GCH implies AC locally

Yuval Paz

May 24, 2019

GCH has 2 standard (equivalent) form:

1. For all x and for all y, if $|X| \leq |Y| < \left|2^X\right|$ implies $|X| = |Y|$
2. For all $\aleph_\alpha$ aleph number, $2^{\aleph_\alpha} = \aleph_{\alpha+1}$

The easiest way to show the equivalence is to show that each implies AC independently from the other, and under ZFC those 2 are trivially equivalent.

Neither (1) nor (2) are easily imply AC, and each proof teachs a lot, I will prove that (1) implies AC.

My proof will be stronger result, I will prove that the implication is *locally.*

Definitions:

- CH($\mathfrak{m}$) : for all Y, $\mathfrak{m} \leq |Y| < 2^{\mathfrak{m}}$ implies $\mathfrak{m} = |Y|$
- GCH : $\mathfrak{m}$ is infinite implies CH($\mathfrak{m}$)
- WO($\mathfrak{m}$) : $\mathfrak{m} = |X|$ for some well orderable X
- AC : $\mathfrak{m}$ is a cardinal implies WO($\mathfrak{m}$)
- If A is a set A^* is the set of finite sequences of elements from A
- $\mathcal{P}(X)$: power set of X
- $\mathcal{O}(X)$: the set $\{R \subseteq X \times X \mid R \text{ is well ordering}\}$
- $\mathcal{W}(X)$: the set $\{A \subseteq X \mid A \text{ is well orderable}\}$
- $a_<$: the set of $<$-less elements $\{b \mid b < a\}$
- $\aleph(\mathfrak{m})$: Hartogs number; the least ordinal that does not inject to $\mathfrak{m}$; $\aleph(\mathfrak{m}) = \min(\alpha \in \text{Ord} \mid \alpha \nleq \mathfrak{m}) = \sup(\alpha \in \text{Ord} \mid \alpha \leq \mathfrak{m})$
- If $F : A \to B$ is a function $F^{-1} : \mathcal{P}(B) \to \mathcal{P}(A)$ is the pre-image function

The question of locally implication is: does CH($\mathfrak{m}$) implies WO($\mathfrak{m}$)?
This question, as far as I know, is still open.

But it is possible if instead of only assuming CH($\mathfrak{m}$) we also assume CH($2^{\mathfrak{m}}$)

Theorem 1(von Neumann, ZF**):** If $F : \mathcal{O}(X) \to X$ a function, then there exists unique $\prec \in \mathcal{O}(X)$ well order over W such that

1. if $w \in W$ then $F\left(\prec \cap w^2_{\prec}\right) = w$
2. $F(\prec) \in W$

This theorem is very interesting, which, in our case, only be useful for technical stuff, but it can gives very nice results very easily(for example you can use it to prove "AC implies well ordering" or cantor theorem in one line)

After the proof one may notice that replacing $\mathcal{O}(X)$ with any one of $\mathcal{W}(X) \setminus \{X\}, \mathcal{W}(X)$,$\mathcal{P}(X) \setminus \{X\}$,$\mathcal{P}(X)$ won't change the proof, which only increase the value of that theorem.

Proof: We call $Y \in \mathcal{W}(X)$ an F-set if there exists a well ordering that witness (1).

- There exists an F-set: $\{F(\emptyset)\}$
- If Y, Z are F-sets with R, S witnesses respectively then (Y, R) is an initial segment of (Z, S) or vice versa.

The proof of the second point goes like that: because both are well orders there exists order preserving injective from the smaller to the other(we know that "smaller" is well defined because they both well ordered), WOLG we may say $i : Y \to Z$ be that injective.

Let t be the R-minimal element such that $i(t) \neq t$, with that we get

$$t = F\left(R \cap t^2_R\right) = F\left(S \cap i(t)^2_S\right) = i(t)$$

Contradiction.

We close the proof by letting $\prec = \bigcup \{R \in \mathcal{O}(X) \mid R \text{ is a witness for an } F\text{-set}\}$, to show that $F(\prec) \in W$, suppose not, then adding $F(\prec)$ to be maximal element, this will result with F-set whose witness containing $\prec$ but not equal, contradiction. ■

Theorem 2(Halbeisen-Shela, ZF**):** If $\aleph_0 \leq |X|$ then $2^{|X|} \nleq |X^*|$.

This is probably the hardest part of the proof, originaly Specker proved that $2^{\mathfrak{m}} \nleq \mathfrak{m}^2$ for $\mathfrak{m} > 5$ and $n \cdot \mathfrak{m} < 2^{\mathfrak{m}}$ for all finite n, but because this theorem is both stronger is not hardered to prove, I will use it.

Proof: Assume that there exists injective $G : \mathcal{P}(X) \to X^*$, we will use G to define $F : \mathcal{O}(X) \to X$ and we will use that F.

Let $R \in \mathcal{O}(X)$, let say that $Y_{(R)}$ is the set on which R is well ordering, because $\left(Y_{(R)}, R\right)$ is well ordering there exists a definable bijective(definable-no need for choice, I won't prove that) $H_{(R)} : Y_{(R)} \to Y^*_{(R)}$, we define

$$D_{(R)} = \left\{x \in Y \mid x \notin G^{-1}\left(H_{(R)}(x)\right)\right\}$$

We notice that $G\left(D_{(R)}\right) \notin Y^*_{(R)}$, indeed if $G\left(D_{(R)}\right) \in Y^*_{(R)}$ then, because $H_{(R)}$ is bijective, there exists $t \in Y$ such that $H_{(R)}(t) = G\left(D_{(R)}\right)$ so $G^{-1}\left(H_{(R)}(t)\right) = D_{(R)}$ which result with

$$t \in G^{-1}\left(H_{(R)}(t)\right) \iff t \notin G^{-1}\left(H_{(R)}(t)\right)$$

Now we define $F(R)$ to be the R-minimal elements of $G\left(D_{(R)}\right)$ that is not in $Y_{(R)}$, with this constructure we have $F(R) \in X \setminus Y_{(R)}$ for all $R \in \mathcal{O}(X)$.

To complete the proof we use **theorem 1**, which states that there exists $\prec \in \mathcal{O}(X)$ above some Y such that $F(\prec) \in Y$, but we just proved that $F(\prec) \in X \setminus Y$, contradiction. ■

With the big theorem out of the way there is one more small theorem:

Theorem 3(ZF**):**

$$2^{\aleph(\mathfrak{m})} \leq 2^{2^{\mathfrak{m}^2}}$$

First we will see the connection between $\mathfrak{m}^2$ and elements bellow $\aleph(\mathfrak{m})$, then between $2^{\mathfrak{m}^2}$ and $\aleph(\mathfrak{m})$ and then we will prove the inequality:

Proof: Given a set X such that $|X| = \mathfrak{m}$ we may look at X^2 as a all the 2-tuples (a, b) such that both a and b are in X, but there is another way to look at it: X^2 is a relation on X that contains **every other relation on** X. Why is it so useful? Let κ be ordinal lesser than $\aleph(\mathfrak{m})$, then there exists injective $\kappa \to X$, that means that there exists $R \subseteq X^2$ which is of order type κ.

We chose κ arbitrarily from $< \aleph(\mathfrak{m})$, so there exists a surjective from $\mathcal{P}\left(X^2\right)$ to $\aleph(\mathfrak{m})$: given $R \subseteq X^2$, if it is well order send it to its' order type, elsewhere send it to $\emptyset$.

We will call the above surjective F, then F^{-1} is injective from $\mathcal{P}(\aleph(\mathfrak{m}))$ to $\mathcal{P}\left(\mathcal{P}\left(X^2\right)\right)$. ■

With that we are done with the hard parts, we will prove 2 quick lemmas about cardinal arithmetic and then we will proceed to the main part.

Lemma 1(ZF + CH$(\mathfrak{m})$**):**

1. $\mathfrak{m} = \mathfrak{m} + 1$
2. $\mathfrak{m} = \mathfrak{m} + \mathfrak{m}$
3. $\mathfrak{m} = \mathfrak{m}^2$

Proof:

1. $\mathfrak{m} \leq \mathfrak{m}+1 \leq 2^{\mathfrak{m}}$, but **theorem 2** proves that $\mathfrak{m}+1 \neq 2^{\mathfrak{m}}$ so $\mathfrak{m} \leq \mathfrak{m}+1 < 2^{\mathfrak{m}}$, by CH$(\mathfrak{m})$ we have $\mathfrak{m} = \mathfrak{m} + 1$. ■

2. $\mathfrak{m} \leq \mathfrak{m}+\mathfrak{m} \leq 2^{\mathfrak{m}}+2^{\mathfrak{m}} = 2^{\mathfrak{m}+1} = 2^{\mathfrak{m}}$, again, from **theorem 2**, $\mathfrak{m}+\mathfrak{m} \neq 2^{\mathfrak{m}}$ so by $\mathrm{CH}(\mathfrak{m})$ we have $\mathfrak{m} = \mathfrak{m}+\mathfrak{m}$. $\blacksquare$

3. $\mathfrak{m} \leq \mathfrak{m}\cdot\mathfrak{m} \leq 2^{\mathfrak{m}}\cdot 2^{\mathfrak{m}} = 2^{\mathfrak{m}+\mathfrak{m}} = 2^{\mathfrak{m}}$, again, from **theorem 2**, $\mathfrak{m}\cdot\mathfrak{m} \neq 2^{\mathfrak{m}}$ so by $\mathrm{CH}(\mathfrak{m})$ we have $\mathfrak{m} = \mathfrak{m}\cdot\mathfrak{m}$. $\blacksquare$

Lemma 2(ZF**):** If $\mathfrak{m}+\mathfrak{m} = \mathfrak{m}$ and $\mathfrak{m}+\mathfrak{n} = 2^{\mathfrak{m}}$ then $\mathfrak{n} = 2^{\mathfrak{m}}$

Proof: $\mathfrak{m}+\mathfrak{n} = 2^{\mathfrak{m}} = 2^{\mathfrak{m}+\mathfrak{m}} = 2^{\mathfrak{m}}\cdot 2^{\mathfrak{m}}$, let X, Y be sets such that $|X| = \mathfrak{m}$ and $|Y| = \mathfrak{n}$, also assume $X \cap Y = \emptyset$, let

$$F : \mathcal{P}(X) \times \mathcal{P}(X) \to X \cup Y$$

be bijective function.

Then there exists $X_0 \in \mathcal{P}(X)$ such that $(X_0, A) \notin F^{-1}(X)$ for all $A \in \mathcal{P}(X)$, if not we may look at $F\upharpoonright_{F^{-1}(X)}$, this is bijection between X and some subset of $\mathcal{P}(X) \times \mathcal{P}(X)$, but if we map (A, B) in that subset into A this is surjective to $\mathcal{P}(X)$, which means that there is surjective from X to $\mathcal{P}(X)$. That mean that the function $G : \mathcal{P}(X) \to Y$, $G(A) = F((X_0, A))$ is injective, so $2^{\mathfrak{m}} \leq \mathfrak{n}$, but $2^{\mathfrak{m}} = \mathfrak{m}+\mathfrak{n} \geq \mathfrak{n}$. $\blacksquare$

Theorem 4(ZF + CH$(\mathfrak{m})$ + CH$(2^{\mathfrak{m}})$**):** WO$(\mathfrak{m})$ and WO$(2^{\mathfrak{m}})$

Proof: We know that

$$2^{\aleph(\mathfrak{m})} \leq 2^{2^{\mathfrak{m}^2}} = 2^{2^{\mathfrak{m}}}$$

and we have

$$2^{\mathfrak{m}} \leq 2^{\mathfrak{m}} + \aleph(\mathfrak{m}) < 2^{2^{\mathfrak{m}}+\aleph(\mathfrak{m})} = 2^{2^{\mathfrak{m}}} \cdot 2^{\aleph(\mathfrak{m})} \leq 2^{2^{\mathfrak{m}}} \cdot 2^{2^{\mathfrak{m}}} = 2^{2^{\mathfrak{m}}+2^{\mathfrak{m}}} = 2^{2^{\mathfrak{m}}}$$

in short

$$2^{\mathfrak{m}} \leq 2^{\mathfrak{m}} + \aleph(\mathfrak{m}) < 2^{2^{\mathfrak{m}}}$$

So by CH$(2^{\mathfrak{m}})$ we have $2^{\mathfrak{m}} = 2^{\mathfrak{m}} + \aleph(\mathfrak{m})$, but also

$$\mathfrak{m} < \mathfrak{m} + \aleph(\mathfrak{m}) \leq 2^{\mathfrak{m}} + \aleph(\mathfrak{m}) = 2^{\mathfrak{m}}$$

So by CH$(\mathfrak{m})$ we have $\mathfrak{m} + \aleph(\mathfrak{m}) = 2^{\mathfrak{m}}$, CH$(\mathfrak{m})$+**lemma 2** gives $\aleph(\mathfrak{m}) = 2^{\mathfrak{m}}$, but $\aleph(\mathfrak{m})$ is defined as an ordinal, so WO$(2^{\mathfrak{m}})$, now to see that WO$(\mathfrak{m})$ let X be a set such that $|X| = \mathfrak{m}$, then let $\prec$ be the well ordering of $\mathcal{P}(X)$, and define on X the order: $a < b \iff \{a\} \prec \{b\}$. $\blacksquare$

Theorem 5(ZF + GCH**):** AC

Proof: Given a set A be infinite, by GCH we have CH$(|A|)$ and CH$\left(2^{|A|}\right)$, by **theorem 4** WO$(|A|)$. $\blacksquare$