ON THE SET OF FINITE SUBSETS OF A SET

J. L. HICKMAN

Communicated by J. N. Crossley

We sometimes think of medial (that is, infinite Dedekind-finite) sets as being "small" infinite sets. Medial cardinals can be defined as those cardinals that are incomparable to $\aleph_0$; hence we tend to think of them as being spread out on a plane "just above" the natural numbers, which seems to lend support to the view expressed above that medial sets are "small".

There are, however, certain results that tend to counteract this intuitive idea. Let a set x be called "quasi-minimal" if x is infinite and every subset of x is either finite or cofinite. Then G. Monro (1973) has shown that given any aleph κ, it is consistent with ZF to assume the existence of a quasi-minimal set x such that $\left| P^3(x) \right| > \kappa$. Here $P(x)$ is the power-set of x, $P^2(x) = P(P(x))$, and so on.

A second result in this vein, discovered by the present author, is that given any aleph κ, it is consistent with ZF to assume the existence of a Dedekind-finite set x such that $\left| x^{[2]} \right| > \kappa$. Here, $x^{[2]} = \{ y \subseteq x; \left| y \right| = 2 \}$. Our main result in this paper is a generalization of this.

THEOREM: *Let (κ_n) be an increasing ω-sequence of alephs, and let θ be the statement $\exists x (\left| x \right| \| \kappa_0 \& (n) (\left| x^{[n+2]} \right| > \kappa_{n+1} \& \left| x^{[n+2]} \right| \| \kappa_{n+2}))$. Then if ZF is consistent, so is $ZF + \{\theta\}$.*

In this theorem, we of course define $x^{[n]}$ to be $\{ y \subseteq x; \left| y \right| = n \}$, $n \geq 1$: also, the symbol "$\|$" denotes cardinal incomparability, that is, if λ, η are two cardinals, ~then $\eta \| \lambda$ if and only if $\eta \nleq \lambda$ and $\lambda \nleq \eta$.

The theorem will be proved if we can construct a ZF model $\mathcal{N}$ such that $\mathcal{N}$ preserves cardinals and $\mathcal{N} \models \theta^{\mathcal{N}}$. Such a model $\mathcal{N}$ will obviously need to fail AC, and so it seems likely that $\mathcal{N}$ will need to be constructed by one of the forcing methods. In fact we use the Boolean technique as outlined by Jech (1972): to save both space and tiresome repetition, we assume familiarity with the relevant parts of Jech (1971), and use results contained therein. On the other hand, since in the author's opinion some of Jech's proofs are highly condensed (to put it mildly), some of the proofs given in Jech (1971) will be repeated here with a little more elaboration.

At this point we note two conventions that will be observed throughout this paper: (1) Each ordinal is identified with the set of all smaller ordinals; and (2) Each aleph is identified with the corresponding initial ordinal. (1) is quite unexceptionable; (2) is highly dubious, but its convenience outweighs its questionable character.

Let $\mathcal{M}$ be a countable transitive model of $ZF + \{AC\}$; unless the contrary is stated explicitly, henceforth all reasoning is assumed to take place within $\mathcal{M}$. Let the increasing ω-sequence (κ_n) be given, let $\kappa = \sup(\kappa_n)$, and for each n put $\Delta_n = (\kappa_{n+1} - \kappa_n) \times (n + 2)$, $\Gamma_n = \Delta_n \times (\kappa_{n+1} - \kappa_n)$. Put $\Delta = \cup \{\Delta_n; n < \omega\}$, and $\Gamma = \cup\{\Gamma_n; n < \omega\}$. We define a poset $(Q, \leqq)$ as follows. The elements of Q (henceforth called "conditions") are those functions $p: \Gamma \times \kappa \to \{0, 1\}$ for which $\mathrm{dom}(p)$ is finite; we put $p \leqq q$ if $p \supseteq q$.

Two conditions p, q are called "incompatible" if there is no condition r such that $r \leqq p$ and $r \leqq q$. We note that p, q are incompatible if and only if there exists $x \in \mathrm{dom}(p) \cap \mathrm{dom}(q)$ such that $p(x) \neq q(x)$, and use this fact to show that $(Q, \leqq)$ satisfies the countable chain condition (c.c.c.), that is, that any set of pairwise incompatible conditions in countable.

Let W be a set of pairwise incompatible conditions, and for each n, put

$$W_n = \{p \in W; |\mathrm{dom}(p)| = n\}.$$

If we can show that each W_n is finite, then it will follow from AC that W is countable. Thus suppose that some W_m is infinite; it follows from the above criterion for incompatibility that there exists x_0 and an infinite subset $W_{m,0}$ of W_m such that $x_0 \in \mathrm{dom}(p)$ for all $p \in W_{m,0}$. By the same criterion, there exists $x_1 \neq x_0$ and an infinite subset $W_{m,1}$ of $W_{m,0}$ such that $x_1 \in \mathrm{dom}(p)$ for all $p \in W_{m,1}$. Proceeding in this manner for $m + 1$ steps, we obtain an infinite subset $W_{m,m}$ of W_m such that $|\mathrm{dom}(p)| > m$ for all $p \in W_{m,m}$. This contradiction shows W_m to be finite; hence W is countable.

We let $\mathcal{B} = RO((Q, \leqq))$ be the complete Boolean algebra that is the canonical extension of $(Q, \leqq)$ (Jech (1971); page 50); since $(Q, \leqq)$ is dense in $\mathcal{B}$, $\mathcal{B}$ satisfies the c.c.c. We need to define a group $\mathcal{G}$ of $\mathcal{B}$-automorphisms, and do this by defining a group G of permutations on Γ; for if g is a Γ-permutation, then g_0 defined by $g^0(p) (g(x), \alpha) = p(x, \alpha)$ is an automorphism on $(Q, \leqq)$, and thence extends canonically to a $\mathcal{B}$-automorphism.

Thus we define a group G of Γ-permutations as follows. $g \in G$ if and only if
(1) g leaves each Γ_n invariant, that is, $g''\Gamma_n = \Gamma_n$;
(2) For $(\alpha, i, \beta) \in \Gamma_n$, if $g(\alpha, i, \beta) = (\alpha', i', \beta')$, then
(a) $\alpha = \alpha'$, and
(b) i' depends only upon i, and not upon β.

This determines G, which in turn determines $\mathcal{G}$.

For any subset J of Γ, we define G^J to be the subgroup of G consisting of those

$g \in G$ that leave J pointwise fixed, that is, $g(x) = x$ for all $x \in J$. We let $\mathcal{G}^J$ be the corresponding subgroup of $\mathcal{G}$. We now define a set $\mathscr{F}$ of subgroups of $\mathcal{G}$ by $\mathscr{F} = \{\mathscr{H} \leq \mathcal{G}; \exists J \subset \Gamma(|J| < \kappa_0 \in \mathcal{G}^J \leq \mathscr{H})\}$. It is easily verified that $\mathscr{F}$ is a normal filter of subgroups of $\mathcal{G}$.

Let U be a generic ultrafilter on $\mathcal{B}$; such a U exists since $\mathcal{M}$ is countable. U determines an interpretation i_U of $\mathcal{M}^{\mathcal{B}}$ (see Jech (1971; page 58)), which in turn determines a model $\mathcal{M}(U) = i_U''\mathcal{M}^{\mathcal{B}}$ of ZF + $\{AC\}$; we note that $\mathcal{M} \subseteq \mathcal{M}(U)$, and use this fact to show that $\mathcal{M}(U)$ preserves cardinals in $\mathcal{M}$.

Let η, λ be cardinals in $\mathcal{M}$ with $\eta < \lambda$. Since the concept of ordinal is absolute, η and λ are certainly ordinals in $\mathcal{M}(U)$, and so to show that η, λ are cardinals in $\mathcal{M}(U)$, it suffices to show that there is no $\mathcal{M}(U)$-bijection: $\eta \simeq \lambda$. Suppose that $f : \eta \simeq \lambda$ is an $\mathcal{M}(U)$-bijection, and let $\underline{f}$ be a name for f (Jech (1971; page 58)). Put $w = [\![\underline{f} : {}^{\vee}\eta \simeq {}^{\vee}\lambda \text{ is a bijection}]\!]$, and for $\alpha < \eta$, $\beta < \lambda$, put $w_{\alpha,\beta} = [\![\underline{f}({}^{\vee}\alpha) = {}^{\vee}\beta]\!] \cdot w$. Then $w \neq 0$, but if $\beta \neq \gamma$, then $w_{\alpha,\beta} \cdot w_{\alpha,\gamma} = 0$. Furthermore, for every $\beta < \lambda$ there exists $\alpha < \eta$ such that $w_{\alpha,\beta} \neq 0$. For if $\beta < \lambda$, then $[\![{}^{\vee}\beta \neq {}^{\vee}\lambda]\!] = 1$, and so

$$[\![\exists \alpha < {}^{\vee}\eta(\underline{f}(\alpha) = {}^{\vee}\beta)]\!] \geq w.$$

We can now use a theorem due to Rosser (1969; Theorem 3.20) to show that $[\![\exists \alpha < {}^{\vee}\eta(\underline{f}(\alpha) = {}^{\vee}\beta)]\!] = \text{SUP}\{[\![\underline{f}({}^{\vee}\alpha) = {}^{\vee}\beta]\!]; \alpha < \eta\}$, from which the desired result immediately follows. Thus $|\{\beta < \lambda; \exists \alpha < \eta(w_{\alpha,\beta} \neq 0)\}| = \lambda$; since in $\mathcal{M}$ we have $\eta < \lambda$, there must exist some $\alpha° < \eta$ such that $|\{\beta < \lambda: w_{\alpha°,\beta} \neq 0\}| = \lambda$. As $\lambda > \aleph_0$, this contradicts the c.c.c., since all these $w_{\alpha°,\beta}$ are pairwise incompatible. Thus no such f can exist, and so η, λ are cardinals in $\mathcal{M}(U)$ with $\eta < \lambda$. This shows that $\mathcal{M}(U)$ preserves cardinals in $\mathcal{M}$.

Now the group $\mathcal{G}$ and the filter $\mathscr{F}$ determine a class HS of hereditarily symmetric elements of $\mathcal{M}^{\mathcal{B}}$ (see Jech (1971; page 115)). HS gives us in turn our desired ZF model $\mathcal{N}$, defined by $\mathcal{N} = i_U''HS$. Clearly $\mathcal{M} \subseteq \mathcal{N} \subseteq \mathcal{M}(U)$, and so follows from the above that $\mathcal{N}$ preserves cardinals in $\mathcal{M}$.

Having obtained our model $\mathcal{N}$ and seen that (κ_n) has the desired meaning in $\mathcal{N}$, we can turn our attention to the task of defining the appropriate $\mathcal{N}$-set, which we shall eventually call "A". To start with, however, we shall define some $\mathcal{N}$-sets b_x, with x ranging over the set Γ. We define $\underline{b}_x \in \mathcal{M}^{\mathcal{B}}$ for $x \in \Gamma$ as follows:- $\text{dom}(\underline{b}_x) = \{{}^{\vee}\alpha; \alpha < \kappa\} \subseteq HS$, and $\underline{b}_x({}^{\vee}\alpha) = \text{SUP}\{p \in Q; p(x,\alpha) = 1\}$; here SUP is the generalized Boolean join operation. Clearly $\mathcal{G}^{\{x\}} \leq \text{sym}(\underline{b}_x)$, and so $\underline{b}_x \in HS$; thus $b_x = i_U(\underline{b}_x) = \{\alpha < \kappa; \exists p \in U(p(x,\alpha) = 1)\}$ is an $\mathcal{N}$-set.

We use these $\mathcal{N}$-sets to construct certain $\mathcal{N}$-sets $a_{\alpha,i}$, $(\alpha, i) \in \Delta$, which in turn will be the elements of our desired $\mathcal{N}$-set A. Thus for $(\alpha, i) \in \Delta$ we define $\underline{a}_{\alpha,i} \in \mathcal{M}^{\mathcal{B}}$ by $\text{dom}(\underline{a}_{\alpha,i}) = \{\underline{b}_{(\alpha,i,\beta)}; (\alpha, i, \beta) \in \Gamma\} \subseteq HS$, $\underline{a}_{\alpha,i}(\underline{b}_{(\alpha,i,\beta)}) = 1$. For any fixed $\beta°$ with $(\alpha, i, \beta°) \in \Gamma$, $\mathcal{G}^{\{(\alpha,i,\beta°)\}} \leq \text{sym}(\underline{a}_{\alpha,i})$, and so

$$a_{\alpha,i} = i_U(\underline{a}_{\alpha,i}) = \{b_{(\alpha,i,\beta)}; (\alpha, i, \beta) \in \Gamma\}$$

is an $\mathcal{N}$-set.

Define $A \in \mathcal{M}^{\mathcal{B}}$ by $\mathrm{dom}(A) = \{\underline{a}_{\alpha,i}; (\alpha, i) \in \Delta\} \subseteq HS$, $S(\underline{a}_{\alpha,i}) = 1$. $\mathrm{sym}(\underline{A}) = \mathcal{G}$, and so $A = i_U(A) = \{a_{\alpha,i}; (\alpha, i) \in \Delta\}$ is an $\mathcal{N}$-set. We now need to show that $\mathcal{N} | = |A| \| \kappa_0$, and we commence by showing that $\mathcal{N} | = b_x \neq b_y$ if $x \neq y$.

Suppose that for some $x, y \in \Gamma$ with $x \neq y$ we have $p \| - \underline{b}_x = \underline{b}_y$ for some $p \in Q$. Since $\mathrm{dom}(p)$ is finite, there is $\alpha < \kappa$ such that neither (x, α) nor (y, α) are in $\mathrm{dom}(p)$. Extending p to a condition q by putting $q(x, \alpha) = 1$ and $q(y, \alpha) = 0$, we see that $q \| - {}^\vee\alpha \in \underline{b}_x$ & ${}^\vee\alpha \notin \underline{b}_y$, and hence that $q \| - \underline{b}_x \neq \underline{b}_y$. Since this contradicts $q \leqq p$, we conclude that no condition forces $\underline{b}_x = \underline{b}_y$. However, $\mathcal{N} | = b_x = b_y$ if and only if $p \| - \underline{b}_x = \underline{b}_y$ for some $p \in U$. It follows immediately that $\mathcal{N} | = b_x \neq b_y$.

As a result of this, we have $\mathcal{N} | = a_{\alpha,i} \neq a_{\beta,k}$ for any (α, i), $(\beta, k) \in \Delta$ with $(\alpha, i) \neq (\beta, k)$: using the definitions of $\mathcal{F}$ and Δ, we conclude that $\mathcal{N} | = |A| \nleqq \kappa_0$. Thus in order to show that $\mathcal{N} | = |A| \| \kappa_0$, it suffices to show that there is no $\mathcal{N}$-injection: $\kappa_0 \to A$.

Suppose that f is such an $\mathcal{N}$-injection; let $\underline{f}$ be a name for f, and let J be such that $|J| < \kappa_0$ and $\mathcal{G}^J \leqq \mathrm{sym}(\underline{f})$. By injectivity, there exists $\sigma < \kappa_0$, and (α, i), $(\alpha, i') \in \Delta$ such that (a) $i \neq i'$, (b) for no β such that $(\alpha, i, \beta) \in \Gamma$ do we have either (α, i, β) or (α, i', β) in J, and (c) $\mathcal{N} | = (f: \kappa_0 \to A$ is injective and $f(\sigma) = a_{\alpha,i})$. As above, we conclude that $p \Vdash (\underline{f}: {}^\vee\kappa_0 \to S$ is injective and $\underline{f}(\sigma^\vee) = \underline{a}_{\alpha,i})$ for some $p \in U$. Since $\mathrm{dom}(p)$ is finite, there exists β^0 such that $(\alpha, i, \beta^0) \in \Gamma$, and for no $\beta > \beta^0$, $\delta < \kappa$, do we have $((\alpha, i, \beta), \delta) \in \mathrm{dom}(p)$.

We now define a permutation g on Γ as follows.

(1) If $(\gamma, j) \neq (\alpha, i)$, (α, i'), and $(\gamma, j) \in \Delta$, then for each β such that $(\gamma, j, \beta) \in \Gamma$, we have $g(\gamma, j, \beta) = (\gamma, j, \beta)$.

(2) For each $\beta \leqq \beta^0$ with $(\alpha, i, \beta) \in \Gamma$, we have $g(\alpha, i, \beta) = (\alpha, i', \beta^0 + \beta)$ and $g(\alpha, i, \beta^0 + \beta) = (\alpha, i, \beta)$.

(3) For each $\beta > \beta^0 2$ with $(\alpha, i, \beta) \in \Gamma$, we have $g(\alpha, i, \beta) = (\alpha, i', \beta)$.

(4) Repeat (2), (3) with i, i' interchanged.

Clearly $g \in G$; in fact $g \in G^J$. Let $g \in \mathcal{G}$ be the corresponding $\mathcal{B}$-automorphism; then $g \in \mathrm{sym}(\underline{f})$. Also, a simple calculation shows that $g(p)$ and p are compatible, and that $g(a_{\alpha,i}) = \underline{a}_{\alpha,i'}$. Taking $q \leqq g(p) \cdot p$, we see that $q \leqq p$ and

$$q \| - \underline{f}(\sigma) = \underline{a}_{\alpha,i'};$$

hence $q \Vdash a_{\alpha,i} = a_{\alpha,i'}$. Since no condition can force $a_{\alpha,i} = a_{\alpha,i'}$, f cannot exist, and thus $\mathcal{N} | = |A| \| \kappa_0$.

The next task is to show that for each n, $\mathcal{N} | = |A^{[n+2]}| > \kappa_{n+1}$, and to do this we construct, for each n, a class of sets $a \in A^{[n+2]}$, where $\alpha \in \kappa_{n+1} - \kappa_n$. For each such α, define $\underline{a}_\alpha \in \mathcal{M}^{\mathcal{B}}$ by $\mathrm{dom}(\underline{a}_\alpha) = \{\underline{a}_{\alpha,i}; i < n + 2\} \subseteq HS$, $\underline{a}_\alpha(\underline{a}_{\alpha,i}) = 1$. $\mathrm{sym}(\underline{a}_\alpha) = \mathcal{G}$, and so $a_\alpha = i_U(\underline{a}_\alpha) = \{a_{\alpha,i}; i < n + 2\}$ is an $\mathcal{N}$-set.

Clearly $\mathcal{N} | = a \in A^{[n+2]}$. Let us now define $\underline{f}_n \in \mathcal{M}^{\mathcal{B}}$ by $\mathrm{dom}(\underline{f}_n) = \{({}^\vee\alpha, \underline{a}_\alpha)^{\mathcal{B}};$ $\alpha \in \kappa_{n+1} - \kappa_n\}$, $\underline{f}_n(({}^\vee\alpha, \underline{a}_\alpha)^{\mathcal{B}}) = 1$. Now $({}^\vee\alpha, \underline{a}_\alpha)^{\mathcal{B}}$ is just the Boolean construction of the ordered pair, and so from the fact that $\mathrm{sym}(\underline{a}_\alpha) = \mathcal{G}$ we deduce that

$\text{sym}((^\vee\alpha, \underline{a}_\alpha)^{\circledast}) = \mathscr{G}$. Thus $\text{dom}(f_n) \subseteq HS$, and since $\text{sym}(f_n) = \mathscr{G}$ we have that $f_n = i_U(f_n) = \{(\alpha, a_\alpha); a \in \kappa_{n+1} - \kappa_n\}$ is an $\mathscr{N}$-set. It is in fact easy to see that f_n is an $\mathscr{N}$-injection: $\kappa_{n+1} - \kappa_n \to A^{[n+2]}$, from which we conclude that $\mathscr{N}| = |A^{[n+2]}| \geqq \kappa_{n+1}$, because $\mathscr{N}$ preserves cardinals in $\mathscr{M}$.

Now it is provable within ZF that given any infinite set x and any m, n with $0 < m \leqq n$, there is an injection $f: x^{[m]} \to x^{[n]}$. Thus if we had $\mathscr{N}| = |A^{[n+2]}| = \kappa_{n+1}$, then we would have $\mathscr{N}| = |A| \leqq \kappa_{n+1}$, which, since both κ_0 and κ_{n+1} are alephs, contradicts $\mathscr{N}| = |A| \| \kappa_0$. Thus it must be the case that $\mathscr{N}| = |A^{[n+2]}| > \kappa_{n+1}$.

Finally, we have to prove that $\mathscr{N}| = |A^{[n+2]}| \| \kappa_{n+2}$. The same reasoning as in the previous paragraph gives $\mathscr{N}| = |A^{[n+2]}| \nleqq \kappa_{n+2}$, and so it suffices to show that there is no $\mathscr{N}$-injection: $\kappa_{n+2} \to A^{[n+2]}$.

Suppose that f is such an injection, and, remembering that $\mathscr{N}$ is a ZF model, let us for the moment reason entirely within $\mathscr{N}$. Let K be the collection of those $\beta < \kappa_{n+2}$ for which there is a finite subset $\mathscr{B}_\beta$ of $\cup\{\{i\} \times (\kappa_{i+1} - \kappa_i); i \leqq n\}$ such that $f(\beta) = \cup\{f_k(\alpha); (k, \alpha) \in \mathscr{B}_\beta\}$. This definition of K is acceptable in the sense that it uses only objects in $\mathscr{N}$, and so K is an $\mathscr{N}$-set. Now if we had $|K| = \kappa_{n+2}$, then since each f_k is injective, we could set up an injection $h: \kappa_{n+2} \to s$, where s is the set of all finite subsets of $\omega \times \kappa_{n+1}$. But this is absurd since the κ_i are alephs and hence $|s| = \kappa_{n+1}$. Thus $|K| < \kappa_{n+2}$, and so $|\kappa_{n+2} - K| = \kappa_{n+2}$.

The above reasoning was carried out within $\mathscr{N}$. Translating, we see that if f is a name for f and $J \subset \Gamma$ such that $|J| < \kappa_0$ and $\mathscr{G}^J \leq \text{sym}(f)$, then there exist $p \in Q$, $\gamma < \kappa_{n+2}$, and (α, i), $(\alpha, i') \ddot{\in} \Delta$ such that $i \neq i'$, neither (α, i, β) nor (α, i', β) belong to J for any β, and $p \| - (\underline{f}:^\vee\kappa_{n+2} \to A^{[n+2]}$ is injective

$$\varepsilon\underline{a}_{\alpha,i} \in \underline{f}(^\vee\gamma)\varepsilon\underline{a}_{\alpha,i}, \notin \underline{f}(^\vee\gamma)).$$

Just as we did in showing that $\mathscr{N}| = |A| \| \kappa_0$, however, we can construct $g \in \mathscr{G}^J$ such that p and $g(p)$ are compatible and g interchanges $\underline{a}_{\alpha,i}$ and $\underline{a}_{\alpha,i'}$. Thus if we take a condition $q \leqq g(p) \cdot p$, we have $q \|| - \underline{a}_{\alpha,i} \in \underline{f}(\gamma)\varepsilon\underline{a}_{\alpha,i} \notin \underline{f}(\gamma)$. This contradiction shows that no such f can exist, which in turn shows that

$$\mathscr{N}| = |A^{[n+2]}| \| \kappa_{n+2}.$$

This completes the proof of the theorem stated on page 1.

If an infinite set x is well-orderable, then we have $|x^{[m]}| = |x^{[n]}|$ for all $m, n \neq 0$. We have just seen that if the condition of "well-orderability" is dropped, then this property can fail quite drastically. Before looking at some other questions related to the above equations, we prove a result mentioned on the previous page.

THEOREM 1. *Let x be an infinite set. For any m, n with $0 < m < n$, there is an injection $f: x^{[m]} \to x^{[n]}$.*

PROOF. The result is clear if $m = 0$ or $m = n$; hence we may assume that $0 < m < n$. Since m, n, are finite, it suffices to demonstrate that for each $m > 0$ there is an injection $f: x^{[m]} \to x^{[m+1]}$. This we now do. Since x is infinite, there exists $y^0 \in x^{[2m+1]}$; by considering $|y^{0[k]}|$ for each $k \leq m$, we see that there exist injections $g_k: y^{0[k]} \to y^{0[k+1]}$. Putting $g = \cup \{g_k; k \leq m\}$, we have an injection $g: y^{0[<m+1]} \to y^{0[<m+2]}$ such that $|g(z)| = 1 + |z|$ for every $z \in \mathrm{dom}(g)$.

Now take any $y \in x^{[m]}$; there is a unique partition $y = y_0 \cup y_1$, with

$$y_0 = y \cup y^0, \quad y_1 = y - y_0.$$

We define f by $f(y) = g(y_0) \cup y_1$; clearly $f''x^{[m]} \subseteq x^{[m+1]}$, and it remains to prove f injective.

But this is clear, since for any y, $z \in x^{[m]}$ with $y \neq z$, then either $y_0 \neq z_0$, in which $y_1 \subseteq x - y^0$, and similarly for z, it follows that $f(y) \neq f(z)$.

The same result has been proved independently by Truss (to appear)

THEOREM 2. *Let x be a nonempty set. Then*

(1) *x is infinite if and only if $n|x| \leq |x^{[2]}|$ for all n.*
(2) *x is Dedekind-infinite only if $\aleph_0|x| \leq |x^{[2]}|$.*
(3) *x is finite if and only if $P(x)$ is Dedekind-finite and $|x^{[2]}| < \aleph_0|x|$.*

PROOF. (1) Suppose x finite, and put $m = |x^{[2]}| + 1$. Then $m|x| > |x^{[2]}|$. Now suppose x infinite, and let $y = \{a_0, \cdots, a_{n-1}\}$ be a fixed element of $x^{[n]}$; then $(x - y)^{[2]}$ is infinite. We define a map $f: n \times (x - y) \to (x^{[2]} - (x - y)^{[2]})$ by $f(i, a) = \{a_i, a\}$: clearly f is injective. Since $n \times y$ is finite, there exists an injection $g: n \times y \to (x - y)^{[2]}$. But now $h = f \cup g: n \times x \to x^{[2]}$ is injective.

(2) Suppose x Dedekind-infinite, and let y be a denumerably infinite subset of x such that $x - y$ is Dedekind-infinite. Define injections

$$f: \omega \times (x - y) \to (x^{[2]} - (x - y)^{[2]})$$

and $g: \omega \times y \to (x - y)^{[2]}$ in the same manner as in (1), and proceed accordingly.

(3) If x is finite, then $P(x)$ and $x^{[2]}$ are also finite, whilst $\omega \times x$ is denumerably infinite. Thus suppose that $P(x)$ is Dedekind-finite and that $|x^{[2]}| < \aleph_0|x|$. Thus there is an injection $f: x^{[2]} \to \omega \times x$. Suppose that for some n we have $f''x^{[2]} \subseteq n \times x$. If $x = \phi$ there is nothing to prove. Thus we may assume $x \neq \phi$, and from the assumption that $P(x)$ is Dedekind-finite, it follows that x is Dedekind-finite, whence $n|x| < (n+1)|x|$. Thus we have $|x^{[2]}| < (n+1)|x|$, and (1) tells us that in this case x is finite.

Thus we may assume that there is an increasing ω-sequence (n_k) of natural numbers such that $f''x^{[2]} \cap (n_k \times x) \neq \phi$ for each k.

Define $g: x \to \omega$ as follows. For $a \in x$,

$$g(a) = \min \{n; \exists b \in x \exists y \in x^{[2]}(a \in y \, \varepsilon f(y) = (n, b))\}.$$

From the preceding observation it follows that $g''x$ is an unbounded subset of ω, whence $P(x)$ is Dedekind-infinite, a contradiction. Thus no such (n_k) exists, and so x must be finite.

A fairly well-known result says that for any set x, if $|x| = 2|x|$, then $|x| = \aleph_0|x|$; an easy consequence of this is that if $m|x| = n|x|$ for some m, n with $m < n$, then $k|x| = \aleph_0^\wedge|x|$ for all $k \geq m$. In fact, as pointed out by the referee, we can deduce $|x| = \aleph_0|x|$. For Tarski (1949) has proved that for any cardinals η, λ, $2\eta = 2\lambda \Rightarrow \eta = \lambda$. Thus suppose $m|x| = n|x|$ for some m, n, $m < n$. Then for some k we have $2^k|x| = 2^{k+1}|x|$, whence by k applications of Tarski's theorem we obtain $|x| = 2|x|$.

Combining these remarks with part (1) of the preceding theorem, we see that there are à priori the following possibilities for an infinite set, x.

(i) $|x| = 2|x| = \cdots = \aleph_0|x| = |x^{[2]}|$.
(ii) $|x| = 2|x| = \cdots = \aleph_0|x| < |x^{[2]}|$.
(iii) $|x| < 2|x| < \cdots < |x^{[2]}|$.

As an example of case (i), any infinite well-ordered set will do: as an example of case (iii), we can take x to be any medial set. To find an example of case (ii), we use our Theorem of the preceding section to assume the existence of a medial set y such that $|y^{[2]}| > \aleph_1$, and we put $x = \omega \times y$. Then clearly

$$|x| = 2|x| = \cdots = \aleph_0|x|.$$

If on the other hand we had $|x| = |x^{[2]}|$, then we would have $\aleph_0|y| > \aleph_1$, from which we could conclude that $|y| > \aleph_{01}$. Thus x is an example of case (ii).

Case (iii) splits into the following subcases:-

(iiia) $|x| < 2|x| < \cdots < \aleph_0|x| < |x^{[2]}|$;
(iiib) $|x| < 2|x| < \cdots < \aleph_0|x| = |x^{[2]}|$;
(iiic) $|x| < 2|x| < \cdots < \aleph_0|x| \parallel |x^{[2]}|$.

Suppose we take a medial set x such that $P(x)$ is also medial; then of course $x^{[2]}$ is medial, and so we cannot have $\aleph_0|x| \leq |x^{[2]}|$. On the other hand, Theorem 2(3) tells us that we cannot have $|x^{[2]}| < \aleph_0|x|$. Thus x satisfies (iiic).

In order to settle (iiia), let us show that for the model $\mathcal{N}$ and the set A constructed in the preceding section, we have $\mathcal{N}|=|A| < 2|A|$. Suppose on the contrary there is an $\mathcal{N}$-injection $f: 2 \times A \to A$; let $\underline{f}$ be a name for f, and let $J \subset \Gamma$ be such that $|J| < \kappa_0$ and $\mathscr{G}^J \leq \text{sym}(\underline{f})$. It follows that there exist $p \in Q$, $i < 2$, and (α, j), $(\beta, k) \in \Delta$ with $\alpha > \kappa_1$ and $(\alpha, j) \neq (\beta, k)$, such that for no σ do we have either (α, j, σ) or (β, k, σ) in J, and such that $p \parallel -\underline{f}(i, \underline{a}_{\alpha,j}) = \underline{a}_{\beta,k}$. But now we obtain a contradiction as in the proof of $\mathcal{N}|=|A|\parallel\kappa_0$. Thus no such f exists, and so $\mathcal{N}|=|A| < 2|A|$. Furthermore, if (in $\mathcal{N}$) λ is a cardinal $< \kappa_0$, then it is a simple matter to construct an $\mathcal{N}$-injection $f_\lambda: \lambda \to A$. This is because f_λ, as a

set of ordered pairs, has cardinality $< \kappa_0$, and so we can simply take $J \subset \Gamma$ large enough so that $\mathscr{G}^J \leqq \operatorname{sym}(f_\lambda)$ and still have $|J| < \kappa_0$.

Thus we may assume the existence of a Dedekind-infinite set x such that $|x| \, \| \, \aleph_1, |x| < 2|x|$, and $|x^{[2]}| > \aleph_2$. Theorem 2(2) tells us that $\aleph_0|x| \leqq |x^{[2]}|$; however, equality would imply that $|x| > \aleph_2$, contradicting $|x| \, \| \, \aleph_1$. Thus x is an example of (iiia). The possibility of (iiib) seems to be an open question.

We conclude by mentioning that in the terminology of the preceding section, in the case $\kappa_0 = \aleph_0$ we have $\mathscr{N}| = \aleph_0 |A| \, \| \, |A^{[2]}|$; the proof of this proceeds along conventional lines. Thus it is possible to have a medial set x such that

$$\aleph_0|x| \, \| \, |x^{[2]}| > \aleph_0.$$

Acknowledgement

References

T. Jech (1971), *Lectures in Set Theory*. (Springer-Verlag 1971.)

G. P. Monro (1973), 'Small sets with large powersets', *Bull. Austral. Math. Soc.* **8**, 413–422.

J. Barkley Rosser (1969), '*Simplified Independence Proofs*'. (Academic Press 1969).

A. Tarski (1949), 'Cancellation laws in the arithmetic of cardinals', *Fund Math.* **36**, 77–92.

J. K. Truss (to appear),'The well-ordered and well-orderable subsets of a set', *Zeit. f. math. Logik*.

Department of Mathematics
Institute of Advanced Studies
Australian National University
Canberra.