Role of Costs in Commitment over Noisy Channels

Anuj Kumar Yadav[†] & Manideep Mamindlapally[‡]

presenting at

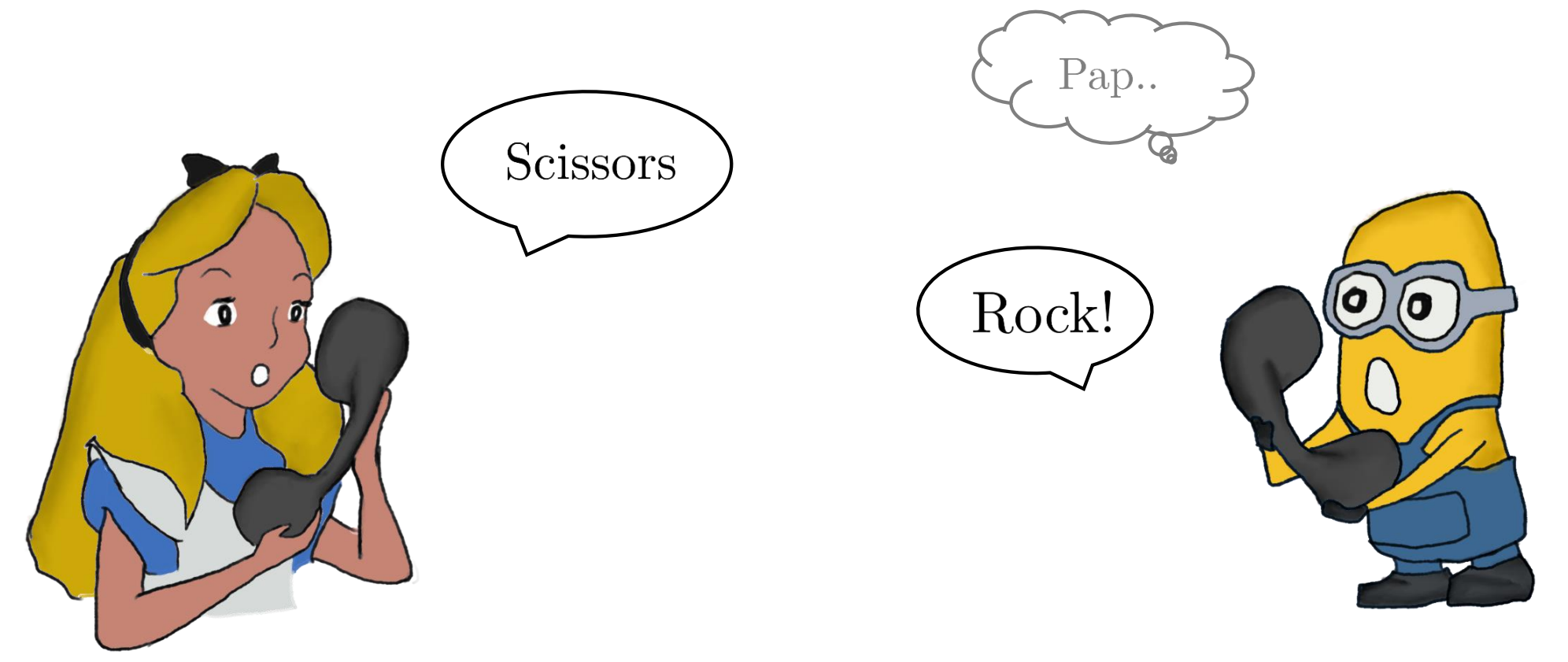
2021 IEEE NORTH AMERICAN SCHOOL OF INFORMATION THEORY

based on work accepted at (2021) ISIT [1]

†: IIT Patna (Email: 1801ee69@iitp.ac.in) ‡: IIT Kharagpur (Email: manideepyx@iitkgp.ac.in)

Motivation

Two **mutually distrustful** friends, Alice and Bob, wish to play a game of Rock-Paper-Scissors on a phone call. They simultaneously yell out their chosen hand. A bad phone signal, however, often causes unpredictable delays in the call, making it seemingly impossible to fairly play the game.



To solve this problem, one can think of a simple scheme.

Step 1: Ask Alice to write her choice on an envelope and send it over post before the phone call.

Step 2: On the phone call, Bob first yells out his hand. Alice then reveals her hand, same as the one she has sent over the post. Accordingly, a winner is decided.

Step 3: Around a week later the postal service delivers Bob, Alice's envelope. He can then verify Alice's revealed hand from earlier.

This is a raw commitment scheme that uses the **postal service** as a *resource*. That makes the scheme only **conditionally** *secure*- conditioned on the reliability of the postal service, which we call is an **active trusted third party**.

Commitment Problem

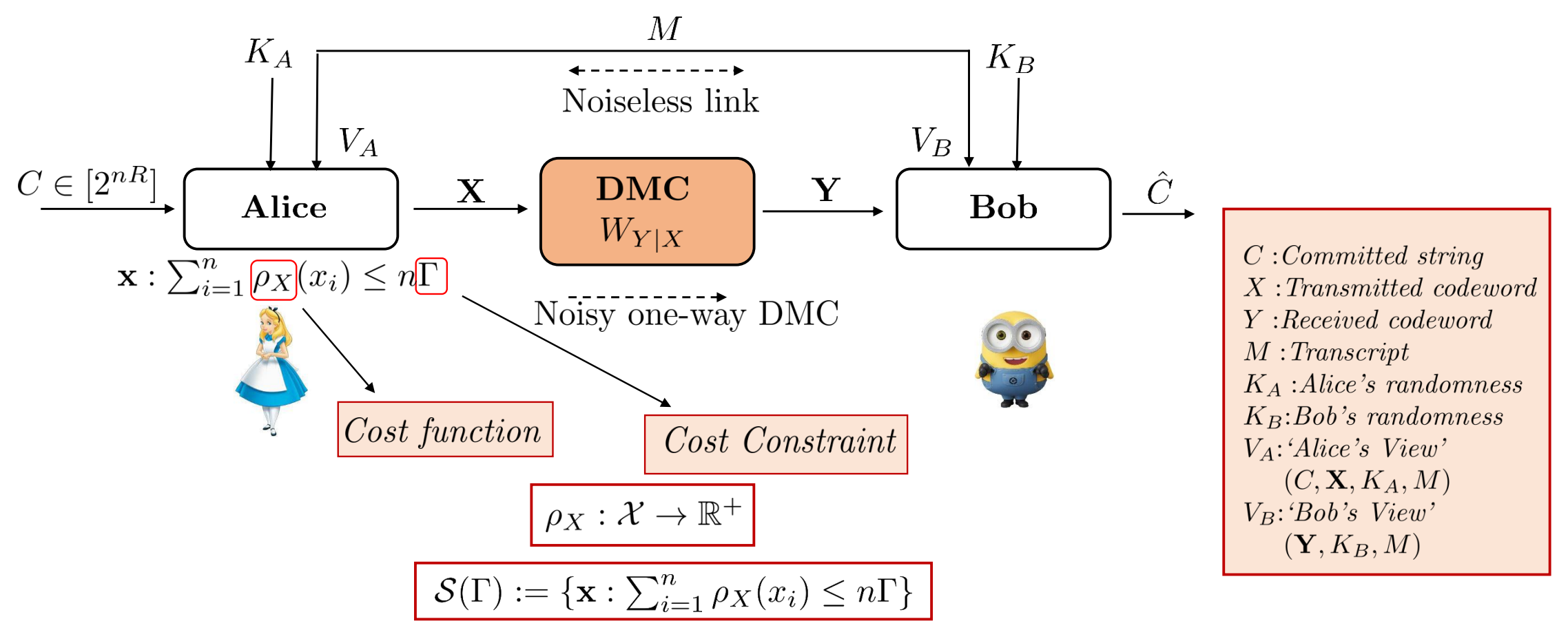
We study commitment protocols that use **noisy communication channels** as the *resource*. Such implementations can be designed to be **information-theoretically** *or* **unconditionally** *secure*. The protocol happens between **mutually distrustful** agents, Alice and Bob in two phases.

1. **Commit** phase: Alice *commits* to a string.
2. **Reveal** phase: Alice *reveals* her (*supposedly*)committed string. Bob then performs a *test* after which he either 'accepts' or 'rejects' the revealed string.

The protocol aims for three security guarantees:

Security Guarantee	**Alice's Behaviour**	**Bob's Behaviour**	**Goal**
Soundness	Honest	Honest	Bob accepts Alice's string
Concealment	Honest	Any	Conceal Alice's commit string from Bob until the reveal phase
Bindingness	Any	Honest	Not allow Alice to fool Bob by revealing a different string

Problem Setup



$\rho_X : \mathcal{X} \to \mathbb{R}^+$

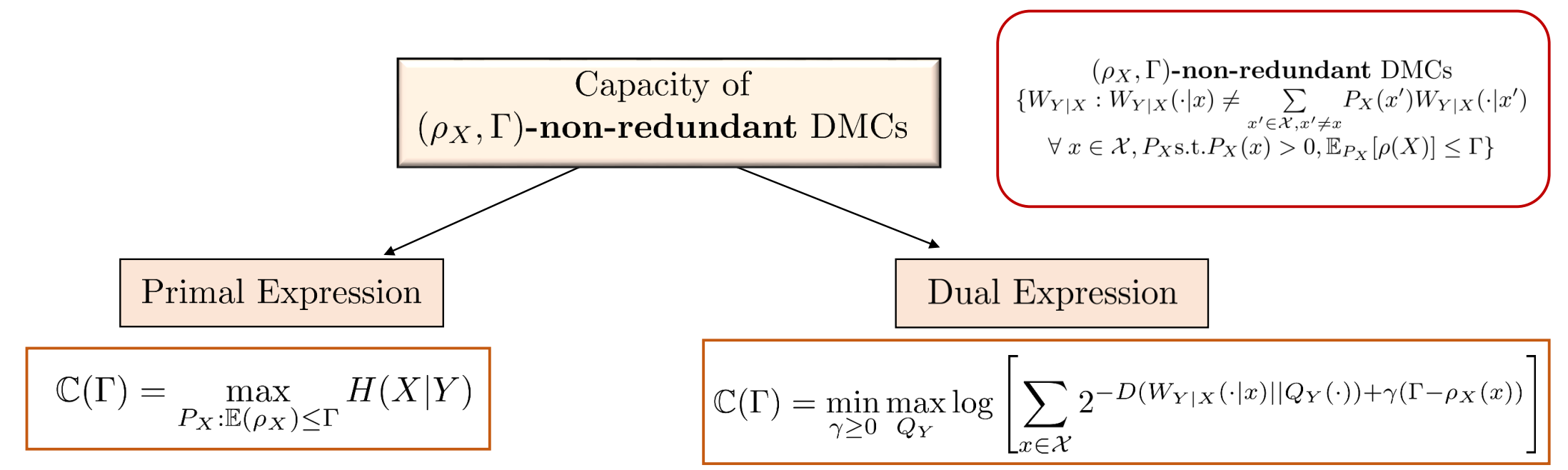
$\mathcal{S}(\Gamma) := \{\mathbf{x} : \sum_{i=1}^{n} \rho_X(x_i) \leq n\Gamma\}$

C : Committed string
X : Transmitted codeword
Y : Received codeword
M : Transcript
K_A *: Alice's randomness*
K_B*: Bob's randomness*
V_A*: 'Alice's View'* $(C, \mathbf{X}, K_A, M)$
V_B*: 'Bob's View'* $(\mathbf{Y}, K_B, M)$

Goal: To characterize Commitment Capacity for cost constrained DMCs.

COMMITMENT CAPACITY FOR DMCS UNDER NO COST CONSTRAINTS[2].

Main Results



Capacity of (ρ_X, Γ)-**non-redundant** DMCs

(ρ_X, Γ)-**non-redundant** DMCs
$\{W_{Y|X} : W_{Y|X}(\cdot|x) \neq \sum_{x' \in \mathcal{X}, x' \neq x} P_X(x') W_{Y|X}(\cdot|x')$
$\forall\, x \in \mathcal{X}, P_X \text{s.t.} P_X(x) > 0, \mathbb{E}_{P_X}[\rho(X)] \leq \Gamma\}$

Primal Expression

$$\mathbb{C}(\Gamma) = \max_{P_X : \mathbb{E}(\rho_X) \leq \Gamma} H(X|Y)$$

- Generalisation of the result by [2] for general $\rho_X : \mathcal{X} \to \mathbb{R}^+$ function
- With stronger achievability : *stronger semantic security (concealment)*
- With stronger converse : *weaker average error condition*

Dual Expression

$$\mathbb{C}(\Gamma) = \min_{\gamma \geq 0} \max_{Q_Y} \log \left[\sum_{x \in \mathcal{X}} 2^{-D(W_{Y|X}(\cdot|x)||Q_Y(\cdot)) + \gamma(\Gamma - \rho_X(x))} \right]$$

- Inspired by 'convex envelope of lines' approach [3]
- Computational aspect for capacity expression
- Unique optimising output distribution Q_Y *(while there may exist different input distributions P_X that all maximise the primal expression)*

As an example we also determine the commitment capacity (using both the primal and dual formulation) of a BSC(p) channel with Γ constraint on hamming weight costs. $\mathbb{C}_{\mathbb{BSC}}(\Gamma) = H_2(p) + H_2(\Gamma) - H_2(p \circledast \Gamma)$

Converse

In the converse, we start with an $(n, R)-$commitment protocol that is ϵ-*sound*, ϵ-*concealing*, ϵ-*binding* and then find an upper bound on R.

$$\begin{aligned}
nR = H(C) &= H(C|V_B) + I(C;V_B) \\
&\leq H(C|\mathbf{Y}, M, K_B) + \epsilon_n \\
&\leq H(C, \mathbf{X}|\mathbf{Y}, M, K_B) + \epsilon_n \\
&= H(\mathbf{X}|\mathbf{Y}, M, K_B) + H(C|\mathbf{X}, \mathbf{Y}, M, K_B) + \epsilon_n \\
&\leq H(\mathbf{X}|\mathbf{Y}) + H(C|\mathbf{X}, V_B) + \epsilon_n \\
&\leq \sum_{i=1}^{n} H(X_i|Y_i) + n\epsilon'_n + \epsilon_n \\
&\leq n \left(\sum_{i=1}^{n} \frac{1}{n} \mathbb{C}(\mathbb{E}[\rho_X(X_i)]) \right) + n\epsilon'_n + \epsilon_n \\
&\leq n\mathbb{C} \left(\frac{1}{n} \sum_{i=1}^{n} \mathbb{E}[\rho_X(X_i)] \right) + n\epsilon'_n + \epsilon_n \\
&\leq n\mathbb{C}(\Gamma) + n\epsilon'_n + \epsilon_n
\end{aligned}$$

ϵ_n-*concealing* $I(C;V_B) \leq \epsilon_n$

Lemma : $H(C|\mathbf{X}, V_B) \leq n\epsilon'_n$
$\epsilon'_n \to 0$ as $\epsilon_n \to 0$

From definition,
$\mathbb{C}(\Gamma) = \max_{P_X : \mathbb{E}(\rho_X) \leq \Gamma} H(X|Y)$
Lemma:
$\mathbb{C}(\Gamma)$ is *non-decreasing* in Γ
$\mathbb{C}(\Gamma)$ is *concave* in Γ

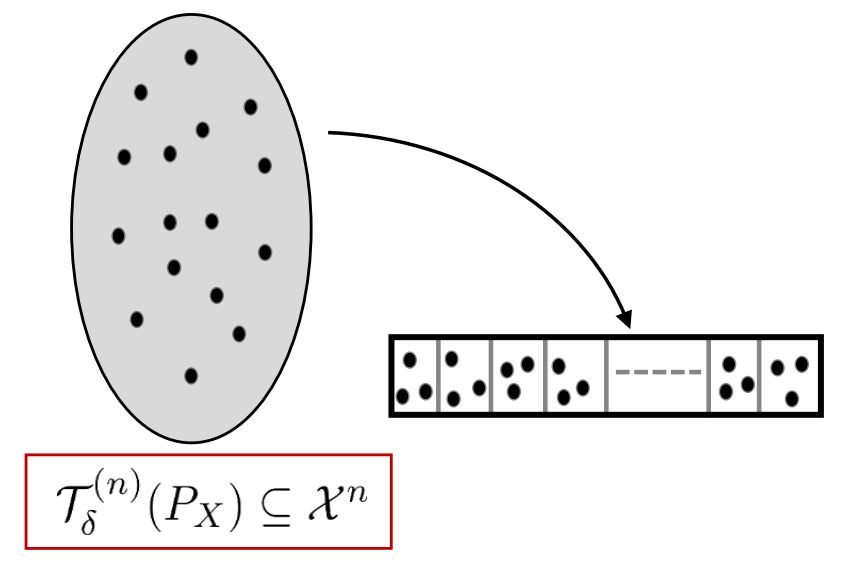
as $n \to \infty$, we have an upper bound $\boxed{R \leq \mathbb{C}(\Gamma)}$

Achievability

We present an $(n, R)-$ commitment protocol based on *random binning codebook* that employs a stochastic encoding strategy by Alice. We then, show that the protocol satisfies the security gurantees.

For an $\varepsilon > 0$, fix:

- $P_X : \mathbb{E}[\rho_X(X)] \leq \Gamma$
- Rate of bin occupancy $(\tilde{R}) = I(X;Y) + \varepsilon/2$
- Binning Rate $(R) = H(X|Y) - \varepsilon$
- Overall Rate $(R_{ov}) = R + \tilde{R} = H(X) - \varepsilon/2$



Lemma:

$\exists$ a *binned codebook*: $\mathcal{A} = \{\bar{x}_{c,k}\}$, for $c \in [2^{nR}]$, $k \in [2^{n\tilde{R}}]$, where $|\mathcal{A}| = 2^{nR_{ov}}$ and $\bar{x}_{c,k} \in \mathcal{T}_\delta^{(n)}(P_X)$, such that:

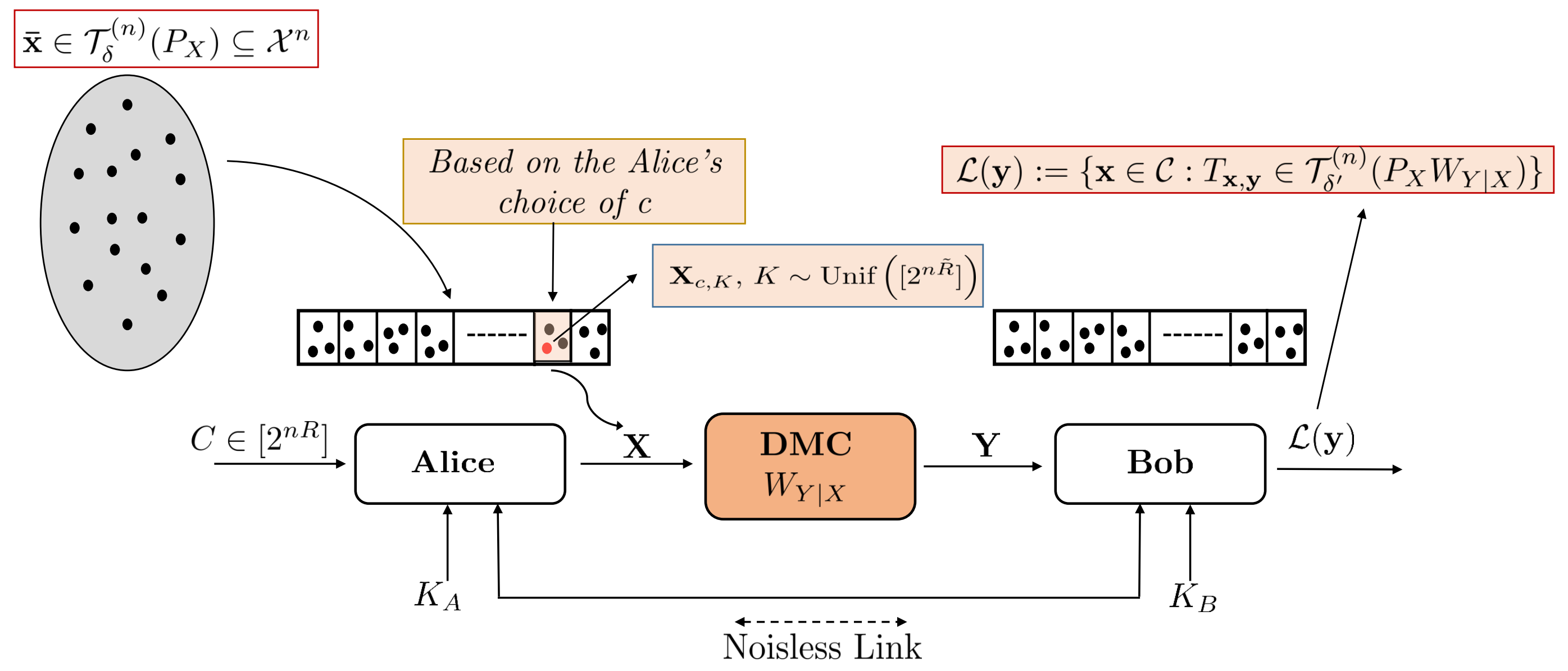
(i) $d_H(\vec{x}_{c,k}, \vec{x}_{c',k'}) \geq 2n\eta$, $\forall c \neq c'$, $c, c' \in [2^{nR}]$, $k, k' \in [2^{n\tilde{R}}]$ — *"minimum distance across bins* property"

(ii) for every $c \in [2^{nR}]$,

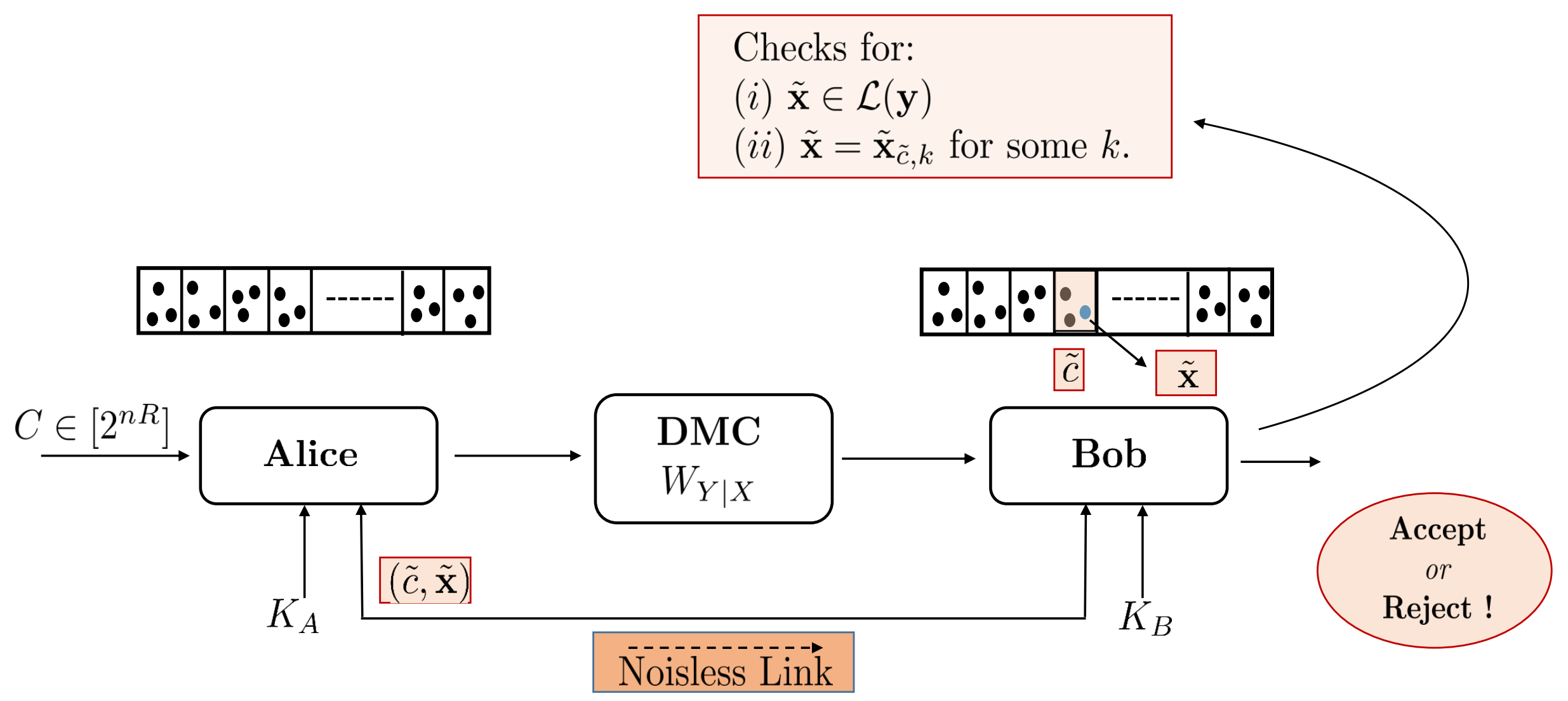
$$D \left(\frac{1}{2^{n\tilde{R}}} \sum_{k=1}^{2^{n\tilde{R}}} W_{Y|X}^{(n)}(\vec{y}|\vec{x}_{c,k}) \middle|\middle| [P_X W_{Y|X}]_Y^{(n)}(\vec{y}) \right) \leq e^{-n\alpha}$$

for some $\alpha(\delta) > 0$, where $\alpha \to 0$ as $\delta \to 0$. — *"Output distribution simulation* property"

Commit Phase



Reveal Phase



Achievability: Analysis of Security Guarantees

Soundness ✓

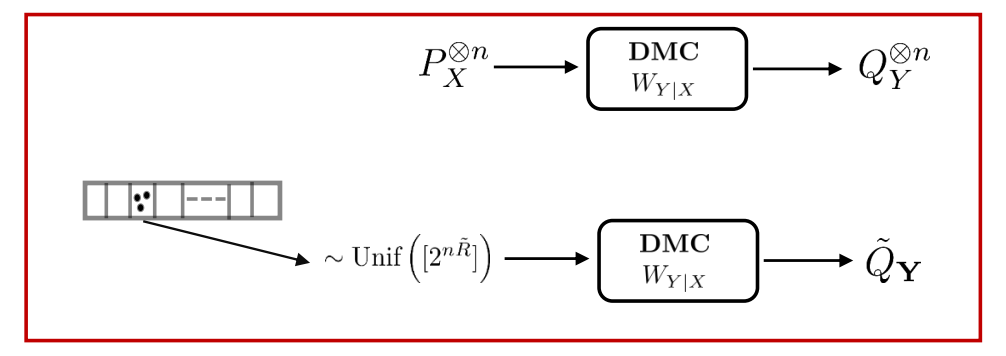
- *Analysing the probability of error* $\mathbf{P}\{\mathbf{X} \notin \mathcal{L}(\mathbf{Y})\}$
- *Using Chernoff Bound,* $\mathbf{P}\{\mathbf{X} \notin \mathcal{L}(\mathbf{Y})\} \leq \epsilon$

$\mathbb{P}(T(C, \mathbf{X}, V_B) = REJECT) \leq \epsilon$

Concealment ✓

$I(C;V_B) \leq \epsilon$

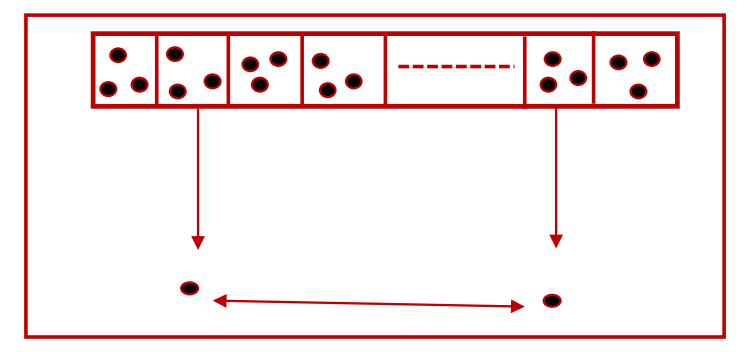
Follows from the ***"Output distribution simulation property"*** *of the constructed random binning codebook.*



Binding ✓

$\mathbb{P}\left(T(\bar{c}, \bar{\mathbf{X}}, V_B) = ACCEPT \ \ \& \ \ T(\hat{c}, \hat{\mathbf{X}}, V_B) = ACCEPT\right) \leq \epsilon$
$\forall (\bar{c}, \bar{\mathbf{X}}), (\hat{c}, \hat{\mathbf{X}}) \ : \ \bar{c} \neq \hat{c}$

Follows from the ***"Minimum distance across bins property"*** *of the constructed random binning codebook.*



The "*Achievability*" and the "*Converse*" proofs settle the primal capacity expression.

Dual Characterization

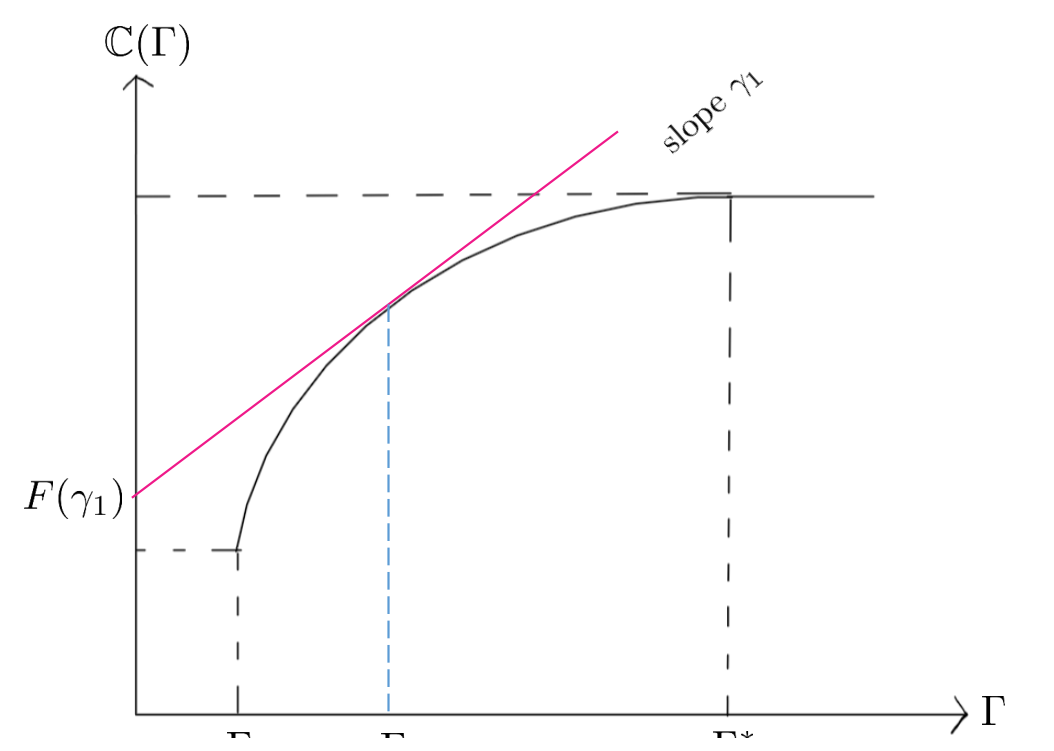
Having proved the primal capacity expression, $\mathbb{C}(\Gamma) = \max_{P_X : \mathbb{E}(\rho_X) \leq \Gamma} H(X|Y)$ we now find a dual characterisation for this optimisation expression.

Recall, $\mathbb{C}(\Gamma)$ is **non-decreasing**, **concave** in Γ. We now plot graph of a general function with such behaviour and observe it in an interval $[\Gamma_0, \Gamma^*]$

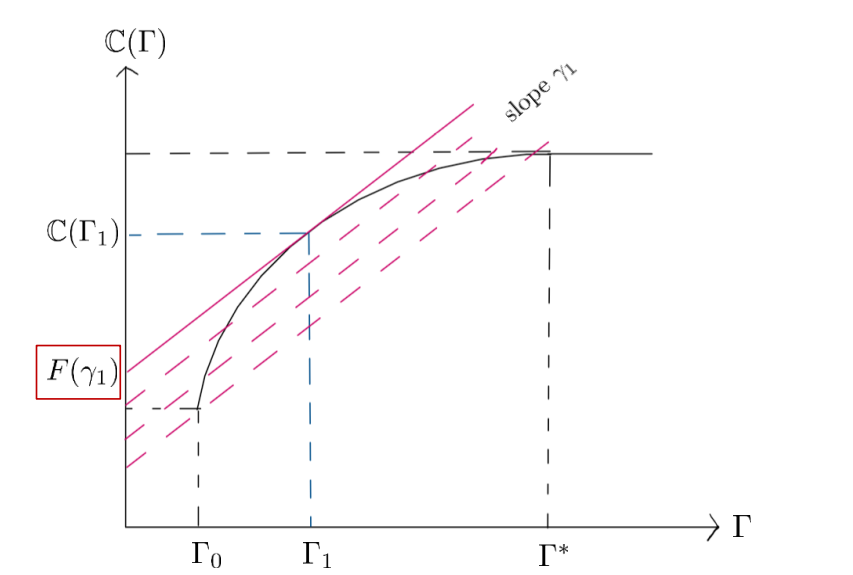
$$\Gamma_0 := \min_x \rho_X(x)$$

$$\Gamma^* := \min\{\Gamma : \mathbb{C}(\Gamma) = \mathbb{C}(\infty)\}$$

For $\Gamma_1 \in [\Gamma_0, \Gamma^*]$, we define
γ_1 : slope of the tangent to $\mathbb{C}(\Gamma)$ at Γ_1
$F(\gamma_1)$: corresponding $y-$intercept

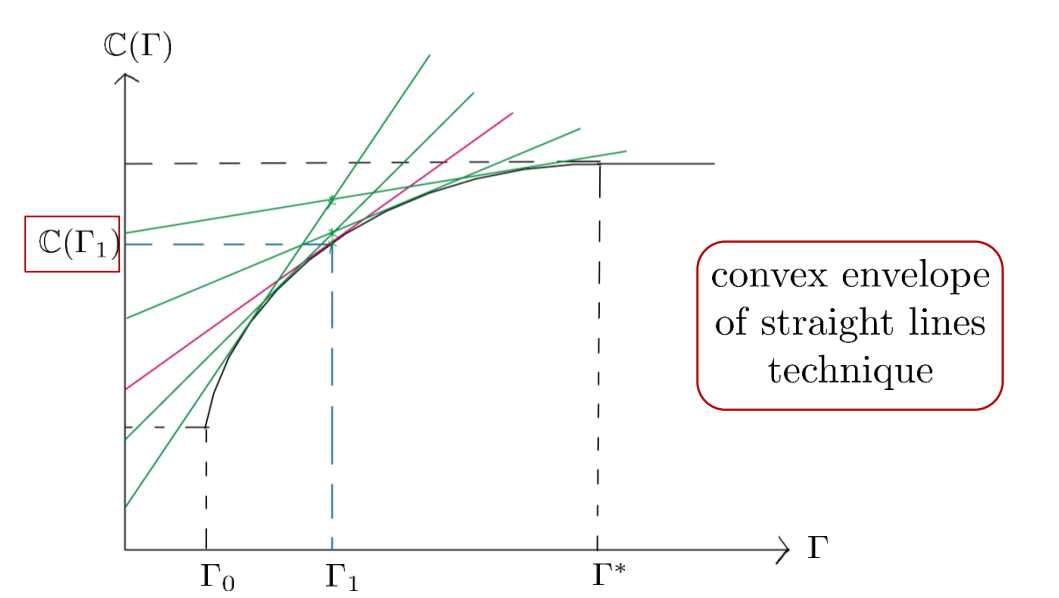


Plotting a family of γ_1-sloped parallel lines over $\mathbb{C}(\Gamma)$ curve



$F(\gamma_1) = \max_{\Gamma} [\mathbb{C}(\Gamma_1) - \gamma_1\Gamma]$

Plotting a family of tangents to $\mathbb{C}(\Gamma)$ curve



$\mathbb{C}(\Gamma_1) = \min_{\gamma \geq 0} [F(\gamma) + \gamma\Gamma_1]$

From this and other non-trivial techniques we arrive at this expression

$$\mathbb{C}(\Gamma) = \min_{\gamma \geq 0} \left[\max_{Q_Y} \log \left(\sum_{x \in \mathcal{X}} \exp[-D(W_{Y|X}(\cdot|x)||Q_Y) - \gamma\rho_X(x)] \right) + \gamma\Gamma \right]$$

References

[1]. M. Mamindlapally, A. K. Yadav, M. Mishra and A. J. Budkuley, "Commitment Capacity under Cost Constraints," in 2021 IEEE International Symposium on Information Theory (ISIT), Australia.

[2]. A. Winter, A. C. A. Nascimento, and H. Imai, "Commitment capacity of discrete memoryless channels," in IMA International Conference on Cryptography and Coding. Springer, 2003, pp. 35˘51.

[3]. Csiszár, Imre, and Jànos Körner. Information theory: coding theorems for discrete memoryless systems. Cambridge University Press, 2011.