New Directions in Randomness

Jason Rute

Pennsylvania State University

Computability, Complexity, and Randomness
June 22–26

Slides available at
www.personal.psu.edu/jmr71/

(Updated on June 22, 2015.)

Introduction

The goals

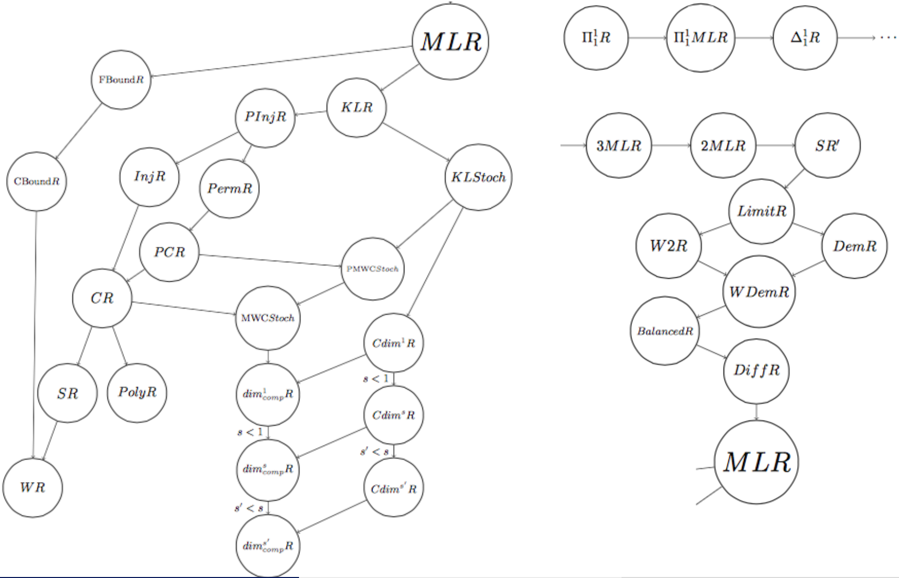
- To make you think about randomness in a new way.
- What is a randomness notion?
- What is a natural randomness notion?
- Can randomness be studied as a theory? Like the theory of groups?
- Can we axiomatize algorithmic randomness?

Organizing the randomness zoo

The Heidelberg zoo

The randomness zoo

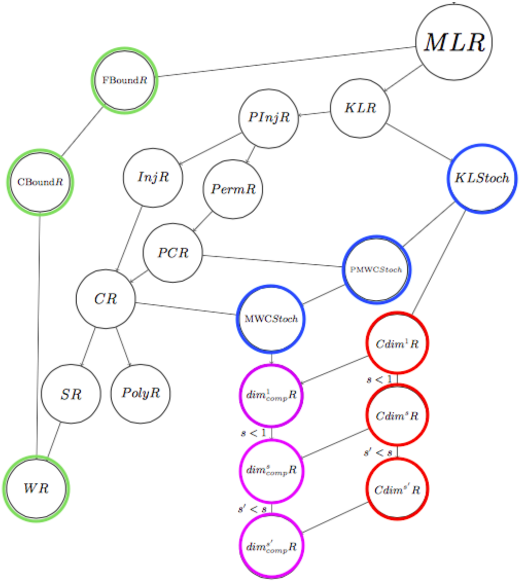
Antoine Taveneaux



Organizing the randomness zoo

Step 1: Organize by σ-ideals

Some randomness notions are not like the others



- Kurtz-like (green)
- Stochastic (blue)
- Partial randomness (purple/red)

- This can largely be explained via σ-ideals.

σ-ideals

- A **σ-ideal** is a collection of sets closed downward and under countable unions.
- Each σ-ideal $\mathcal{I}$ provides a notion of "small set" or "null set".
- Examples:
  - meager sets
  - null sets
  - sets of Hausdorff dimension $\leqslant s$ (for a fixed $0 \leqslant s \leqslant 1$).
- Every "randomness" notion is associated with a σ-ideal $\mathcal{I}$.

Example: σ-ideals of Kurtz randomness

- $x \in 2^{\mathbb{N}}$ is **Kurtz random** (or **weak random**) if x is not in any Π^0_1 null set.
- Common complaint: “Kurtz randomness is really a genericity notion.”

- Let Kurtz^A be the set of A-Kurtz random sequences for the oracle A.
- Let $\mathcal{I}_{\mathsf{Kurtz}}$ be the σ-ideal of subsets of $2^{\mathbb{N}} \smallsetminus \mathsf{Kurtz}^A$ for some A.
- $\mathcal{I}_{\mathsf{Kurtz}}$ is the exactly the σ-ideal of subsets of F_σ (i.e. $\mathbf{\Sigma}^0_2$) null sets.
- These are the null sets associated with Riemann integrable functions, a.e. continuous functions, and Jordan-Peano measurable sets.
- $\mathcal{I}_{\mathsf{Kurtz}}$ is a sub-σ-ideal of both the ideals of meager sets and the ideal of null sets.

- Kurtz randomness is both a genericity notion and a randomness notion.

σ-ideals and their "randomness notions"

σ-Ideal	Randomness (Genericity) notions
Meager	weakly 1-generic, 1-generic
Subsets of F_σ-null	Kurtz, finite bounded, Kurtz$^{\emptyset'}$
(Lebesgue) null	**Sch, CR, ML, W2R, 2R, etc.**
μ-null	**μ-Sch, μ-CR, μ-ML, μ-W2R, μ-2R, etc.**
Hausdorff dimension $\leqslant s$	Sch-dim $> s$, cdim $> s$
Null s-dim. Hausdorff measure	strong s-randomness: $KM(x \upharpoonright n) \geqslant^+ sn$
Null s-dim. Riesz capacity	s-energy randomness: $\sum_n 2^{sn-KM(x\upharpoonright n)} < \infty$

- It is not clear what the σ-ideals are for
  - the stochasticity notions
  - constructive dimension = 1
  - (weak) s-randomness
  - UD randomness
- However, they are clearly not the σ-ideal of Lebesgue null sets.

σ-ideal zoo

$$\begin{tikzcd}
\begin{array}{c}\text{meager}\\ \text{(W1G, 1G)}\end{array} & & \begin{array}{c}\textbf{NULL}\\ \text{(SR, MLR)}\end{array} & \\
& \begin{array}{c}\subseteq \text{null } F_\sigma\\ \text{(Kurtz)}\end{array} \arrow[ul] \arrow[ur] & & \begin{array}{c}s\text{-Riesz null}\\ (s\text{-energy rand})\end{array} \arrow[ul] \\
& & & \begin{array}{c}s\text{-Hausdorff null}\\ (\text{strong } s\text{-rand})\end{array} \arrow[u] \\
& & & \begin{array}{c}\text{Hdim} \leqslant s\\ (\text{cdim} > s)\end{array} \arrow[u]
\end{tikzcd}$$

- From here on, we will focus on the σ-ideal of Lebesgue (or μ-) null sets.

Organizing the randomness zoo

Step 2: Organize by computability

True randomness vs. algorithmic randomness

- x is **truly random** if x avoids every null set.
- Except for a pesky problem...

- Our "solution" is to consider **algorithmic** null sets.
- However, what type of algorithmic?

Levels of computability in algorithmic randomness

Poly-time randomness notions

- Poly-time Schnorr random
- Poly-time random
- ...
- Computable randomness notions
    - Schnorr random
    - Computably random
    - Martin-Löf random
    - Weak 2-random
    - 2-random
    - ...
    - Higher randomness notions
        - Δ^1_1 random
        - Π^1_1 MLR random
        - Π^1_1 random
        - ...

- Forcing randomness notions
    - Solovay genericity
    - ...
    - "Pointless" randomness notions
        - True randomness

- **From now on, we will just work at the computable level.**

Organizing the randomness zoo

Step 3: Mark the minimal sufficient randomness notion in each computability level

Schnorr randomness is sufficient

- A **μ-Schnorr test** is a computable sequence of Σ^0_1 sets such that $\mu(U_n) \leqslant 2^{-n}$ and $\mu(U_n)$ is computable in n.
- x is **μ-Schnorr random** if $x \notin \bigcap_n U_n$ for any μ-Schnorr test.

- Schnorr randomness is closely connected to constructive mathematics.
- See the slides for my VAI 2015 talk (available on my webpage).
- Schnorr null sets where first called "null sets in the sense of Brouwer."
- Constructively provable a.e. theorems are true for Schnorr randomness.

Schnorr randomness is minimally sufficient

- Schnorr randomness is the minimal randomness notion for working with **computable measurable objects.**

Definition

A function $f\colon 2^{\mathbb{N}} \to \mathbb{R}$ is **L^1-computable** if there is a computable sequence of rational step functions f_n such that

$$\|f_n - f\|_1 = \int |f_n - f|\, d\mu \leqslant 2^{-n}.$$

- Only on Schnorr randoms is the convergence of $f_n(x)$ guaranteed.
- Moreover, if the computable sequence g_n also converges rapidly to f in L^1, then $\lim_n g_n(x) = \lim_n f_n(x)$ for all Schnorr randoms x.

- This is one of many such similar examples.

Other computability notions

- There is no obvious reason why these ideas cannot be extended to lower and higher computability notions.

Conjectures

1. **Poly-time Schnorr randomness** is the minimal sufficient randomness notion with respect to **poly-time computability**.
2. **Higher Schnorr randomness** (i.e. Δ^1_1 **randomness**) is the minimal sufficient randomness notion with respect to **higher computability**.

- These conjectures extend to basically every idea in this talk.

Organizing the randomness zoo

Step 4:
Separate the wheat from the chaff,
the sheep from the goats,
the good randomness notions from the bad

Work with many randomness notions at once

- Why prove a theorem for one randomness notion when you can prove it for all of them?

- For example, the theorem

  Schnorr randomness satisfies the strong law of large numbers.

  holds for all stronger randomness notions (CR, MLR, W2R, 2R, etc.).

- However, many theorems of randomness are not of this form.
- For example,

  Schnorr randomness is closed under computable permutations of bits.

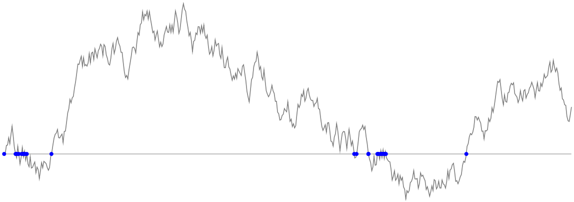
  is not satisfied by partial computable randomness (PCR) even though PCR is stronger than Schnorr randomness.

Developing a framework of randomness notions

- The rest of this talk is devoted to developing a **system of axioms** which are sufficient for **working with randomness in practice**.
- The randomness notions satisfying these axioms are the natural ones.
- The unnatural ones should be demoted to footnotes in our zoo.

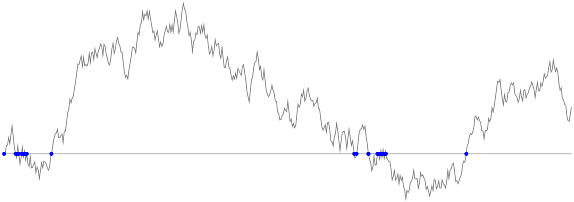
Properties desired of an algorithmic randomness notion

A very informal guiding principle



- A natural randomness notion should be sufficient for working constructively with Brownian motion

Extendable to other spaces



- Brownian motion is given by the Wiener measure on $C[0,1]$ or $C[0,\infty)$.

Generalization

Randomness should generalize to all computable probability spaces $(\Omega, \mathbf{P})$.

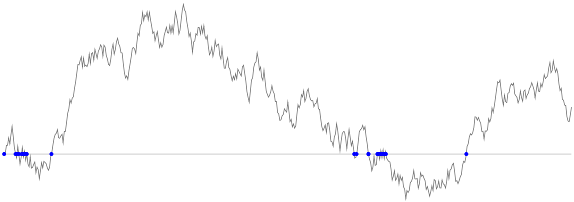
Extendable to other spaces

- Schnorr randomness, Martin-Löf randomness, weak-n-randomness, n-randomness are all naturally extendable to other spaces.
- Computable randomness also has a consistent extension to other probability spaces (R.).
  - A **measure bounded integral test** on (X, μ) is a lowersemicomputable function $t \colon X \to [0, \infty]$ and a computable measure ν such that

$$\int_A t(x)\, d\mu(x) \leqslant \nu(A) \quad (A \subseteq X \text{ measurable}).$$

  - $x \in X$ is **μ-computably random** if $t(x) < \infty$ for all measure bounded integral tests t.
- For some of the more combinatorial randomness notions (e.g. partial computable randomness or Kolmogorov-Loveland randomness) it is not so clear.

Invariant under isomorphisms



- Brownian motion can be transformed via a number of isomorphisms.
- For example, if $B(t)$ is a BM, then the following are BMs:

$$-B(t) \qquad \text{and} \qquad tB(1/t).$$

- Moreover, all the standard constructions of BM are isomorphisms between other probability spaces and the Wiener measure.

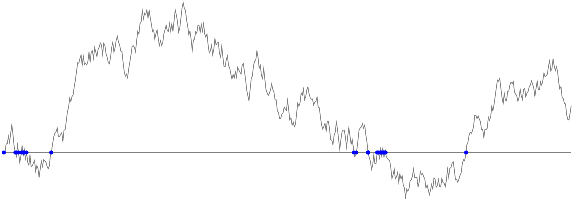
Preservation under isomorphisms

If $I\colon (\Omega_1, \mathbf{P}_1) \simeq (\Omega_2, \mathbf{P}_2)$ is an effectively measurable isomorphism, then ω is $\mathbf{P}_1$-random if and only if $I(\omega)$ is $\mathbf{P}_2$-random.

Invariant under isomorphisms

- Schnorr randomness, Martin-Löf randomness, weak-n-randomness, n-randomness are all invariant under isomorphisms.
- Computable randomness is also invariant under isomorphisms (R.).
- Partial computable randomness is not invariant under permutations of bits.

Randomness preservation



- The probability distribution of $B(1)$ is the Gaussian measure on $\mathbb{R}$.
- In other words, the Gaussian measure is the push-forward of the Wiener measure along the map $B \mapsto B(1)$.

Preservation of randomness

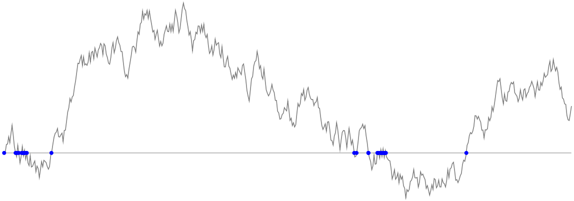
Assume $T\colon (\Omega, \mathbf{P}) \to (X, \mathbf{P}_T)$ is an effectively measurable map. If ω is $\mathbf{P}$-random, then $T(\omega)$ is $\mathbf{P}_T$-random. (Here $\mathbf{P}_T$ is the pushforward measure of $\mathbf{P}$ along T.)

Randomness preservation

- Schnorr randomness, Martin-Löf randomness, weak-n-randomness, n-randomness all satisfy randomness preservation.
- Computable randomness does not (Bienvenu/Porter; R.).

- Although, I will have more to say about this in a bit...

Equivalent measures share randoms



- The Gaussian measure and the Lebesgue measure on $\mathbb{R}$ are equivalent measures, i.e. they have the same null sets.

Equivalent measures share randoms

"Effectively equivalent" measures have the same randoms.

Equivalent measures share randoms

- This property can be stated with the following two properties.

Equivalent measures share randoms

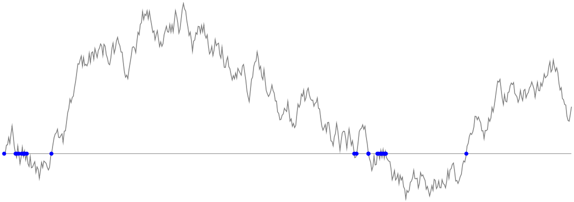
1. If x is μ-random and $\mu \leqslant c\nu$ for some constant c, then x is ν-random.
2. Assume $\mu \ll \nu$ with an $L_1(\nu)$-computable density $f = \frac{d\mu}{d\nu}$, that is

$$\mu(A) = \int_A f\, d\nu \quad (A \subseteq X).$$

Then, x is μ-random iff both x is ν-random and $f(x) > 0$

- The standard randomness notions satisfy both of these:
  - SR, CR, MLR, n-random, weak n-random

No randomness from nothing



- Again consider that a Gaussian distribution can be found from a Brownian distribution.

No randomness from nothing (a.k.a no randomness ex nihilo)

Assume $T\colon (\Omega, \mathbf{P}) \to (X, \mathbf{P}_T)$ is an effectively measurable map. If x is $\mathbf{P}_T$-random, then there is a $\mathbf{P}$-random ω such that $x = T(\omega)$.

No randomness from nothing

- No-randomness-from-nothing holds for Martin-Löf randomness, n-randomness, weak 2-randomness, difference randomness.

Theorem (R.)

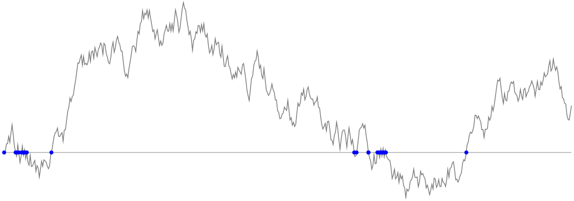
- No-randomness-from-nothing holds for computable randomness.
- However, it does not hold for Schnorr randomness:
- If x is not CR, then there is a measure-preserving almost-everywhere computable map T such that the preimage of x under T is empty.

Theorem (R.)

- Martin-Löf randomness is the smallest randomness notion satisfying both no-randomness-from-nothing and randomness preservation.

- It is interesting (but not damning!) that NRFN fails for SR.

Van Lambalgen and combining measures



- A Brownian motion on $[0,1]$ can be **constructed** by "gluing together" two independent BM on $[0,1/2]$.
- And vice versa, a Brownian motion on $[0,1]$ can be **decomposed** into two independent BM on $[0,1/2]$.

Van Lambalgen's theorem

(ω_1, ω_2) is $\mathbf{P}_1 \times \mathbf{P}_2$-random iff ω_1 is $\mathbf{P}_1$-random and ω_2 is $\mathbf{P}_2$-random independently of ω_1.

Independence

Van Lambalgen's theorem

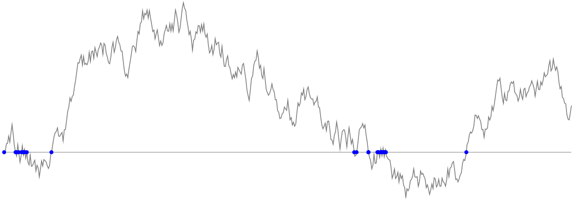
(ω_1, ω_2) is $\mathbf{P}_1 \times \mathbf{P}_2$-random iff ω_1 is $\mathbf{P}_1$-random and ω_2 is $\mathbf{P}_2$-random **independently of** ω_1.

- "Independent" is often taken one of two ways:
  - ω is $\mathbf{P}$-random **relative** to A means there is no test T^A computable from A that derandomizes ω.
  - ω is $\mathbf{P}$-random **uniformly relative** to A means there is no computably indexed family of tests $\{T^B\}$, one test for each oracle B, such that T^A derandomizes ω.
- For Martin-Löf and n-randomness, relative and uniformly relative are the same.
- (Others have suggested that "independent" should mean whatever makes van Lambalgen's theorem holds.)

Van Lambalgen's theorem

- Martin-Löf randomness and n-randomness satisfy van Lambalgen's theorem with both **uniform relativization** and **relativization** (because they are the same!).
- The following satisfy van Lambalgen's theorem for **uniform relativization**:
  - Schnorr randomness (Miyabe; Miyabe and R.)
  - Demuth randomness (Diamondstone, Greenberg, Turetsky)
- For computable randomness
  - One direction is true for **uniform relativization** (Miyabe and R.).
  - The other direction fails for both types of relativization (Bauwens, last week!)
- For other types of randomness, the details are not fully worked out.

Van Lambalgen's theorem gives other results



- Notice that one can construct a Brownian motion with two steps:
  1. Choose a value a at $t = 1$ from a Gaussian distribution.
  2. Connect $(0,0)$ to $(1,a)$ via a **Brownian bridge ending at a**
- The distribution in the second step is computable uniformly from the chosen a.
- Using this idea we can, in many cases, recover randomness preservation for computable randomness and no-randomness-from-nothing for Schnorr randomness.

Generalized van Lambalgen's theorem

- Let $(\Omega_1, \mathbf{P}_1)$ be a computable probability measure.
- Let $\mathbf{P}(\cdot \mid \omega)$ be a **computable kernel**, that is a family of probability measures on the space Ω_2 such that the map $\omega \mapsto \mathbf{P}(\cdot|\omega)$ is effectively measurable.
- Combine $\mathbf{P}_1$ and $\mathbf{P}(\cdot \mid \omega)$ into one probability space $(\Omega_1 \times \Omega_2, \mathbf{P})$ via

$$\mathbf{P}(A \times B) = \int_A \mathbf{P}(B \mid \omega_1)\, d\mathbf{P}_1(\omega_1).$$

Generalized van Lambalgen's theorem

(ω_1, ω_2) is $\mathbf{P}$-random iff ω_1 is $\mathbf{P}_1$-random and ω_2 is **$\mathbf{P}(\cdot \mid \omega_1)$-random** independently of ω_1.

- Besides interpreting "independently", we also have to figure out what "$\mathbf{P}(\cdot \mid \omega_1)$-random" means since this measure may not be computable
- It could mean using $\mathbf{P}(\cdot \mid \omega_1)$ as an oracle.
- It could mean using $\mathbf{P}(\cdot \mid \omega_1)$ uniformly as an oracle.

Generalized van Lambalgen's theorem

- Generalized van Lambalgen's theorem holds for
  - Martin-Löf randomness (Takahashi)
  - Schnorr randomness (R., using uniform relativization)

Van Lambalgen's theorem for maps

- Assume $T\colon (\Omega, \mathbf{P}) \to (X, \mathbf{P}_T)$ is an effectively measurable map.
- Assume the conditional probability $x \mapsto \mathbf{P}(\cdot \mid T = x)$ is effectively measurable as a map from $(X, \mathbf{P}_T)$ to measures.

van Lambalgen's theorem for maps

$$\begin{pmatrix} \omega \text{ is } \mathbf{P}\text{-random} \\ \& \quad x = T(\omega) \end{pmatrix} \Leftrightarrow \begin{pmatrix} x \text{ is } \mathbf{P}_T\text{-random} \quad \& \\ \omega \text{ is } \mathbf{P}(\,\cdot \mid T = x)\text{-random independent of } x \end{pmatrix}$$

- The $\Rightarrow$ direction is a stronger version of randomness preservation.
- The $\Leftarrow$ version is a stronger version of no-randomness-from-nothing.
- It also lets one prove that if $P \ll Q$ with an L^1-computable density function f, then x is P-random if and only if x is Q-random and $f(x) > 0$.

Proposed axioms of randomness

Tentative randomness axioms

- $\langle x, \mu, a \rangle \in \mathcal{R}$ means x is μ-random independent of a.

- Axiom 1: For all μ and a, $\mu\{x : \langle x, \mu, a \rangle \in \mathcal{R}\} = 1$.
- Axiom 2: If $\langle x, \mu, a \rangle \in \mathcal{R}$, then x is μ-Schnorr random uniformly relativized to a.
- Axiom 3: If b is computable uniformly in (a, μ), then $\langle x, \mu, a \rangle \in \mathcal{R}$ implies $\langle x, \mu, b \rangle \in \mathcal{R}$.
- Axiom 4: If μ is computable uniformly in a, $T \colon \Omega \to \Omega$ is μ-effectively measurable uniformly in a, and $y \mapsto \mu(\cdot \mid T = y)$ is μ_T-effectively measurable uniformly in a, then

$$\begin{pmatrix} \langle x, \mu, a \rangle \in \mathcal{R} \\ \text{and } y = T(x) \end{pmatrix} \Leftrightarrow \begin{pmatrix} \langle y, \mu_T, a \rangle \in \mathcal{R} \text{ and} \\ \langle x, \mu(\cdot \mid T = y), (y, a) \rangle \in \mathcal{R} \end{pmatrix}.$$

Work in progress

- These axioms are a work in progress.
- However, I can already do cool things with them.
- I have a new randomness reducibility as well.
- It treats randoms as infinitesimally small point masses and compares their relative masses.
- It says, for example, if $x \in 2^{\mathbb{N}}$ is random on the Lebesgue measure, then $0x$ is exactly half as random as x.
- There are now more questions than answers.

Other randomness axioms

- van Lambalgen two related axiomatizations of randomness.
- Alex Simpson is currently developing a set theoretic axiomatization of randomness based on independence.

Closing Thoughts

New directions in randomness

- I hope I made you think about algorithmic randomness in new and interesting ways.
- I hope I inspired the poly-time randomness folks and the higher randomness folks to consider how much of this applies to their world.
- I hope those interested in Schnorr and computable randomness found some interesting new theorems.

Thank You!

These slides will be available on my webpage:

http://www.personal.psu.edu/jmr71/

Or just Google™ me, "Jason Rute".

P.S. I am on the job market.