

Algorithmic Randomness and Complexity

Rod Downey
Victoria University
Wellington
New Zealand

Wellington, 2009

THANKS

- Denis Hirschfeldt from whom I pinched some slides.
- Supported by the Marsden Fund of New Zealand.
- The New Zealand Institute of Mathematics and its Applications.
- And of course a James Cook Fellowship

- Lets begin by examining the title:
- Algorithmic
- Randomness
- and Complexity

ALGORITHMIC

- Etymology : Al-Khwārizmī, Persian astronomer and mathematician, wrote a treatise in 825 AD, **On Calculation with Hindu Numerals**, together with an error in the Latin translation.
- **What we intuitively mean**
- From a set of basic instructions (ingredients) specify a mechanical method to obtain the desired result.
- Already you can see that I plan to be sloppy, but you should try to get the **feel** of the subject.
- I will try to have a general overview but will talk about some of my own work. Not to say that my work is the most important, but that I actually know something about it!

No. 1 – THE REVEREND JOHN MACFARLANE

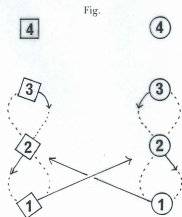
(Reel)

MUSIC	DESCRIPTION
<p><i>Bars</i></p> <p>1– 8</p>	<p>1st woman dances a reel of three on the men's side with 2nd and 3rd men, while 1st man dances a reel of three on the women's side with 2nd and 3rd women. (Fig.)</p> <p>1st couple finish in partner's place.</p>
<p>9–12</p>	<p>1st couple dance a half figure of eight round 2nd couple.</p>
<p>13–16</p>	<p>1st couple, joining both hands, dance four slip steps down the middle to third place and then set with hands still joined. (1st man sets to the left and then to the right.) 2nd and 3rd couples step up and 4th couple step in to meet on bars 15–16.</p>
<p>17–24</p>	<p>1st and 4th couples pousette.</p>
<p>25–28</p>	<p>2nd couple with 3rd couple and 4th couple with 1st couple dance right hands across once round to places.</p>
<p>29–32</p>	<p>2nd, 3rd, 4th and 1st couples turn partners once round with the left hand.</p> <p>Repeat with a new top couple.</p>

This dance commemorates the 150th anniversary of the founding in Wellington of New Zealand's first Scots Church, later known as St. Andrews.

The Rev. John Macfarlane, the first minister of Martyr's Memorial Church, Paisley, arrived in New Zealand on 20th February, 1840 and he held the first service on the beach at Petone on Sunday 23rd February.

Devised by Gary W. Morris (New Zealand Branch).



ice when it reaches the mushy stage and every 30 minutes after that until it is ready to serve, to insure smoothness. Garnish with pitted black cherries.

CREAM FRITTERS

READY TRAY

Serves 4 to 6

- 4 egg yolks
- ¼ cup sugar
- ½ cup flour
- Salt to taste
- 4 cups milk, scalded
- 1 teaspoon grated orange or lemon rind
- 1 egg, beaten
- Breadcrumbs
- 2 tablespoons oil
- 2 tablespoons butter
- Powdered sugar
- 2 tablespoons brandy or rum

Beat egg yolks and sugar in top of double boiler. Cook over low heat, stirring with wooden spoon until slightly thickened. Mix in ¼ cup flour, salt and gradually add milk. Simmer, stirring, until very thick. At no time allow to boil. Blend in rind.

Rinse a square dish or pan with cold water and pour in mixture to a depth of 2 inches. Chill until firm. Cut into squares or rectangular pieces 2 inches long. Dip in remaining flour, in egg and then in breadcrumbs. Brown gently on both sides in hot oil and butter. Serve sprinkled with sugar, and flame with heated brandy or rum.

FRIED RICOTTA

READY TRAY

Serves 8

- ½ pound macaroons
- 1 pound ricotta cheese
- Pinch cinnamon
- 3 eggs
- Breadcrumbs
- ¼ pound butter
- Powdered sugar
- Brandy

ALGORITHMIC

- From a set of basic instructions (ingredients) specify a mechanical method to obtain the desired result.

GREATEST COMMON DIVISORS

- The **greatest common divisor** of two numbers x and y is the biggest number that is a factor of both.
- For instance, the greatest common divisor, $\gcd(4,8)$ is 4.
 $\gcd(6,10)=2$; $\gcd(16,13)=1$.
- Euclid, or perhaps **Team Euclid**, (around 300BC) devised what remains the “best” algorithm for determining the gcd of two numbers.

EUCLID'S ALGORITHM

- To find $\gcd(1001, 357)$.
- $1001 = 357 \cdot 2 + 287$
- $357 = 287 \cdot 1 + 70$
- $287 = 70 \cdot 4 + 7$
- $70 = 7 \cdot 10$
- $7 = \gcd(1001, 357)$.

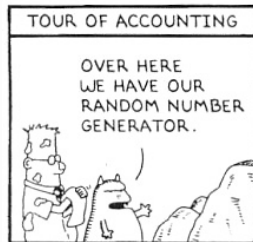
RANDOMNESS

*“How dare we speak of the laws of chance?
Is not chance the antithesis of all law?”*

— Joseph Bertrand, Calcul des Probabilités, 1889

INTUITIVE RANDOMNESS

DILBERT By SCOTT ADAMS



www.dilbert.com
scottadams@aol.com



© 2001 United Feature Syndicate, Inc.



INTUITIVE RANDOMNESS

Partial Randomness: mixing random and nonrandom sequences.

A

00

B

0011010011010011010011010011010011010011010011010011010011010011

C

010001101100000101001110010111011100000010010001101000101

D

0010011011011000100011110101001110110010011000000010110101

E

0101011101101111011100100110101101110011011010000110111101

F

0111011111001101100110100100001111110011011000000110110101

THREE APPROACHES TO RANDOMNESS AT AN INTUITIVE LEVEL

- **The statistician's approach:** Deal directly with rare patterns using measure theory. Random sequences should not have effectively rare properties. (von Mises, 1919, finally Martin-Löf 1966)
- Computably generated null sets represent effective statistical tests.
- **The coder's approach:** Rare patterns can be used to compress information. Random sequences should not be compressible (i.e., easily describable) (Kolmogorov, Levin, Chaitin 1960-1970's).
- Kolmogorov complexity; the complexity of σ is the length of the shortest description of σ .
- **The gambler's approach:** A betting strategy can exploit rare patterns. Random sequences should be unpredictable. (Solomonoff, 1961, Schnorr, 1975, Levin 1970)
- No effective martingale (betting) can make an infinite amount betting of the bits.

AND...

- They all give the same class of **randoms**!
- Many variations depending of sensitivity of the tests.
Implementations approximate the truth: ZIP, GZIP, RAR and other text compression programmes.

AND COMPLEXITY

- How hard is it to compute the solution?
- How many steps does the algorithm take?
- E.g. CD's vs efficient beer delivery to cities.
- The first takes 00000000...11111111 and amplifies to something of length 256, so there are 2^{256} many possible codewords, which are decoded, and they are n real time.
- **Yet** Beer delivery (TSP) for 256 cities is computationally impossible.
- Sometimes intractability is good e.g. RSA and credit cards.

SOME APPLICATIONS

- Using Chaos and randomness enable us to treat dynamical systems like the weather.
- Replace statistical tools by computational ones.
- Speeding up algorithms. E.g. supplying primes for things like RSA. (of course open if $BPP=P$)
- Phylogeny and language etc evolution (something of a dream).
- Understanding how levels of randomness relate to performance, etc.
- Differential geometry, reverse mathematics, Brownian motion, sampling randoms, etc. (AND misuses such as creationists!)

MY WORK

- What is “random”? What level of randomness is necessary for applications.
- Suppose I have a source of weak randomness, how can I amplify this to get better randomness?
- How can we calibrate levels randomness? Among randoms?, Among non-randoms?
- How does this relate to classical computability notions, which calibrate levels of computational complexity? If a real is random does it have strong or weak computational power?

ONE EXAMPLE-FROM MUSIC

- We now know that there are two kinds of randoms, those which resemble Chaitin's $\Omega = \sum_{\sigma} 2^{-K(\sigma)}$ and more typical ones. (Specifically a Theorem of Stephan in 2002.)
- The first are random as they are so smart that they **know** how to be stupid, the second **really are** stupid.
- That is, with sufficient randomness, randomness begins to resemble order. This is kind of remarkable.
- One of the following music examples is **aleatoric** (or chance) and the other is **totally serial** (based on a pattern). Which is which?

HOW CHAOS RESEMBLES ORDER

Highly random objects can resemble highly patterned ones.

A musical example.

Excerpt A: from *Music of Changes* by John Cage

Excerpt B: from *Structures for Two Pianos* by Pierre Boulez

Cage's piece is an example of aleatory music.

Boulez's piece is an example of total serialism.

WANT TO KNOW MORE

- My homelage : just type Rod Downey into google and I am the one who is not the author of Gay Porn.
- Buy that wonderful book, soon to appear.....
- Buy some for your friends.
- Thanks