Automorphisms and a Further Failure of AC

Thomas Forster and Randall Holmes

January 5, 2025

ABSTRACT

We refute an innocent-looking consequence of AC in NF. (It concerns big sets). We comment on why this demonstration does not work in NFU

Contents

1 Introduction and Summary

We show that the conjunction of the two following principles must fail in NF:

- Øre's principle [2] says that in a full symmetric group on any set, two permutations of the same cycle type are conjugate.
- If $\mathbb{P}$ is a partition of V into (finite-or)-countable sets then its power set $\mathcal{P}(\mathbb{P})$ is the same size as the set $\iota``V$ of all singletons.

In the first bullet two permutations "have the same cycle type" iff they have the same number of cycles of each order. Øre's principle follows from a principle I have elsewhere [1] called GC, that says that every set of (finite-or)-countable sets has a choice function. Suppose there is a bijection f between the σ-cycles and the τ-cycles and f preserves order. Now each pair c, c' of a σ-cycle with a τ-cycle joined by f can be given a bijection by picking one member of c and one member of c' and mapping the one to the other. By GC we can pick members of c and of c' in this way since they are countable.

The second bullet would follow from "Every partition of V into countable pieces is of size $T|V|$" (which is saying that a partition of V into small sets cannot be too small). It would be nice if this were to follow from GC, but all GC seems to give is that such a partition injects into $\iota``V$.

Another – perhaps more natural formulation – of the second principle that would serve is “For any permutation σ, the partition of V into σ-cycles is the same size as ι“V the set of all singletons.”

Both principles are stratified and both follow from AC.

We will show that in any model of NF one of these principles must fail: no model of NF can believe both of them. This is a sharper refutation of AC than any seen before in the literature, but it is not a refutation of any version of AC concerning small sets. Countable choice, wellordering of wellfounded sets – these have not been refuted. Since both these principles are consequences of AC, and AC is consistent with NFU, our refutation will fail there; it will instructive to see how this plays out. We discuss this in section 2.

The argument revolves around $\in$-automorphisms. A permutation τ of V is an $\in$-automorphism iff $\tau = j\tau$, where j is defined so that $j\tau(x) = \tau$“x.

1.1 The Plan of the Proof

The plan is to show that if τ is an automorphism with an infinite cycle then, for every order, $j\tau$ has $T|V|$ cycles of that order. This uses the second principle. Thus $j\tau$ and $j^2\tau$ have the same cycle type and – by Øre’s principle – are conjugate. If $\sigma \cdot j\tau \cdot \sigma^{-1} = j^2\tau$ then, in the permutation model V^σ, $j\tau$ has become an automorphism of infinite order. Such an automorphism has cycles of all finite orders. Next we show that every cycle of an automorphism is cantorian. Thus – in the permutation model V^σ – every natural number is cantorian. This is the Axiom of Counting. The Axiom of Counting is invariant, so it must have been true in the model we started in. So it is a consequence of the two principles. However it has been long known [3] that the Axiom of Counting is not a theorem of any stratified extension of NF. The two principles we set out above are both stratified. So their conjunction is refuted in NF.

This establishes

Theorem 1 *No model of NF can satisfy both the above principles.*

Now for the details.

One way to prove that σ and $j\sigma$ have the same cycle type is to prove, for each order o, that they have as many cycles of order o as they possibly could. (There may be another route but if this one works we won’t go looking). So one wants to show – for a start – that both σ and $j\sigma$ have $|V|$ fixed points; this is the same as saying they both have $T|V|$ 1-cycles. What about 2-cycles? How do we best say that there are as many 2-cycles as there could be? Do we want to say that there are $T|V|$-many 2-cycles, or that there are $|V|$-many things that live in 2-cycles? And similarly for other orders: do we want to say that there are $|V|$-many things that live in o-cycles or that there are $T|V|$-many o-cycles? To hack through this bush we will arm ourselves with a choic-y principle that says that these two things are the same for every o. This is where the second principle comes from.

Thus armed, the way forward for us is to find a permutation τ such that $j\tau$ and $j^2\tau$ both have $T|V|$-many o-cycles for every order o. As it turns out, any permutation that has cycles of all orders will serve our purposes.

Lemma 1
Let τ be a permutation with cycles of all orders.
Then $j\tau$ and (therefore also $j^2\tau$) has $T|V|$-many o-cycles for every order o.

Proof:

> We remark without proof that there is no shortage of permutations of V that have cycles of all orders.

Clearly if τ has an infinite cycle I then ι“I is an infinite $j\tau$-cycle. So $j\tau$ has an infinite cycle; if N is a τ-cycle of order n then ι“N is a $j\sigma$-cycle of order Tn. By assumption τ has cycles of all orders so $j\tau$ does too.

Next we show that $j\tau$ has $T|V|$-many o-cycles for every order o.

Let N be a τ n-cycle and consider the partition $\mathbb{P}$ of $V \setminus N$ into τ-cycles (strictly: *carrier sets* of τ-cycles). Let X be a union of pieces of $\mathbb{P}$; X is fixed by $j\tau$, and $X \cup N$ belongs to a $j\tau$ n-cycle, and the other members of this cycle are $X \cup \tau$“N, $X \cup \tau^2$“N and so on. Distinct Xs give distinct $j\tau$ cycles, and – by the second principle – there are $2^{|\mathbb{P}|} = |V|$ of them, whence $T|V|$ distinct n-cycles under $j\tau$.

Notice that the argument in the last paragraph would have worked equally well if N had been an infinite cycle. So we have proved that $j\tau$ has $T|V|$-many infinite cycles.

All this followed from τ having cycles of all orders; $j\tau$, too, has cycles of all orders, so all the above consequences for $j\tau$ follow also for $j^2\tau$.

■

> Notice that the partition $\mathbb{P}$ that we reason about above is 1-equivalent to a partition of V, since $V \setminus N$ is of size $|V|$. It looks as if what we needed was “If $\mathbb{P}$ is a partition of a co-countable set into countable pieces then $2^{|\mathbb{P}|} = |V|$” but the two are equivalent.

Lemma 2 *If τ is an automorphism then every τ-cycle is cantorian.*

Proof:

Fix x; then $(\forall n \in \mathbb{N})((j\tau)^{Tn}(x) = j(\tau^n)(x))$. (This last observation holds for all permutations τ, not just automorphisms. It is stratified and can be proved by mathematical induction on ‘n’)

Now $\tau = j\tau$ whence $(\forall n \in \mathbb{N})(\tau^{Tn}(x) = \tau^n(x))$.

So, when n is the order of the τ-cycle containing x, $\tau^n(x) = x$.

So $\tau^{Tn}(x) = x$.

So $Tn = n$.

■

Can you cast an eye over this bit. I'm still quite bervous about it. And it's crucial!

2 The Situation in NFU

Space here for Wise Tho'rts from Professor Holmes.

3 Coda

It may be that there could be found something apparently weaker and simpler from which the second principle can be derived. The countable-or-finite pieces in the partitions of interest to us have extra structure, being cycles of a permutation. This can surely be put to good use. Let $\mathbb{P}$ be such a partition into cycles. By GC we can pick an "origin" in each cycle, and then every singleton $\{x\}$ can be given an "address" which is the ordered pair $\langle p, n\rangle$ where p is that element of $\mathbb{P}$ to which x belongs, and n is how far x is from the chosen origin of that piece. This shows that $T|V| \leq \aleph_0 \cdot |\mathbb{P}|$. But that doesn't seem to be enough to imply $T|V| = |\mathbb{P}|$. It would suffice if we had $\aleph_0 \cdot |\mathbb{P}| \leq |\mathbb{P}|$ but i see no way of getting that.

What is true is that the set of cardinals ϕ s.t. ϕ is the cardinality of a partition of V into countable pices is closed under multiplication by $\aleph_0$.

So we want $\aleph_0 \cdot |\mathbb{P}| = |\mathbb{P}|$.

References

[1] Thomas Forster "Set Theory with a Universal Set" Oxford Logic guides **20**. Oxford University Press 1992.

[2] Oystein Øre "Some Remarks on Commutators" Proceedings of the American Mathematical Society **2** No. 2 (Apr., 1951), pp. 307–314.

Stable URL: `http://www.jstor.org/stable/2032506` .

[3] Orey, S. "New Foundations and the Axiom of Counting". Duke Mathematical Journal **31**, (1964) pp. 655-660.