On a cardinal equation in set theory

J.L. Hickman

We work in a Zermelo-Fraenkel set theory without the Axiom of Choice. In the appendix to his paper "Sur les ensembles finis", Tarski proposed a finiteness criterion that we have called "C-finiteness": a nonempty set is called "C-finite" if it cannot be partitioned into two blocks, each block being equivalent to the whole set. Despite the fact that this criterion can be shown to possess several features that are undesirable in a finiteness criterion, it has a fair amount of intrinsic interest. In Section 1 of this paper we look at a certain class of C-finite sets; in Section 2 we derive a few consequences from the negation of C-finiteness; and in Section 3 we show that not every C-infinite set necessarily possesses a linear ordering. Any unexplained notation is given in my paper, "Some definitions of finiteness", Bull. Austral. Math. Soc. 5 (1971).

1.

Throughout this paper we assume a Zermelo-Fraenkel set theory without the Axiom of Choice. We define C-finiteness as follows:

**Definition 1.** \( FC(x) \leftrightarrow x = \emptyset \lor \forall y (y \in P(x) \land y \equiv x + \neg (x-y = x)) \).

Intuitively, a set \( x \) is C-finite if \( x \) is empty or if there is no 2-partition of \( x \) with each block being equivalent to \( x \). Alternatively, a cardinal \( \psi \) is C-finite if either \( \psi = 0 \) or \( 2\psi > \psi \). It can be shown that for nonzero cardinals \( \psi \), we have \( 2\psi = \psi \) if, and only if, \( \omega \psi = \psi \). An elegant proof of this fact can be found in [1].

As usual, medial sets are those that are D\( \Omega \) but not N-finite (see

Received 2 February 1972.
The sets that we wish to study in this section are called "W-sets":

**DEFINITION 2.** \( W(x) \leftrightarrow \exists y (\text{med}(y) \land x = \omega \cup y) \).

Before establishing any properties of \( W \)-sets, we give two trivial results on \( FC \)-sets, using the alternative characterization mentioned above.

**LEMMA 1.**

(i) \( \forall x \forall y \left( \neg FC(x) \land \neg FC(y) \land FC(x \cup y) \right) \).

(ii) \( \forall x \forall y \left( \neg FC(x) \land y \neq \emptyset \land FC(x \times y) \right) \).

**Proof.** (i) \( x \times (x \cup y) = (\omega \times x) \cup (\omega \times y) = x \cup y \).

(ii) Since \( y \neq \emptyset \), we have \( x \times y \neq \emptyset \) and \( x \times (x \times y) = (\omega \times x) \times y = x \times y \). Of course it is also clear that \( FDO \land FC \).

**THEOREM 1.** \( W \land FC \).

**Proof.** That \( W \land FC \) is trivial. To prove \( W \land FC \), take \( x \) medial, and put \( y = \omega \cup x \); then we know that \( y \neq \omega \). Assume \( y = y_1 \cup y_2 \), with bijections \( f_i : y = y_i \), with \( y_1 \cap y_2 = \emptyset \). From \( \text{med}(x) \) we obtain \( FN(\omega \cap f_i x) \), \( i = 1, 2 \). But this implies \( \{x \cap f_i x\} \geq \omega \), which is a contradiction.

**COROLLARY.** \( FC \land FDO \land FC \).

**Proof.** It suffices to show, under the assumption \( FC \land FDO \), that \( FDO \land FN \). Now if \( FDO \land FN \) does not hold, then there exists a medial set \( x \). But then \( y = \omega \cup x \) is a \( W \)-set, and so by Theorem 1, is \( FC \) but not \( FDO \).

An alternative statement and proof of this corollary is given as Theorem 2.3 in [1]. Theorem 1 allows us to deduce a consequence that in my opinion is completely undesirable in any finiteness criterion, namely, it is possible to have a \( C \)-finite set with a \( C \)-infinite subset. For, as we have seen, any \( W \)-set is \( FC \), but each \( W \)-set contains a countably infinite subset, which is certainly not \( FC \). We can in fact show that countably infinite subsets of \( W \)-sets are the only \( C \)-infinite subsets of \( W \)-sets.
THEOREM 2. \( \forall x \left[ \neg \text{FC}(x) \rightarrow y = \omega \right] \).

Proof. Take \( x \) medial, and \( y \in P(\omega x) \). Then \( y = (\omega x) \cup (x y) \) gives a 2-partition (since we may assume \( \omega \cap x = \emptyset \) ) in which we have \( \text{FC}(x y) \) and either \( \text{FC}(\omega x) \) or \( \omega \cap y = \omega \). Thus if \( y \) is not countable, then we must have \( y = \omega \cup z \) for some medial \( z \). The result now follows.

The class of \( \mathcal{W} \)-sets is closed under union, but not under products.

THEOREM 3. \( \forall x \forall y \left[ \neg \text{FC}(x) \land \neg \text{FC}(y) \rightarrow \mathcal{W}(x \cup y) \right] \).

Proof. Take \( x = (\omega \times \{0\}) \cup u \), \( y = (\omega \times \{1\}) \cup v \), with \( u, v \) medial. Then \( u \cup v \) is medial, and since \( (\omega \times \{0\}) \cup (\omega \times \{1\}) = \omega \), we have \( x \cup y = \omega \cup (\omega u v) \).

A lemma is required to show that the class of \( \mathcal{W} \)-sets is not closed under products.

Lemma 2. \( \forall x \forall y \left[ \text{med}(x) \land \text{med}(y) \rightarrow \neg \text{FC}(x \times y) \right] \).

Proof. Since \( \text{med}(x) \land \text{med}(y) \rightarrow \text{FC}(x) \lor \text{FC}(y) \), this is a trivial consequence of Theorem 2.

THEOREM 4. \( \forall x \forall y \left[ \neg \text{FC}(x) \land \text{FC}(y) \rightarrow \mathcal{W}(x \times y) \right] \).

Proof. Since \( (\omega x) \times (\omega y) = \omega \times (\omega x \cup (0)) \cup (u \times v) \), the result follows from Lemma 2.

Just as we used the distinction between \( N \)-finiteness and \( DO \)-finiteness to define the class of medial sets, so we can use the distinction between \( DO \)-finiteness and \( C \)-finiteness to define another class of sets — we call these "LC-sets".

DEFINITION 3. \( LC(x) \leftrightarrow \text{FC}(x) \land \neg \text{DO}(x) \).

Clearly the class of \( LC \)-sets contains the class of \( \mathcal{W} \)-sets. Nothing presented in this paper so far, however, could really lead us to believe that the reverse inclusion does not hold. That it does not in fact hold will emerge as a simple corollary to a result that will be presented in Section 2 of this paper. The one result to be given in this section on \( LC \)-sets is as follows.

THEOREM 5. \( \forall x \left[ LC(x) \rightarrow \neg \text{FC}(P(x)) \right] \).
Proof. From $LC(x)$ we obtain $\neg PDO(x)$, whence $x = x \cup \{x\}$. But from this it follows that $P(x) = \{0, 1\} \times P(x)$.

We conclude this section by using some of the above results to give an alternative proof of a "classical" theorem of cardinal arithmetic.

**Theorem 6.** Let $c$ be the cardinality of the continuum. Then the equation $\omega_0 + \psi = c$ has a unique solution, namely $\psi = c$.

Proof. Clearly $c$ is a solution. Thus let $\psi$ be any solution; then obviously we have $\neg FN(\psi)$, whence we obtain either $med(\psi)$ or $\neg PDO(\psi)$. Now if $med(\psi)$ holds, then we have $W(c)$, and hence $FC(c)$.

Since, however, $c = 2^{\omega_0}$, this contradicts Theorem 5. Thus we cannot have $med(\psi)$, and so are left with $\neg PDO(\psi)$, in which case we have $c = \omega_0 + \psi = \psi$.

2.

Let $C$ denote the Axiom of Choice, and let $D$ denote the statement $\forall \kappa (\neg FN(\kappa) + 2\kappa = \kappa)$. Then of course it is known that $ZFC \vdash D$, whilst the converse $ZFD \vdash C$ is still an open problem. I do not believe that this converse implication holds, for whilst we can deduce $\omega_0 \kappa = \kappa$ from $2\kappa = \kappa$, the proof of this is achieved, essentially, by taking iterates of certain bijections, and there seems to be no way past the $\omega$-th iterate: hence to me it seems doubtful that we could even obtain any of the equations $\omega_\alpha \kappa = \kappa$ for $\alpha > 0$, let alone the equation $\kappa^2 = \kappa$ required by $C$.

On the other hand, the axiom $D$ does permit a certain deduction that bears a vague resemblance to a cardinal equivalent to $C$.

**Theorem 7.** $ZFD \vdash \exists \kappa \exists \psi \left( \neg FN(\kappa) \vee FN(\psi) \vee \text{inc}(\kappa, \psi) \right) + \kappa + \psi = \max(\kappa, \psi)$.

Proof. $\text{inc}(\kappa, \psi)$ means that $\kappa$ and $\psi$ are incomparable. Thus assume that $\kappa$ and $\psi$ are $\aleph$-infinite, comparable cardinals, say $\kappa \leq \psi$. Thus we have some cardinal $\zeta$ such that $\kappa + \zeta = \psi$. But now by using axiom $D$, we have $\kappa + \psi = \kappa + \kappa + \zeta = 2\kappa + \zeta = \kappa + \zeta = \psi$. Similarly, if $\psi \leq \kappa$, we obtain $\kappa + \psi = \kappa$.

Clearly the comparability condition is necessary; and of course it is not known whether the multiplicative analogue of this theorem holds, for
A cardinal equation 451

If a ZF-model fails $D$ at all, then it fails $D$ at arbitrarily high levels. This is the content of the following theorem, in which the variable $a$ ranges over ordinals, with $\omega_a$ indicating alephs (initial ordinals).

THEOREM 8. $ZF \vdash \forall \kappa (\omega_a + \kappa > \kappa \land \forall \omega (\omega_a + \kappa > \omega + \kappa))$.

Proof. Let $\kappa$ be an $\aleph$-infinite cardinal with $\omega_a + \kappa = \kappa$, and let $\omega_a$ be any aleph. Clearly if $\omega_a < \kappa$, then $\omega_a + \kappa = \kappa$, and so $2(\omega_a + \kappa) = 2\kappa > \kappa = \omega_a + \kappa$. On the other hand, $\omega_a \geq \kappa$ would imply $2\kappa = \kappa$, contrary to hypothesis. Thus we may assume $\text{inc}(\omega_a, \kappa)$. Clearly we have $2(\omega_a + \kappa) = \omega_a + 2\kappa$. Assume that $\omega_a + 2\kappa = \omega_a + \kappa$, let $A$ be a set of power $\omega_a$, $K, K_0, K_1$ be sets of power $\kappa$, with $A, K, K_0, K_1$ pairwise disjoint, and let $\kappa$ a bijection. Put $N = f''(K_0 \cup K_1)$, $B_i = A \cap f''(K_i)$, and $N_i = N - B_i$, for $i < 2$. Now $B_1 \in P(A)$, and so there are ordinals $\beta, \gamma$ such that $|B_0| = \omega_\beta$, $|B_1| = \omega_\gamma$. Thus $|B_0 \cup B_1| = \omega_\delta$, where $\delta = \max(\beta, \gamma)$. Put $\zeta = |N_0 \cup N_1|$, since $N_0 \cup N_1 \in P(K)$, we have $\zeta \leq \kappa$. Now $\omega_\beta = |B_0| \leq |K_0| = \kappa$; similarly $\omega_\gamma \leq \kappa$; hence $\omega_\delta \leq \kappa$. However, $|N| = 2\kappa$, and so we have $2\kappa = \omega_\beta + \omega_\gamma + \zeta = \omega_\delta + \zeta \leq \omega_\delta + \kappa = \kappa$, a contradiction. Therefore we must have $2(\omega_a + \kappa) = \omega_a + 2\kappa > \omega_a + \kappa$.

COROLLARY. $ZF \vdash \exists x LC(x) \land \exists x (LC(x) \land \neg \omega(x))$.

The result contained in this section in my opinion casts doubt upon the conjecture $ZFD \vdash C$. We construct a model $M$ of $ZF$ in which there is a cardinal $\kappa$ (strictly speaking, a set of power $\kappa$) such that $\kappa \neq 0$, $2\kappa = \kappa$, but in which there is no linear ordering of $\kappa$.

Now if it could be shown that $M \models D$, then of course we would have the independence of $C$ from $ZFD$; in fact we would have the stronger
result of the independence from ZFD of Mostowski's axiom that every set can be linearly ordered.

Unfortunately it does not seem possible to prove that \( M \models D \), and so we cannot deduce the desired result. Nevertheless, it does seem to me that the result obtained in this section makes the independence of \( C \) from ZFD very plausible. For we know that \( \kappa \) satisfies the equation \( 2\kappa = \kappa \); and if in fact \( D \) implies even Mostowski's axiom, then it seems that we should be able to prove the existence of an ordering on \( \kappa \) from the properties of \( \kappa \) alone. However, this of course is merely a heuristic argument.

The model \( M \) is constructed by the boolean technique; the standard text for this is Rosser [4], and familiarity with this book will be assumed throughout this section. The main notational variation from [4] is the use of "p( )" instead of Rosser's "|| ||". Other notational variants are either obvious or will be explained at the appropriate time.

Our model \( M \) will be completely determined by the specification of a complete boolean algebra \( A \), a group \( G \) of \( A \)-automorphisms, and a strongly normal filter \( F \) on the subgroup lattice of \( G \).

As in all the cases in [4], our algebra \( A \) will be the algebra of regular open sets of a certain Tychonoff space; in our case this space will be \( 2^{\omega \times \omega} \). We denote the usual subbasis elements of our space by \( B_{m,n}^i \).

Thus we have our algebra \( A \); we need now to perform the slightly more complex task of defining the appropriate group \( G \) of \( A \)-automorphisms. It seems to be a general rule in constructing boolean ZF-models that the most difficult chore is choosing the right \( G \) for the job you have in mind. First we need a couple of preliminary definitions.

**DEFINITION 4.** For each \( i < 4 \), we put \( \{i\} = \{n \mid n \equiv i \mod 4\} \); for \( i, j < 4 \), we put \( \{i, j\} = \{i\} \cup \{j\} \).

**DEFINITION 5.** We define the map \( p_0 : \omega \to \langle 0, 2 \rangle \) by \( p_0(n) = 4n + 2 \), \( n \in \langle 0, 1 \rangle \), and \( p_0(n) = 4n \), \( n \in \langle 2, 3 \rangle \). We define the map \( p_1 : \omega \to \langle 1, 3 \rangle \) by \( p_1(n) = 4n + 3 \), \( n \in \langle 0, 1 \rangle \), and \( p_1(n) = 4n + 1 \), \( n \in \langle 2, 3 \rangle \). We can now define \( G \) as follows.
DEFINITION 6. We let $G$ be the set of permutations $g$ on $\omega$ that satisfy the following:

1. for each $i < \lambda$, $g^a(i) = (i)$;
2. for $j < 2$, $g$ commutes with $p_j$, that is, $gp_j = p_jg$.

For each $g \in G$, let $g$ be the $A$-automorphism induced by the subbasis transformation $B^i_{m,n} + \rho^i_{m,n}(n) = (i, m, n) \in 2 \times \omega \times \omega$. We now define $G$ to be that subgroup of the full $A$-automorphism group generated by the set $\{g; g \in G\}$ of $A$-automorphisms.

For each subset $J$ of $\omega$, we define $G_J$ to be that subgroup of $G$ consisting of precisely those $g \in G$ that leave $B^i_{m,n}$ invariant whenever $n \in J$. Using this last piece of terminology, we can define our filter $F$ in the following manner.

DEFINITION 7. $F = \{H \leq G; \exists J \in \mathcal{P}(\omega) \& F(N(J) \& G_J \leq H)\}$.

LEMMA 3. $F$ is strongly normal.

Proof. By definition, $F$ is strongly normal if it is closed under inner automorphisms, that is, if for every $g \in G$ and $H \leq G$, we have $gHg^{-1} \in F$ whenever $H \in F$. But this is immediate from Definition 7.


We denote the set of finite subsets of $\omega$ by $\mathcal{P}_f(\omega)$, and commence with a lemma.

LEMMA 4. $\forall J \in \mathcal{P}_f(\omega) \& g \in G \rightarrow \exists h \in G \& g|J = h|J \& g \neq h$.

Proof. Take $J \in \mathcal{P}_f(\omega)$ and $g \in G$. Since $J$ is finite, there exists $n$ such that $J \subseteq h^n$. Suppose that the value $g(h^n)$ is determined by the restriction $g|J$. Then we must have $g(h^n) = f(g(k))$ for some $k \in J$, where $f$ is algebraic over $p_0, p_1, p_0^{-1}, p_1^{-1}$. By (2) of Definition 6, we must have $g(h^n) = g(f(k))$, whence, since $g$ is
injective, we have $h^n = f(k)$. By inspection, we see that this restricts $n$ to a limited number of possibilities. This proves the lemma.

Now as a brief examination of the construction of models given in [4] shows, our model $M$ is the union of an increasing sequence of sets, which we denote by $\omega_\alpha$, where the subscripts range over the ordinals of our base model of ZF. Again as described in [4], $\omega_{\alpha+1}$ consists of the elements of $\omega_\alpha$, together with certain maps $\omega_\alpha \to A$.

**DEFINITION 9.** For each $n$, we define the (constant) map $a_n : \omega \to A$ by $a_n(x) = \inf \{ B^0_{m,n} ; m \in \omega \}$, $x \in \omega$.

**THEOREM 9.** Each $a_n$ is an $M$-set (that is, belongs to the model $M$), and for $m \neq n$ we have $M \models a_m \neq a_n$.

Proof. In order to show that $a_n$ is an $M$-set, we need to show that $a_n$ is extensional ((3.33) of [4]), and that $G_{a_n} \in F$ ((3.36) of [4]). Since $a_n$ is a constant map, extensionality is trivially satisfied; hence we concentrate on the second property. By definition, $G_{a_n} = \{ g \in G ; \rho(g(a_n) = a_n) = 1 \}$. Take any $g \in G$; we have $g(a_n)(x) = g(a_n(g^{-1}(x)))$ for $x \in D(a_n)$, by definition. But $g(a_n(g^{-1}(x))) = \inf \{ g(B^0_{m,n}) ; m \in \omega \}$. Hence we have $G_{a_n} \subseteq G_{a_n}$, and so by Definition 7, $G_{a_n} \in F$. Thus $a_n$ is an $M$-set.

In order to prove the second part of our theorem, we must show that for $m \neq n$ we have $\rho(a_m = a_n) = 0$. Now if we use the fact that $a_m$, $a_n$ are constant maps with the same domain, a straightforward but tedious simplification of (3.29) of [4] tells us that $\rho(a_m = a_n) = 0$ if, and only if, $\inf \{ B^0_k,m = B^0_k,n ; k \in \omega \} = 0$. However, we now have the same
situation as given by (6.14) of Theorem 6.4 in [4], and may complete the
proof in precisely the same way as done there.

**DEFINITION 10.** We define \( a : \omega^{\omega+1} \to A \) by
\[
a(x) = \sup\{\rho(x = a_n) ; n \in \omega\} , x \in \omega^{\omega+1}.
\]

**THEOREM 10.** \( a \) is an M-set, and \( M \models \forall x (x \in a \iff \exists n (x = a_n)) \).

Proof. To show extensionality, we have to prove that for any
\( x, y \in D(a) \) we have \( a(x) \land \rho(x = y) \leq a(y) \). This comes out easily by
using Definition 10 and the equality axioms. Now it is easy to show that
any \( g \in G \) simply acts as a permutation on the collection of \( a_n \), and
from this observation it is a simple matter to deduce that \( G_a = G \in F \).
Thus \( a \) is an M-set.

We now turn to the second part of the theorem. In one direction this
is trivial, for if \( M \models x = a_n \), that is, \( \rho(x = a_n) = 1 \), then
\( a(x) \geq \rho(x = a_n) \), and so \( a(x) = 1 \), that is, \( M \models x \in a \). The converse
implication, however, because our definition of \( a \) was "standard", is a
special case of Theorem 3.10 of [4]. Thus Theorem 10 is proved.

We now have a certain M-set \( a \); we let \( \kappa \) be the power of \( a \) in
\( M \), that is, \( \kappa = |a|^M \), and show that \( \kappa \) satisfies our two requirements.

**THEOREM 11.** \( M \models 2\kappa = \kappa \).

Proof. Define \( b_0 : \omega^{\omega+1} \to A \) by
\[
b_0(x) = \sup\{\rho(x = a_n) ; n \in \{0, 2\}\} , x \in \omega^{\omega+1},
\]
and \( b_1 : \omega^{\omega+1} \to A \) by
\[
b_1(x) = \sup\{\rho(x = a_n) ; n \in \{1, 3\}\} , x \in \omega^{\omega+1}.
\]
Since we are dealing with "standard" definitions, the extensionality of
the \( b_j \) is assured, whilst from Definition 6 (1) we see that \( G_{b_j} \in F \);
thus the \( b_j \) are M-sets, and it is routine to show, via Theorem 3.10 of
[4], that \( M \models \forall x \langle x \in b_0 \iff \exists n (n \in \{0, 2\} \& x = a_n) \rangle \), and similarly for
b_1. We now show that \( M \models a = b_0 \), the proof for \( b_1 \) being exactly analogous. By the Cantor-Bernstein Theorem it suffices to show the existence of an \( M \)-injection \( f: a \to b_0 \). We define \( f: \omega_\omega + 3 \to A \) as follows.

\[
f(x) = \sup \left\{ \rho \left( x = (a_n, a_{\omega n+2}) \right) ; n \in \langle 0, 1 \rangle \right\} + \sup \left\{ \rho \left( x = (a_n, a_{\omega n}) \right) ; n \in \langle 2, 3 \rangle \right\}, \ x \in \omega_\omega + 3.
\]

Since this definition is again of standard type, extensionality follows, and it is routine to deduce from Definition 6 (2) that \( G_f = G \). The rest is straightforward.

**Theorem 12.** \( M \models (\text{there is no linear ordering on } a) \).

Proof. Suppose that \( \tilde{d} \in P(a^2) \) is an \( M \)-linear ordering on \( a \); clearly we may assume \( \tilde{d} \) irreflexive. Let \( J \in P(\omega) \) be such that \( G_J \leq G_{\tilde{d}} \); it follows from Lemma 4 that we can choose \( m, n, m \neq n \), such that for some \( g \in G_J \) we have \( g(a_{\omega n}) = a_{\omega n} \) and \( g(a_{\omega n}) = a_{\omega n} \). Since this \( g \) leaves \( \tilde{d} \) invariant and \( \tilde{d} \) was assumed irreflexive, this is a contradiction.

**References**


