Generalizations of Hall's theorem in reverse mathematics

Noah A. Hughes
University of Connecticut
noah.hughes@uconn.edu

Monday, 8th July, 2019

IMS Graduate Summer School in Logic

Reverse mathematics: the motivation

The central question:

> *What is the appropriate axiomatization of a given fragment of (countable) mathematics?*

Reverse mathematics: the method

Let $\Xi = \{\xi_0, \xi_1, \ldots, \xi_n\}$ be some fragment of mathematics and $\mathcal{B}$ an axiom system too weak to prove Ξ.

Determine an addiontal axiom $\mathcal{A}$ outside of $\mathcal{B}$ such that

$$\mathcal{B} \vdash \mathcal{A} \leftrightarrow \xi_i \quad \text{for } 0 \leq i \leq n.$$

Then $\mathcal{B} + \mathcal{A}$ is a necessary and sufficient axiomatization of Ξ.

$\mathcal{B} \vdash \mathcal{A} \to \xi_i$
a "regular" proof

$\mathcal{B} \vdash \xi_i \to \mathcal{A}$
a "reversed" proof

Reverse mathematics: the setting

We consider five subsystems of second-order arithmetic.

The base system RCA_0 consists of axioms for arithmetic, induction for Σ^0_1 formula, and set comprehension for Δ^0_1 formula.

The system WKL_0 consists of RCA_0 plus
weak Kőnig's lemma:

Every infinite binary tree has an infinite path.

The system ACA_0 consists of RCA_0 plus
axioms for set comprehension for all arithmetical formula.

The system ATR_0 consists of ACA_0 plus
axioms for iterating arithmetical set comprehension along any (countable) well-order.

The system $\Pi^1_1{-}\mathsf{CA}_0$ consists of ACA_0 plus
axioms for set comprehension for Π^1_1 formula.

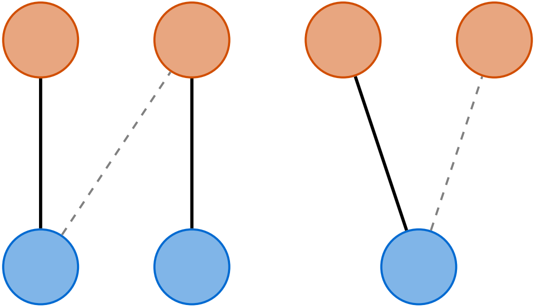
Reverse mathematics: the "big five"

$$
\begin{array}{rl}
\mathsf{RCA}_0: & \text{arithmetic, } \Sigma^0_1\text{-induction, recursive comprehension} \\
\cap & \\
\mathsf{WKL}_0: & \mathsf{RCA}_0 + \text{"every infinite binary tree has an infinite path"} \\
\cap & \\
\mathsf{ACA}_0: & \mathsf{RCA}_0 + \text{comprehension for arithmetical formulas} \\
\cap & \\
\mathsf{ATR}_0: & \mathsf{ACA}_0 + \text{iterability of arithmetical operators} \\
\cap & \qquad\qquad\qquad\qquad\qquad\qquad \text{along any well-order} \\
\Pi^1_1\text{-}\mathsf{CA}_0: & \mathsf{ACA}_0 + \text{comprehension for } \Pi^1_1 \text{ formulas}
\end{array}
$$

Reverse mathematics: the “big five” in context

RCA_0	$\vdash$	the intermediate value theorem
$\top$		
WKL_0	$\leftrightarrow$	the Heine/Borel covering lemma;
ACA_0	$\leftrightarrow$	the Bolzano/Weierstaß theorem;
ATR_0	$\leftrightarrow$	the perfect set theorem;
$\Pi^1_1\!-\!\mathsf{CA}_0$	$\leftrightarrow$	the Cantor/Bendixson theorem.

Matching problems: the idea

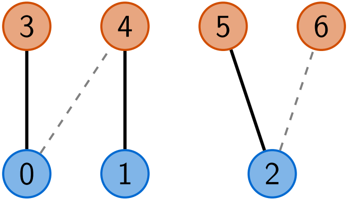


Matching problems: the formalization

A matching problem is a triple $P = (A, B, R)$ where $A, B \subseteq \mathbb{N}$ and $R \subseteq A \times B$.

If $(a, b) \in R$ we say b is a permissable match of a and set $R(a) = \{b : (a, b) \in R\}$.

A solution to a matching problem is an injection $f : A \to B$ such that $f(a) \in R(a)$ for all $a \in A$.



$$A = \{0, 1, 2\}$$

$$B = \{3, 4, 5, 6\}$$

$$R = \{(0, 3), (0, 4), (1, 4), (2, 5), (2, 6)\}$$

$$f_1 = \begin{cases} 0 \mapsto 3 \\ 1 \mapsto 4 \\ 2 \mapsto 5 \end{cases} \quad f_2 = \begin{cases} 0 \mapsto 3 \\ 1 \mapsto 4 \\ 2 \mapsto 6 \end{cases}$$

Matching problems: Hall's theorem

Theorem (Philip Hall)

Let $P = (A, B, R)$ be a matching problem in which A is finite and every element has finitely many permissable matches. If $|A_0| \leq |R(A_0)|$ for every $A_0 \subseteq A$, then P has a solution.

Theorem (Marshall Hall)

Let $P = (A, B, R)$ be a matching problem in which every element has finitely many permissable matches. If $|A_0| \leq |R(A_0)|$ for every $A_0 \subseteq A$, then P has a solution.

Theorem (Hirst)

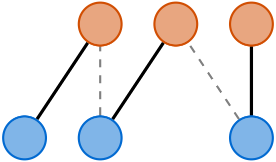
The following are provable in RCA_0

1. *Philip Hall's theorem*
2. $\mathrm{ACA}_0 \leftrightarrow$ *Marshall Hall's theorem*

Matching problems: unique matchings

Theorem (Hirst, Hughes)

A matching problem $P = (A, B, R)$, in which every element has finitely many permissable matches, has a unique solution if and only if there is an enumeration of A, say $\langle a_i \rangle_{i \geq 1}$ such that for every $n \geq 1$, $|R(a_1, a_2, \ldots, a_n)| = n$.



Theorem (Hirst, Hughes)

Over RCA_0*, the following are equivalent*

1. ACA_0
2. *The above theorem*

Matching problems: many (possible) matches

Consider matching problems in which any element may have infinitely many permissable matches.

Theorem

A matching problem $P = (A, B, R)$ has a unique solution if and only if there is a well-order $(A, <_A)$ such that for each $a \in A$, there is a unique $b \in B$ satisfying

$$R(a) - R(\{a' : a' <_A a\}) = \{b\}.$$

Label the forward direction STO and the reverse direction OTS.

Conjecture (Hirst)

Over RCA_0

1. ATR_0 *is provably equivalent to* STO
2. *and* ACA_0 *is provably equivalent to* OTS*.*

Current results: a partial answer

Theorem (Hughes)

Over RCA_0*, the following are equivalent*

1. ACA_0
2. OTS*: A matching problem* $P = (A, B, R)$ *has a unique solution if there is a well-order* $(A, <_A)$ *such that for each* $a \in A$*, there is a unique* $b \in B$ *satisfying*

$$R(a) - R(\{a' : a' <_A a\}) = \{b\}.$$

Theorem (Hughes)

The following is provable in ATR_0*:*

STO*: A matching problem* $P = (A, B, R)$ *has a unique solution only if there is a well-order* $(A, <_A)$ *such that for each* $a \in A$*, there is a unique* $b \in B$ *satisfying* $R(a) - R(\{a' : a' <_A a\}) = \{b\}$.

Current results: an equivalence to ACA_0

Theorem (Hughes)

Over RCA_0*, the following are equivalent*

1. ACA_0
2. OTS*: A matching problem* $P = (A, B, R)$ *has a unique solution if there is a well-order* $(A, \leq_A)$ *such that for each* $a \in A$*, there is a unique* $b \in B$ *satisfying*

$$R(a) - R(\{a' : a' \leq_A a\}) = \{b\}.$$

Proof: To show (1) implies (2), we are given a matching problem and appropriate well-order and we arithemetically define the unique solution.

$$(a, b) \in f \leftrightarrow [(a, b) \in R \wedge \forall a'(a' <_A a \rightarrow (a, b) \notin R)].$$

Current results: an equivalence to ACA_0

Lemma (Simpson)

Over RCA_0*, the following are equivalent*

1. ACA_0
2. *For any injection* $g : \mathbb{N} \to \mathbb{N}$

$$\exists X \forall y (y \in X \leftrightarrow \exists x\, f(x) = y)$$

   that is, the range of g *exists.*

Thus, to show

$$\mathsf{RCA}_0 \vdash \mathsf{OTS} \to \mathsf{ACA}_0$$

we instead show

$$\mathsf{RCA}_0 \vdash \mathsf{OTS} \to \text{Item 2} \leftrightarrow \mathsf{ACA}_0.$$

Current results: an equivalence to ACA_0

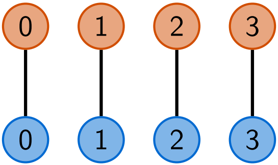
Let $g : \mathbb{N} \to \mathbb{N}$ be an arbitrary injection. (e.g. $g(4) = 1$)

Construct a matching problem $P = (A, B, R)$ and well-order $(A, <_A)$ as follows:

$A = B = \mathbb{N}$ and build R in stages:

at stage $2s$ add $(2s, 2s)$ to R,

at stage $2s + 1$. check if $m \leq 2s$ is in $\mathrm{ran}(g)$: if so add $(2m, 2s + 1), (2s + 1, 2m)$ to R. If not, add $(2s + 1, 2s + 1)$ to R.



$0 <_A 1 \qquad <_A 2 <_A 3$

Current results: an equivalence to ACA_0

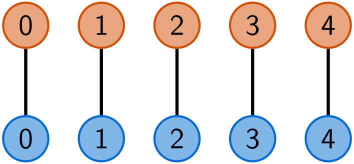
Let $g : \mathbb{N} \to \mathbb{N}$ be an arbitrary injection. (e.g. $g(4) = 1$)

Construct a matching problem $P = (A, B, R)$ and well-order $(A, <_A)$ as follows:

$A = B = \mathbb{N}$ and build R in stages:

at stage $2s$ add $(2s, 2s)$ to R,

at stage $2s+1$. check if $m \leq 2s$ is in $\mathrm{ran}(g)$: if so add $(2m, 2s+1), (2s+1, 2m)$ to R. If not, add $(2s+1, 2s+1)$ to R.



$0 <_A 1 \quad <_A 2 <_A 3 <_A 4$

Current results: an equivalence to ACA_0

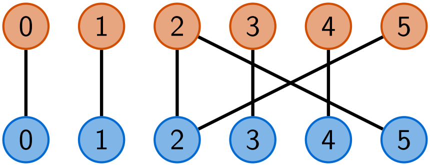
Let $g : \mathbb{N} \to \mathbb{N}$ be an arbitrary injection. (e.g. $g(4) = 1$)

Construct a matching problem $P = (A, B, R)$ and well-order $(A, <_A)$ as follows:

$A = B = \mathbb{N}$ and build R in stages:

at stage $2s$ add $(2s, 2s)$ to R,

at stage $2s + 1$. check if $m \leq 2s$ is in $\mathrm{ran}(g)$: if so add $(2m, 2s + 1), (2s + 1, 2m)$ to R. If not, add $(2s + 1, 2s + 1)$ to R.



$0 <_A 1 \quad <_A 2 <_A 3 <_A 4$

Current results: an equivalence to ACA_0

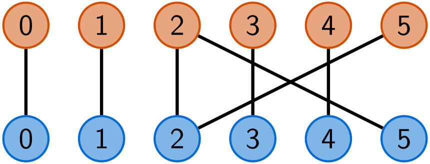
Let $g : \mathbb{N} \to \mathbb{N}$ be an arbitrary injection. (e.g. $g(4) = 1$)

Construct a matching problem $P = (A, B, R)$ and well-order $(A, <_A)$ as follows:

$A = B = \mathbb{N}$ and build R in stages:

at stage $2s$ add $(2s, 2s)$ to R,

at stage $2s + 1$. check if $m \leq 2s$ is in $\operatorname{ran}(g)$: if so add $(2m, 2s + 1), (2s + 1, 2m)$ to R. If not, add $(2s + 1, 2s + 1)$ to R.



$0 <_A 1 <_A 5 <_A 2 <_A 3 <_A 4$

Current results: an equivalence to ACA_0

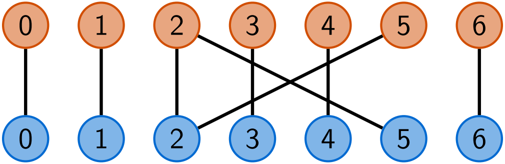
Let $g : \mathbb{N} \to \mathbb{N}$ be an arbitrary injection. (e.g. $g(4) = 1$)

Construct a matching problem $P = (A, B, R)$ and well-order $(A, <_A)$ as follows:

$A = B = \mathbb{N}$ and build R in stages:

at stage $2s$ add $(2s, 2s)$ to R,

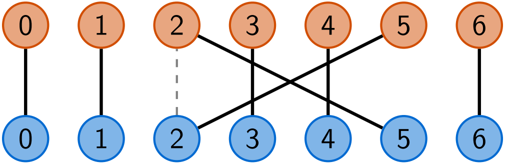
at stage $2s + 1$. check if $m \leq 2s$ is in ran(g): if so add $(2m, 2s + 1), (2s + 1, 2m)$ to R. If not, add $(2s + 1, 2s + 1)$ to R.



$0 <_A 1 <_A 5 <_A 2 <_A 3 <_A 4 <_A 6$

Current results: an equivalence to ACA_0

Apply OTS to obtain a unique solution f:



$$f = \begin{cases} 0 \mapsto 0 \\ 1 \mapsto 1 \\ 2 \mapsto 5 \\ 3 \mapsto 3 \\ 4 \mapsto 4 \\ 5 \mapsto 2 \\ 6 \mapsto 6 \end{cases} \implies f(2n) \neq 2n \leftrightarrow n \in \mathrm{ran}(g)$$

So, OTS implies ACA_0. $\square$

Current results: a proof in ATR_0

Theorem (Hughes)

The following is provable in ATR_0*:*

> STO*: A matching problem* $P = (A, B, R)$ *has a unique solution only if there is a well-order* $(A, <_A)$ *such that for each* $a \in A$*, there is a unique* $b \in B$ *satisfying* $R(a) - R(\{a' : a' <_A a\}) = \{b\}$.

Current results: a proof in ATR_0

Fix a matching problem $P = (A, B, R)$ with unique solution f.

Our goal is to build a well-order such that each element has exactly one permissable match that it's predeccesors do not have.

Given an initial segment $(A_0, \leq)$ of the desired well-order $(A, \leq)$, it is arithmetical to find a suitable next element:

$$\psi(A_0, a) : R(a) - \bigcup_{a' \in A_0} R(a') = \{f(a)\}.$$

Thus, in ATR_0, we may iteratively construct the desired well-order by applying ψ at each stage to find an appopriate $a \in A$ to append to the order.

We need only determine which well-order to iterate upon.

Current results: a proof in ATR_0

Given a tree T, recall the Kleene-Brouwer order of T, $\mathrm{KB}(T)$ is defined by

$$\sigma <_{\mathrm{KB}} \tau \iff \sigma \succ \tau \vee \exists n(\sigma \upharpoonright n = \tau \upharpoonright n \wedge \sigma(n) < \tau(n))$$

ACA_0 suffices to show that $\mathrm{KB}(T)$ is a well-order when T is well-founded.

We construct a well-founded tree T which encodes the dependencies of elements of A and iterate upon $\mathrm{KB}(T)$.

Let

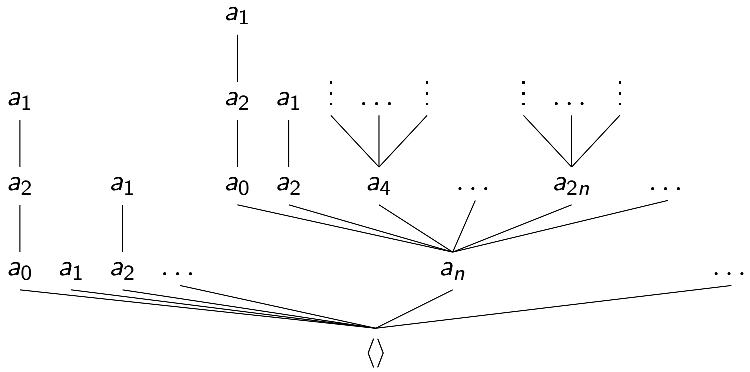
$$\begin{aligned} T_0 &= \langle\rangle \cup \{\langle a\rangle : a \in A\} \\ T_{s+1} &= T_s \cup \{\sigma^\frown\langle a\rangle : \sigma \in T_s, a \neq \sigma(|\sigma|-1), f(a) \in R(\sigma(|\sigma|-1))\} \end{aligned}$$

And set $T = \cup_{s\in\omega} T_s$.

Current results: a proof in ATR_0

The unique solution of P guarentees T is well-founded.

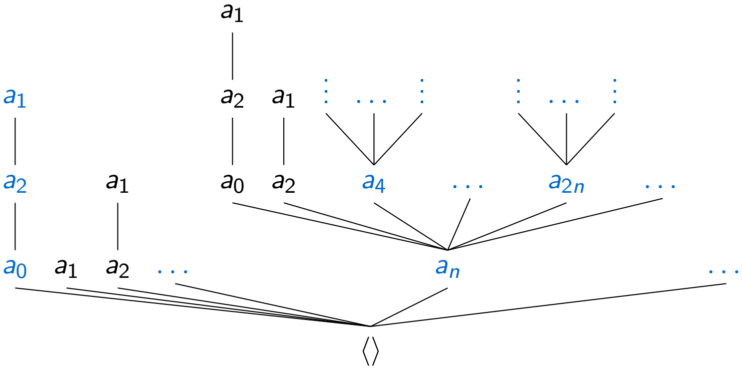
$$R(a_0) = \{f(a_0), f(a_2)\}, \quad R(a_1) = \{f(a_1)\}, \quad R(a_2) = \{f(a_2), f(a_1)\},$$
$$\text{and } R(a_n) = \{f(a_n)\} \cup \{f(a_{2i}) : i \in \omega\}$$



Current results: a proof in ATR_0

The unique solution of P guarentees T is well-founded.

$$R(a_0) = \{f(a_0), f(a_2)\}, \quad R(a_1) = \{f(a_1)\}, \quad R(a_2) = \{f(a_2), f(a_1)\},$$
$$\text{and } R(a_n) = \{f(a_n)\} \cup \{f(a_{2i}) : i \in \omega\}$$



Current results: a more formal proof in ATR_0

We define two formulas $\psi(\sigma, Y)$:

$$[(\neg\exists j \in X)\,\big(\sigma(|\sigma|-1), j\big) \in Y] \qquad \wedge$$
$$\left(R\big(\sigma(|\sigma|-1)\big) - \bigcup_{\{a:(\exists j \in X)\,(a,j)\in Y\}} R(a) = \{f\big(\sigma(|\sigma|-1)\big)\}\right)$$

and $\theta(n, Y)$:

$$(\exists \sigma \in T)\Big[\big(\psi(\sigma, Y) \wedge \big((\forall \tau \in T)\,\psi(\tau, Y) \to \sigma \leq_{\mathrm{KB}} \tau\big)\big)$$
$$\wedge\ \big(n = \sigma(|\sigma|-1)\big)\Big].$$

ATR_0 contains axioms which guarentee the existence of a set Y such that $H_\theta(\mathrm{KB}(T), Y)$ holds.

We then verify that Y orders all of A, is well founded, and satsifies the desired property. □

Current results: a reversal to WKL_0

Consider the principle STO(F):

Let $P = (A, B, R)$ be a matching problem with a unique solution in which every element has finitely many permissible matches. Then there is a well-order $(A, <_A)$ such that for every $a \in A$, there is a unique $b \in B$ such that

$$R(a) - R(\{a' : a' <_A a\}) = \{b\}.$$

If the order type of the well-order is prescribed as ω, this principle is equivalent to ACA_0.

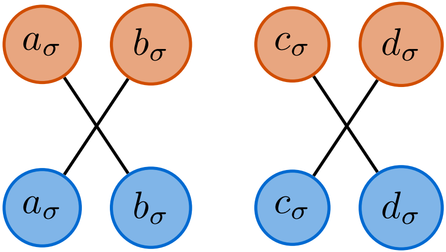
Theorem (Hughes)

Over RCA_0, STO(F) *implies* WKL_0*.*

Current results: a reversal to WKL_0

Given an infinite binary tree T, construct a matching problem $P = (A, B, R)$ whose well-order computes a path in T as follows:

$A = B = \{a_\sigma, b_\sigma, c_\sigma, d_\sigma : \sigma \in T\}$ and
$R = \{(a_\sigma, b_\sigma), (b_\sigma, a_\sigma), (c_\sigma, d_\sigma), (d_\sigma, c_\sigma) : \sigma \in T\}$.



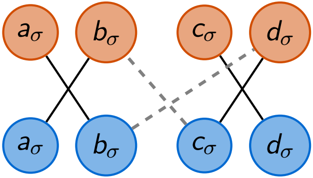
Current results: a reversal to WKL_0

Given an infinite binary tree T, construct a matching problem $P = (A, B, R)$ whose well-order computes a path in T as follows:

$A = B = \{a_\sigma, b_\sigma, c_\sigma, d_\sigma : \sigma \in T\}$ and
$R = \{(a_\sigma, b_\sigma), (b_\sigma, a_\sigma), (c_\sigma, d_\sigma), (d_\sigma, c_\sigma) : \sigma \in T\}$.

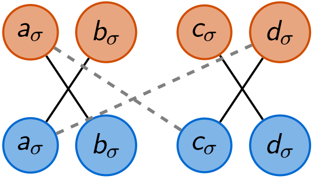
If $\sigma^\frown 0 \in T$ but $\sigma^\frown 1 \notin T$
Add (c_σ, b_σ) and (b_σ, d_σ) to R.

This forces $a_\sigma < b_\sigma$. ("go left")



If $\sigma^\frown 0 \notin T$ but $\sigma^\frown 1 \in T$
Add (c_σ, a_σ) and (a_σ, d_σ) to R.

This forces $a_\sigma > b_\sigma$. ("go right")



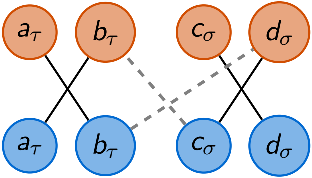
Current results: a reversal to WKL_0

Given an infinite binary tree T, construct a matching problem $P = (A, B, R)$ whose well-order computes a path in T as follows:

$A = B = \{a_\sigma, b_\sigma, c_\sigma, d_\sigma : \sigma \in T\}$ and
$R = \{(a_\sigma, b_\sigma), (b_\sigma, a_\sigma), (c_\sigma, d_\sigma), (d_\sigma, c_\sigma) : \sigma \in T\}$.

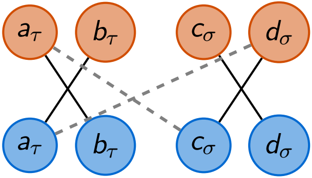
If $\sigma^\frown 0 \notin T$ but $\sigma^\frown 1 \notin T$

Add (c_σ, b_τ) and (b_τ, d_σ) to R if $\tau(|\sigma|) = 1$ (“go left instead”)



Add (c_σ, a_τ) and (a_τ, d_σ) to R if $\tau(|\sigma|) = 0$ (“go right instead”)

where τ is the longest predeccesor of σ with a long enough extension in T.

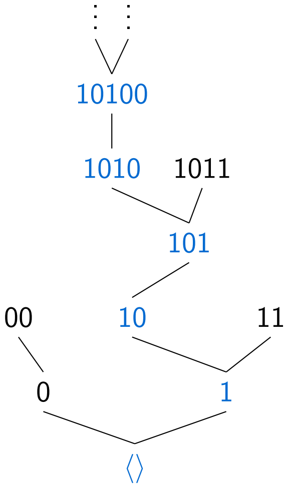


If $\sigma^\frown 0 \in T$ and $\sigma^\frown 1 \in T$
“wait.”

Current results: a reversal to WKL_0

$P = (A, B, R)$ has a unique solution $f : a_\sigma \mapsto b_\sigma, b_\sigma \mapsto a_\sigma, \ldots$
Apply STO to well-order A and notice the construction guarantees:

Stage	Order
2	$a_{\langle\rangle} > b_{\langle\rangle}$
1	$a_0 < b_0$
2	$a_1 < b_1$
2	$a_{00}\ ?\ b_{00}$
2	$a_{10} > b_{10}$
2	$a_{11}\ ?\ b_{11}$
4	$a_{101} < b_{101}$
4	$a_{1010} < b_{1010}$
4	$a_{1011}\ ?\ b_{1011}$
$\vdots$	$a_{10100}\ ?\ b_{10100}$



From the order, we compute a path. $\square$

References

[1] Harvey M. Friedman, *Systems of second order arithmetic with restricted induction, I, II* (abstracts), J. Symbolic Logic **41** (1976), no. 2, 557–559.

[2] Marshall Hall Jr., *Distinct representatives of subsets*, Bull. Amer. Math. Soc. **54** (1948), 922–926. DOI 10.1090/S0002-9904-1948-09098-X. MR0027033 (10,238g)

[3] 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)

[4] Jeffry L. Hirst and Noah A. Hughes, *Reverse mathematics and marriage problems with unique solutions.*, Arch. Math. Logic **54** (2015), 49-57. DOI 10.1007/s00153-014-0401-z.

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

Thank you for your attention!