Tranter Chapter 7

EE571
Generation of Random Numbers

Dr. Samir Alghadhban

1

Content

- Linear Congruence Random Number Generators (RNG)
- Pseudonoise (PN) Sequence Generators
- Randomness Tests
- Examples of RNG with very long periods

2

Linear Congruence

Definition: $X_{i+1} = [\, a X_i + c \,]\mathrm{mod}(m)$

a = multiplier

c = offset

m = modulus

X_0 = seed

- The maximum period is m. The problem is to select a, c and m so that the maximum period is achieved.
- Note that the algorithm is algebraic and deterministic.

3

Mixed and Multiplicative Congruence

- Mixed Congruence (maximum period = $\boldsymbol{m}$)

  $\boldsymbol{X_{i+1}} = [\, \boldsymbol{a X_i + c} \,]\mathrm{mod}(\boldsymbol{m})$

- Multiplicative Congruence (maximum period = $\boldsymbol{m} - 1$)

  $\boldsymbol{X_{i+1}} = [\boldsymbol{a X}_{\mathrm{i}} \,]\mathrm{mod}(\boldsymbol{m})$

- The multiplicative algorithm is somewhat faster since the addition operation is not required. How much faster depends upon the computer used and the number representation.

4

Desired Attributes

- A long period is desired (The period should be longer the simulation runlength.)
- Adjacent samples should be uncorrelated. Ideally the sequence should be delta correlated for most applications. This, of course yields a white noise sequence.
- The desired attributes are usually application dependent.
- Fast execution is essential.

5

Multiplicative LCG Full Period Design

- The generator

$$X_{i+1} = [\ a\,X_i\ ]\mathrm{mod}(m)$$

- is full period (generates all integers in [1, m–1] before repeating) if

  a) m is prime

  b) a is a primitive element modulo m

6

Primitive Elements

Definition:

a is a primitive element mod(m) if $a^{i-1} - 1$ is a multiple of m for $i = m$ but no smaller i.

In other words

$(a^{i-1} - 1) / m = k$ for $i = m$ but not for $i = 1, 2, 3, \cdots, m-1$ where k is an integer.

7

Multiplicative LCG - Example

- Class Activity
  - Design a multiplicative LCG, Select the values of m and a to have a full period generator.

8

Multiplicative LCG - Example

- Verify that 5 is a primitive element mod(7)

Let $f\,(i)$ = $(5^{i-1} - 1) / 7$.

Test $f\,(i)$ for $i = m = 7$. $f\,(7) = 2232$ (an integer)

Test f (i) for $i < m = 7$.

$f\,(6) = 446.2857$, $f\,(5) = 89.1429$

$f\,(4) = 17.7143$, $f\,(3) = 3.4286$

$f\,(2) = 0.5714$

9

Multiplicative LCG - Example

5 is a primitive element mod(7) and 7 is a prime number. Thus, $\boldsymbol{X}_{i+1}$ = [5 $\boldsymbol{X}_i$]mod(7) is a full period generator. It generates the sequence (assume $\boldsymbol{X}_0$ = 3)

3(5)mod(7) = 1

1(5)mod(7) = 5

5(5)mod(7) = 4

4(5)mod(7) = 6

6(5)mod(7) = 2

2(5)mod(7) = 3

3(5)mod(7) = 1 (sequence repeats)

10

Mixed LCG Design

The generator

X_{i+1} = [a X_i + c]mod(m)

is full period (generates all integers in [0, m–1] before repeating) if

a) c and m are relatively prime

b) a –1 is a multiple of every prime p which divides m

c) a –1 is a multiple of 4 if 4 divides m

11

Mixed LCG - Example

Consider: X_i+1 = [121 X_i + 567]mod(1000)
This is a full period generator [Bratley,1987].
Proof:

a) 567 = 3·3·3·3·7
1000 = 2·2·2·5·5·5
Thus c and m are relatively prime.

b) Two prime numbers (2 and 5) divide **m**.
a – 1 = 120 120/2 = 60 120/5 = 24

c) 4 divides 100 and a – 1 = 120 is a multiple of 4

12

Mixed LCG - Special Case

The generator

$$X_{i+1} = [\ a\ X_i + c\ ]\text{mod}(m)$$

for $c > 0$, n > 1 is full period (generates all integers in [0, m–1] before repeating) if c is odd and $a - 1$ is a multiple of 4 so that $a = 4\ k + 1$. The proof is simple.

a) The only prime factor of m is 2. If c is odd m and c are relatively prime.

b) 2 is the only prime factor of m. $a - 1 = 4\ k$ is a multiple of 2.

c) $a - 1 = 4\ k$ is a multiple of 4.

Mixed LCG - An Important Example

Consider a mixed LCG with $a = c = 1$. Also let $X_0 = 0$.

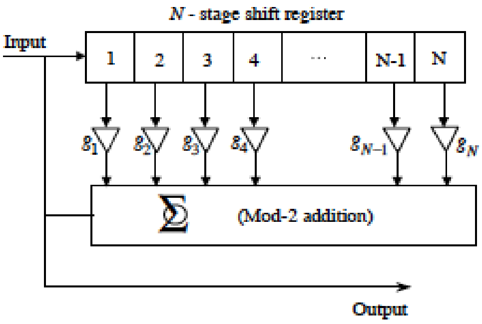
The algorithm is $X_{i+1} = [\ X_i + 1]\text{mod}(32)$. The sequence generated is

$$0, 1, 2, 3, 4, 5, \cdots, 29, 30, 31, 0, \cdots$$

This is clearly full period (period = m = 32). It clearly fails most tests of randomness. What went wrong?

Answer: Nothing went wrong. The procedures we have considered only show us how to develop a full period LCG. Nothing else is guaranteed.

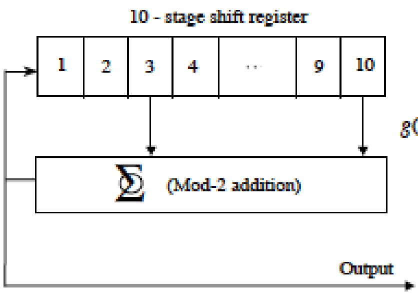
PN Sequence Generator



$$g(D)=g_0+g_1D+g_2D^2+\cdots+g_{N-1}D^{N-1}+g_ND^N$$

15

PN Sequence Generator (N=10)



$$g(D)=1+D^3+D^{10}$$

Note: $g(D)$ is a primitive polynomial.

16

Primitive Polynomials

Where did **g**(**D**) come from?

- A PN sequence generator will have maximum period if **g**(**D**)is primitive.
- Fortunately we have tables of primitive polynomials.
    - See for example: R. E. Ziemer and R. L. Peterson, **Digital Communications and Spread Spectrum Systems,** Macmillan, 1985, pp. 390-391.

g(D)= 2 0 1 1 (octal)

g(D)= 0 1 0 0 0 0 0 0 1 0 0 1 (binary) → $1+D^3+D^{10}$

17

Primitive Polynomials / 2

Definition of a primitive polynomial:

- The polynomial **g**(**D**) of degree **N** is a primitive polynomial if the smallest integer **k** for which **g**(**D**) divides D^k+1 is $k=2^N-1$.

Note that testing a polynomial of large degree is a time consuming task.

18

Proof Octal [1,3] is Primitive

- Claim: Octal [1,3] => 001 101 is primitive

Proof: $g(D)=1+D^2+D^3$

$$m=7 \qquad \begin{array}{r|l} & 1+D^2+D^3+D^4 \\ \hline 1+D^2+D^3 & 1+D^7 \\ & 1+D^2+D^3 \\ & D^2+D^3+D^7 \\ & D^2+D^4+D^5 \\ & D^3+D^4+D^5+D^7 \\ & D^3+D^5+D^6 \\ & D^4+D^6+D^7 \\ & \underline{\underline{D^4+D^6+D^7}} \end{array}$$

Proof Octal [1,3] is Primitive

$$m=6 \qquad \begin{array}{r|l} & 1+D^2+D^3+D^4 \\ \hline 1+D^2+D^3 & 1+D^6 \\ & 1+D^2+D^3 \\ & D^2+D^4+D^5 \\ & D^3+D^4+D^5+D^6 \\ & D^3+D^5+D^6 \\ & D^4 \\ & D^4+D^6+D^7\ XXXXX \end{array}$$

$$m=5 \qquad \begin{array}{r|l} & 1+D^2+D^3 \\ \hline 1+D^2+D^3 & 1+D^5 \\ & 1+D^2+D^3 \\ & D^2+D^3+D^5 \\ & D^2+D^4+D^5 \\ & D^3+D^4 \\ & D^3+D^5+D^6\ XXXXX \end{array}$$

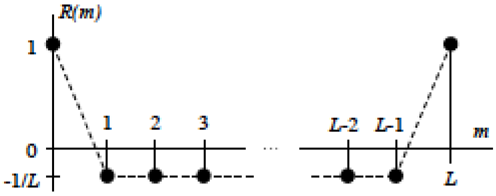
$$m=4 \qquad \begin{array}{r|l} & 1+D^2 \\ \hline 1+D^2+D^3 & 1+D^4 \\ & 1+D^2+D^3 \\ & D^2+D^3+D^4 \\ & D^2+D^4+D^5\ XXXXX \end{array}$$

$$m=3 \qquad \begin{array}{r|l} & 1+D^2 \\ \hline 1+D^2+D^3 & 1+D^3 \\ & 1+D^2+D^3 \\ & D^2 \\ & D^2+D^4+D^5\ XXXXX \end{array}$$

Test for Maximum Length

```
pntaps = [0 0 1 0 0 0 0 0 0 1];       % Shift register taps
pninitial = [0 0 0 0 0 0 0 0 0 1];     % Initial shift register state
pnregister = pninitial;
n = 0;
kk = 0;
while kk == 0
    data = pnregister(1,1);                        % data symbol
    feedback = rem((pnregister*pntaps'),2);
    pnregister = [feedback,pnregister(1,1:9)];
    n = n+1;
    if pnregister == pninitial
        kk = 1;
    end
end
n                                         % Display n
```


PN Sequence Autocorrelation Function



For large L the autocorrelation function approximates an impulse. Therefore the power spectral density approximates a delta correlated sequence (white noise).

Example of an Autocorrelation Function

The autocorrelation is

$$R(\Delta) = \frac{N_A - N_U}{L}$$

Consider S= 1001011, the autocorrelation of the sequence is:

S	1	0	0	1	0	1	1	
0	1	0	0	1	0	1	1	$N_A = 7, N_U = 0, R = 1$
1	1	1	0	0	1	0	1	$N_A = 3, N_U = 4, R = -1/7$
2	1	1	1	0	0	1	0	$N_A = 3, N_U = 4, R = -1/7$
3	0	1	1	1	0	0	1	$N_A = 3, N_U = 4, R = -1/7$
4	1	0	1	1	1	0	0	$N_A = 3, N_U = 4, R = -1/7$
5	0	1	0	1	1	1	0	$N_A = 3, N_U = 4, R = -1/7$
6	0	0	1	0	1	1	1	$N_A = 3, N_U = 4, R = -1/7$
7	1	0	0	1	0	1	1	$N_A = 7, N_U = 0, R = 1$

23

Autocorrelation Function

The preceding result is general.

- Note that the shift register cannot contain all zeros but can contain all ones.
- As a result, the PN sequence will contain 1 run of ones of length N and 1 run of zeros of length N-1.
- As a result there is one more 1 than 0s in a sequence. The mod-2 sum of two "words" is another word. (See previous result as an example.) As a result $N_A - N_U = -1$ for all $\Delta \neq 0$.

24

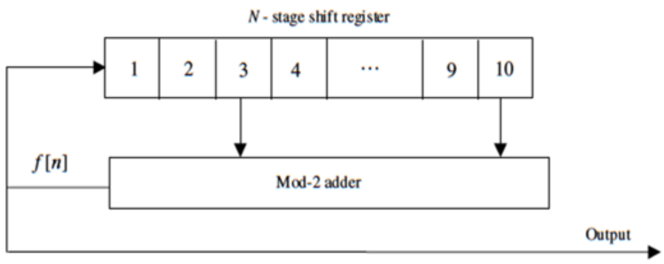
Table for Primitive Polynomials

Table 7.1 Short Table of Primitive Polynomials

N	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}
3	1	0	1											
4	1	0	0	1										
5	0	1	0	0	1									
6	1	0	0	0	0	1								
7	0	0	1	0	0	0	1							
8	0	1	1	1	0	0	0	1						
9	0	0	0	1	0	0	0	0	1					
10	0	0	1	0	0	0	0	0	0	1				
11	0	1	0	0	0	0	0	0	0	0	1			
12	1	0	0	1	0	1	0	0	0	0	0	1		
13	1	0	1	1	0	0	0	0	0	0	0	0	1	
14	1	0	0	0	0	1	0	0	0	1	0	0	0	1

25

Example for N=10

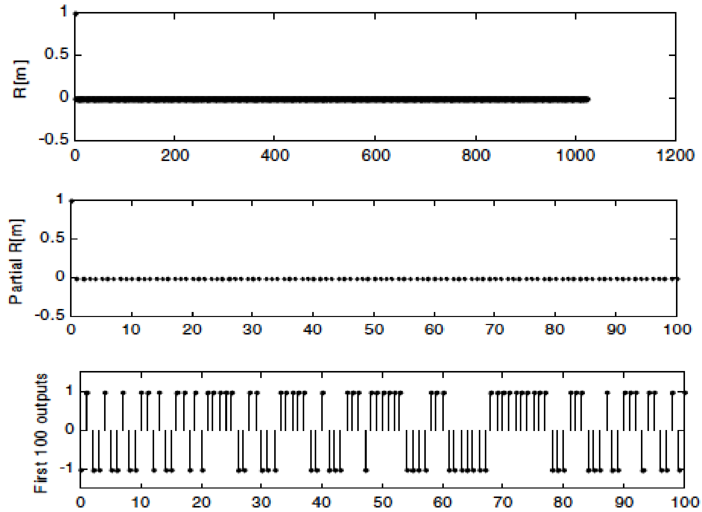


G = [0 0 1 0 0 0 0 0 0 1]

26

Example for N=10,

Tranter's Book Example 7.12



27

Testing Random Number Generators

- A number of procedures have been developed for testing the randomness of a given sequence. Among the most popular of these are the Chi-square test, the Kolomogorov-Smirnov test, and the spectral test.
- We consider two tests: scatterplots and the Durbin-Watson test.

28

Scatterplots

A scatterplot is a plot of $\mathbf{x_{i+1}}$ as a function of $\mathbf{x_i}$, and represents an empirical measure of the quality of the number generator.

For example, we consider two number generators defined by:

G1: $x_{i+1}=(65x_i+1)\mathrm{mod}(2048)$

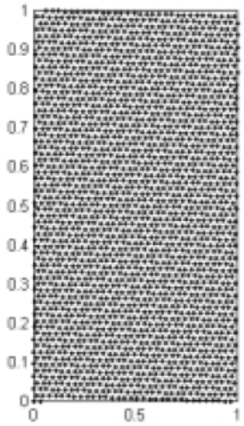
G2: $x_{i+1}=(1229x_i+1)\mathrm{mod}(2048)$

29

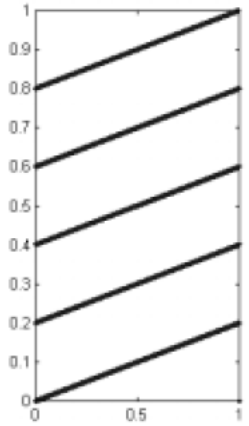
Scatterplots,

Tranter's Book Example 7.5

$x_{i+1}=(65x_i+1)\mathrm{mod}(2048)$



$x_{i+1}=(1229x_i+1)\mathrm{mod}(2048)$



Which one looks more random ?

30

The Durbin-Watson Test

The Durbin-Watson test for independence is implemented by calculating the Durbin parameter

$$D = \frac{\sum_{n=2}^{N} \left[X(n) - X(n-1)\right]^2}{\sum_{n=1}^{N} \left[X(n)\right]^2}$$

Note the if ***X(n)*** and ***X(n – 1)*** are uncorrelated (correlation = 0), then **D** would have an expected value of 2.

The value of **D** would be much smaller than 2 if there is strong positive correlation

and would approach 4 if there is strong negative correlation.

The Durbin-Watson Test,
Example 7.6 in Tranter's Book

- For the two random number generators

G1: $x_{i+1}=(65x_i+1)\mathrm{mod}(2048)$

G2: $x_{i+1}=(1229x_i+1)\mathrm{mod}(2048)$

- Applying the test in Example 7.6, we got:
  - D_1= 1.9925 and ρ_1= 0.0037273
  - D_2 = 1.6037 and ρ_2= 0.19814

Random Number Generators with very long periods

- Lewis, Goodman and Miller

  $X_{i+1}=(16807x_i)\mathrm{mod}(2147483647)$

in which *m* is the Mersenne prime $2^{31} - 1$.

33

The Wichmann-Hill Algorithm

- Combine several number generators having different but approximately the same periods.

  $x_{i+1}=(171x_i)\mathrm{mod}(30269)$
  $y_{i+1}=(170y_i)\mathrm{mod}(30307)$
  $z_{i+1}=(172z_i)\mathrm{mod}(30323)$

Period is around 7.0 x 10^{12}

$$\Rightarrow \quad u_i = \left(\frac{x_i}{30269} + \frac{y_i}{30307} + \frac{z_i}{30323} \right) \mathrm{mod}(1)$$

34

Marsaglia – Zaman Algorithm

- We will describe the subtract-with-borrow algorithm, which has the form:

$$Z_i = X_{i-r} - X_{i-s} - C_{i-1}$$

$$X_i = \begin{cases} Z_i & \text{if} \quad Z_i \geq 0 \\ Z_i + b & \text{if} \quad Z_i < 0 \end{cases}$$

$$C_i = \begin{cases} 0 & \text{if} \quad Z_i \geq 0 \\ 1 & \text{if} \quad Z_i < 0 \end{cases}$$

Where all integers and I > r

For maximum period (M-1), the constants b, r, and s must be chosen such that $M=b^r-b^s+1$ is a prime with b a primitive root mod M.

For $b=2^{32}-1$, r=43, and s=22, the period is:

$M-1 \approx 1.65 \times 10^{414}$

35

Mapping Target pdf and PSD

EE571

Dr. Samir Alghadhban

36

Goals

- We now know how to generate samples of a random variable, *U,* (actually pseudo-random) that are uniformly distributed over the range (0,1). The goal here is to map *U* to a target probability density function (pdf). The technique used is dictated by whether or not the cumulative distribution function (cdf) is known.

pdf: $f_X(x)dx = \Pr\{x - dx < X < x\}$

cdf: $F_X(x) = \int_{-\infty}^{x} f_X(y)dy$

37

Mapping U to a Desired pdf

There are a number of interesting and important cases.

Case 1. Both pdf and cdf can be written in closed form.
- Technique: Inverse transform mapping.
- Example: Exponential pdf.

Case 2. The pdf can be written in closed form but the cdf cannot be written in closed form.
- Technique: *ad-hoc* methods, rejection techniques.
- Example: Gaussian pdf.

Case 3. Neither the pdf or the cdf can be written in closed form.
- Technique: Histogram-based method.
- Example: Experimental data

38

pdf and CDF both Known in Closed Form

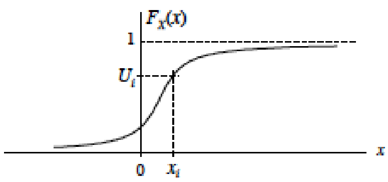
Since

$U = F_X(x), \quad X = F^{-1}(U)$

The algorithm for generating *X* from a uniform random variable *U*, with pdf $f_x(x)$ is:

1. Form *U*
2. Set $F_x(x) = U$
3. Solve for *X*
4. Return *X*

CDF



$$U_i = \Pr[X \le x_i] = F_X(x_i) = \int_{-\infty}^{x_i} f_X(x)dx$$

Example 1 - Exponential RV

Problem: Map a uniform (0,1) RV, denoted *U*, to the exponential pdf:

$$f_X(x) = \beta \exp(-\beta x) u(x)$$

Solution: the CDF is

$$F_X(x) = \int_0^x \beta \exp(-\beta y) dy = -\exp(\beta y) \Big|_{y=0}^{y=x}$$

$$F_X(x) = 1 - \exp(-\beta x) = u$$

In terms of random variables we write

$$\exp(-\beta X) = 1 - U = U$$

Note that the random variables *U* and 1- *U* are equivalent

Example 1 - Exponential RV

$$\exp(-\beta X) = 1 - U = U$$

To develop the algorithm solve for X.

$$-\beta X = \ln(U)$$
$$X = -\frac{1}{\beta}\ln(U)$$

Pseudocode:

1. Generate U
2. $X \leftarrow \frac{1}{\beta}\ln(U)$
3. Return X

41

Example 1 - MATLAB Demo

Problem: Generate a set of samples having the pdf

$$f_X(x) = \beta\exp(-\beta x)u(x)$$

Let:

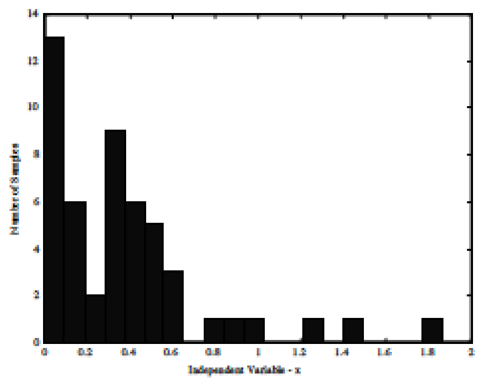
1. $\beta = 3$
2. Number of histogram bins = 20
3. Number of samples generated = 50 and 2000

42

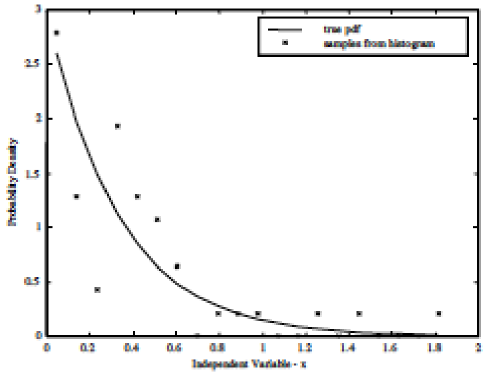
Demo Program for Example 1

```
clear all                               % be safe
n = input('Enter number of points > ');

b = 3;                                  % set pdf parameter
u = rand(1,n);                          % generate U
y_exp = -log(u)/b;                      % transformation
[N_samp,x] = hist(y_exp,20);            % get histogram parameters
bar(x,N_samp,1)                         % plot histogram

pause                           % pause for comparison

y = b*exp(-3*x);                % calculate pdf
del_x = x(3)-x(2);              % determine bin width
p_hist = N_samp/n/del_x;        % probability from histogram
plot(x,y,x,p_hist,'X')          % compare
```

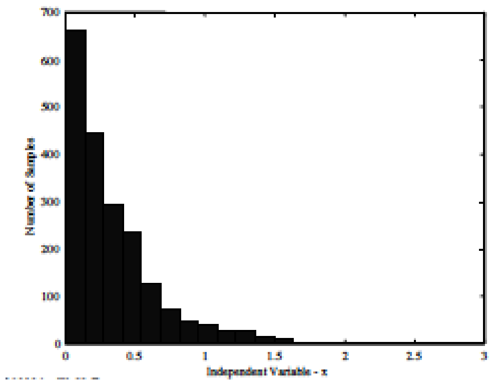

Example 1 Results (N=50 points)



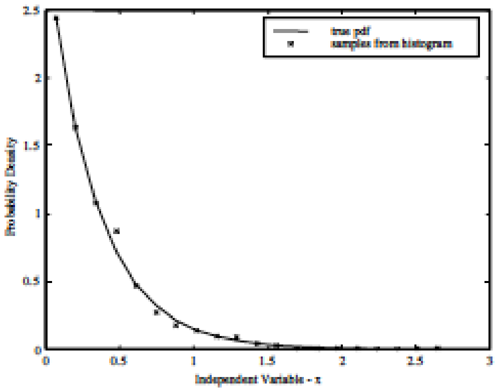
Example 1 Results (N=50 points)



Example 1 Results (N=2000 points)



Example 1 Results (N=2000 points)



47

Group Exercise
Example 2 - Rayleigh pdf

The target pdf is

$$f_R(r) = \frac{r}{\sigma^2}\exp\left(-\frac{r^2}{2\sigma^2}\right)$$

Find the CDF of the Rayleigh RV

The cdf is

$$F_R(r) = \int_0^r \frac{y}{\sigma^2}\exp\left(-\frac{y^2}{2\sigma^2}\right)dy$$

$$F_R(r) = -\exp\left(-\frac{y^2}{2\sigma^2}\right)\Bigg|_{y=0}^{y=r} = 1 - \exp\left(-\frac{r^2}{2\sigma^2}\right)$$

The algorithm is defined by

$$1 - \exp\left(-\frac{R^2}{2\sigma^2}\right) = U \quad \text{or} \quad \exp\left(-\frac{R^2}{2\sigma^2}\right) = 1 - U = U$$

48

Example 2 - Rayleigh pdf

We solve the following for *X*:

$$\exp\left(-\frac{R^2}{2\sigma^2}\right)=1-U=U$$

$$-\frac{R^2}{2\sigma^2}=\ln(U)$$

This is

$$R=\sqrt{-2\sigma^2\ln(U)}$$

This is often referred to as the Box-Muller transformation and is a fundamental step in the generation of Gaussian random variables.

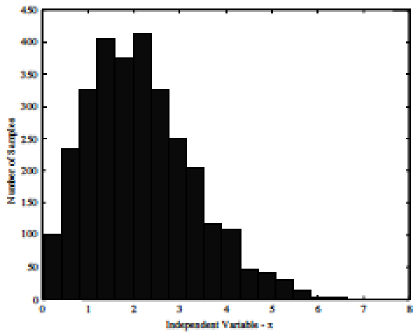
49

Example 2 – MATLAB Problem

```
clear all                            % be safe
n = input('Enter number of points > ');

varR = 3;                            % set pdf parameter
u = rand(1,n);                       % generate U
y_exp = sqrt(-2*varR*log(u));        % transformation
[N_samp,r] = hist(y_exp,20);         % get histogram parameters
bar(r,N_samp,1)                      % plot histogram

pause                                % pause for comparison

term1 = r.*r/2/varR;                 % exponent
ray = (r/varR).*exp(-term1);         % Rayleigh pdf
del_r = r(3)-r(2);                   % determine bin width
p_hist = N_samp/n/del_r;             % probability from histogram
plot(r,ray,r,p_hist,'X')             % compare results
```

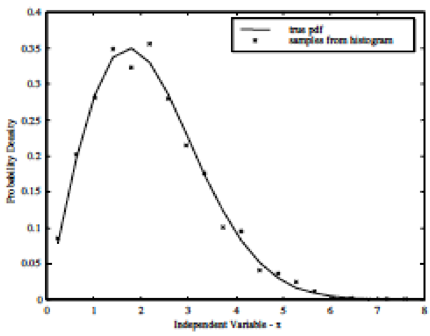
50

Example 2 Results (N=3000 points)



51

Example 2 Results (N=3000 points)



52

Generation of Gaussian RV
Box-Muller Method

Theorem: Orthogonal projections of a Rayleigh random variable produce two independent Gaussian random variables. In other words, if *R* is Rayleigh, *X* and *Y* are Gaussian and independent where

$$X = R\cos\theta \quad \text{and} \quad Y = R\sin\theta$$

and θ is uniformly distributed in the range

$$0 \le \theta < 2\pi$$

53

Independent Gaussian pdfs

Proof: The target pdfs are

$$f_X(x) = \frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{x^2}{2\sigma^2}\right), \quad -\infty < x < \infty$$

$$f_Y(y) = \frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{y^2}{2\sigma^2}\right), \quad -\infty < y < \infty$$

If *X* and *Y* are statistically independent, the joint pdf is given by

$$f_{XY}(x,y) = f_X(x)f_Y(y) = \frac{1}{2\pi\sigma^2}\exp\left(-\frac{x^2+y^2}{2\sigma^2}\right)$$

54

Gaussian to Rayleigh Transformation

$$f_{XY}(x,y)=f_X(x)f_Y(y)=\frac{1}{2\pi\sigma^2}\exp\left(-\frac{x^2+y^2}{2\sigma^2}\right)$$

Since

$$x=r\cos\theta \quad \text{and} \quad y=r\sin\theta$$

we have

$$\frac{dx}{dr}=\cos\theta,\ \frac{dx}{d\theta}=-r\sin\theta,\ \frac{dy}{dr}=\sin\theta,\ \text{and}\ \frac{dy}{d\theta}=r\cos\theta$$

This gives the Jacobian

$$J(x,y,r,\theta)=\begin{vmatrix}\cos\theta & -r\sin\theta\\ \sin\theta & r\cos\theta\end{vmatrix}=r(\cos^2\theta+\sin^2\theta)=r$$

55

Gaussian to Rayleigh Transformation

$$f_{XY}(x,y)=f_X(x)f_Y(y)=\frac{1}{2\pi\sigma^2}\exp\left(-\frac{x^2+y^2}{2\sigma^2}\right)$$

The target joint pdf is

$$f_{R\Theta}(r,\theta)=f_{XY}(x,y)\,J(x,y,r,\theta)=\frac{J}{2\pi\sigma^2}\exp\left(-\frac{x^2+y^2}{2\sigma^2}\right)\Bigg|_{\substack{J=r\\ x=r\cos\theta\\ y=r\sin\theta}}$$

Since

$$x^2+y^2=r^2$$

we have

$$f_{R\Theta}(r,\theta)=\frac{r}{2\pi\sigma^2}\exp\left(-\frac{r^2}{2\sigma^2}\right)u(r)$$

The unit step is required to make the joint pdf is 0 for negative values of r.

56

Marginal pdf s

$$f_{R\Theta}(r,\theta)=\frac{r}{2\pi\sigma^2}\exp\left(-\frac{r^2}{2\sigma^2}\right)u(r)$$

The marginal pdfs are

$$f_R(r)=\int_0^{2\pi}\frac{r}{2\pi\sigma^2}\exp\left(-\frac{r^2}{2\sigma^2}\right)d\theta=\frac{r}{2\pi\sigma^2}\exp\left(-\frac{r^2}{2\sigma^2}\right)\int_0^{2\pi}d\theta$$

$$f_R(r)=\frac{r}{\sigma^2}\exp\left(-\frac{r^2}{2\sigma^2}\right)u(r)\quad \text{(Rayleigh - This proves the theorem.)}$$

$$f_\Theta(\theta)=\int_0^\infty\frac{r}{2\pi\sigma^2}\exp\left(-\frac{r^2}{2\sigma^2}\right)dr=-\frac{1}{2\pi}\int_0^\infty\exp\left(-\frac{r^2}{2\sigma^2}\right)\left(-\frac{2r}{2\sigma^2}\right)dr$$

$$f_\Theta(\theta)=-\frac{1}{2\pi}\exp\left(-\frac{r^2}{2\sigma^2}\right)\Bigg|_{r=0}^{r\to\infty}=-\frac{1}{2\pi}(0-1)=\frac{1}{2\pi},\quad \text{(uniform)}$$

57

Box-Muller Method

The pseudocode is as follows:

1. Generate U_1 in (0,1)
2. Generate U_2 in (0,1)
3. Set variance
4. $R\leftarrow\sqrt{-2\sigma^2\ln(U_1)}$
5. $\theta\leftarrow 2\pi U_2$
6. $X\leftarrow R\cos\theta$
7. $Y\leftarrow R\sin\theta$

58

Example 3 MATLAB Code

```
clear all                               % be safe
n = input('Enter number of points > ');

varXY = 3;                              % set target variance
u1 = rand(1,n);                         % generate U1
u2 = rand(1,n);                         % generate U2
r = sqrt(-2*varXY*log(u1));             % generate r
theta = 2*pi*u2;                        % generate theta
x_gaus = r.*cos(theta);                 % generate X
y_gaus = r.*sin(theta);                 % generate Y

[N_samp,x_hist] = hist(x_gaus,20); % get parameters
bar(x_hist,N_samp,1)                    % plot histogram

pause                                   % pause for comparison
```

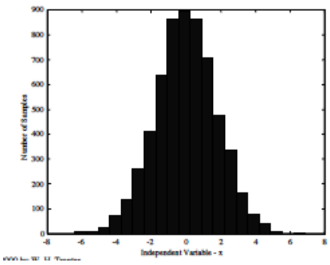
59

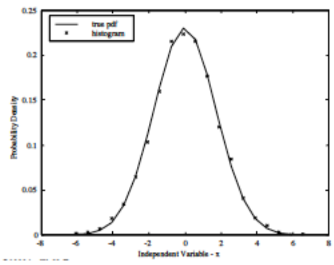
Example 3 MATLAB Code

```
term1 = x_hist.*x_hist/2/varXY;    % exponent
term2 = 1/(sqrt(2*pi*varXY));      % multiplier
gx = term2*exp(-term1);            % Gaussian pdf
del_x = x_hist(3)-x_hist(2);       % determine bin width
p_hist = N_samp/n/del_x;           % histogram points
plot(x_hist,gx,x_hist,p_hist,'X') % compare results

mean_x = mean(x_gaus)              % mean of X
mean_y = mean(y_gaus)              % mean of Y
var_x = cov(x_gaus)                % variance of X
var_y = cov(y_gaus)                % variance of Y
% The next statement deterines the correlation coefficient
rho = mean(x_gaus.*y_gaus)/std(x_gaus)/std(y_gaus)
```

60

Example 3 (N=6000)





mean_x = 0.0099

mean_y = -0.0023

var_x = 3.1511

var_y = 2.9252

rho = -0.0149

Generation of Gaussian RV Sum-of-*K* Method

- Suppose we generate *K* independent values of a uniform random variable *U,* add them together and multiply the result by a constant *B.* As *K* becomes large, the result, *N,* becomes Gaussian.

$$N = B\sum_{i=1}^{K}\left(U_i - \frac{1}{2}\right)$$

The mean is:

$$E\{N\} = E\left[B\sum_{i=1}^{K}\left(U_i - \frac{1}{2}\right)\right] = B\sum_{i=1}^{K}\left(E[U_i] - \frac{1}{2}\right) = 0$$

Sum-of-*K* Method

The variance is:

Since the uniform variants are independence, the variance of N is:

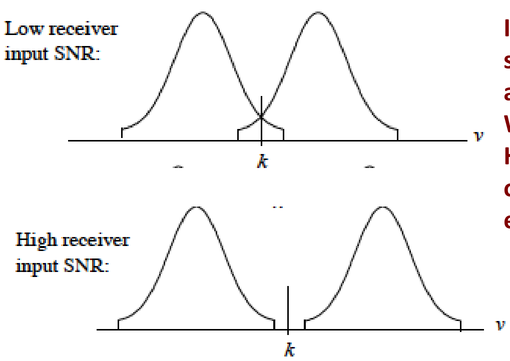
$$\sigma_N^2 = KB^2\sigma_U^2 = \frac{KB^2}{12}$$

For a given value of *K* the value of *B* can be adjusted to obtain any desired variance.

63

Effect of Tail Truncation

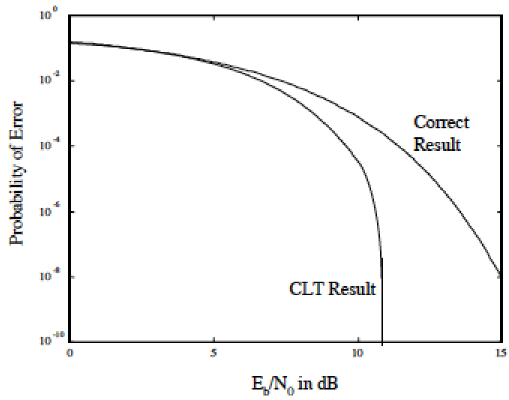
- A significant problem of sum-of-K method is tail truncation of the Gaussian pdf.



In digital communications link simulations the tails of the pdf are <u>most</u> important.
When the SNR becomes sufficiently High, the conditional pdfs no longer overlap and the error becomes exactly zero.

64

Effect of Tail Truncation on BER

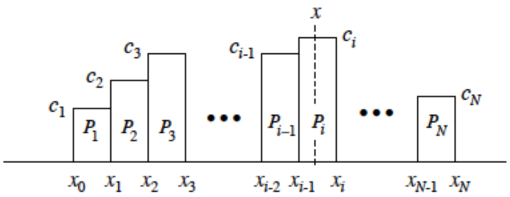


Observations

- For any given SNR one can find a value of *K* which makes this effect negligible. However, since *K* calls to a uniform random number generator are required for each Gaussian variate, the process is too slow to be of practical use.
- These techniques are useful, however, when one requires a random variable that is approximately Gaussian in the neighborhood of the mean.
- An advantage of the CLT method is that, for large *K*, the random variable *N* is approximately Gaussian, at least in the neighborhood of the mean, even if the constituent variables *U* fail to be uniform.

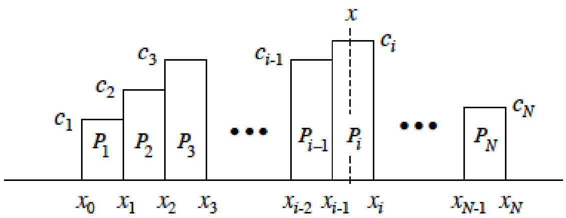
Histogram-based Method

- Problem: Suppose we have a set of experimental data and wish to develop a noise generator that generates numbers with the same pdf as the experimental data. The first step is to approximate the pdf of the experimental data by the histogram.



67

Histogram-based Method



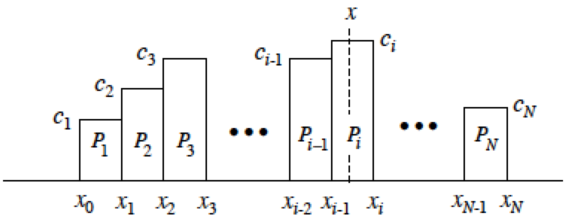
$$f_X(x) \approx \begin{cases} c_i, & x_{i-1} \le x \le x_i, \quad i = 1,2,3,\cdots,N \\ 0, & \text{otherwise} \end{cases}$$

$$P_i = \int_{x_{i-1}}^{x_i} f_X(x)dx, \quad i = 1,2,\cdots,N$$

$$F_i = \sum_{j=1}^{i} P_j$$

68

Histogram-based Method



The CDF at the point $X = x$ is

$$F_X(x) = \sum_{j=1}^{i-1} P_j + \int_{x_{i-1}}^{x_i} c_i \, dx = F_{i-1} + c_i(x - x_{i-1})$$

With $F_X(x) = U$ we have

$$F_X(X) = U = F_{i-1} + c_i(X - x_{i-1})$$

69

Histogram-based Method

Solving

$$F_X(X) = U = F_{i-1} + c_i(X - x_{i-1})$$

gives

$$X = x_{i-1} + \frac{1}{c_i}\left(U - F_{i-1}\right)$$

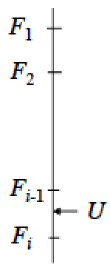
The algorithm is

1. Generate U
2. Find i from

$$F_{i-1} < U \le F_i$$

3. $X \leftarrow x_{i-1} + \frac{1}{c_i}\left(U - F_{i-1}\right)$

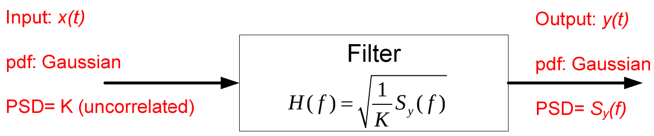
4. Return X



70

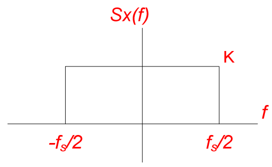
Generating Correlated Gaussian Random Process

Establishing an Arbitrary PSD and Autocorrelation Function



From Linear System Theory:

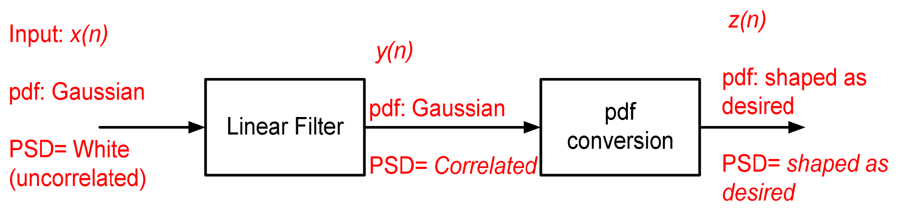
$$S_y(f)=|H(f)|^2\,S_x(f)$$



Example: Jakes Filter Model

Dr Samir Alghadhban

Establishing a pdf and a PSD



Establishing a Given Correlation Coefficient

- Let X and Y be two uncorrelated Gaussian random variables with mean zero and variance σ^2

$$X \sim N(0,\sigma^2) \quad \text{and} \quad Y \sim N(0,\sigma^2)$$

Then, $$Z = \rho X + \sqrt{1-\rho^2}\,Y$$

Will be: $$Z \sim N(0,\sigma^2)$$

and the correlation coefficient between X and Z is

$$\rho_{xz} = \rho$$

Establishing a given correlation coefficient: proof

The mean:

$$E[Z] = \rho E[X] + \sqrt{1-\rho^2}\,E[Y] = 0$$

The variance:

$$\sigma_Z^2 = E[Z^2] = E\left\{\left[\rho X + \sqrt{1-\rho^2}\,Y\right]^2\right\}$$

$$= \rho^2 E[X^2] + 2\rho\sqrt{1-\rho^2}\,E[XY] + (1-\rho^2)E[Y^2]$$

since $E[XY] = E[X]E[Y] = 0$

$$\sigma_Z^2 = \rho^2\sigma^2 + (1-\rho^2)\sigma^2 = \sigma^2$$

Cont.

The Covariance:

$$E[XZ] = E\left\{X\left[\rho X + \sqrt{1-\rho^2}\,Y\right]\right\}$$

$$= \rho E[X^2] + \sqrt{1-\rho^2}\,\underbrace{\cancel{E[XY]}}_{=0}$$

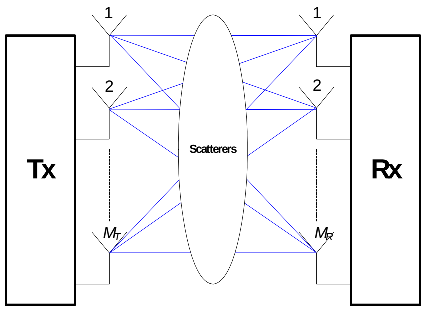
$$= \rho E[X^2] = \rho\sigma^2$$

The Correlation Coefficient:

$$\rho_{XZ} = \frac{E[XZ]}{\sigma_X\sigma_Z} = \frac{\rho\sigma^2}{\sigma^2} = \rho$$

Spatial Correlation: Correlated MIMO Channel Model

$$\mathbf{H}(t) = \begin{bmatrix} h_{11}(t) & \cdots & h_{1M_T}(t) \\ \vdots & \ddots & \vdots \\ h_{M_R1}(t) & \cdots & h_{M_RM_T}(t) \end{bmatrix}$$

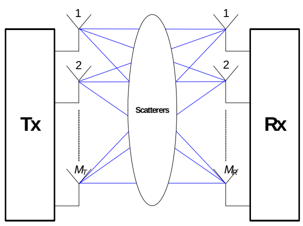


Multiple Input Multiple Output (MIMO) Channels

Correlated MIMO Channel Model

- the spatial covariance matrix of the MIMO channel is

$$\mathbf{R}_{MIMO} = E\{vec(\mathbf{H}) \cdot vec(\mathbf{H})^H\} = \mathbf{R}_R \otimes \mathbf{R}_T$$



$\mathbf{R}_{MIMO}$ is an $M_R M_T \times M_R M_T$ spatial covariance matrix

$vec(\mathbf{H})$ is the vector operator that stacks the columns of the $M_R \times M_T$ matrix $(\mathbf{H})$ into an $M_R M_T \times 1$ column vector .

$\mathbf{H}$ is the $M_R \times M_T$ MIMO channel matrix.

$\mathbf{H}^H$ the superscript $(^H)$ denotes the complex conjugate transpose, known as the Hermitian conjugate.

$E\{\cdot\}$ is the expectation operator.

$\otimes$ is the Kronecker product. The Kronecker product between two matrices is defined as:

$$\mathbf{A}_{m\times n} \otimes \mathbf{B}_{p\times q} = \begin{bmatrix} \mathbf{A}(1,1)\mathbf{B} & \mathbf{A}(1,2)\mathbf{B} & \cdots & \mathbf{A}(1,n)\mathbf{B} \\ \mathbf{A}(2,1)\mathbf{B} & \mathbf{A}(2,2)\mathbf{B} & \cdots & \mathbf{A}(2,n)\mathbf{B} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}(m,1)\mathbf{B} & \mathbf{A}(m,2)\mathbf{B} & \cdots & \mathbf{A}(m,n)\mathbf{B} \end{bmatrix}_{mp\times nq}$$

Where $\mathbf{R_R}$ and $\mathbf{R_T}$ are normalized spatial covariance matrices of the transmitter and receiver elements

Cont.

- Since the covariance matrix is nonnegative definite, it can be factorized using Cholesky decomposition

$$\mathbf{R}_T = \mathbf{L}_T^H \cdot \mathbf{L}_T$$,where **L** is a lower triangular matrix

$$\mathbf{R}_R = \mathbf{L}_R^H \cdot \mathbf{L}_R$$

It is shown that the spatially correlated MIMO channel matrix can be modeled as:

$$\mathbf{H}_{cor} = \mathbf{L}_R^H \cdot \mathbf{H}_{unc} \cdot \mathbf{L}_T^*$$

79

Correlated Rayleigh Fading Channel Simulator Using FIR Filters

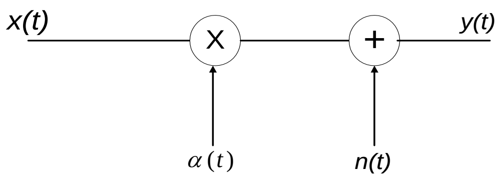
80

Outline

- Motivation
- Rayleigh Channel Model
- Jakes' Spectrum
- Design procedure
- Examples

81

Rayleigh Channel Model



$$y(t) = \alpha(t)x(t) + n(t)$$

Where, $\alpha(t) = \alpha_I(t) + j\alpha_Q(t)$

Zero mean complex Gaussian Random Process

82

Rayleigh Channel Model; Cont.

Envelope $r = |\alpha(t)| = \sqrt{\alpha_I^{\,2} + \alpha_Q^{\,2}}$

$$p(r) = \frac{r}{\sigma^2}\exp(-\frac{r^2}{2\sigma^2}), \qquad r \geq 0$$

Phase $\theta = \tan^{-1}(\alpha_Q / \alpha_I)$

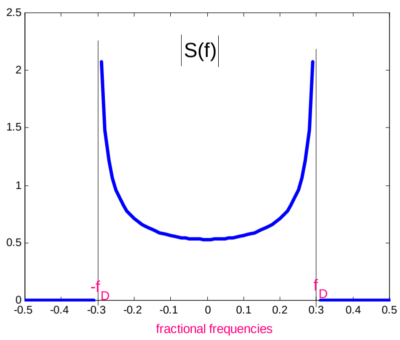
$$p(\theta) = \frac{1}{2\pi}[u(\theta+\pi) - u(\theta-\pi)]$$

83

Mobile Channel Model, Jakes' Spectrum

$$f_D = \frac{v}{c} f_C$$

$$S_J(f) = \begin{cases} \dfrac{\sigma^2}{2\pi f_D\sqrt{1-\left(\dfrac{f}{f_D}\right)^2}}, & |f| < f_D \\ 0, & otherwise \end{cases}$$



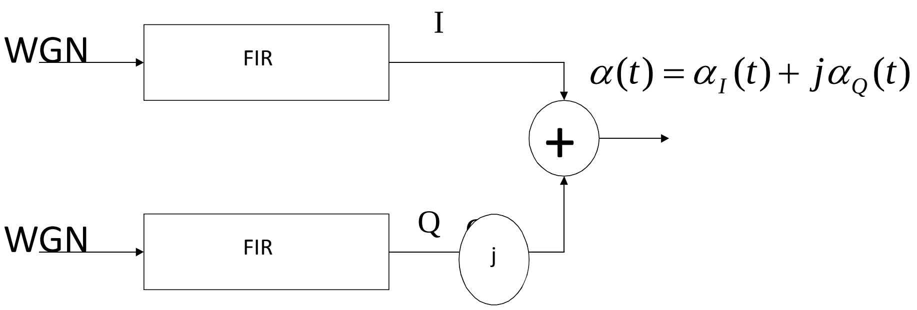
$$R_h(\tau) = \sigma^2 J_0(2\pi f_D \tau)$$

$$J_0(x) = \sum_{n=0}^{\infty}(-1)^2(\frac{x^n}{2^n n!})^2$$

1/30/2014

84

Simulator



Power spectral Density

$$S_{yy}(f) = S_{xx}(f)\left|H(f)\right|^2$$

For the WGRV, $S_{xx}(f) = \sigma_n^2$ For all f. Let σ_n^2 be one

$$S_{yy}(f) = \left|H(f)\right|^2$$

Then, if

$$\boxed{H(f) = \sqrt{S_J(f)} \Rightarrow S_{yy}(f) = S_J(f)}$$

Design Measures

- For a given Doppler Frequency f_D, Divide it by the system Symbol rate f_S. The term $f_D T_S$ is known as the fade rate and it is our main target. Each I and Q components should have this fade rate
- The envelope should be Rayleigh distributed and the phase should be uniformly distributed from $[-\pi, \pi]$
- The mean of each I and Q component should be zero and the power should be normalized to one.

87

Based on Window design

- Find the fade rate $f_D T_S$
- Take enough sample from $S_J(f) = \begin{cases} \dfrac{\sigma^2}{2\pi f_D T_s \sqrt{1 - \left(\dfrac{f}{f_D T_s}\right)^2}}, & |f| < f_D T_s \\ 0, & otherwise \end{cases}$
- h=fir2(N,f,sqrt(Sf),window)
- Since $y[n] = \sum_{k=0}^{N} h[k] x[n-k]$

$$E[y[n]] = \sum_{k=0}^{N} h[k] E[x[n-k]] = 0$$

$$\mathrm{var}[y[n]] = \sum_{k=0}^{N} h^2[k]\, \mathrm{var}[x[n-k]] = \sum_{k=0}^{N} h^2[k] = K$$

88

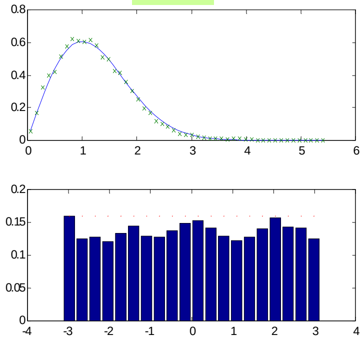
Example; $f_D T_s$=0.01

- Assume a vehicle speed of 60 mi/h, a carrier frequency =900 MHz and a symbol rate of 8000 symbols/s. This results in a $f_D T_s = 0.01$.

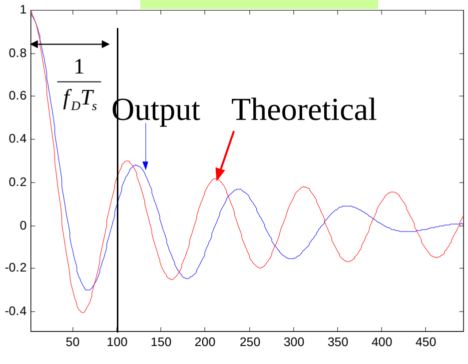
89

Rectangular Window, N=600

PDF

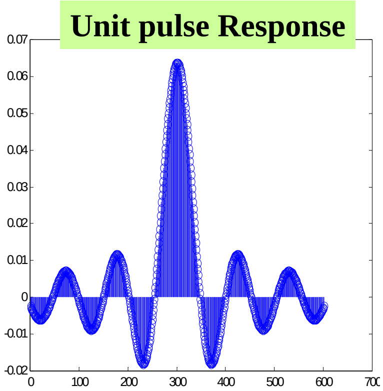


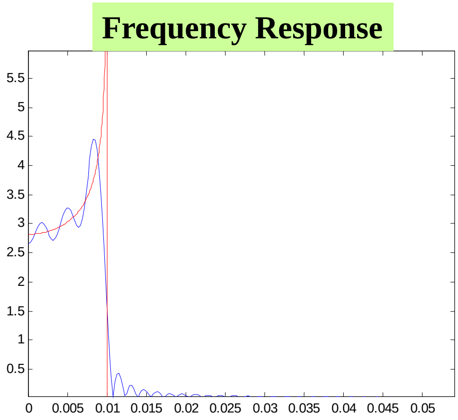
Autocorrelation



90

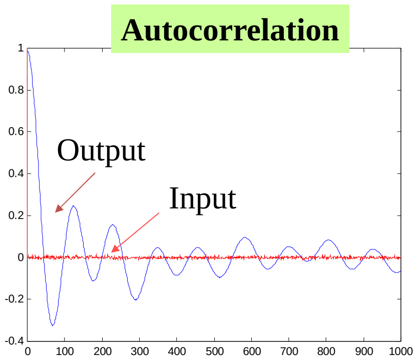
Example1,Cont.



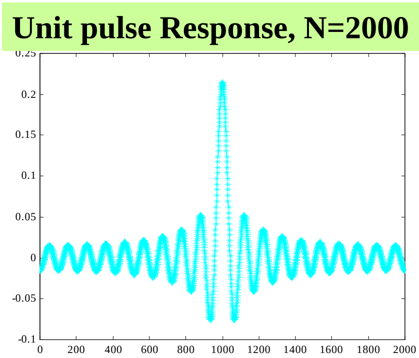


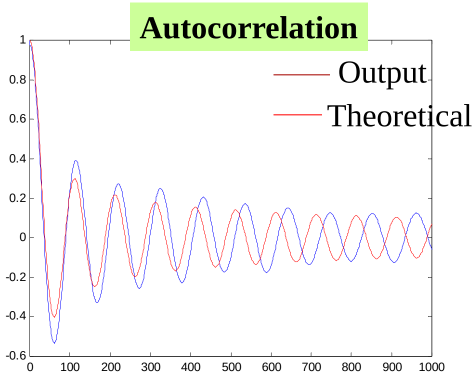
Input vs. Output

	Input	Output
Mean	0.0024	0.0144
Variance	0.9477	0.9957



Frequency Sampling





93