More Than 3 Users

Abbas El Gamal

Stanford University

ITMANET 2009

Background

- Real-world MANETs have many users

Background

- Real-world MANETs have many users
- However, most known results on their capacity/rate region (and bounds therein) are for ≤ 3 users

Background

- Real-world MANETs have many users
- However, most known results on their capacity/rate region (and bounds therein) are for ≤ 3 users
- Sometimes we are lucky and these results extend to more users:
  - MAC
  - Degraded BC
  - MIMO BC
  - Slepian–Wolf

Background

- Real-world MANETs have many users
- However, most known results on their capacity/rate region (and bounds therein) are for ≤ 3 users
- Sometimes we are lucky and these results extend to more users:
  - MAC
  - Degraded BC
  - MIMO BC
  - Slepian–Wolf
- In some cases naive extensions of ≤ 3 users results are suboptimal, and better results can be obtained using new coding techniques

Background

- Real-world MANETs have many users
- However, most known results on their capacity/rate region (and bounds therein) are for ≤ 3 users
- Sometimes we are lucky and these results extend to more users:
  - MAC
  - Degraded BC
  - MIMO BC
  - Slepian–Wolf
- In some cases naive extensions of ≤ 3 users results are suboptimal, and better results can be obtained using new coding techniques
- For example, naive extension of Han-Kobayashi inner bound to > 2 user-pair IC can be improved using interference alignment [1]

Background

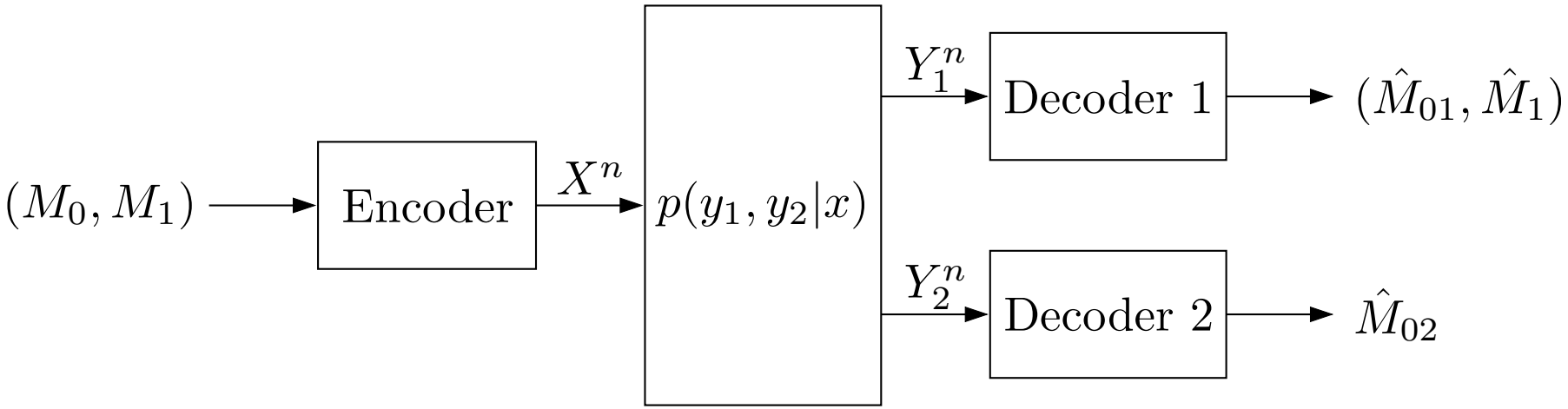
- Real-world MANETs have many users
- However, most known results on their capacity/rate region (and bounds therein) are for ≤ 3 users
- Sometimes we are lucky and these results extend to more users:
  - MAC
  - Degraded BC
  - MIMO BC
  - Slepian–Wolf
- In some cases naive extensions of ≤ 3 users results are suboptimal, and better results can be obtained using new coding techniques
- For example, naive extension of Han-Kobayashi inner bound to > 2 user-pair IC can be improved using interference alignment [1]
- We present two other examples of such cases

DM-BC with Degraded Message Sets

- Consider a 2-receiver DM-BC $(\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2)$
- Sender X wishes to send:

  common message $M_0 \in [1 : 2^{nR_0}]$ to both receivers, and

  private message $M_1 \in [1 : 2^{nR_1}]$ to receiver Y_1



- The capacity region is the closure of the set of achievable rate pairs (R_0, R_1)

Theorem (Körner–Marton [2])

The capacity region of the DM-BC with degraded message sets is the set of rate pairs (R_0, R_1) *such that*

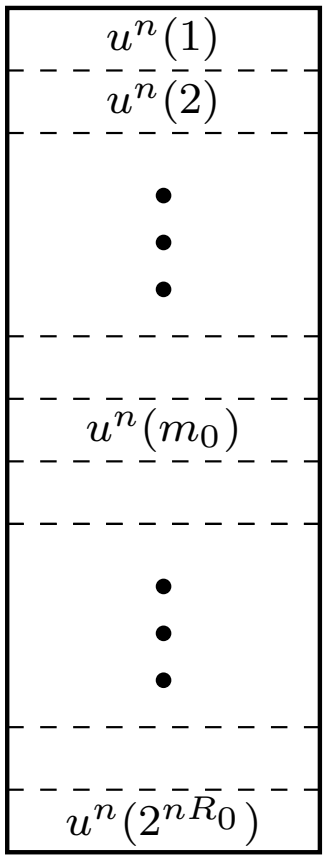
$$\begin{aligned} R_0 &\le I(U;Y_2), \\ R_1 &\le I(X;Y_1|U), \\ R_0 + R_1 &\le I(X;Y_1) \end{aligned}$$

for some $p(u,x)$

- Achievability follows by superposition coding

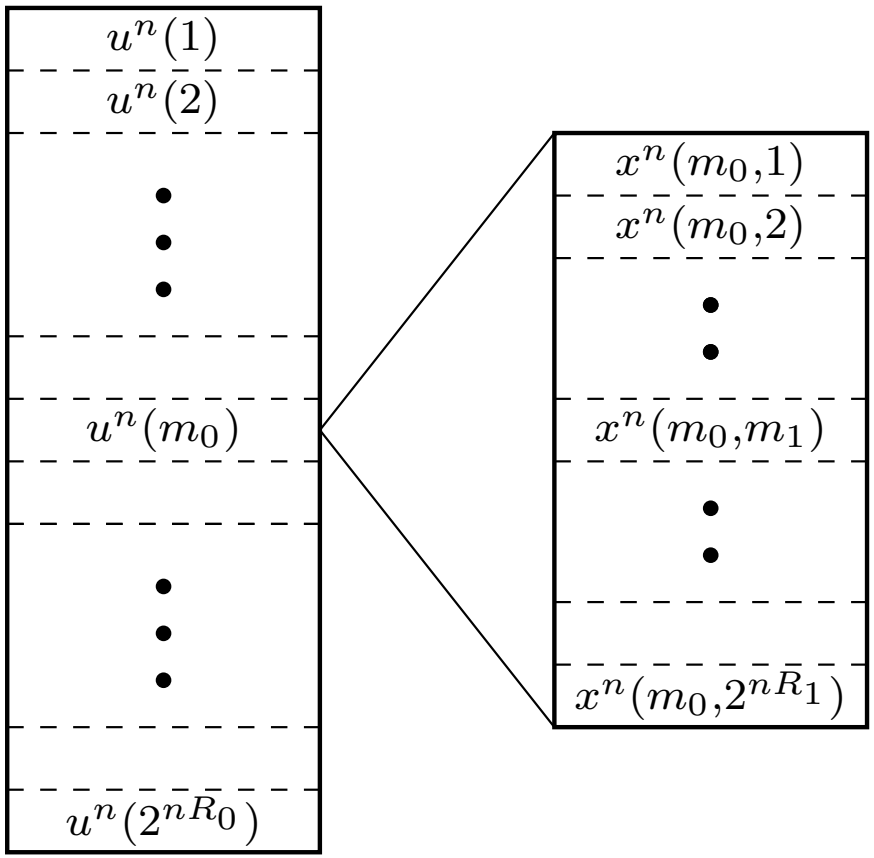
Outline of Achievability: Codebook Generation

- Fix $p(u, x)$. Generate 2^{nR_0} i.i.d. sequences (cloud centers) $u^n \sim \prod_{i=1}^{n} p(u_i)$



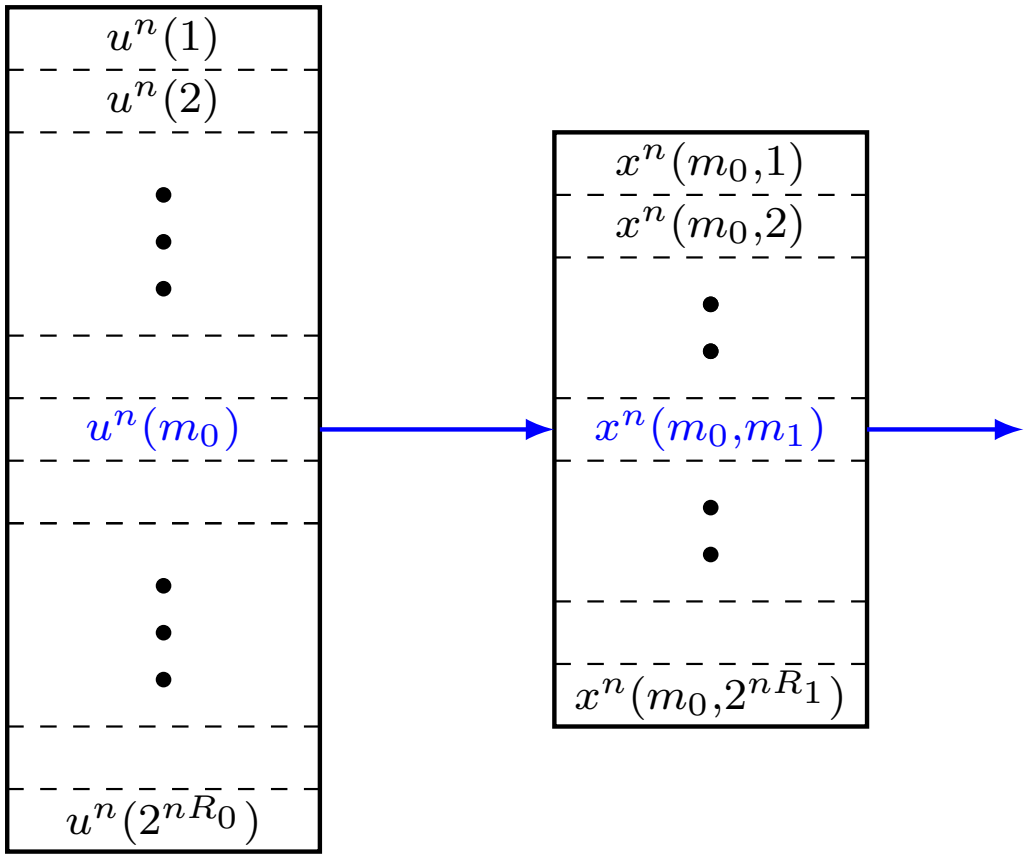
Outline of Achievability: Codebook Generation

- For each $u^n(m_0)$, generate 2^{nR_1} conditionally i.i.d. sequences (satellite codewords) $x^n \sim \prod_{i=1}^{n} p(x_i|u_i)$



Outline of Achievability: Encoding

- To send message pair (m_0, m_1), transmit satellite codeword $x^n(m_0, m_1)$



Outline of Achievability: Decoding

- Y_2 declares that a message $\hat{m}_{02}$ is sent if it is the unique message such that $(u^n(\hat{m}_{02}), y_2^n) \in \mathcal{T}_\epsilon^{(n)}$

  The probability of error $\to 0$ as $n \to \infty$ if

$$R_0 < I(U; Y_2)$$

Outline of Achievability: Decoding

- Y_2 declares that a message $\hat{m}_{02}$ is sent if it is the unique message such that $(u^n(\hat{m}_{02}), y_2^n) \in \mathcal{T}_\epsilon^{(n)}$

  The probability of error $\to 0$ as $n \to \infty$ if

$$R_0 < I(U; Y_2)$$

- Y_1 declares that message pair $(\hat{m}_{01}, \hat{m}_1)$ is sent if it is the unique message pair such that $(u^n(\hat{m}_{01}), x^n(\hat{m}_{01}, \hat{m}_1), y_1^n) \in \mathcal{T}_\epsilon^{(n)}$

  The probability of error $\to 0$ as $n \to \infty$ if

$$\begin{aligned} R_1 &< I(X; Y_1|U), \\ R_0 + R_1 &< I(X; Y_1) \end{aligned}$$

- This completes the proof of achievability

Alternative Characterization

- We can prove the weak converse for the region consisting of rate pairs (R_0, R_1) satisfying

$$\begin{aligned} R_0 &\leq I(U;Y_2), \\ R_0 + R_1 &\leq I(U;Y_2) + I(X;Y_1|U), \\ R_0 + R_1 &\leq I(X;Y_1) \end{aligned}$$

  for some $p(u,x)$

- Clearly this region includes the first characterization region
  We can also show that they have the same boundary points

Alternative Characterization

- We can prove the weak converse for the region consisting of rate pairs (R_0, R_1) satisfying

$$\begin{aligned} R_0 &\leq I(U;Y_2), \\ R_0 + R_1 &\leq I(U;Y_2) + I(X;Y_1|U), \\ R_0 + R_1 &\leq I(X;Y_1) \end{aligned}$$

  for some $p(u,x)$

- Clearly this region includes the first characterization region
  We can also show that they have the same boundary points
- Can we show that the above region is achievable directly?

Alternative Characterization

- We can prove the weak converse for the region consisting of rate pairs (R_0, R_1) satisfying

$$\begin{aligned} R_0 &\leq I(U;Y_2), \\ R_0 + R_1 &\leq I(U;Y_2) + I(X;Y_1|U), \\ R_0 + R_1 &\leq I(X;Y_1) \end{aligned}$$

  for some $p(u,x)$
- Clearly this region includes the first characterization region
  We can also show that they have the same boundary points
- Can we show that the above region is achievable directly?
- The answer is yes, and the proof involves (unnecessary) rate splitting:

  Divide M_1 into two independent messages; M_{10} at rate R_{10} and M_{11} at rate R_{11}. Represent (M_0, M_{10}) by U and (M_0, M_{10}, M_{11}) by X

- We can show that (R_0, R_{10}, R_{11}) is achievable if

$$\begin{aligned} R_0 + R_{10} &< I(U; Y_2), \\ R_{11} &< I(X; Y_1|U), \\ R_0 + R_1 &< I(X; Y_1) \end{aligned}$$

  for some $p(u, x)$
- Substituting $R_1 = R_{10} + R_{11}$ and performing Fourier–Motzkin (F–M) elimination establishes the achievability of the region

- We can show that (R_0, R_{10}, R_{11}) is achievable if

$$\begin{aligned} R_0 + R_{10} &< I(U; Y_2), \\ R_{11} &< I(X; Y_1|U), \\ R_0 + R_1 &< I(X; Y_1) \end{aligned}$$

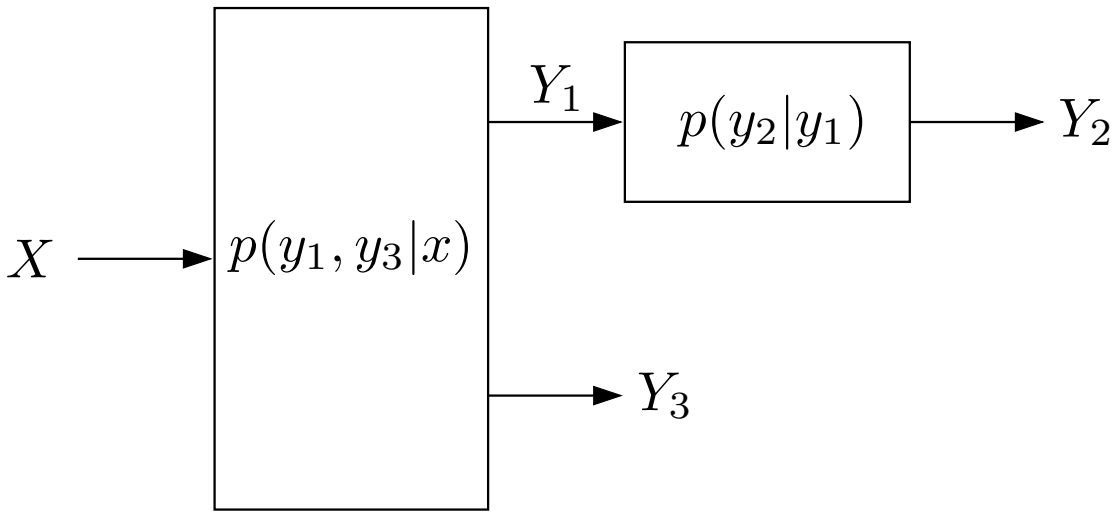
  for some $p(u, x)$
- Substituting $R_1 = R_{10} + R_{11}$ and performing Fourier–Motzkin (F–M) elimination establishes the achievability of the region
- The above rate splitting idea turns out to be crucial for 3-receiver DM-BC

Multi-level DM-BC with Degraded Message Sets

- A *multilevel* DM-BC [3] $(\mathcal{X}, p(y_1, y_3|x)p(y_2|y_1), \mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Y}_3)$ is a 3-receiver DM-BC where Y_2 is a degraded version of Y_1
- Sender X wishes to send

  common message $M_0 \in [1 : 2^{nR_0}]$ to *all* receivers

  private message $M_1 \in [1 : 2^{nR_1}]$ only to receiver Y_1



- What is the capacity region?

- A straightforward extension of Körner–Marton capacity region for 2 receivers gives the inner bound consisting of (R_0, R_1) such that

$$R_0 < \min\{I(U;Y_2), I(U;Y_3)\},$$
$$R_1 < I(X;Y_1|U)$$

for some $p(u,x)$
Note the bound $R_0 + R_1 < I(X;Y_1)$ drops out since $X \to Y_1 \to Y_2$

- A straightforward extension of Körner–Marton capacity region for 2 receivers gives the inner bound consisting of (R_0, R_1) such that

$$R_0 < \min\{I(U;Y_2), I(U;Y_3)\},$$
$$R_1 < I(X;Y_1|U)$$

for some $p(u,x)$
Note the bound $R_0 + R_1 < I(X;Y_1)$ drops out since $X \to Y_1 \to Y_2$

- This region turned out not to be optimal in general

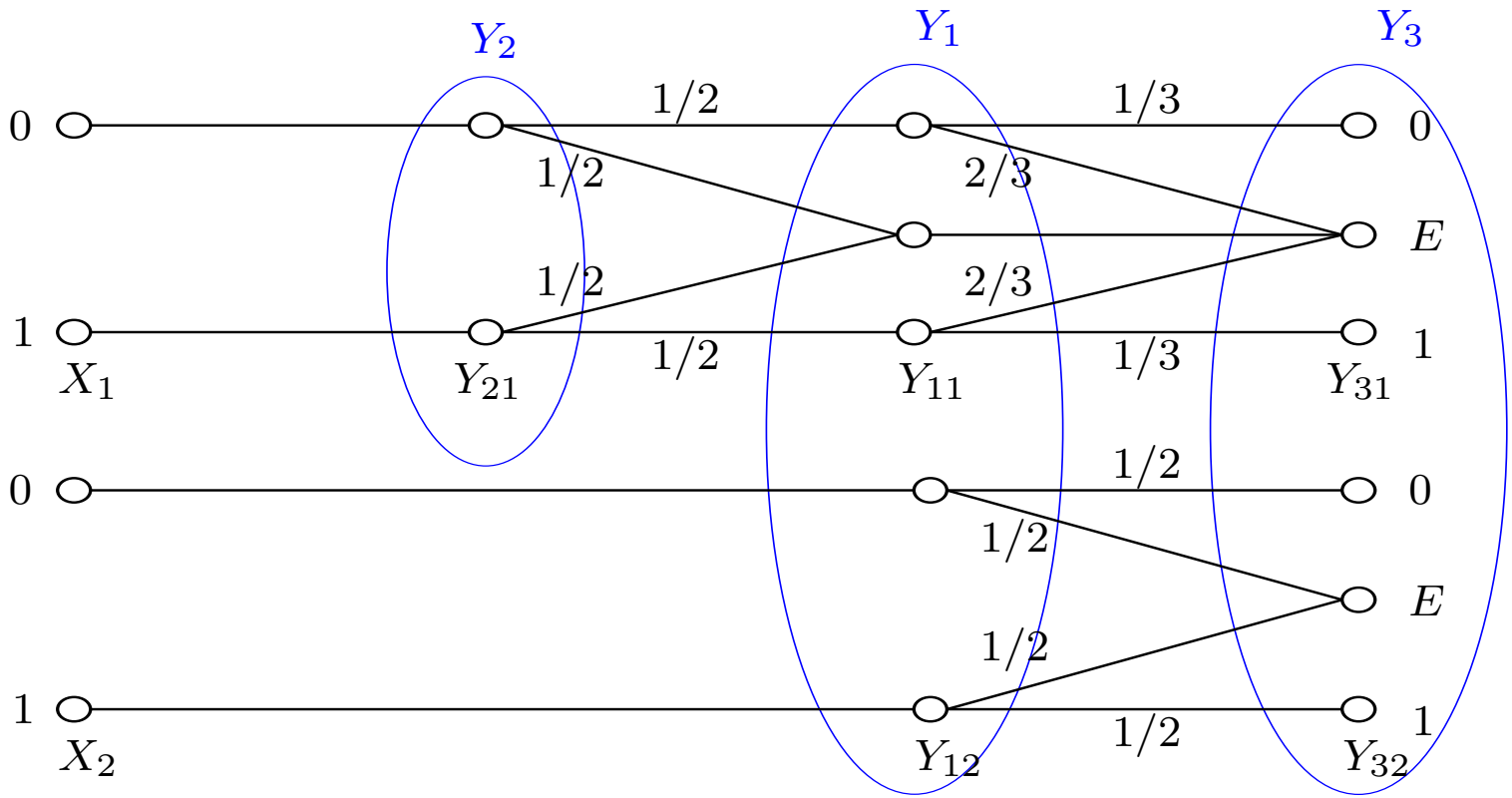
Theorem (Nair–El Gamal [4])

The capacity region of the 3-receiver multi-level DM-BC is the set of rate pairs (R_0, R_1) such that

$$R_0 \le \min\{I(U;Y_2), I(V;Y_3)\},$$
$$R_1 \le I(X;Y_1|U),$$
$$R_0 + R_1 \le I(V;Y_3) + I(X;Y_1|V)$$

for some $p(u,v)p(x|v)$

Reversely Degraded BEC Example [4]



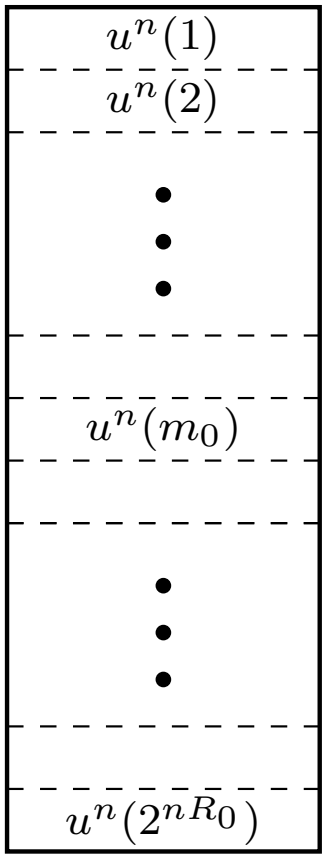
- Fix $R_0 = 1/2$:
  - With Körner-Marton extension: $R_1 = 5/12$
  - Capacity region: $R_1 = 1/2$

Outline of Achievability: Codebook Generation

- Split R_1 into R_{10} and R_{11}; $R_1 = R_{10} + R_{11}$

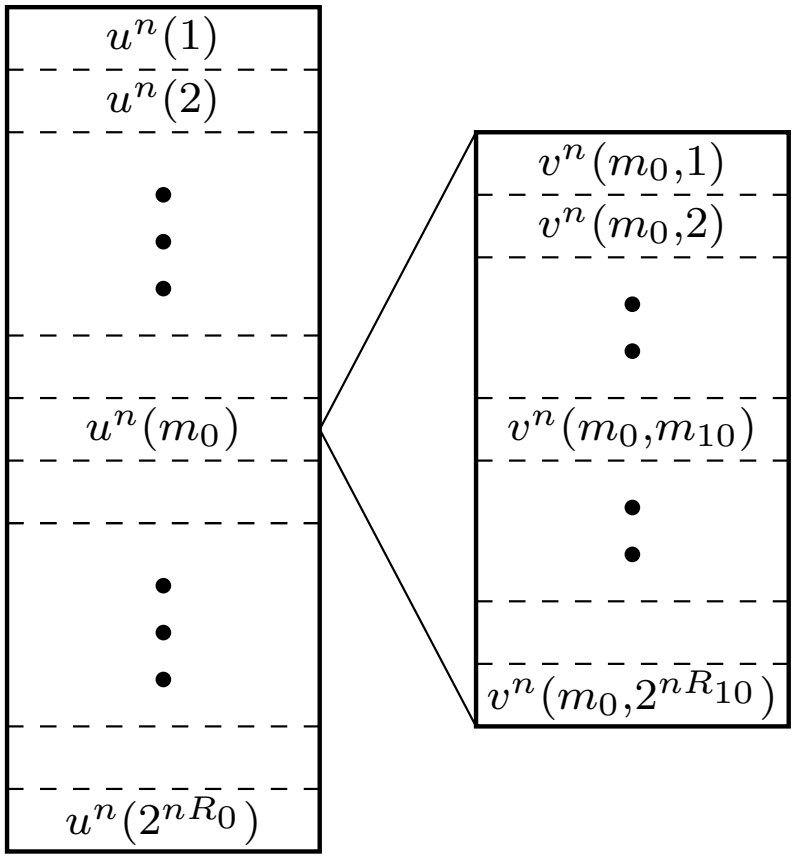
Outline of Achievability: Codebook Generation

- Fix $p(u,v)p(x|v)$. Generate 2^{nR_0} i.i.d. $u^n \sim \prod_{i=1}^{n} p(u_i)$



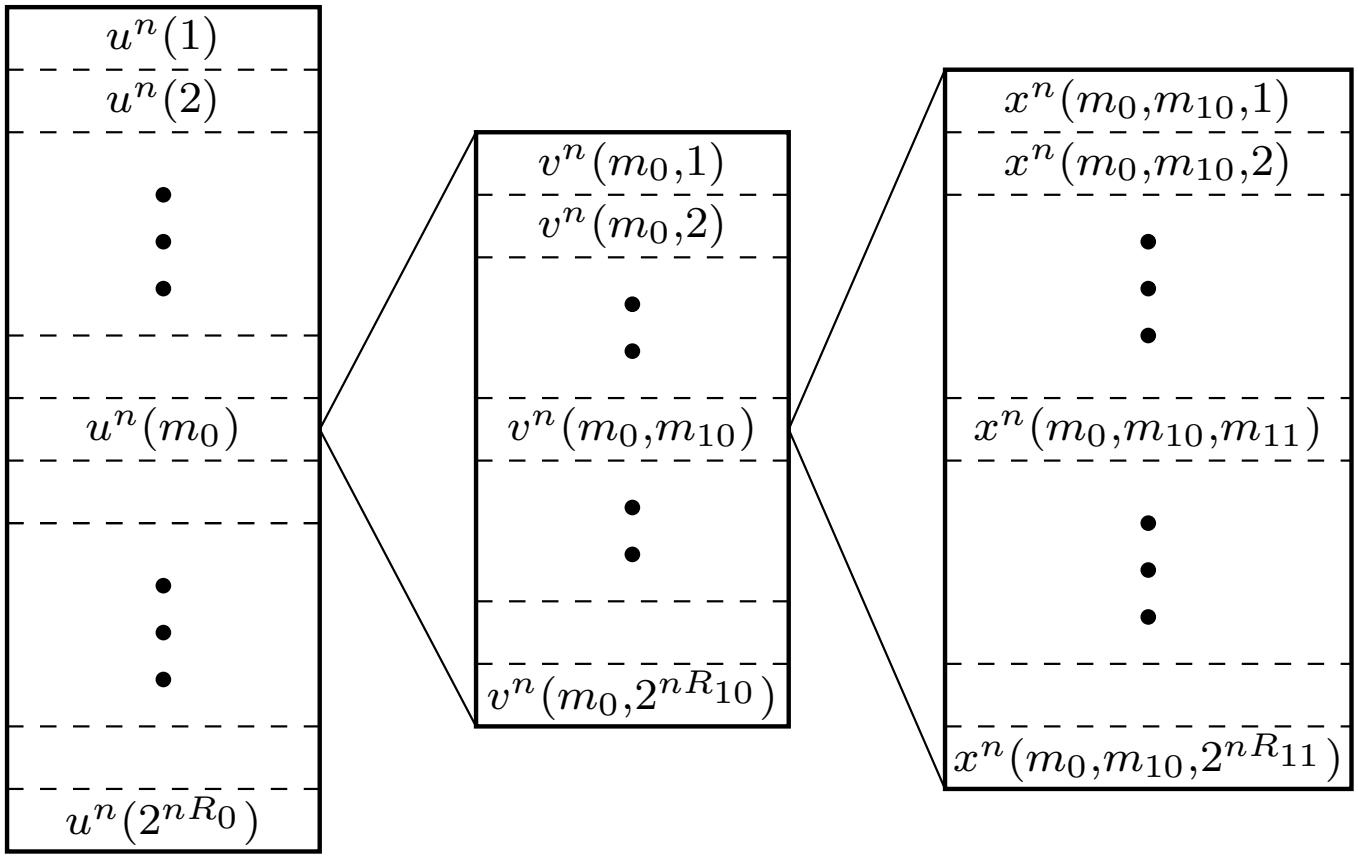
Outline of Achievability: Codebook Generation

- For each u^n, generate $2^{nR_{10}}$ conditionally i.i.d. $v^n \sim \prod_{i=1}^{n} p(v_i|u_i)$



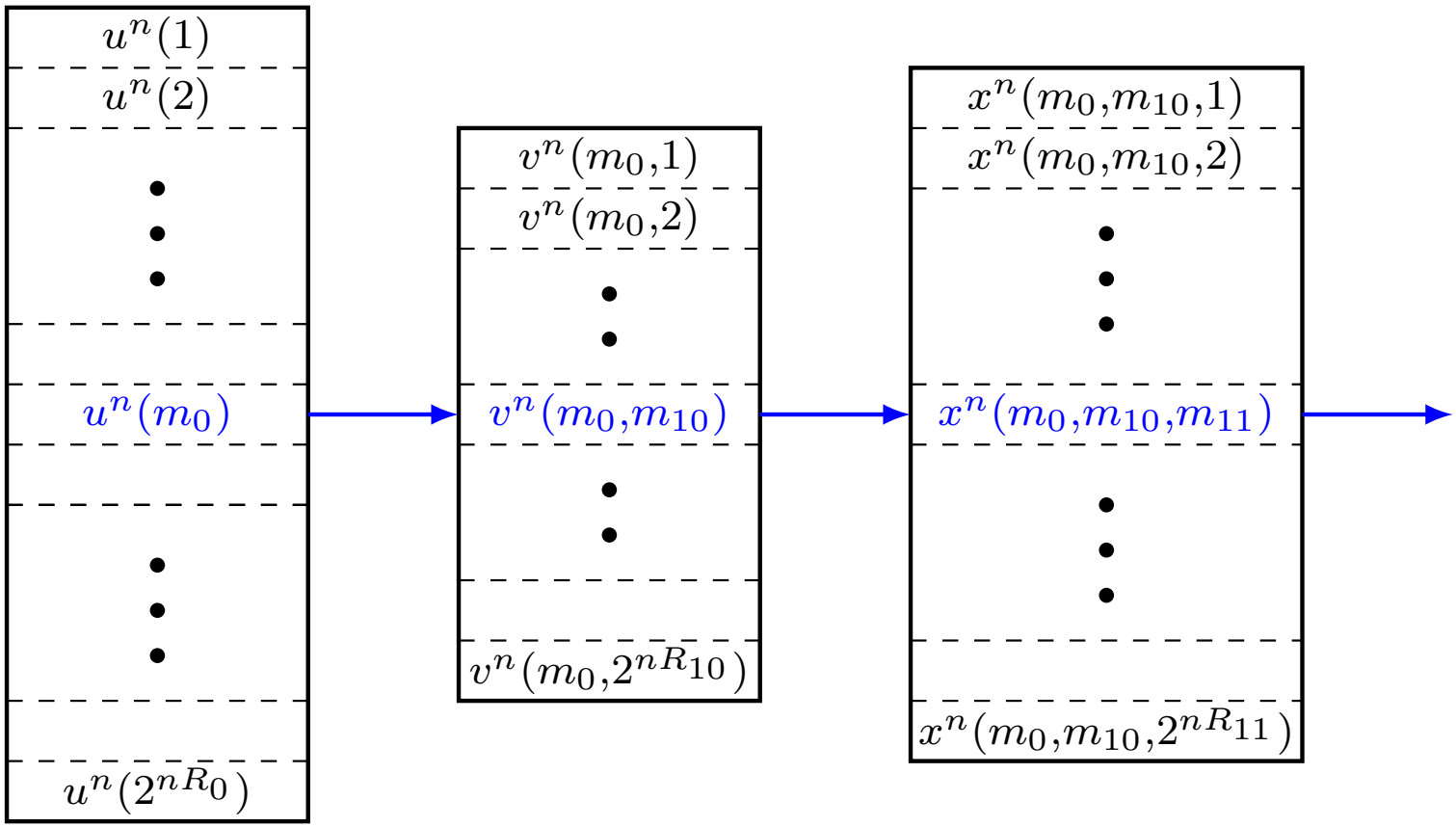
Outline of Achievability: Codebook Generation

- For each v^n, generate $2^{nR_{11}}$ conditionally i.i.d. $x^n \sim \prod_{i=1}^{n} p(x_i|v_i)$



Outline of Achievability: Encoding

- To send (m_0, m_1), transmit $x^n(m_0, m_{10}, m_{11})$



Outline of Achievability: Decoding

- Y_2 declares that $\hat{m}_{02} \in [1 : 2^{nR_0}]$ is sent if it is the unique message such that $(u^n(\hat{m}_{02}), y_2^n) \in \mathcal{T}_\epsilon^{(n)}$

  The probability of error $\to 0$ as $n \to \infty$ if

$$R_0 < I(U; Y_2)$$

Outline of Achievability: Decoding

- Y_2 declares that $\hat{m}_{02} \in [1 : 2^{nR_0}]$ is sent if it is the unique message such that $(u^n(\hat{m}_{02}), y_2^n) \in \mathcal{T}_\epsilon^{(n)}$

  The probability of error $\to 0$ as $n \to \infty$ if

$$R_0 < I(U; Y_2)$$

- Y_1 declares that $(\hat{m}_{01}, \hat{m}_{10}, \hat{m}_{11})$ is sent if it is the unique triple such that $(u^n(\hat{m}_{01}), v^n(\hat{m}_{01}, \hat{m}_{10}), x^n(\hat{m}_{01}, \hat{m}_{10}, \hat{m}_{11}), y_1^n) \in \mathcal{T}_\epsilon^{(n)}$

  The probability of error $\to 0$ as $n \to \infty$ if

$$\begin{aligned} R_{11} &< I(X; Y_1|V), \\ R_{10} + R_{11} &< I(X; Y_1|U), \\ R_0 + R_{10} + R_{11} &< I(X; Y_1) \end{aligned}$$

Outline of Achievability: Decoding

- If receiver Y_3 decodes m_0 directly by finding the unique $\hat{m}_{03}$ such that $(u^n(\hat{m}_{03}), y_3^n) \in \mathcal{T}_\epsilon^{(n)}$, we have $R_0 < I(U; Y_3)$, which together with previous conditions gives the extended Körner–Marton region

Outline of Achievability: Decoding

- If receiver Y_3 decodes m_0 directly by finding the unique $\hat{m}_{03}$ such that $(u^n(\hat{m}_{03}), y_3^n) \in \mathcal{T}_\epsilon^{(n)}$, we have $R_0 < I(U; Y_3)$, which together with previous conditions gives the extended Körner–Marton region

- To achieve the larger region, receiver Y_3 decodes m_0 indirectly:

  It declares that $\hat{m}_{03}$ is sent if it is the unique index such that $(v^n(\hat{m}_{03}, m_{10}), y_3^n) \in \mathcal{T}_\epsilon^{(n)}$ *for some* $m_{10} \in [1 : 2^{nR_{10}}]$
  The probability of error $\to 0$ as $n \to \infty$ if

$$R_0 + R_{10} < I(V; Y_3)$$

Outline of Achievability: Decoding

- If receiver Y_3 decodes m_0 directly by finding the unique $\hat{m}_{03}$ such that $(u^n(\hat{m}_{03}), y_3^n) \in \mathcal{T}_\epsilon^{(n)}$, we have $R_0 < I(U; Y_3)$, which together with previous conditions gives the extended Körner–Marton region

- To achieve the larger region, receiver Y_3 decodes m_0 indirectly:

  It declares that $\hat{m}_{03}$ is sent if it is the unique index such that $(v^n(\hat{m}_{03}, m_{10}), y_3^n) \in \mathcal{T}_\epsilon^{(n)}$ *for some* $m_{10} \in [1 : 2^{nR_{10}}]$
  The probability of error $\to 0$ as $n \to \infty$ if

$$R_0 + R_{10} < I(V; Y_3)$$

- Combining the bounds, substituting $R_{10} + R_{11} = R_1$, and performing F–M to eliminate R_{10} and R_{11} completes the proof of achievability

Extensions

- A new inner bound for general 3-receiver BC with degraded message sets can be obtained by combining Marton coding with rate splitting, indirect decoding, and superposition coding

Extensions

- A new inner bound for general 3-receiver BC with degraded message sets can be obtained by combining Marton coding with rate splitting, indirect decoding, and superposition coding

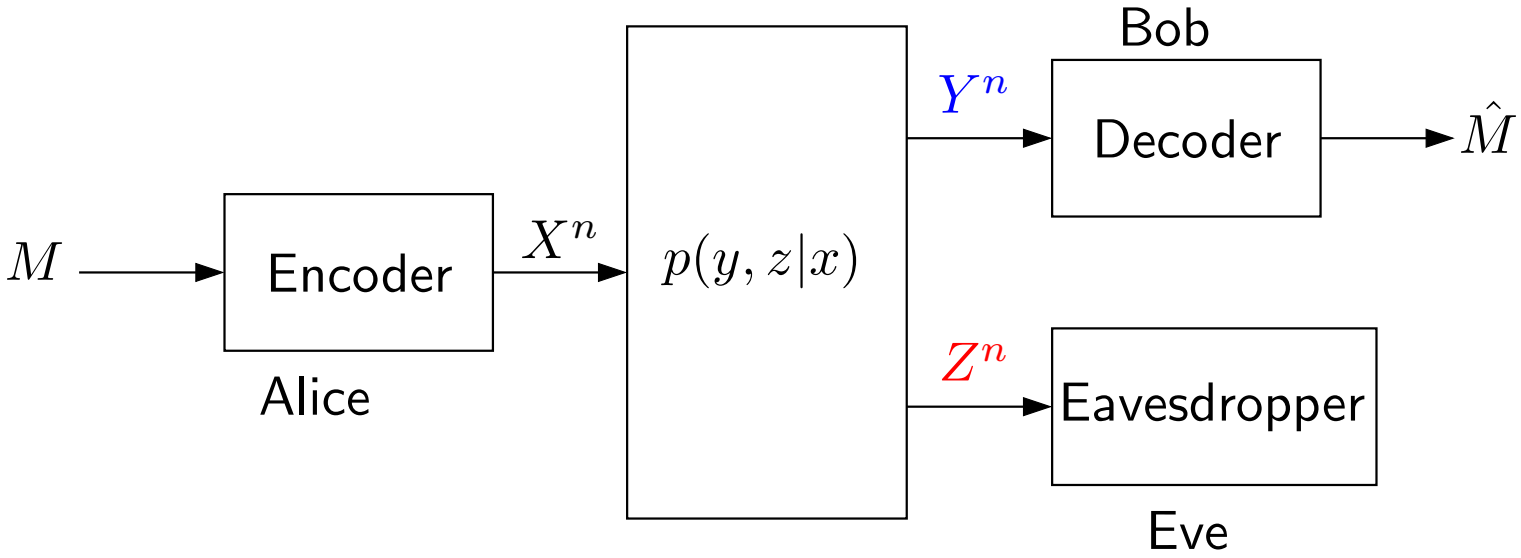
- This leads to a general method for constructing inner bounds for general k-receiver BCs with arbitrary messaging requirements, which is at least as large as existing inner bounds

Extensions

- A new inner bound for general 3-receiver BC with degraded message sets can be obtained by combining Marton coding with rate splitting, indirect decoding, and superposition coding
- This leads to a general method for constructing inner bounds for general k-receiver BCs with arbitrary messaging requirements, which is at least as large as existing inner bounds
- Optimality of these general results are not known

Wiretap channel

- Consider a 2-receiver DM-BC
- Sender X wishes to send a message $M \in [1 : 2^{nR}]$ to Y, while keeping it secret from Z



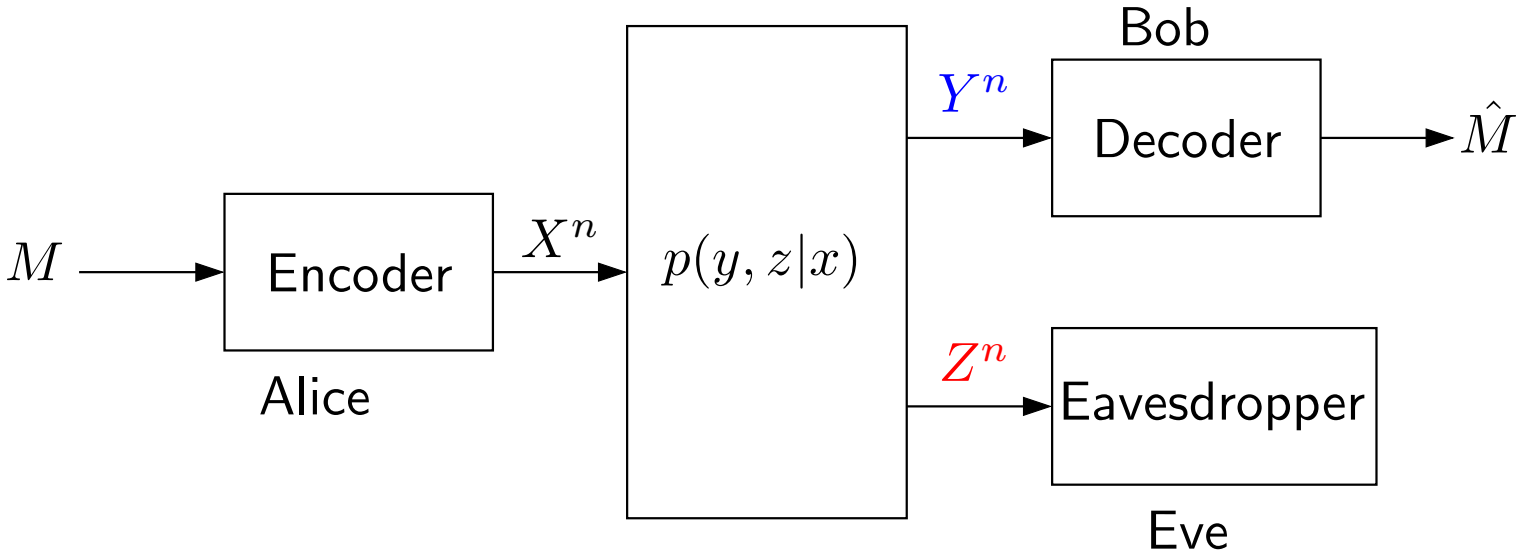
- Rate R is achievable if:

  Probability of error: $P_e^{(n)} = \mathsf{P}\{\hat{M} \neq M\} \to 0$ as $n \to \infty$

  Secrecy constraint: $I(M; Z^n)/n \to 0$ as $n \to \infty$
- The secrecy capacity C_{S} is the supremum of all achievable rates

Wiretap channel

- Consider a 2-receiver DM-BC
- Sender X wishes to send a message $M \in [1 : 2^{nR}]$ to Y, while keeping it secret from Z

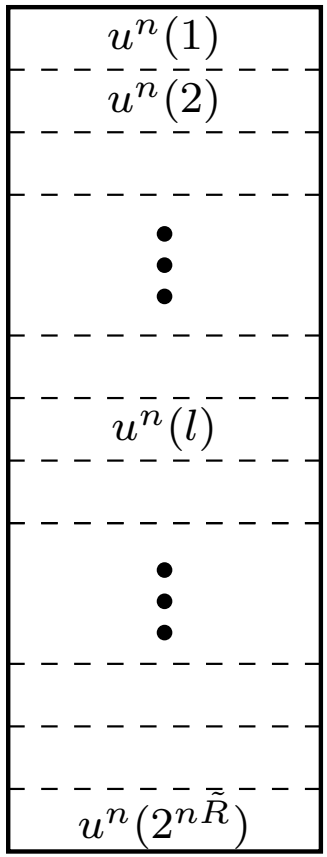


Theorem (Wyner [5], Csiszár–Körner [6])

$$C_{\mathrm{S}} = \max_{p(u,x)} \left(I(U;Y) - I(U;Z) \right)$$

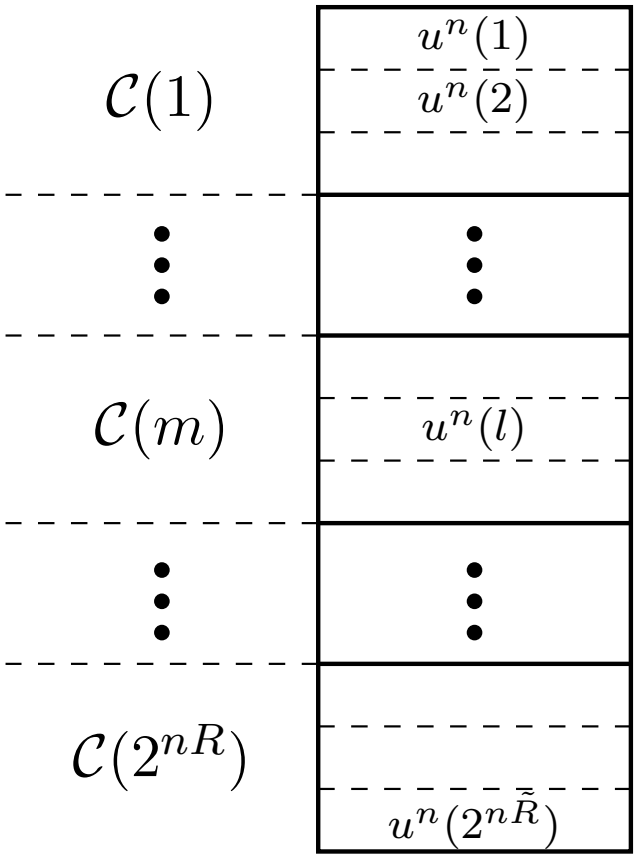
Outline of Achievability: Codebook Generation

- Generate $2^{n\tilde{R}}$ i.i.d. $u^n \sim \prod_{i=1}^{n} p(u_i)$.



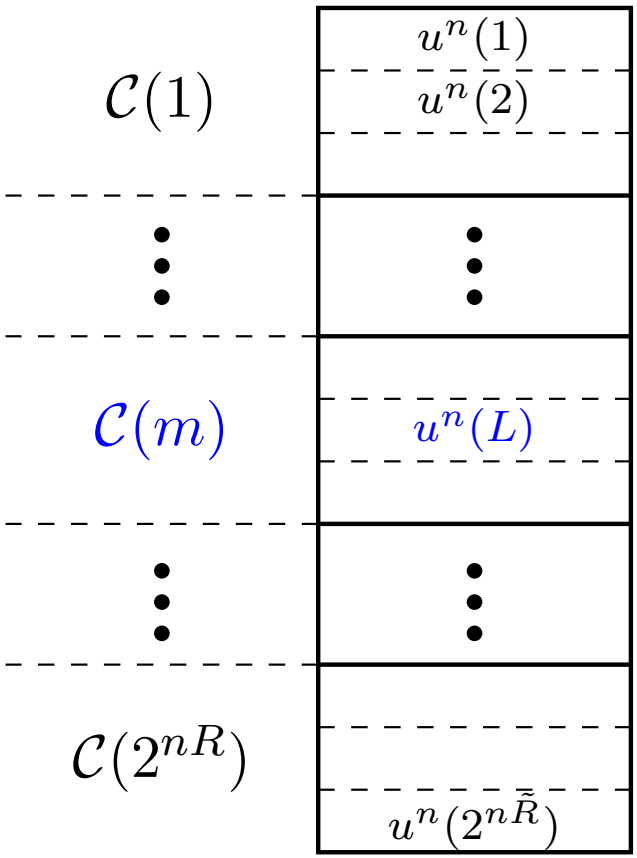
Outline of Achievability: Codebook Generation

- Generate $2^{n\tilde{R}}$ i.i.d. $u^n \sim \prod_{i=1}^{n} p(u_i)$. Partition into 2^{nR} subcodes



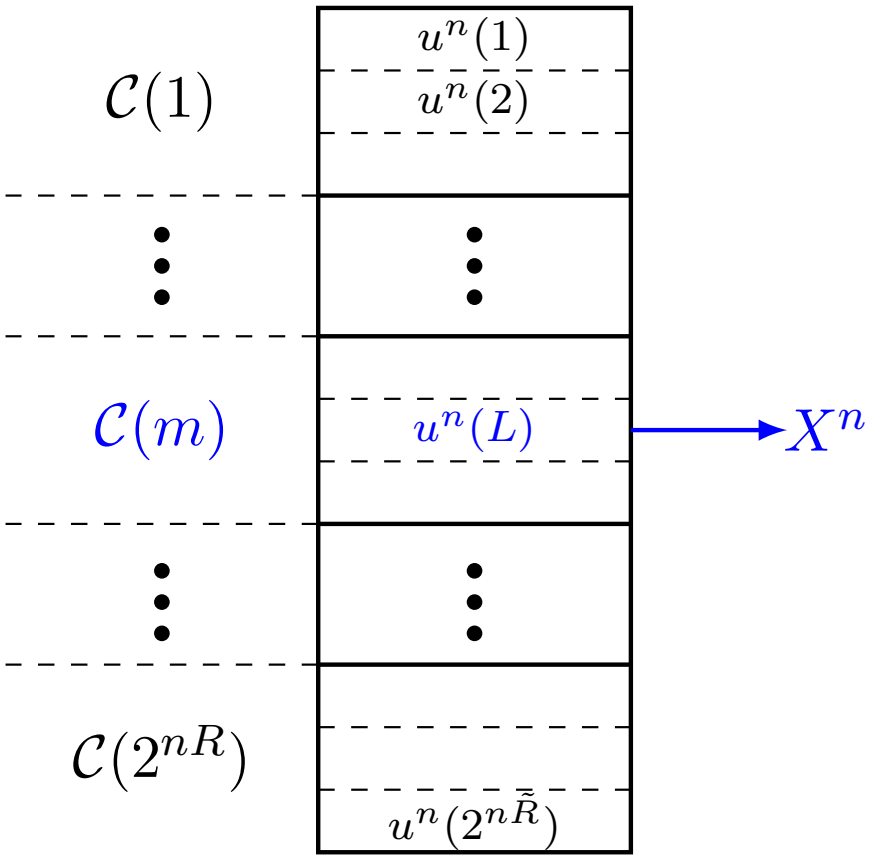
Outline of Achievability: Encoding

- To send m, choose random $u^n(L) \in \mathcal{C}(m)$.



Outline of Achievability: Encoding

- To send m, choose random $u^n(L) \in \mathcal{C}(m)$. Transmit $X^n \sim \prod_{i=1}^n p(x_i|u_i)$



Decoding and Analysis of Secrecy Constraint

- Decoding: Y declares that $\hat{l}$ is sent if it is the unique index such that $(u^n(\hat{l}), y^n) \in \mathcal{T}_\epsilon^{(n)}$; declares message sent to be subcode index $\hat{m}$ of $u^n(\hat{l})$

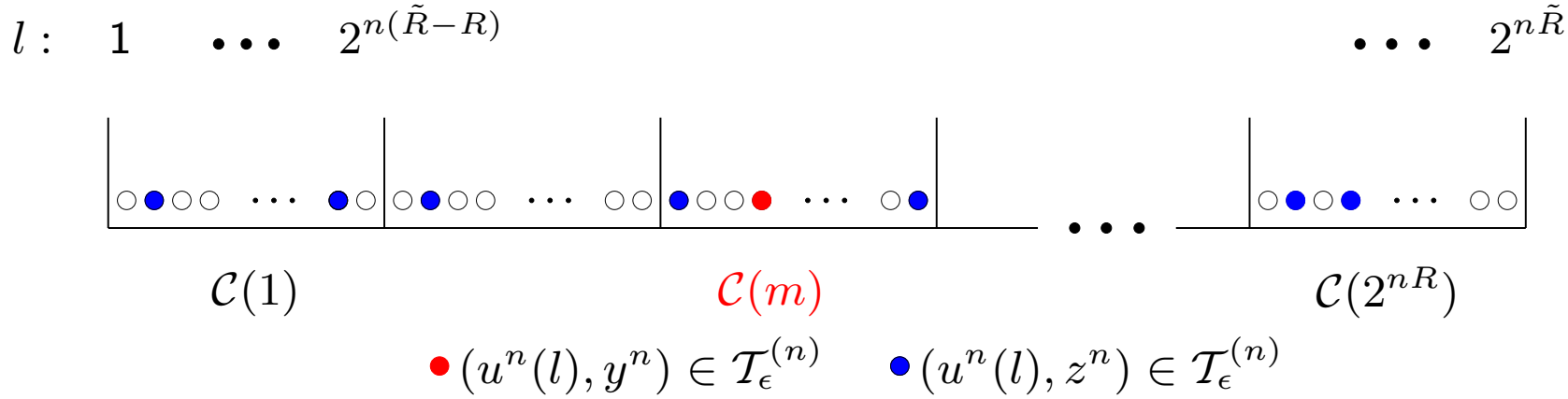
  The probability of error $\to 0$ as $n \to \infty$ if $\tilde{R} < I(U;Y)$

Decoding and Analysis of Secrecy Constraint

- Decoding: Y declares that $\hat{l}$ is sent if it is the unique index such that $(u^n(\hat{l}), y^n) \in \mathcal{T}_\epsilon^{(n)}$; declares message sent to be subcode index $\hat{m}$ of $u^n(\hat{l})$

  The probability of error $\to 0$ as $n \to \infty$ if $\tilde{R} < I(U;Y)$

- Secrecy constraint: For each subcode $\mathcal{C}(m)$, Z has $\doteq 2^{n(\tilde{R}-R-I(U;Z))}$ jointly typical $u^n(l)$ sequences with z^n

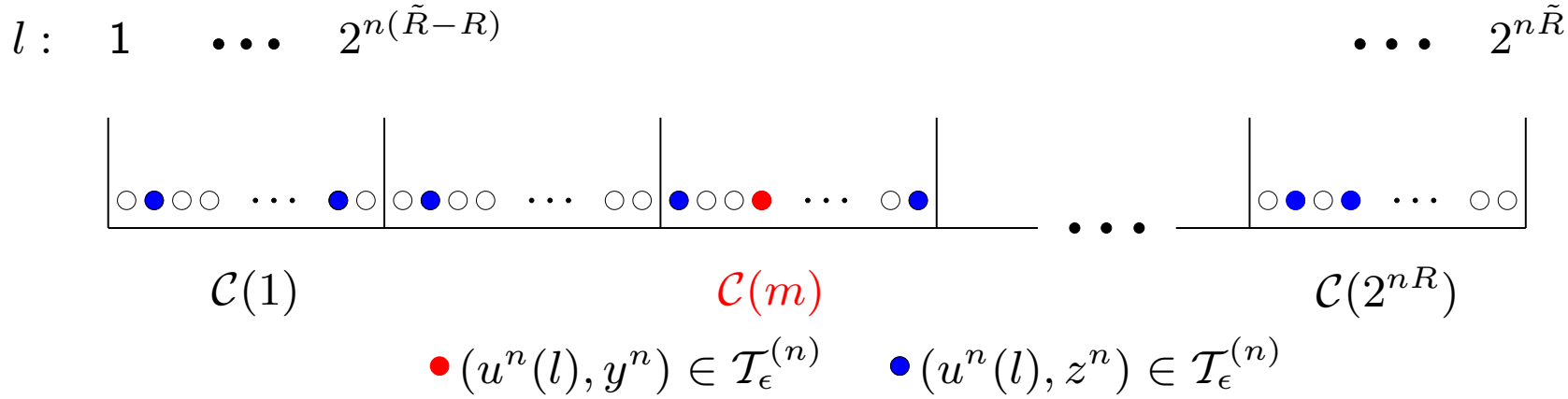


Decoding and Analysis of Secrecy Constraint

- Decoding: Y declares that $\hat{l}$ is sent if it is the unique index such that $(u^n(\hat{l}), y^n) \in \mathcal{T}_\epsilon^{(n)}$; declares message sent to be subcode index $\hat{m}$ of $u^n(\hat{l})$

  The probability of error $\to 0$ as $n \to \infty$ if $\tilde{R} < I(U;Y)$

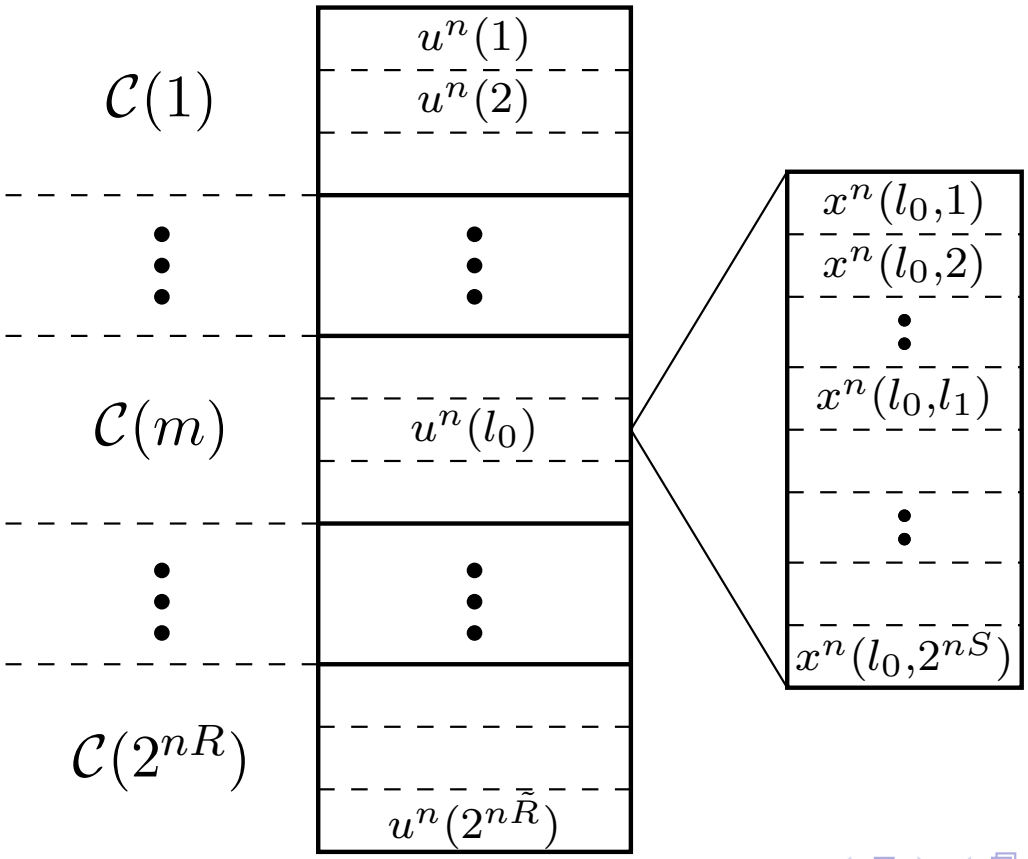
- Secrecy constraint: For each subcode $\mathcal{C}(m)$, Z has $\doteq 2^{n(\tilde{R}-R-I(U;Z))}$ jointly typical $u^n(l)$ sequences with z^n



Thus if $\tilde{R} - R > I(U;Z)$, Z has roughly equal number of indices in each subcode, providing it with no information about the message

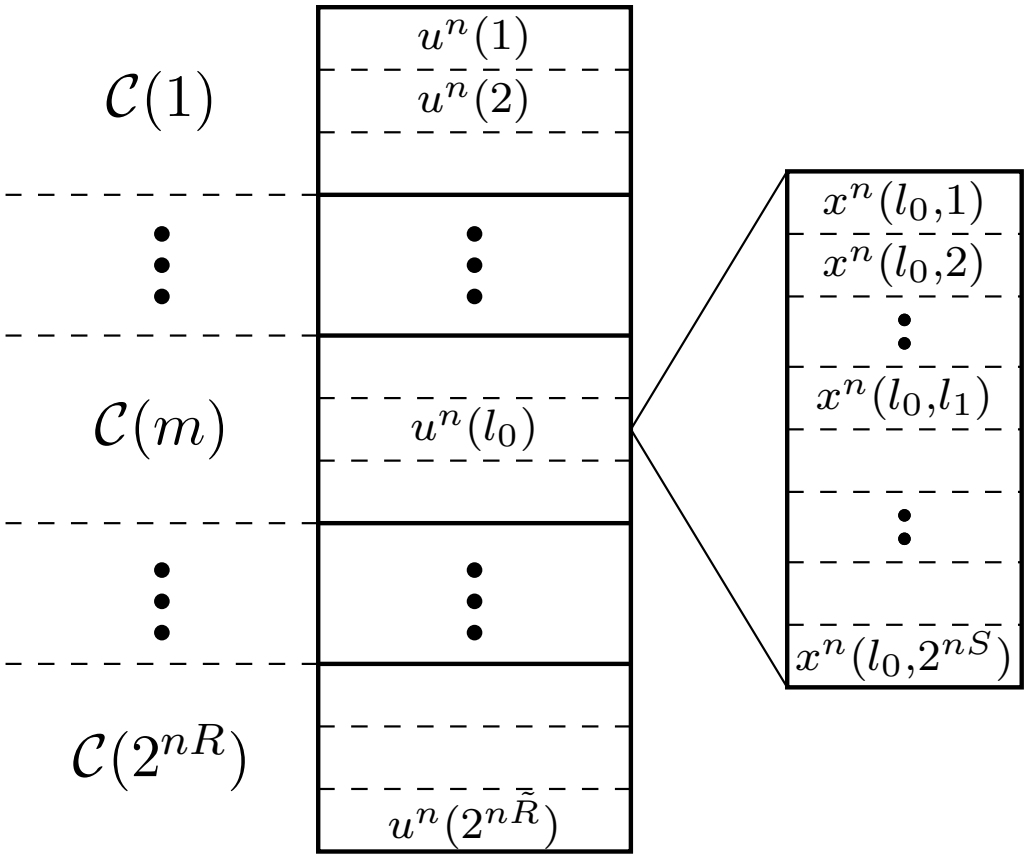
Observation

- Instead of choosing X^n at random, can generate for each u^n a subcode consisting of 2^{nS} conditionally i.i.d. codewords $x^n \sim \prod_{i=1}^n p(x_i|u_i)$; choose one at random for transmission



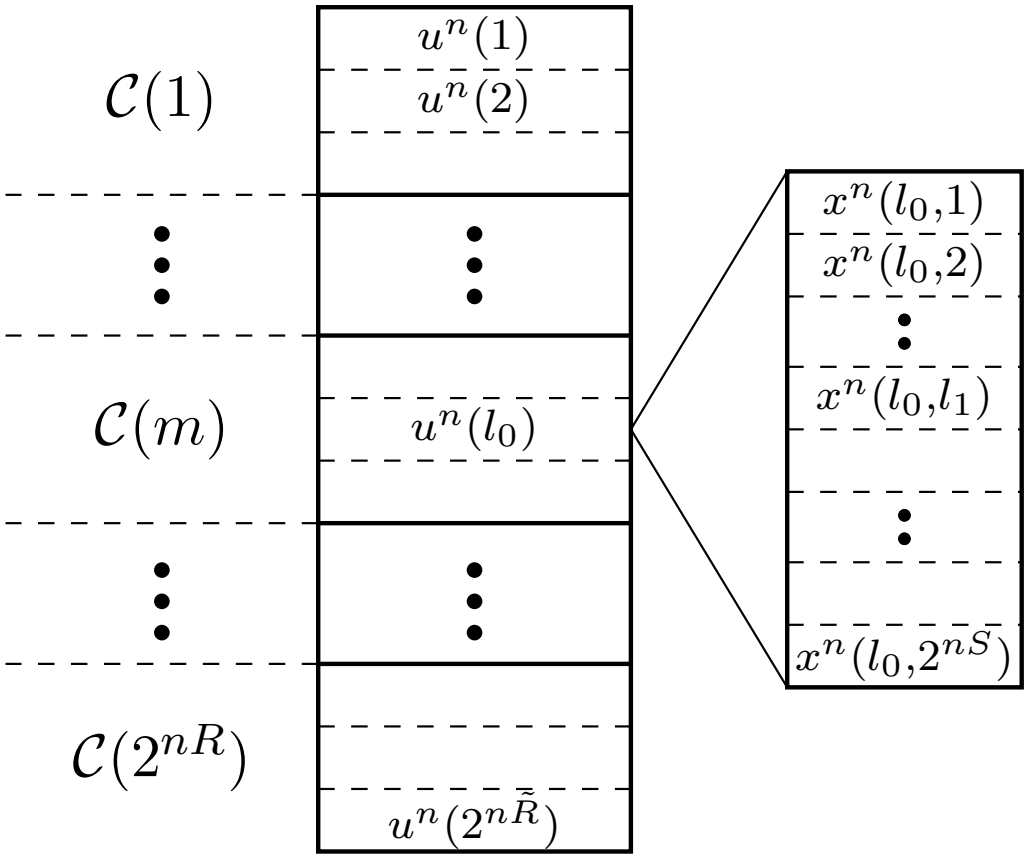
Observation

- Z cannot decode U indirectly through X if $S + \tilde{R} - R \geq I(X;Z)$, or equivalently if $S \geq I(X;Z) - I(U;Z)$



Observation

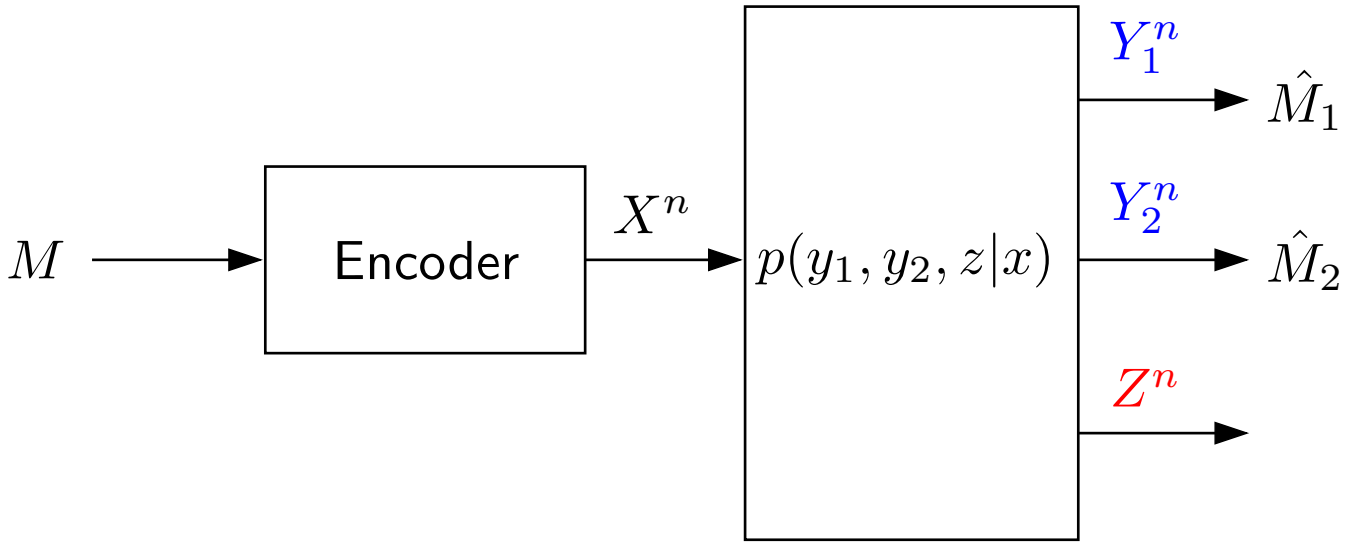
- Z cannot decode U indirectly through X if $S + \tilde{R} - R \geq I(X;Z)$, or equivalently if $S \geq I(X;Z) - I(U;Z)$



- This observation turned out to be crucial for ≥ 3 receivers

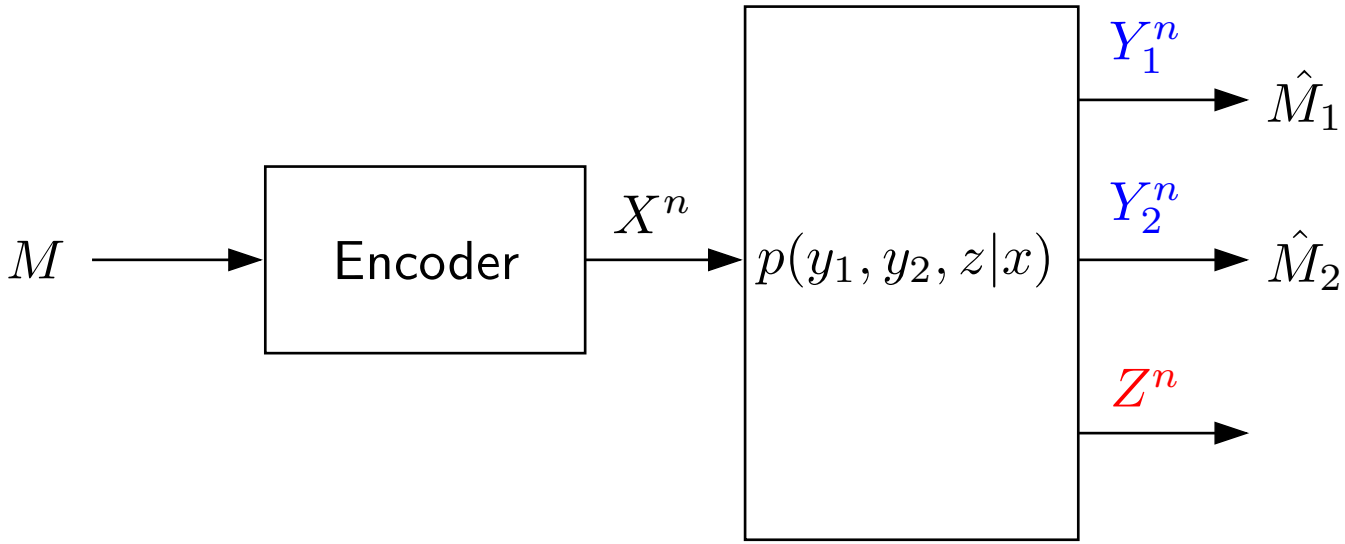
2 Receivers, 1 Eavesdropper Wiretap Channel

- Consider a 3-receiver DM-BC
- Sender X wishes to send a message $M \in [1 : 2^{nR}]$ to Y_1 and Y_2, while keeping it secret from eavesdropper Z



2 Receivers, 1 Eavesdropper Wiretap Channel

- Consider a 3-receiver DM-BC
- Sender X wishes to send a message $M \in [1 : 2^{nR}]$ to Y_1 and Y_2, while keeping it secret from eavesdropper Z



- Rate R is achievable if:

  Probability of error: $P_e^{(n)} = \mathsf{P}\{\hat{M}_1 \neq M \text{ or } \hat{M}_2 \neq M\} \to 0$ as $n \to \infty$

  Secrecy constraint: $I(M; Z^n)/n \to 0$ as $n \to \infty$

- Secrecy capacity C_{S} is the supremum of achievable rates

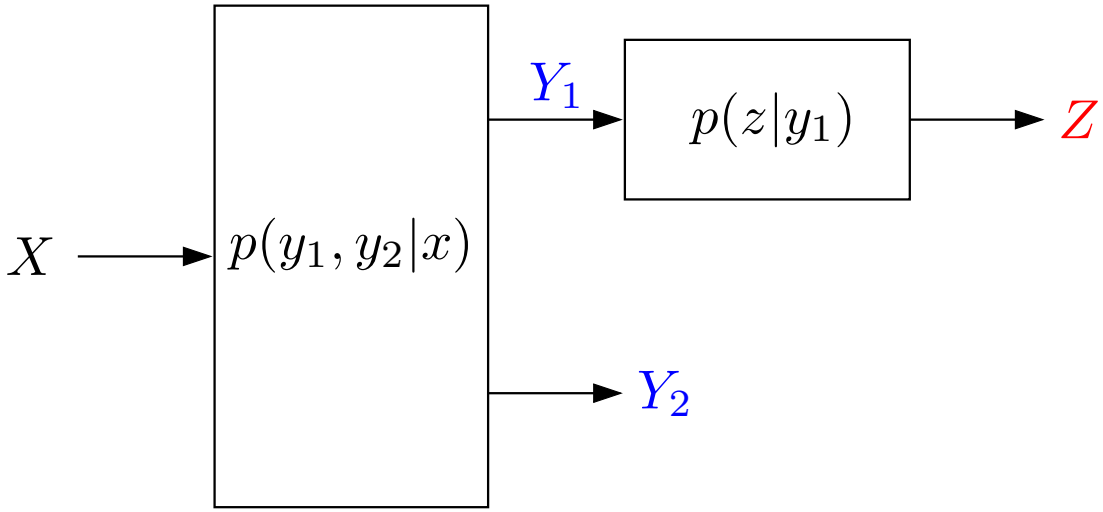
- Straightforward extension of Csiszár–Körner achievability scheme:

$$C_{\mathrm{S}} \geq \max_{p(u,x)} \min\{I(U;Y_1) - I(U;Z), I(U;Y_2) - I(U;Z)\}$$

- Straightforward extension of Csiszár–Körner achievability scheme:

$$C_{\mathrm{S}} \geq \max_{p(u,x)} \min\{I(U;Y_1) - I(U;Z), I(U;Y_2) - I(U;Z)\}$$

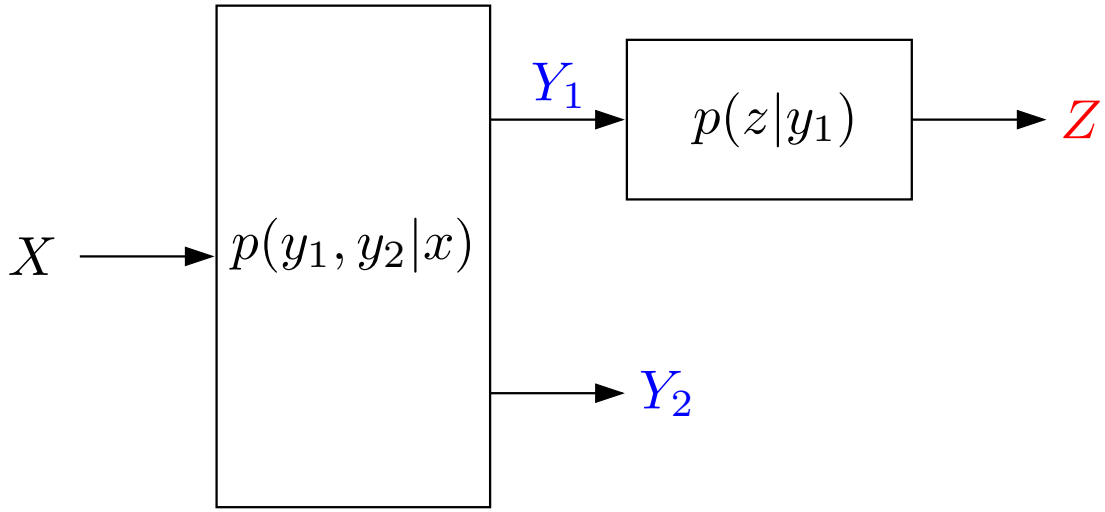
- Consider multilevel-BC case:



- Straightforward extension of Csiszár–Körner achievability scheme:

$$C_{\mathrm{S}} \geq \max_{p(u,x)} \min\{I(U;Y_1) - I(U;Z), I(U;Y_2) - I(U;Z)\}$$

- Consider multilevel-BC case:

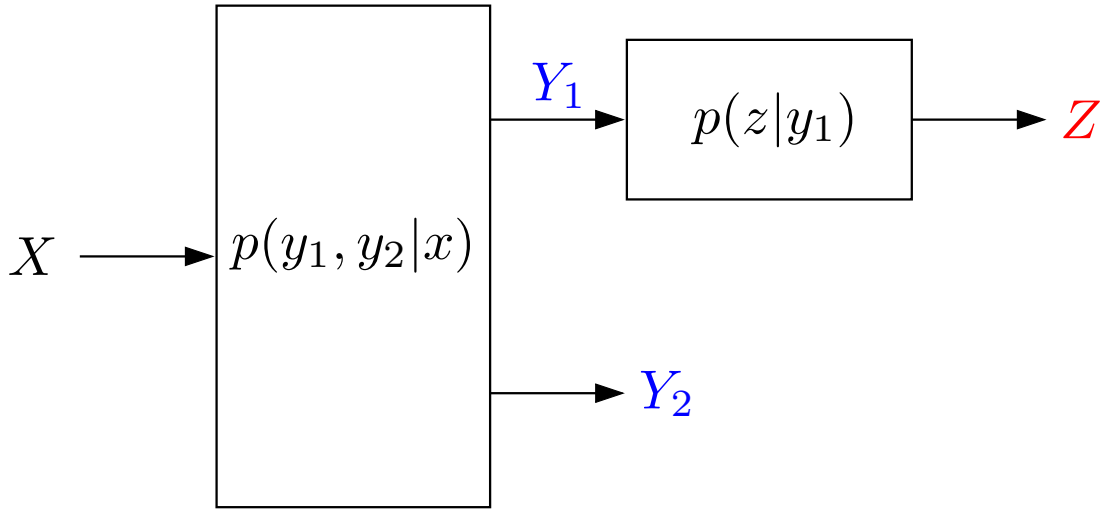


- $I(X;Y_1) - I(X;Z) \geq I(U;Y_1) - I(U;Z)$; not true in general for Y_2

- Straightforward extension of Csiszár–Körner achievability scheme:

$$C_{\mathrm{S}} \geq \max_{p(u,x)} \min\{I(U;Y_1) - I(U;Z), I(U;Y_2) - I(U;Z)\}$$

- Consider multilevel-BC case:

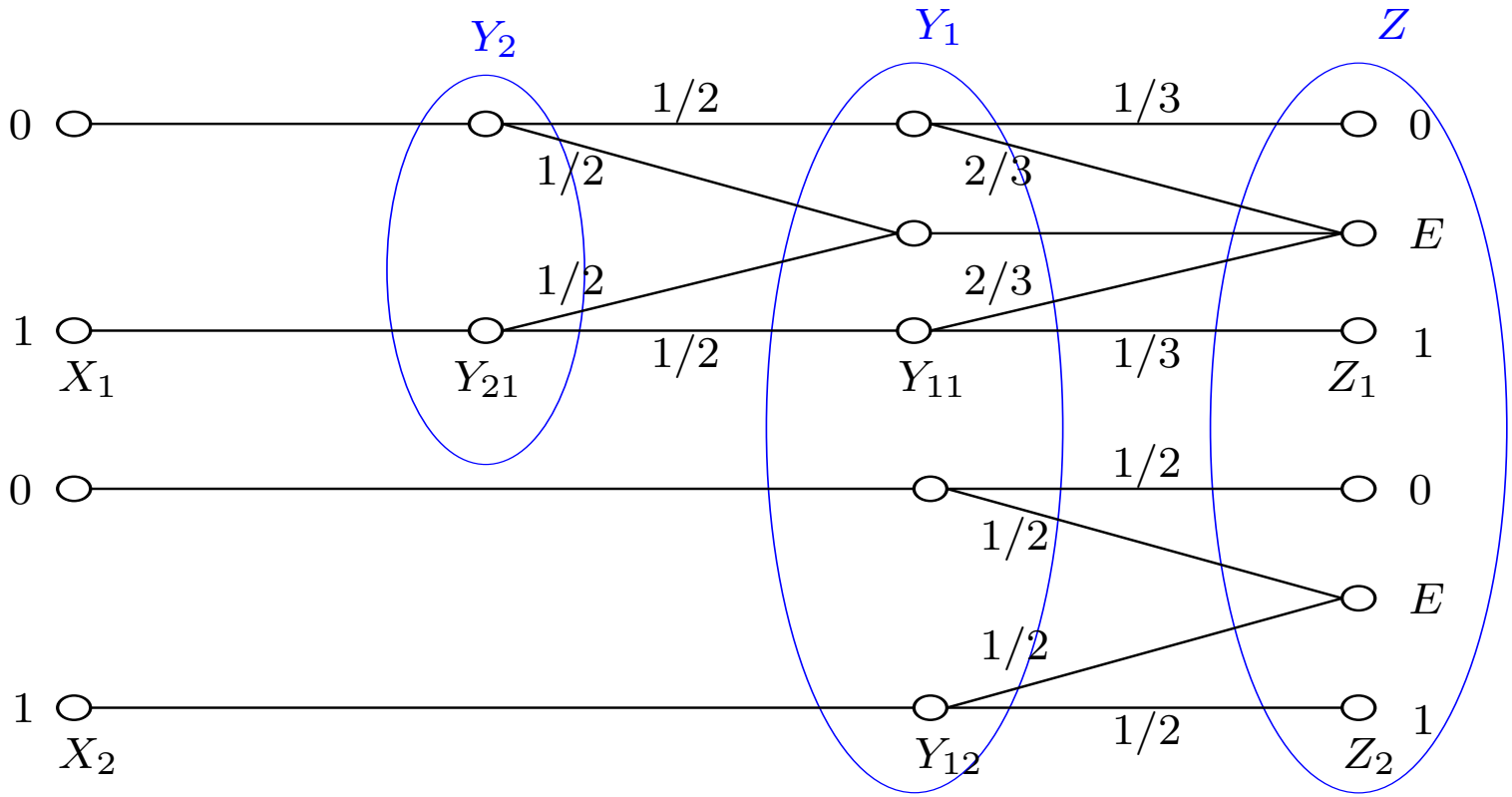


- $I(X;Y_1) - I(X;Z) \geq I(U;Y_1) - I(U;Z)$; not true in general for Y_2

New lower bound (Chia–El Gamal [7])

$$C_{\mathrm{S}} \geq \max_{p(u,x)} \min\{I(X;Y_1) - I(X;Z), I(U;Y_2) - I(U;Z)\}$$

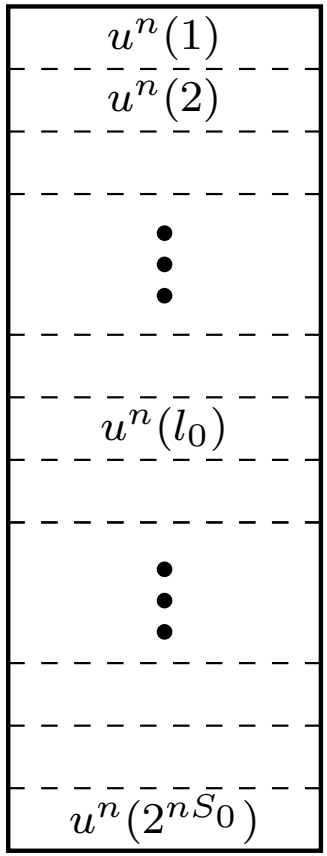
Reversely Degraded BEC Example [4]



- With Csiszár–Körner extension: Optimal secrecy rate $R < 5/6$
- With new scheme, set $U = X_1$; X_1 and X_2 independent $\mathrm{Bern}(1/2)$ $\Rightarrow C_{\mathrm{S}} = 5/6$ [8]

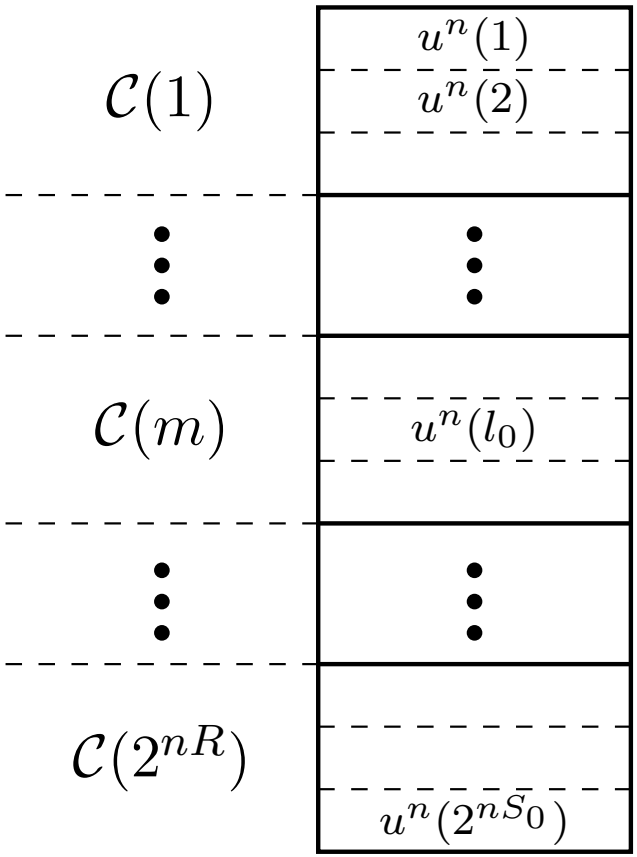
Outline of Achievability: Codebook Generation

- Generate 2^{nS_0} i.i.d. $u^n \sim \prod_{i=1}^{n} p_U(u_i)$.



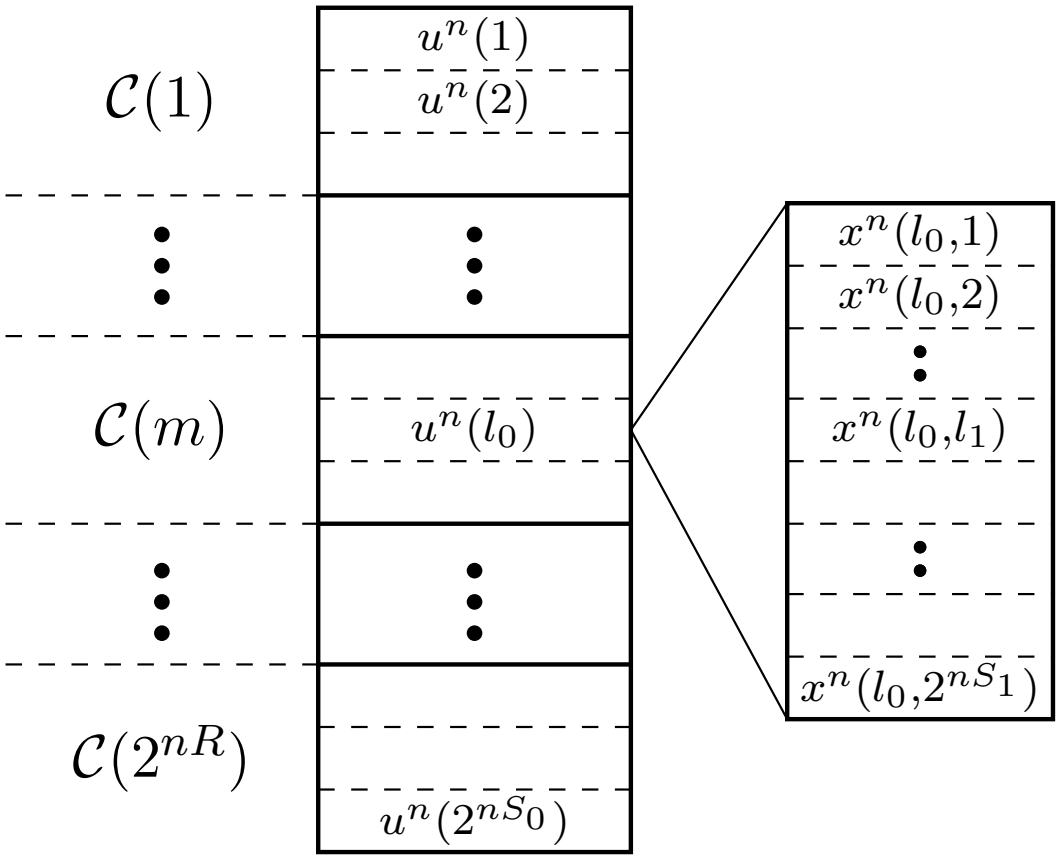
Outline of Achievability: Codebook Generation

- Generate 2^{nS_0} i.i.d. $u^n \sim \prod_{i=1}^{n} p_U(u_i)$. Partition into 2^{nR} subcodes



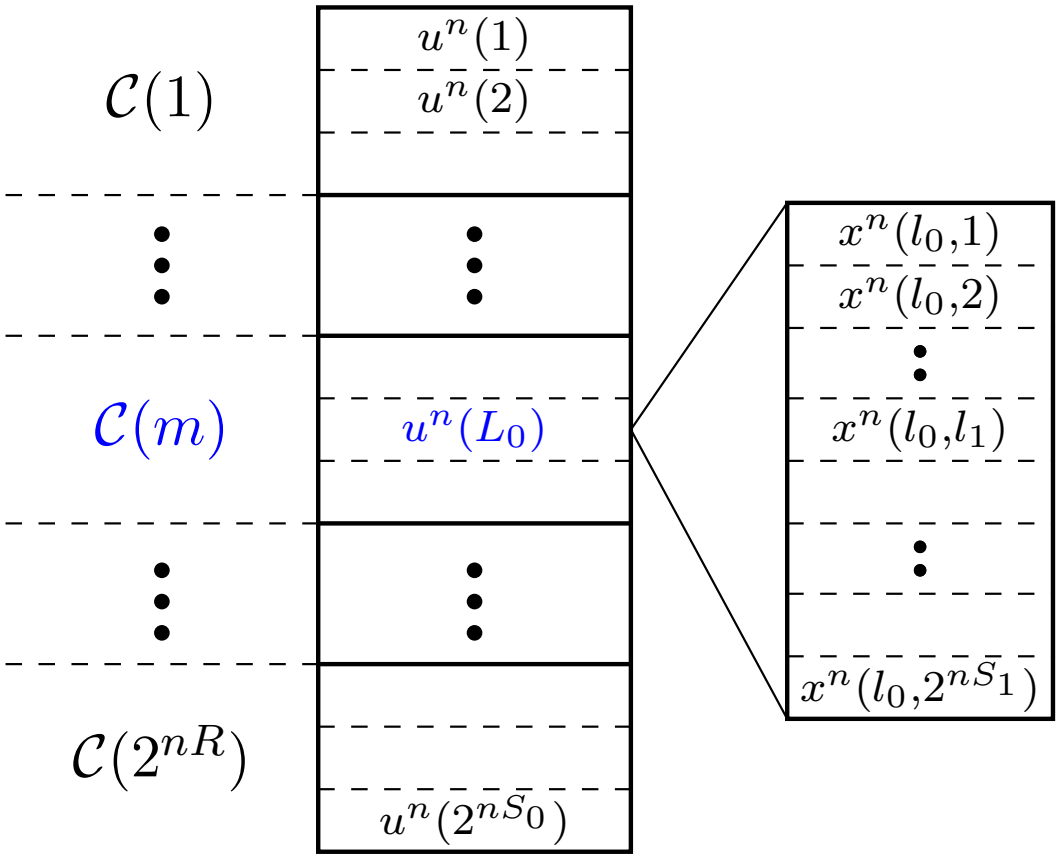
Outline of Achievability: Codebook Generation

- For each u^n, generate subcode of 2^{nS_1} conditionally i.i.d. sequences $x^n \sim \prod_{i=1}^{n} p(x_i|u_i)$



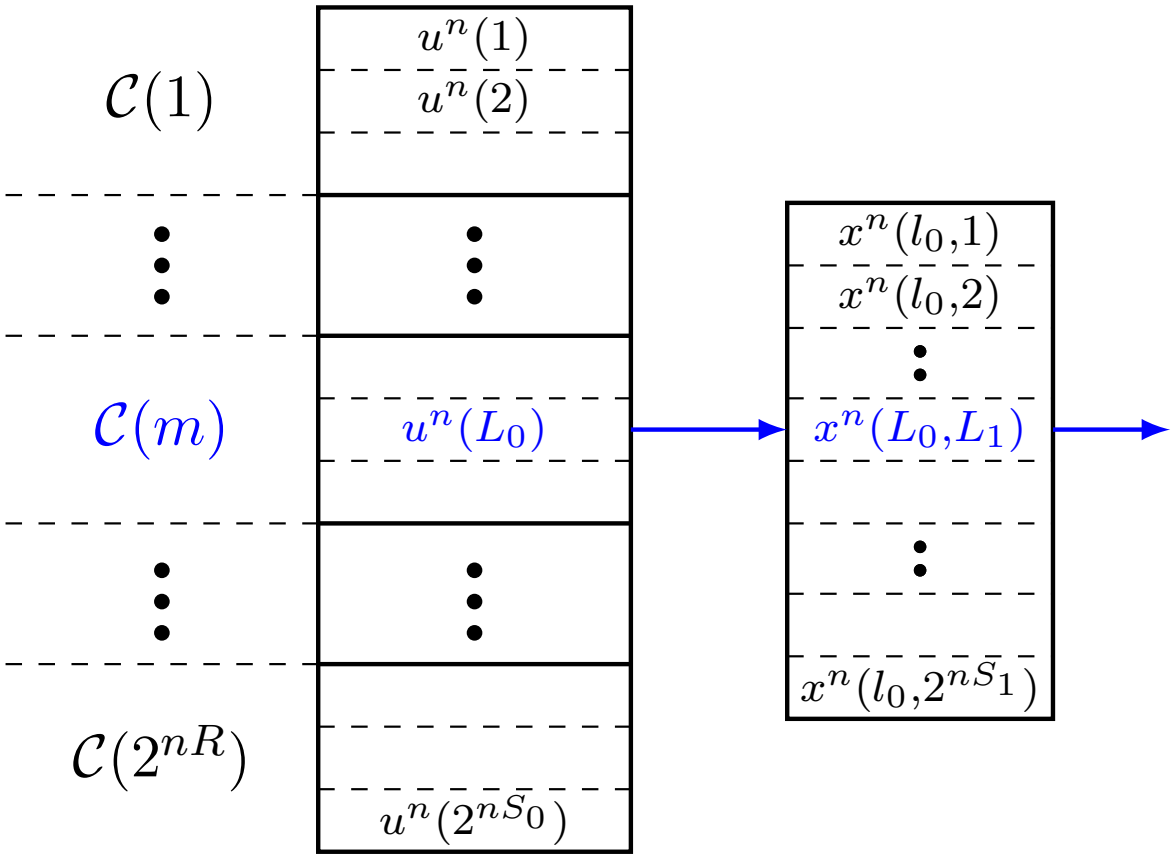
Outline of Achievability: Encoding

- To send m, choose random $u^n(L_0) \in \mathcal{C}(m)$.



Outline of Achievability: Encoding

- To send m, choose random $u^n(L_0) \in \mathcal{C}(m)$. Choose random L_1 and transmit $x^n(L_0, L_1)$



Decoding and Analysis of Secrecy Constraint

- Decoding: Y_2 finds L_0 (hence m) by decoding U directly

Decoding and Analysis of Secrecy Constraint

- Decoding: Y_2 finds L_0 (hence m) by decoding U directly

  The probability of error $\to 0$ as $n \to \infty$ if

$$S_0 < I(U; Y_2)$$

Decoding and Analysis of Secrecy Constraint

- Decoding: Y_2 finds L_0 (hence m) by decoding U directly

  The probability of error $\to 0$ as $n \to \infty$ if

  $$S_0 < I(U;Y_2)$$

- Y_1 finds L_0 indirectly through X

  The probability of error $\to 0$ as $n \to \infty$ if

  $$S_0 + S_1 < I(X;Y_1)$$

Decoding and Analysis of Secrecy Constraint

- Decoding: Y_2 finds L_0 (hence m) by decoding U directly

  The probability of error $\to 0$ as $n \to \infty$ if

$$S_0 < I(U; Y_2)$$

- Y_1 finds L_0 indirectly through X

  The probability of error $\to 0$ as $n \to \infty$ if

$$S_0 + S_1 < I(X; Y_1)$$

- Secrecy constraint: Z cannot decode L_0 directly through U if

$$S_0 - R \geq I(U; Z)$$

  Z cannot decode L_0 indirectly through X if

$$S_0 + S_1 - R \geq I(X; Z)$$

Decoding and Analysis of Secrecy Constraint

- Decoding: Y_2 finds L_0 (hence m) by decoding U directly

  The probability of error $\to 0$ as $n \to \infty$ if

  $$S_0 < I(U; Y_2)$$

- Y_1 finds L_0 indirectly through X

  The probability of error $\to 0$ as $n \to \infty$ if

  $$S_0 + S_1 < I(X; Y_1)$$

- Secrecy constraint: Z cannot decode L_0 directly through U if

  $$S_0 - R \geq I(U; Z)$$

  Z cannot decode L_0 indirectly through X if

  $$S_0 + S_1 - R \geq I(X; Z)$$

- Combining bounds and performing Fourier–Motzkin elimination completes the proof

- By using Marton coding in addition, we obtain the following:

Generalized Lower Bound (Chia–El Gamal [7])

A rate R is achievable for sending a confidential message to receivers Y_1 and Y_2, while keeping it secret from eavesdropper Z if

$$R < \min\{I(U_1;Y_1|Q) - I(U_1;Z|Q),\ I(U_2;Y_2|Q) - I(U_2;Z|Q)\},$$
$$2R < I(U_1;Y_1|Q) + I(U_2;Y_2|Q) - 2I(U_0;Z|Q) - I(U_1;U_2|U_0)$$

for some $p(q,u_0,u_1,u_2,x) = p(q)p(u_0|q)p(u_1|u_0)p(x,u_2|u_0,u_1) = p(q)p(u_0|q)p(u_2|u_0)p(x,u_1|u_0,u_2)$ such that

$$I(U_1,U_2;Z|U_0) \le I(U_1;Z|U_0) + I(U_2;Z|U_0) - I(U_1;U_2|U_0)$$

- Optimal for:
  - Both Y_1 and Y_2 are less noisy than Z
  - Reversely degraded product channels [8]
  - MIMO?

Final Remarks

- More results in poster

Final Remarks

- More results in poster
- Also, see poster on $>$ 2-user pair cyclically symmetric interference channel

Final Remarks

- More results in poster
- Also, see poster on $>$ 2-user pair cyclically symmetric interference channel
- Current work:
  - Completing work on general inner bound for DM-BC with ≥ 3 receivers
  - Completing work on wiretap channel with ≥ 3 receivers
  - Achievability scheme for 3 user-pair El Gamal–Costa deterministic interference channel
  - Compress–forward for networks

Final Remarks

- More results in poster
- Also, see poster on $>$ 2-user pair cyclically symmetric interference channel
- Current work:
  - Completing work on general inner bound for DM-BC with ≥ 3 receivers
  - Completing work on wiretap channel with ≥ 3 receivers
  - Achievability scheme for 3 user-pair El Gamal–Costa deterministic interference channel
  - Compress–forward for networks
- Important research direction because it leads to new coding techniques for networks

Acknowledgments

- The talk is based on joint work with Chandra Nair and Yeow-Khiang Chia

- Work partially supported under DARPA ITMANT

References

[1] Viveck Cadambe and Syed Ali Jafar.
Interference alignment and degrees of freedom of the k-user interference channel.
IEEE Trans. Inf. Theory, 54(8):3425–3441, 2008.

[2] János Körner and Katalin Marton.
General broadcast channels with degraded message sets.
IEEE Trans. Inf. Theory, 23(1):60–64, 1977.

[3] Shashi Borade, Lizhong Zheng, and Mitchell Trott.
Multilevel broadcast networks.
In *Proc. IEEE International Symposium on Information Theory*, pages 1151–1155, Nice, France, June 2007.

[4] Chandra Nair and Abbas El Gamal.
The capacity region of a class of 3-receiver broadcast channels with degraded message sets.
2008.

[5] A. D. Wyner.
The wire-tap channel.
Bell System Tech. J., 54(8):1355–1387, 1975.

[6] Imre Csiszár and János Körner.
Broadcast channels with confidential messages.
IEEE Trans. Inf. Theory, 24(3):339–348, 1978.

[7] Yeow-Khiang Chia and Abbas El Gamal.
3-receiver broadcast channels with common and confidential messages.
In *Proc. IEEE International Symposium on Information Theory*, Seoul, Korea, June/July 2009.

[8] Ashish Khisti, Aslan Tchamkerten, and Gregory W. Wornell.
Secure broadcasting over fading channels.
IEEE Trans. Inf. Theory, 54(6):2453–2469, 2008.