An Introduction to Reverse Mathematics

Noah A. Hughes
Appalachian State University
Boone, NC

March 28, 2014

Appalachian State University
Mathematical Sciences Colloquium Series

Outline

- Preliminary Definitions
- Motivations
- Reverse mathematics
- Constructing the *big five* subsystems
- Original results regarding *marriage theorems*

Preliminaries

An **axiom system** is a set of mathematical statements we take as true. We then use the *axioms* to deduce mathematical theorems.

Example: ZFC is the standard foundation for mathematics.

Example: The *Peano axioms* are nine statements which define the natural numbers.

Preliminaries

An **axiom system** is a set of mathematical statements we take as true. We then use the *axioms* to deduce mathematical theorems.

Example: ZFC is the standard foundation for mathematics.

Example: The *Peano axioms* are nine statements which define the natural numbers.

If we can prove a theorem φ in an axiom system $\mathfrak{T}$ then we write

$$\mathfrak{T} \vdash \varphi.$$

If φ requires an additional axiom A (along with those in $\mathfrak{T}$) to be proven we write

$$\mathfrak{T} + A \vdash \varphi \qquad \longleftrightarrow \qquad \mathfrak{T} \vdash A \Rightarrow \varphi.$$

Preliminaries

We build **formulas** from the three atomic formula

$$x = y, x < y, x \in X,$$

using logical connectives and quantifiers.

Logical Connectives:

$$\rightarrow, \leftrightarrow, \neg, \bigwedge, \bigvee$$

Quantifiers:

$$\exists x\,, \forall y\,, \exists X\,, \forall Y$$

<u>Example:</u>

$$x \in X \leftrightarrow \exists y\,(x = 2 \cdot y).$$

A Question

How do theorems relate in mathematics?

A Question

How do theorems relate in mathematics?

Suppose we have two mathematical theorems φ_1 and φ_2 that we would like to compare.

$\rightarrow$ What does it mean to say φ_1 is “stronger” than φ_2?

$\rightarrow$ Or to say φ_1 and φ_2 are “equivalent”?

$\rightarrow$ Can we determine if these theorems are even *comparable* or are they independent of each other?

$\rightarrow$ What if φ_1 and φ_2 are from different areas of mathematics?

A Possible Strategy

Suppose we have a substantially weak axiom system $\mathfrak{B}$ (the *base theory*) that proves φ_1 but not does not prove φ_2:

$$\mathfrak{B} \vdash \varphi_1 \qquad\qquad \mathfrak{B} \nvdash \varphi_2.$$

A Possible Strategy

Suppose we have a substantially weak axiom system $\mathfrak{B}$ (the *base theory*) that proves φ_1 but not does not prove φ_2:

$$\mathfrak{B} \vdash \varphi_1 \qquad\qquad \mathfrak{B} \nvdash \varphi_2.$$

If we find an additional axiom A_1 and show that

$$\mathfrak{B} + A_1 \vdash \varphi_2,$$

then we may conclude φ_2 is logically stronger than φ_1.

A Possible Strategy

Suppose we have a substantially weak axiom system $\mathfrak{B}$ (the *base theory*) that proves φ_1 but not does not prove φ_2:

$$\mathfrak{B} \vdash \varphi_1 \qquad\qquad \mathfrak{B} \nvdash \varphi_2.$$

If we find an additional axiom A_1 and show that

$$\mathfrak{B} + A_1 \vdash \varphi_2,$$

then we may conclude φ_2 is logically stronger than φ_1.

This is a rough measure of logical strength. A_1 may be wildly powerful and give us little insight into the difference in φ_1 and φ_2

“Reversing” mathematics for a better measure

Because $\mathfrak{B} + A_1 \vdash \varphi_2$ we already know

$$\mathfrak{B} \vdash A_1 \Rightarrow \varphi_2.$$

Suppose we can show $\mathfrak{B} + \varphi_2 \vdash A_1$, that is,

$$\mathfrak{B} \vdash \varphi_2 \Rightarrow A_1.$$

“Reversing” mathematics for a better measure

Because $\mathfrak{B} + A_1 \vdash \varphi_2$ we already know

$$\mathfrak{B} \vdash A_1 \Rightarrow \varphi_2.$$

Suppose we can show $\mathfrak{B} + \varphi_2 \vdash A_1$, that is,

$$\mathfrak{B} \vdash \varphi_2 \Rightarrow A_1.$$

This is called *reversing* the theorem φ_2 to the axiom A_1.

“Reversing” mathematics for a better measure

Because $\mathfrak{B} + A_1 \vdash \varphi_2$ we already know

$$\mathfrak{B} \vdash A_1 \Rightarrow \varphi_2.$$

Suppose we can show $\mathfrak{B} + \varphi_2 \vdash A_1$, that is,

$$\mathfrak{B} \vdash \varphi_2 \Rightarrow A_1.$$

This is called *reversing* the theorem φ_2 to the axiom A_1.

We can now conclude that A_1 and φ_2 are *provably equivalent* over the base theory $\mathfrak{B}$, *i.e.*

$$\mathfrak{B} \vdash A_1 \iff \varphi_2.$$

Extending this classification

Let's consider a third theorem φ_3.

Suppose after some analysis we find another axiom A_2 differing from A_1 such that

$$\mathfrak{B} \vdash A_2 \iff \varphi_3.$$

What can we conclude about the relationships between our three theorems φ_1, φ_2 and φ_3?

Extending this classification

Let's consider a third theorem φ_3.

Suppose after some analysis we find another axiom A_2 differing from A_1 such that

$$\mathfrak{B} \vdash A_2 \iff \varphi_3.$$

What can we conclude about the relationships between our three theorems φ_1, φ_2 and φ_3?

To determine the relationship between φ_2 and φ_3 we need to know how A_1 and A_2 compare.

Is this a good strategy?

Is this a good strategy?

Possible complications:

- It may be extremely difficult to determine the relationship between two axioms.
- The theorems of mathematics are extremely diverse. As we consider more theorems we may need more and more axioms to determine their logical strength.
- Each of these axioms may only classify a small number of theorems.

Is this a good strategy?

Possible complications:

- It may be extremely difficult to determine the relationship between two axioms.
- The theorems of mathematics are extremely diverse. As we consider more theorems we may need more and more axioms to determine their logical strength.
- Each of these axioms may only classify a small number of theorems.

In short, this could become a real mess.

It is! (Surprisingly)

It turns out that with the specific base theory RCA_0 we need only **four** additional axioms (A_1, A_2, A_3, A_4) to classify an *enormous* amount of mathematical theorems.

We call RCA_0 and the four axiom systems which are obtained from appending A_1, A_2, A_3 or A_4 to the base theory the *big five:*

$$\mathrm{RCA}_0 \qquad \mathrm{WKL}_0 \qquad \mathrm{ACA}_0 \qquad \mathrm{ATR}_0 \qquad \Pi^1_1-\mathrm{CA}_0.$$

It is! (Surprisingly)

It turns out that with the specific base theory RCA_0 we need only **four** additional axioms (A_1, A_2, A_3, A_4) to classify an *enormous* amount of mathematical theorems.

We call RCA_0 and the four axiom systems which are obtained from appending A_1, A_2, A_3 or A_4 to the base theory the *big five:*

$$\mathrm{RCA}_0 \qquad \mathrm{WKL}_0 \qquad \mathrm{ACA}_0 \qquad \mathrm{ATR}_0 \qquad \Pi^1_1 - \mathrm{CA}_0.$$

Reverse mathematics is the program dedicated to classifying the logical strength of mathematical theorems via these five axiom systems.

Reverse mathematics

$$\mathrm{RCA}_0 \qquad \mathrm{WKL}_0 \qquad \mathrm{ACA}_0 \qquad \mathrm{ATR}_0 \qquad \Pi^1_1 - \mathrm{CA}_0$$

Each is a *weak* subsystem of *second order arithmetic*.

The strength of each system is measured by the amount of *set comprehension* available.

Example: Take our three theorems φ_1, φ_2 and φ_3. If we show

$$\mathrm{RCA}_0 \vdash \varphi_1$$

$$\mathrm{RCA}_0 \vdash \mathrm{WKL}_0 \iff \varphi_2$$

$$\mathrm{RCA}_0 \vdash \mathrm{ACA}_0 \iff \varphi_3,$$

we know the theorems compare in terms of logical strength.

Second Order Arithmetic

Denoted $\mathbf{Z}_2$.

Language:
Number variables: x, y, z Set variables: X, Y, Z

basic arithmetic axioms

$$n+1 \neq 0$$
$$m+1 = n+1 \rightarrow m = n$$
$$m+0 = m$$
$$m+(n+1) = (m+n)+1$$
$$m \cdot 0 = 0$$
$$m \cdot (n+1) = (m \cdot n) + m$$
$$\neg\, m < 0$$
$$m < n+1 \leftrightarrow (m < n \vee m = n)$$

Second Order Arithmetic

Denoted $\mathbf{Z}_2$.

Language:
Number variables: x, y, z Set variables: X, Y, Z

basic arithmetic axioms
(0, 1, +, $\times$, =, and $<$ behave as usual.)

Second Order Arithmetic

Denoted $\mathbf{Z}_2$.

Language:
Number variables: x, y, z Set variables: X, Y, Z

basic arithmetic axioms
(0, 1, +, $\times$, =, and $<$ behave as usual.)

The second order induction scheme
$(\psi(0) \wedge \forall n\,(\psi(n) \rightarrow \psi(n+1))) \rightarrow \forall n\,\psi(n)$
where $\psi(n)$ is any *formula* in $\mathbf{Z}_2$.

Second Order Arithmetic

Denoted $\mathbf{Z}_2$.

Language:
Number variables: x, y, z Set variables: X, Y, Z

basic arithmetic axioms
(0, 1, +, $\times$, =, and $<$ behave as usual.)

The second order induction scheme
$(\psi(0) \wedge \forall n\,(\psi(n) \to \psi(n+1))) \to \forall n\,\psi(n)$
where $\psi(n)$ is any *formula* in $\mathbf{Z}_2$.

Set comprehension

$$\exists X\,\forall n\,(n \in X \leftrightarrow \varphi(n))$$

where $\varphi(n)$ is any formula of $\mathbf{Z}_2$ in which X does not occur freely.

Recursive Comprehension and RCA_0

RCA_0 is the subsystem of $\mathbf{Z}_2$ whose axioms are:

basic arithmetic axioms

Restricted induction

$$(\psi(0) \wedge \forall n\,(\psi(n) \rightarrow \psi(n+1))) \rightarrow \forall n\,\psi(n)$$

where $\psi(n)$ has (at most) one number quantifier.

Recursive set comprehension

Recursive or *computable* sets exist.

Coding

In $\mathbf{Z}_2$ we can only speak of natural numbers and sets of natural numbers but we can *encode* a surprising amount of mathematics using only these tools.

Coding

In $\mathbf{Z}_2$ we can only speak of natural numbers and sets of natural numbers but we can *encode* a surprising amount of mathematics using only these tools.

The *pairing map*:

$$(i, j) = (i + j)^2 + i.$$

This encodes pairs as a single natural number:

$$(2, 3) = (2 + 3)^2 + 2 = 27 \qquad (0, 17) = (0 + 17)^2 + 0 = 17^2$$

Coding

In $\mathbf{Z}_2$ we can only speak of natural numbers and sets of natural numbers but we can *encode* a surprising amount of mathematics using only these tools.

The *pairing map*:

$$(i, j) = (i + j)^2 + i.$$

This encodes pairs as a single natural number:

$$(2, 3) = (2 + 3)^2 + 2 = 27 \qquad (0, 17) = (0 + 17)^2 + 0 = 17^2$$

We can use sets of pairs to describe a function or a countable sequence.

Coding

In $\mathbf{Z}_2$ we can only speak of natural numbers and sets of natural numbers but we can *encode* a surprising amount of mathematics using only these tools.

The *pairing map*:

$$(i, j) = (i + j)^2 + i.$$

This encodes pairs as a single natural number:

$$(2, 3) = (2 + 3)^2 + 2 = 27 \qquad (0, 17) = (0 + 17)^2 + 0 = 17^2$$

We can use sets of pairs to describe a function or a countable sequence.

Encoding a triple:
$(2, 3, 4) = ((2, 3), 4) = (27, 4) = (27 + 4)^2 + 27$

Coding

$\mathbf{Z}_2$ is remarkably expressive.

Within RCA_0 we may construct the number system of the integers $\mathbb{Z}$.

Coding

$\mathbf{Z}_2$ is remarkably expressive.

Within RCA_0 we may construct the number system of the integers $\mathbb{Z}$.

Using the pairing map, we identify the (code for the) pair (m, n) with the integer $m - n$.

To define arithmetic on $\mathbb{Z}$ we make several definitions for "$\mathbb{Z}$ arithmetic" on these pairs.

$$\begin{aligned}
(m,n) +_{\mathbb{Z}} (p,q) &= (m+p, n+q) \\
(m,n) -_{\mathbb{Z}} (p,q) &= (m+q, n+p) \\
(m,n) \cdot_{\mathbb{Z}} (p,q) &= (m \cdot p + n \cdot q, m \cdot q + n \cdot p) \\
(m,n) <_{\mathbb{Z}} (p,q) &\leftrightarrow m+q < n+p \\
(m,n) =_{\mathbb{Z}} (p,q) &\leftrightarrow m+q = n+p
\end{aligned}$$

Coding

We can encode much more within RCA_0, including:

- The rational numbers.
- Real numbers.
- Countable abelian groups and vector spaces.
- Continuous real-valued functions.
- Complete separable metric spaces.

How strong is RCA_0?

Theorem

The following are provable in RCA_0*.*

(i) *The system* $\mathbb{Q}, +, -, \cdot, 0, 1, <$ *is an ordered field. (Simpson)*

(ii) *The uncountability of* $\mathbb{R}$*. (Simpson)*

(iii) *The intermediate value theorem on continuous real-valued functions. If* $f(x)$ *is a continuous real-valued function on the unit interval* $0 \leqslant x \leqslant 1$ *and* $f(0) < 0 < f(1)$*, then there exists* c *such that* $0 < c < 1$ *and* $f(c) = 0$*. (Simpson)*

(iv) *Basics of real linear algebra, including Gaussian Elimination. (Simpson)*

How strong is RCA_0?

Theorem

The following are **not** *provable in* RCA_0*.*

(i) *The maximum principle: Every continuous real-valued function on* $[0,1]$ *attains a supremum. (Simpson)*

(ii) *For every continuous function* $f(x)$ *on a closed bounded interval* $a \leqslant x \leqslant b$*, the Riemann integral* $\int_a^b f(x)dx$ *exists and is finite. (Simpson)*

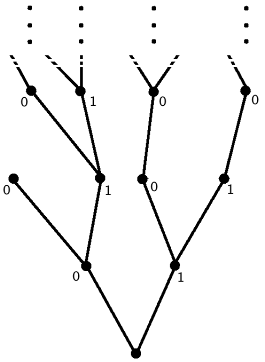
So we see RCA_0 does not prove everything. This is desirable.

Weak König's Lemma and WKL_0

The next subsystem of $\mathbf{Z}_2$ is obtained by appending *weak König's lemma* to RCA_0.

Weak König's lemma states that:

If T is an infinite binary tree, then T contains an infinite path.

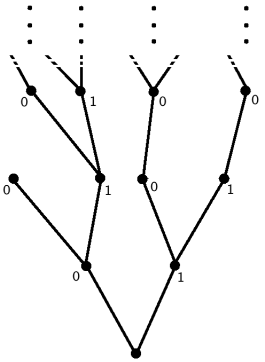


Weak König's Lemma and WKL_0

The next subsystem of $\mathbf{Z}_2$ is obtained by appending *weak König's lemma* to RCA_0.

Weak König's lemma states that:

If T is an infinite binary tree, then T contains an infinite path.



So weak König's lemma basically says:

"Big, skinny trees are tall."

$\mathsf{RCA}_0 \nvdash$ weak König's lemma

How strong is WKL_0?

Theorem

One can prove the following statements equivalent to WKL_0 *over* RCA_0.

(i) *The maximum principle: Every continuous real-valued function on* $[0, 1]$ *attains a supremum. (Simpson)*

(ii) *Every continuous real-valued function on* $[0, 1]$ *is bounded. (Simpson)*

(iii) *For every continuous function* $f(x)$ *on a closed bounded interval* $a \leqslant x \leqslant b$*, the Riemann integral* $\int_a^b f(x)dx$ *exists and is finite. (Simpson)*

(iv) *Every countable field has a unique algebraic closure. (Friedman, Simpson, and Smith)*

(v) Peano's existence theorem *for solutions to ODEs. (Simpson)*

Arithmetical Comprehension and ACA_0

ACA_0 is RCA_0 plus comprehension for arithmetically definable sets.

The arithmetical comprehension scheme:

> For any formula $\theta(n)$ with only number quantifiers, the set $\{n \in \mathbb{N} \mid \theta(n)\}$.

Note: $\mathsf{WKL}_0 \nvdash \mathsf{ACA}_0$ but $\mathsf{ACA}_0 \vdash \mathsf{WKL}_0$.

How strong is ACA_0?

Theorem

One can prove the following statements equivalent to ACA_0 *over* RCA_0.

(i) *Cauchy sequences converge. (Simpson)*

(ii) *The Bolzano/Weierstraß theorem: Every bounded sequence of real numbers contains a convergent subsequence. (Friedman)*

(iii) *The Ascoli lemma. (Simpson)*

(iv) *Ramsey's theorem for triples. (Simpson)*

Arithmetical Transfinite Recursion and ATR_0

ATR_0 consists of RCA_0 plus axioms which allow for iteration of arithmetical comprehension along any well ordering. This allows transfinite constructions.

This system is *vastly* stronger than ACA_0.

Arithmetical Transfinite Recursion and ATR_0

ATR_0 consists of RCA_0 plus axioms which allow for iteration of arithmetical comprehension along any well ordering. This allows transfinite constructions.

This system is *vastly* stronger than ACA_0.

Theorem

One can prove the following statements equivalent to ATR_0 *over* RCA_0*.*

(i) *Any two well orderings are comparable. (Friedman)*

(ii) *Every countable reduced Abelian p-group has an Ulm resolution. (Friedman, Simpson, and Smith)*

(iii) Sherman's Inequality: *If* α, β *and* γ *are countable well orderings, then* $(\alpha + \beta)\gamma \leqslant \alpha\gamma + \beta\gamma$*. (Hirst)*

Π^1_1 Comprehension and $\Pi^1_1 - \mathsf{CA}_0$

The system $\Pi^1_1 - \mathsf{CA}_0$ consists of RCA_0 plus comprehension for Π^1_1 definable sets. That is, we can assert the existence of the set

$$\{n \in \mathbb{N} \mid \theta(n)\}$$

where θ is a Π^1_1 formula, meaning θ has one universal set quantifier $(\forall X)$ and no other set quantifiers.

Theorem

The following are provably equivalent to $\Pi^1_1 - \mathsf{CA}_0$ *over* RCA_0.

(i) *The* Cantor/Bendixson theorem for $\mathbb{N}^{\mathbb{N}}$: *Every closed set in* $\mathbb{N}^{\mathbb{N}}$ *is the union of a perfect closed set and a countable set. (Simpson)*

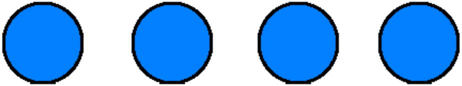
(ii) *Every countable Abelian group is the direct sum of a divisible group and a reduced group. (Friedman, Simpson, and Smith)*

Consequences of Reverse Math

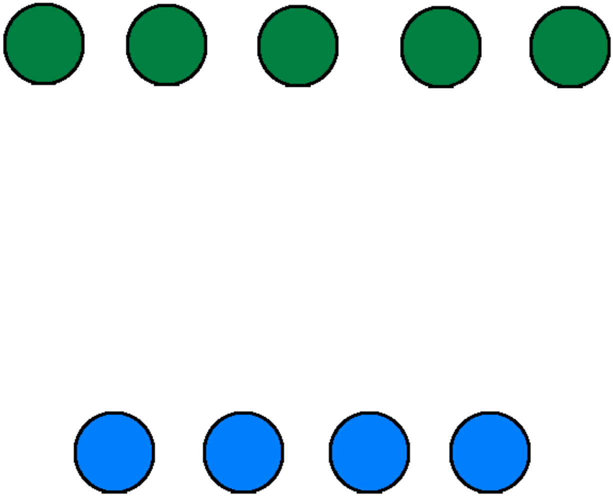
- We can formalize many of the theorems in mathematics as one of only *five* statements.
- This makes the exceptions that much more interesting.
- Reverse math over stronger systems, *e.g.,* ZFC as the base theory.

Marriage Problems

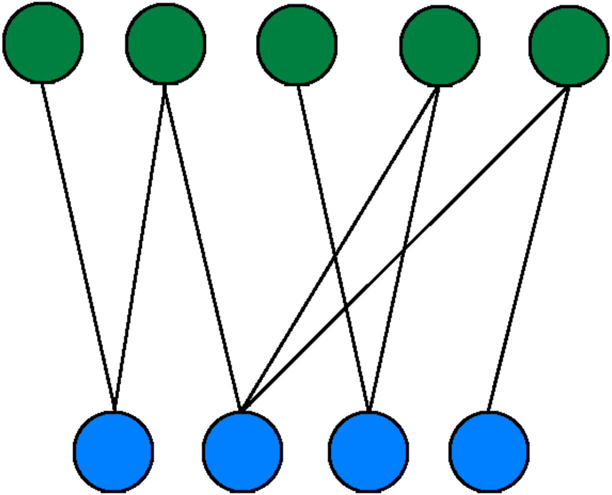
Marriage Problems



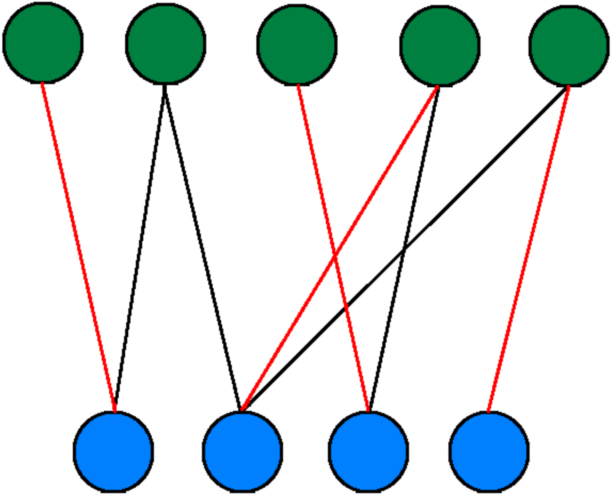
Marriage Problems



Marriage Problems



Marriage Problems



Some Notation

A marriage problem M consists of three sets B, G and R.

B is the set of boys,

G is the set of girls, and

R is the relation between the boys and girls.

$R \subset B \times G$ where $(b, g) \in R$ means "b knows g".

Some Notation

A marriage problem M consists of three sets B, G and R.

B is the set of boys,

G is the set of girls, and

R is the relation between the boys and girls.

$R \subset B \times G$ where $(b, g) \in R$ means "b knows g".

$G(b)$ is convenient shorthand for the set of girls b knows, *i.e.*

$$G(b) = \{g \in G \mid (b, g) \in R\}.$$

$G(b)$ is *not* a function.

Some More Notation

A *solution* to $M = (B, G, R)$ is an injection

$$f : B \to G$$

such that $(b, f(b)) \in R$ for every $b \in B$.

Some More Notation

A *solution* to $M = (B, G, R)$ is an injection

$$f : B \to G$$

such that $(b, f(b)) \in R$ for every $b \in B$.

M is a:

finite marriage problem if $|B|$ is finite.

infinite marriage problem if $|B|$ is not finite.

bounded marriage problem if there is a function $h : B \to G$ so that for each $b \in B$, $G(b) \subseteq \{0, 1, \ldots, h(b)\}$.

Previous Work

Jeff Hirst showed the following theorem of Philip Hall is provable within RCA_0.

Theorem

(RCA_0) *If $M = (B, G, R)$ is a finite marriage problem such that $|G(B_0)| \geqslant |B_0|$ for every $B_0 \subset B$, then M has a solution.*

Marshall Hall Jr. extended Philip Hall's work to the infinite case.

Theorem

If $M = (B, G, R)$ is an infinite marriage problem where each boy knows only finitely many girls and $|G(B_0)| \geqslant |B_0|$ for every $B_0 \subset B$, then M has a solution.

Previous Work

Hirst proved the following equivalence results.

Theorem

(RCA_0) *The following are equivalent:*

1. ACA_0
2. *If $M = (B, G, R)$ is an infinite marriage problem where each boy knows only finitely many girls and $|G(B_0)| \geqslant |B_0|$ for every $B_0 \subset B$, then M has a solution.*

Theorem

(RCA_0) *The following are equivalent:*

1. WKL_0
2. *If $M = (B, G, R)$ is a bounded marriage problem such that $|G(B_0)| \geqslant |B_0|$ for every $B_0 \subset B$, then M has a solution.*

Unique Solutions

What are the necessary and sufficient conditions for a marriage problem to have a *unique* solution?

Unique Solutions

What are the necessary and sufficient conditions for a marriage problem to have a *unique* solution?

In the finite case, we found the following necessary and sufficient condition.

Theorem

(RCA_0) *If $M = (B, G, R)$ is a finite marriage problem with n boys a unique solution f, then there is an enumeration of the boys $\langle b_i \rangle_{i \leqslant n}$ such that for every $1 \leqslant m \leqslant n$, $|G(\{b_1, b_2, \ldots, b_m\})| = m$.*

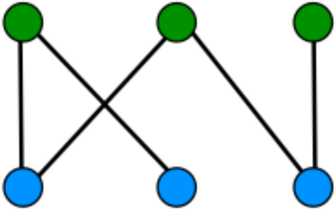
Unique Solutions

What are the necessary and sufficient conditions for a marriage problem to have a *unique* solution?

In the finite case, we found the following necessary and sufficient condition.

Theorem

(RCA_0) *If $M = (B, G, R)$ is a finite marriage problem with n boys a unique solution f, then there is an enumeration of the boys $\langle b_i \rangle_{i \leqslant n}$ such that for every $1 \leqslant m \leqslant n$, $|G(\{b_1, b_2, \ldots, b_m\})| = m$.*



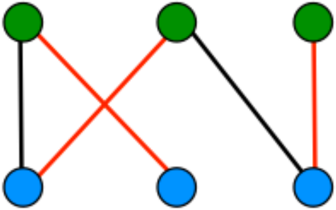
Unique Solutions

What are the necessary and sufficient conditions for a marriage problem to have a *unique* solution?

In the finite case, we found the following necessary and sufficient condition.

Theorem

(RCA_0) *If* $M = (B, G, R)$ *is a finite marriage problem with n boys a unique solution f, then there is an enumeration of the boys* $\langle b_i \rangle_{i \leqslant n}$ *such that for every* $1 \leqslant m \leqslant n$, $|G(\{b_1, b_2, \dots, b_m\})| = m$.



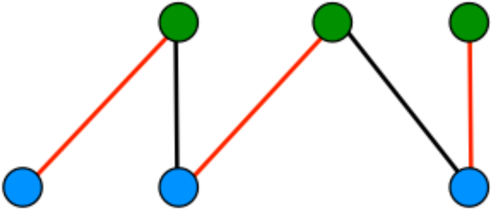
Unique Solutions

What are the necessary and sufficient conditions for a marriage problem to have a *unique* solution?

In the finite case, we found the following necessary and sufficient condition.

Theorem

(RCA_0) *If $M = (B, G, R)$ is a finite marriage problem with n boys a unique solution f, then there is an enumeration of the boys $\langle b_i \rangle_{i \leqslant n}$ such that for every $1 \leqslant m \leqslant n$, $|G(\{b_1, b_2, \ldots, b_m\})| = m$.*



Sketch of the proof

Lemma

(RCA_0) *If $M = (B, G, R)$ is a finite marriage problem with a unique solution f, then some boy knows exactly one girl.*

Sketch of the proof

Suppose we have $M = (B, G, R)$ as stated above with some initial enumeration of B. Apply the lemma and let b_1 be the first boy such that $|G(b_1)| = 1$.

Define $M_2 = (B - \{b_1\}, G - G(b_1), R_2)$. Because M has a unique solution, M_2 has a unique solution, namely the restriction of f to the sets of M_2. Apply the lemma once more and let b_2 be the first boy in $B - \{b_1\}$ such that $|G_{M_2}(b_2)| = 1$.

Continuing this process inductively yields the j^{th} boy in our desired enumeration from
$M_j = (B - \{b_1, b_2, \ldots, b_{j-1}\}, G - G(b_1, b_2, \ldots, b_{j-1}), R_j)$.

After the n^{th} iteration we have $(b_1, b_2, \ldots, b_n)$ where for every $1 \leqslant m \leqslant n$, $|G(\{b_1, b_2, \ldots, b_m\})| = m$. $\square$

Infinite Marriage Problems

The statement regarding finite marriage problems with unique solutions can be generalized to the *infinite* case. Paralleling the previous work we see:

Theorem

(RCA_0) *The following are equivalent:*

1. ACA_0
2. *If $M = (B, G, R)$ is an infinite marriage problem where each boy knows only finitely many girls and has a unique solution f, then there is an enumeration of the boys $\langle b_i \rangle_{i \geqslant 1}$ such that for every $n \geqslant 1$, $|G(\{b_1, b_2, \ldots, b_n\})| = n$.*

Sketch of the reversal

We assume statement (2) in order to prove statement (1). By Lemma III.1.3 of Simpson [3], it suffices to show (2) implies the existence of the range of an arbitrary injection.

Sketch of the reversal

We assume statement (2) in order to prove statement (1). By Lemma III.1.3 of Simpson [3], it suffices to show (2) implies the existence of the range of an arbitrary injection.

To that end, let $f : \mathbb{N} \to \mathbb{N}$ be an injection and construct $M = (B, G, R)$ as follows:

- $B = \{c_n \mid n \in \mathbb{N}\} \cup \{d_n \mid n \in \mathbb{N}\}$,
- $G = \{g_n \mid n \in \mathbb{N}\} \cup \{r_n \mid n \in \mathbb{N}\}$,
- for every i, $(c_i, g_i) \in R$ and $(d_i, r_i) \in R$, and
- if $f(m) = n$ then $(c_n, r_m) \in R$.

Sketch of the reversal

We assume statement (2) in order to prove statement (1). By Lemma III.1.3 of Simpson [3], it suffices to show (2) implies the existence of the range of an arbitrary injection.

To that end, let $f : \mathbb{N} \to \mathbb{N}$ be an injection and construct $M = (B, G, R)$ as follows:

- $B = \{c_n \mid n \in \mathbb{N}\} \cup \{d_n \mid n \in \mathbb{N}\}$,
- $G = \{g_n \mid n \in \mathbb{N}\} \cup \{r_n \mid n \in \mathbb{N}\}$,
- for every i, $(c_i, g_i) \in R$ and $(d_i, r_i) \in R$, and
- if $f(m) = n$ then $(c_n, r_m) \in R$.

Let $h : B \to G$ such that $h(d_i) = r_i$ and $h(c_i) = g_i$ for each $i \in \mathbb{N}$.

h is injective and a unique solution to M.

Sketch of the reversal

Apply the enumeration theorem to obtain $\langle b_i \rangle_{i \geqslant 1}$ where for every $n \geqslant 1$ $|G(b_1, \ldots, b_n)| = n$.

Sketch of the reversal

Apply the enumeration theorem to obtain $\langle b_i \rangle_{i \geqslant 1}$ where for every $n \geqslant 1$ $|G(b_1, \ldots, b_n)| = n$.

Suppose $f(j) = k$. Then $(c_k, r_j) \in R$ and $G(c_k) = \{g_k, r_j\}$.

Note $G(d_j) = \{r_j\}$. So d_j must appear before c_k in the enumeration of B.

Sketch of the reversal

Apply the enumeration theorem to obtain $\langle b_i \rangle_{i \geqslant 1}$ where for every $n \geqslant 1$ $|G(b_1, \ldots, b_n)| = n$.

Suppose $f(j) = k$. Then $(c_k, r_j) \in R$ and $G(c_k) = \{g_k, r_j\}$.

Note $G(d_j) = \{r_j\}$. So d_j must appear before c_k in the enumeration of B.

Well, this implies that k is in the range of f if and only if some boy d_j appears before c_k in the enumeration and $f(j) = k$.

We need only check finitely many values of f to see if k is in the range, hence, recursive comprehension proves the existence of the range of f.

Sketch of the reversal

Apply the enumeration theorem to obtain $\langle b_i \rangle_{i \geqslant 1}$ where for every $n \geqslant 1$ $|G(b_1, \ldots, b_n)| = n$.

Suppose $f(j) = k$. Then $(c_k, r_j) \in R$ and $G(c_k) = \{g_k, r_j\}$.

Note $G(d_j) = \{r_j\}$. So d_j must appear before c_k in the enumeration of B.

Well, this implies that k is in the range of f if and only if some boy d_j appears before c_k in the enumeration and $f(j) = k$.

We need only check finitely many values of f to see if k is in the range, hence, recursive comprehension proves the existence of the range of f. $\square$

Bounded Marriage Problems

In the *bounded* case, the result, as expected, paralleled the previous work.

Theorem

(RCA_0) *The following are equivalent:*

1. WKL_0
2. *If* $M = (B, G, R)$ *is a bounded marriage problem with a unique solution* f*, then there is an enumeration of the boys* $\langle b_i \rangle_{i \geqslant 1}$ *such that for every* $n \geqslant 1$, $|G(\{b_1, b_2, \ldots, b_n\})| = n$.

An Open Question

To prove the enumeration theorem for infinite marriage problems we employed the following lemma.

Lemma

Suppose $M = (B, G, R)$ is a marriage problem with a unique solution, then for any $b \in B$ there is a finite set F such that $b \in F \subset B$ and $|G(F)| = |F|$.

The exact strength of this statement is still unknown.

References

[1] Jeffry L. Hirst, *Marriage theorems and reverse mathematics*, Logic and computation (Pittsburgh, PA, 1987), Contemp. Math., vol. 106, Amer. Math. Soc., Providence, RI, 1990, pp. 181–196. DOI 10.1090/conm/106/1057822. MR1057822 (91k:03141)

[2] Jeffry L. Hirst and Noah A. Hughes, *Reverse mathematics and marriage problems with unique solutions*. Submitted.

[3] Stephen G. Simpson, *Subsystems of second order arithmetic*, 2nd ed., Perspectives in Logic, Cambridge University Press, Cambridge, 2009. DOI 10.1017/CBO9780511581007 MR2517689.

Questions?

Thank You.