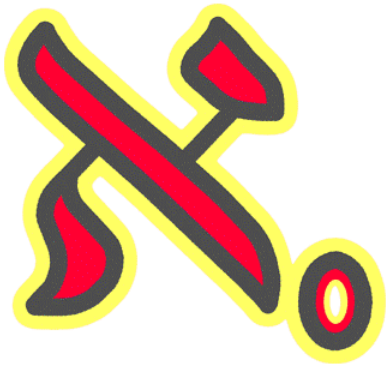

GCH implies AC
a Metamath Formalization

MARIO CARNEIRO

22 JULY 2015

What is Metamath?

- A computer language for representing mathematical proofs
  - The Metamath spec is two pages, one verifier exists in ≈300 lines of Python
  - Eight independent verifiers exist in eight different languages
  - Two proof assistants (MM-PA and mmj2) with another (smm) in development
- A project to formalize modern mathematics from a simple foundation
- Four major databases
  - ZFC set theory (set.mm)
    - Over 25000 proofs, 500K lines, 24M file
  - HOL type theory (hol.mm)
  - Intuitionistic logic (iset.mm)
  - NF set theory (nf.mm)
    - Including Specker's proof of $\neg\mathrm{AC}$

What is GCH?

- The Generalized Continuum Hypothesis

1) $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ for every ordinal α
2) There are no infinite cardinals $\mathfrak{m} < \mathfrak{n} < 2^{\mathfrak{m}}$

- Equivalence of (1) and (2) needs the axiom of regularity, which we prefer to avoid when possible – we use definition (2)

Localizing GCH

- The Generalized Continuum Hypothesis

1) $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ for every ordinal α
2) There are no infinite cardinals $\mathfrak{m} < \mathfrak{n} < 2^{\mathfrak{m}}$

- Equivalence of (1) and (2) needs the axiom of regularity, which we prefer to avoid when possible – we use definition (2)
- Define a GCH-set to be a cardinal $\mathfrak{m}$ that is finite or satisfies $\neg(\mathfrak{m} < \mathfrak{n} < 2^{\mathfrak{m}})$ for all cardinals $\mathfrak{n}$
  - Often written $\mathrm{CH}(\mathfrak{m})$, Metamath notation is $\mathfrak{m} \in \mathrm{GCH}$
  - Then GCH is equivalent to "every set is a GCH-set", written $\mathrm{GCH} = \mathrm{V}$

$$\mathrm{GCH} = \mathrm{Fin} \cup \{x | \forall y \, \neg(x \prec y \wedge y \prec \mathcal{P}x)\}$$

What is AC?

- The Axiom of Choice
- Many equivalent formulations
- The one useful to us is “every set is well-orderable/equinumerous to an ordinal”
- Metamath notation for “A is well-orderable” is $A \in \mathrm{dom}\,\mathrm{card}$ because the cardinality function is only defined on sets equinumerous to an ordinal

$$\mathrm{CHOICE} \leftrightarrow \mathrm{dom}\,\mathrm{card} = \mathrm{V}$$

GCH implies AC

- Written in Metamath notation as $\mathrm{GCH} = \mathrm{V} \rightarrow \mathrm{CHOICE}$
- What does a local version look like?
- Specker (1954): If $\mathfrak{m}$ is infinite and $\mathrm{CH}(\mathfrak{m})$, $\mathrm{CH}(2^{\mathfrak{m}})$, then $2^{\mathfrak{m}} = \aleph(\mathfrak{m})$, so $\mathfrak{m}$ is well-orderable
  - $\aleph(\mathfrak{m})$ is the Hartogs number of $\mathfrak{m}$, the set of all ordinals $\leq \mathfrak{m}$

$$\mathrm{har} = (x \mapsto \{y \in \mathrm{On} | y \preccurlyeq x\})$$

  - Metamath version (completed 31 May 2015):

$$\omega \preccurlyeq A \wedge A \in \mathrm{GCH} \wedge \mathcal{P}(A) \in \mathrm{GCH} \rightarrow \mathrm{har}(A) \approx \mathcal{P}(A)$$

- The source for this work was “Does GCH imply AC locally?” by Akihiro Kanamori and David Pincus (2002)
  - http://math.bu.edu/people/aki/7.pdf
- Aside: Not many formal systems could even state this theorem (HOL too weak, Mizar too strong)

GCH implies AC

http://us.metamath.org/mpegif/gchhar.html

Home

Metamath Proof Explorer

< Previous Next >
Related theorems
Unicode version

Theorem gchhar 7513

Description: A "local" form of gchac 7515. If A and $\mathcal{P} A$ are GCH-sets, then the Hartogs number of A is $\mathcal{P} A$ (so $\mathcal{P} A$ and a fortiori A are well-orderable). The proof is due to Specker. Theorem 2.1 of [KanamoriPincus] p. 419. (Contributed by Mario Carneiro, 31-May-2015.)

Assertion

Ref	Expression
gchhar	$\vdash ((\omega \preccurlyeq A \wedge A \in \mathrm{GCH} \wedge \mathcal{P} A \in \mathrm{GCH}) \rightarrow (\mathrm{har}`A) \approx \mathcal{P} A)$

Canonical Constructions

- Specker's proof (via Kanamori & Pincus) uses the lemma that $\mathrm{CH}(\mathfrak{m})$ implies $\mathfrak{m} + \mathfrak{m} = \mathfrak{m}^2 = \mathfrak{m}$
  - If it were not the case, then $2^{\mathfrak{m}} \leq \mathfrak{m}^2 \leq \mathrm{Seq}(\mathfrak{m})$ where $\mathrm{Seq}(\mathfrak{m})$ is the set of finite sequences
- Halbeisen & Shelah (1994): If $\omega \leq X$ then $2^{|X|} \not\leq |\mathrm{Seq}(X)|$
  - Requires a bijection (or at least an injection) $F_\alpha : \mathrm{Seq}(\alpha) \to \alpha$
  - "For infinite, well-orderable Y, we have $|Y| = |\mathrm{Seq}(Y)|$; in fact, to every infinite well-ordering of a set Y we can canonically associate a bijection between Y and $\mathrm{Seq}(Y)$." – Kanamori & Pincus
    - This is the sort of thing that makes a formalizer's job hard!
- This bijection is Corollary 3 of Halbeisen & Shelah:
  - "Proof: Use the Cantor Normal Form Theorem, Corollary 2, order the finite subsets of α and then use the Cantor-Bernstein Theorem."

Cantor Normal Form

- Textbook version:
  Every ordinal number α can be uniquely written as $\omega^{\beta_1} c_1 + \omega^{\beta_2} c_2 + \cdots + \omega^{\beta_k} c_k$, where k is a natural number, $c_1, c_2, \ldots, c_k$ are positive integers, and $\beta_1 > \beta_2 > \cdots > \beta_k \geq 0$ are ordinal numbers. (Wikipedia)
- Metamath version (cantnf):
  Define the map $\mathrm{CNF}_{\alpha,\beta}$ from the set $\alpha^{\beta}_{\mathrm{Fin}}$ of finitely supported functions $f : \beta \to \alpha$ to the ordinal exponential α^{β} as $\mathrm{CNF}_{\alpha,\beta}(f) = \sum_{\gamma \in \mathrm{supp}(f)} \alpha^{\gamma} f(\gamma)$. Then $\mathrm{CNF}_{\alpha,\beta}$ is a bijection, and in fact an order isomorphism from $(\alpha^{\beta}_{\mathrm{Fin}}, \lhd)$ to $(\alpha^{\beta}, \in)$ (where $f \lhd g$ when $f \neq g$ and the maximal γ with $f(\gamma) \neq g(\gamma)$ satisfies $f(\gamma) < g(\gamma)$).
  - It is easier for us to work with finitely supported function spaces than parallel sequences

Reversing Cantor Normal Form

- Corollary 2 of Halbeisen & Shelah
  - If $\alpha = \omega^{\beta_1} c_1 + \omega^{\beta_2} c_2 + \cdots + \omega^{\beta_k} c_k$, then defining $\check{\alpha} = \omega^{\beta_k} c_k + \cdots + \omega^{\beta_2} c_2 + \omega^{\beta_1} c_1$, $\alpha \approx \check{\alpha}$
- Ordinal absorption laws:
  - $\alpha + \beta = \beta$ when $\alpha < \omega^\gamma \leq \beta$
  - $\alpha\omega^\gamma = \omega^\gamma$ when $0 < \alpha < \omega$ and $0 < \gamma$
- Ordinal equinumerosity laws:
  - $\alpha + \beta \approx \alpha \sqcup \beta \approx \beta + \alpha$
  - $\alpha\beta \approx \alpha \times \beta \approx \beta\alpha$
  - $\alpha^\beta_{\mathrm{Fin}} \approx \alpha^\beta$ (Cantor normal form), so $\alpha \approx \alpha'$ and $\beta \approx \beta'$ implies $\alpha^\beta \approx \alpha'^{\beta'}$
- Important: all equinumerosity relations here are canonical – $\alpha \approx \beta$ here actually means $F: \alpha \to \beta$ is a bijection where F is some complicated term

Reversing Cantor Normal Form

- Corollary 2 of Halbeisen & Shelah
  - If $\alpha = \omega^{\beta_1} c_1 + \omega^{\beta_2} c_2 + \cdots + \omega^{\beta_k} c_k$, then defining $\bar{\alpha} = \omega^{\beta_k} c_k + \cdots + \omega^{\beta_2} c_2 + \omega^{\beta_1} c_1$, $\alpha \approx \bar{\alpha}$
- Ordinal absorption laws:
  - $\alpha + \beta = \beta$ when $\alpha < \omega^\gamma \leq \beta$
  - $\alpha\omega^\gamma = \omega^\gamma$ when $0 < \alpha < \omega$ and $0 < \gamma$
- The ordinal absorption laws imply $\alpha \approx \bar{\alpha} = \omega^{\beta_k} c_k \approx c_k \omega^{\beta_k} = \omega^{\beta_k}$, so every ordinal is (definably) equinumerous to a power of ω

Reversing Cantor Normal Form

Theorem cnfcom3 6672

Description: Any infinite ordinal B is equinumerous to a power of ω. (We are being careful here to show explicit bijections rather than simple equinumerosity because we want a uniform construction for cnfcom3c 6674.) (Contributed by Mario Carneiro, 30-May-2015.)

Hypotheses

Ref	Expression
cnfcom.s	$\vdash S = \mathrm{dom}\,(\omega \mathrm{CNF}\ A)$
cnfcom.a	$\vdash (\varphi \rightarrow A \in \mathrm{On})$
cnfcom.b	$\vdash (\varphi \rightarrow B \in (\omega \uparrow_o A))$
cnfcom.f	$\vdash F = (\smile(\omega \mathrm{CNF}\ A)`B)$
cnfcom.g	$\vdash G = \mathrm{OrdIso}(\mathrm{E}, (\smile F``(\mathrm{V} \setminus 1_o)))$
cnfcom.h	$\vdash H = \mathrm{seq}_\omega((k \in \mathrm{V}, z \in \mathrm{V} \mapsto (M +_o z)), \varnothing)$
cnfcom.t	$\vdash T = \mathrm{seq}_\omega((k \in \mathrm{V}, f \in \mathrm{V} \mapsto K), \varnothing)$
cnfcom.m	$\vdash M = ((\omega \uparrow_o (G`k)) \cdot_o (F`(G`k)))$
cnfcom.k	$\vdash K = ((x \in M \mapsto (\mathrm{dom}\ f +_o x)) \cup \smile(x \in \mathrm{dom}\ f \mapsto (M +_o x)))$
cnfcom.w	$\vdash W = (G`\bigcup \mathrm{dom}\ G)$
cnfcom3.1	$\vdash (\varphi \rightarrow \omega \subseteq B)$
cnfcom.x	$\vdash X = (u \in (F`W), v \in (\omega \uparrow_o W) \mapsto (((F`W) \cdot_o v) +_o u))$
cnfcom.y	$\vdash Y = (u \in (F`W), v \in (\omega \uparrow_o W) \mapsto (((\omega \uparrow_o W) \cdot_o u) +_o v))$
cnfcom.n	$\vdash N = ((X \circ \smile Y) \circ (T`\mathrm{dom}\ G))$

Assertion

Ref	Expression
cnfcom3	$\vdash (\varphi \rightarrow N : B \underset{\text{onto}}{1\text{-}1} (\omega \uparrow_o W))$

Theorem cnfcom3c 6674

Description: Wrap the construction of cnfcom3 6672 into an existence quantifier. For any $\omega \subseteq b$, there is a bijection from b to some power of ω. Furthermore, this bijection is *canonical* , which means that we can find a single function g which will give such bijections for every b less than some arbitrarily large bound A. (Contributed by Mario Carneiro, 30-May-2015.)

Assertion

Ref	Expression
cnfcom3c	$\vdash (A \in \mathrm{On} \rightarrow \exists g \forall b \in A\, (\omega \subseteq b \rightarrow \exists w \in (\mathrm{On} \setminus 1_o)(g`b) : b \underset{\text{onto}}{1\text{-}1} (\omega \uparrow_o w)))$

$\alpha \times \alpha \approx \alpha$, definably

$$\alpha \times \alpha \approx \omega^{\gamma} \times \omega^{\gamma} \approx \omega^{\gamma 2} \approx \omega^{2\gamma} = (\omega^2)^{\gamma} \approx \omega^{\gamma} \approx \alpha$$

- The real proof uses definable bijections instead of equinumerosity (existence of a bijection)
  - Compare:

Theorem infxpen 6892

Description: Every infinite ordinal is equinumerous to its cross product. Proposition 10.39 of [TakeutiZaring] p. 94, whose proof we follow closely. The key idea is to show that the relation R is a well-ordering of $(\mathrm{On} \times \mathrm{On})$ with the additional property that R-initial segments of $(x \times x)$ (where x is a limit ordinal) are of cardinality at most x. (Contributed by Mario Carneiro, 9-Mar-2013.)

Assertion

Ref	Expression
infxpen	$\vdash ((A \in \mathrm{On} \wedge \omega \subseteq A) \rightarrow (A \times A) \approx A)$

Theorem infxpenc2 6899

Description: Existence form of infxpenc 6895. A "uniform" or "canonical" version of infxpen 6892, asserting the existence of a single function g that simultaneously demonstrates product idempotence of all ordinals below a given bound. (Contributed by Mario Carneiro, 30-May-2015.)

Assertion

Ref	Expression
infxpenc2	$\vdash (A \in \mathrm{On} \rightarrow \exists g \forall b \in A\,(\omega \subseteq b \rightarrow (g\text{`}b):(b \times b)\underset{\text{onto}}{\overset{1\text{-}1}{\rightarrow}}b))$

$\alpha \times \alpha \approx \alpha$, definably

$$\alpha \times \alpha \approx \omega^\gamma \times \omega^\gamma \approx \omega^{\gamma 2} \approx \omega^{2\gamma} = (\omega^2)^\gamma \approx \omega^\gamma \approx \alpha$$

- The real proof uses definable bijections instead of equinumerosity (existence of a bijection)
- We can use this to construct an injection from $\mathrm{Seq}(\alpha) \to \alpha$ by recursion, given a bijection $g: \alpha \times \alpha \to \alpha$:

$$f(\langle\rangle) = g(0,0) \qquad f(\langle\alpha_1, \alpha_2, \dots, \alpha_k\rangle) = g\big(k, g(f(\langle\alpha_1, \alpha_2, \dots, \alpha_{k-1}\rangle), \alpha_k)\big)$$

The de Bruijn Factor

- The *de Bruijn factor* is the quotient of the size of a formalization of a mathematical text and the size of its informal original (Wiedijk)
- Because this project was principally the near-complete formalization of a single text (Kanamori & Pincus), it is possible to calculate a de Bruijn factor for the work
  - Because the TeX for Kanamori & Pincus was not available, Google OCR of the PDF was used instead, which may make the calculated factors higher than they should be since some formatting was lost
- Metamath has a surprisingly low de Bruijn factor! (Compare intrinsic factors 3.1, 3.7, 4.1 from [Wiedijk])
  - Why?

	informal	formal	de Bruijn Factor	
uncompressed	18092	60106	apparent	3.32
compressed	7545	19579	intrinsic	2.59

Questions