Reductions and (resolvable) combinatorial designs

Goh Jun Le
Joint work with David Belanger, Damir Dzhafarov (ongoing)

Asian Logic Conference, Tianjin, China
Oct 2023

Pigeonhole principle: If $m > n$, there is no injection $f : m \to n$.

View this as a problem:

$(m \not\to n)$

- Given an instance $f : m \to n$,
- a solution is any pair $i < j < m$ such that $f(i) = f(j)$.

Another relevant problem:
For fixed k, define:

id_k

- Given an instance $j \in [k]$,
- a solution is j itself.

Uniformly computable reductions between problems

A problem P is strongly Weihrauch reducible to a problem Q if there is a forward functional Φ and a backward functional Ψ such that:

- Given a name p for a P-instance,

  $$\Phi(p)$$

  names a Q-instance.
- Given a name q for any Q-solution of $\Phi(p)$,

  $$\Psi(q)$$

  names a P-solution to the P-instance named by p.

We write $\mathsf{P} \leq_{\mathrm{sW}} \mathsf{Q}$.

P is Weihrauch reducible to Q if the above holds with $\Psi(q)$ replaced by $\Psi(p, q)$. We write $\mathsf{P} \leq_{\mathrm{W}} \mathsf{Q}$.

Basic facts

Proposition

$\mathrm{id}_2 <_{\mathrm{sW}} \mathrm{id}_3 <_{\mathrm{sW}} \dots$

Proposition

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

Proposition

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

- $\leq$: $\Phi(f) = \langle i, j \rangle$, where $i < j$ is the least pair such that $f(i) = f(j)$. $\Psi(\langle i, j \rangle) = \{i, j\}$.
- $\geq$: For each pair $i < j$, there is a function $\Phi(\langle i, j \rangle) : n+1 \to n$ such that $i < j$ is the unique pair with $f(i) = f(j)$.

$m \geq n^2$: The edge of id_k's relevance

Proposition

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

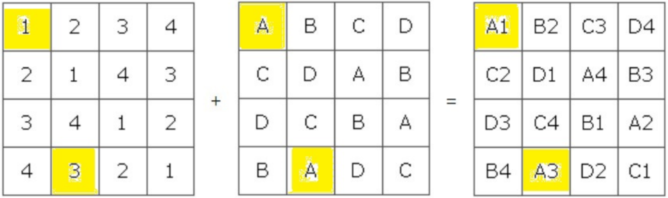
$\Phi(1)$: Arrange n^2 as an $n \times n$ grid and partition using vertical lines.
$\Phi(2)$: Partition using horizontal lines instead.
$\Psi(\{i, j\})$: Return 1 if i and j lie in the same vertical line, otherwise return 2.

Proof by contradiction: Given any two functions $\Phi(1), \Phi(2) : n^2 + 1 \to n$, there is some pair $i \neq j$ such that

$$\Phi(1)(i) = \Phi(1)(j) \quad \text{and} \quad \Phi(2)(i) = \Phi(2)(j).$$

(Apply pigeonhole twice.) So $\Psi(\{i, j\})$ equals both 1 and 2.

More on $m = n^2$: Orthogonal Latin squares



Picture from The 36 officers problem by Marianne Freiberger, published in *Plus* (terrible coloring by me)

The above shows $\mathrm{id}_{2+2} = \mathrm{id}_4 \leq_{\mathrm{sW}} (16 \not\to 4)$:

- Each of the two Latin squares on the left yields a partition of 16 into 4 classes (of size 4)
- We get two more partitions by considering columns and rows respectively
- From a solution (i.e., 2 out of 16 small squares) we can uniquely reconstruct which partition it "came from"

More on $m = n^2$: Mutually orthogonal Latin squares

The arguments on the previous slide can be extended as follows:

- Given k many $n \times n$ Latin squares which are mutually orthogonal, we can build a reduction from id_{k+2} to $(n^2 \not\rightarrow n)$.
- Given a reduction from id_{k+2} to $(n^2 \not\rightarrow n)$, we can read off k mutually orthogonal $n \times n$ Latin squares.

Theorem

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

The number of mutually orthogonal Latin squares which may exist is unknown, for many values of n.

Corollary

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

For many values of n, it is unknown whether there exists a finite affine plane of order n.

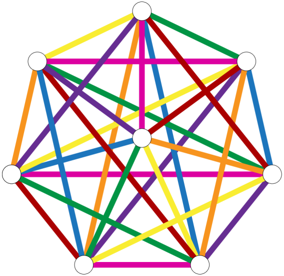
$m \leq 2n$: Reductions using graph packings

A perfect matching on $2n$ vertices corresponds to a function $2n \to n$.

Proposition

$\mathrm{id}_{2n-1} \leq_{\mathrm{sW}} (2n \not\to n)$.

Key fact: K_{2n} can be decomposed into $2n-1$ perfect matchings.



1-factorization of K_8, David Eppstein

Similar results (of the form $\mathrm{id}_k \leq_{\mathrm{sW}} (m \not\to n)$ for $n+1 \leq m \leq 2n$) can be obtained using:

- decompositions of K_m into almost perfect matchings
- decompositions of K_m into Hamiltonian cycles.

$m = qn$, $q \leq n$: Resolvable combinatorial designs

A resolvable balanced incomplete block design (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 $[m]$ (each called a parallel class).

Example

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

Proposition

If there is some RBIBD(qn, q)*, then* $\mathrm{id}_{\frac{qn-1}{q-1}} \leq_{\mathrm{sW}} (qn \not\to n)$.

(Elementary arguments prove that if there is some RBIBD(qn, q), then $q - 1 \mid qn - 1$ and $q \leq n$.)

A counting lemma

Using convexity we can prove:

Lemma

Each function $f : qn \to n$ has at least $n\binom{q}{2}$ solutions. Furthermore, if f has exactly $n\binom{q}{2}$ solutions, then $|f^{-1}(j)| = q$ for every $j < n$.

Theorem

There exists some $\mathrm{RBIBD}(qn, q)$ *if and only if* $\mathrm{id}_{\frac{qn-1}{q-1}} \leq_{\mathrm{sW}} (qn \not\to n)$.

The theorem generalizes our corollary on affine planes (which is the extreme case $q = n$).

The other extreme ($q = 2$) is the result which was proved by decomposing K_{2n} into perfect matchings.

More applications of the counting lemma

Lemma

$\mathrm{id}_k \not\leq_{\mathrm{sW}} (qn \not\to n)$ as long as $k > \frac{qn-1}{q-1}$.

Similar methods yield analogous nonreductions for $(m \not\to n)$ even if n does not divide m.

Corollary

For all $n \geq 3$, $(n+2 \not\to n) <_{\mathrm{sW}} \mathrm{id}_{\binom{n+1}{2}} \equiv (n+1 \not\to n)$.

Corollary

$(2n+1 \not\to n) <_{\mathrm{sW}} (2n \not\to n)$.

So we know at least (for $n \geq 3$):

$$
\begin{aligned}
&(n+1 \not\leftrightarrow n) \\
>\ &(n+2 \not\leftrightarrow n) \\
\geq\ &(2n \not\leftrightarrow n) \\
>\ &(2n+1 \not\leftrightarrow n) \\
\geq\ &(n^2 \not\leftrightarrow n) \\
>\ &(n^2+1 \not\leftrightarrow n) \\
\geq\ &\cdots
\end{aligned}
$$

Jump of $(m \not\to n)$: Motivations from reverse math

Theorem (Dimitracopoulos, Paris 1986; Hirst 1987)

Over RCA_0, *TFAE:*

- *The infinite pigeonhole principle*
- $(\forall n)$(*there is no* Σ^0_2 *injection* $f : n+1 \to n$).

Theorem (Belanger, Chong, Wang, Wong, Yang 2021)

Over RCA_0,

$$(\forall n)(\text{there is no } \Sigma^0_2 \text{ injection } f : 2n \to n)$$
$$\nvdash (\forall n)(\text{there is no } \Sigma^0_2 \text{ injection } f : n+1 \to n).$$

They proved that $(\forall n)$(there is no Σ^0_2 injection $f : 2n \to n$) characterizes the first-order theory of a variant of weak weak König's lemma.

Definition (Brattka, Gherardi, Marcone 2011)

For any problem P, the jump of P, denoted P', is the problem whose:

- instances are limit approximations to names of P-instances
- solutions are P-solutions to the limit P-instance.

Example

$\mathrm{id}'_k \equiv_{\mathrm{sW}} \mathsf{lim}_k$.

Proposition (Brattka, Gherardi, Marcone 2011)

For all problems P *and* Q, *if* $\mathsf{P} \leq_{\mathrm{sW}} \mathsf{Q}$, *then* $\mathsf{P}' \leq_{\mathrm{sW}} \mathsf{Q}'$.

The converse holds, but with continuous sW-reducibility $\leq^{\mathrm{c}}_{\mathrm{sW}}$:

Theorem (essentially Brattka, Hölzl, Kuyper 2017)

If $\mathsf{P} \not\leq^{\mathrm{c}}_{\mathrm{sW}} \mathsf{Q}$, *then* $\mathsf{P}' \not\leq^{\mathrm{c}}_{\mathrm{sW}} \mathsf{Q}'$.

Lifting our previous results

All reductions $\mathrm{id}_k \leq_{\mathrm{sW}} (m \not\to n)$ lift to $\lim_k \leq_{\mathrm{sW}} (m \not\to n)'$, even $\lim_k \leq_{\mathrm{W}} (m \not\to n)'$. Same for nonreductions.

Theorem

TFAE:

1. $\lim_k \leq_{\mathrm{W}} (m \not\to n)'$
2. $\lim_k \leq_{\mathrm{sW}} (m \not\to n)'$
3. $\lim_k \leq_{\mathrm{sW}}^{\mathrm{c}} (m \not\to n)'$
4. $\mathrm{id}_k \leq_{\mathrm{sW}}^{\mathrm{c}} (m \not\to n)$
5. $\mathrm{id}_k \leq_{\mathrm{sW}} (m \not\to n)$

(1) $\Rightarrow$ (2): Next slide.
(3) $\Rightarrow$ (4): Apply the theorem of Brattka, Hölzl, Kuyper.
(4) $\Rightarrow$ (5): Given a reduction, the forward and backward functionals are automatically continuous.
(5) $\Rightarrow$ (2): Apply the proposition of Brattka, Gherardi, Marcone.

Upgrading $\leq_{\mathrm{W}}$ to $\leq_{\mathrm{sW}}$

Definition (Dorais, Dzhafarov, Hirst, Mileti, Shafer 2016)

A problem P is finitely tolerant if there is a partial computable function T such that given any two P-instances with finite difference, a bound after which they agree, and a P-solution of one of the instances, T computes a solution for the other.

Examples include RT^n_k, COH, $\lim_X$.

Lemma (Dzhafarov, G., Hirschfeldt, Patey, Pauly 2020)

Suppose

- *all* P- *and* Q*-solutions lie in a fixed finite set*
- *any finite modification of a* P*-instance is still a* P*-instance*
- P *is finitely tolerant.*

Then if $\mathsf{P} \leq_{\mathrm{W}} \mathsf{Q}$*, we have* $\mathsf{P} \leq_{\mathrm{sW}} \mathsf{Q}$*.*

Apply the lemma with $\mathsf{P} = \lim_k$ and $\mathsf{Q} = (m \not\to n)'$.

Weihrauch degree of $(m \not\to n)'$: $m = n^2 + 1$

Recall: $\mathrm{id}_2 \not\leq_{\mathrm{sW}} (n^2 + 1 \not\to n)$. So $\lim_2 \not\leq_{\mathrm{W}} (n^2 + 1 \not\to n)'$. More is true:

All-or-unique choice AoUC_k is C_k restricted to $\{k\} \cup \{\{i\} : i \in k\}$.

Fact

$\mathsf{AoUC}_k <_{\mathrm{W}} \lim_2$ (LPO, even).

Proposition

$\mathsf{AoUC}_{\binom{n+1}{2}+1} \not\leq_{\mathrm{W}} (n^2 + 1 \not\to n)'$.

Our AoUC-instance pretends to be "all" until Ψ commits on "enough" pairs, then diagonalizes against Ψ's outputs on said pairs. We can arrange "enough" so that some pair persists as a solution after diagonalization.

Weihrauch degree of $(m \not\to n)'$: $m = n^3$ and more

All-or-co-unique choice ACC_k is $\mathsf{C}_k \restriction \{k\} \cup \{k - \{i\} : i < k\}$.

$$\mathsf{C}_2 \equiv_{\mathrm{W}} \mathsf{ACC}_2 >_{\mathrm{W}} \mathsf{ACC}_3 >_{\mathrm{W}} \dots \qquad \text{(Weihrauch)}$$

Proposition

$\mathsf{ACC}_k \leq_{\mathrm{W}} (n^{k+1} \not\to n)'$ but $\mathsf{ACC}_k \not\leq_{\mathrm{W}} (n^{k+1} + 1 \not\to n)'$.

So we have separations at $n^3, n^4, \dots$, in addition to $n+1$, $2n$, n^2:

Corollary

For all $\ell \geq 3$, $(n^\ell + 1 \not\to n)' <_{\mathrm{W}} (n^\ell \not\to n)'$.
Therefore, $(n^\ell + 1 \not\to n) <_{\mathrm{sW}} (n^\ell \not\to n)$.

Fun sidenote

Could we perhaps prove the nonreductions

$$\mathsf{AoUC}_{\binom{n+1}{2}+1} \not\leq_{\mathrm{W}} (n^2+1 \not\to n)'$$
$$\mathsf{ACC}_k \not\leq_{\mathrm{W}} (n^{k+1}+1 \not\to n)'$$

by lifting some nonreduction of the form

$$\mathsf{P} \not\leq_{\mathrm{sW}} (n^k+1 \not\to n)?$$

No: $\mathsf{AoUC}_{\binom{n+1}{2}+1}$ and ACC_k do not bound any noncomputable P'.

(The same is true more generally of LPO.)

An adhoc reduction: $\mathsf{C}_3 \leq_{\mathrm{W}} (8 \not\to 2)'$

From before we know $\mathsf{C}_2 \leq_{\mathrm{W}} (8 \not\to 2)'$. We improve this to

Theorem

$\mathsf{C}_3 \leq_{\mathrm{W}} (8 \not\to 2)'$.

For each initial segment of a given name for a C_3-instance, we represent the information so far as a string:

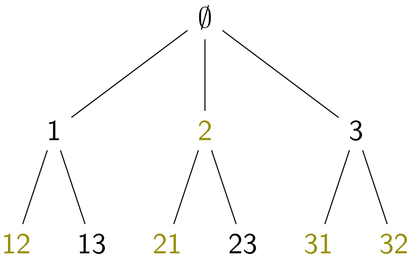
$\emptyset$ (nothing has entered the complement so far), or

a (*a* has entered the complement), or

ab (*a* has entered the complement, followed by *b*)

ab is different from *ba*!

Definition of Φ witnessing $\mathsf{C}_3 \leq_{\mathrm{W}} (8 \not\to 2)'$



$$
\begin{aligned}
f_\emptyset &= (1234)(5678)\\
f_1 &= (1256)(3478)\\
f_{12} = f_{21} &= (1278)(3456)\\
f_3 = f_{13} &= (1458)(2367)\\
f_2 = f_{32} &= (1357)(2468)\\
f_{23} &= (1368)(2457)\\
f_{31} &= (1467)(2358)
\end{aligned}
$$

What should $\Psi(p, \{1, 7\})$ do?

- $\{1, 7\}$ is a solution of f_{12}, f_{21}, f_2, f_{32}, f_{31}.
- So $\Psi(p, \{1, 7\})$ can wait for the first number to appear in p.
- If the first number is 1 or 2, Ψ can answer 3.
- If the first number is 3, Ψ knows that a second number (1 or 2) will appear in p. So Ψ can wait for the second number and answer accordingly.

Thanks!

Definition of $\Psi(p, \{i, j\})$ witnessing $\mathsf{C}_3 \leq_{\mathrm{W}} (8 \not\to 2)'$

$\{i, j\}$	Possible $\lim \Phi(p)$	Ψ's action
$\{1, 2\}$	$f_\emptyset$, f_1, f_{12}, f_{21}	Output 3
$\{1, 3\}$	$f_\emptyset$, f_2, f_{32}, f_{23}	Output 1
$\{1, 4\}$	$f_\emptyset$, f_3, f_{13}, f_{31}	Output 2
$\{1, 5\}$	f_1, f_3, f_{13}, f_2, f_{32}	1 in $p \to$ output 2
		2 or 3 in $p \to$ output 1
$\{1, 6\}$	f_1, f_{23}, f_{31}	1 or 3 in $p \to$ output 2
		2 in $p \to$ output 1
$\{1, 7\}$	f_{12}, f_{21}, f_2, f_{32}, f_{31}	1 or 2 in $p \to$ output 3
		31 in $p \to$ output 2
		32 in $p \to$ output 1
$\{1, 8\}$	f_{12}, f_{21}, f_3, f_{13}, f_{23}	3 in $p \to$ output 1
		12 or 21 in $p \to$ output 3
		13 in $p \to$ output 2
		23 in $p \to$ output 1

$\vdots$