Randomness notions in Muchnik and Medvedev degrees

Kenshi Miyabe @ Meiji University
joint work with Rupert Hölzle

CTFM2016 @ Waseda University
20 Sep 2016
Motivation
Main Question

Could we construct a more random set from a given random set?

How to formalize? Why important?
Computable

- Logicians … computable by a Turing machine

- Mathematicians … a formula can be simplified such as 2+3, 2x+1+4x, some integration, etc.

- Statisticians and data scientists … computable with random access
With random access

Which sets are computable with random access?

An old answer: computable sets
Theorem (De Leeuwe, Moore, Shannon, Shapiro (1956), Sacks). *If A is not computable, then the class*

\[ \{ X \in 2^\omega : A \leq_T X \} \]

*has measure 0.*

So, if a set is computable with random access, then the set should be computable. The story is over, in this case.

One variant is the case of poly-time computability, which is the famous question of BPP = P?
If there many answers,

- Problem: Construct some non-computable set.
- Without random access: Impossible.
- With random access: Possible.

- How difficult is it to compute a set in a given class?
Definition. Let $P, Q \subseteq 2^\omega$. We say that $P$ is Muchnik reducible to $Q$, denoted by $P \leq_w Q$, if, for every $f \in Q$, there exists $g \in P$ such that $g \leq_T f$.

Loosely speaking, any element in $Q$ can compute some element in $P$. 
Definition. Let $P, Q \subseteq 2^\omega$. We say that $P$ is Medvedev reducible to $Q$, denoted by $P \leq_s Q$, if there exists a Turing functional $\Phi$ such that $\Phi^f \in P$ for every $f \in Q$.

The difference is uniformity.
<table>
<thead>
<tr>
<th>Functional</th>
<th>non-uniform</th>
<th>uniform</th>
</tr>
</thead>
<tbody>
<tr>
<td>reverse math</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Muchnik degree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medvedev degree</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Theorem (Simpson 2004).

\[ 2^\omega \prec_w \text{MLR} \prec_w \text{PA} \]

where

- MLR is the class of all ML-random sets,
- PA is the class of consistent complete extensions of Peano arithmetic.

The class of random sets seems natural examples in Muchnik degrees.
**Theorem** (from algorithmic randomness).

\[ \text{WR} \leftarrow \text{SR} \leftarrow \text{CR} \leftarrow \text{MLR} \]

and

\[ \text{MLR} \leftarrow \text{DiffR} \leftarrow \text{W2R} \leftarrow \text{2R} \leftarrow \text{DemR} \]

*Every arrow is strict.*
Theorem (Muchnik degrees).

\[ WR \leftarrow SR \longrightarrow CR \leftarrow MLR \]

and

\[ MLR \leftrightarrow DiffR \leftrightarrow 2R \]

\[ W2R \longrightarrow 2R \leftarrow \text{DemR} \]
We ask whether each arrow is strict. This can be interpreted as we ask whether we can construct a more random set from a given random set.

In particular, we look at how uniformity plays a role in this setting.
Proof
Theorem.

\[ \text{CR} <_w \text{MLR} \]

Proof. Suppose MLR \(<_w\) CR for a contradiction.

There exists a high minimal degree \( a \) by Cooper ’73.

Then, there exists a computably random set \( X \in a \), because every high degree contains a computably random set by Nies, Stephan, and Terwijn ’05.

By the assumption there exists a ML-random set \( Y \leq_T X \). Since \( a \) is minimal and \( Y \) can not be computable, we have \( Y \equiv_T X \). Thus, the Turing degree of \( Y \) is minimal.

However, any ML-random degree can not be minimal by van Lambalgen’s theorem. \( \square \)
Theorem.

\[ SR \equiv_w CR \]

Proof. Every Schnorr random set can compute a computably random set, because

(i) if the Schnorr random set is not high, then it is already ML-random,

(ii) if the Schnorr random set is high, then it computes a computably random set.

\[ \square \]

Rather non-uniform proof!
Theorem.

$$\text{MLR} \equiv_w \text{DiffR}$$

Proof. Every ML-random set can compute a difference random. Let $X \oplus Y$ be a ML-random set.

(i) If $X \geq_T \emptyset'$, then $Y$ is 2-random, thus difference random.

(ii) If $X \not\geq_T \emptyset'$, then $X$ is difference random.

\[\square\]

Again, non-uniform proof.
Theorem.

\[ MLR <_s \text{DiffR} \]

Theorem.

\[ SR <_s \text{CR} \]
$X \in 2^\omega$ is not computably random if (and only if) $M(X \upharpoonright n) = \infty$ for some computable martingale $M$.

$X \in 2^\omega$ is not Schnorr random if and only if $M(X \upharpoonright f(n)) > n$ for infinitely many $n$ for some computable order $f$ and some computable martingale $M$.

The difference between CR and SR is the rate of divergence.
CR \not\subseteq_s SR means that, for every Turing functional \( \Phi \), there exists \( A \in SR \) such that \( \Phi^A \not\in CR \).

When \( \Phi = id \), it means that there exists \( A \in SR \) such that \( A \not\in CR \).

In fact we extend the method of separating SR and CR.
Construct a random set $A$

Forcing $A(n_k)=0$ in sparse positions
$\Rightarrow$ too sparse not to be Schnorr random

Number of candidates of $n_k$ is small
$\Rightarrow$ so small that some computable martingale succeeds (very slowly)
random part

\[ A(n_0) = 0 \]

random part

\[ A(n_1) = 0 \]

candidates of \( n_0 \)

the number is small

candidates of \( n_1 \)
Construct A in SR and \( B = \Phi(A) \) not in CR

Forcing \( B(n_k) = 0 \) in some positions

Number of candidates of \( n_k \) should be small

However, measure of inverse image may be too small (may be empty) and some computable martingale may succeed in Schnorr sense even if \( n_k \) is very sparse
\[
\begin{align*}
\Phi &\quad \Phi^{-1} \\
\Phi &\quad \text{measure may be small} \\
\Phi &\quad \Rightarrow \text{not Schnorr random}
\end{align*}
\]
Induced measure is “close to” uniform measure
=> The same method can be applied

Induced measure is “far from” uniform measure
=> The another method will be applied
Let $\Phi : \subseteq 2^\omega \rightarrow 2^\omega$ be a.e. computable function. Then, the \textbf{induced measure} $\mu$ is defined by

$$\mu(\sigma) = \lambda(\{X \in 2^\omega : \Phi(X) \in [\sigma]\}).$$

The measure $\mu$ is computable.

The dividing condition is

\textbf{Case 1} $\text{CR}(\mu) \subseteq \text{CR}(\lambda)$
\textbf{Case 2} $\text{CR}(\mu) \not\subseteq \text{CR}(\lambda)$
Case 2: \( \text{CR}(\mu) \not\subseteq \text{CR}(\lambda) \)

Proof. There exists \( Y \in \text{CR}(\mu) \setminus \text{CR}(\lambda) \).

By the no-randomness-from-nothing result for computable randomness by Rute, there exists \( X \in \text{CR}(\lambda) \) such that \( \Phi(X) = Y \).

Then, \( X \in \text{SR} \) and \( \Phi(X) \not\in \text{CR} \). \( \square \)
Case 1: $\text{CR}(\mu) \subseteq \text{CR}(\lambda)$

**Lemma.** Let $\mu, \nu$ be computable measures. Then, we have $\text{CR}(\mu) \subseteq \text{CR}(\nu) \Rightarrow \text{MLR}(\mu) \subseteq \text{MLR}(\nu) \Rightarrow \nu \ll \mu$.

*Here, $\ll$ means absolute continuity.*
Case 1: $\text{CR}(\mu) \subseteq \text{CR}(\lambda)$

**Lemma.** Let $\Phi : \subseteq 2^\omega \to 2^\omega$ be an a.e. computable function. Let $\mu$ be the measure induced from $\Phi$ and $\lambda$. Assume that $\lambda \ll \nu$. Then, for each $\sigma \in 2^{<\omega}$, we have

$$\lim_{n \to \infty} \lambda\{ X \in [\sigma] : \Phi(X)(n) = 0 \} = \frac{1}{2} \lambda(\sigma).$$

**Proof.** By the Radon-Nikodym theorem and Lévy’s zero-one law. \qed
We studied randomness notions in Muchnik degrees and Medvedev degrees. They are related to reverse maths and Weihrauch degrees.

We found two problems that is possible non-uniformly but impossible uniformly.

Interesting interaction between analysis and computability.