CS61B Lecture #35

om Numbers (Chapter 11)

e random sequences?

andom sequences"?

om sequences.

ne.

a library classes and methods.

nutations.

Why Random Sequences?

stical samples

rithms

y:

random keys and *nonces* (random one-time values used
essages unique.)

g streams of random bits (e.g., stream ciphers encrypt
by xor'ing reproducible streams of pseudo-random bits
bits of the message.)

se, games

What Is a "Random Sequence"?

a sequence where all numbers occur with equal frequency"?

3, 4, ...?

ow about: "an unpredictable sequence where all numbers
qual frequency?"

0, 1, 1, 2, 2, 2, 2, 2, 3, 4, 4, 0, 1, 1, 1,...?

t is wrong with 0, 0, 0, 0, ... anyway? Can't that occur
election?

Pseudo-Random Sequences

nable, a "truly" random sequence is difficult (i.e., slow)
er (or human) to produce. Must have some nondeterministic
rce. Can use:

etween radioactive decays.

etween keystrokes or incoming internet message.

rposes, we need only a sequence that satisfies certain
roperties, even if deterministic (as is useful for reproducibility).

e.g., cryptography) we need sequence that is *hard* or
to predict.

om sequence: deterministic sequence that passes some
statistical tests that random sequences (probably) pass.

look at lengths of *runs:* increasing or decreasing contiguous
s.

ly, statistical criteria to be used are quite involved. For
Knuth, volume 2.

nerating Pseudo-Random Sequences

as you might think.

mplex jumbling methods can give rise to bad sequences.

uential method is a simple method used by Java:

$$X_0 = \textit{arbitrary seed}$$
$$X_i = (aX_{i-1} + c) \bmod m, \quad i > 0$$

large power of 2.

sults, want $a \equiv 5 \bmod 8$, and a, c, m with no common

nerator with a *period of m* (length of sequence before
and reasonable *potency* (measures certain dependencies
ent X_i.)

ts of a to "have no obvious pattern" and pass certain
(see Knuth).

$= 25214903917$, $c = 11$, $m = 2^{48}$, to compute 48-bit
om numbers. It's good enough for many purposes, but
aphically secure.

What Can Go Wrong (I)?

*considers arithmetical methods of producing random
course, in a state of sin.*
JOHN VON NEUMANN (1951)

ls, many impossible values: E.g., a, c, m even.

erns. E.g., just using lower 3 bits of X_i in Java's 48-bit
o get integers in range 0 to 7. By properties of modular

$$\bmod 8 = (25214903917X_{i-1} + 11 \bmod 2^{48}) \bmod 8$$
$$= (5(X_{i-1} \bmod 8) + 3) \bmod 8$$

period of 8 on this generator; sequences like

$$0, 1, 3, 7, 1, 2, 7, 1, 4, \ldots$$

le. This is why Java doesn't give you the raw 48 bits.

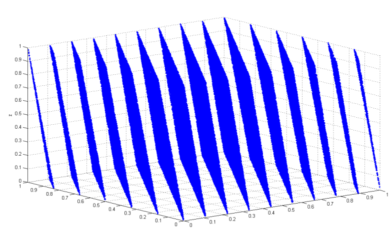
What Can Go Wrong (II)?

ds to bad correlations.

s IBM generator RANDU: $c = 0$, $a = 65539$, $m = 2^{31}$.

U is used to make 3D points: $(X_i/S, X_{i+1}/S, X_{i+2}/S)$, es to a unit cube, ...

be arranged in parallel planes with voids between. So its" won't ever get near many points in the cube:



uis Sanchez at English Wikipedia - Transferred from en.wikipedia to Commons ., CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=3832343]

Additive Generators

erator:

$$X_n = \begin{cases} \textit{arbitary value}, & n < 55 \\ (X_{n-24} + X_{n-55}) \bmod 2^e, & n \ge 55 \end{cases}$$

es than 24 and 55 possible.

period of $2^f(2^{55} - 1)$, for some $f < e$.

mentation with circular buffer:

```
55;
+31) % 55];  // Why +31 (55-24) instead of -24?
   /* modulo 2^32 */
```

. 54] is initialized to some "random" initial seed values.

phic Pseudo-Random Number Generators

orm of linear congruential generators means that one future values after seeing relatively few outputs.

ou want *unpredictable* output (think on-line games involving domly generated keys for encrypting your web traffic.)

phic pseudo-random number generator (CPRNG) has the nat

ts of a sequence, no polynomial-time algorithm can guess oit with better than 50% accuracy.

current state of the generator, it is also infeasible to ct the bits it generated in getting to that state.

aphic Pseudo-Random Number Generator Example

good *block cipher*—an encryption algorithm that encrypts bits (not just one byte at a time as for Enigma). AES is

rovide a key, K, and an initialization value I.

do-random number is now $E(K, I + j)$, where $E(x, y)$ is on of message y using key x.

djusting Range and Distribution

quence of numbers, X_i, from above methods in range ^{48}, how to get uniform random integers in range 0 to

easy: use top k bits of next X_i (bottom k bits not as

be careful of slight biases at the ends. For example, if $X_i/(2^{48}/n)$ using all integer division, and if $(2^{48}/n)$ gets n, then you can get n as a result (which you don't want).

fix that by computing $(2^{48}/(n-1))$ instead, the probability $- 1$ will be wrong.

Adjusting Range (II)

ias problems when n does not evenly divide 2^{48}, Java alues after the largest multiple of n that is less than

```
m integer in the range 0 .. n-1, n>0. */
nt(int n) {
 = next random long (0 ≤ X < 2^48);
s 2^k for some k)
urn top k bits of X;

 = largest multiple of n that is < 2^48;
X_i >= MAX)
 = next random long (0 ≤ X < 2^48);
 X_i / (MAX/n);
```

Arbitrary Bounds

rbitrary range of integers (L to U)?

m `float`, x in range $0 \le x < d$, compute

```
nextInt(1<<24) / (1<<24);
```

ble a bit more complicated: need two integers to get

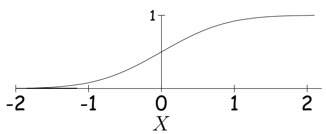
```
and = ((long) nextInt(1<<26) << 27)
        + (long) nextInt(1<<27);
 * bigRand / (1L << 53);
```


eneralizing: Other Distributions

have some desired probability distribution function, and random numbers that are distributed according to that How can we do this?

normal distribution:

$X)$

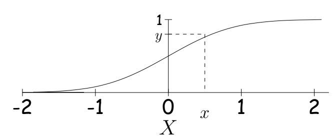


desired probability distribution. $P(Y \le X)$ is the hat random variable Y is $\le X$.

eralizing: Other Distributions (II)

e y uniformly between 0 and 1, and the corresponding x ed according to P.

$\le Y)$



Java Classes

(): random double in $[0..1)$.

til.Random: a random number generator with constructors:

erator with "random" seed (based on time).

d) generator with given starting value (reproducible).

random integer

nt in range $[0..n)$.

andom 64-bit integer.

(), nextFloat(), nextDouble() Next random values of other types.

n() normal distribution with mean 0 and standard deviation rve").

.shuffle(L, R) for list L and Random R permutes L ing R).

Shuffling

a random permutation of some sequence.

b technique for sorting N-element list:

N random numbers

ch to one of the list elements

ist using random numbers as keys.

a bit better:

```
e(List L, Random R) {
 i = L.size(); i > 0; i -= 1)
 elements i-1 and R.nextInt(i) of L;
```

0	1	2	3	4	5	Swap items	0	1	2	3	4	5
A♣	2♣	3♣	A♡	2♡	3♡	$3 \Longleftrightarrow 3$	A♣	3♡	2♡	A♡	3♣	2♣
A♣	3♡	3♣	A♡	2♡	2♣	$2 \Longleftrightarrow 0$	2♡	3♡	A♣	A♡	3♣	2♣
A♣	3♡	2♡	A♡	3♣	2♣	$1 \Longleftrightarrow 0$	3♡	2♡	A♣	A♡	3♣	2♣

Random Selection

que would allow us to select N items from list:

```
 L and return sublist of K>=0 randomly
elements of L, using R as random source. */
(List L, int k, Random R) {
i = L.size(); i+k > L.size(); i -= 1)
ement i-1 of L with element
tInt(i) of L;
sublist(L.size()-k, L.size());
```

 efficient for selecting random sequence of K distinct m $[0..N)$, with $K \ll N$.

ernative Selection Algorithm (Floyd)

```
ence of K distinct integers
 0<=K<=N. */
elect(int N, int K, Random R)

eger> S = new ArrayList<>();

N-K; i < N; i += 1) {
es in S are < i
andInt(i+1); // 0 <= s <= i < N
get(j) for some j)
 value i (which can't be there
fter the s (i.e., at a random
other than the front)
 i);

 random value s (which can't be
yet) at front
s);
```

Example

i	s	S
5	4	[4]
6	2	[2, 4]
7	5	[5, 2, 4]
8	5	[5, 8, 2, 4]
9	4	[5, 8, 2, 4, 9]

`selectRandomIntegers(10, 5, R)`