Non-injection principles and uniformity

Damir D. Dzhafarov
University of Connecticut

20 April 2024

Joint work with David Belanger and Jun Le Goh.

Reverse mathematics and computability

There is a deep correspondence—"a constant and fruitful interplay" (Downey, Hirschfeldt, Lempp, and Solomon 2001)—between computability theory on the one hand and reverse mathematics on the other.

- Set-existence theorems, calibrated using standard subsystems of second-order arithmetic, correspond with natural computability-theoretic classes and operations.
- Arithmetical theorems, calibrated using fragments of Peano arithmetic, correspond with uniformity results in computability theory.

More on this in Reed Solomon's talk.

Non-injection principles and induction

Over $\mathsf{PA}^- + \mathsf{I}\Sigma^0_k$, it can be shown that for all $n < m$, there is no Σ^0_k-definable injection $m \to n$.

Thm (Dimitracopoulos, Paris 1986; Hirst 1987). TFAE over RCA_0:

1. The infinitary pigeonhole principle.
2. $(\forall n)$[there is no Σ^0_2 injection $n+1 \to n$].

Thm (Belanger, Chong, Wang, Wong, Yang 2021).

Over RCA_0,

$$\begin{array}{ll} & (\forall n)[\text{there is no } \Sigma^0_2 \text{ injection } 2n \to n] \\ \nvdash & (\forall n)[\text{there is no } \Sigma^0_2 \text{ injection } n+1 \to n]. \end{array}$$

Instance-solution problems

An instance-solution problem is specified by a non-empty set of instances, and for each instance, a non-empty set of solutions (all coded by elements of ω^ω).

Defn. Fix $n < m$. $(m \not\to n)$ is the following problem:

- instances are functions $f : m \to n$;
- the solutions to f are all pairs $\{i, j\}$ such that $i < j < m$ and $f(i) = f(j)$.

Defn.

- id_k is the problem whose instances are elements $i < k$, with the unique solution to any such i being i itself.
- $\lim_k$ is the problem whose instances are functions $g : \omega \to k$ such that $\lim_s g(s)$ exists, with the solution to any such g being $\lim_s g(s)$.

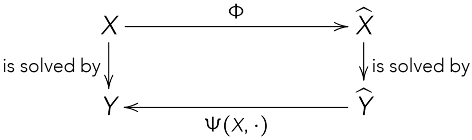
Weihrauch reducibility

Let P and Q be instance-solution problems.

P is Weihrauch reducible to Q, written $P \leq_W Q$, if

- every instance X of P uniformly computes an instance $\widehat{X}$ of Q,
- every Q-solution $\widehat{Y}$ to $\widehat{X}$, together with X, uniformly computes a P-solution Y to X.

So the following diagram "commutes":



(Weihrauch 1992; Brattka; Gherardi and Marcone 2008; DDHMS 2016.)

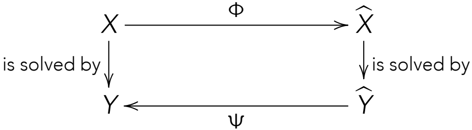
Strong Weihrauch reducibility

Let P and Q be instance-solution problems.

P is strongly Weihrauch reducible to Q, written $P \leq_{sW} Q$, if

- every instance X of P uniformly computes an instance $\widehat{X}$ of Q,
- every Q-solution $\widehat{Y}$ to $\widehat{X}$ uniformly computes a P-solution Y to X.

So the following diagram "commutes":



$\leq_{sW}$ is less natural than $\leq_{W}$, but it is easier to work with. Often, results can be lifted from $\leq_{sW}$ to $\leq_{W}$.

Jumps in the Weihrauch degrees

For any problem P, the jump of P, denoted P′, is the following problem:

- the instances of P′ are limit approximations to instances of P;
- the solutions to a limit P-instance are the solutions to the P-instance.

Example. For all k, $\mathrm{id}_k' \equiv_{\mathrm{sW}} \lim_k$.

Thm (Brattka, Gherardi, Marcone 2011).
For all problems P and Q, $\mathsf{P} \leq_{\mathrm{sW}} \mathsf{Q}$ if and only if $\mathsf{P}' \leq_{\mathrm{W}} \mathsf{Q}'$.

So in the Weihrauch degrees, a computable instance of $(m \not\to n)'$ can be thought of as an analogue of a Σ^0_2-definable function $f : m \to n$.

We can study $(m \not\to n)'$ under $\leq_{\mathrm{W}}$ by studying $(m \not\to n)$ under $\leq_{\mathrm{sW}}$.

Basic facts

Prop. $\mathrm{id}_2 \leq_{\mathrm{sW}} \mathrm{id}_3 \leq_{\mathrm{sW}} \ldots$

Prop. For each n, $(n+1 \not\to n) \geq_{\mathrm{W}} (n+2 \not\to n) \geq_{\mathrm{W}} \ldots$

Prop. For each n, $(n+1 \not\to n) \equiv_{\mathrm{sW}} \mathrm{id}_{\binom{n+1}{2}}$.

A very useful, but less obvious, fact is the following:

Thm. $\mathrm{id}_k \leq_{\mathrm{sW}} (m \not\to n)$ if and only if there exist functions $f_1, \ldots, f_k : m \to n$ with no common solution.

We will give tighter characterizations in the special case $m = n^2$, and more generally, $m = qn$ for $q \leq n$.

A motivating example

Prop $\mathrm{id}_2 \leq_{\mathrm{sW}} (n^2 \not\leftrightarrow n)$ but $\mathrm{id}_2 \not\leq_{\mathrm{sW}} (n^2 + 1 \not\leftrightarrow n)$.

To show $\mathrm{id}_2 \leq_{\mathrm{sW}} (n^2 \not\leftrightarrow n)$:

- $\Phi(0)$: Arrange n^2 as an $n \times n$ grid and partition using vertical lines.
- $\Phi(1)$: Partition using horizontal lines instead.
- $\Psi(\{i, j\})$: Return 0 if i and j lie in the same vertical line, otherwise return 1.

To show $\mathrm{id}_2 \not\leq_{\mathrm{sW}} (n^2 + 1 \not\leftrightarrow n)$:

- Suppose otherwise, as witnessed by Φ and Ψ. So $\Phi(0), \Phi(1) : n^2 + 1 \to n$.
- There exist $i \neq j$ such that $\Phi(0)(i) = \Phi(0)(j)$ and $\Phi(1)(i) = \Phi(1)(j)$. (Apply pigeonhole twice.)
- Then $\Psi(\{i, j\})$ equals both 0 and 1, contradiction.

Affine planes

These ideas can be pushed to obtain the following surprising result:

Thm. $\mathrm{id}_{k+2} \leq_{\mathrm{sW}} (n^2 \not\to n)$ if and only if there exist k mutually orthogonal Latin squares of order n.

Cor. $\mathrm{id}_{n+1} \leq_{\mathrm{sW}} (n^2 \not\to n)$ if and only if there is a finite affine plane of order n.

It is a longstanding open question in combinatorics to determine for which n there exists an affine plane of order n.

This seems to be a nice new example of the empirical observation that computability-theoretic notions tend to be combinatorially natural, and vice-versa.

Block designs

A resolvable balanced incomplete block design, abbreviated RBIBD(m, q), is a family of distinct q-subsets (blocks) of $[m]$ such that:

- each pair of distinct numbers from $[m]$ is contained in exactly 1 block
- the set of blocks can be partitioned into partitions of $[m]$ (parallel classes).

Example. A decomposition of K_{2n} into perfect matchings is an RBIBD$(2n, 2)$ where each perfect matching is a parallel class.

Thm. For all $q \leq n$, we have $\mathrm{id}_{\frac{qn-1}{q-1}} \leq_{\mathrm{sW}} (qn \not\to n)$ if and only if there exists an RBIBD(qn, q).

(The extreme case $q = n$ corresponds to our earlier result on affine planes.)

More general cases

By ad hoc means, we can prove a variety of other reductions and separations.

Example.

- $\mathrm{id}_3 \equiv_{\mathrm{sW}} (3 \not\to 2) \equiv_{\mathrm{sW}} (4 \not\to 2) >_{\mathrm{sW}} (5 \not\to 2) >_{\mathrm{sW}} (6 \not\to 2) >_{\mathrm{sW}} (7 \not\to 2)$.
- For $n > 2$, $\mathrm{id}_{\binom{n+1}{2}} \equiv_{\mathrm{sW}} (n+1 \not\to n) >_{\mathrm{sW}} (n+2 \not\to n) \geq_{\mathrm{sW}} (2n \not\to n)$ $>_{\mathrm{sW}} (2n+1 \not\to n) \geq_{\mathrm{sW}} (n^2 \not\to n) >_{\mathrm{sW}} (n^2+1 \not\to n)$.

Example. C_k is the problem whose instances are co-enumerations of non-empty subsets of $[k]$, with the solutions to any such instance being all $i < k$ not enumerated.

Thm. $\mathsf{C}_3 \leq_{\mathrm{W}} (8 \not\to 2)'$. [With computer help.]

We are not aware of a general theory to study these cases.

Thank you for your attention!