Lecture 22 : Distributed Function Computation

Instructor: Rajesh Sundaresan *Scribe: Premkumar K.*

1 Achievable Rate Region for Computation of Some Functions

Recall: SW problem. Suppose now we wish to compute a function of X_1X_2 instead of reproducing X_1X_2 at the output.

- (X_1, X_2) discrete memoryless multi source
- $F(X_1, X_2)$ an arbirary function of $X_{[2]}$
- $f_k : \mathbb{X}_k^n \to [\mathbb{M}_k], k = 1, 2$ (Encoders)
- $g : [\mathbb{M}_1] \times [\mathbb{M}_2] \to \mathbb{Z}^n$ (Decoder)
- $R_k := \frac{1}{n} \log |\mathbb{M}_k|, k = 1, 2$
- $P_e^{(n)} := pr\{F(X_1^n, X_2^n) \neq g(f_1(X_1^n), f_2(X_2^n))\}$
- (R_1, R_2) is achievable for F if $\forall \eta > 0, \lambda \in (0, 1)$, $\exists f_k, g, \mathbb{M}_k, k = 1, 2$ such that

$$\begin{aligned} \frac{\log M_k}{n} &\underset{n}{\leqslant} R_k + \eta, \quad k = 1, 2 \\ P_e^{(n)} &\underset{n}{\leqslant} \lambda, \quad k = 1, 2 \end{aligned}$$

- Achievable rate region is the set of all achievable rate pairs.

Example 1: $F(X_1X_2) = X_1X_2$ (Slepian–Wolf)
Achievable rate region is the SW region

$$\left\{ (R_1, R_2) \in \mathbb{R}_+^2 \;\middle|\; \begin{aligned} R_1 &\geqslant H(X_1|X_2) \\ R_2 &\geqslant H(X_2|X_1) \\ R_1 + R_2 &\geqslant H(X_1X_2) \end{aligned} \right\}$$

Remarks: (1) SW region depends on $p_{X_1X_2}$
(2) Since $H(X_1|X_2)$, $H(X_2|X_1)$, $H(X_1X_2)$ are continous functions of $p_{X_1X_2}$, the rate region is continuous in some sense.

Example 2: $F(X_1X_2)$ is given by

	0	1
0	0	0
1	1	2

SW region is given by $H(X_1|X_2) = H(2\delta)$, $H(X_2|X_1) = H(1/2)$, $H(X_1X_2) = \log 2 + H(2\delta)$. As $\delta \downarrow 0$, $\{R_1 \geqslant 0, R_2 \geqslant 1\}$.
Claim: It turns out that when $\delta > 0$, this is indeed the achievable rate region to compute F. However when $\delta = 0$, achievable rate region is $\{R_1 \geqslant 0, R - 2 \geqslant 0\}$ which is different from the SW region.
Remark: Achievable rate region is not continous in $p_{X_1X_2}$. Notation : $\mathscr{R}(F)$.
Example 3: $\mathbb{X}_1 = \mathbb{X}_2 = \{0, 1\}$. $F(X_1X_2) = X_1 \oplus X_2$.
claim:

- Achievable rate region is $\{R_1 \geqslant H(Z), R_2 \geqslant H(Z)\}$ (Korner–Marton 1979).
- Can extend to $\mathbb{X}_k = \mathbb{F}_q$, q prime, $F(X_1X_2) = X_1 + X_2$, where "$+$" is the same operator as in $\mathbb{F}_q$.

Technique: (Ahlswede–Han 1983, Elias)

- If Z is a DMS on $\mathbb{F}_q$, then $\forall \epsilon > 0, \lambda \in (0,1)$, sufficiently large n, $\exists\ A \in \mathbb{F}_q^{m\times n}$, $g : \mathbb{F}_q^m \to \mathbb{F}_q^n$ such that

  1. $m \log q \leqslant nH(Z) + \epsilon$
  2. $\Pr\left\{ \begin{pmatrix} Z_1 \\ \cdots \\ Z_n \end{pmatrix} \neq g\left(A \begin{pmatrix} Z_1 \\ \cdots \\ Z_n \end{pmatrix} \right) \right\} \leqslant \lambda$

- Each terminal sends $A \begin{pmatrix} Z_1 \\ \cdots \\ Z_n \end{pmatrix}$ using $m \log q$ bits. Decoder sums $\sum_{k=1}^{2} AX_k^n$, then applies g. ■

- Motivated by Example 2, since we would like to avoid discontinuous regions (as a function of $p_{X_1X_2}$), we focus on $|\mathbb{X}_k| \geqslant 2$, and

  Definition 1 (Definition). $\mathscr{P} := \left\{ p_{X_1X_2} : p_{X_1X_2}(x_1x_2) > 0,\ \forall x_{[2]} \in \mathbb{X}_{[2]} \right\}$

- If a function F requires rates corresponding to the SW region regardless of $p_{X_{[2]}} \in \mathscr{P}$, does not admit distributed computation.

  Definition 2 (Definition). $\mathscr{C}_1 := \left\{ F : \forall p_{X_{[2]}} \in \mathscr{P},\ \ \textit{the achievable rate region equals the SW region} \right\}$

Theorem 1. $X_{[2]} \in \mathscr{P}$. *Arrange F as a matrix of size $|\mathbb{X}_1| \times |\mathbb{X}_2|$.*
(1) If any two rows of the F matrix are different, then every achievable rate pair for F satisfies $R_1 \geqslant H(X_1|X_2)$. — (a)
(2) If any two columns of the F matrix are different, then every achievable rate pair for F satisfies $R_2 \geqslant H(X_2|X_1)$ — (b)
(3) If (a) and (b) hold, and $k_1 \neq k_2$, $h_1 \neq h_2 \implies F(k_1h_1) \neq F(_2h_2)$, — (c) then every achievable rate pair for F satisfies $R_1 + R_2 \geqslant H(X_1X_2)$.

Remark:

- Revisit Example 2. F matrix satisfies all conditions $(a), (b), (c)$. So the achievable rate region coincides with the SW region when $\delta > 0$.

- Proof makes an ingenious use of Fano's inequality.

Theorem 2. *The achievable rate region for F equals the SW region for every $p_{X_{[2]}} \in \mathscr{P}$ if and only if the F matrix satisfies $(a), (b)$, and (c) above.*

Remark:

- The functions that do not admit distributed computation, i.e., the class $\mathscr{C}_1$, are completely charaterised by readily checkable conditions $(a), (b), (c)$ of the F matrix. This is so regardless of the statistics of the source, so long as $p_{X_{[2]}} \in \mathscr{P}$.

- It is insightful to see the necessity of (a).

  Suppose (a) does not hold. $F(k_1, h) = F(k_2, h), \forall h \in \mathbb{X}_2$, $(k_1 \neq k_2)$. Define $\mathbb{X}_1' = \mathbb{X}_1 - \{k_2\}$ as

  (1) $p_{X_1'X_2}(k_1h) = p_{X_1X_2}(k_1, h) + p_{X_1X_2}(k_2, h)$
  (2) $p_{X_1'X_2}(kh) = p_{X_1X_2}(k, h),\ k \neq k_1$

  Clearly $p_{X_1'X_2} \in \mathscr{P}$ on $\mathbb{X}_1'\mathbb{X}_2$.
  Now, $\mathscr{R}(F) \supseteq \mathscr{R}\left((X_1', X_2)\right) \cup \mathscr{R}\left((X_1, X_2)\right) \supsetneq \mathscr{R}\left((X_1, X_2)\right)$ since $H(X_1|X_2) > H(X_1'|X_2)$. ■

- It is also insightful to look at the necessity of (c). If (c) fails, then $\exists$ submatrix such that

$$\begin{array}{c|cc} & h_1 & h_2 \\ \hline k_1 & 0 & 0 \\ k_2 & 0 & 0 \end{array} \text{ or } \begin{array}{c|cc} & h_1 & h_2 \\ \hline k_1 & 0 & 0 \\ k_2 & X & 0 \end{array} \text{ or } \begin{array}{c|cc} & h_1 & h_2 \\ \hline k_1 & 0 & \Delta \\ k_2 & X & 0 \end{array}$$

- Focus on (3): If (3) is easy (i.e., requires lesser rate than SW) (1) and (2) are easier.
- Further consider (3') which is all different elements except (k_1h_1) and (k_2h_2). If (3') is easy so is (3).
- Now consider a 1–1 mapping of the range of F with that of another F'. Then we can compute F' easily and reliably, and then map to F.
- F'. $a = |\mathbb{X}_1| = |\mathbb{X}_1'|$, $b = |\mathbb{X}_2| = |\mathbb{X}_2'|$, $\mathbb{X}_1' = \{0, 1, 2, \cdots, a-1\}$, $\mathbb{X}_2' = \{0, a-1, 2a-1, \cdots, (b-1)a-1\}$, $F' = (x_1' + x_2')$

  In $\mathbb{X}_2'$, there is only one gap of $a-1$. Others are a. So $F'(0, a-1) = F'(a-1, 0)$. All other evaluations are distinct. Every value between 0 and $ab-2$ is taken. $(a-1)$ taken twice. Choose $q > ab-2$.
- $\Pr\{x_1'x_2'\} := \begin{cases} \frac{1-\delta}{2}, & (x_1'x_2') = (0, a-1) \text{ or } (a-1, 0) \\ \frac{\delta}{ab-2}, & \text{otherwise} \end{cases}$
- $(H(Z), H(Z))$ is achievable. $H(Z) = H(\delta) + \delta \log(ab-2) \to 0$.
- On the other hand, SW region has $R_1 + R_2 \geqslant (1-\delta)\log 2 + H(\delta) + \delta \log(ab-2) \to \log 2$.
- By choosing δ sufficiently small, yet > 0, we can make

  $2H(\delta) + 2\delta \log(ab-2) < (1-\delta)\log 2 + H(\delta) + \delta \log(ab-2)$.

  So $(H(\delta) + \delta \log(ab-2), H(\delta) + \delta \log(ab-2)) \notin$ SW, yet is achievable for F' (and therefore F).

2 Generalisations

- $\mathscr{R}(F) =$ SW region $\forall p_{X_{[J]}} \in \mathscr{P}$, $F \in \mathscr{C}_1$ implies the following condition.

  (0) $\forall S, \forall x_S', x_S'' \in \mathbb{X}_S$ such that $x_j' \neq x_j'', j \in S$, there exists some $x_{S^c} \in \mathbb{X}_{S^c}$ such that $F(x_S' x_{S^c}) \neq F(x_S'' x_{S^c})$ (necessity).
- Suppose

  (1) $\forall i, \forall x_{[J]\}\{i\}}', x_{[J]\}\{i\}}'', x_{[J]\}\{i\}}' \neq x_{[J]\}\{i\}}''$, $\exists x_i \in \mathbb{X}_i$ such that

  $F(x_{[J]\}\{i\}}', x_i) \neq F(x_{[J]\}\{i\}}'', x_i)$

  (2) $\forall z$, all the elements of $F^{-1}(\{z\})$ agree on some component $j \in [J]$. Then $F \in \mathscr{C}_1$ (sufficiency).

  Remarks:
- condition (1) implies the necessity condition (0) for all S with $|S| < J$ (use contrapositive).
- (0) $\implies (a), (b), (c)$ when $J = 2$.
- (1) and (2) $\implies (a), (b), (c)$ when $J = 2$.
- What is the condition to identify elements of $\mathscr{C}_1$? Open.