Information Theory

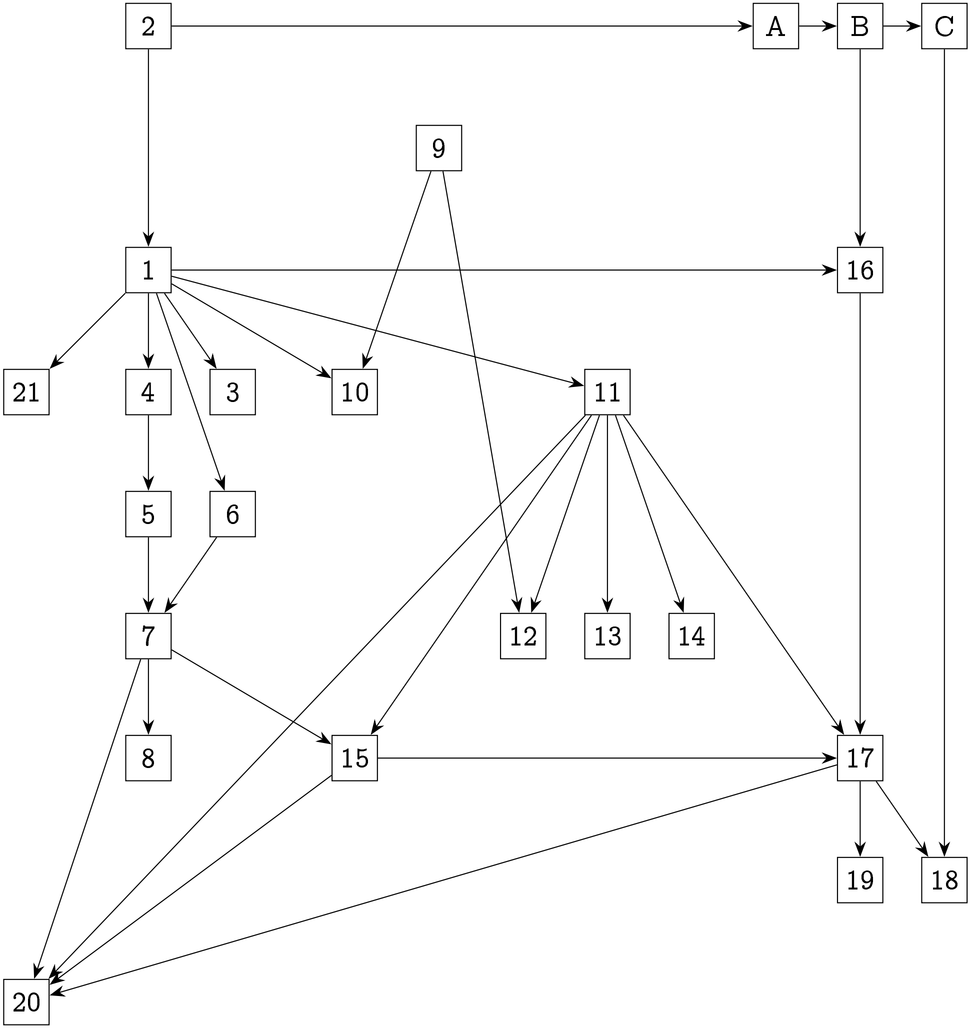
Lecture Notes

Stefan M. Moser

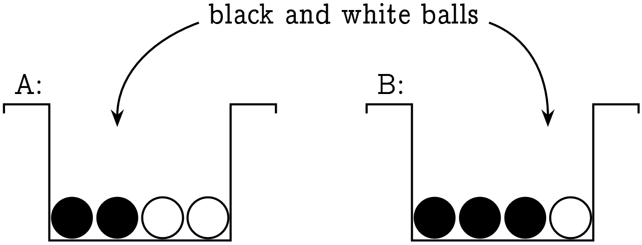
Signal and Information Processing Lab
ETH Zurich
Zurich, Switzerland

Institute of Communications Engineering
National Yang Ming Chiao Tung University (NYCU)
Hsinchu, Taiwan

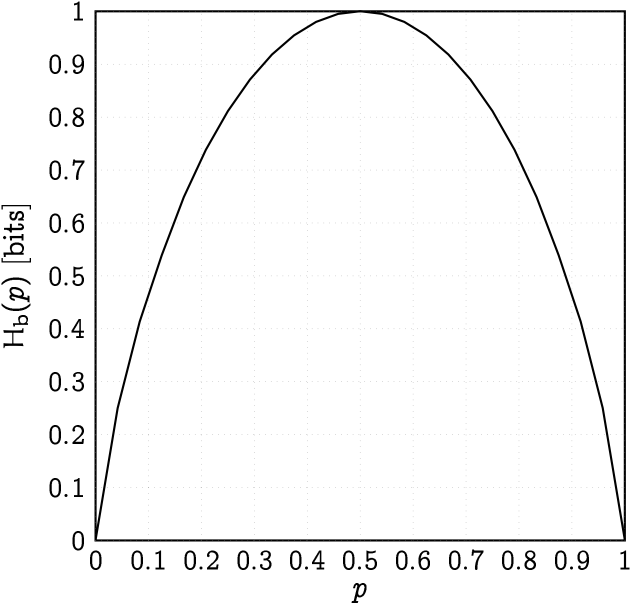
6^{th} Edition — 2018.
Version 6.16.
Compiled on 10 July 2024.
For the latest version see https://moser-isi.ethz.ch/scripts.html



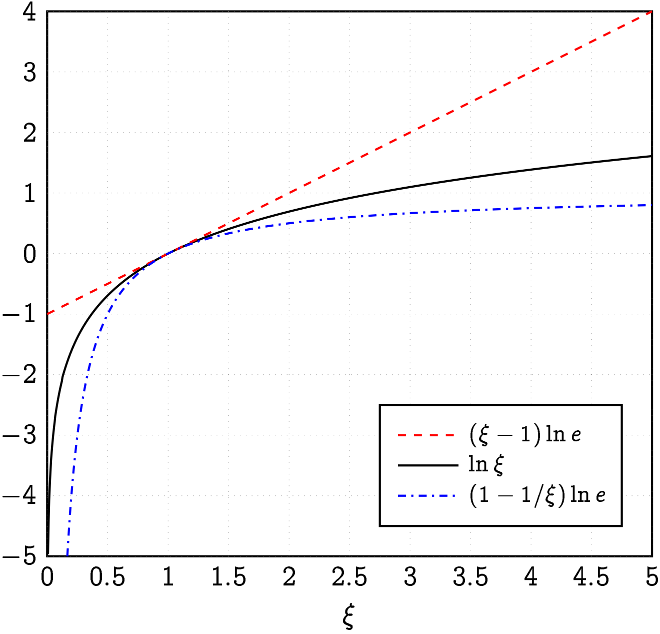
Chapter dependency chart. An arrow has the meaning of “is required for”.



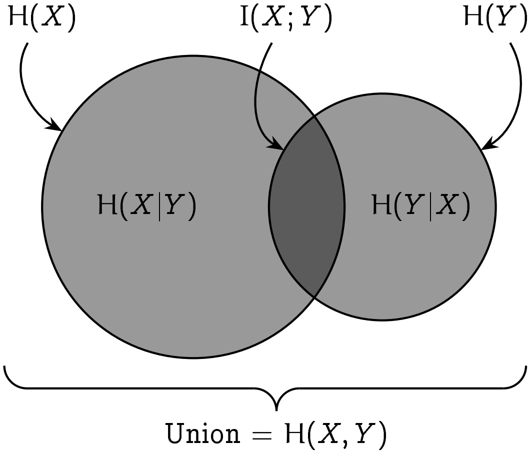
Stefan M. Moser, *Information Theory*, Version 6.16.



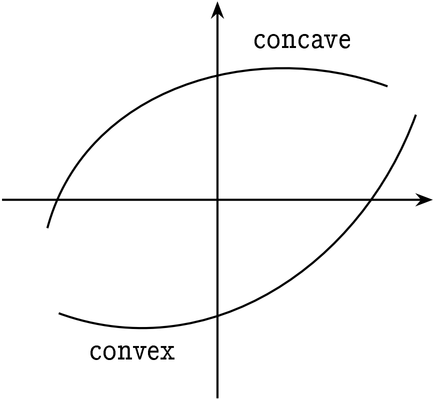
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1
$H_b(p)$ [bits]
p

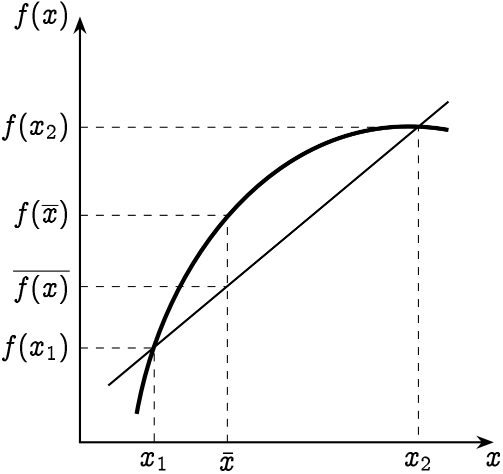


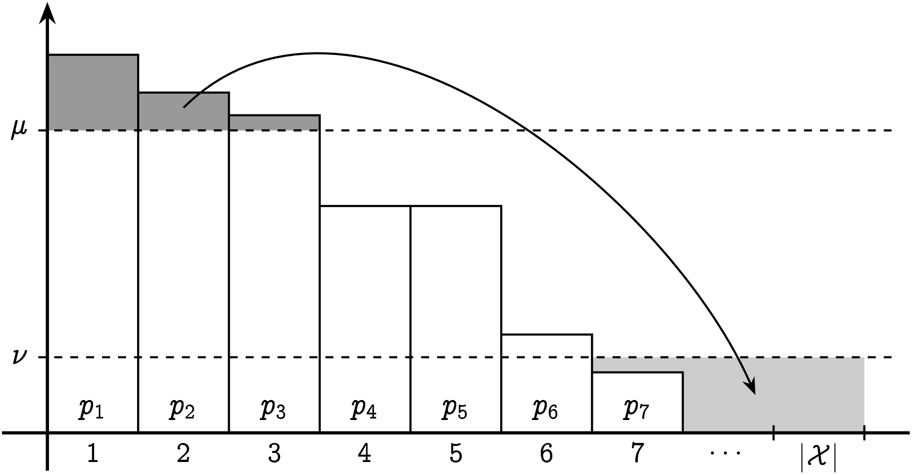
4
3
2
1
0
−1
−2
−3
−4
−5
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
5
ξ
(ξ − 1) ln e
ln ξ
(1 − 1/ξ) ln e



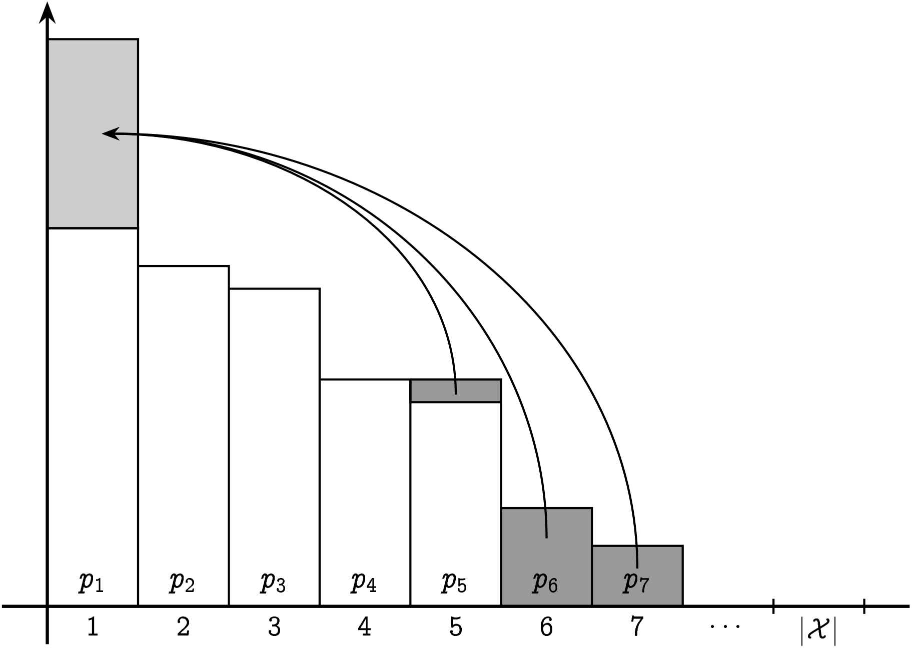
H(X)
I(X; Y)
H(Y)
H(X|Y)
H(Y|X)
Union = H(X, Y)


concave
convex


$f(x)$
$f(x_2)$
$f(\overline{x})$
$\overline{f(x)}$
$f(x_1)$
x_1
$\bar{x}$
x_2
x

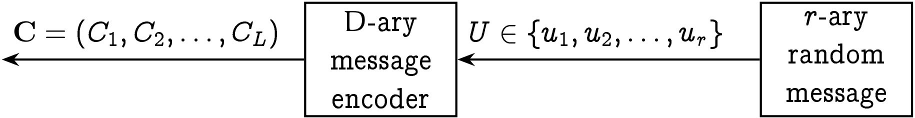


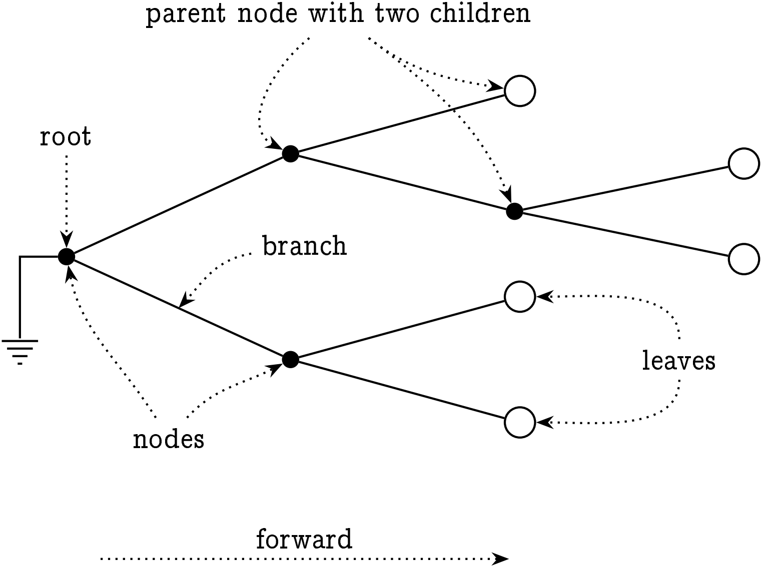
μ
ν
p1
p2
p3
p4
p5
p6
p7
1
2
3
4
5
6
7
· · ·
|𝒳|

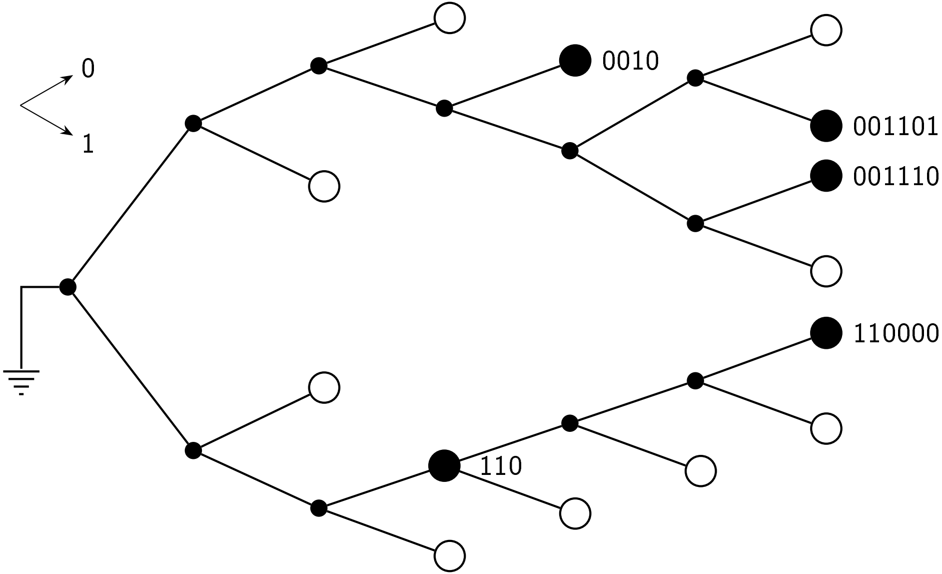


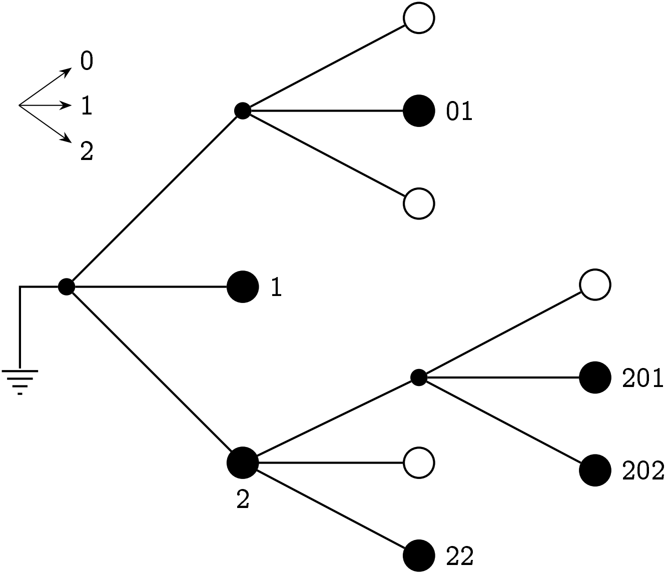
p_1
p_2
p_3
p_4
p_5
p_6
p_7
1
2
3
4
5
6
7
$\cdots$
$|\mathcal{X}|$

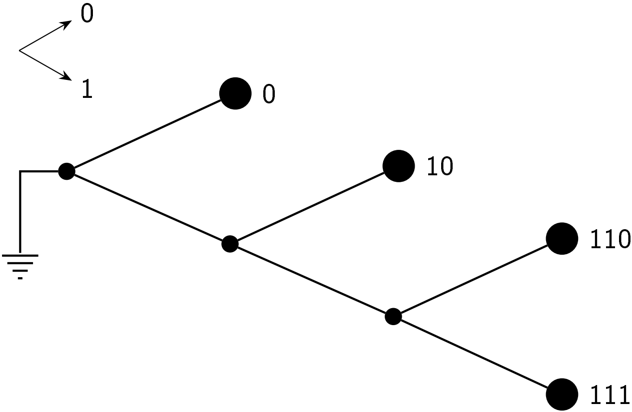
Friend		Alice	Bob	Carol
Probability		$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$
Phone numbers	(i)	0011	0011	1100
	(ii)	001101	001110	110000
	(iii)	0	1	10
	(iv)	00	11	10
	(v)	0	11	10
	(vi)	10	0	11

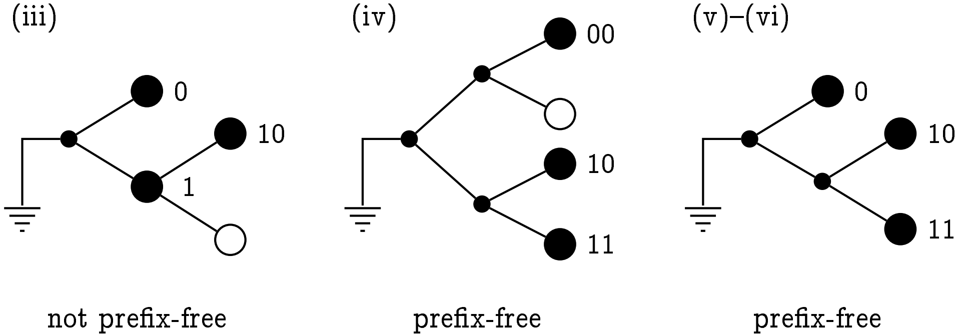

$\mathbf{C} = (C_1, C_2, \ldots, C_L)$
D-ary message encoder
$U \in \{u_1, u_2, \ldots, u_r\}$
r-ary random message

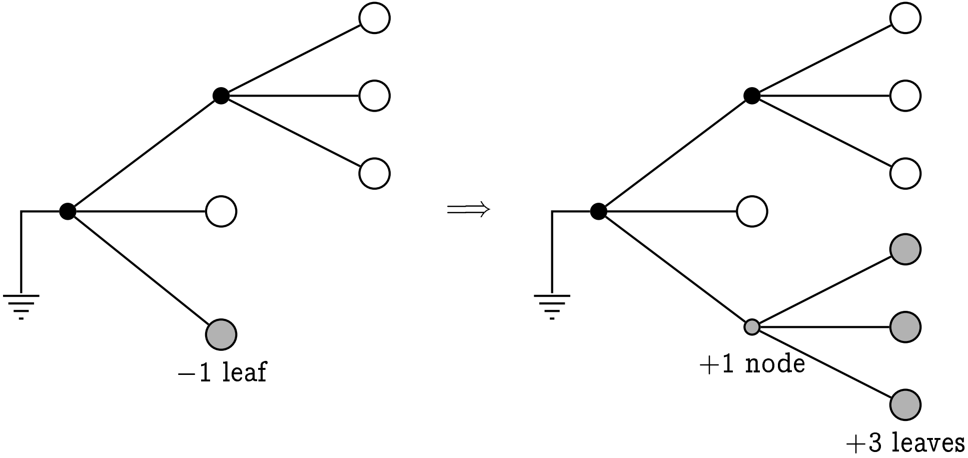

parent node with two children
root
branch
leaves
nodes
forward


0
1
0010
001101
001110
110000
110

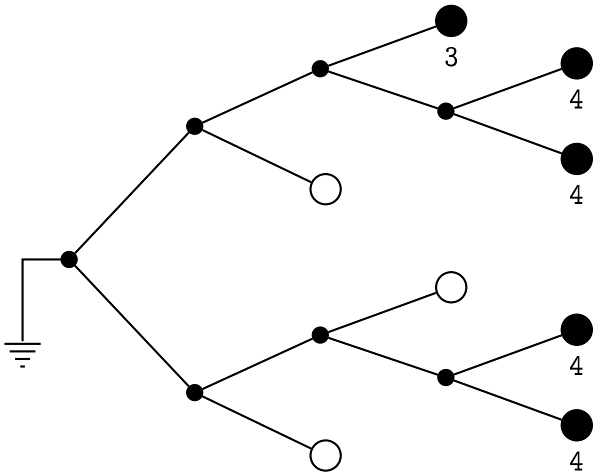

0
1
2
01
1
201
202
2
22

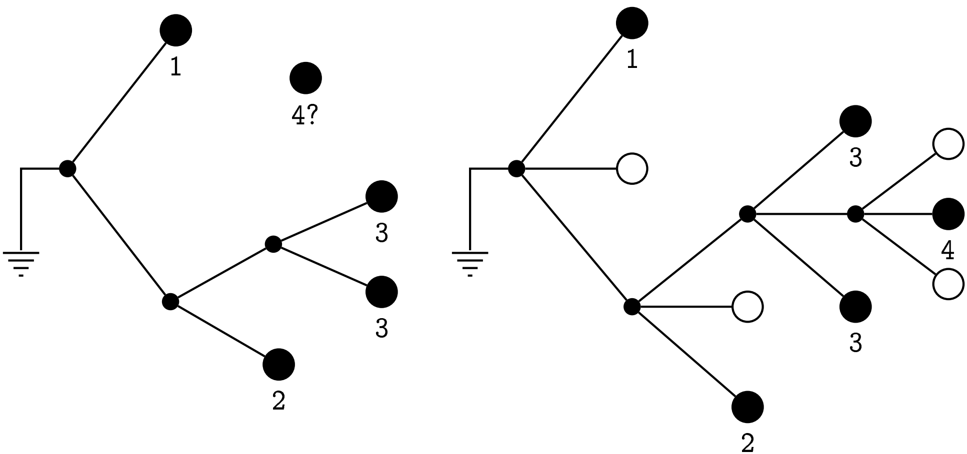

0
1
0
10
110
111

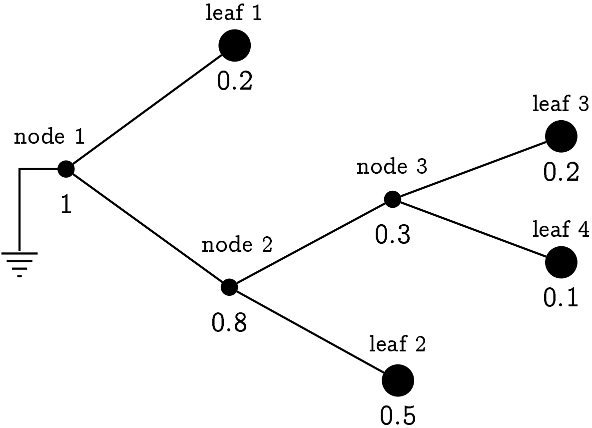

(iii)
0
10
1
not prefix-free
(iv)
00
10
11
prefix-free
(v)–(vi)
0
10
11
prefix-free

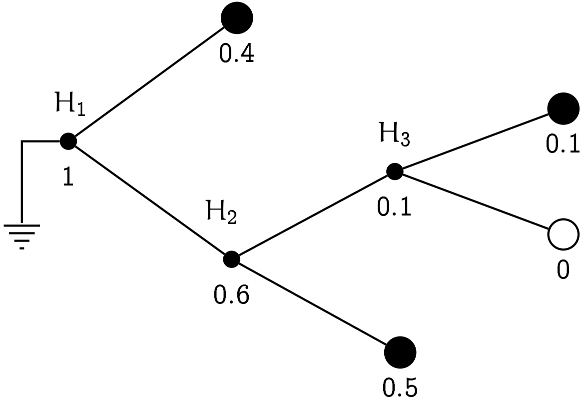


−1 leaf
⟹
+1 node
+3 leaves

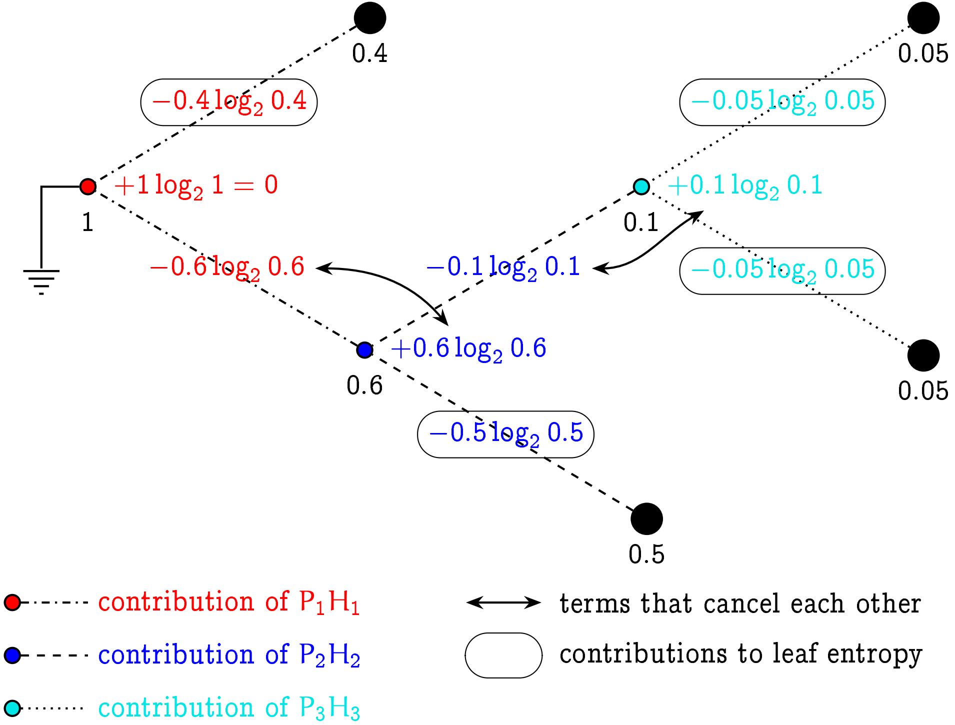

3
4
4
4
4

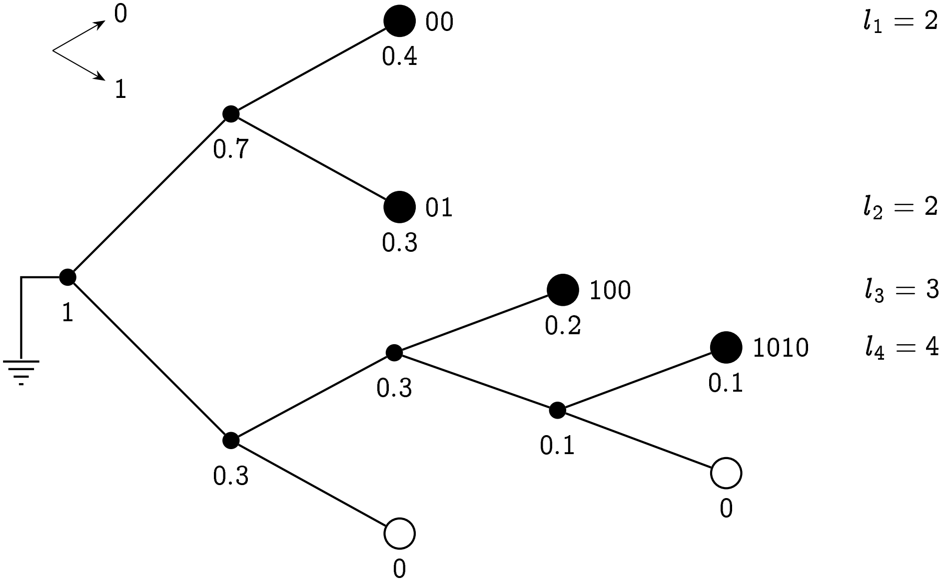

1
4?
3
3
2
1
3
4
3
2

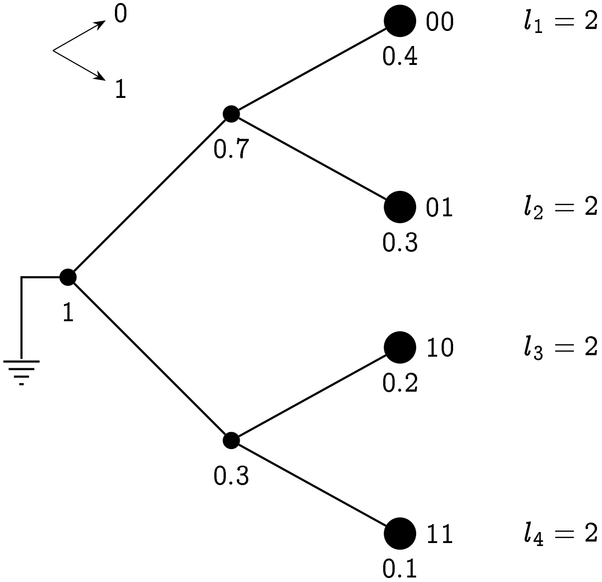

leaf 1
0.2
node 1
1
node 2
0.8
node 3
0.3
leaf 3
0.2
leaf 4
0.1
leaf 2
0.5



0.4
H1
1
H2
0.6
H3
0.1
0.1
0
0.5


0.4
0.05
$-0.4 \log_2 0.4$
$-0.05 \log_2 0.05$
$+1 \log_2 1 = 0$
$+0.1 \log_2 0.1$
1
0.1
$-0.6 \log_2 0.6$
$-0.1 \log_2 0.1$
$-0.05 \log_2 0.05$
$+0.6 \log_2 0.6$
0.05
0.6
$-0.5 \log_2 0.5$
0.5
contribution of $P_1 H_1$
terms that cancel each other
contribution of $P_2 H_2$
contributions to leaf entropy
contribution of $P_3 H_3$


0
1
00
0.4
0.7
01
0.3
1
100
0.2
1010
0.3
0.1
0.1
0.3
0
0
$l_1 = 2$
$l_2 = 2$
$l_3 = 3$
$l_4 = 4$


0
1
00
0.4
$l_1 = 2$
0.7
01
0.3
$l_2 = 2$
1
10
0.2
$l_3 = 2$
0.3
11
0.1
$l_4 = 2$

	u_1	u_2	u_3	u_4
p_i	0.4	0.3	0.2	0.1
F_i	0	0.4	0.7	0.9
binary representation	0.0	0.01100...	0.10110...	0.11100...
$\left\lceil \log_2 \frac{1}{p_i} \right\rceil$	2	2	3	4
shortened representation	0.00	0.01	0.101	0.1110
$\mathbf{c}_i$	00	01	101	1110

	u_1	u_2	u_3	u_4
p_i	0.4	0.3	0.2	0.1
F_i	0	0.4	0.7	0.9
ternary representation	0.0	0.10121...	0.20022...	0.22002...
$\left\lceil \log_3 \frac{1}{p_i} \right\rceil$	1	2	2	3
shortened representation	0.0	0.10	0.20	0.220
$\mathbf{c}_i$	0	10	20	220

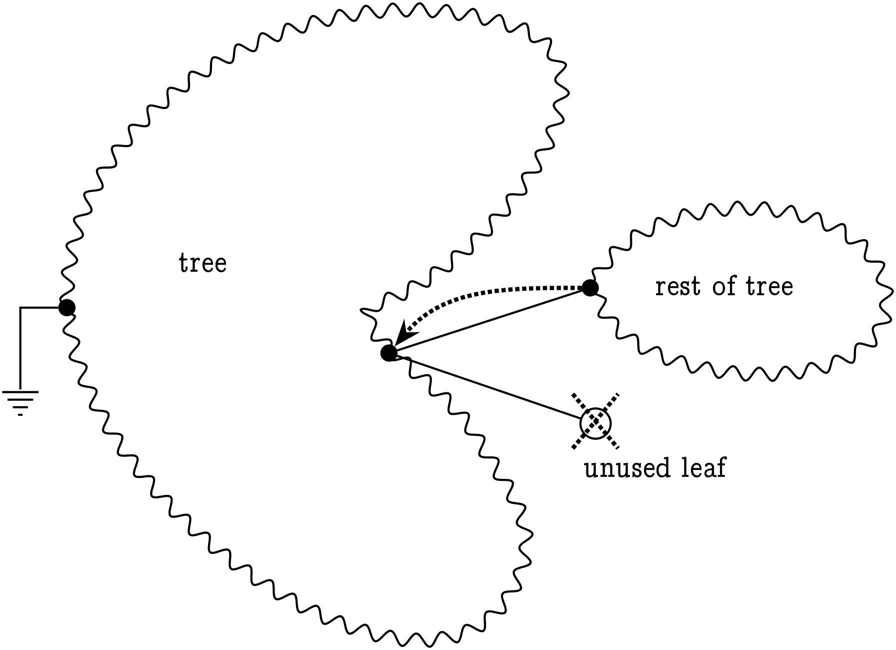
p_1	p_2	p_3	p_4	p_5
0.35	0.25	0.15	0.15	0.1
0.6		0.4		
0		**1**		
0.35	0.25	0.15	0.15	0.1
		0.15	0.25	
0	**1**	**0**	**1**	
			0.15	0.1
			0	**1**
00	**01**	**10**	**110**	**111**

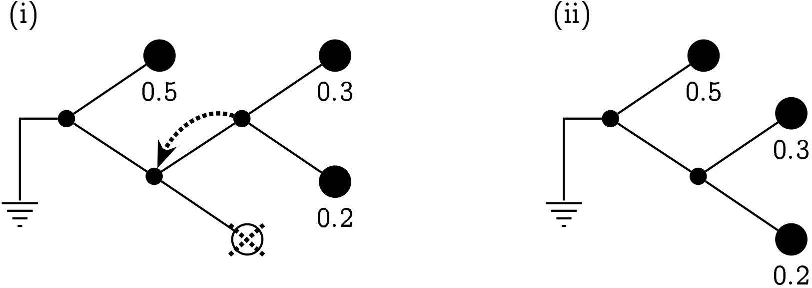
p_1	p_2	p_3	p_4	p_5
0.35	0.25	0.15	0.15	0.1
0.35	0.25	0.4		
0	**1**	**2**		
		0.15	0.15	0.1
		0	**1**	**2**
0	**1**	**20**	**21**	**22**

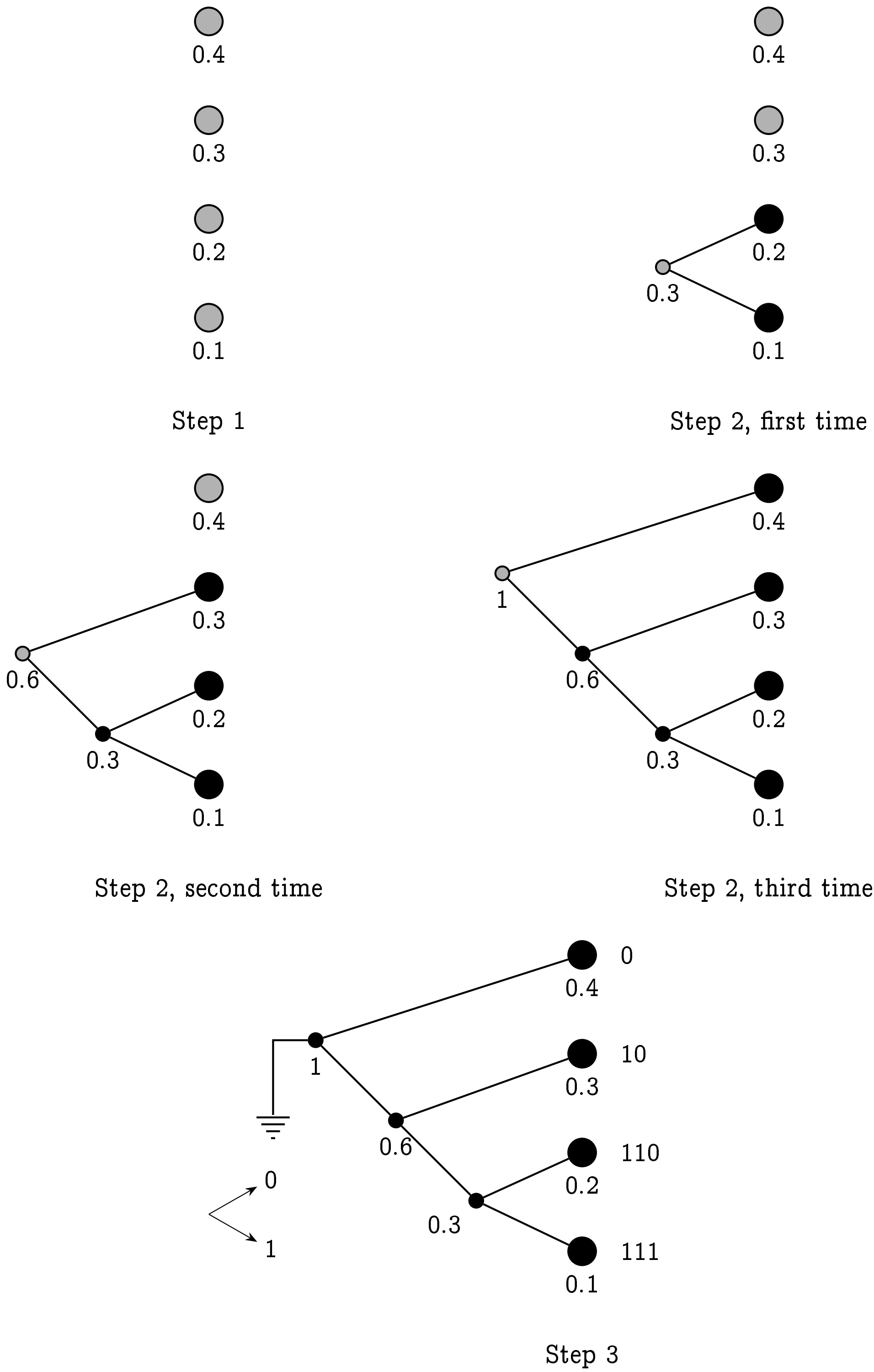
<table>
<tr><td>p_1</td><td>p_2</td><td>p_3</td><td>p_4</td><td>p_5</td><td>p_6</td><td>p_7</td></tr>
<tr><td>0.35</td><td>0.3</td><td>0.15</td><td>0.05</td><td>0.05</td><td>0.05</td><td>0.05</td></tr>
<tr><td colspan="2">0.65
0</td><td colspan="5">0.35
1</td></tr>
<tr><td>0.35</td><td>0.3</td><td>0.15</td><td>0.05</td><td>0.05</td><td>0.05</td><td>0.05</td></tr>
<tr><td>**0**</td><td>**1**</td><td colspan="2">0.2
0</td><td colspan="3">0.15
1</td></tr>
<tr><td></td><td></td><td>0.15</td><td>0.05</td><td>0.05</td><td>0.05</td><td>0.05</td></tr>
<tr><td></td><td></td><td>**0**</td><td>**1**</td><td colspan="2">0.1
0</td><td>0.05
1</td></tr>
<tr><td></td><td></td><td></td><td></td><td>0.05</td><td>0.05</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td>**0**</td><td>**1**</td><td></td></tr>
<tr><td>**00**</td><td>**01**</td><td>**100**</td><td>**101**</td><td>**1100**</td><td>**1101**</td><td>**111**</td></tr>
</table>

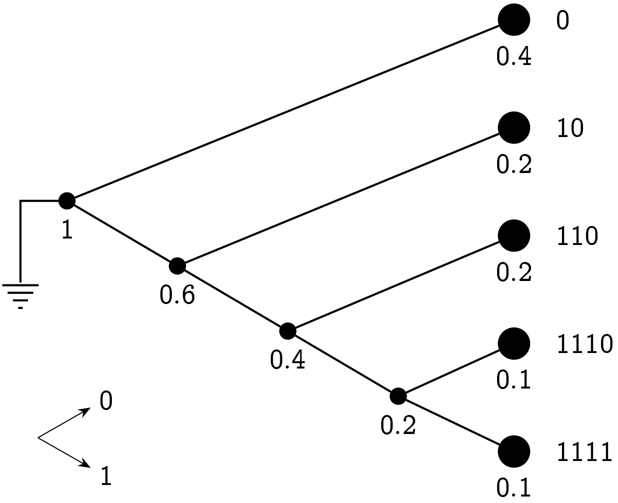
p_1	p_2	p_3	p_4	p_5	p_6	p_7
0.35	0.3	0.15	0.05	0.05	0.05	0.05
0.35	0.65					
0	**1**					
	0.3	0.15	0.05	0.05	0.05	0.05
	0.3	0.35				
	0	**1**				
		0.15	0.05	0.05	0.05	0.05
		0.15	0.2			
		0	**1**			
			0.05	0.05	0.05	0.05
			0.1		0.1	
			0		**1**	
			0.05	0.05	0.05	0.05
			0	**1**	**0**	**1**
0	**10**	**110**	**11100**	**11101**	**11110**	**11111**

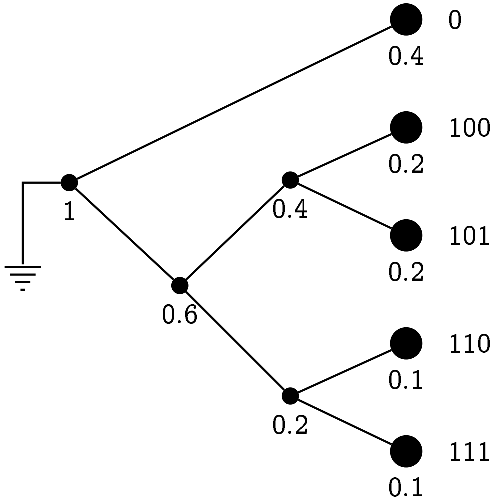
p_1	p_2	p_3	p_4	p_5	p_6	p_7
0.35	0.3	0.15	0.05	0.05	0.05	0.05
0.35	0.65					
0	**1**					
	0.3	0.15	0.05	0.05	0.05	0.05
	0.3	0.35				
	0	**1**				
		0.15	0.05	0.05	0.05	0.05
		0.2		0.15		
		0		**1**		
		0.15	0.05	0.05	0.05	0.05
				0.1		0.05
		0	**1**	**0**		**1**
				0.05	0.05	
				0	**1**	
0	**10**	**1100**	**1101**	**11100**	**11101**	**1111**

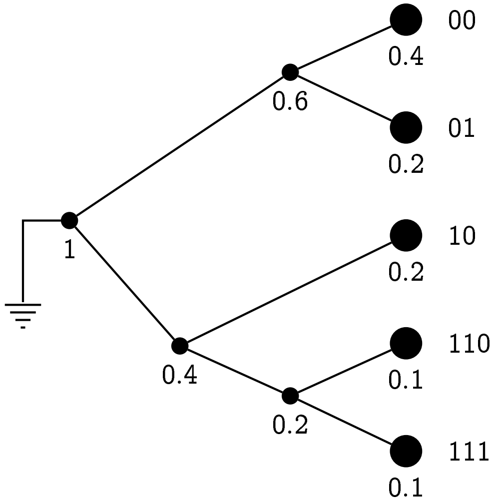

tree
rest of tree
unused leaf

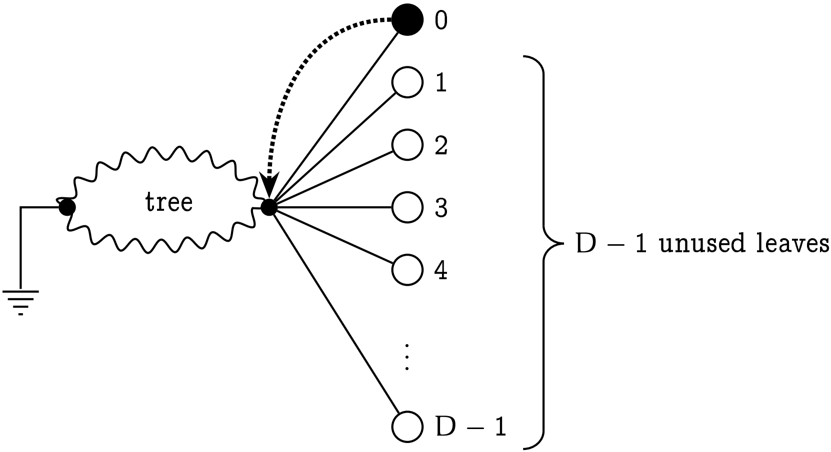

(i)
0.5
0.3
0.2
(ii)
0.5
0.3
0.2

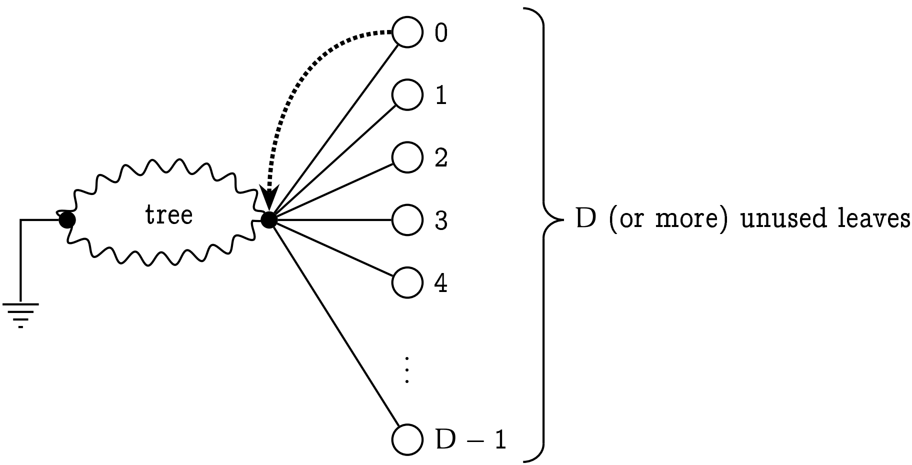

0.4
0.3
0.2
0.1
Step 1
0.4
0.3
0.2
0.3
0.1
Step 2, first time
0.4
0.3
0.6
0.2
0.3
0.1
Step 2, second time
0.4
1
0.3
0.6
0.2
0.3
0.1
Step 2, third time
0
0.4
1
10
0.3
0.6
110
0.2
0
0.3
1
111
0.1
Step 3

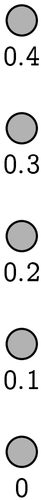

0
0.4
10
0.2
110
0.2
1110
0.1
1111
0.1
1
0.6
0.4
0.2
0
1


0
0.4
100
0.2
101
0.2
110
0.1
111
0.1
1
0.4
0.6
0.2

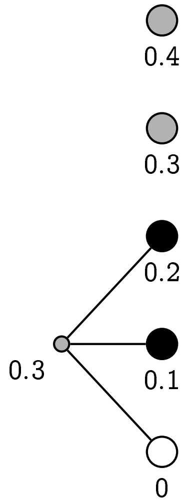

00
0.4
01
0.2
10
0.2
110
0.1
111
0.1
1
0.6
0.4
0.2


0
1
2
3
4
D − 1
tree
D − 1 unused leaves

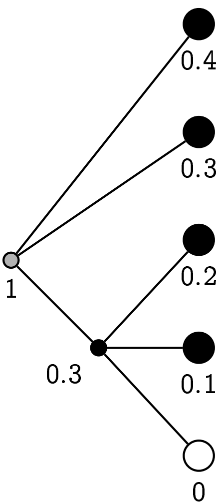

0
1
2
3
4
D − 1
tree
D (or more) unused leaves



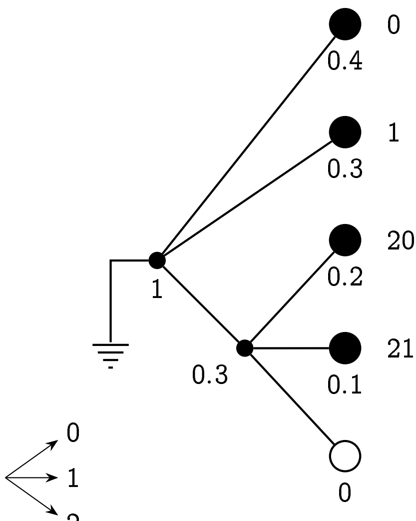
Step 1



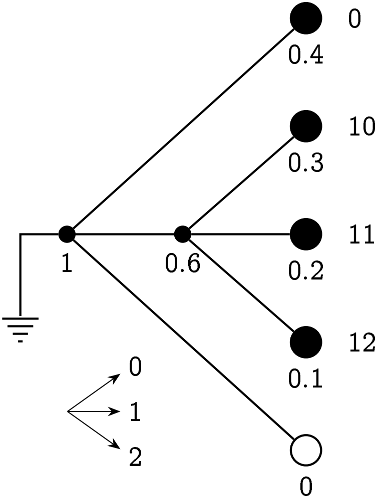
Step 2, first time



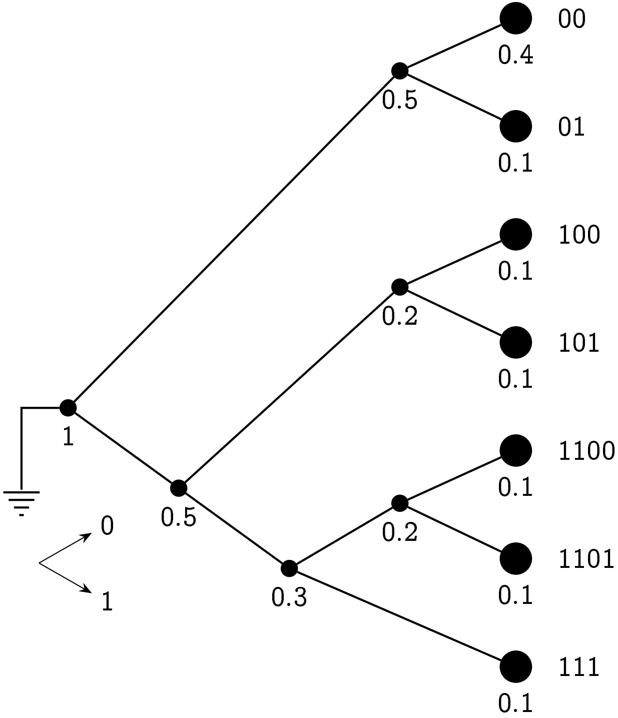
Step 2, second time



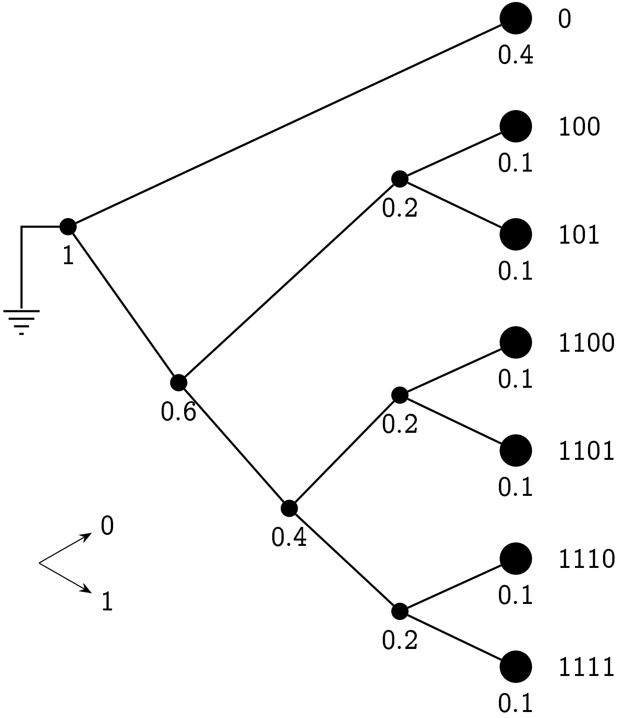
Step 3


0
0.4
10
0.3
11
1
0.6
0.2
12
0.1
0
1
2
0

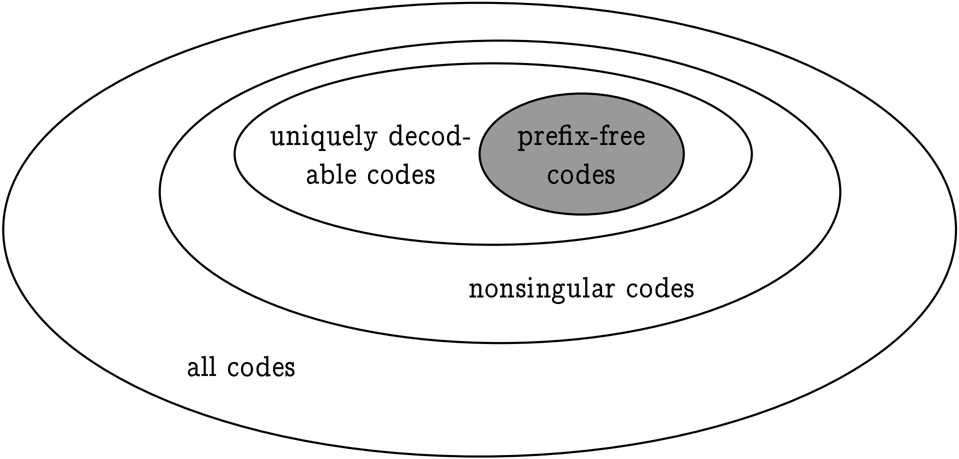
p_1	p_2	p_3	p_4	p_5	p_6	p_7
0.4	0.1	0.1	0.1	0.1	0.1	0.1
0.5				0.5		
0				**1**		
0.4	0.1	0.1	0.1	0.1	0.1	0.1
		0.2		0.3		
0	**1**	**0**		**1**		
		0.1	0.1	0.1	0.1	0.1
				0.2		0.1
		0	**1**	**0**		**1**
				0.1	0.1	
				0	**1**	
00	**01**	**100**	**101**	**1100**	**1101**	**111**

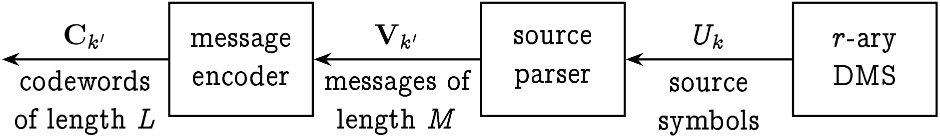

00
0.4
0.5
01
0.1
100
0.1
0.2
101
0.1
1
1100
0.1
0.5
0.2
0
1101
0.1
0.3
1
111
0.1

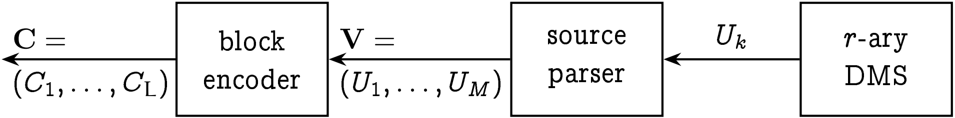
	u_1	u_2	u_3	u_4	u_5	u_6	u_7
p_i	0.4	0.1	0.1	0.1	0.1	0.1	0.1
F_i	0	0.4	0.5	0.6	0.7	0.8	0.9
binary representation	0.0	0.01100	0.1	0.10011	0.10110	0.11001	0.11100
$\left\lceil \log_2 \frac{1}{p_i} \right\rceil$	2	4	4	4	4	4	4
shortened representation	0.00	0.0110	0.1000	0.1001	0.1011	0.1100	0.1110
$\mathbf{c}_i$	00	0110	1000	1001	1011	1100	1110

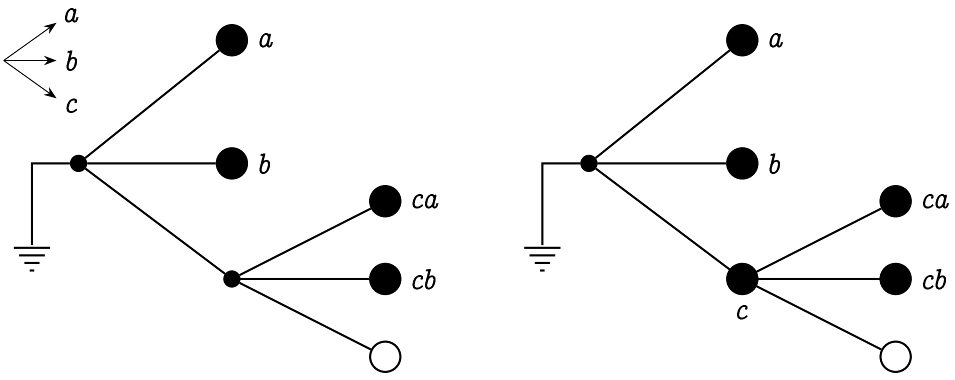

0
0.4
100
0.1
0.2
101
0.1
1
1100
0.1
0.6
0.2
1101
0.1
0
0.4
1110
0.1
1
0.2
1111
0.1

U	Code (i)	Code (ii)	Code (iii)	Code (iv)
a	0	0	10	0
b	0	010	00	10
c	1	01	11	110
d	1	10	110	111

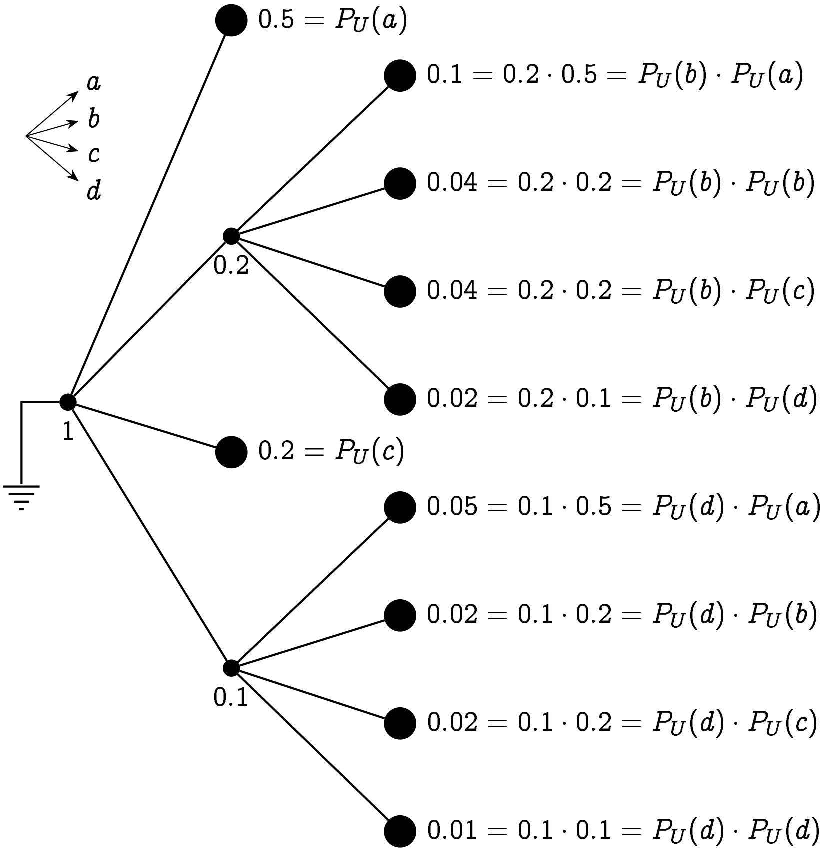

uniquely decod-
able codes
prefix-free
codes
nonsingular codes
all codes

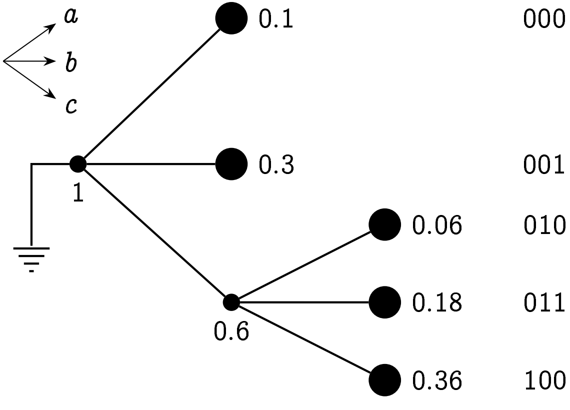

$\mathbf{C}_{k'}$
codewords
of length L
message
encoder
$\mathbf{V}_{k'}$
messages of
length M
source
parser
U_k
source
symbols
r-ary
DMS


C =
(C1, . . . , CL)
block
encoder
V =
(U1, . . . , UM)
source
parser
Uk
r-ary
DMS

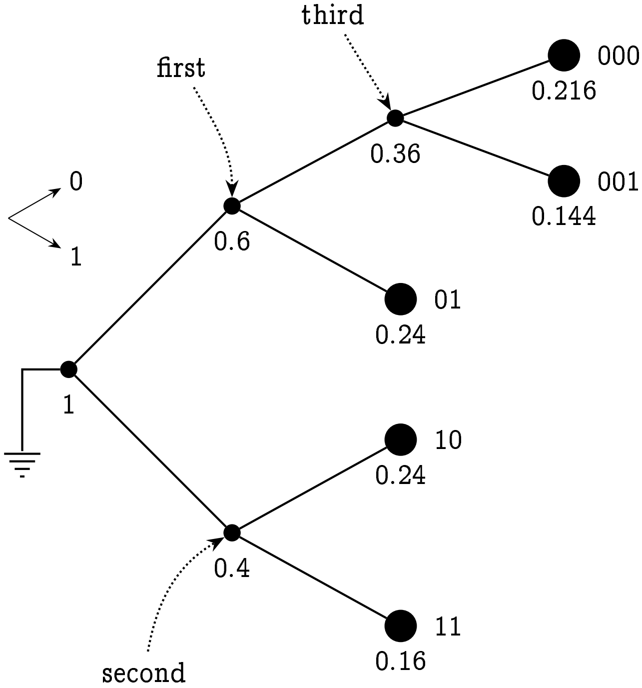


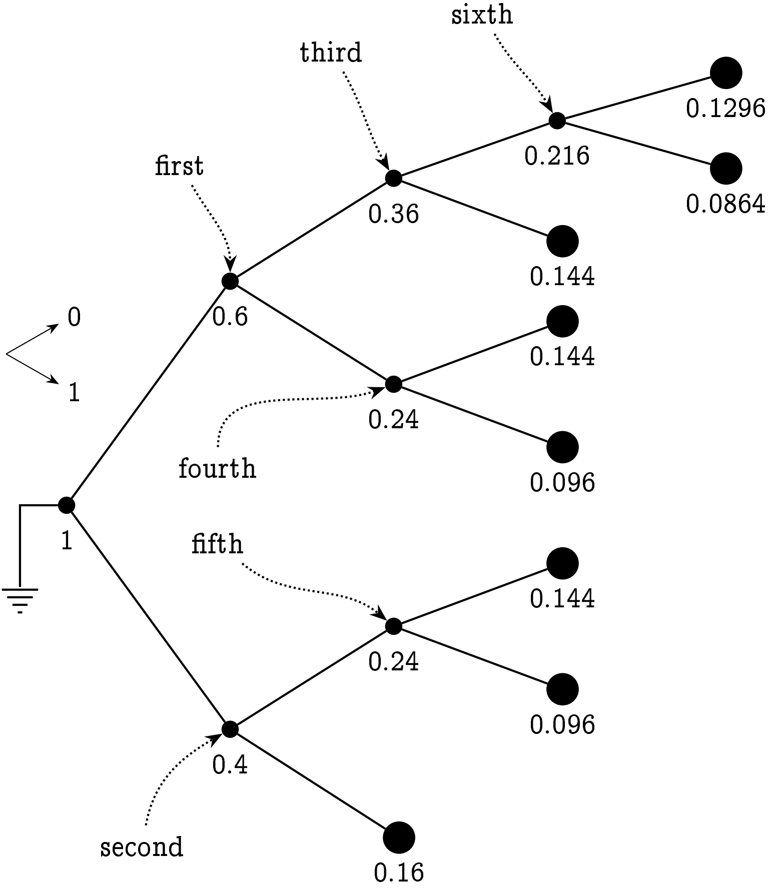
“illegal” “legal”, but not proper


$0.5 = P_U(a)$
a
b
c
d
$0.1 = 0.2 \cdot 0.5 = P_U(b) \cdot P_U(a)$
$0.04 = 0.2 \cdot 0.2 = P_U(b) \cdot P_U(b)$
0.2
$0.04 = 0.2 \cdot 0.2 = P_U(b) \cdot P_U(c)$
$0.02 = 0.2 \cdot 0.1 = P_U(b) \cdot P_U(d)$
1
$0.2 = P_U(c)$
$0.05 = 0.1 \cdot 0.5 = P_U(d) \cdot P_U(a)$
$0.02 = 0.1 \cdot 0.2 = P_U(d) \cdot P_U(b)$
0.1
$0.02 = 0.1 \cdot 0.2 = P_U(d) \cdot P_U(c)$
$0.01 = 0.1 \cdot 0.1 = P_U(d) \cdot P_U(d)$



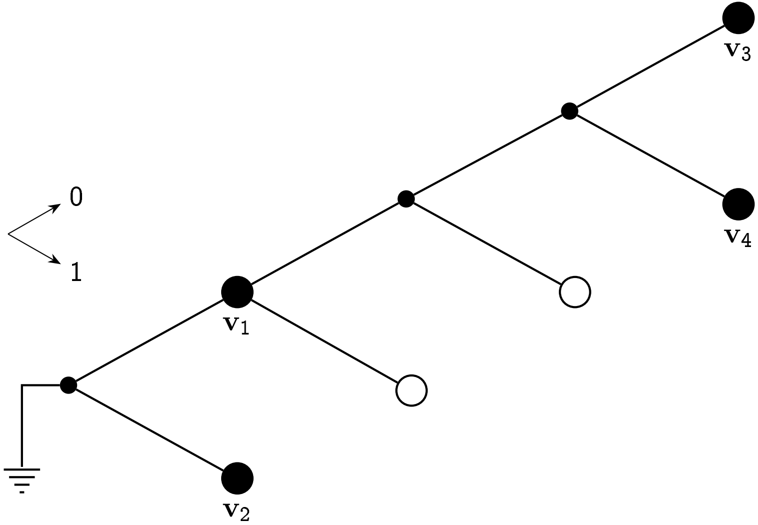
a
b
c
0.1
000
0.3
001
1
0.06
010
0.18
011
0.6
0.36
100


third
first
000
0.216
0.36
001
0.144
0
1
0.6
01
0.24
1
10
0.24
0.4
11
0.16
second

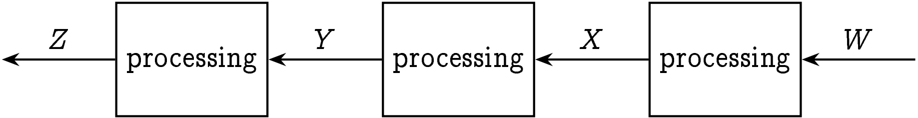


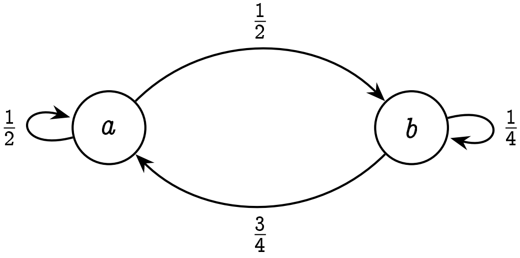
sixth
third
first
0.1296
0.216
0.0864
0.36
0.144
0.6
0
0.144
1
0.24
fourth
0.096
1
fifth
0.144
0.24
0.096
0.4
second
0.16

Message	Codewords
0000	000
0001	001
001	010
010	011
011	100
100	101
101	110
11	111

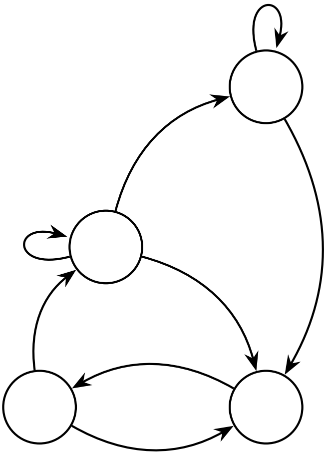


0
1
$\mathbf{v}_3$
$\mathbf{v}_4$
$\mathbf{v}_1$
$\mathbf{v}_2$

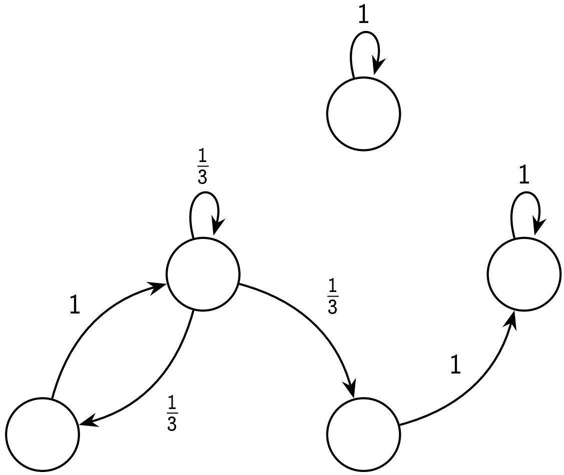

Z
processing
Y
processing
X
processing
W



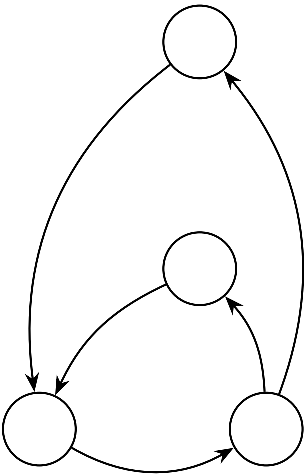
1/2
1/2
a
b
1/4
3/4



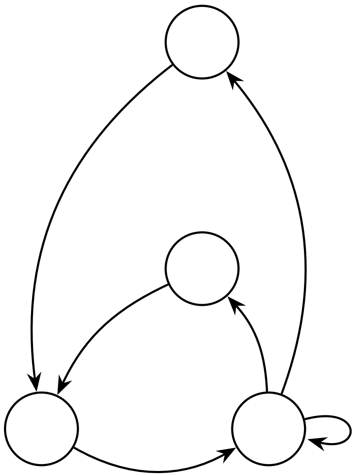
irreducible



reducible



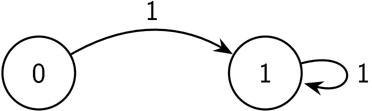
periodic



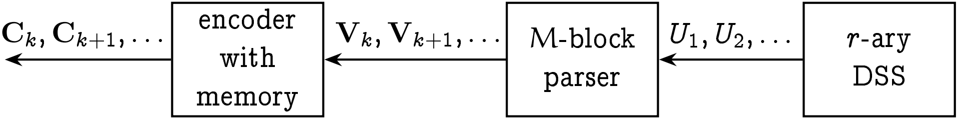
aperiodic

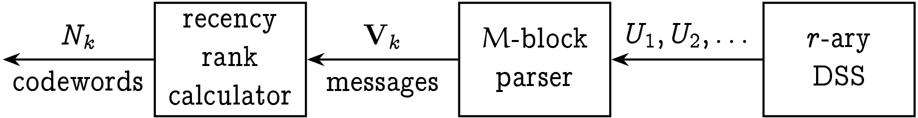
$P_{X_k}(\cdot)$	$k=1$	$k=2$	$k=3$	$k=4$
$\mathsf{P}[X_k=a]$	1	$\frac{1}{2}=0.5$	$\frac{5}{8}=0.625$	$\frac{19}{32}=0.59375$
$\mathsf{P}[X_k=b]$	0	$\frac{1}{2}=0.5$	$\frac{3}{8}=0.375$	$\frac{13}{32}=0.40625$

$P_{X_k}(\cdot)$	$k=5$	$\ldots$	$k=\infty$
$\mathsf{P}[X_k=a]$	$\frac{77}{128}=0.6015625$	$\ldots$	$\frac{3}{5}=0.6$
$\mathsf{P}[X_k=b]$	$\frac{51}{128}=0.3984375$	$\ldots$	$\frac{2}{5}=0.4$



1
0
1
1


$\mathbf{C}_k, \mathbf{C}_{k+1}, \ldots$
encoder with memory
$\mathbf{V}_k, \mathbf{V}_{k+1}, \ldots$
M-block parser
$U_1, U_2, \ldots$
r-ary DSS



N_k
codewords
recency
rank
calculator
$\mathbf{V}_k$
messages
M-block
parser
$U_1, U_2, \ldots$
r-ary
DSS

Message	Recency Rank at Time k
00	4
01	1
10	3
11	2

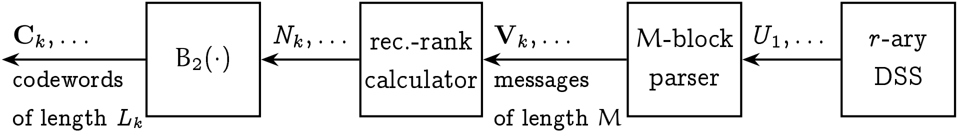
Message	Recency Rank at Time $k+1$
00	4
01	2
10	1
11	3

Message	Recency Rank at Time 1 (by definition)
00	1
01	2
10	3
11	4

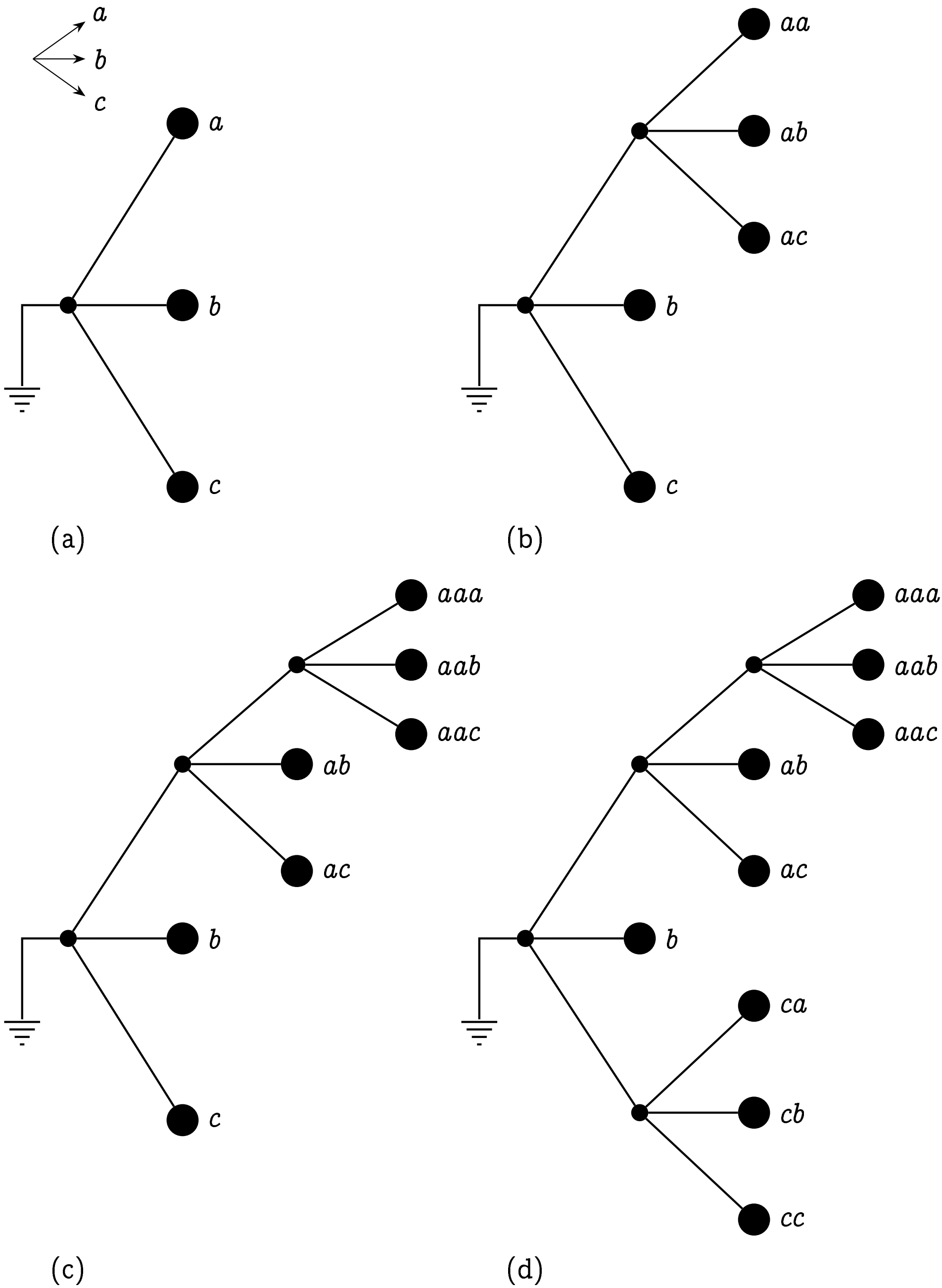
n	1	2	3	4	5	6	7	8	9	10	$\cdots$
$\mathrm{B}_0(n)$	1	10	11	100	101	110	111	1000	1001	1010	$\cdots$

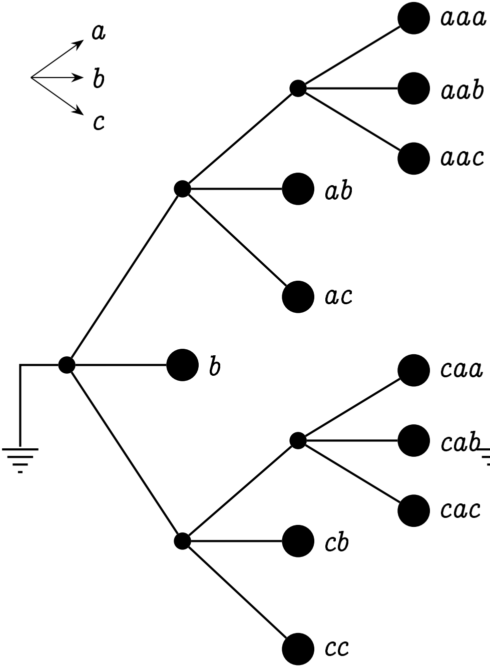
n	1	2	3	4	5	6
$\mathrm{B}_0(n)$	1	10	11	100	101	110
$\mathrm{L}_{\mathrm{B}_0}(n) - 1$	0	1	1	2	2	2
$\mathrm{B}_1(n)$	1	010	011	00100	00101	00110
n	7	8	9	10	11	$\cdots$
$\mathrm{B}_0(n)$	111	1000	1001	1010	1011	$\cdots$
$\mathrm{L}_{\mathrm{B}_0}(n) - 1$	2	3	3	3	3	$\cdots$
$\mathrm{B}_1(n)$	00111	0001000	0001001	0001010	0001011	$\cdots$

n	1	2	3	4	5	6
$B_0(n)$	1	10	11	100	101	110
$L_{B_0}(n)$	1	2	2	3	3	3
$B_1(L_{B_0}(n))$	1	010	010	011	011	011
$B_2(n)$	1	0100	0101	01100	01101	01110
n	7	8	9	10	11	$\cdots$
$B_0(n)$	111	1000	1001	1010	1011	$\cdots$
$L_{B_0}(n)$	3	4	4	4	4	$\cdots$
$B_1(L_{B_0}(n))$	011	00100	00100	00100	00100	$\cdots$
$B_2(n)$	01111	00100000	00100001	00100010	00100011	$\cdots$



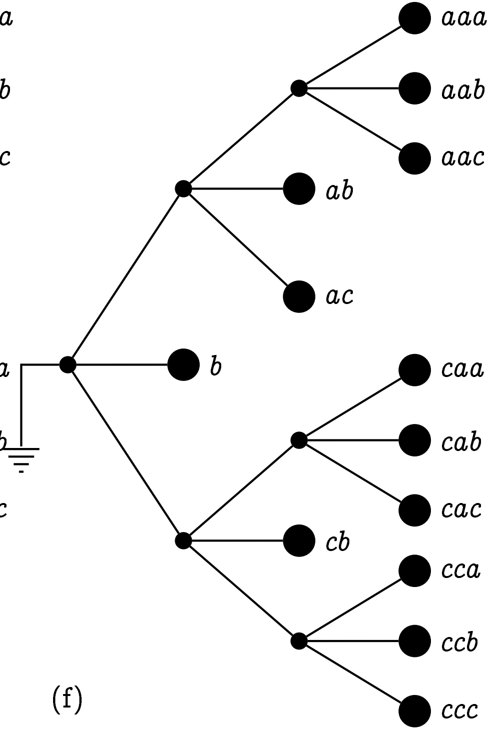
$\mathbf{C}_k, \ldots$
codewords
of length L_k
$\mathrm{B}_2(\cdot)$
$N_k, \ldots$
rec.-rank
calculator
$\mathbf{V}_k, \ldots$
messages
of length M
M-block
parser
$U_1, \ldots$
r-ary
DSS


a
b
c
a
b
c
(a)
aa
ab
ac
b
c
(b)
aaa
aab
aac
ab
ac
b
c
(c)
aaa
aab
aac
ab
ac
b
ca
cb
cc
(d)



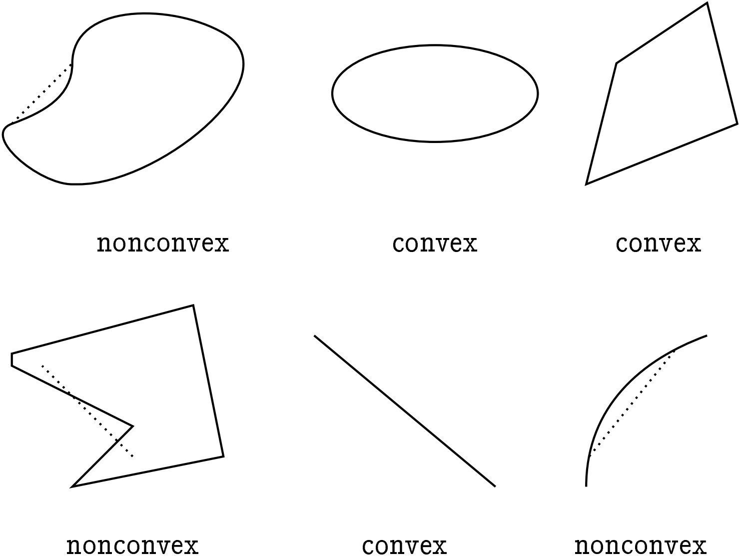
a
b
c
aaa
aab
aac
ab
ac
b
caa
cab
cac
cb
cc

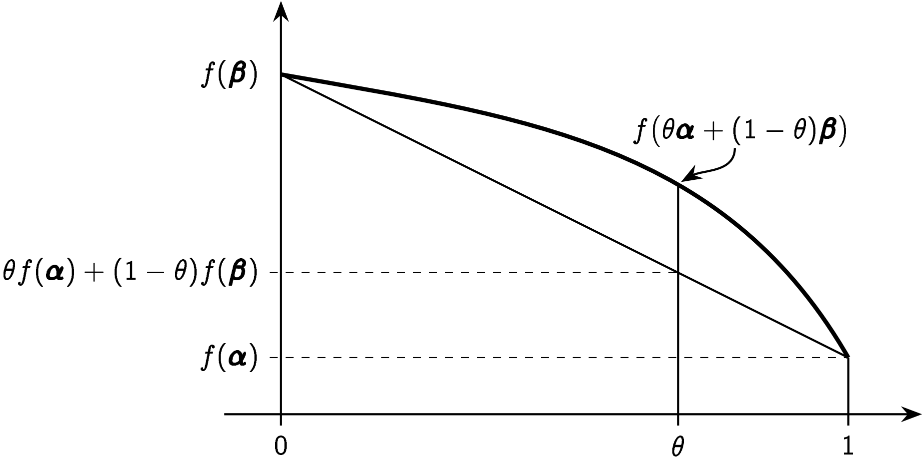
(e)



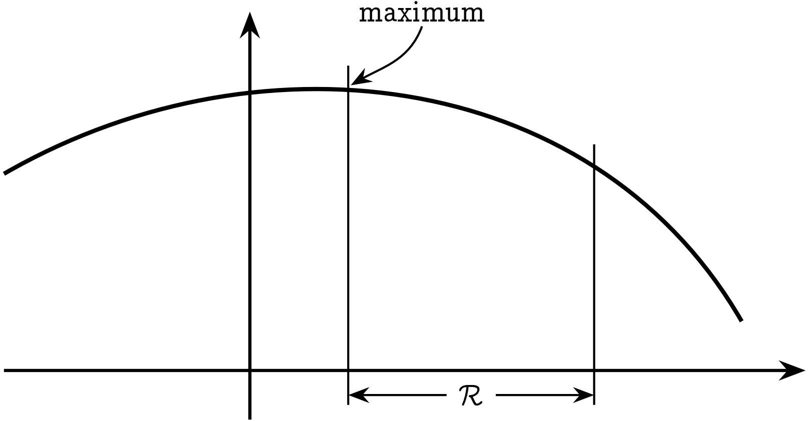
aaa
aab
aac
ab
ac
b
caa
cab
cac
cb
cca
ccb
ccc

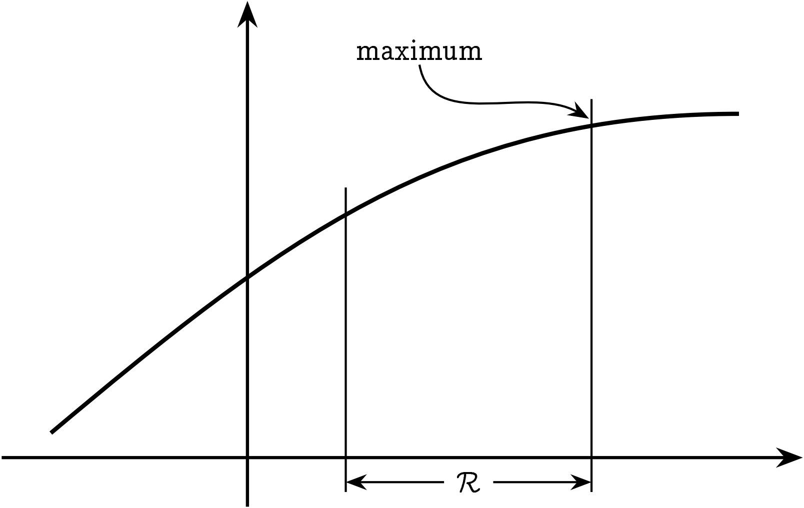
(f)


nonconvex
convex
convex
nonconvex
convex
nonconvex

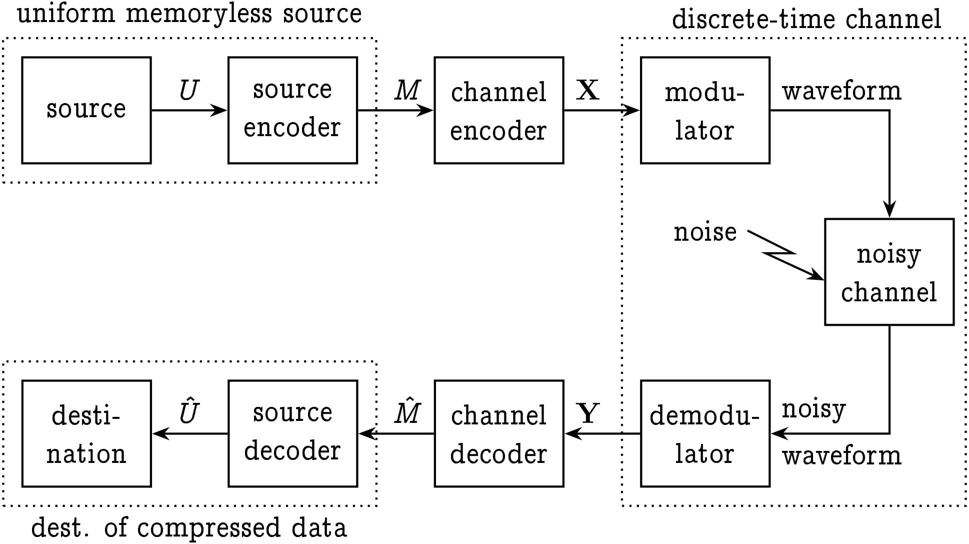


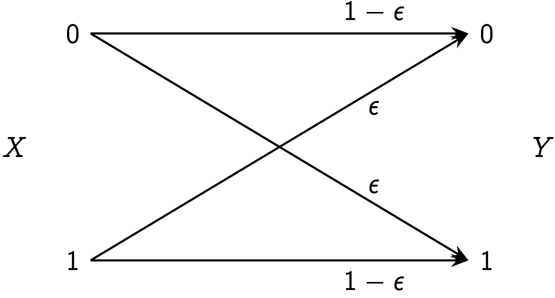
$f(\boldsymbol{\beta})$
$f(\theta\boldsymbol{\alpha} + (1-\theta)\boldsymbol{\beta})$
$\theta f(\boldsymbol{\alpha}) + (1-\theta) f(\boldsymbol{\beta})$
$f(\boldsymbol{\alpha})$
0
θ
1


maximum
$\mathcal{R}$

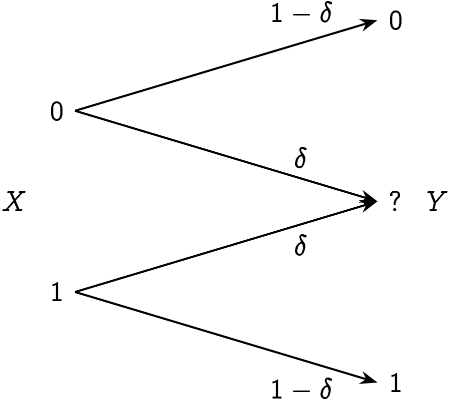

maximum
$\mathcal{R}$

original name	2	3	1
new name t	1	2	3
p_i	0.2	0.1	0.7
o_i	6	10	1.2
$p_i o_i$	1.2	1.0	0.84
	$\vee$	$\vee$	$\wedge$
β_t	1	0.96	0.955

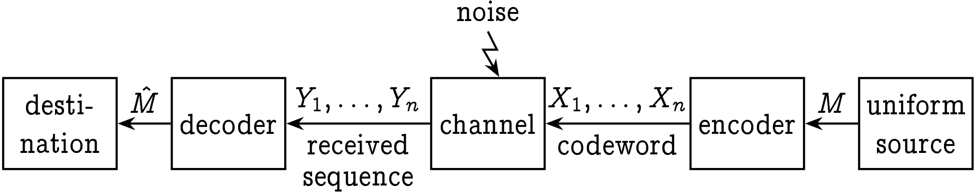

uniform memoryless source
discrete-time channel
source
U
source encoder
M
channel encoder
$\mathbf{X}$
modu-lator
waveform
noise
noisy channel
desti-nation
$\hat{U}$
source decoder
$\hat{M}$
channel decoder
$\mathbf{Y}$
demodu-lator
noisy waveform
dest. of compressed data

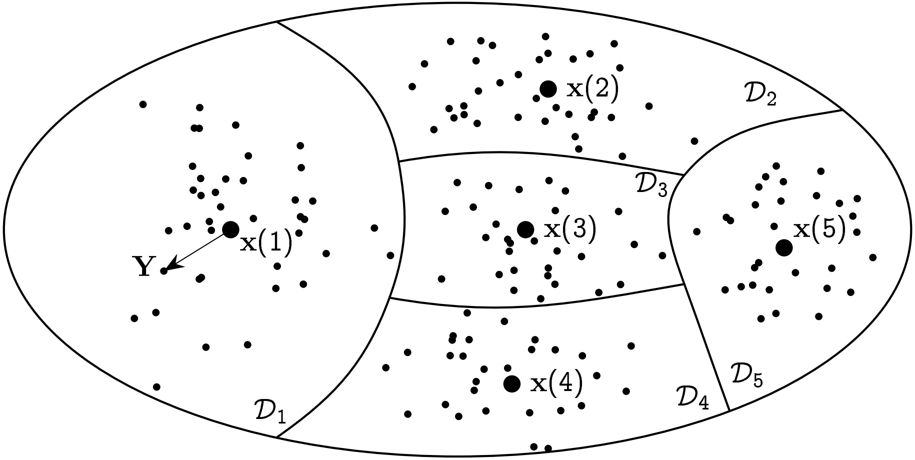


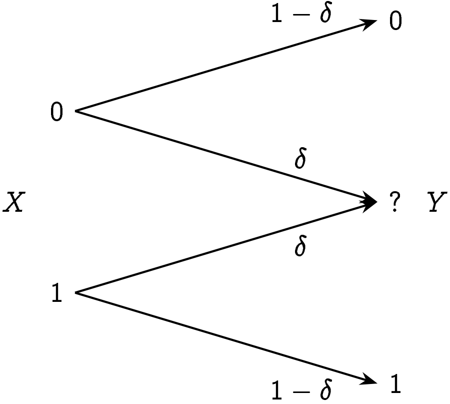
0
1 − ϵ
0
ϵ
X
Y
ϵ
1
1
1 − ϵ

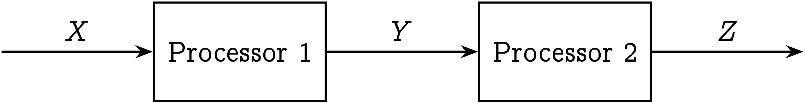


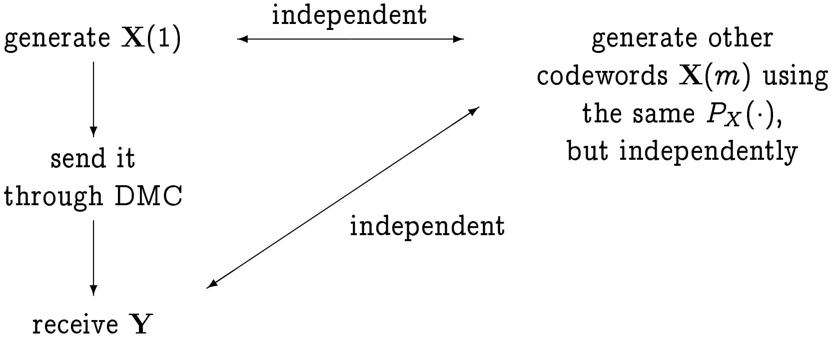
$1-\delta$
0
0
δ
X
?
Y
δ
1
$1-\delta$
1

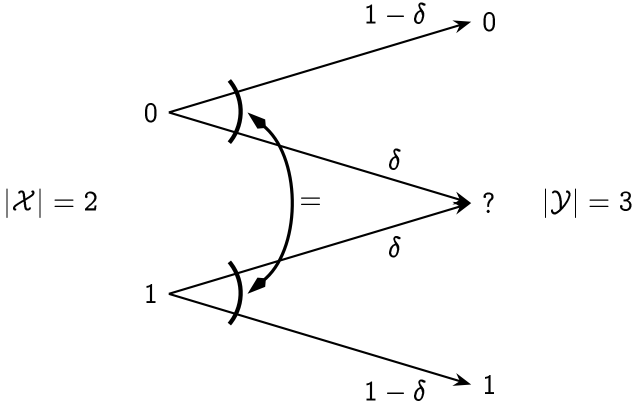

noise
destination
$\hat{M}$
decoder
$Y_1, \ldots, Y_n$
received sequence
channel
$X_1, \ldots, X_n$
codeword
encoder
M
uniform source

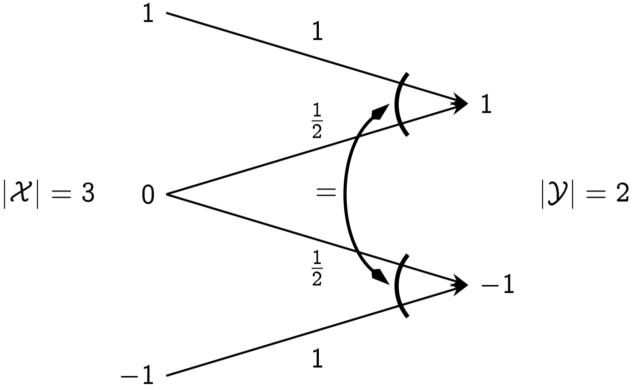

x(1)
Y
D_1
x(2)
D_2
x(3)
D_3
x(4)
D_4
x(5)
D_5

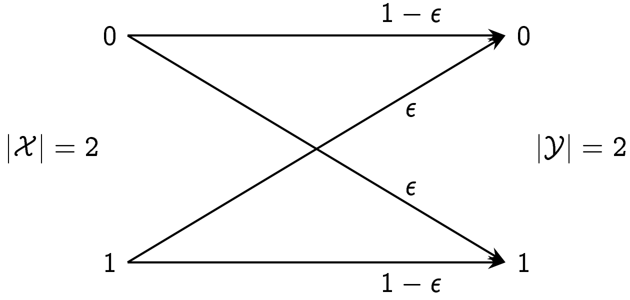

$1-\delta$
0
0
δ
X
?
Y
δ
1
$1-\delta$
1

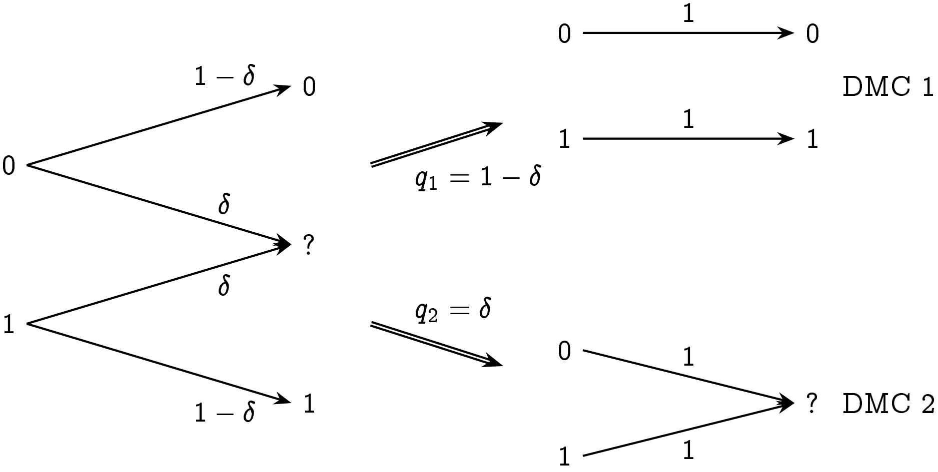

X
Processor 1
Y
Processor 2
Z


generate $\mathbf{X}(1)$
independent
generate other codewords $\mathbf{X}(m)$ using the same $P_X(\cdot)$, but independently
send it through DMC
independent
receive $\mathbf{Y}$

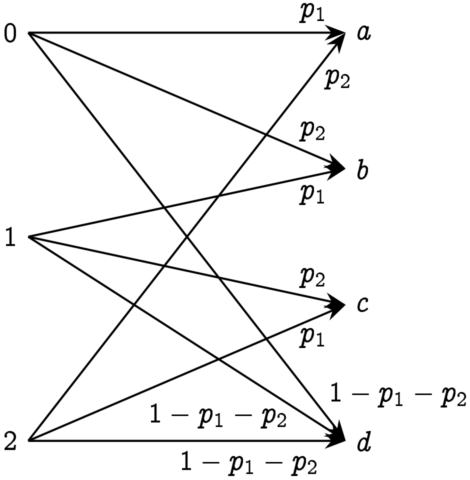

$1-\delta$
0
0
δ
$|\mathcal{X}|=2$
$=$
?
$|\mathcal{Y}|=3$
δ
1
1
$1-\delta$


1
1
1
$\frac{1}{2}$
$|\mathcal{X}| = 3$
0
=
$|\mathcal{Y}| = 2$
$\frac{1}{2}$
-1
1
-1

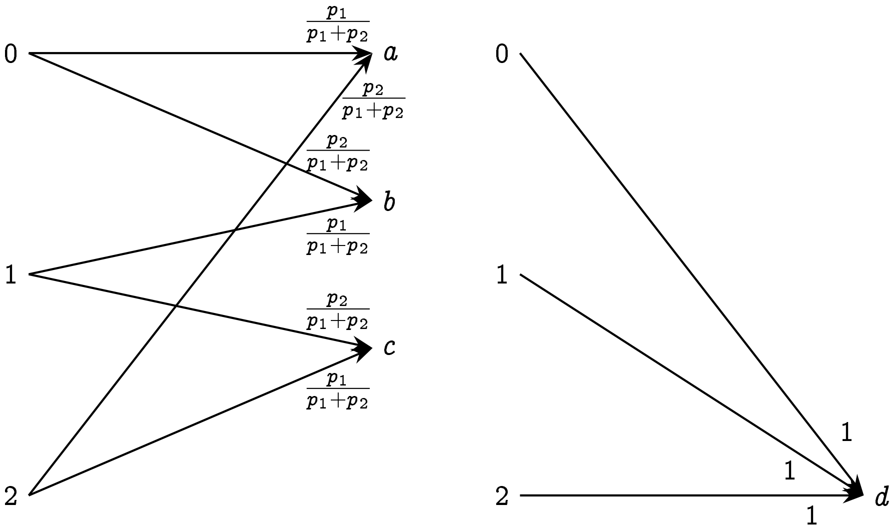

$1-\epsilon$
0
0
ϵ
$|\mathcal{X}| = 2$
$|\mathcal{Y}| = 2$
ϵ
1
1
$1-\epsilon$

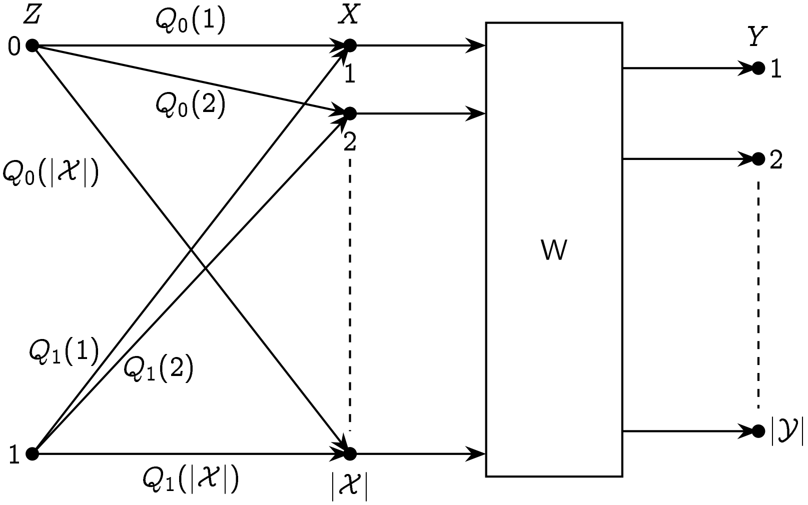


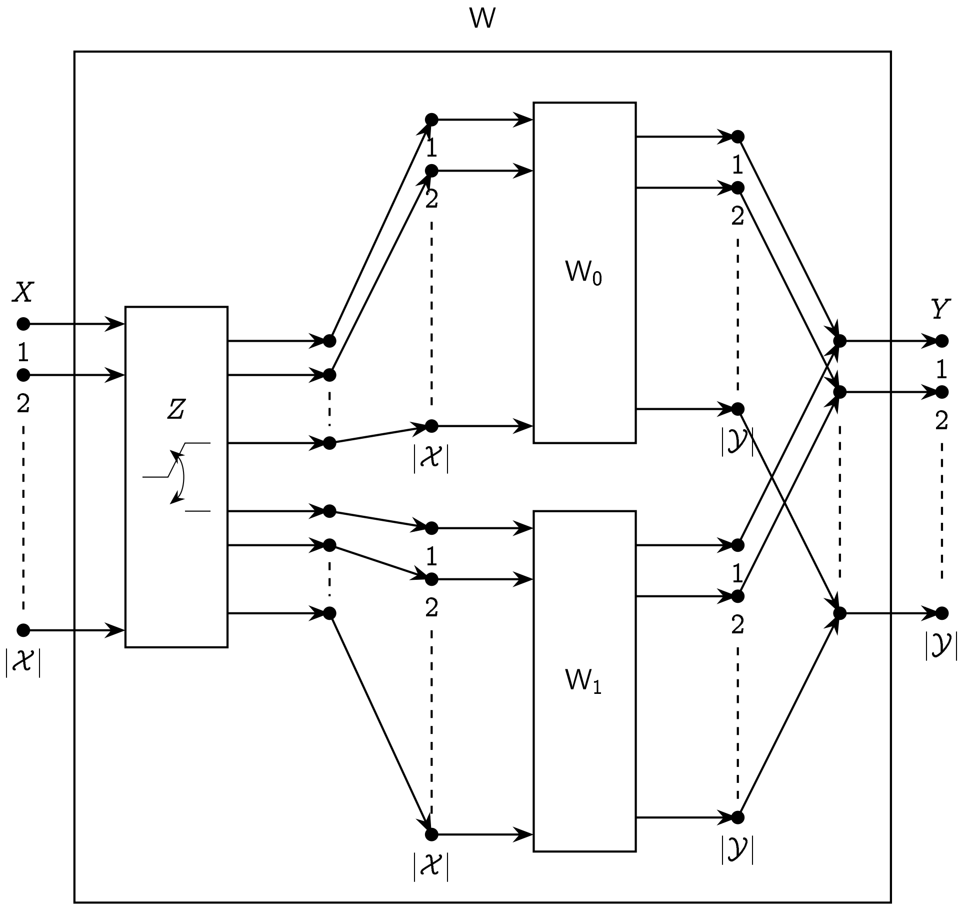
1
0
0
1 − δ
0
DMC 1
1
1
1
0
q1 = 1 − δ
δ
?
δ
q2 = δ
1
0
1
1 − δ
1
?
DMC 2
1
1

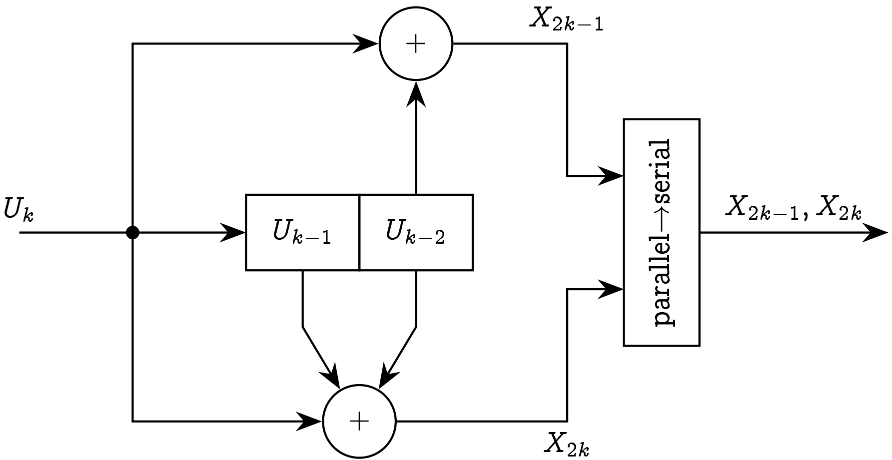


0
1
2
a
b
c
d
p_1
p_2
p_2
p_1
p_2
p_1
$1-p_1-p_2$
$1-p_1-p_2$
$1-p_1-p_2$

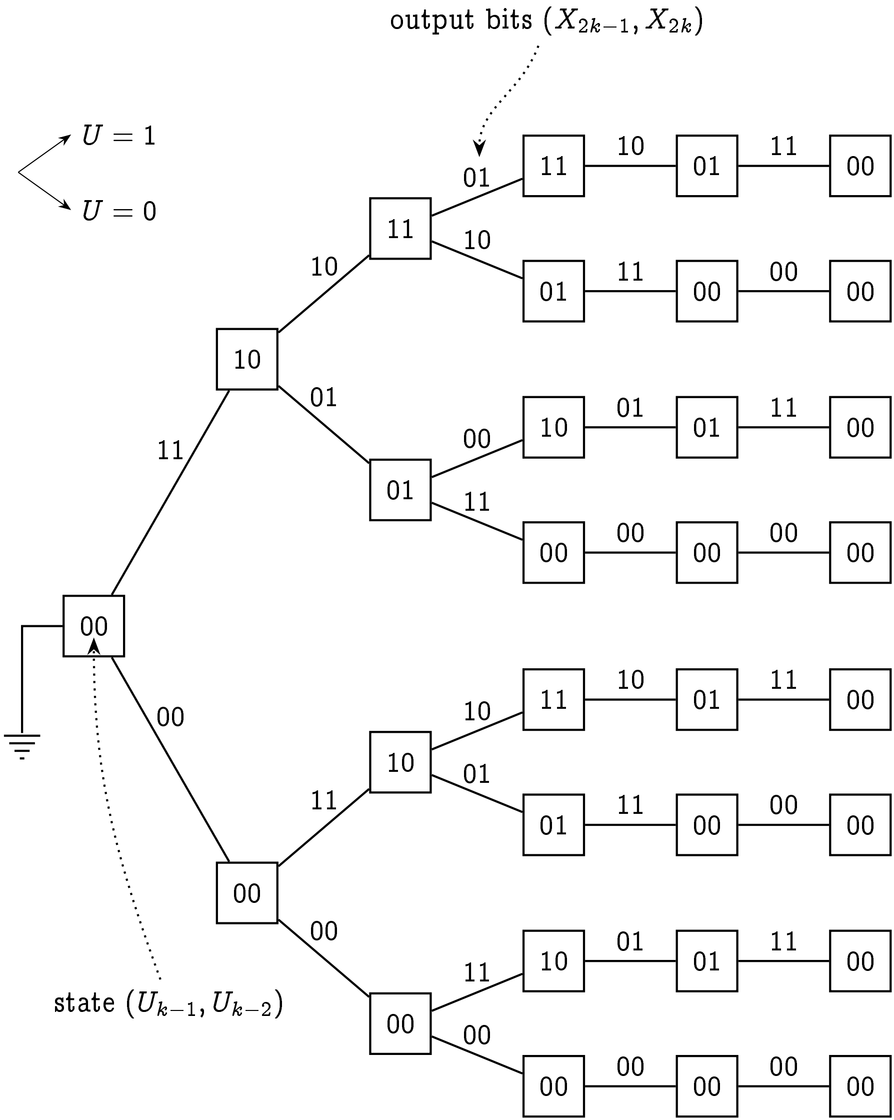

0
1
2
a
b
c
$\frac{p_1}{p_1+p_2}$
$\frac{p_2}{p_1+p_2}$
$\frac{p_2}{p_1+p_2}$
$\frac{p_1}{p_1+p_2}$
$\frac{p_2}{p_1+p_2}$
$\frac{p_1}{p_1+p_2}$
0
1
2
d
1
1
1

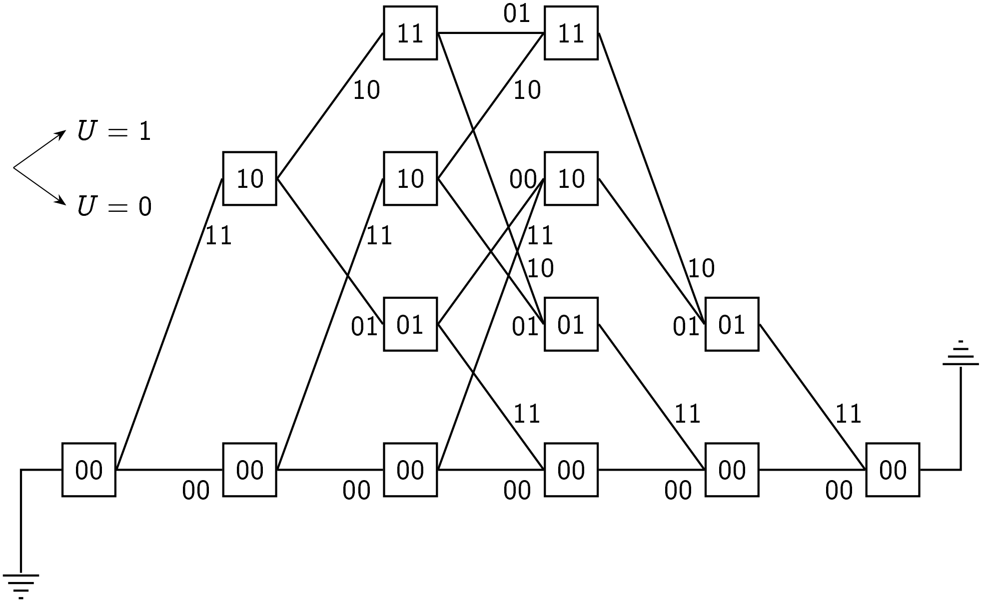

Z
X
Y
0
1
Q_0(1)
Q_0(2)
Q_0(|𝒳|)
Q_1(1)
Q_1(2)
Q_1(|𝒳|)
1
2
|𝒳|
W
1
2
|𝒴|


W
X
1
2
|𝒳|
Z
1
2
|𝒳|
W$_0$
1
2
|𝒴|
1
2
|𝒳|
W$_1$
1
2
|𝒴|
Y
1
2
|𝒴|

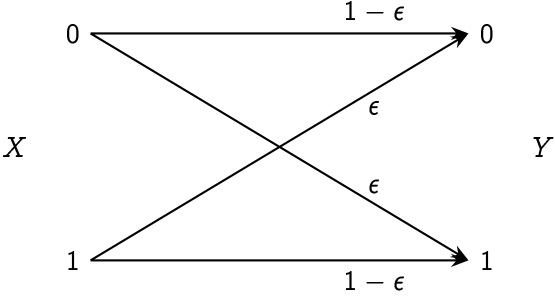


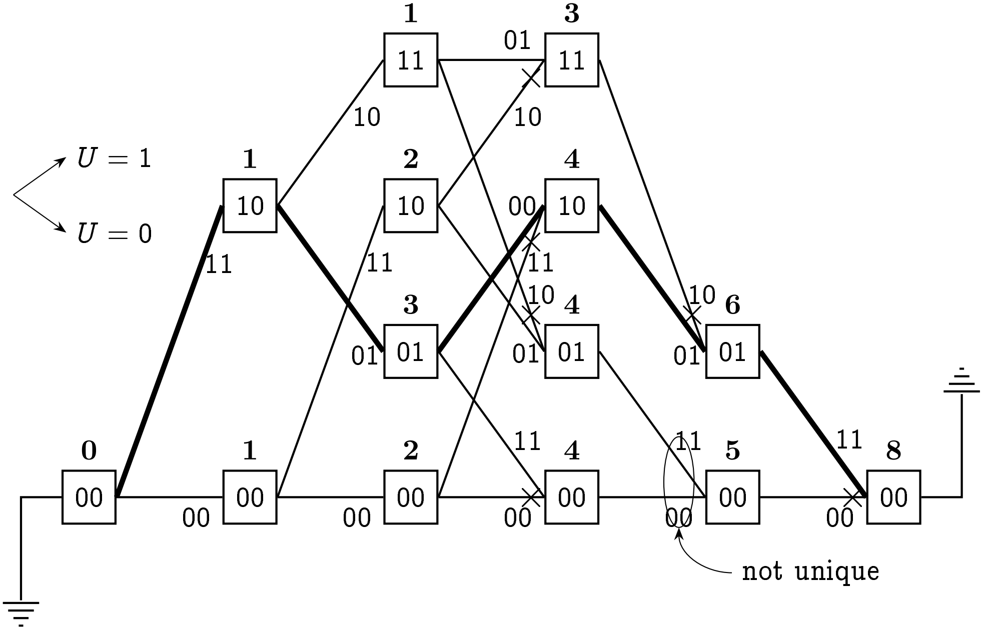
X_{2k-1}
U_k
U_{k-1}
U_{k-2}
parallel→serial
X_{2k-1}, X_{2k}
X_{2k}


output bits (X_{2k-1}, X_{2k})
$U = 1$
$U = 0$
state (U_{k-1}, U_{k-2})
00
11
00
10
00
10
01
11
00
11
11
10
01
01
10
00
00
11
11
10
01
10
00
11
01
00
00
11
10
01
11
01
01
00
11
00
00
10
01
11
01
11
00
00
00
00
00
00
00
01
11
00
00
11
00
01
00
10
01
11
01
11
00
00
00
00
00
00
00
00
01
11
00
00
00
00
00

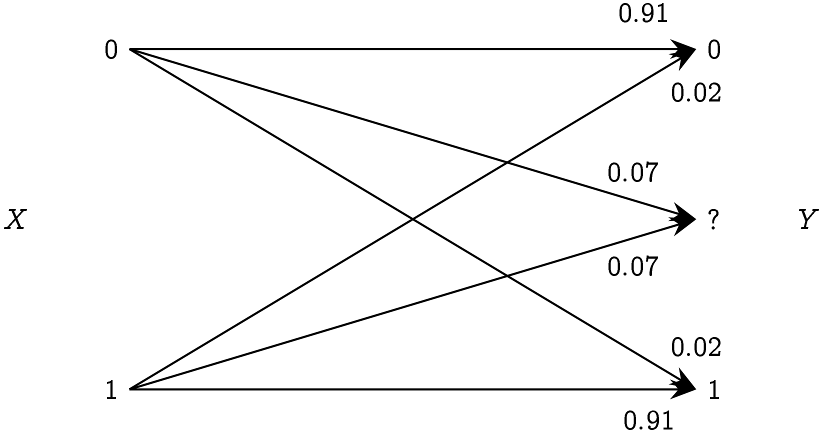


U = 1
U = 0
00
00
00
00
00
00
00
00
00
00
00
00
10
10
10
11
11
11
11
01
01
01
01
01
01
10
10
10
10
00
11
11
11
11
11
10
01


1 − ϵ
0
0
ϵ
X
Y
ϵ
1
1
1 − ϵ

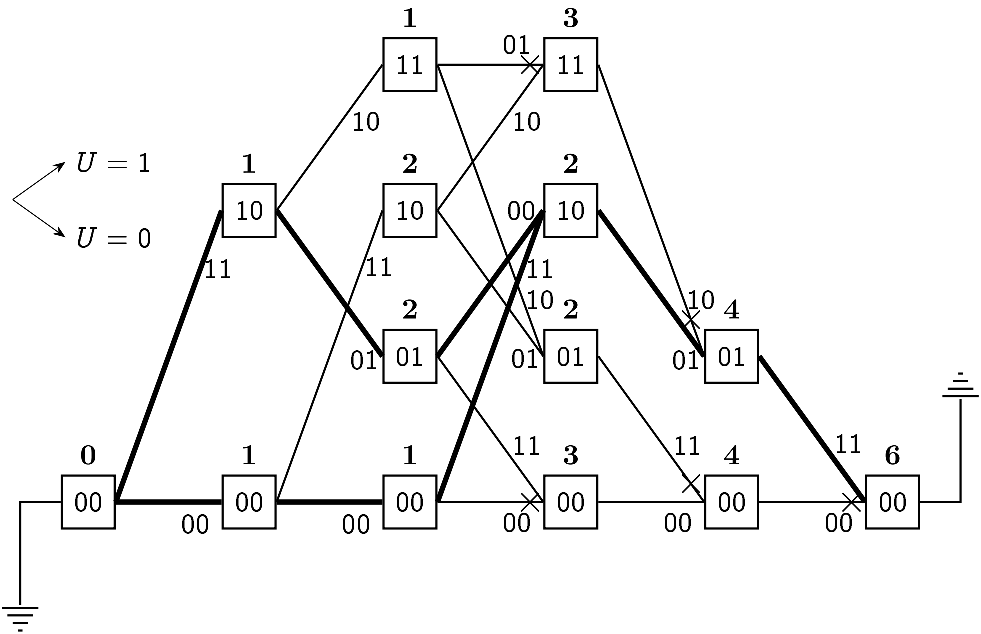


$\mathbf{y} =$	01	01	01	01	11
$\hat{\mathbf{x}} =$	11	01	00	01	11
$\hat{\mathbf{u}} =$	1	0	1		

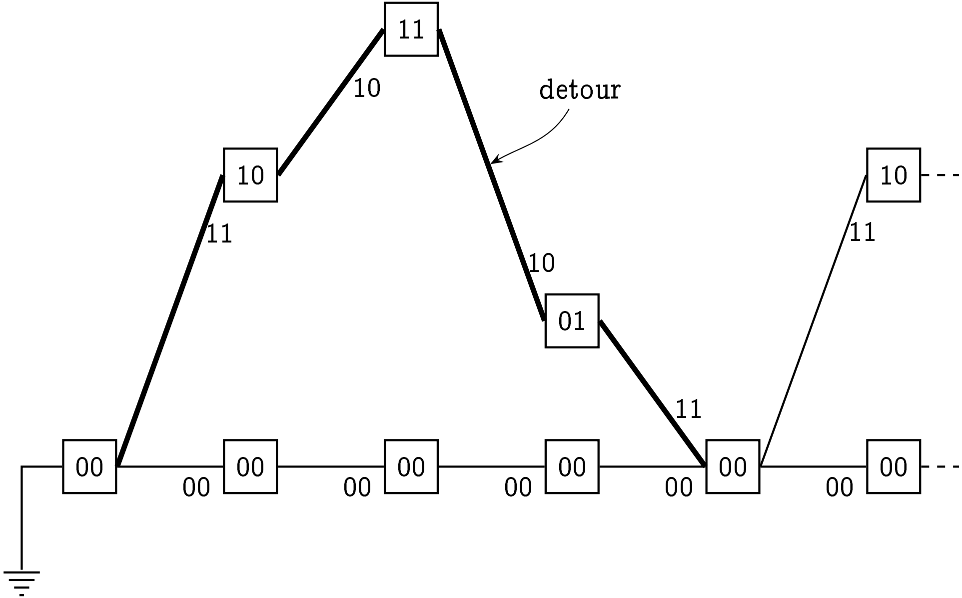

0.91
0
0
0.02
0.07
X
?
Y
0.07
0.02
1
1
0.91

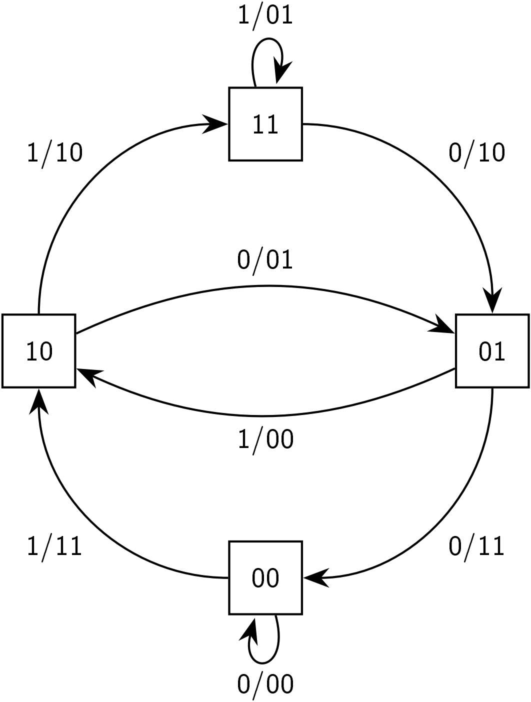
	$y = 0$	$y = ?$	$y = 1$
$x = 0$	$\log 0.91 - \log 0.02$ ≈ 5.50	$\log 0.07 - \log 0.07$ $= 0$	$\log 0.02 - \log 0.02$ $= 0$
$x = 1$	$\log 0.02 - \log 0.02$ $= 0$	$\log 0.07 - \log 0.07$ $= 0$	$\log 0.91 - \log 0.02$ ≈ 5.50

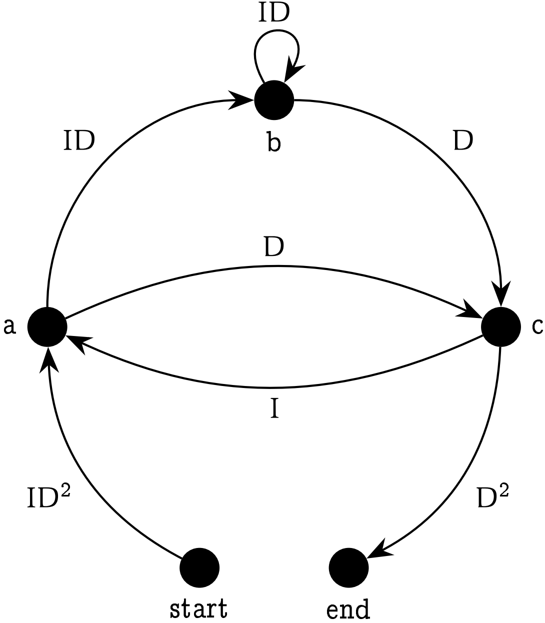
	$y=0$	$y=?$	$y=1$
$x=0$	1	0	0
$x=1$	0	0	1

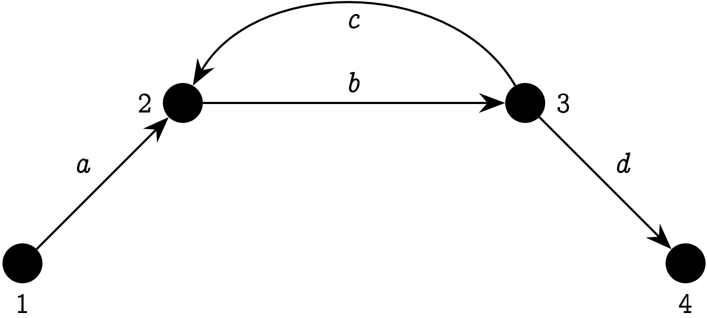


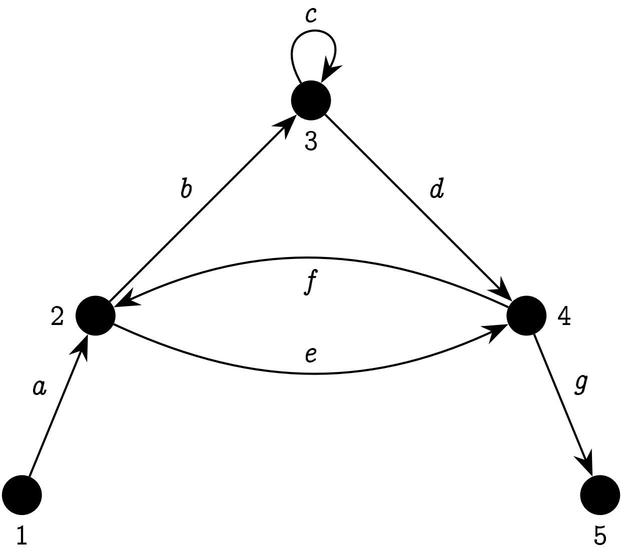
$\mathbf{y} =$	01	?1	1?	01	11
$\hat{\mathbf{x}} =$	11	01	00	01	11
	00	00	11	01	11
$\hat{\mathbf{u}} =$	1	0	1		
	0	0	1		

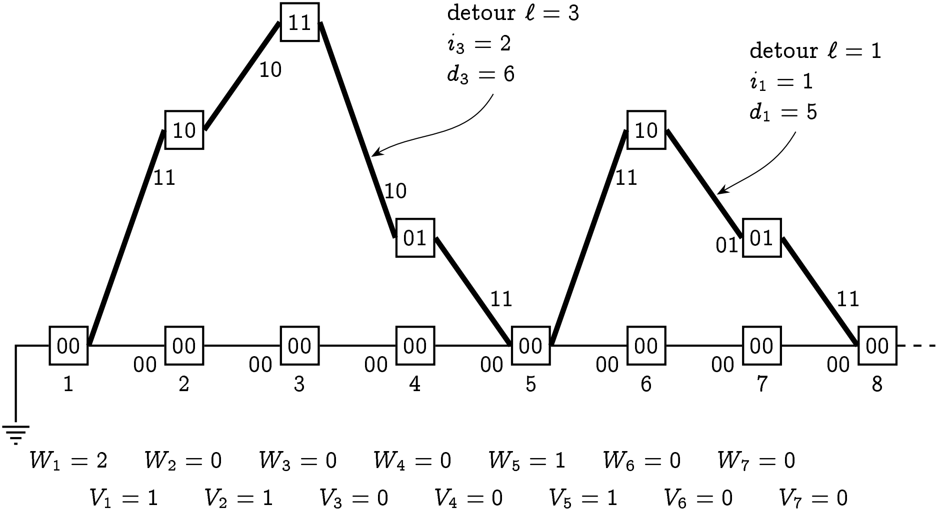

11
detour
10
10
11
10
01
11
11
10
00
00
00
00
00
00
00
00
00
00
00
00

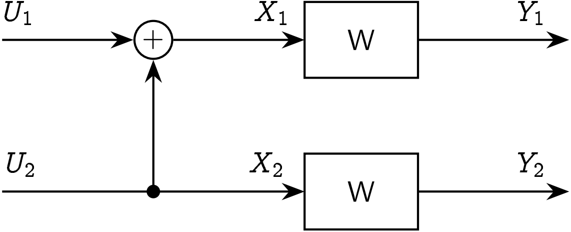

1/01
11
1/10
0/10
0/01
10
01
1/00
1/11
0/11
00
0/00


ID
b
ID
D
D
a
c
I
ID^2
D^2
start
end

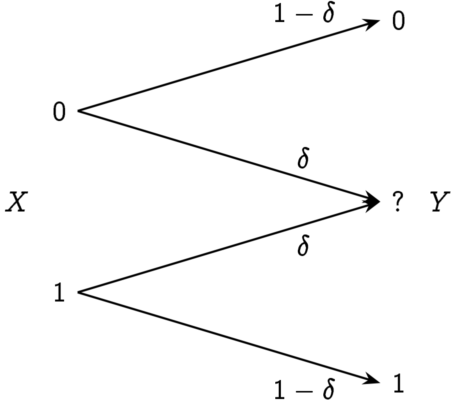

c
b
2
3
a
d
1
4


c
3
b
d
f
2
4
e
a
g
1
5

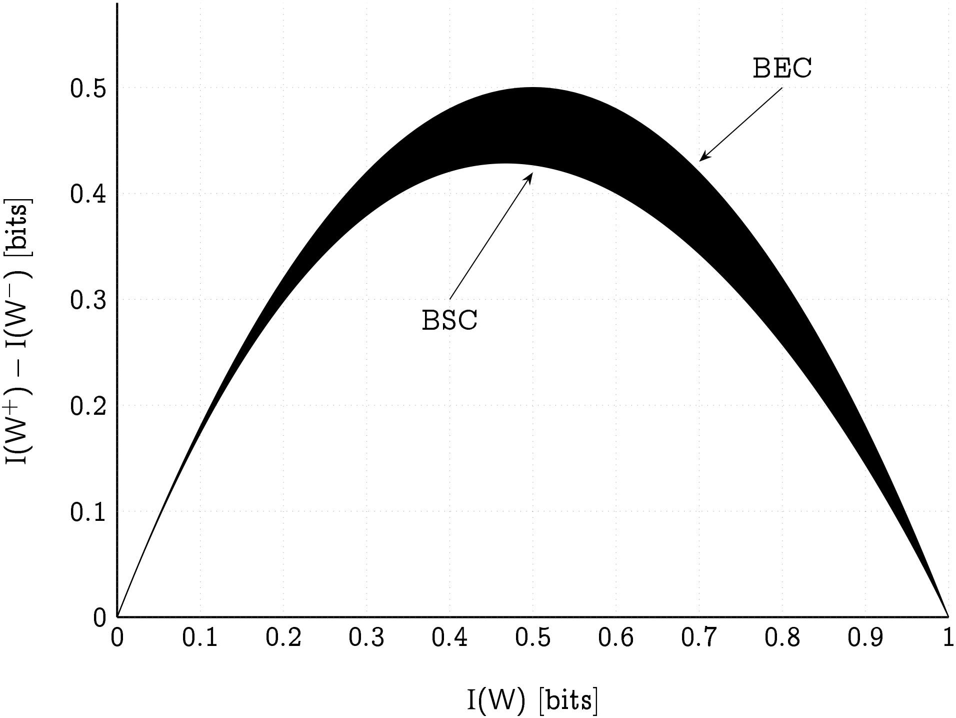

detour $\ell = 3$
$i_3 = 2$
$d_3 = 6$
detour $\ell = 1$
$i_1 = 1$
$d_1 = 5$
11
10
10
11
11
01
11
00
00
00
00
00
00
00
00
00
00
00
00
00
00
00
10
11
01
10
01
00
1
2
3
4
5
6
7
8
$W_1 = 2$ $W_2 = 0$ $W_3 = 0$ $W_4 = 0$ $W_5 = 1$ $W_6 = 0$ $W_7 = 0$
$V_1 = 1$ $V_2 = 1$ $V_3 = 0$ $V_4 = 0$ $V_5 = 1$ $V_6 = 0$ $V_7 = 0$

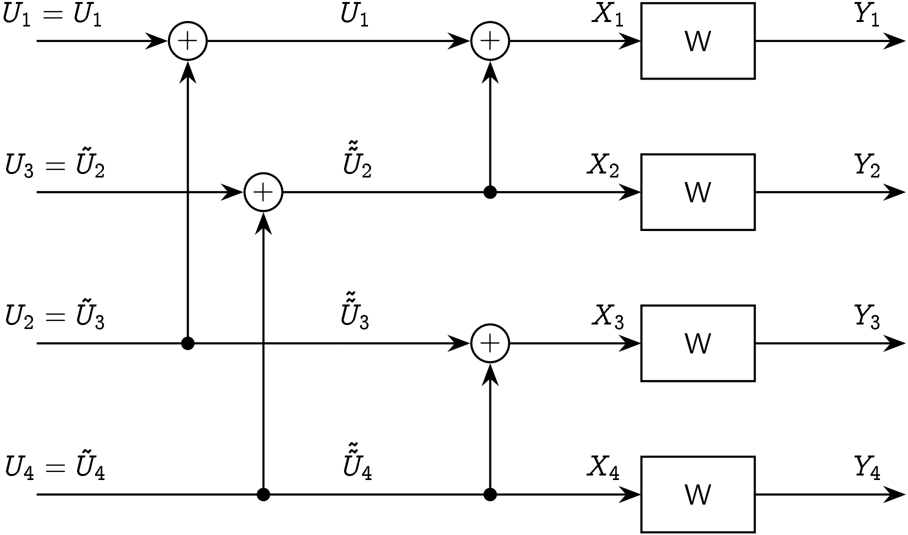


U_1
X_1
W
Y_1
U_2
X_2
W
Y_2

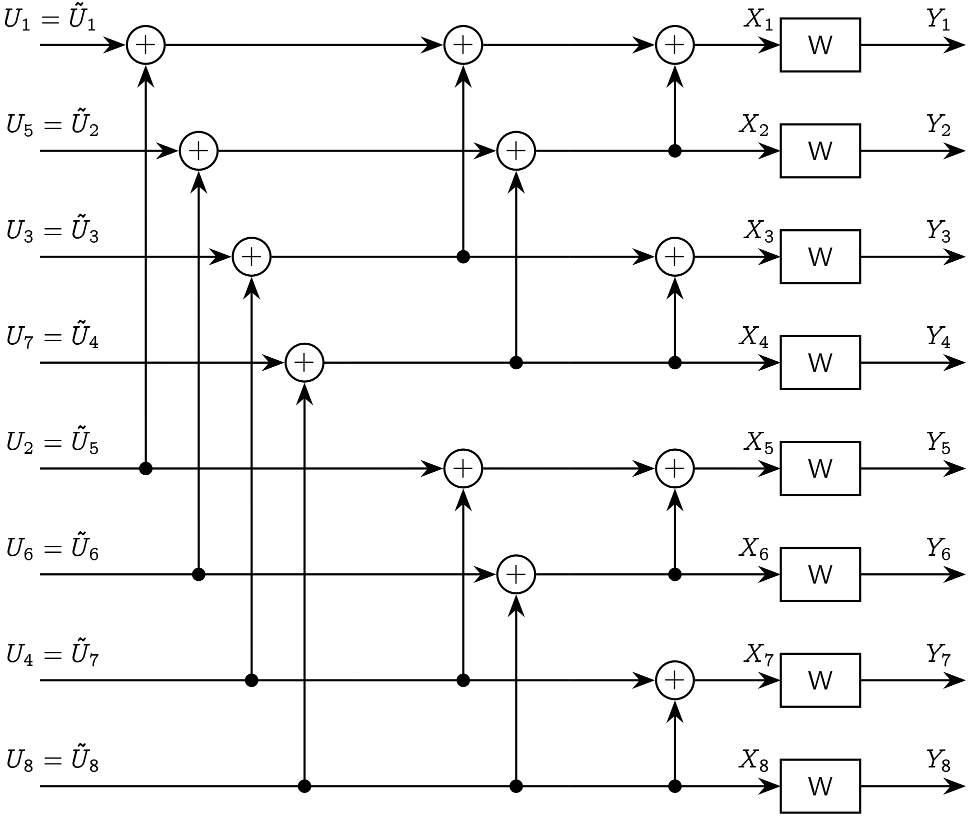

$1-\delta$
0
0
δ
X
?
Y
δ
1
$1-\delta$
1

y_1	y_2	$W^-(y_1, y_2 \mid 0)$	$W^-(y_1, y_2 \mid 1)$
0	0	$(1-\delta)^2/2$	0
0	?	$\delta(1-\delta)/2$	$\delta(1-\delta)/2$
0	1	0	$(1-\delta)^2/2$
?	0	$\delta(1-\delta)/2$	$\delta(1-\delta)/2$
?	?	δ^2	δ^2
?	1	$\delta(1-\delta)/2$	$\delta(1-\delta)/2$
1	0	0	$(1-\delta)^2/2$
1	?	$\delta(1-\delta)/2$	$\delta(1-\delta)/2$
1	1	$(1-\delta)^2/2$	0

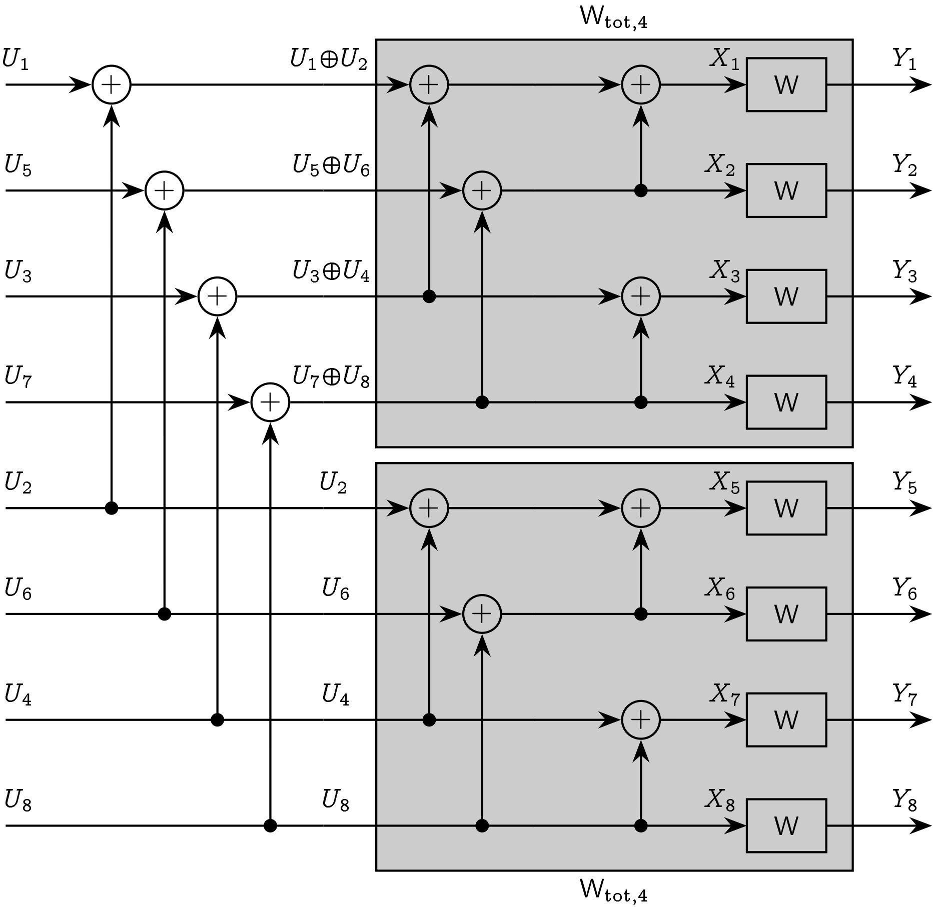

BEC
BSC
0.5
0.4
0.3
0.2
0.1
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
I(W⁺) − I(W⁻) [bits]
I(W) [bits]

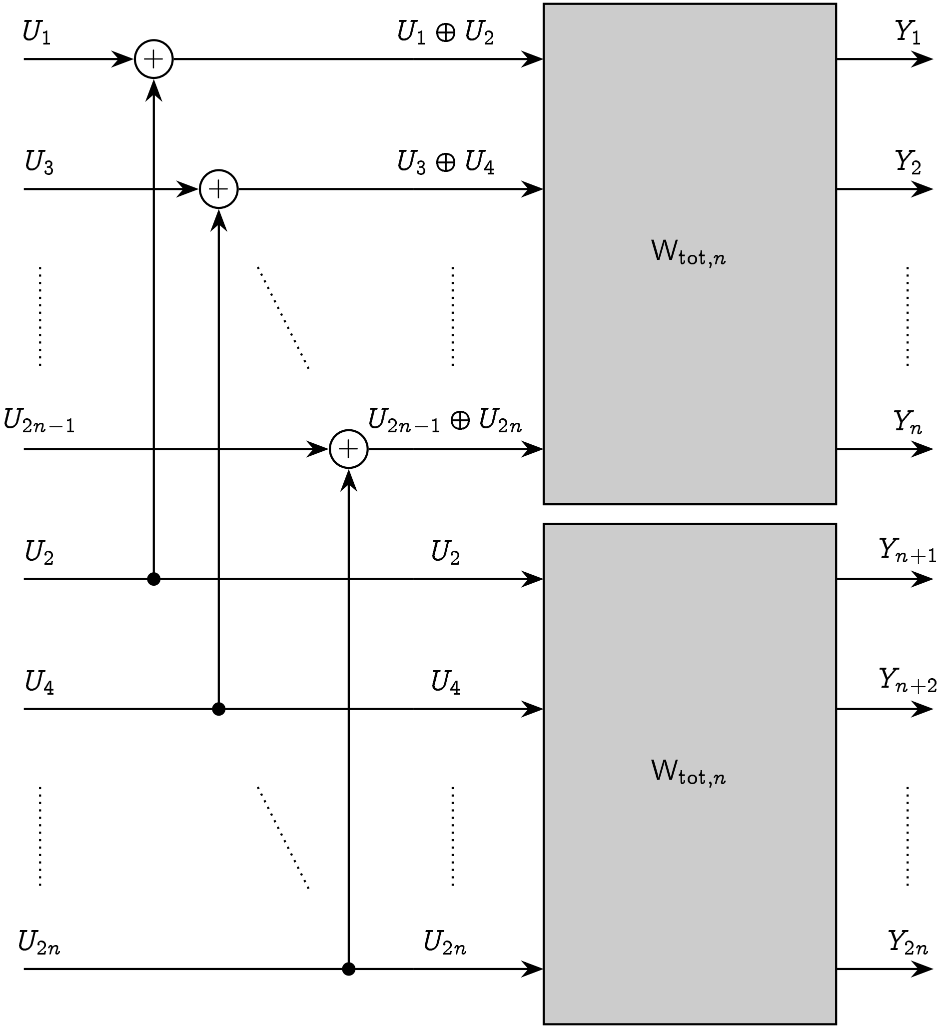


$U_1 = \tilde{U}_1$
$\tilde{\tilde{U}}_1$
X_1
W
Y_1
$U_3 = \tilde{U}_2$
$\tilde{\tilde{U}}_2$
X_2
W
Y_2
$U_2 = \tilde{U}_3$
$\tilde{\tilde{U}}_3$
X_3
W
Y_3
$U_4 = \tilde{U}_4$
$\tilde{\tilde{U}}_4$
X_4
W
Y_4

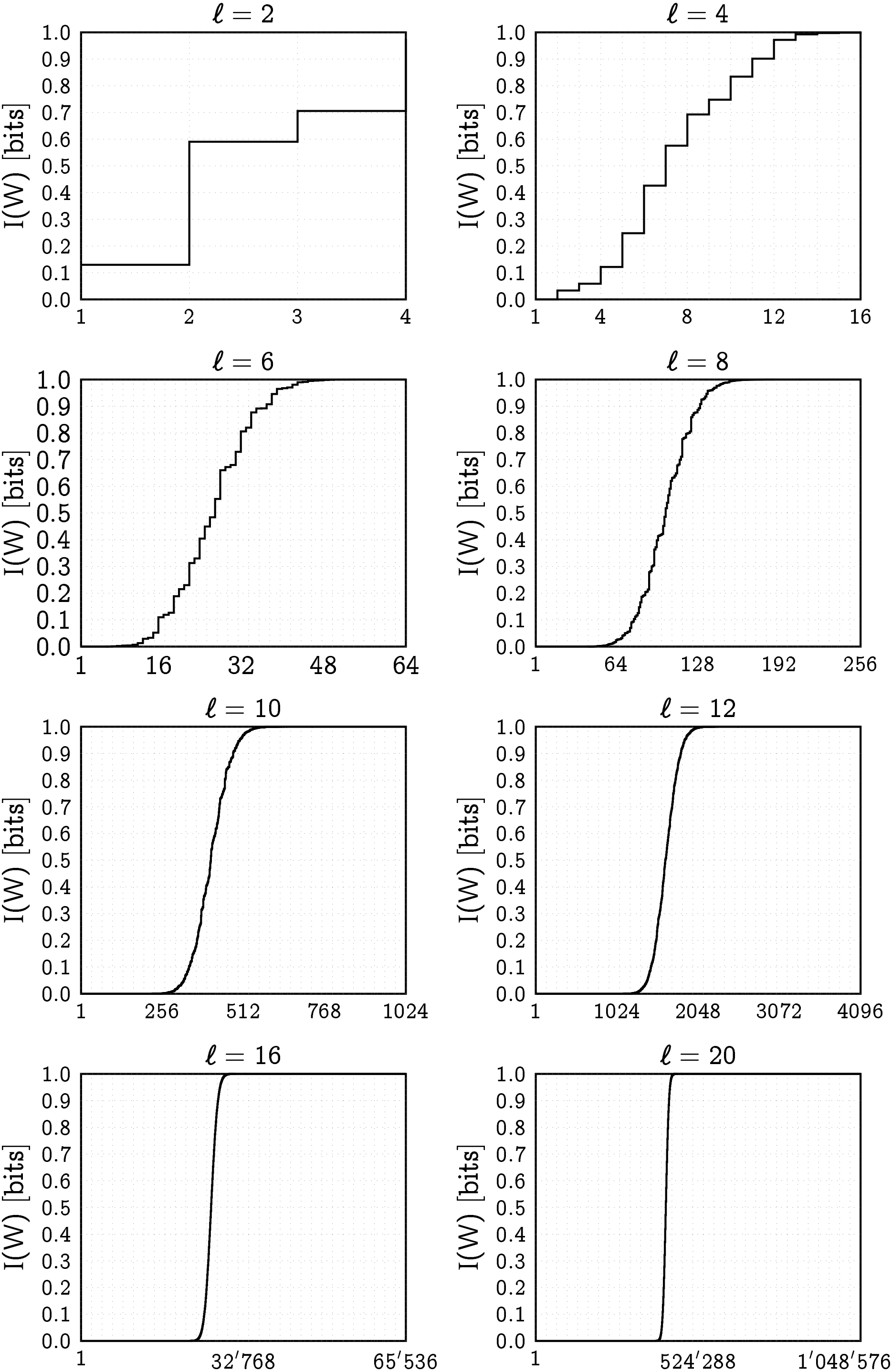


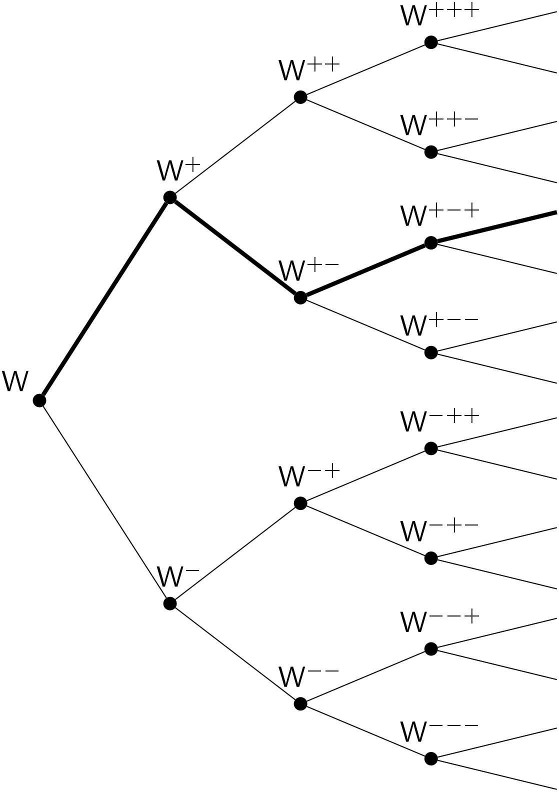
$U_1 = \tilde{U}_1$
$U_5 = \tilde{U}_2$
$U_3 = \tilde{U}_3$
$U_7 = \tilde{U}_4$
$U_2 = \tilde{U}_5$
$U_6 = \tilde{U}_6$
$U_4 = \tilde{U}_7$
$U_8 = \tilde{U}_8$
X_1
X_2
X_3
X_4
X_5
X_6
X_7
X_8
W
W
W
W
W
W
W
W
Y_1
Y_2
Y_3
Y_4
Y_5
Y_6
Y_7
Y_8

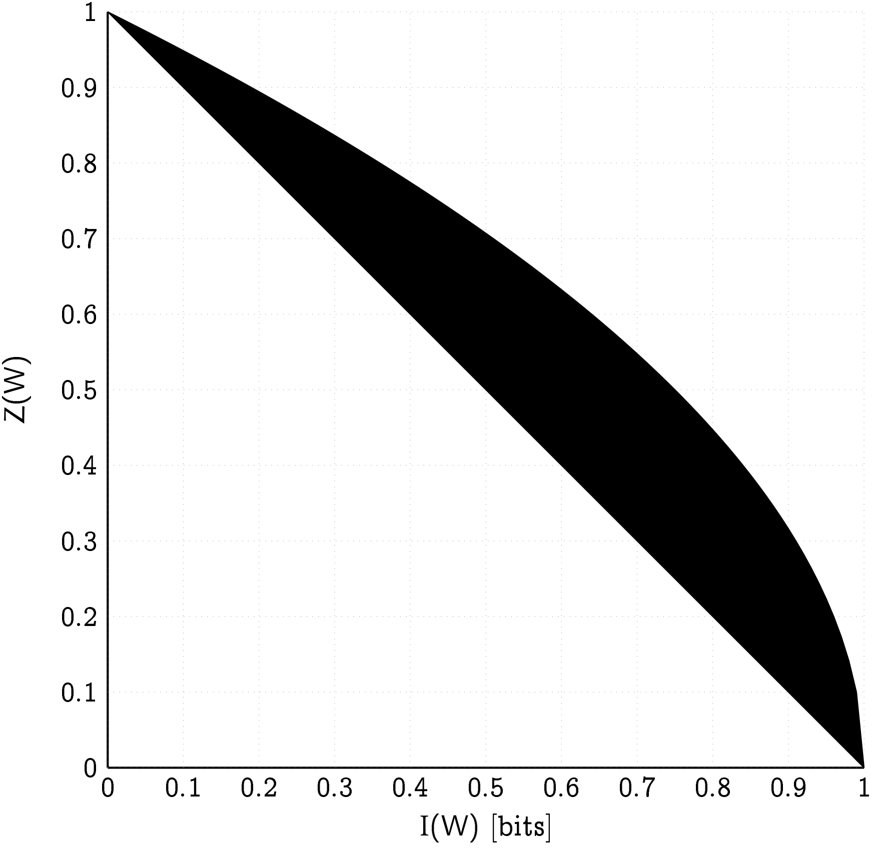

W_tot,4
U1
U1⊕U2
X1
Y1
W
U5
U5⊕U6
X2
Y2
W
U3
U3⊕U4
X3
Y3
W
U7
U7⊕U8
X4
Y4
W
U2
U2
X5
Y5
W
U6
U6
X6
Y6
W
U4
U4
X7
Y7
W
U8
U8
X8
Y8
W
W_tot,4



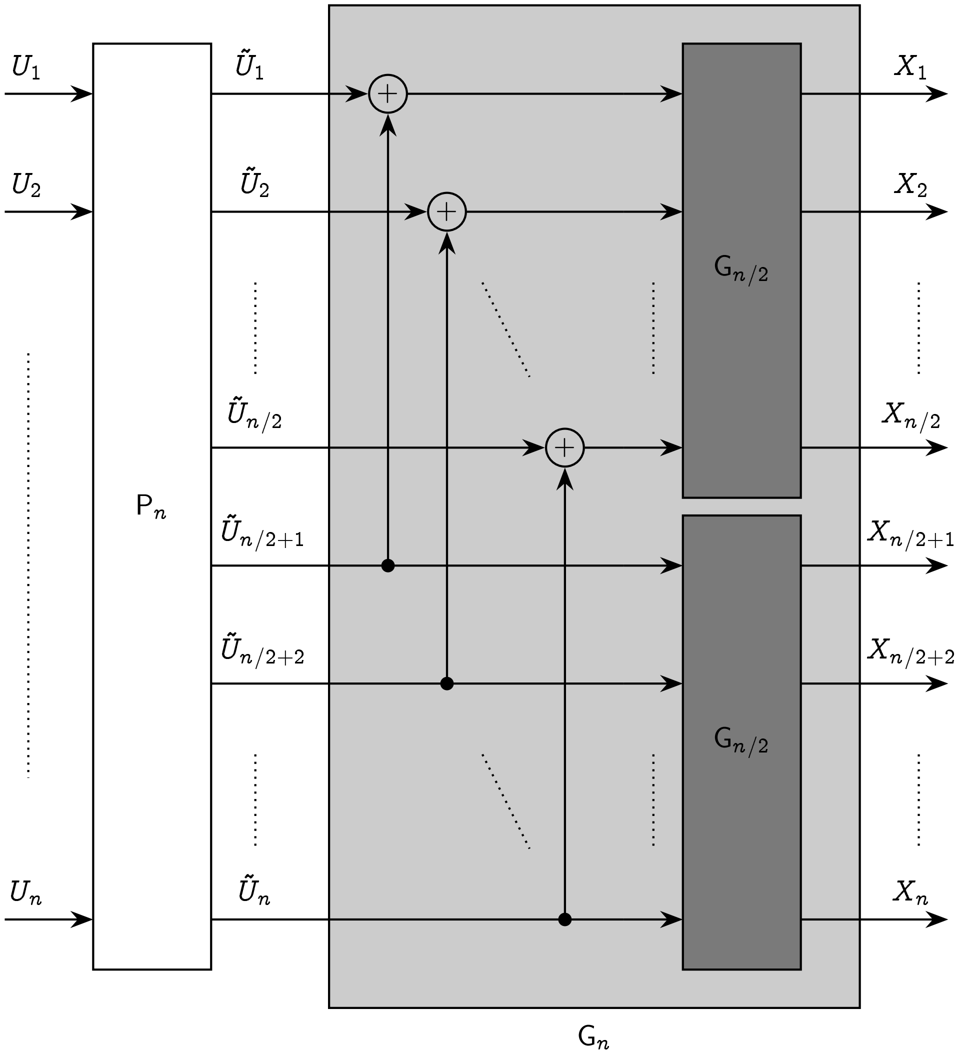
U_1
$U_1 \oplus U_2$
Y_1
U_3
$U_3 \oplus U_4$
Y_2
$\mathsf{W}_{\mathsf{tot},n}$
U_{2n-1}
$U_{2n-1} \oplus U_{2n}$
Y_n
U_2
U_2
Y_{n+1}
U_4
U_4
Y_{n+2}
$\mathsf{W}_{\mathsf{tot},n}$
U_{2n}
U_{2n}
Y_{2n}


ℓ = 2
ℓ = 4
ℓ = 6
ℓ = 8
ℓ = 10
ℓ = 12
ℓ = 16
ℓ = 20
I(W) [bits]
1.0 0.9 0.8 0.7 0.6 0.5 0.4 0.3 0.2 0.1 0.0
1 2 3 4
1 4 8 12 16
1 16 32 48 64
1 64 128 192 256
1 256 512 768 1024
1 1024 2048 3072 4096
1 32′768 65′536
1 524′288 1′048′576

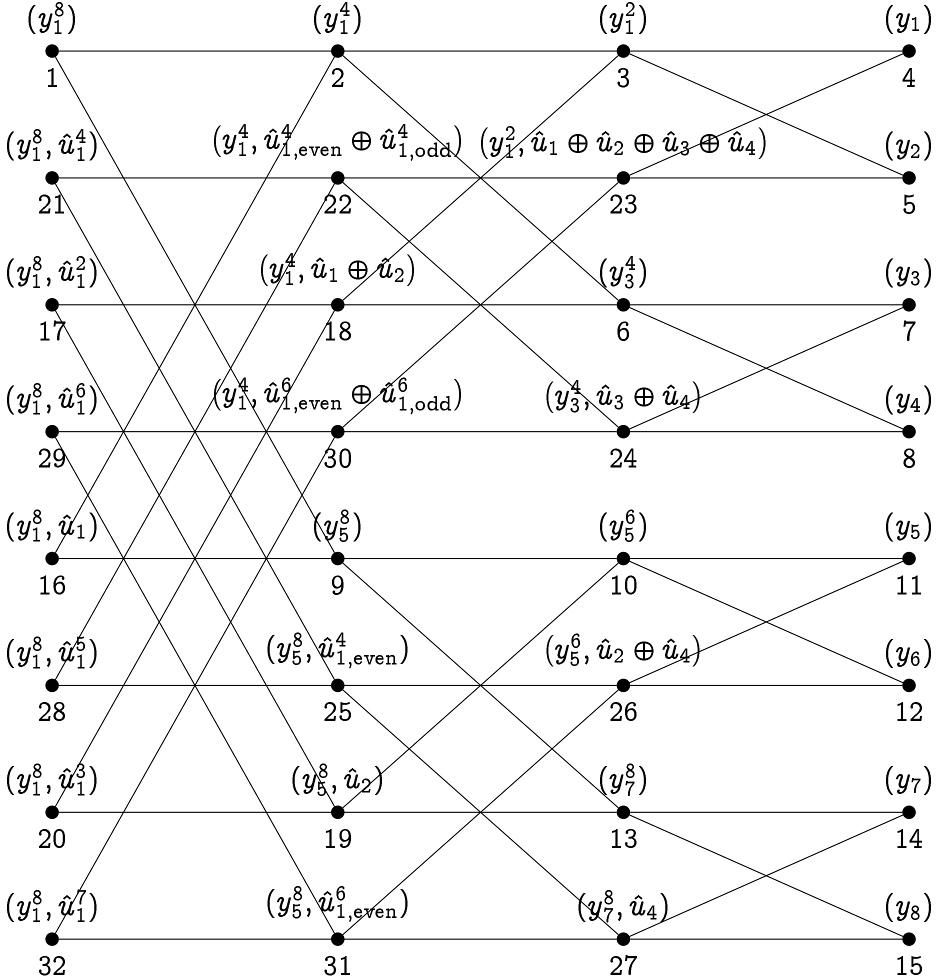

W
W^{+}
W^{-}
W^{++}
W^{+-}
W^{-+}
W^{--}
W^{+++}
W^{++-}
W^{+-+}
W^{+--}
W^{-++}
W^{-+-}
W^{--+}
W^{---}



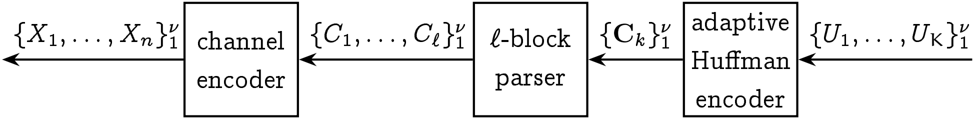
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
Z(W)
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
I(W) [bits]

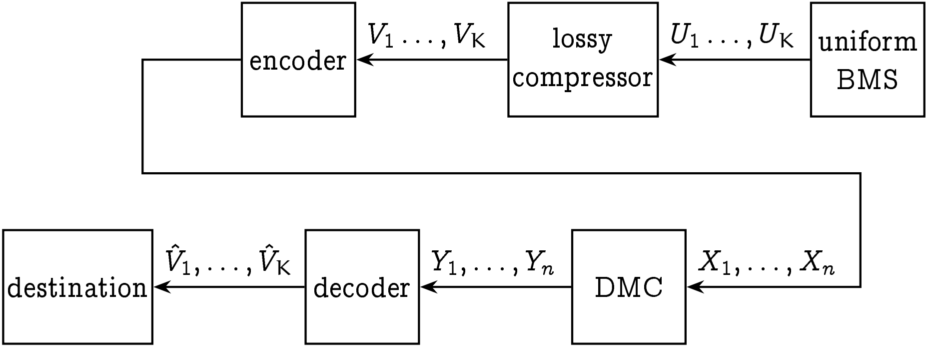


U_1
U_2
U_n
P_n
$\tilde{U}_1$
$\tilde{U}_2$
$\tilde{U}_{n/2}$
$\tilde{U}_{n/2+1}$
$\tilde{U}_{n/2+2}$
$\tilde{U}_n$
$\mathsf{G}_{n/2}$
$\mathsf{G}_{n/2}$
X_1
X_2
$X_{n/2}$
$X_{n/2+1}$
$X_{n/2+2}$
X_n
G_n

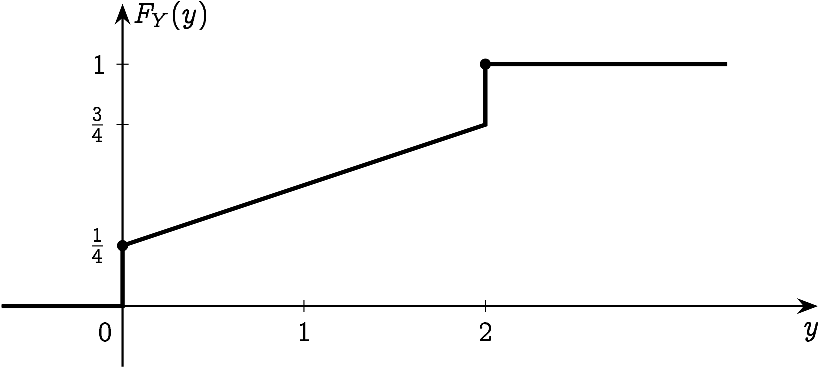

(y_1^8)
1
(y_1^4)
2
(y_1^2)
3
(y_1)
4
$(y_1^8, \hat{u}_1^4)$
21
$(y_1^4, \hat{u}_{1,\text{even}}^4 \oplus \hat{u}_{1,\text{odd}}^4)$
22
$(y_1^2, \hat{u}_1 \oplus \hat{u}_2 \oplus \hat{u}_3 \oplus \hat{u}_4)$
23
(y_2)
5
$(y_1^8, \hat{u}_1^2)$
17
$(y_1^4, \hat{u}_1 \oplus \hat{u}_2)$
18
(y_3^4)
6
(y_3)
7
$(y_1^8, \hat{u}_1^6)$
29
$(y_1^4, \hat{u}_{1,\text{even}}^6 \oplus \hat{u}_{1,\text{odd}}^6)$
30
$(y_3^4, \hat{u}_3 \oplus \hat{u}_4)$
24
(y_4)
8
$(y_1^8, \hat{u}_1)$
16
(y_5^8)
9
(y_5^6)
10
(y_5)
11
$(y_1^8, \hat{u}_1^5)$
28
$(y_5^8, \hat{u}_{1,\text{even}}^4)$
25
$(y_5^6, \hat{u}_2 \oplus \hat{u}_4)$
26
(y_6)
12
$(y_1^8, \hat{u}_1^3)$
20
$(y_5^8, \hat{u}_2)$
19
(y_7^8)
13
(y_7)
14
$(y_1^8, \hat{u}_1^7)$
32
$(y_5^8, \hat{u}_{1,\text{even}}^6)$
31
$(y_7^8, \hat{u}_4)$
27
(y_8)
15

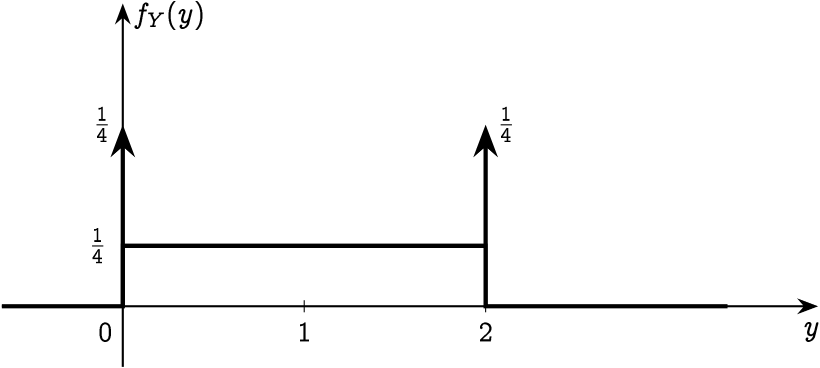

dest.
$\hat{U}_1, \ldots, \hat{U}_K$
decoder
$Y_1, \ldots, Y_n$
DMC
$X_1, \ldots, X_n$
encoder
$U_1, \ldots, U_K$
DSS

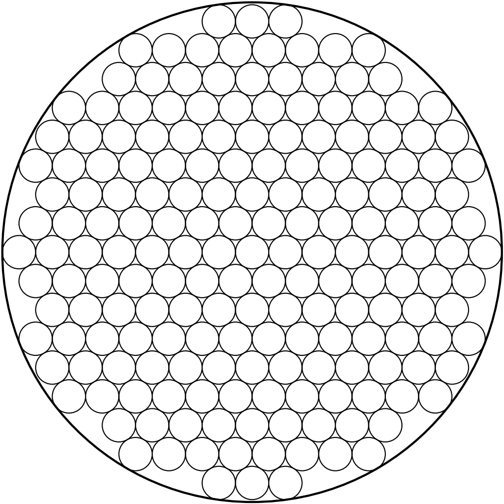

$\{X_1, \ldots, X_n\}_1^\nu$
channel encoder
$\{C_1, \ldots, C_\ell\}_1^\nu$
ℓ-block parser
$\{\mathbf{C}_k\}_1^\nu$
adaptive Huffman encoder
$\{U_1, \ldots, U_\mathsf{K}\}_1^\nu$



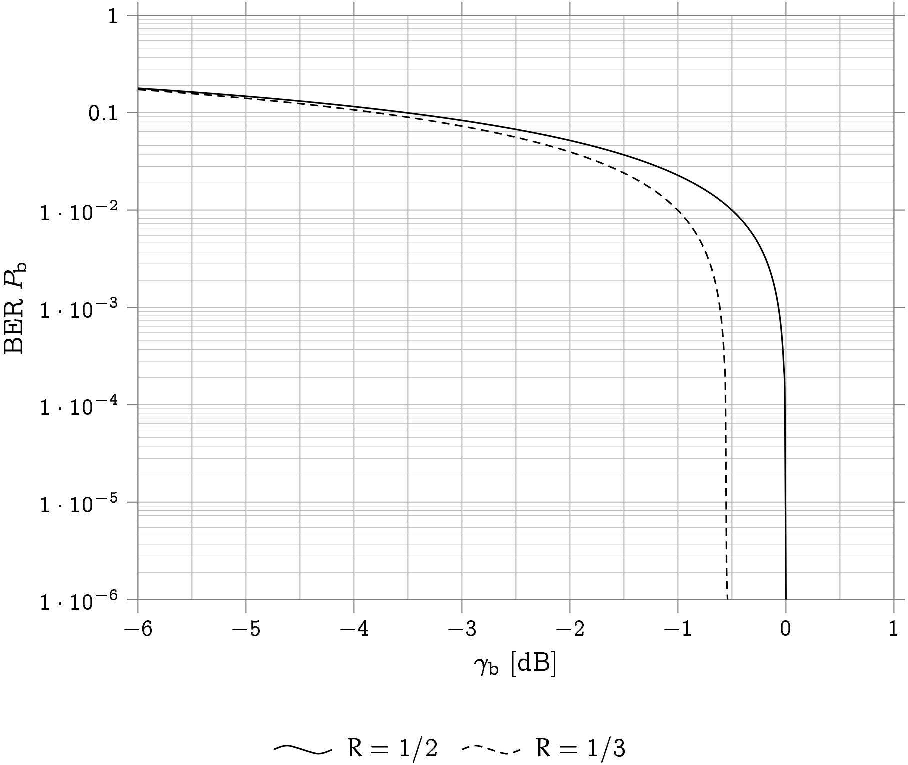
encoder
$V_1 \ldots, V_K$
lossy compressor
$U_1 \ldots, U_K$
uniform BMS
destination
$\hat{V}_1, \ldots, \hat{V}_K$
decoder
$Y_1, \ldots, Y_n$
DMC
$X_1, \ldots, X_n$


$F_Y(y)$
1
$\frac{3}{4}$
$\frac{1}{4}$
0
1
2
y

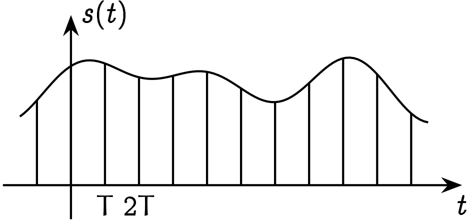

$f_Y(y)$
$\frac{1}{4}$
$\frac{1}{4}$
$\frac{1}{4}$
0
1
2
y

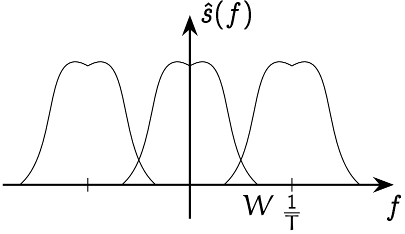


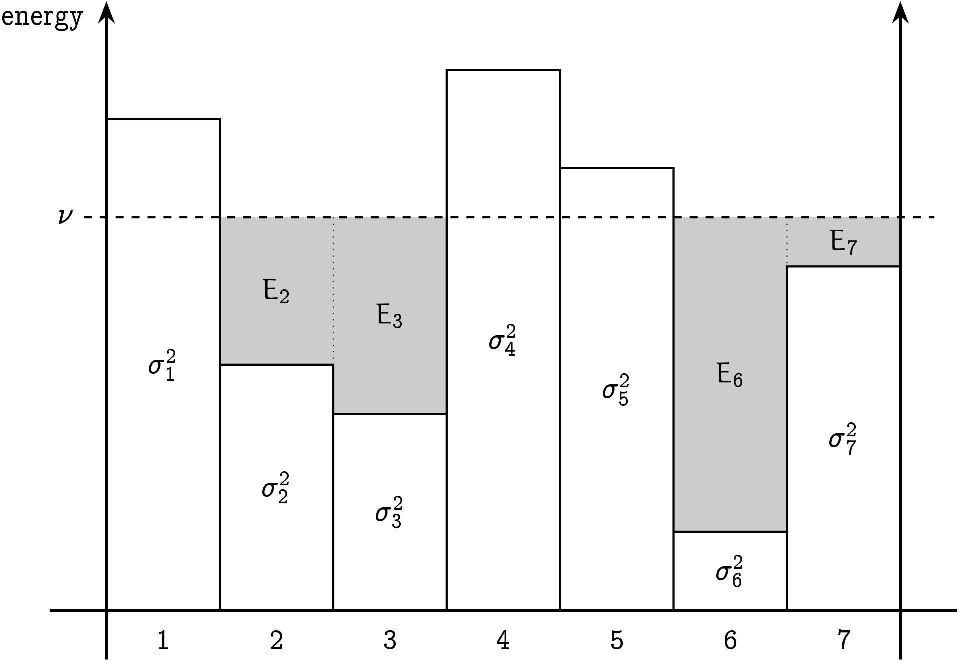

dest.
$\hat{U}_1, \ldots, \hat{U}_\mathsf{K}$
decoder
$Y_1, \ldots, Y_n$
Gauss. channel
$X_1, \ldots, X_n$
encoder
$U_1, \ldots, U_\mathsf{K}$
DSS

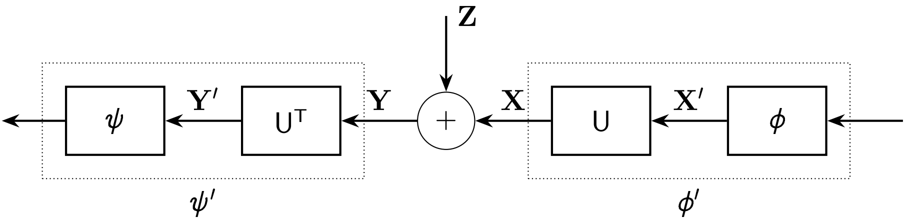


1
0.1
1 · 10^−2
1 · 10^−3
1 · 10^−4
1 · 10^−5
1 · 10^−6
BER P_b
−6
−5
−4
−3
−2
−1
0
1
γ_b [dB]
R = 1/2
R = 1/3

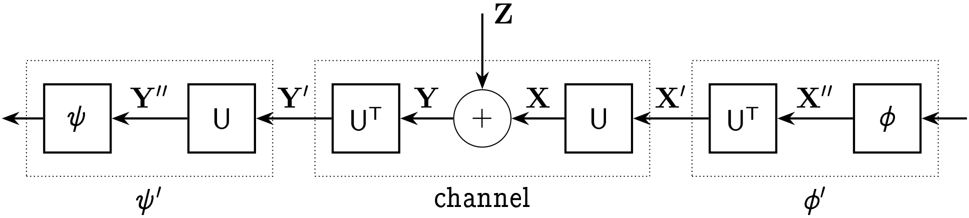

$s(t)$
T 2T
t

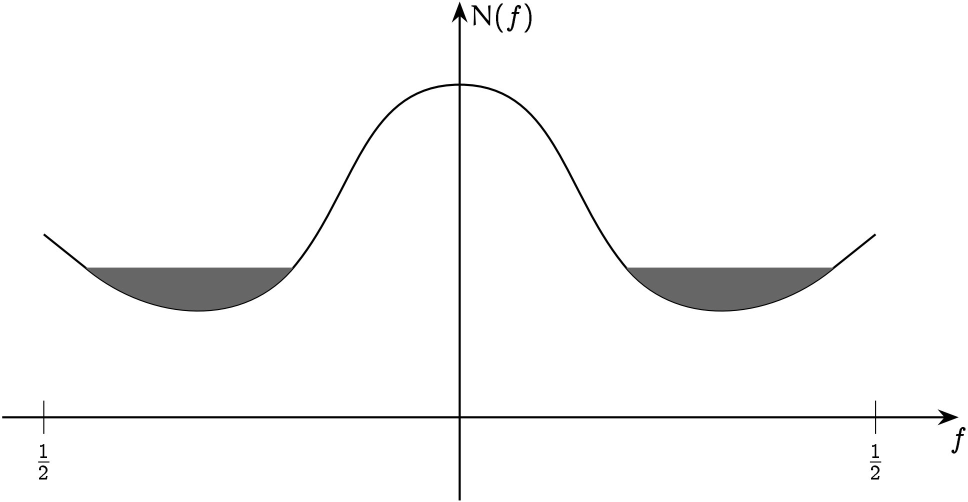

$\hat{s}(f)$
W
$\frac{1}{T}$
f

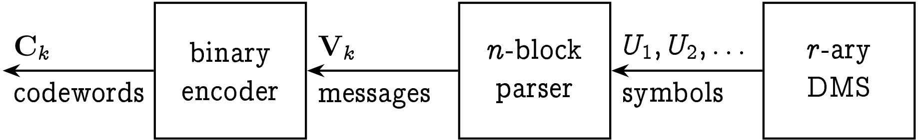

energy
ν
E_2
E_3
E_6
E_7
σ_1^2
σ_2^2
σ_3^2
σ_4^2
σ_5^2
σ_6^2
σ_7^2
1
2
3
4
5
6
7



Z
ψ
$\mathbf{Y}'$
U^T
$\mathbf{Y}$
+
$\mathbf{X}$
U
$\mathbf{X}'$
ϕ
ψ'
ϕ'

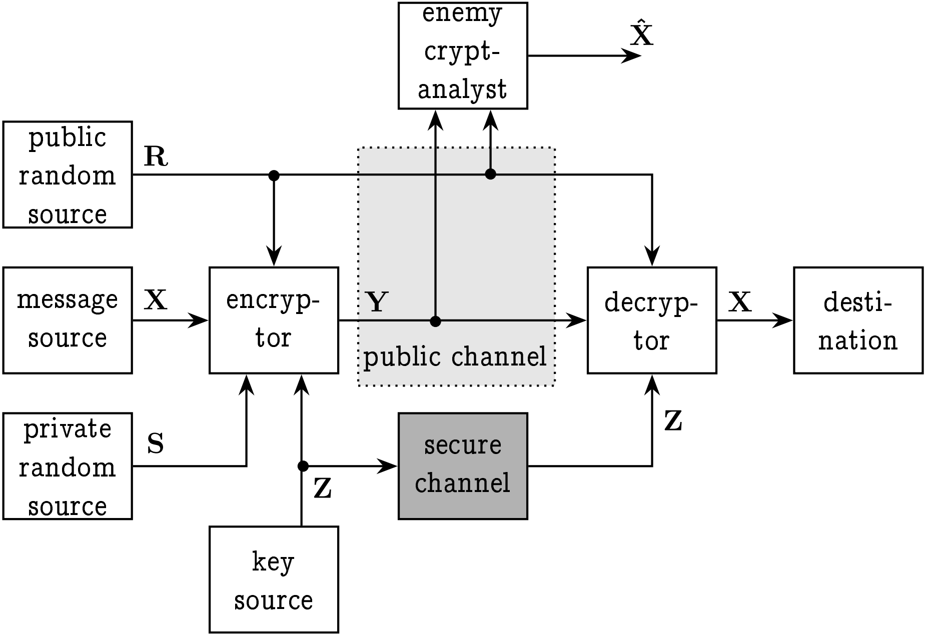

Z
Y''
Y'
Y
X
X'
X''
ψ
U
Uᵀ
+
U
Uᵀ
ϕ
ψ'
channel
ϕ'

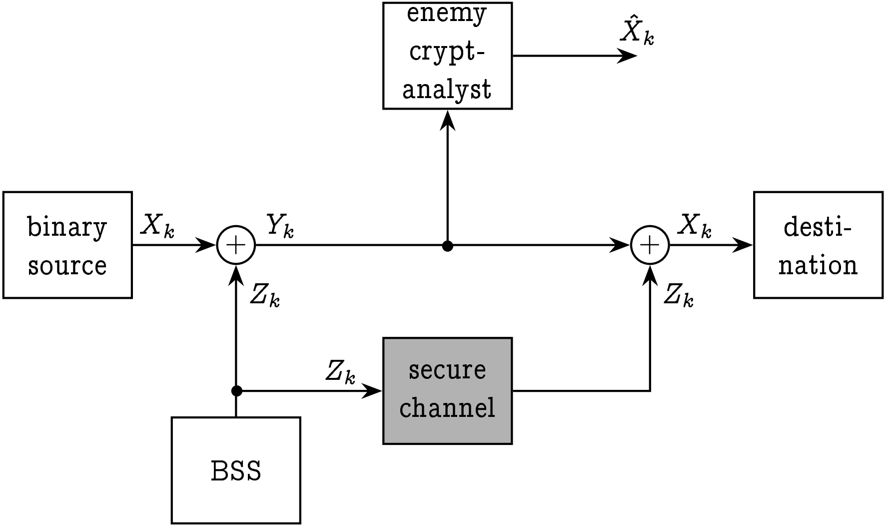

N(f)
f
1/2
1/2

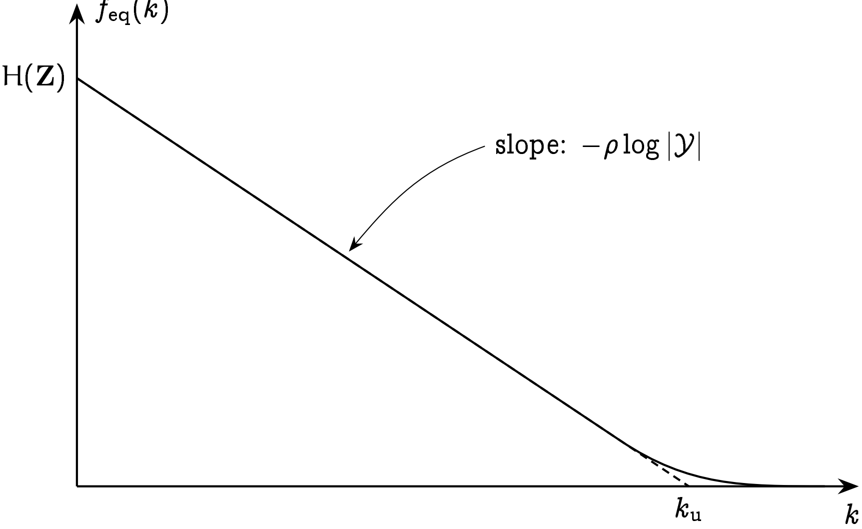


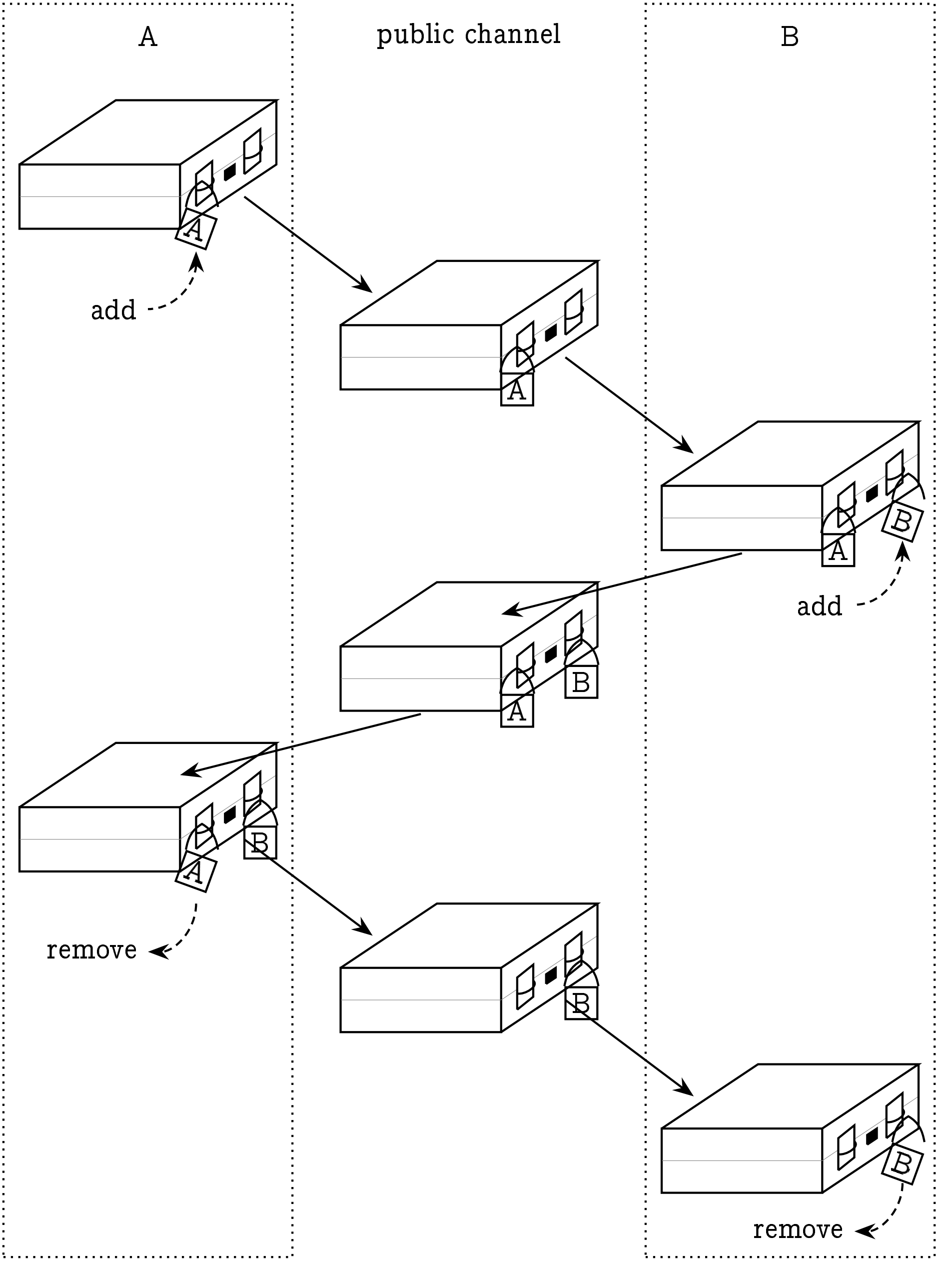
$\mathbf{C}_k$
codewords
binary
encoder
$\mathbf{V}_k$
messages
n-block
parser
$U_1, U_2, \ldots$
symbols
r-ary
DMS

$P_{X,Y}$	$Y=0$	$Y=1$	$Y=2$	P_X
$X=0$	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{3}{4}$
$X=1$	0	$\frac{1}{4}$	0	$\frac{1}{4}$
P_Y	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	

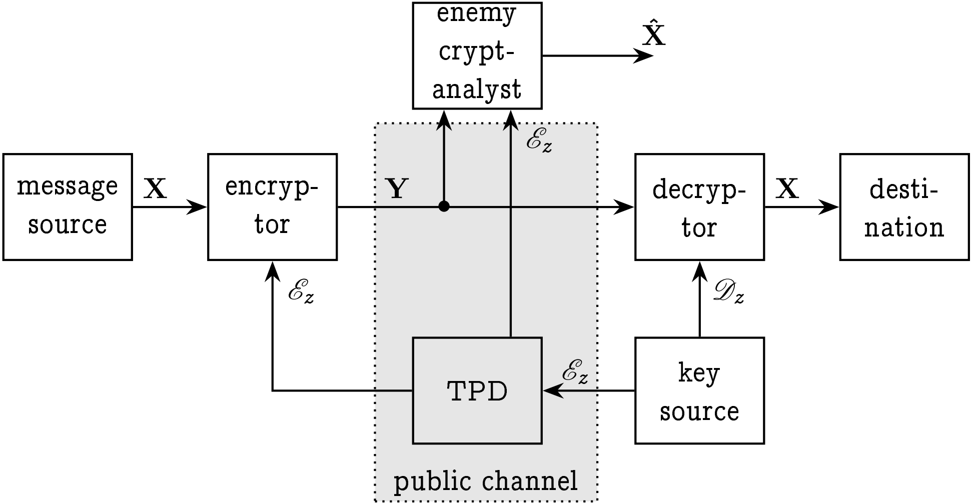

enemy crypt-analyst
$\hat{\mathbf{X}}$
public random source
R
message source
X
encryp-tor
Y
public channel
decryp-tor
X
desti-nation
private random source
S
Z
secure channel
Z
key source

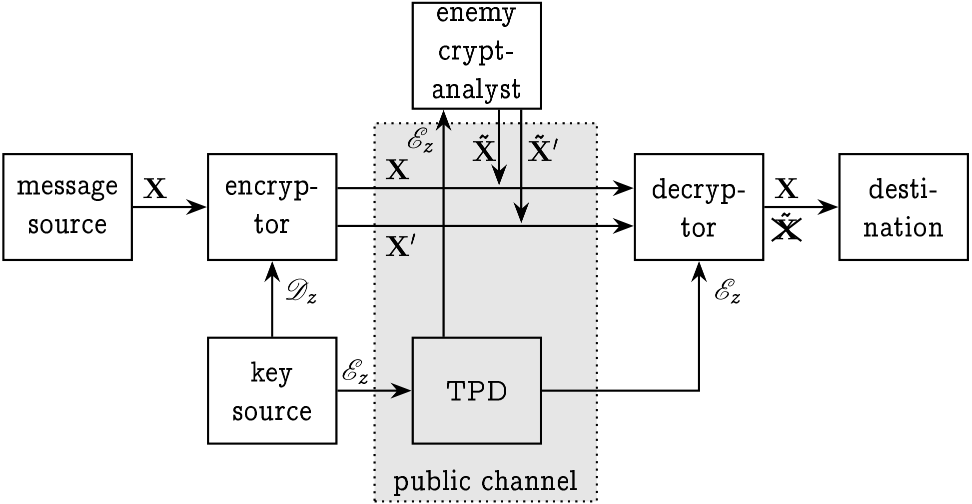

enemy
crypt-
analyst
$\hat{X}_k$
binary
source
X_k
Y_k
X_k
desti-
nation
Z_k
Z_k
Z_k
secure
channel
BSS

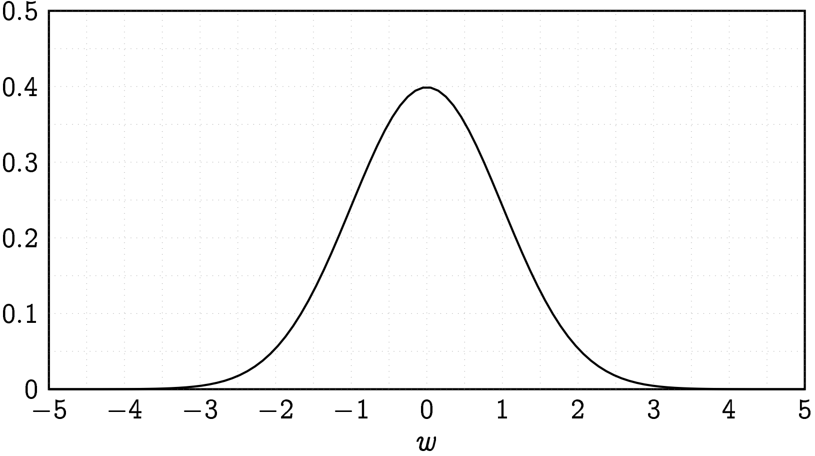

$f_{\text{eq}}(k)$
$\text{H}(\mathbf{Z})$
slope: $-\rho \log |\mathcal{Y}|$
k_{u}
k

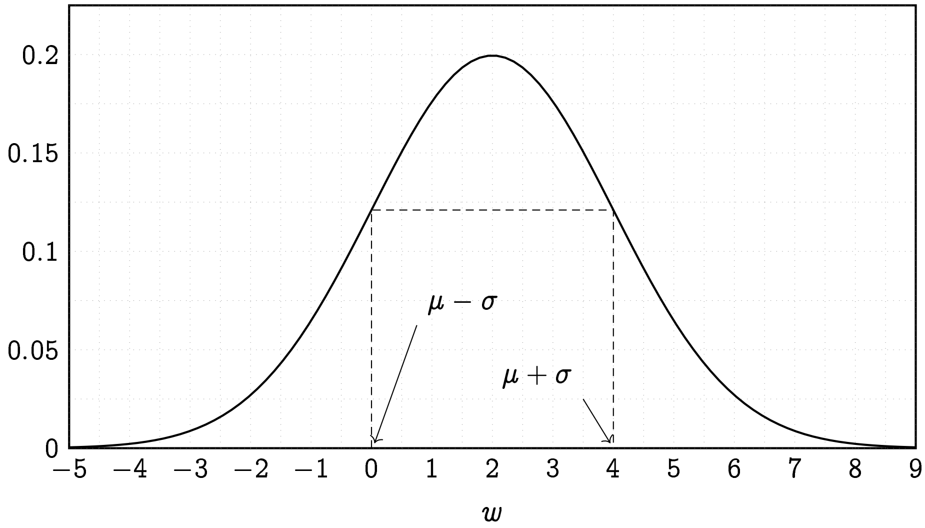


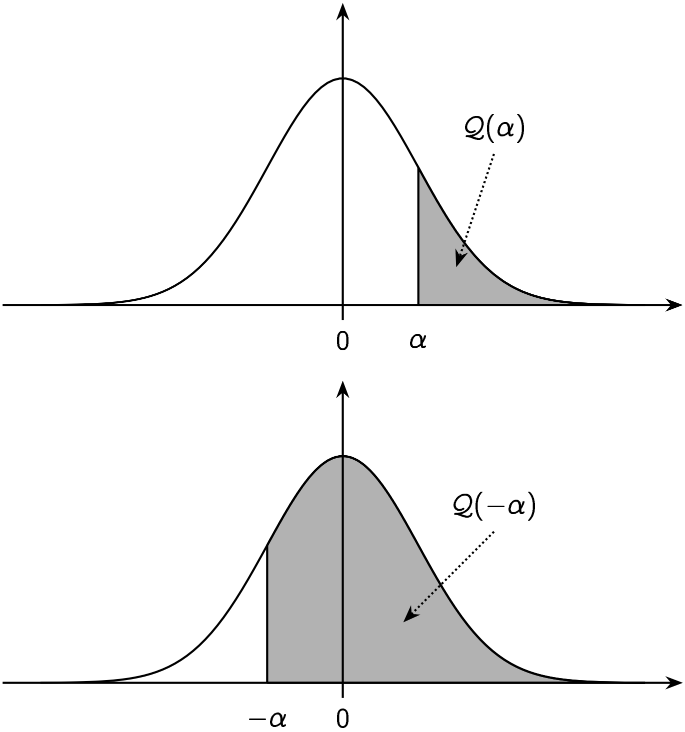
A
public channel
B
A
add
A
A
B
add
A
B
A
B
remove
B
B
remove


enemy crypt-analyst
$\hat{\mathbf{X}}$
$\mathscr{E}_z$
message source
$\mathbf{X}$
encryp-tor
$\mathbf{Y}$
decryp-tor
$\mathbf{X}$
desti-nation
$\mathscr{E}_z$
$\mathscr{D}_z$
TPD
$\mathscr{E}_z$
key source
public channel

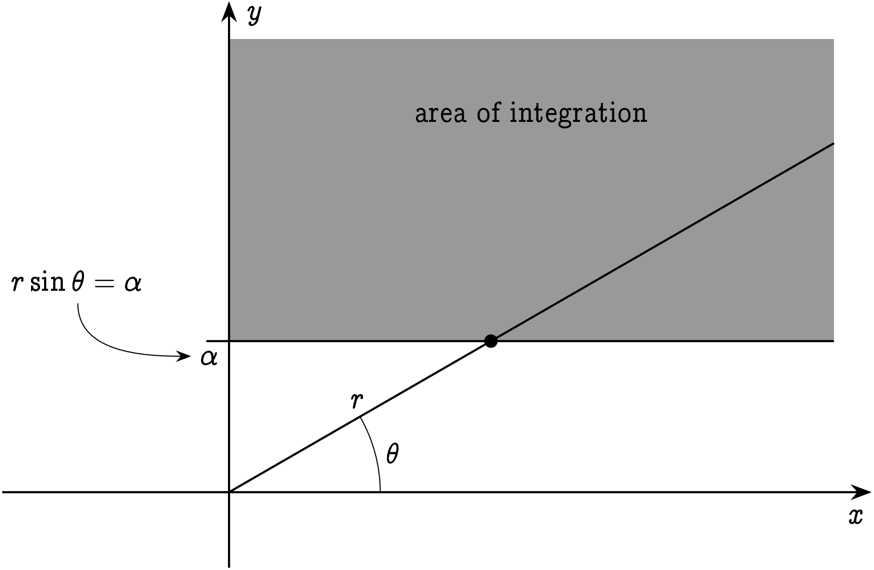

enemy
crypt-
analyst
message
source
X
encryp-
tor
X
X′
$\mathscr{E}_z$
$\tilde{\mathbf{X}}$
$\tilde{\mathbf{X}}'$
decryp-
tor
X
$\tilde{\mathbf{X}}$
desti-
nation
$\mathscr{D}_z$
$\mathscr{E}_z$
key
source
$\mathscr{E}_z$
TPD
public channel


0.5
0.4
0.3
0.2
0.1
0
−5
−4
−3
−2
−1
0
1
2
3
4
5
w

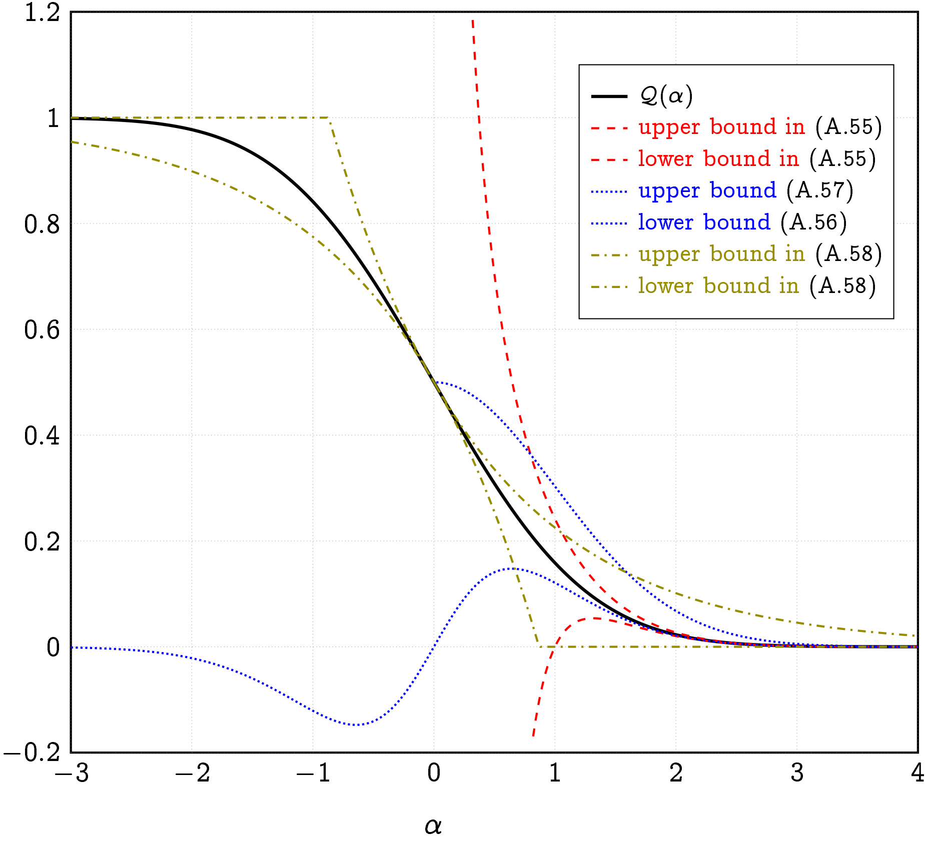

0.2
0.15
0.1
0.05
0
−5 −4 −3 −2 −1 0 1 2 3 4 5 6 7 8 9
w
μ − σ
μ + σ



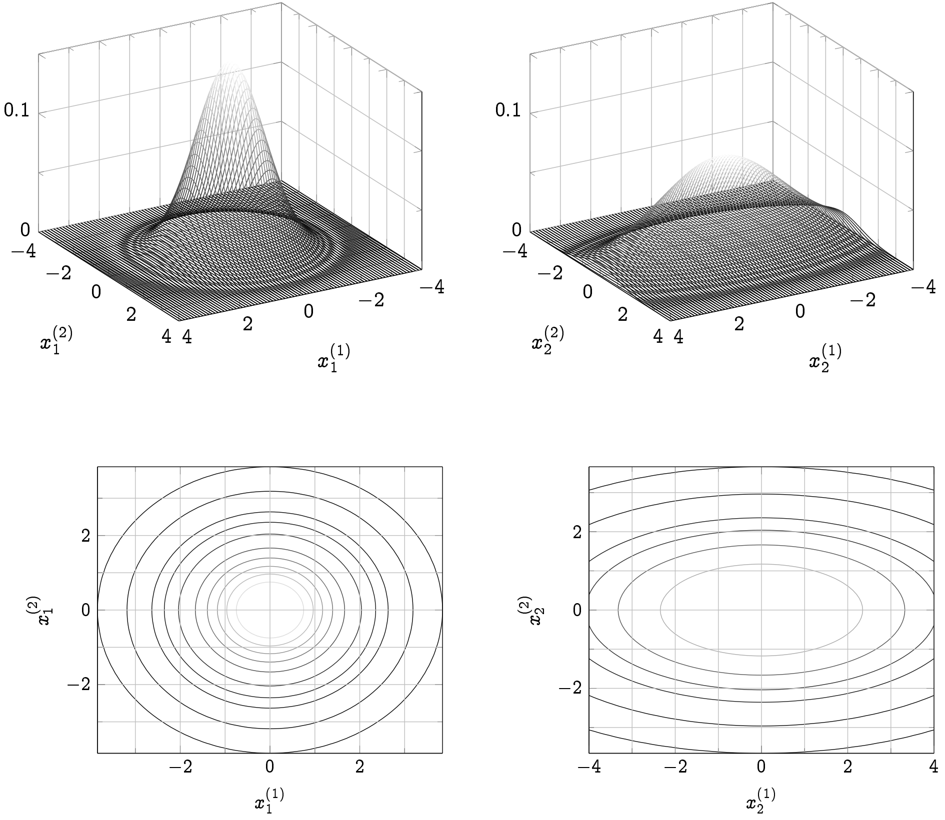
$\mathcal{Q}(\alpha)$
0
α
$\mathcal{Q}(-\alpha)$
$-\alpha$
0

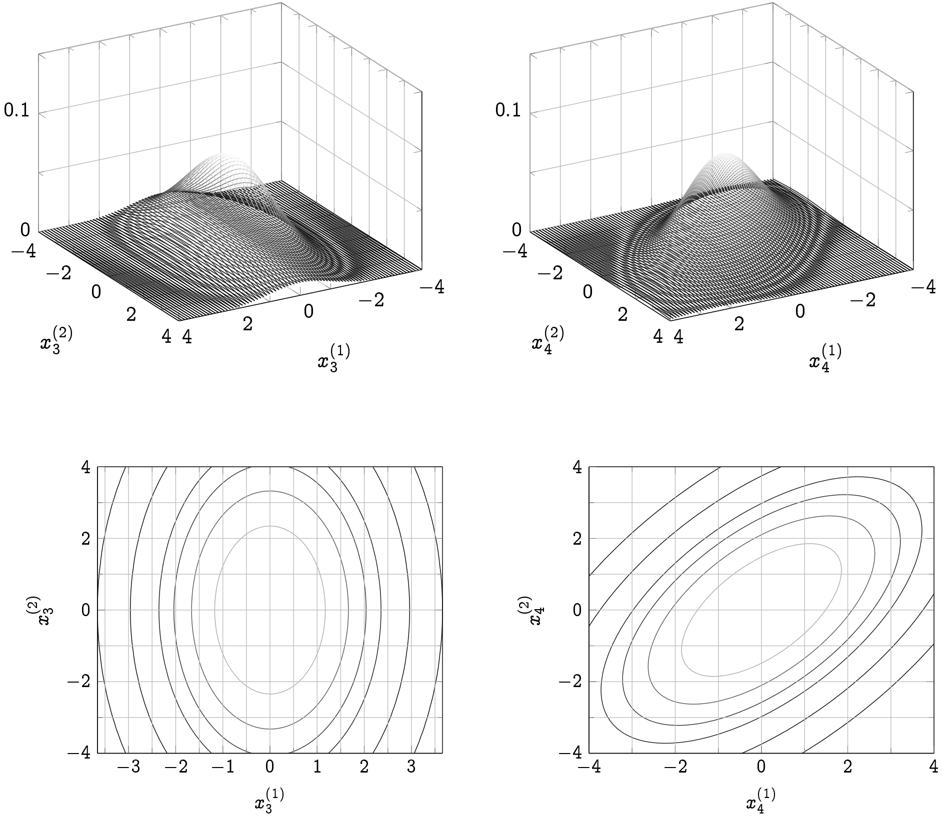


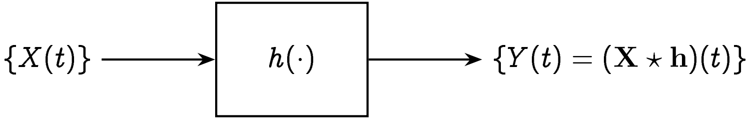
y
area of integration
$r \sin\theta = \alpha$
α
r
θ
x



1.2
1
0.8
0.6
0.4
0.2
0
−0.2
−3
−2
−1
0
1
2
3
4
α
Q(α)
upper bound in (A.55)
lower bound in (A.55)
upper bound (A.57)
lower bound (A.56)
upper bound in (A.58)
lower bound in (A.58)


0.1
0
−4
−2
0
2
4
$x_1^{(2)}$
$x_1^{(1)}$
$x_2^{(2)}$
$x_2^{(1)}$


0.1
0
−4
−2
0
2
4
4
2
0
−2
−4
$x_3^{(2)}$
$x_3^{(1)}$
0.1
0
−4
−2
0
2
4
4
2
0
−2
−4
$x_4^{(2)}$
$x_4^{(1)}$
4
2
0
−2
−4
−3 −2 −1 0 1 2 3
$x_3^{(2)}$
$x_3^{(1)}$
4
2
0
−2
−4
−4 −2 0 2 4
$x_4^{(2)}$
$x_4^{(1)}$


{X(t)}
h(·)
{Y(t) = (X ⋆ h)(t)}