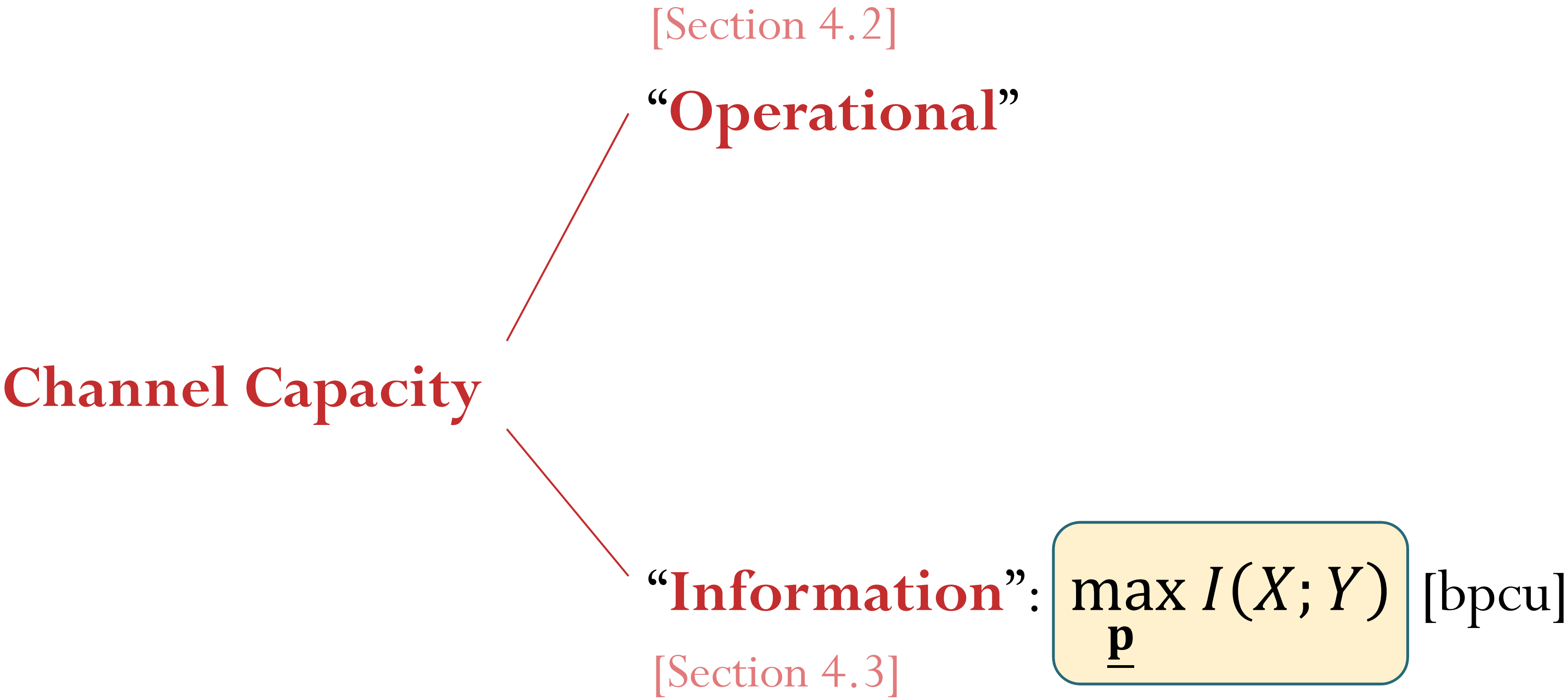
Digital Communication Systems ECS 452

Asst. Prof. Dr. Prapun Suksompong

prapun@siit.tu.ac.th

4.2 Operational Channel Capacity

Channel Capacity



[Section 4.2]

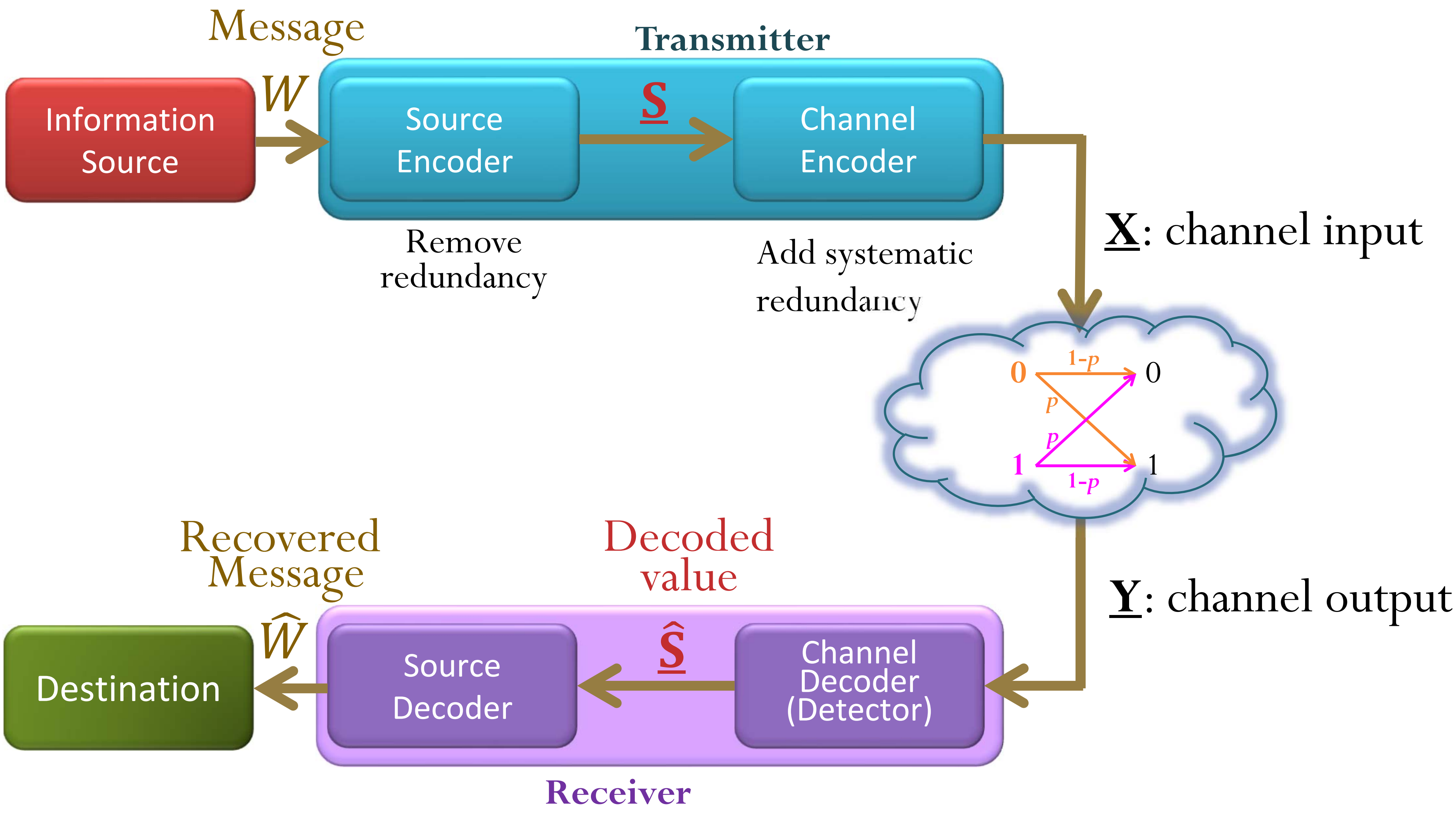
"Operational"

Channel Capacity

"Information": $\boxed{\max_{\underline{\mathbf{p}}} I(X;Y)}$ [bpcu]

[Section 4.3]

System Model for Section 3.5



Message

W

Information Source

Transmitter

Source Encoder

$\underline{S}$

Channel Encoder

Remove redundancy

Add systematic redundancy

$\underline{X}$: channel input

$\underline{Y}$: channel output

Recovered Message

$\hat{W}$

Destination

Decoded value

Source Decoder

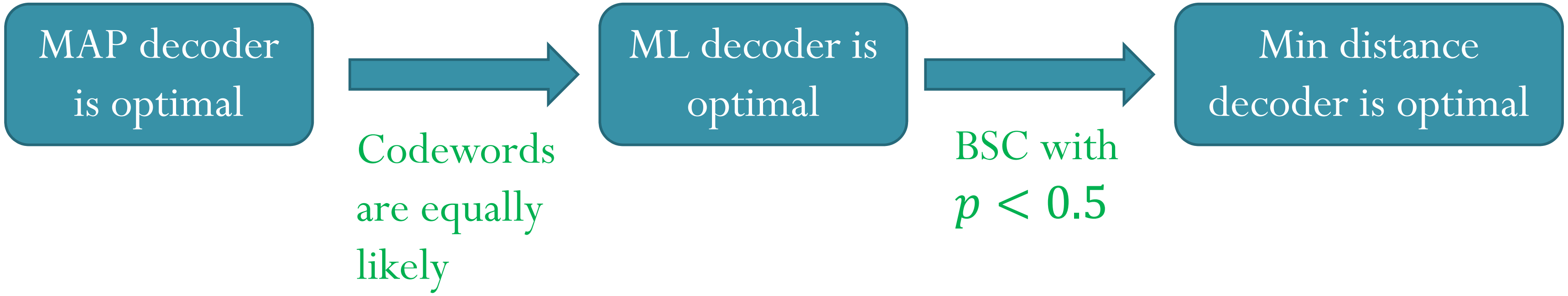
$\hat{\underline{S}}$

Channel Decoder (Detector)

Receiver

System Model for Section 3.5

- Assumptions:
  - BSC
    - with $p < 0.5$.
  - Codewords are equally likely.
- Under such assumption,
  minimum distance decoder is optimal.



MAP decoder is optimal

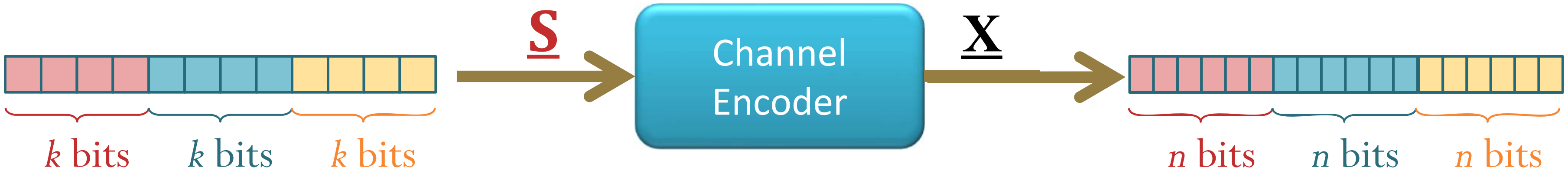
Codewords are equally likely

ML decoder is optimal

BSC with $p < 0.5$

Min distance decoder is optimal

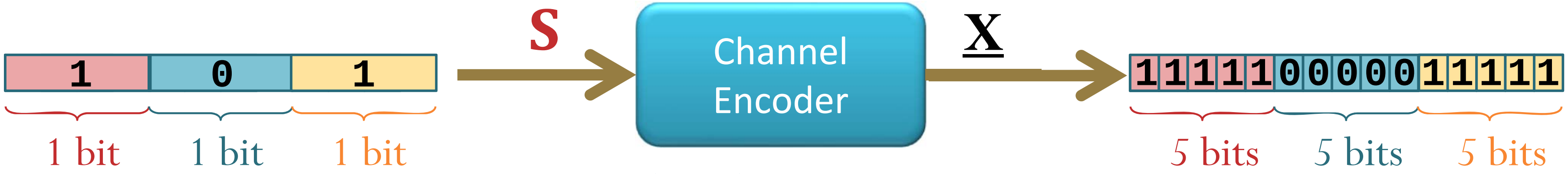
[3.62] Block Encoding



(n, k) code

$\text{Code rate} = \frac{k}{n}$ [bpcu]

Example: Repetition Code



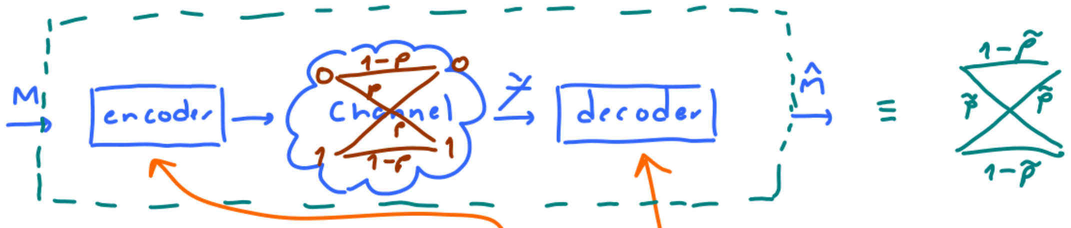
$(5, 1)$ code

$\text{Code rate} = \frac{1}{5}$ [bpcu]

Review

[From ECS315]

One method of reducing the error rate is to use error-correcting codes:



A simple error-correcting code is the *repetition code*. Example of such code is described below:

Two ways to calculate the probability of error:

(a) (transmission) error occurs if and only if the number of bits in error are ≥ 3.

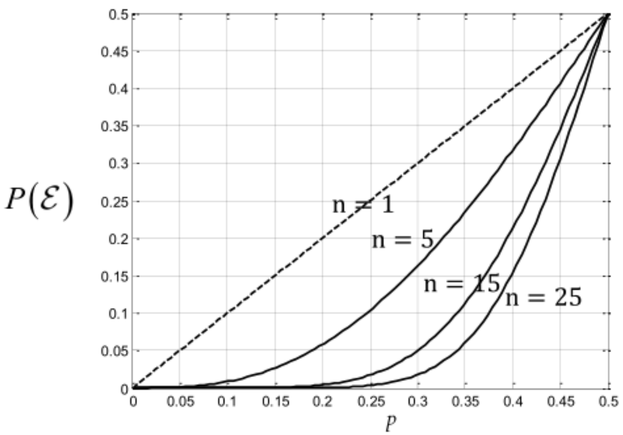
$$\tilde{p} \equiv P(\mathcal{E}) = \underbrace{\binom{5}{3}p^3(1-p)^2}_{}\!\!\overset{\text{exactly 3 error bits}}{} + \overset{4}{\binom{5}{4}p^4(1-p)} + \overset{5}{\binom{5}{5}p^5\cancel{(1-p)^0}}$$

with $p = 0.01$

$P(\mathcal{E}) \approx 10^{-5}$

(b) (transmission) error occurs if and only if the number of bits *not* in error are ≤ 2. → 0, 1, 2

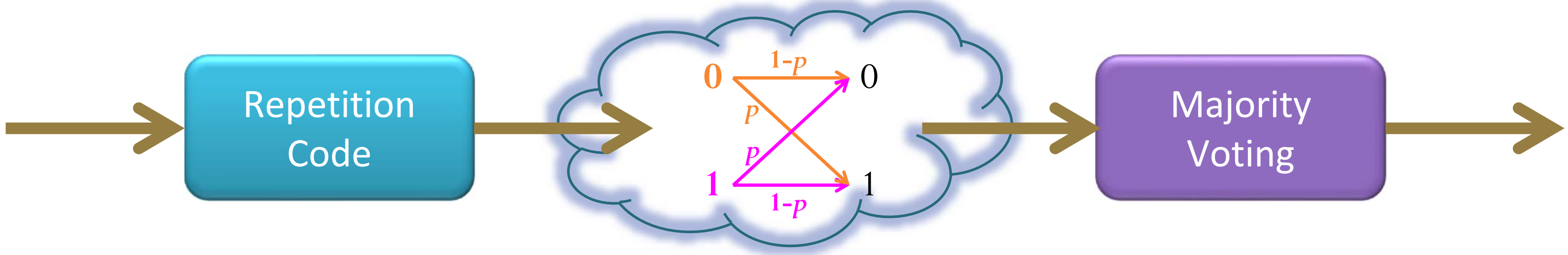
$$P(\mathcal{E}) = \binom{5}{0}(1-p)^0p^5 + \binom{5}{1}(1-p)^1p^4 + \binom{5}{2}(1-p)^2p^3$$



Example: Repetition Code

[ECS315]

BSC with $p = 0.2$

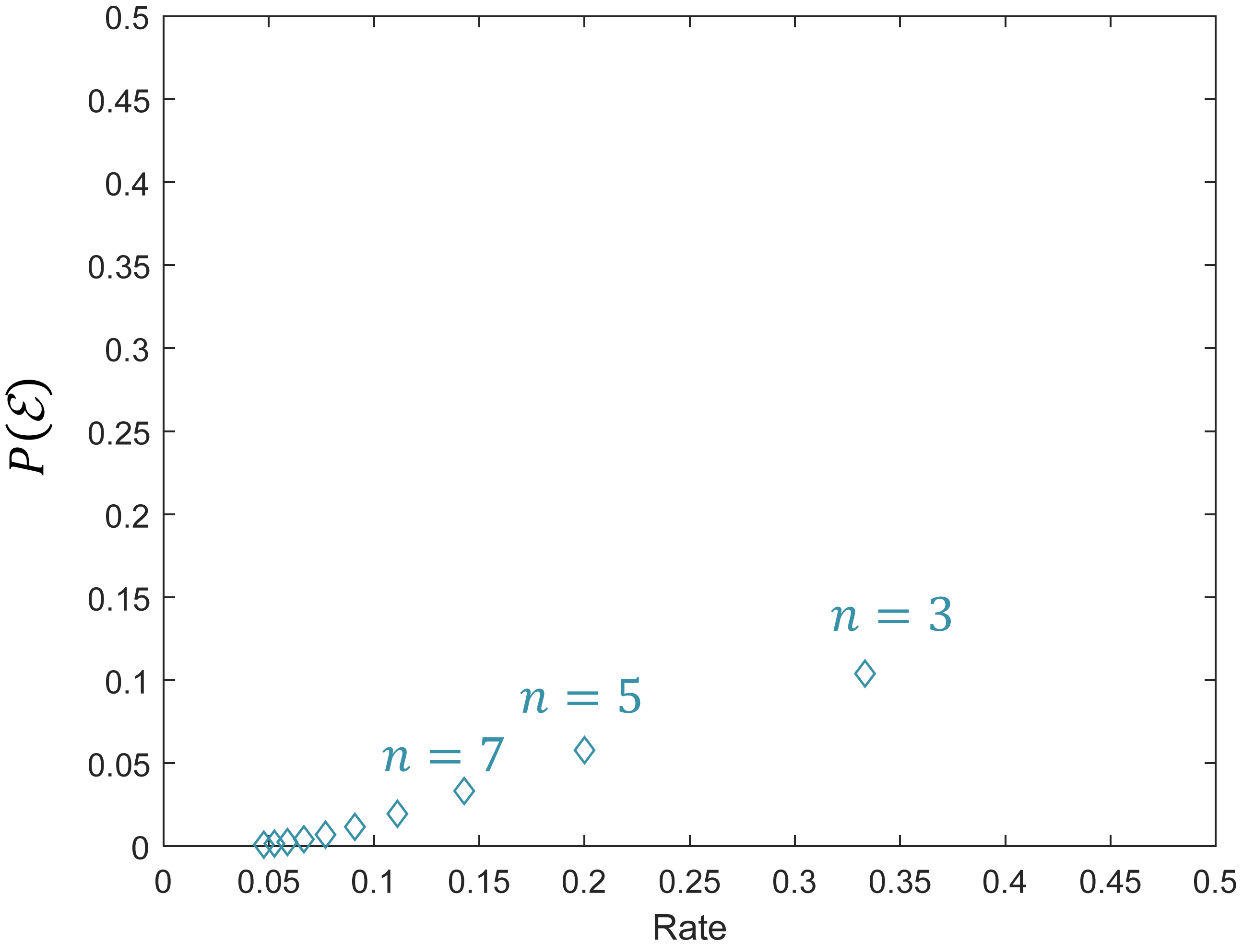

Repetition Code

Majority Voting

n	$P(\mathcal{E})$ Probability that more than half of the bits are in error	Code Rate
1	$p = 0.2$	$\frac{1}{1} = 1$
3	$\binom{3}{2}p^2(1-p) + \binom{3}{3}p^3 \approx 0.1040$	$\frac{1}{3} \approx 0.33$
5	$\binom{5}{3}p^3(1-p)^2 + \binom{5}{4}p^4(1-p)^1 + \binom{5}{5}p^5 \approx 0.0579$	$\frac{1}{5} = 0.2$
7	≈ 0.0333	$\frac{1}{7} \approx 0.1429$
9	≈ 0.0196	$\frac{1}{9} \approx 0.1111$
11	≈ 0.0117	$\frac{1}{11} \approx 0.0909$

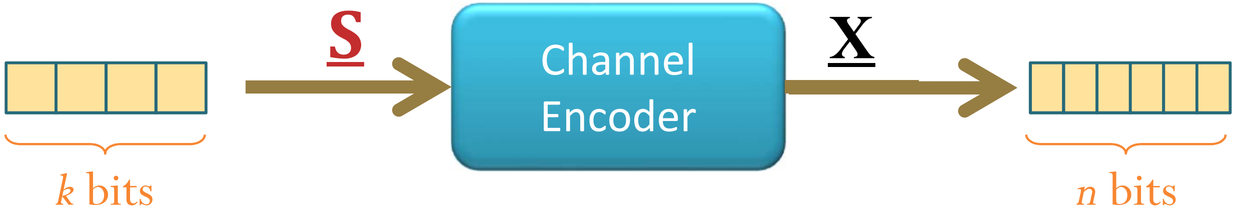
Achievable Performance

BSC with $p = 0.2$ Repetition Code $(k = 1)$

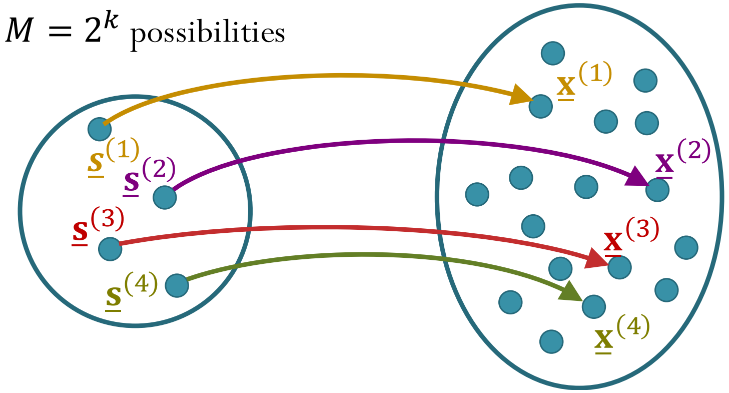


Designing Channel Encoder

[3.61]



[Figure 13]


$M = 2^k$ possibilities
$\underline{\mathbf{s}}^{(1)}$
$\underline{\mathbf{s}}^{(2)}$
$\underline{\mathbf{s}}^{(3)}$
$\underline{\mathbf{s}}^{(4)}$
$\underline{\mathbf{x}}^{(1)}$
$\underline{\mathbf{x}}^{(2)}$
$\underline{\mathbf{x}}^{(3)}$
$\underline{\mathbf{x}}^{(4)}$

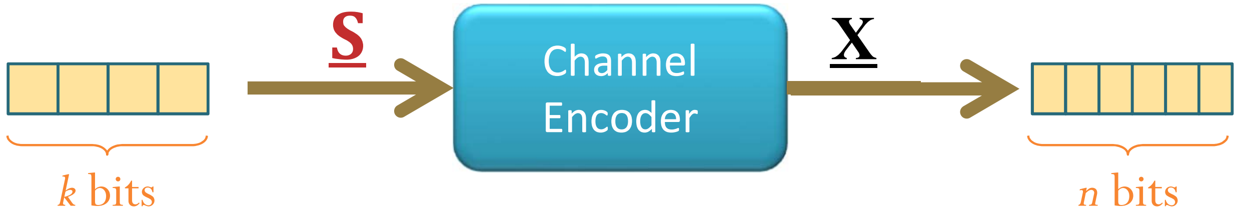
Choose $M = 2^k$ from 2^n possibilities to be used as codewords.

Codebook

index i	info-block $\underline{\mathbf{s}}$	codeword $\underline{\mathbf{x}}$
1	$\underline{\mathbf{s}}^{(1)} = 000\dots0$	$\underline{\mathbf{x}}^{(1)} =$
2	$\underline{\mathbf{s}}^{(2)} = 000\dots1$	$\underline{\mathbf{x}}^{(2)} =$
$\vdots$	$\vdots$	$\vdots$
M	$\underline{\mathbf{s}}^{(M)} = 111\dots1$	$\underline{\mathbf{x}}^{(M)} =$

Designing Channel Encoder

[3.61]



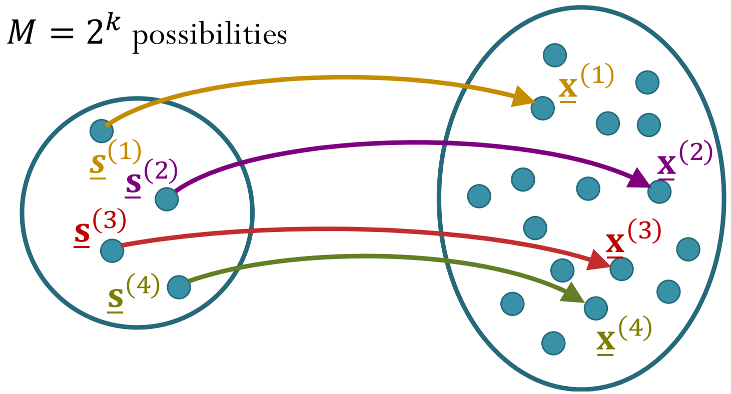
$\underline{\mathbf{S}}$

Channel Encoder

$\underline{\mathbf{X}}$

k bits

n bits



$M = 2^k$ possibilities

$\underline{\mathbf{s}}^{(1)}$ $\underline{\mathbf{s}}^{(2)}$ $\underline{\mathbf{s}}^{(3)}$ $\underline{\mathbf{s}}^{(4)}$

$\underline{\mathbf{x}}^{(1)}$ $\underline{\mathbf{x}}^{(2)}$ $\underline{\mathbf{x}}^{(3)}$ $\underline{\mathbf{x}}^{(4)}$

Choose $M = 2^k$ from 2^n possibilities to be used as codewords.

[Figure 13]

Codebook

$\underline{\mathbf{s}}$	$\underline{\mathbf{x}}$
00	? ? ? ? ?
01	? ? ? ? ?
10	? ? ? ? ?
11	? ? ? ? ?

Designing Channel Encoder

2^k rows

$\underline{\mathbf{s}}$	$\underline{\mathbf{x}}$
00	? ? ? ? ?
01	? ? ? ? ?
10	? ? ? ? ?
11	? ? ? ? ?

n columns

Each "?" can be 0 or 1.

So, there are

$$2^{\left(n2^k\right)}$$

possibilities.

Designing Channel Encoder

2^k rows

$\underline{\mathbf{s}}$	$\underline{\mathbf{x}}$
00	? ? ? ? ?
01	? ? ? ? ?
10	? ? ? ? ?
11	? ? ? ? ?

n columns

Each "?" can be 0 or 1.

So, there are

$$2^{(n2^k)}$$ $= 1{,}048{,}576$ for $n = 5$, $k = 2$

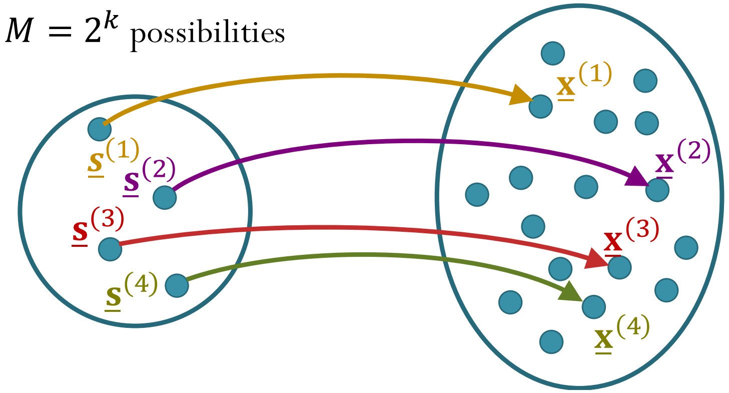
possibilities.

But we don't want to use the same codeword to represent two different info blocks.

So, actually, we need to consider

$$\binom{2^n}{2^k}$$ $= 35{,}960$ for $n = 5$, $k = 2$

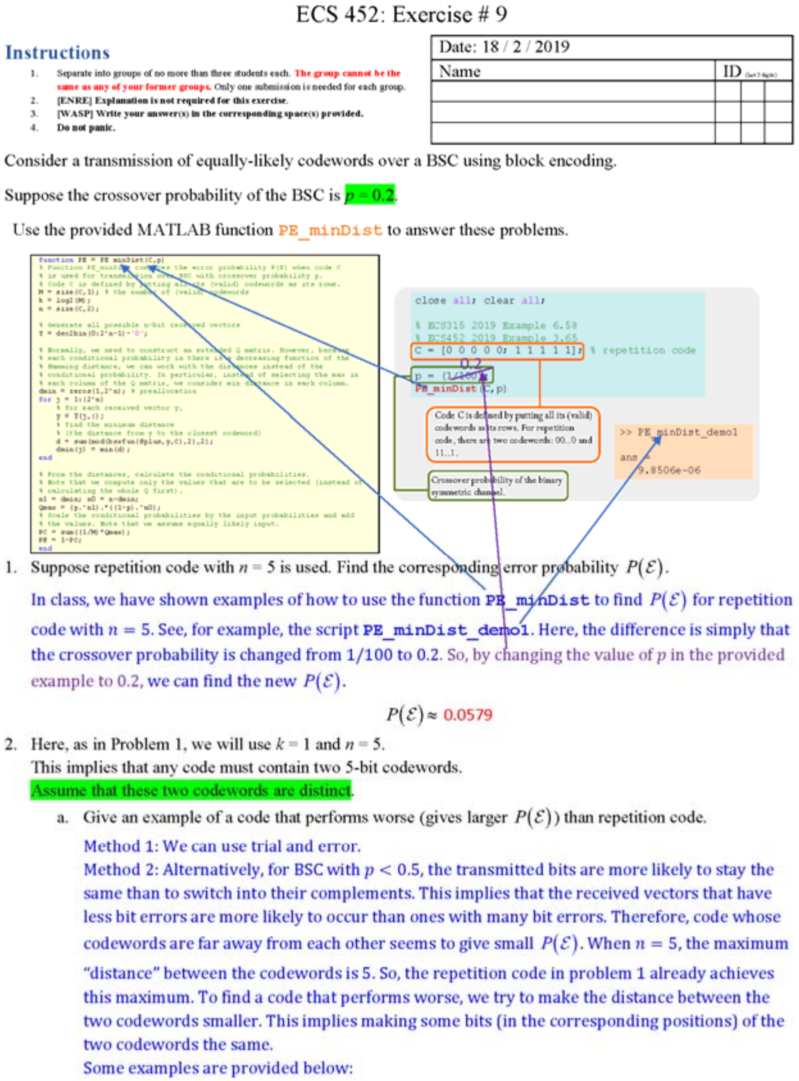
possibilities.



$M = 2^k$ possibilities
$\underline{\mathbf{s}}^{(1)}$
$\underline{\mathbf{s}}^{(2)}$
$\underline{\mathbf{s}}^{(3)}$
$\underline{\mathbf{s}}^{(4)}$
$\underline{\mathbf{x}}^{(1)}$
$\underline{\mathbf{x}}^{(2)}$
$\underline{\mathbf{x}}^{(3)}$
$\underline{\mathbf{x}}^{(4)}$

Choose $M = 2^k$ from 2^n possibilities to be used as codewords.

Exercise 9



ECS 452: Exercise # 9

Instructions

1. Separate into groups of no more than three students each. **The group cannot be the same as any of your former groups.** Only one submission is needed for each group.
2. **[ENRE] Explanation is not required for this exercise.**
3. **[WASP] Write your answer(s) in the corresponding space(s) provided.**
4. **Do not panic.**

Date: 18 / 2 / 2019			
Name	ID (last 3 digits)		

Consider a transmission of equally-likely codewords over a BSC using block encoding.

Suppose the crossover probability of the BSC is $p = 0.2$.

Use the provided MATLAB function `PE_minDist` to answer these problems.

```
function PE = PE_minDist(C,p)
% Function PE_minDist computes the error probability P(E) when code C
% is used for transmission over BSC with crossover probability p.
% Code C is defined by putting all its (valid) codewords as its rows.
M = size(C,1); % the number of (valid) codewords
k = log2(M);
n = size(C,2);

% Generate all possible n-bit received vectors
Y = dec2bin(0:2^n-1)-'0';

% Normally, we need to construct an extended Q matrix. However, because
% each conditional probability in there is a decreasing function of the
% Hamming distance, we can work with the distances instead of the
% conditional probability. In particular, instead of selecting the max in
% each column of the Q matrix, we consider min distance in each column.
dmin = zeros(1,2^n); % preallocation
for j = 1:(2^n)
    % for each received vector y,
    y = Y(j,:);
    % find the minimum distance
    % (the distance from y to the closest codeword)
    d = sum(mod(bsxfun(@plus,y,C),2),2);
    dmin(j) = min(d);
end

% From the distances, calculate the conditional probabilities.
% Note that we compute only the values that are to be selected (instead of
% calculating the whole Q first).
n1 = dmin; n0 = n-dmin;
Qmax = (p.^n1).*((1-p).^n0);
% Scale the conditional probabilities by the input probabilities and add
% the values. Note that we assume equally likely input.
PC = sum((1/M)*Qmax);
PE = 1-PC;
end
```

```
close all; clear all;

% ECS315 2019 Example 6.58
% ECS452 2019 Example 3.65
C = [0 0 0 0 0; 1 1 1 1 1]; % repetition code
         0.2
p = (1/100);
PE_minDist(C,p)
```

Code C is defined by putting all its (valid) codewords as its rows. For repetition code, there are two codewords: 00..0 and 11..1.

Crossover probability of the binary symmetric channel.

```
>> PE_minDist_demo1

ans =
   9.8506e-06
```

1. Suppose repetition code with $n = 5$ is used. Find the corresponding error probability $P(\mathcal{E})$.

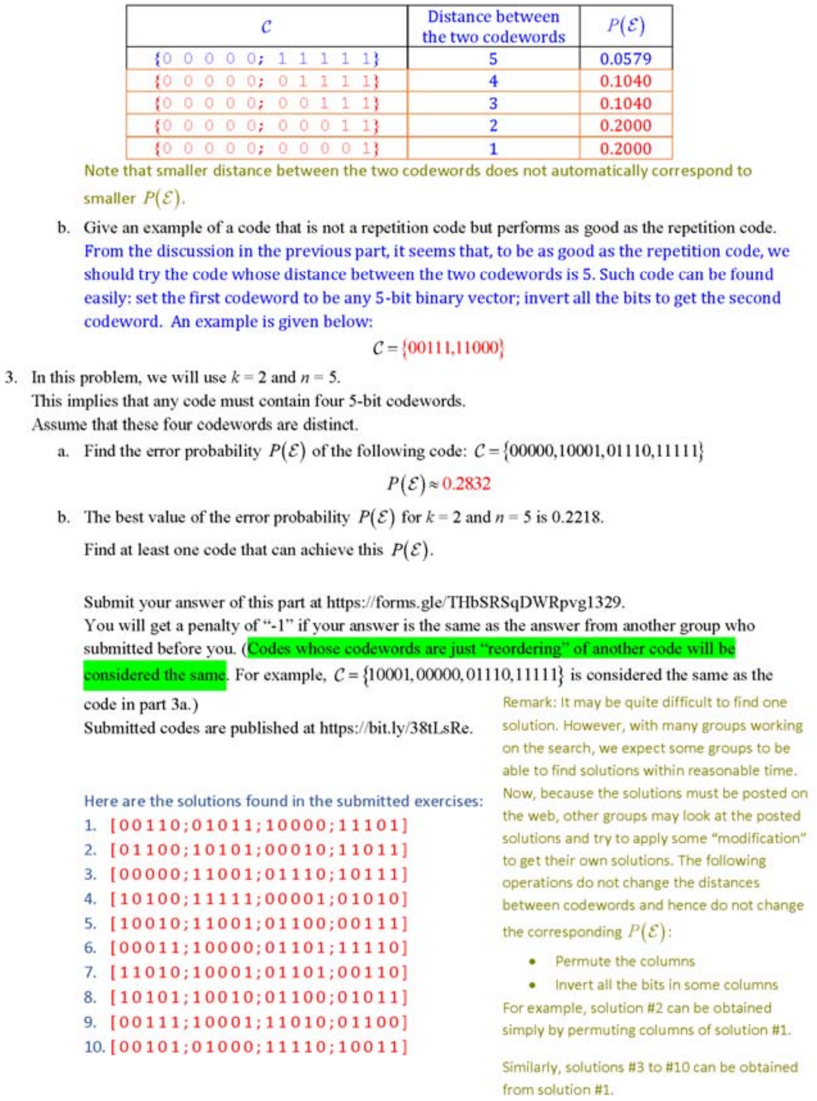
   In class, we have shown examples of how to use the function `PE_minDist` to find $P(\mathcal{E})$ for repetition code with $n = 5$. See, for example, the script `PE_minDist_demo1`. Here, the difference is simply that the crossover probability is changed from 1/100 to 0.2. So, by changing the value of p in the provided example to 0.2, we can find the new $P(\mathcal{E})$.

   $$P(\mathcal{E}) \approx 0.0579$$

2. Here, as in Problem 1, we will use $k = 1$ and $n = 5$.
   This implies that any code must contain two 5-bit codewords.
   Assume that these two codewords are distinct.

   a. Give an example of a code that performs worse (gives larger $P(\mathcal{E})$) than repetition code.

      Method 1: We can use trial and error.
      Method 2: Alternatively, for BSC with $p < 0.5$, the transmitted bits are more likely to stay the same than to switch into their complements. This implies that the received vectors that have less bit errors are more likely to occur than ones with many bit errors. Therefore, code whose codewords are far away from each other seems to give small $P(\mathcal{E})$. When $n = 5$, the maximum "distance" between the codewords is 5. So, the repetition code in problem 1 already achieves this maximum. To find a code that performs worse, we try to make the distance between the two codewords smaller. This implies making some bits (in the corresponding positions) of the two codewords the same.
      Some examples are provided below:



$\mathcal{C}$	Distance between the two codewords	$P(\mathcal{E})$
{0 0 0 0 0; 1 1 1 1 1}	5	0.0579
{0 0 0 0 0; 0 1 1 1 1}	4	0.1040
{0 0 0 0 0; 0 0 1 1 1}	3	0.1040
{0 0 0 0 0; 0 0 0 1 1}	2	0.2000
{0 0 0 0 0; 0 0 0 0 1}	1	0.2000

Note that smaller distance between the two codewords does not automatically correspond to smaller $P(\mathcal{E})$.

   b. Give an example of a code that is not a repetition code but performs as good as the repetition code.
      From the discussion in the previous part, it seems that, to be as good as the repetition code, we should try the code whose distance between the two codewords is 5. Such code can be found easily: set the first codeword to be any 5-bit binary vector; invert all the bits to get the second codeword. An example is given below:

      $$\mathcal{C} = \{00111, 11000\}$$

3. In this problem, we will use $k = 2$ and $n = 5$.
   This implies that any code must contain four 5-bit codewords.
   Assume that these four codewords are distinct.

   a. Find the error probability $P(\mathcal{E})$ of the following code: $\mathcal{C} = \{00000, 10001, 01110, 11111\}$

      $$P(\mathcal{E}) \approx 0.2832$$

   b. The best value of the error probability $P(\mathcal{E})$ for $k = 2$ and $n = 5$ is 0.2218.

      Find at least one code that can achieve this $P(\mathcal{E})$.

      Submit your answer of this part at https://forms.gle/THbSRSqDWRpvg1329.
      You will get a penalty of "-1" if your answer is the same as the answer from another group who submitted before you. (Codes whose codewords are just "reordering" of another code will be considered the same. For example, $\mathcal{C} = \{10001, 00000, 01110, 11111\}$ is considered the same as the code in part 3a.)
      Submitted codes are published at https://bit.ly/38tLsRe.

      Here are the solutions found in the submitted exercises:
      1. [00110;01011;10000;11101]
      2. [01100;10101;00010;11011]
      3. [00000;11001;01110;10111]
      4. [10100;11111;00001;01010]
      5. [10010;11001;01100;00111]
      6. [00011;10000;01101;11110]
      7. [11010;10001;01101;00110]
      8. [10101;10010;01100;01011]
      9. [00111;10001;11010;01100]
      10. [00101;01000;11110;10011]

Remark: It may be quite difficult to find one solution. However, with many groups working on the search, we expect some groups to be able to find solutions within reasonable time. Now, because the solutions must be posted on the web, other groups may look at the posted solutions and try to apply some "modification" to get their own solutions. The following operations do not change the distances between codewords and hence do not change the corresponding $P(\mathcal{E})$:

- Permute the columns
- Invert all the bits in some columns

For example, solution #2 can be obtained simply by permuting columns of solution #1.

Similarly, solutions #3 to #10 can be obtained from solution #1.

MATLAB

```
function PE = PE_minDist(C,p)
% Function PE_minDist_3 computes the error probability P(E) when code C
% is used for transmission over BSC with crossover probability p.
% Code C is defined by putting all its (valid) codewords as its rows.
M = size(C,1);
k = log2(M);
n = size(C,2);

% Generate all possible received vectors
Y = dec2bin(0:2^n-1)-'0';

% Normally, we need to construct an extended Q matrix. However, because
% each conditional probability in there is a decreasing function of the
% Hamming distance, we can work with the distances instead of the
% conditional probability. In particular, instead of selecting the max in
% each column of the Q matrix, we consider min distance in each column.
dmin = zeros(1,2^n);
for j = 1:(2^n)
    % for each received vector y,
    y = Y(j,:);
    % find the minimum distance (the distance from y to the closest
    % codeword)
    d = sum(mod(bsxfun(@plus,y,C),2),2);
    dmin(j) = min(d);
end

% From the distances, calculate the conditional probabilities.
% Note that we compute only the values that are to be selected (instead of
% calculating the whole Q first).
n1 = dmin; n0 = n-dmin;
Qmax = (p.^n1).*((1-p).^n0);
% Scale the conditional probabilities by the input probabilities and add
% the values. Note that we assume equally likely input.
PC = sum((1/M)*Qmax);
PE = 1-PC;
end
```

MATLAB

```
close all; clear all;

% ECS315 2019 Example 6.58
% ECS452 2019 Example 3.65
C = [0 0 0 0 0; 1 1 1 1 1]; % repetition code

p = (1/100);
PE_minDist(C,p)
```

Code C is defined by putting all its (valid) codewords as its rows. For repetition code, there are two codewords: 00..0 and 11..1.

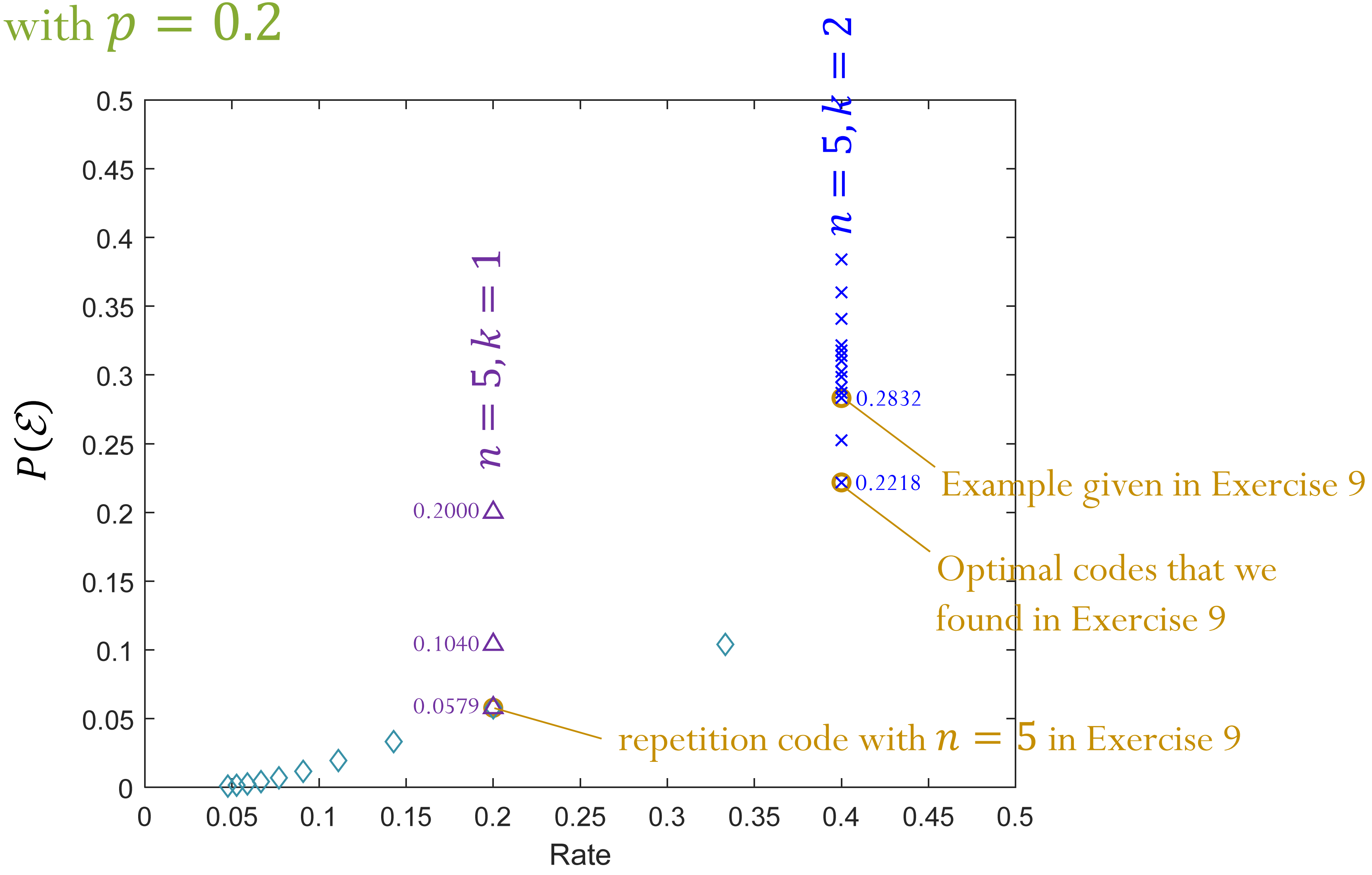
Crossover probability of the binary symmetric channel.

```
>> PE_minDist_demo1

ans =
   9.8506e-06
```

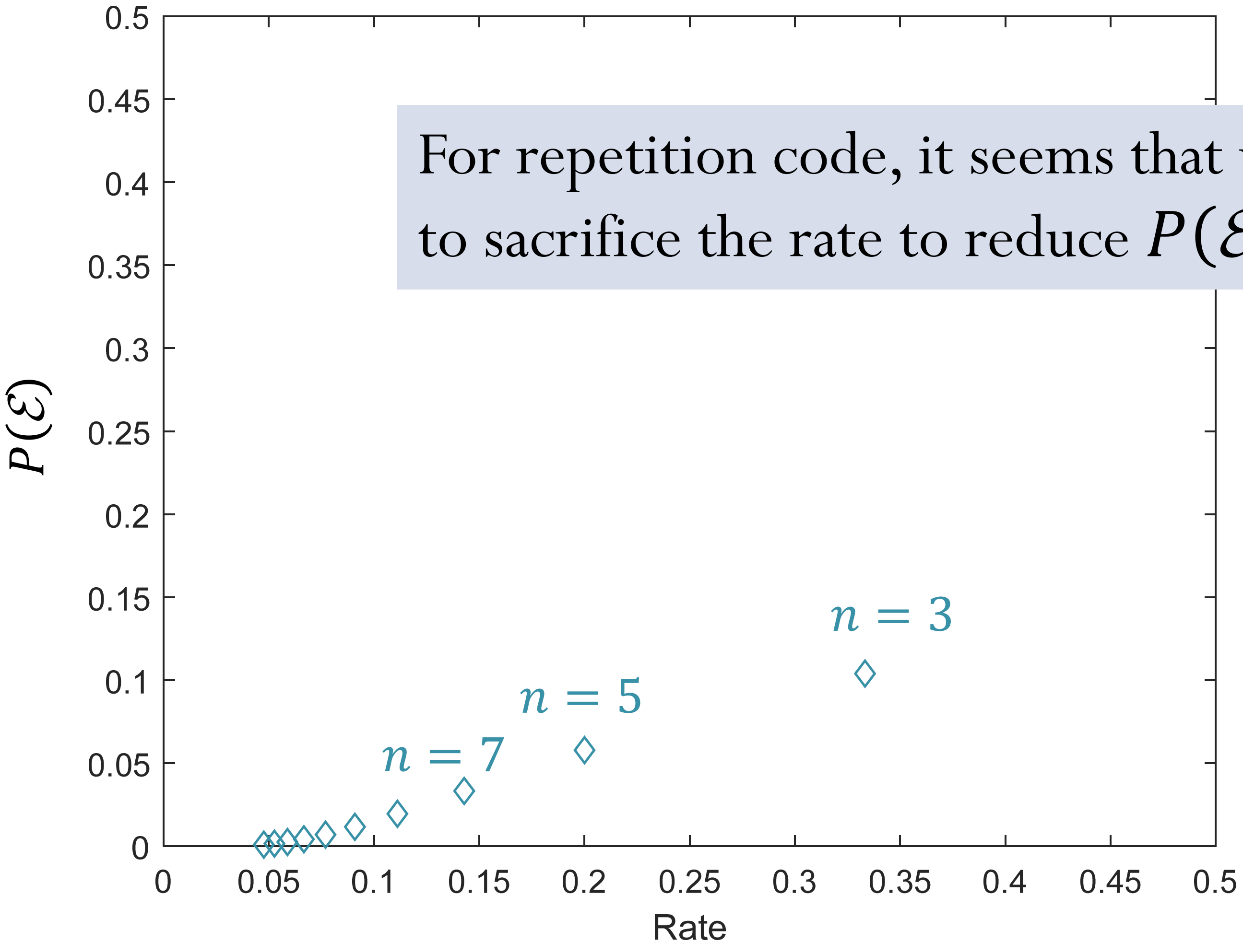
Achievable Performance

BSC with $p = 0.2$



Achievable Performance

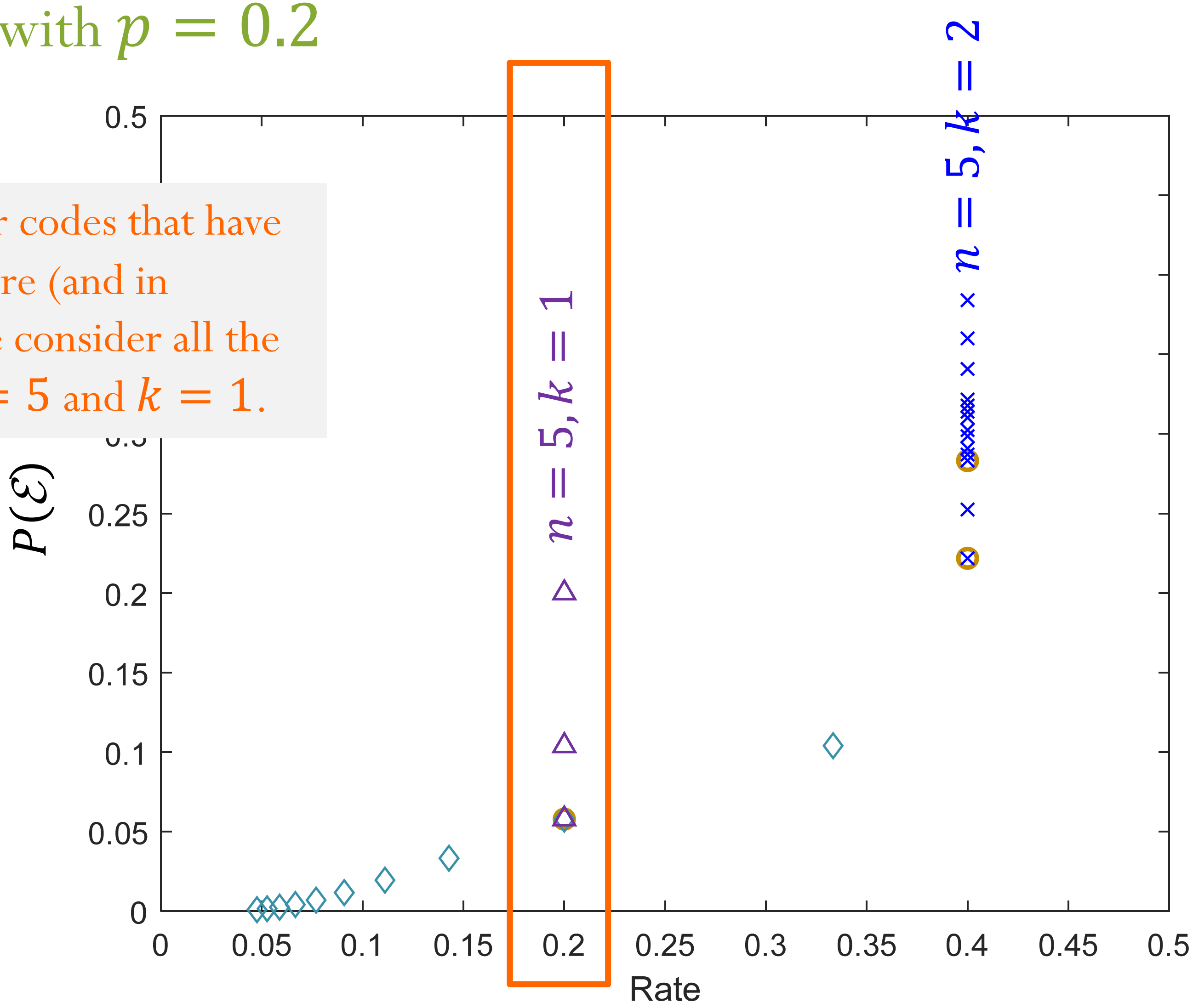
BSC with $p = 0.2$ Repetition Code ($k = 1$)



For repetition code, it seems that we have to sacrifice the rate to reduce $P(\mathcal{E})$

Achievable Performance

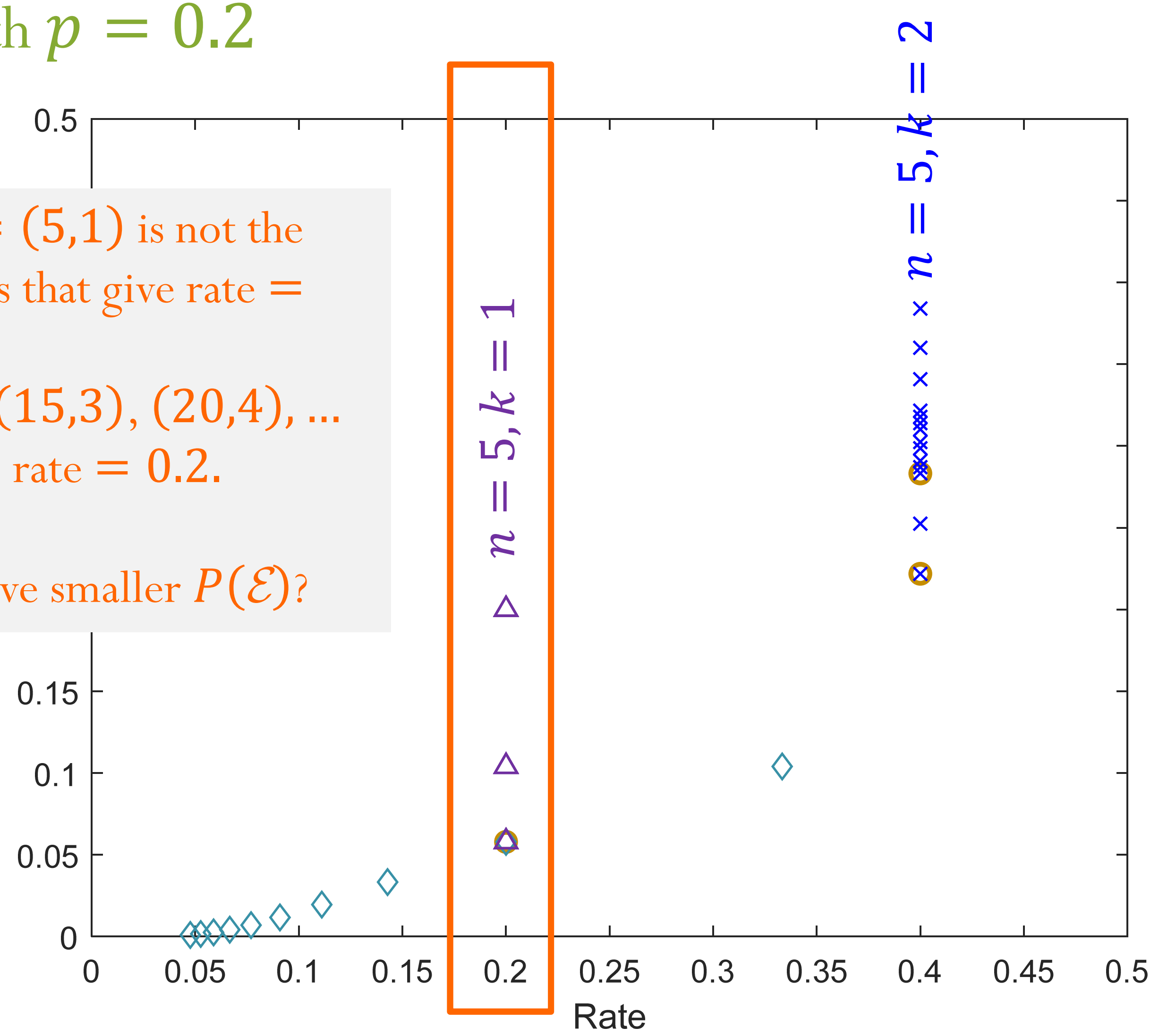
BSC with $p = 0.2$



There are other codes that have rate $= 0.2$. Here (and in Exercise 9), we consider all the codes with $n = 5$ and $k = 1$.

Achievable Performance

BSC with $p = 0.2$



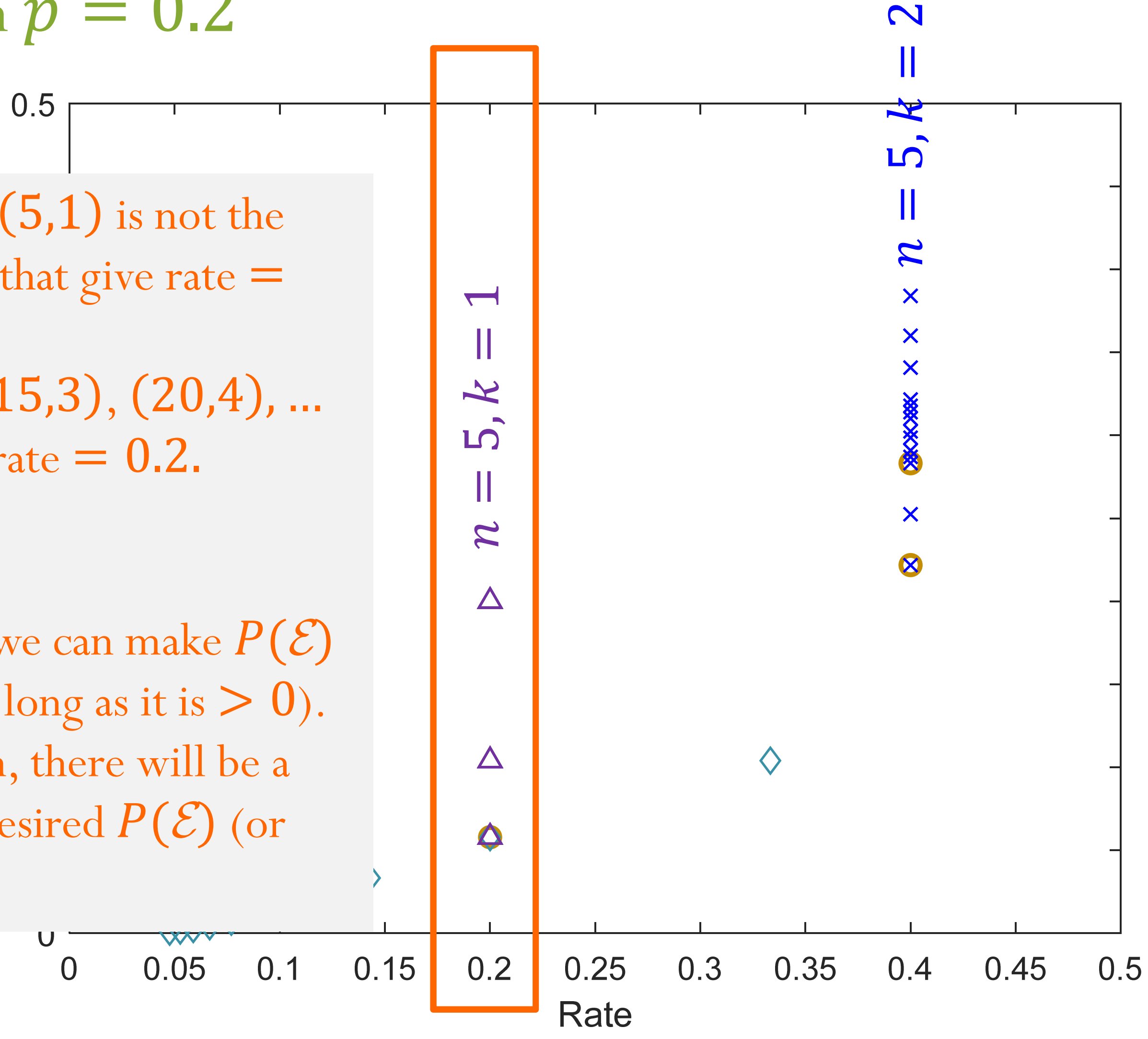
Note that $(n, k) = (5,1)$ is not the only family of codes that give rate $= 0.2$.

$(n, k) = (10,2), (15,3), (20,4), \ldots$ also corresponds to rate $= 0.2$.

Will these codes have smaller $P(\mathcal{E})$?

Achievable Performance

BSC with $p = 0.2$



Note that $(n, k) = (5,1)$ is not the only family of codes that give rate $= 0.2$.
$(n, k) = (10,2), (15,3), (20,4), \ldots$ also corresponds to rate $= 0.2$.

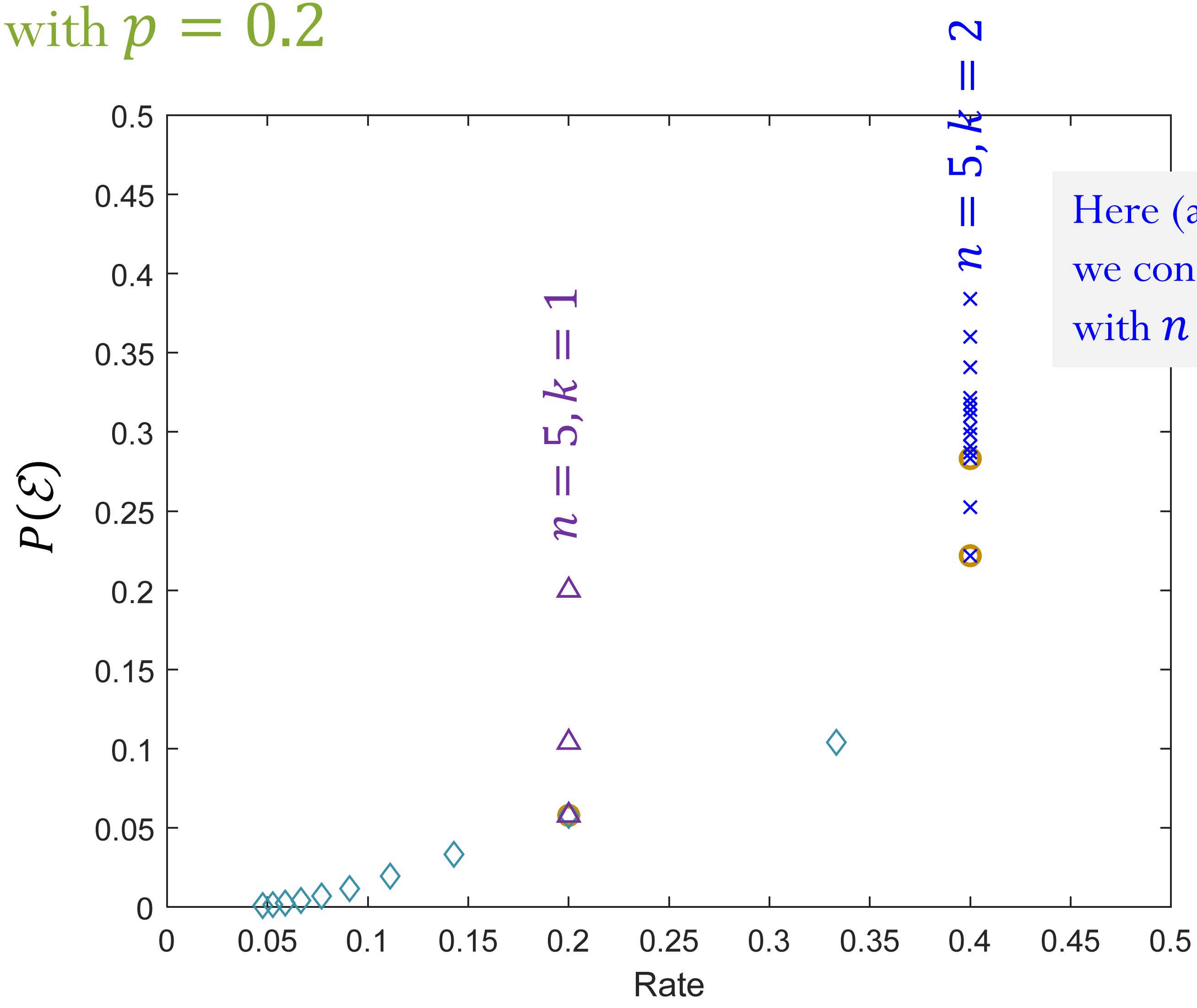
At rate $= 0.2$,
Shannon found that we can make $P(\mathcal{E})$ as small we want (as long as it is > 0).
With n large enough, there will be a code that gives the desired $P(\mathcal{E})$ (or smaller).

Reliable communication

- **Reliable communication** (at a particular rate) means arbitrarily small error probability can be achieved (at that rate).
- In our example, Shannon showed that reliable communication is achievable at rate $= 0.2$.
- Turn out that reliable communication is not achievable at rate $= 0.4$.

Achievable Performance

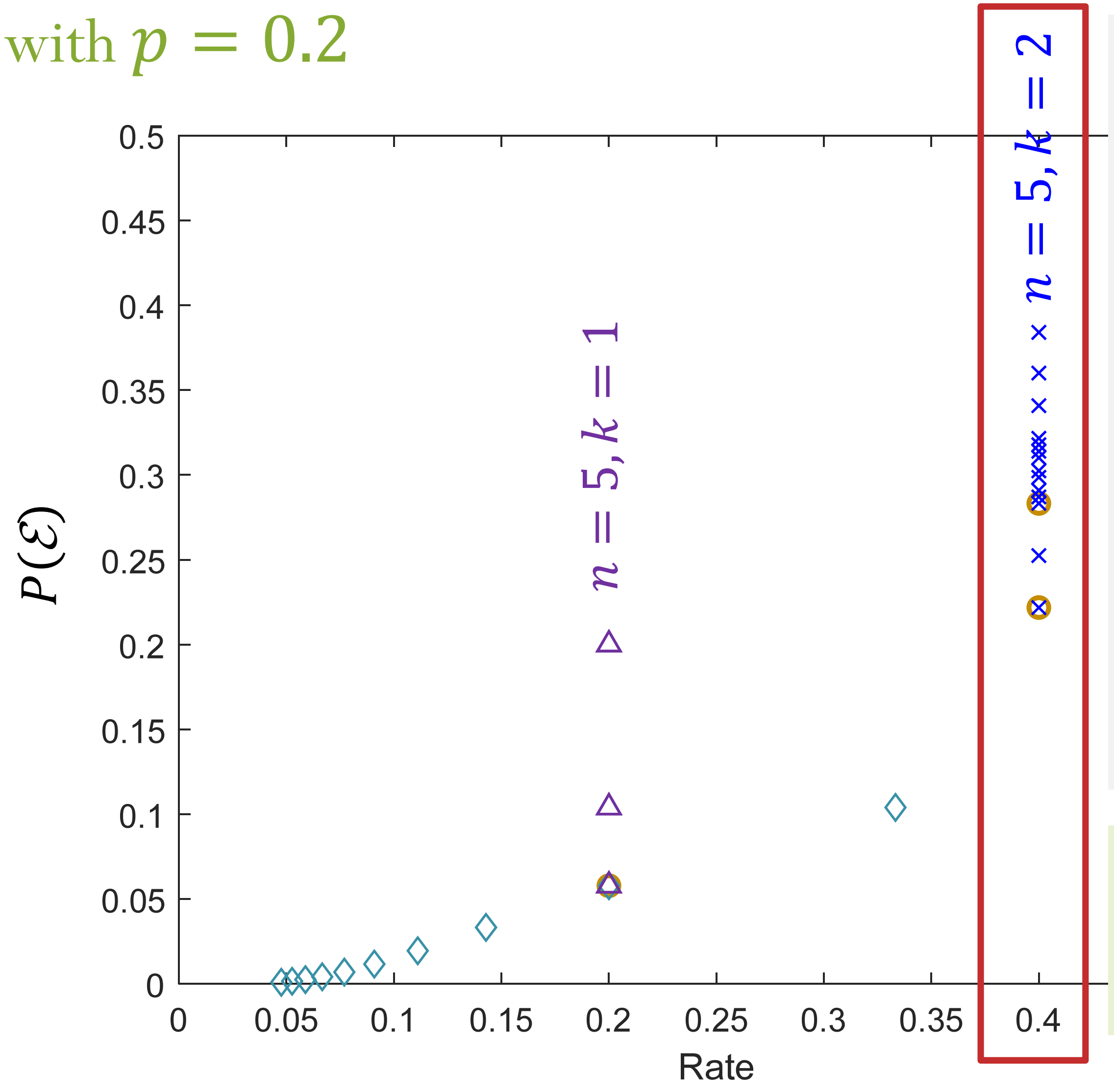
BSC with $p = 0.2$



Here (and in Exercise 9), we consider all the codes with $n = 5$ and $k = 2$.

Achievable Performance

BSC with $p = 0.2$



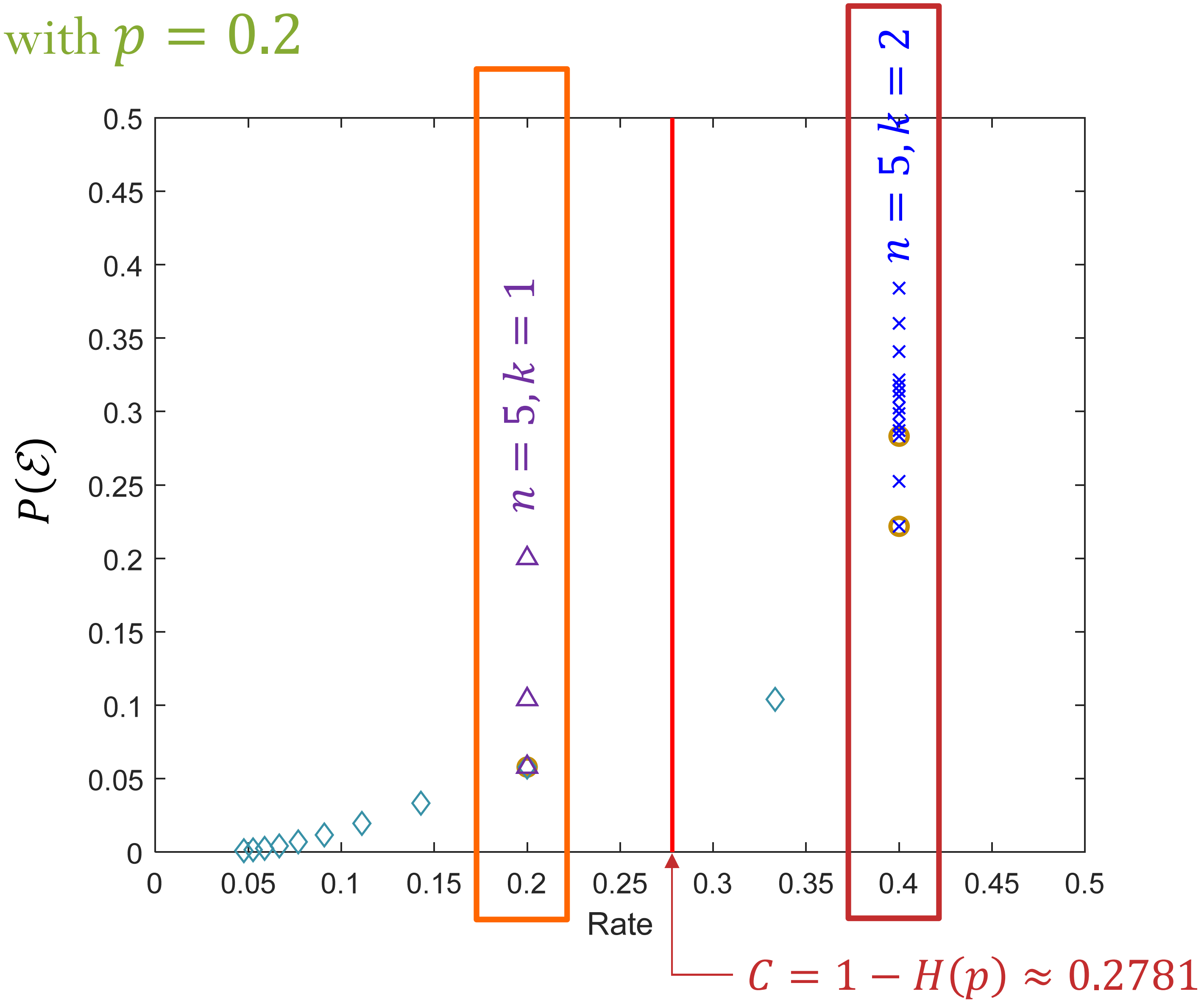
Note that $(n, k) = (5,2)$ is not the only family of codes that give rate $= 0.4$. $(n, k) = (10,4), (15,6), (20,8), \ldots$ also corresponds to rate $= 0.4$.

At rate $= 0.4$, Shannon found that we **cannot** make $P(\mathcal{E})$ as small as we want; even when we use large n.

So, how can we determine which rate can have arbitrarily small $P(\mathcal{E})$?

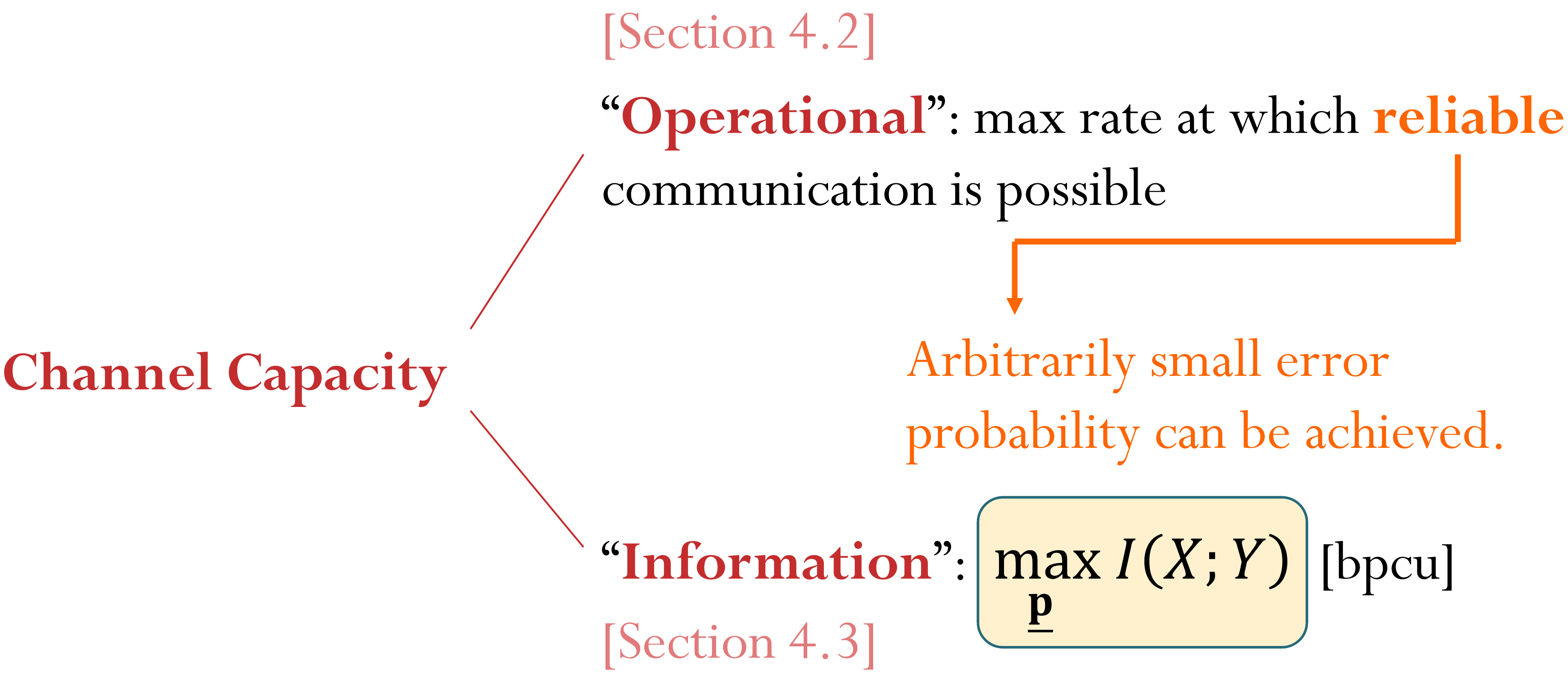
Achievable Performance

BSC with $p = 0.2$



$C = 1 - H(p) \approx 0.2781$

Channel Capacity



[Section 4.2]

"**Operational**": max rate at which **reliable** communication is possible

Arbitrarily small error probability can be achieved.

Channel Capacity

"**Information**": $\boxed{\max_{\underline{\mathbf{p}}} I(X;Y)}$ [bpcu]

[Section 4.3]

Shannon [1948] showed that these two quantities are actually the same.