq \min\{i, g_0(i)\}$ then $f^m(i) > \max\{i, g_0(i)\}$ and $g_1(f^m(i)) > \max\{i, g_0(i)\}$.*

Proof. Let k be so large that for all $i \geq k$, $d(\min\{i, g_0(i)\}) > \max\{i, g_0(i)\}$ as well as $d(i) > g_1^{-1}(j)$ for all $j \leq \max\{i, g_0(i)\}$.

First note that by definition of f, one always has $f^m(i) \geq d(i)$ in case $f^m(i) > i$. (This is trivial if i is the minimum of an f-orbit. If not, there is $j < i$ such that $f(j) = i$ or $f^{-1}(j) = i$. By definition of f, $f^{\operatorname{sgn}(m)(|m|-1)}(i) \geq j$ and, again by definition of f, $f^m(i) \geq d(f(j)) = d(i)$.)

So if $f^m(i) > i$, $f^m(i) > g_0(i)$ follows. Therefore assume $f^m(i) < i$. Put $j := f^m(i)$. Then $f^{-m}(j) > j \geq g_0(i)$. Thus $i = f^{-m}(j) \geq d(j) \geq d(g_0(i)) > i$, a contradiction. Next assume $j := g_1(f^m(i)) \leq \max\{i, g_0(i)\}$. Then $f^m(i) = g_1^{-1}(j) < d(i) \leq f^m(i)$, again a contradiction. ∎

SUBLEMMA 4.3. *Given $g \in G \setminus \{\mathrm{id}\}$ there is $k = k_1(g)$ such that for all $i \geq k$, i and $g(i)$ belong to different f-orbits.*

Proof. Let k be so large that for all $i \geq k$, $d(\min\{i, g(i)\}) > \max\{i, g(i)\}$ and at most one of the numbers i and $g(i)$ belongs to $\operatorname{ran}(d)$. To see this works, note that then at least one of i and $g(i)$ must be the minimum of an f-orbit and that it can be mapped only to numbers larger than $\max\{i, g(i)\}$ by repeated application of f or f^{-1}. ∎

SUBLEMMA 4.4. *Given $g \in G \setminus \{\mathrm{id}\}$ and $m \in \mathbb{Z}$ there is $k = k_2(g, m)$ such that for all $i \geq k$, if $f^m(i) > i$, then $g(f^m(i))$ is a minimal element of an f-orbit and $g(f^m(i)) > i$.*

Proof. Let k be so large that for all $i \geq k$, $g(d(i)) > i$ and at most one of the numbers i and $g(i)$ belongs to $\operatorname{ran}(d)$. The latter condition easily gives that $g(f^m(i))$ is a minimum of an f-orbit, and since $f^m(i) = d(j)$ for some $j \geq i$, we see $g(f^m(i)) = g(d(j)) > j \geq i$. ∎

SUBLEMMA 4.5. *Given g_0, $g_1 \in G \setminus \{\mathrm{id}\}$ and m^0, $m^1 \in \mathbb{Z}$ there is $k = k_3(g_0, g_1, m^0, m^1)$ such that for all i_0, $i_1 \geq k$, if i_0 and i_1 belong to different f-orbits and $f^{m^j}(i_j) > i_j$ for $j = 0, 1$, then $g_0(f^{m^0}(i_0))$ and $g_1(f^{m^1}(i_1))$ are minimal elements of two distinct f-orbits.*

Proof. Let k be so large that for all $i \geq k$, at most one of the numbers i, $g_0(i)$, $g_1(i)$, and $g_0^{-1}(g_1(i))$ belongs to $\operatorname{ran}(d)$.

Since i_0 and i_1 belong to different f-orbits, so do $f^{m^0}(i_0)$ and $f^{m^1}(i_1)$. As $f^{m^j}(i_j) > i_j$, $f^{m^j}(i_j) \in \operatorname{ran}(d)$ for $j = 0, 1$. Thus neither $g_0(f^{m^0}(i_0))$ nor $g_1(f^{m^1}(i_1))$ belong to ran(d). So they must be minimal elements of f-orbits. Because $f^{m^1}(i_1) \in \operatorname{ran}(d)$, we also see $g_0(f^{m^0}(i_0)) \neq g_1(f^{m^1}(i_1))$ so that they belong to different f-orbits. ∎

Proof of Main Lemma 4.1. Since application of a power of f does not change the f-orbit, we may assume, without loss, that none of g_0, g_n is the identity. For $0 \leq j \leq n$ let

$$v_j = f^{m_{j-1}} \cdot g_{j-1} \cdot \dots \cdot f^{m_0} \cdot g_0$$

and

$$w_j = g_j \cdot v_j = g_j \cdot f^{m_{j-1}} \cdot \dots \cdot f^{m_0} \cdot g_0.$$

So $v_0 = \mathrm{id}$ and $w_n = w$. Choose first

$$\bar{k} = \max\Big\{k_0\big(g_{j_0}^{e_0}, g_{j_1}^{e_1}\big), k_1\big(g_j^e\big), k_2\big(g_j^e, m\big), k_3\big(g_{j_0}^{e_0}, g_{j_1}^{e_1}, m^0, m^1\big);$$
$$j, j_0, j_1 \leq n, e, e_0, e_1 \in \{1, -1\}, |m|, |m^0|, |m^1| \leq \max\big\{|m_j|; j < n\big\}\Big\}$$

and then let k^* be so large that $w_j(i)$, $v_j(i) \geq \bar{k}$ for all $j \leq n$ and all $i \geq k^*$.

Fix $i \geq k^*$. Let j^* be such that either $v_{j^*}(i)$ or $w_{j^*}(i)$ is minimal among the values $\{v_j(i), w_j(i); 0 \leq j \leq n\}$. We first note that by Sublemma 4.2 and the choice of k^*, we must then have that $v_{j^*-1}(i) = g_{j^*-1}^{-1}(w_{j^*-1}(i))$, $w_{j^*-1}(i) = f^{-m_{j^*-1}}(v_{j^*}(i))$, $v_{j^*+1}(i) = f^{m_{j^*}}(w_{j^*}(i))$, and $w_{j^*+1}(i) = g_{j^*+1}(v_{j^*+1}(i))$ are all larger than both $v_{j^*}(i)$ and $w_{j^*}(i)$. Furthermore, by Sublemma 4.3 and the choice of k^*, $v_{j^*}(i)$ and $w_{j^*}(i)$ must belong to different f-orbits.

Put $\bar{j} = \min\{j^*, n - j^*\}$. Let $\hat{j} = n - 2\bar{j}$. Assume without loss $j^* \leq \frac{n}{2}$ (the other case being analogous). So $\bar{j} = j^*$ and $n = j^* + \hat{j} + \bar{j}$. By the choice of k^*, we can apply Sublemma 4.4 repeatedly and see that the pairs $v_{j^*}(i)$ and $w_{j^*+1}(i)$, $v_{j^*}(i)$ and $w_{j^*+2}(i), \dots, v_{j^*}(i)$ and $w_{j^*+\hat{j}}(i)$ belong to different f-orbits.

Finally, by the choice of k^* and by applying Sublemma 4.5 repeatedly, we get that the pairs $v_{j^*-1}(i)$ and $w_{j^*+\hat{j}+1}(i)$, $v_{j^*-2}(i)$ and $w_{j^*+\hat{j}+2}(i), \dots, v_{j^*-\bar{j}}(i) = i$ and $w_{j^*+\hat{j}+\bar{j}}(i) = w(i)$ belong to different f-orbits. So we are done. ∎

We conclude our considerations with some open problems. Let $\mathfrak{a}_{\mathfrak{g}}$ be the least λ such that there exists a maximal family F of size λ of almost disjoint subsets of $\omega \times \omega$, each of which is the graph of a partial function from ω to ω. Following A. Miller and E. van Douwen (see, e.g., [M]), we say that two functions f, $g \in \omega^\omega$ are *eventually different* iff $|f \cap g| < \omega$. We define $\mathfrak{a}_\mathfrak{e}$ as the least λ such that there exists a maximal eventually different family on ω^ω of cardinality λ. It is well known (and easy to see) that

PROPOSITION 4.6. $\operatorname{non}(\mathscr{M}) \leq \mathfrak{a}_\mathfrak{e}, \mathfrak{a}_\mathfrak{s}$.

We now have four cardinals with a very similar definition which sit above $\operatorname{non}(\mathscr{M})$, namely $\mathfrak{a}_\mathfrak{s}$, $\mathfrak{a}_\mathfrak{e}$, $\mathfrak{a}_\mathfrak{p}$, and $\mathfrak{a}_\mathfrak{g}$. No relationship among them is known so far. Can we prove any ZFC-inequality between some of these cardinals? Theorem 2.2 makes $\mathfrak{a}_\mathfrak{e} \leq \mathfrak{a}_\mathfrak{p}$ plausible, but it does not follow from the proof because f needs to be injective for the construction. The only result known additionally is the trivial $\mathfrak{a} \leq \mathfrak{a}_\mathfrak{s}$.

On the other hand, in all known models of ZFC, one seems to have $\operatorname{non}(\mathscr{M}) = \mathfrak{a}_\mathfrak{s} = \mathfrak{a}_\mathfrak{e} = \mathfrak{a}_\mathfrak{p} = \mathfrak{a}_\mathfrak{g}$. Can one prove any consistency result showing that some of these cardinals may not be equal?

REFERENCES

[A] S. A. Adeleke, Embeddings of infinite permutation groups in sharp, highly transitive, and homogeneous groups, *Proc. Edinburgh Math. Soc.* **31** (1981), 169–178.

[B] A. Blass, Combinatorial cardinal characteristics of the continuum, *in* "Handbook of Set Theory" (A. Kanamori, Ed.), Kluwer Academic, Dordrecht/Norwell, MA, in press.

[B1] A. Blass, Simple cardinal characteristics of the continuum, *in* "Set Theory of the Reals" (H. Judah, Ed.), Israel Mathematical Conference Proceedings, Vol. 6, pp. 63–90, Am. Math. Soc., Providence, 1993.

[BJ] T. Bartoszyński and H. Judah, "Set Theory, On the Structure of the Real Line," Peters, Wellesley, MA, 1995.

[C] P. J. Cameron, Cofinitary permutation groups, *Bull. London Math. Soc.* **28** (1996), 113–140.

[vD] E. van Douwen, The integers and topology, *in* "Handbook of Set Theoretic Topology" (K. Kunen and J. Vaughan, Eds.), pp. 111–167, North-Holland, Amsterdam, 1984.

[G] M. Goldstern, unpublished notes, 1997.

[HSZ] M. Hrusak, J. Steprāns, and Y. Zhang, Permutation groups, almost disjoint and dominating families, *J. Symbolic Logic*, to appear.

[K] M. Kada, The Baire category theorem and the evasion number, *Proc. Amer. Math. Soc.* **126** (1998), 3381–3383.

[M] A. Miller, Some interesting problems, *in* "Set Theory of the Reals" (H. Judah, Ed.), Israel Mathematical Conference Proceedings, Vol. 6, pp. 645–654, Am. Math. Soc., Providence, 1993.

[S] M. Scheepers, Meager sets and infinite games, *Contemp. Math.* **192** (1996), 77–89.

[T] J. K. Truss, Embeddings of infinite permutation groups, *in* "Proceedings of Groups —St. Andrews 1985," London Math. Soc. Lecture Note Ser. 121 (E. Robertson and C. M. Campbell, Eds.), pp. 335–351, Cambridge Univ. Press, Cambridge, UK, 1986.

[T1] J. K. Truss, Joint embeddings of infinite permutation groups, *in* "Advances in Algebra and Model Theory" (M. Droste and R. Göbel, Eds.), Algebra, Logic and Applications, Vol. 9, pp. 121–134, Gordon and Breach, New York, 1997.

[Z] Y. Zhang, Maximal cofinitary groups, *Arch. Math. Logic*, to appear.

[Z1] Y. Zhang, Permutation groups and covering properties, *J. London Math. Soc.*, to appear.

[Z2] Y. Zhang, On a class of MAD families, *J. Symbolic Logic* **64** (1999), 737–746.