Telecom ParisTech — ACCQ204, Coding Theory
Teacher: Aslan Tchamkerten — December 2017

ASSIGNMENT 4: SOLUTION

Exercise 1. The goal of this exercise is to derive a general formula for decoding order of rows in successive cancellation decoding.

1. $N = 4$. Consider Fig. 1:

   i. What is the bit decoding order for successive cancellation for Fig. 1.a? Call this ordering vector "O".

   ii. Find the matrix B_4 such that $[1 \quad 2 \quad 3 \quad 4] \times B_4 = O$.

   iii. Argue that in Fig. 1.b, the bit decoding order is $[1 \quad 2 \quad 3 \quad 4]$.

2. Do part 1. for $N = 8$.

3. Show that for $N = 2^n$,

$$B_N = R_N \times \begin{bmatrix} B_{N/2} & 0 \\ 0 & B_{N/2} \end{bmatrix}$$

   where R_N is the permutation matrix given by

$$[1 \quad 2 \quad \cdots \quad N] \times R_N = [1 \quad 3 \quad 5 \cdots \quad N-1 \quad 2 \quad 4 \quad 6 \quad \cdots \quad N].$$

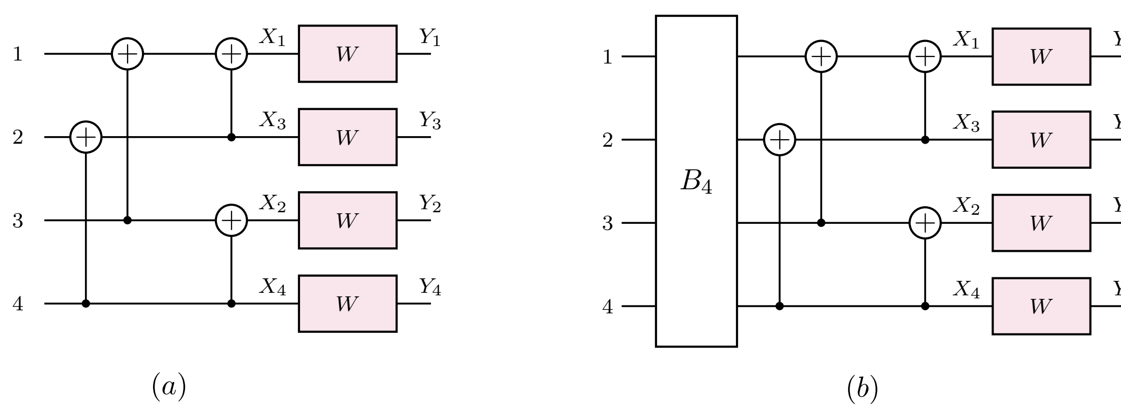
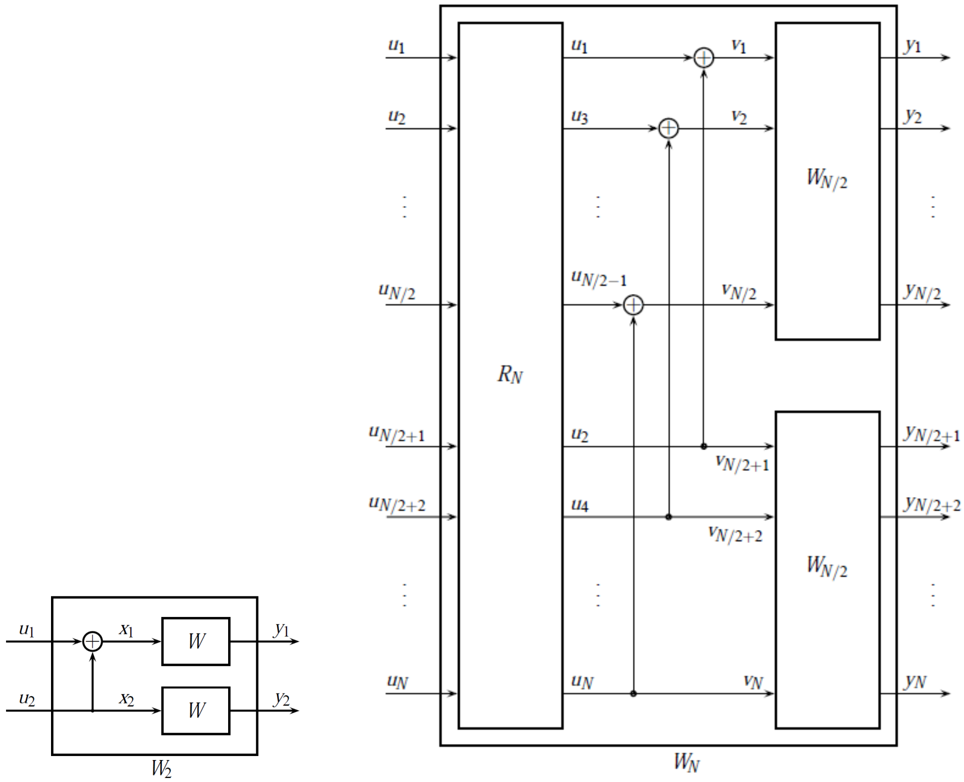


Figure 1: N=4

Solution: 1. i. $O = \begin{bmatrix}1 & 3 & 2 & 4\end{bmatrix}$.

ii. $B_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$.

iii. This can be deduced since due to the definition of B_4, the lines 1 to 4 in in Fig. 1.a are correspondent to lines 1, 3, 2, and 4 in Fig. 1.b, respectiveley.



(a) (b)

Figure 2: (a) First level of recursion, and (b) General form of recursion

2. i. $O = \begin{bmatrix} 1 & 5 & 3 & 7 & 2 & 6 & 4 & 8 \end{bmatrix}$.

   ii. $B_8 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$.

   iii. Same argument as in Part 1.iii.

3. We show it by induction on n, where $N = 2^n$. For $n = 1$ it is trivial. Suppose that this holds for $n = k - 1$, we show this holds for $n = k$ and $N = 2^n$. We need to show that the order of

decoding is $O = \begin{bmatrix} 1 & 2 & \cdots & N \end{bmatrix} \times B_N$. Note that

$$
\begin{aligned}
O &= \begin{bmatrix} 1 & 2 & \cdots & N \end{bmatrix} \times B_N \\
&= \begin{bmatrix} 1 & 2 & \cdots & N \end{bmatrix} \times R_N \times \begin{bmatrix} B_{N/2} & 0 \\ 0 & B_{N/2} \end{bmatrix} \\
&= \begin{bmatrix} 1 & 3 & \cdots & N-1 & 2 & 4 & \cdots & N \end{bmatrix} \times \begin{bmatrix} B_{N/2} & 0 \\ 0 & B_{N/2} \end{bmatrix} \\
&= \begin{bmatrix} \begin{bmatrix} 1 & 3 & \cdots & N-1 \end{bmatrix} \times B_{N/2} & & \begin{bmatrix} 2 & 4 & \cdots & N \end{bmatrix} \times B_{N/2} \end{bmatrix}.
\end{aligned}
$$

This together with the assumptuion of the induction that $\begin{bmatrix} 1 & 2 & \cdots & N/2 \end{bmatrix} \times B_{N/2}$ is the order of decoding for polar coding of size $N/2$, completes the proof.

□

Exercise 2. For systematic construction of the polar coding we do as following:

We combine copies of a given B-DMC W in a recursive manner to produce a vector channel $W_N : \mathcal{X}^N \to \mathcal{Y}^N$, where N can be any power of two, $N = 2^n$, $n \geq 0$. The recursion begins at the 0-th level ($n = 0$) with only one copy of W and we set $W_1 \triangleq W$. The first level ($n = 1$) of the recursion combines two independent copies of W_1 as shown in Fig. 2(a) and obtains the channel $W_2 : \mathcal{X}^2 \to \mathcal{Y}^2$ with the transition probabilities

$$W_2(y_1, y_2|u_1, u_2) = W(y_1|u_1 \oplus u_2)W(y_2|u_2).$$

The general form of the recursion is shown in Fig. 2(b) where two independent copies of $W_{N/2}$ are combined to produce the channel W_N.

Show that for any binary discrete memoryless channel W in Fig. 2(a)

1.

$$W_2^{(1)}(y_1, y_2|u_1) = \sum_{u_2} \frac{1}{2} W(y_1|u_1 \oplus u_2)W(y_2|u_2)$$

and

$$W_2^{(2)}(y_1, y_2, u_1|u_2) = \frac{1}{2} W(y_1|u_1 \oplus u_2)W(y_2|u_2)$$

2.

$$
\begin{aligned}
&W_{2N}^{(2i-1)}(y_1^{2N}, u_1^{2i-2}|u_{2i-1}) = \\
&\qquad \sum_{u_{2i}} \frac{1}{2} W_N^{(i)}(y_1^N, u_1 \oplus u_2, \cdots, u_{2i-3} \oplus u_{2i-2}|u_{2i-1} \oplus u_{2i}) \cdot W_N^{(i)}(y_{N+1}^{2N}, u_2, u_4, \cdots, u_{2i-2}|u_{2i})
\end{aligned}
$$

and

$$
\begin{aligned}
&W_{2N}^{(2i)}(y_1^{2N}, u_1^{2i-1}|u_{2i}) = \\
&\qquad \frac{1}{2} W_N^{(i)}(y_1^N, u_1 \oplus u_2, \cdots, u_{2i-3} \oplus u_{2i-2}|u_{2i-1} \oplus u_{2i}) \cdot W_N^{(i)}(y_{N+1}^{2N}, u_2, u_4, \cdots, u_{2i-2}|u_{2i})
\end{aligned}
$$

This is the method to recursively compute the probabilities of synthetic channels which will be used in the next exercise for decoding.

Solution: 1. Note that by definition $W_2(y_1, y_2|u_1, u_2) = p(y_1, y_2|u_1)$.

$$\begin{aligned}
W_2^{(1)}(y_1, y_2|u_1) &= \sum_{u_2} W_2^{(1)}(y_1, y_2, u_2|u_1) \\
&= \sum_{u_2} W_2(y_1, y_2|u_2, u_1)p(u_2|u_1) \\
&\overset{(a)}{=} \sum_{u_2} \frac{1}{2} W_2(y_1, y_2|u_2, u_1) \\
&\overset{(b)}{=} \sum_{u_2} \frac{1}{2} W_2(y_1, y_2|u_1, \oplus u_2, u_2) \\
&\overset{(c)}{=} \sum_{u_2} \frac{1}{2} W_2(y_1, y_2|x_1, x_2) \\
&= \sum_{u_2} \frac{1}{2} W(y_1|x_1)W(y_2|x_2) \\
&= \sum_{u_2} \frac{1}{2} W(y_1|u_1 \oplus u_2)W(y_2|u_2)
\end{aligned}$$

where (a) is true since u_1 and u_2 are chosen independently and uniformly, (b) is true since (u_1, u_2) and $(u_1, \oplus u_2, u_2)$ are equivalent, and (c) is true since $x_1 = u_1, \oplus u_2$ and $x_2 = u_2$ by Fig. 2.a.

Similarly we have

$$\begin{aligned}
W_2^{(2)}(y_1, y_2, u_1|u_2) &= W_2(y_1, y_2|u_1, u_2)p(u_1|u_2) \\
&= \frac{1}{2} W(y_1|u_1 \oplus u_2)W(y_2|u_2).
\end{aligned}$$

2. Similar to the Part 1. we have

$$\begin{aligned}
&W_{2N}^{(2i-1)}(y_1^{2N}, u_1^{2i-2}|u_{2i-1}) \\
&= \sum_{u_{2i}^{2N}} \frac{1}{2^{2N-1}} W_{2N}(y_1^{2N}|u_1^{2N}) \\
&= \sum_{u_{2i}^{2N}} \frac{1}{2^{2N-1}} W_N(y_1^N|u_1 \oplus u_2, u_3 \oplus u_4, \cdots, u_{N-1} \oplus u_N)W_N(y_{N+1}^{2N}|u_2, u_4, \cdots, u_N) \\
&= \sum_{u_{2i}} \frac{1}{2} \cdot \sum_{u_{2i}, u_{2i+2}, \cdots, u_{2N}} \frac{1}{2^{N-1}} W_N(y_{N+1}^{2N}|u_2, u_4, \cdots, u_N) \\
&\qquad \cdot \sum_{u_{2i+1}, u_{2i+3}, \cdots, u_{2N-1}} \frac{1}{2^{N-1}} W_N(y_1^N|u_1 \oplus u_2, u_3 \oplus u_4, \cdots, u_{N-1} \oplus u_N) \\
&= \sum_{u_{2i}} \frac{1}{2} \cdot W_N^{(i)}(y_{N+1}^{2N}, u_2, u_4, \cdots, u_{2i-2}|u_{2i}) \cdot W_N^{(i)}(y_1^N, u_1 \oplus u_2, \cdots, u_{2i-3} \oplus u_{2i-2}|u_{2i-1} \oplus u_{2i}).
\end{aligned}$$

Similarly we have

$$W_{2N}^{(2i)}(y_1^{2N}, u_1^{2i-1}|u_{2i}) =$$
$$\frac{1}{2}W_N^{(i)}(y_1^N, u_1 \oplus u_2, \cdots, u_{2i-3} \oplus u_{2i-2}|u_{2i-1} \oplus u_{2i}) \cdot W_N^{(i)}(y_{N+1}^{2N}, u_2, u_4, \cdots, u_{2i-2}|u_{2i})$$

□

Exercise 3 (Successive cancellation)**.** Consider a binary symmetric channel with transition probability 0.08 and the associated polar code for $N = 8$. As in Exercise 3 we consider the systematic construction of polar codes, so that the successive decoder decodes the data bit in the natural order $U_1, U_2, \ldots$. The frozen bits correspond to the rows $\{1, 2, 3, 5\}$ and their values is set to be zero. The information bits correspond to the rows $\{4, 6, 7, 8\}$. The messages and their corresponding data bit representation is given by:

network	0000
channel coding	0001
the	0010
we	0011
shannon	0100
polar coding	0101
learn	0110
introduced	0111
information theory	1000
strong	1001
a powerful tool	1010
is	1011
interesting	1100
typicality	1101
great	1110
know	1111

So, to send for example "polar coding", first we find the associated code which is 0101, then we assign it to the information bits. Since frozen bits have been chosen as 0000, the input data of the polar code is $(U_1, U_2, \cdots, U_8) = 00010010$.

We have received the following outputs from the channel.

0. 10110011 10100100 10000110
1. 00001101 00101001 10101110
2. 00001000 10001010 10000101 01100010
3. 11010101 10011101 11100101 01001010
4. 11011100 11001011 11111000 10111010

Using the successive cancellation decoder of the previous exercise decode sentence $i \mod 5$ where $i \in \{1, 2, \ldots, 26\}$ denotes the position of the first letter of your first name.

You are allowed to use any software you want.

Solution:

0. Polar coding is great.
1. We know coding theory.
2. Network coding theory is interesting.
3. Strong typicality is a powerful tool.
4. Hamming introduced the coding theory.

$\square$