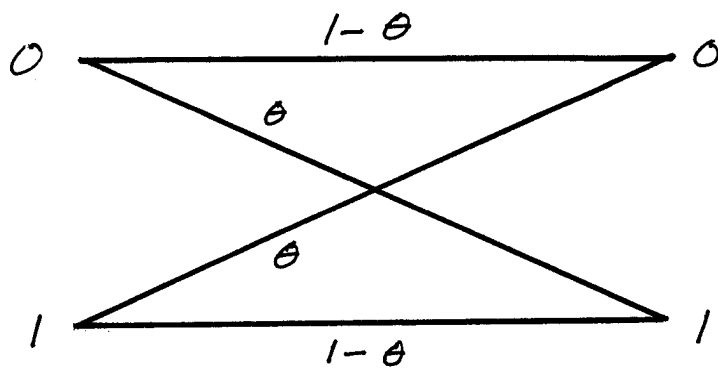


# APPLICATION: BINARY SYMMETRIC CHANNEL

---

In a binary symmetric channel (BSC), whenever we transmit a bit (0 or 1), the bit is flipped with probability  $\theta \in [0, 1]$ .



BSC is a very common model in digital comm. systems

If we denote

$x$  = transmitted bit

$y$  = received bit

then

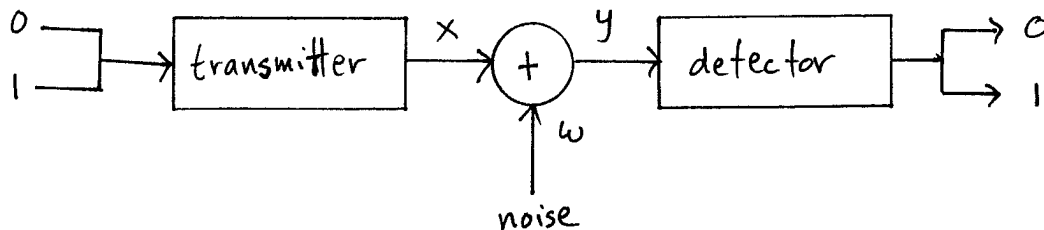
$$y = x + w$$

where

$w \sim \text{Bernoulli}(\theta)$

modular arithmetic:  
 $1 + 1 = 0$

Our job is to build a detector to determine the transmitted bit from the received bit



Let's set this up as a hypothesis testing problem:

$$H_0: y = 0 + w$$

$$H_1: y = 1 + w$$

Equivalently

$$H_0: y \sim \text{Bernoulli}(\theta)$$

$$H_1: y \sim$$

②

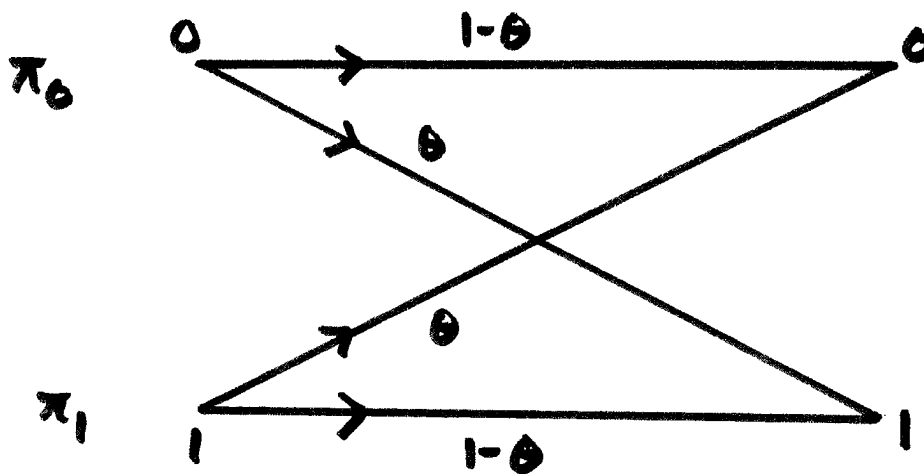
Our goal is effectively to form an estimate  $\hat{x}$  of the transmitted bit  $x$ .

Let's assume  $\theta < \frac{1}{2}$ : more often than not a bit is uncorrupted.

Also assume prior probabilities

$$\pi_i = \Pr\{X = i\}$$

are known.



How should we decode/detect  $y$  so as to minimize the probability of error?

We want to minimize  $P\{\hat{x} \neq x\}$ .

Since this is a very simple detection problem,  
we can write down all 4 possible decision  
rules.

1.  $0 \rightarrow 0$   
 $1 \rightarrow 1$

2.  $0 \rightarrow 0$   
 $1 \rightarrow 0$

3.  $0 \rightarrow 1$   
 $1 \rightarrow 1$

4.  $0 \rightarrow 1$   
 $1 \rightarrow 0$

$$P_e = P\{\hat{x} \neq x\} = P(H_0, H_1) + P(H_1, H_0)$$
$$= \pi_1 P(H_0 | H_1) + \pi_0 P(H_1 | H_0)$$

(b)

$$= \left\{ \begin{array}{l} 1. \\ 2. \\ 3. \\ 4. \end{array} \right.$$

Which is smallest?

Since  $\theta < \frac{1}{2}$ , we know  $\theta < 1 - \theta$ ,  
so the 4th rule never has smallest  $P_e$ .

So there are 3 cases:

- ①
- 1) If  $\theta < \pi_1, \pi_2$   $\hat{x} =$
  - 2) If  $\pi_1 < \theta$   $\hat{x} =$
  - 3) If  $\pi_0 < \theta$   $\hat{x} =$

In general, it will be extremely tedious,  
if not impossible, to enumerate all  
possible decision rules.

Fortunately, there is a systematic way  
to find the decision rule with  
smallest  $P_e$ .

$P_e$  is minimized by the LRT:

$$\Lambda(y) = \frac{f_1(y)}{f_0(y)} \underset{H_0}{\overset{H_1}{>}} \frac{\pi_0}{\pi_1} = \eta$$

where

$$f_1(y) = \begin{cases} 1-\theta & \text{if } y=1 \\ 0 & \text{if } y=0 \end{cases}$$

$$f_0(y) = \begin{cases} \theta & \text{if } y=1 \\ 1-\theta & \text{if } y=0 \end{cases}$$

So

(d)

$$\Lambda(y) =$$

=

Let's apply monotonic transformations to simplify the LRT:

$$\frac{\theta}{1-\theta} \cdot \left(\frac{1-\theta}{\theta}\right)^{2y} \underset{H_0}{\overset{H_1}{\ll}} \eta$$



$$\left(\frac{1-\theta}{\theta}\right)^{2y} \underset{H_0}{\overset{H_1}{\ll}} \eta \cdot \frac{1-\theta}{\theta}$$



$$2y \ln\left(\frac{1-\theta}{\theta}\right) \underset{H_0}{\overset{H_1}{\ll}} \ln(\eta) + \ln\left(\frac{1-\theta}{\theta}\right)$$



$$y \underset{H_0}{\overset{H_1}{\ll}} \frac{1}{2} + \frac{1}{2} \cdot \frac{\ln(\eta)}{\ln\left(\frac{1-\theta}{\theta}\right)} \equiv \delta$$

Note:  $\theta < \frac{1}{2} \Rightarrow \frac{1-\theta}{\theta} > 1 \Rightarrow \ln\left(\frac{1-\theta}{\theta}\right) > 0$

## Three cases:

threshold	decision rule
$\gamma > 1$	$\hat{x} = 0$
$\gamma < 0$	$\hat{x} = 1$
$0 < \gamma < 1$	$\hat{x} = y$

Question Do we need to worry about  $\gamma = 0$  or  $\gamma = 1$ ?

Let's consider each case: Recall  $\gamma = \frac{1}{2} + \frac{1}{2} \frac{\ln(\eta)}{\ln(\frac{1-\theta}{\theta})}$

$$\boxed{\gamma > 1} \iff \frac{\ln(\eta)}{\ln(\frac{1-\theta}{\theta})} > 1$$

$$\iff \ln(\eta) > \ln\left(\frac{1-\theta}{\theta}\right)$$

$$\iff \eta > \frac{1-\theta}{\theta} \quad \left[ \text{Recall } \eta = \frac{\pi_0}{\pi_1} = \frac{1-\pi_1}{\pi_1} \right]$$

$$\iff \frac{1-\pi_1}{\pi_1} > \frac{1-\theta}{\theta}$$

$$\iff \frac{1}{\pi_1} - 1 > \frac{1}{\theta} - 1$$

$$\iff \frac{1}{\pi_1} > \frac{1}{\theta} \iff \boxed{\pi_1 < \theta}$$



$$\boxed{\gamma < 0} \iff \frac{\ln(\eta)}{\ln\left(\frac{1-\theta}{\theta}\right)} < -1$$

$$\iff \ln(\eta) < \ln\left(\frac{\theta}{1-\theta}\right)$$

$$\iff \eta < \frac{\theta}{1-\theta}$$

$$\iff \frac{\pi_0}{1-\pi_0} < \frac{\theta}{1-\theta}$$

$$\iff \frac{1-\pi_0}{\pi_0} > \frac{1-\theta}{\theta}$$

$$\iff \frac{1}{\pi_0} - 1 > \frac{1}{\theta} - 1$$

$$\iff \frac{1}{\pi_0} > \frac{1}{\theta} \iff \boxed{\pi_0 < \theta}$$

$\boxed{0 < \gamma < 1}$  From the previous two cases,

we conclude

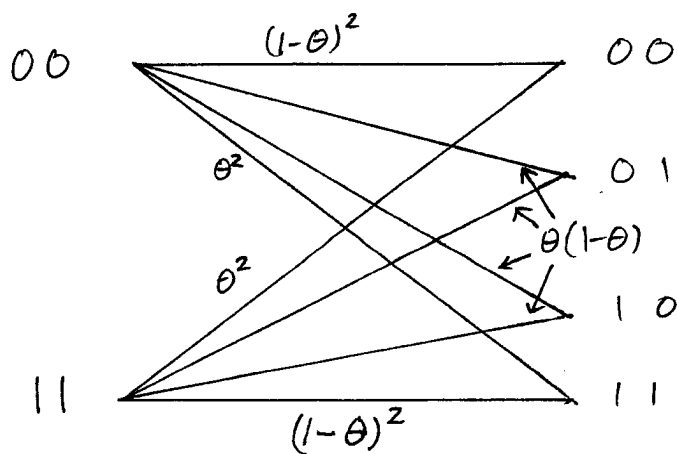
$$0 < \gamma < 1 \iff \boxed{\theta < \pi_1 \text{ and } \theta < \pi_2.}$$

Conclusion. The LRT coincides with the minimum probability of error detector we derived by hand, for each case of  $\theta, \pi_1, \pi_2$ .

# Binary Repetition Code

In an effort to decrease  $P_e$ , let's send  $N$  copies of each "information" bit:

Example |  $N=2$



As a hypothesis testing problem, we have

$$H_0: \underline{y} = 00 \dots 0 + \underline{w}$$

$$H_1: \underline{y} = 11 \dots 1 + \underline{w}$$

where

$$\underline{y} = (y_1, \dots, y_N)^T$$

$$\underline{w} = (w_1, \dots, w_N)^T$$

$$w_n \stackrel{iid}{\sim} \text{Bernoulli}(\theta)$$

The brute force approach is impractical for large  $N$ .

② The total number of possible decision rules is \_\_\_\_\_.

Exercise 1 Apply the LRT to determine the min  $P_E$  detector. Express your answer in terms of a one dimensional test statistic. Derive a formula for  $P_E$  in terms of  $N$ ,  $\theta$ , and  $\eta = \frac{\pi_0}{\pi_1}$ .

# Solution

$$\Lambda(\underline{y}) = \frac{f_1(\underline{y})}{f_0(\underline{y})} = \frac{\prod_{n=1}^N (1-\theta)^{y_n} \theta^{1-y_n}}{\prod_{n=1}^N \theta^{y_n} (1-\theta)^{1-y_n}}$$

$$k = \sum_{n=1}^N y_n$$

sufficient  
statistic

$$= \frac{(1-\theta)^k \theta^{N-k}}{\theta^k (1-\theta)^{N-k}} = \left(\frac{1-\theta}{\theta}\right)^{2k-N}$$

After some simplification

$$\Lambda(\underline{y}) \underset{H_0}{\overset{H_1}{\gtrless}} \eta \iff (2k-N) \ln\left(\frac{1-\theta}{\theta}\right) \underset{H_0}{\overset{H_1}{\gtrless}} \ln(\eta)$$

$$\iff k \underset{H_0}{\overset{H_1}{\gtrless}} \frac{N}{2} + \frac{1}{2} \frac{\ln(\eta)}{\ln\left(\frac{1-\theta}{\theta}\right)} \equiv \gamma$$

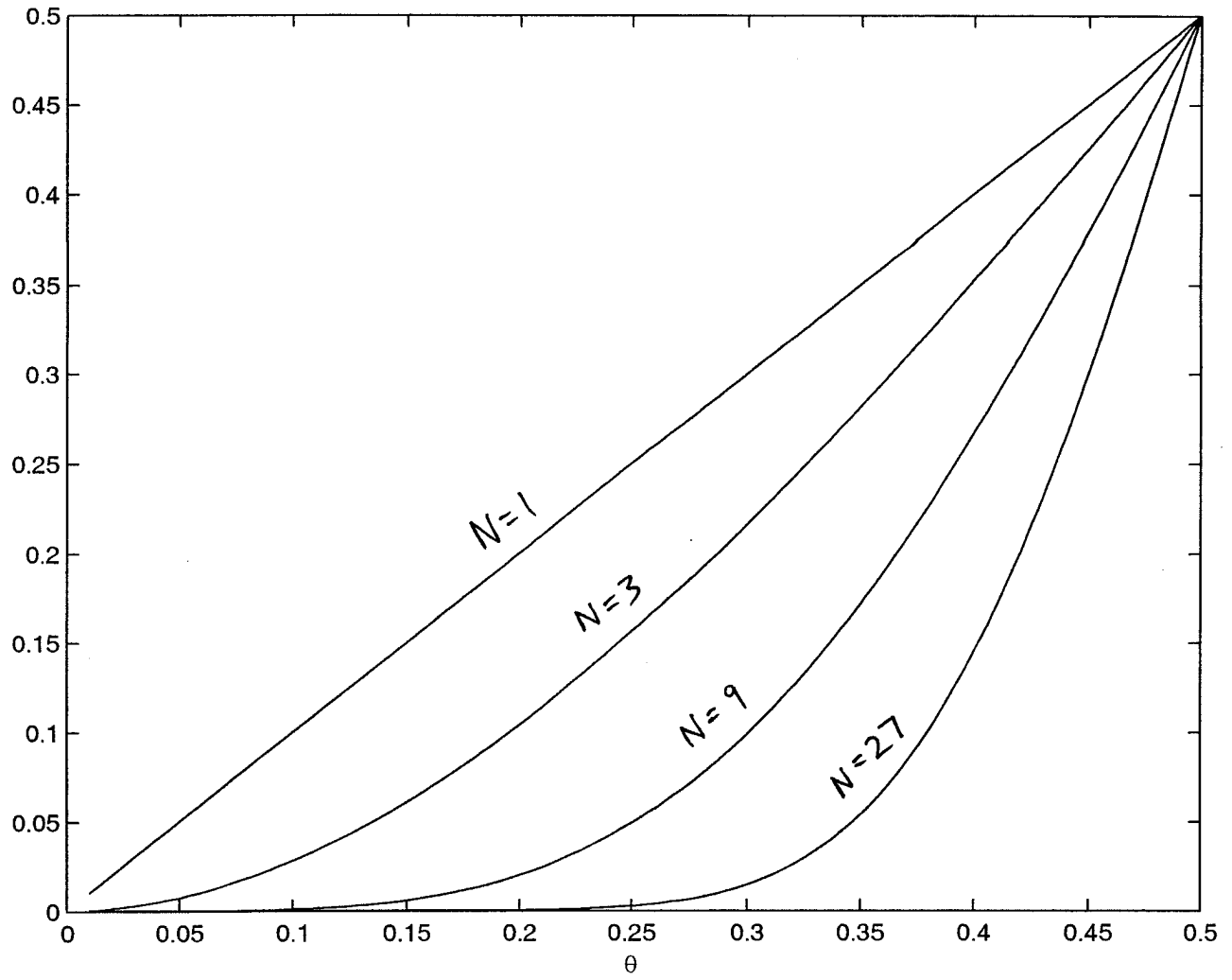
In the special case  $\eta = 1$  ( $\pi_0 = \pi_1 = \frac{1}{2}$ ),

$$k \underset{H_0}{\overset{H_1}{\gtrless}} \frac{N}{2}$$

"majority vote"

In case  $k = \gamma$ , let's declare  $H_0$ .

$P_e$  versus  $\theta$



---

---

```
% Binary repetition code
```

```
close all
```

```
for N=[1 3 9 27]
```

```
    Npts=100;
```

```
    p=linspace(.01,.5,Npts);
```

```
    pi0=1/2;
```

```
    pi1=1-pi0;
```

```
    eta=pi0/pi1;
```

```
    for j=1:Npts
```

```
        gam=N/2 +.5*(log(eta)/log((1-p)/p));
```

```
        pmf0=zeros(1,N+1);
```

```
        for k=0:N
```

```
            pmf0(k+1)=nchoosek(N,k)*(p(j)^k)*((1-p(j))^(N-k));
```

```
        end
```

```
        Pf = sum(pmf0(find(0:N>gam)));
```

```
        pmf1=zeros(1,N+1);
```

```
        for k=0:N
```

```
            pmf1(k+1)=nchoosek(N,k)*((1-p(j))^k)*(p(j)^(N-k));
```

```
        end
```

```
        Pm = sum(pmf1(find(0:N<=gam)));
```

```
        Pe(j)=pi0*Pf+pi1*Pm;
```

```
    end
```

```
    plot(p,Pe)
```

```
    hold on
```

```
end
```

```
xlabel('\theta');
```

Now let's design a Neyman-Pearson detector:

To be concrete, let's say  $N=15$ ,  $\theta = \frac{1}{4}$ ,  $\alpha = 0.2$

We need to find  $\gamma, \rho$  such that

$$P(k > \gamma | H_0) + \rho P(k = \gamma | H_0) = \alpha$$

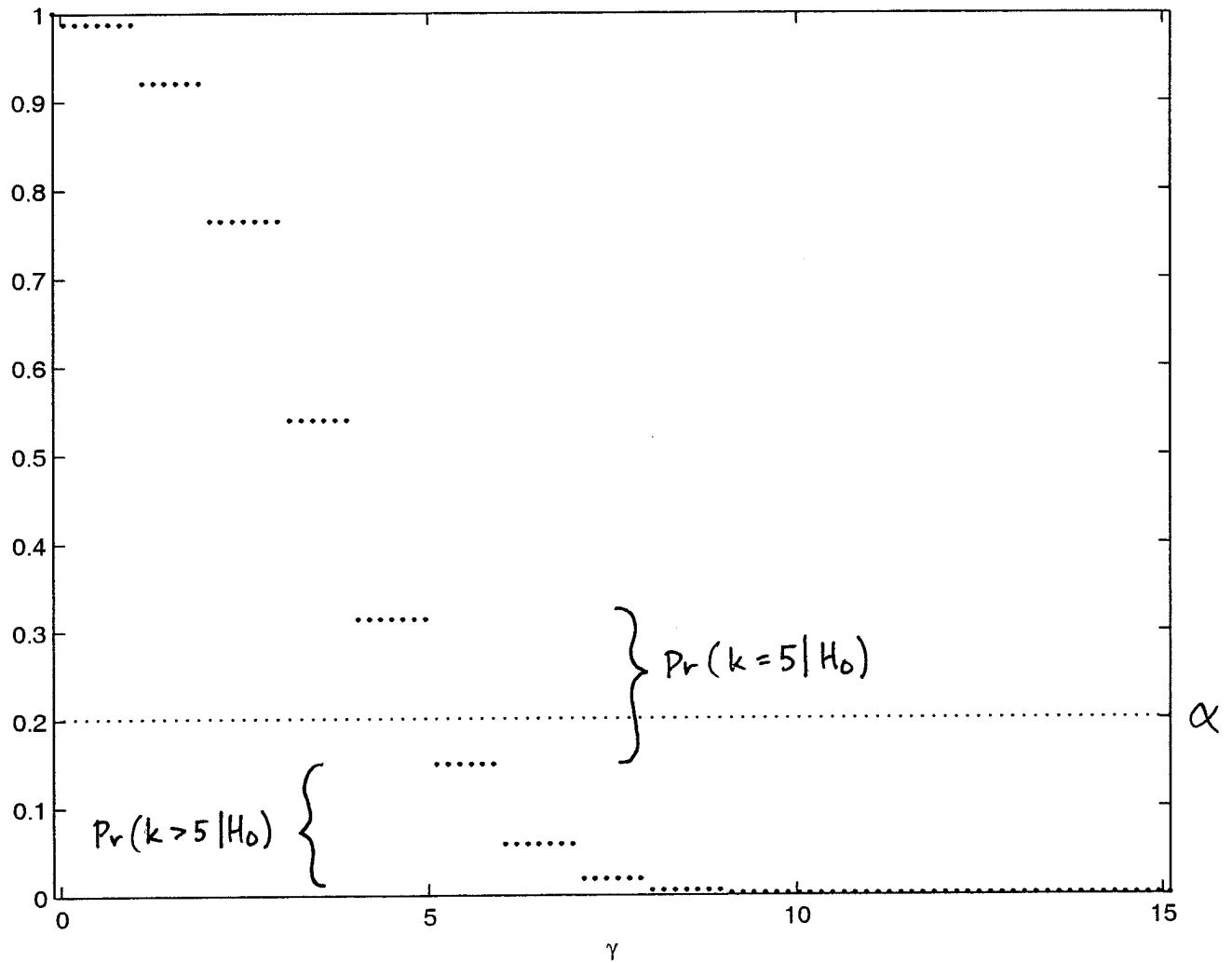
where  $\gamma \in \{0, 1, \dots, N\}$ ,  $\rho \in [0, 1)$ .

[see plot on next page]

So the NP detector is

- If  $k > 5$ , declare  $H_1$
- If  $k < 5$ , declare  $H_0$
- If  $k = 5$ , flip a coin that turns up heads ( $H_1$ ) with probability  $\rho = .3126$

$$\Pr(k > \gamma | H_0)$$



$$\rho = \frac{\alpha - \Pr(k > 5 | H_0)}{\Pr(k = 5)} = .3126$$

$$\Leftrightarrow P_F = \Pr(k > 5 | H_0) + \rho \Pr(k = 5 | H_0) = \alpha$$



---

```
% Binary repetition code
```

```
close all
```

```
N=15;  
alpha=0.2;  
p=.25;
```

```
pmf0=zeros(1,N+1);  
for k=0:N  
    pmf0(k+1)=nchoosek(N,k)*(p^k)*((1-p)^(N-k));  
end
```

```
Npts=100;  
gam = linspace(-.1,N+.1,Npts);  
for j=1:Npts  
    Pf(j) = sum(pmf0(find(0:N>gam(j))));  
end
```

```
plot(gam,Pf, '.')  
hold on  
plot(gam,alpha,'--')
```

```
xlabel('\gamma');  
axis tight
```

```
% gamma = 5 by inspection of graph  
rho = (alpha - sum(pmf0(0:N>5)))/pmf0(5+1) % recall Matlab indexing starts  
at 1
```

# Error Correcting Codes

There are more sophisticated ways of introducing redundancy in order to reduce the probability of error per "information bit."

## Example Hamming (7,4) code

$\underline{x}_1$	00000000	$\underline{x}_9$	1000011
$\underline{x}_2$	0001111	$\underline{x}_{10}$	1001100
$\underline{x}_3$	0010110	$\underline{x}_{11}$	1010101
$\underline{x}_4$	0011001	$\underline{x}_{12}$	1011010
$\underline{x}_5$	0100101	$\underline{x}_{13}$	1100110
$\underline{x}_6$	0101010	$\underline{x}_{14}$	1101001
$\underline{x}_7$	0110011	$\underline{x}_{15}$	1110000
$\underline{x}_8$	0110100	$\underline{x}_{16}$	1111111

"information bits"
"parity check bits"

## M-ary hypothesis test

$$\begin{aligned}
 H_1 : \underline{y} &= \underline{x}_1 + \underline{w} \\
 &\vdots \\
 H_M : \underline{y} &= \underline{x}_M + \underline{w}
 \end{aligned}$$

Recall the MAP detector:

Choose  $H_i$  such that  $\pi_i f_i(\underline{y})$  is maximal

In communication systems, we often know

$$\pi_1 = \pi_2 = \dots = \pi_M = \frac{1}{M}$$

in which case we get the maximum likelihood detector:

choose  $H_i$  such that  $f_i(\underline{y})$  is maximal

In general,  $f_i(\underline{y})$  is easily computed as a product of Bernoulli likelihoods, since  $x_i$  is known.

## Key

a. Bernoulli ( $1-\theta$ )

b. 1.  $\pi_1 \cdot \theta + \pi_0 \cdot \theta = \theta$

2.  $\pi_1 \cdot 1 + \pi_0 \cdot 0 = \pi_1$

3.  $\pi_1 \cdot 0 + \pi_0 \cdot 1 = \pi_0$

4.  $\pi_1 (1-\theta) + \pi_0 (1-\theta) = 1-\theta$

c. 1.  $\hat{x} = y$

2.  $\hat{x} = 0$

3.  $\hat{x} = 1$

d.  $\lambda(y) = \frac{(1-\theta)^y \theta^{1-y}}{\theta^y (1-\theta)^{1-y}} = \frac{\theta}{1-\theta} \cdot \left(\frac{1-\theta}{\theta}\right)^{2y}$

e.  $2^{2^N}$

f. Under  $H_0$ ,  $k \sim \text{Binom}(N, \theta)$

$$f_0(k) = \binom{N}{k} \theta^k (1-\theta)^{N-k}$$

$$P_F = \sum_{k > \gamma} \binom{N}{k} \theta^k (1-\theta)^{N-k}$$

Under  $H_1$ ,  $k \sim \text{Binom}(N, 1-\theta)$