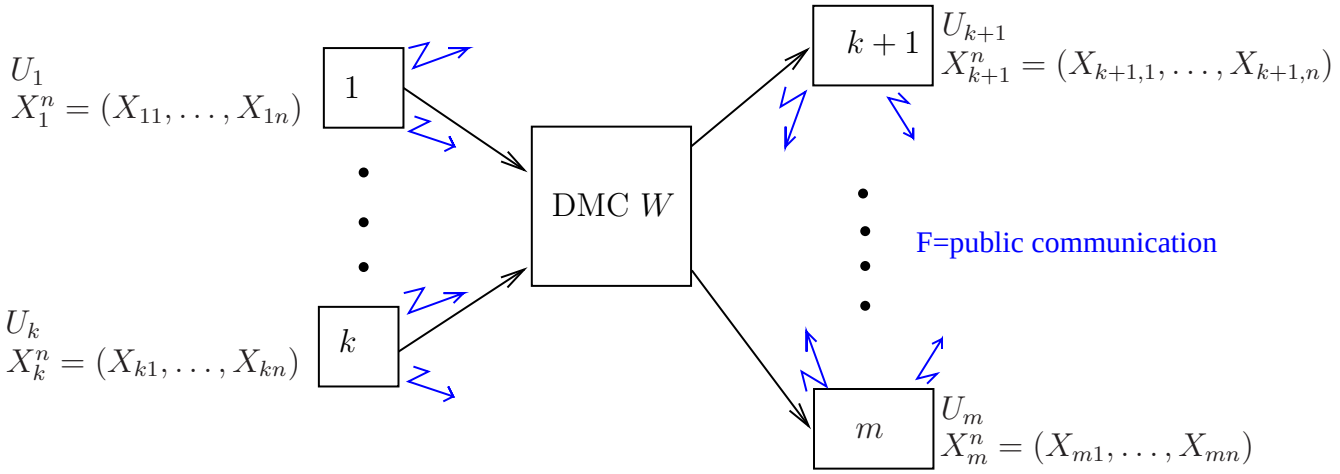
Multiaccess Channels, Feedback and Secrecy Generation

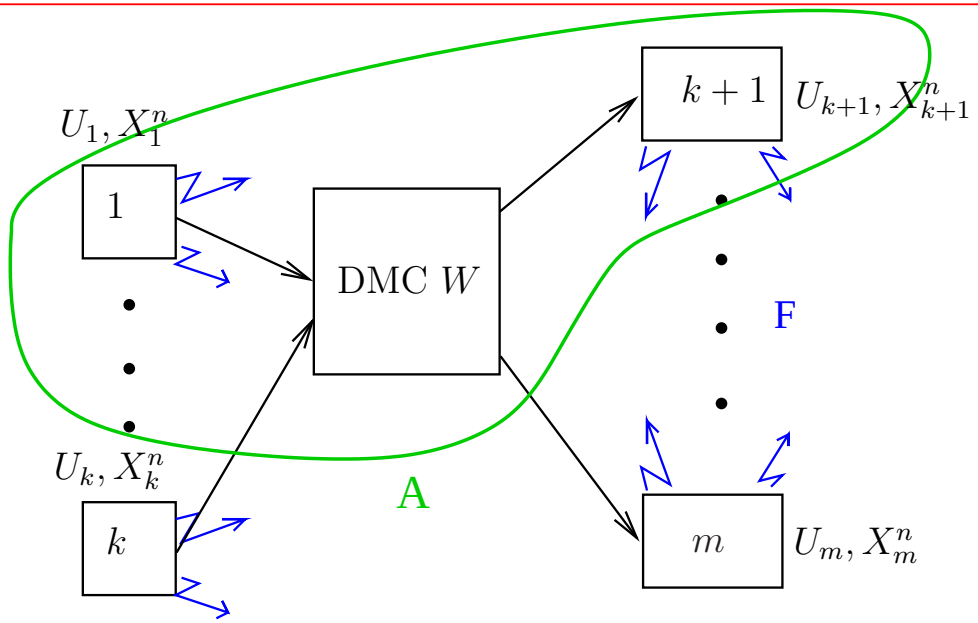
Imre Csiszár Prakash Narayan

Multiterminal Channel Model



- Terminals $1, \ldots, m$ cooperate in secrecy generation.
- Terminals $1, \ldots, k$ govern the inputs of a *secure* DMC W, with input terminal i transmitting a sequence $X_i^n = (X_{i1}, \ldots, X_{in})$ of length n which is not necessarily i.i.d. Terminals $k+1, \ldots, m$ observe the corresponding output sequences, with output terminal i observing X_i^n of length n.
- Following each simultaneous transmission of symbols over the DMC, communication over a *public noiseless channel of unlimited capacity* is allowed among all the terminals, perhaps interactively, and observed by all the terminals. Let $\mathbf{F}$ denote collectively all such public communication.
- Randomization is permitted at the terminals, and is modeled by the rvs $U_i,\ i = 1, \ldots, m$, which are taken to be mutually independent.

Secret Key



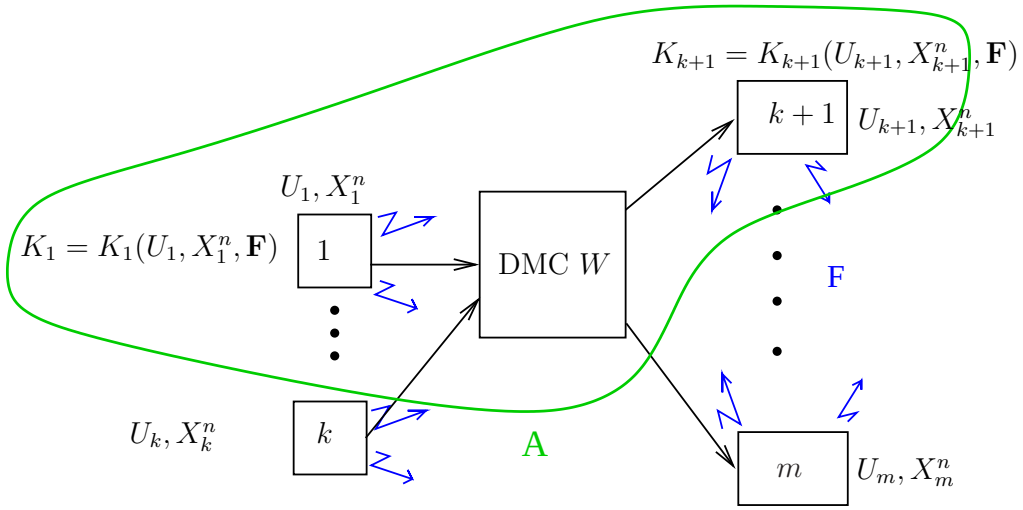
Objective: To generate a *secret key* at the largest rate for a given set $A \subseteq \mathcal{M} = \{1, \ldots, m\}$ of terminals, $|A| \geq 2$, i.e., *common randomness* shared by the terminals in A, which is

- of near uniform distribution;
- concealed from an eavesdropper that observes the public communication $\mathbf{F}$.

All the terminals in $\mathcal{M} = \{1, \ldots, m\}$ cooperate in achieving this goal.

Assume: The eavesdropper is passive and cannot wiretap.

Secret Key Capacity



- *Common randomness*: $\Pr\{K = K_i,\ i \in A\} \cong 1$.
- *Secrecy & Uniformity*: Security index

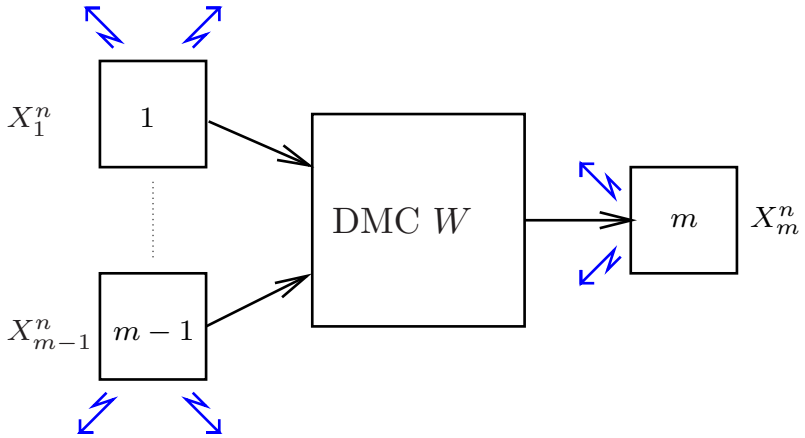
$$s(K;\mathbf{F}) \stackrel{\triangle}{=} \log|\mathcal{K}| - H(K|\mathbf{F}) = I\left(K \wedge \mathbf{F}\right) + \log|\mathcal{K}| - H(K) \cong 0.$$

Thus, a secret key (SK) is effectively concealed from an eavesdropper with access to $\mathbf{F}$, and is nearly uniformly distributed.

SK capacity $C_S(A)$ = largest achievable rate $\frac{1}{n}\log|\mathcal{K}^{(n)}|$ of such a SK for A.

Throughout this talk: $A = \mathcal{M}$ and $C_S(A) = C_S(\mathcal{M}) \equiv C_S$.

Channel with Single Output: SK Capacity and MAC Capacity Region



- Consider the DMC $W : \mathcal{X}_1 \times \cdots \times \mathcal{X}_{m-1} \to \mathcal{X}_m$.
- Let $\mathcal{C} =$ (average) error capacity region of the MAC W.

Theorem 1:

$$C_S \;\geq\; \max\Big\{R : (R, \ldots, R) \in \mathcal{C}\Big\}.$$

Further, any R such that $(R, \ldots, R) \in \mathcal{C}$ can be achieved as an SK rate with no public communication by the input terminals and with only the output terminal m sending a public message.

Proof of Theorem 1

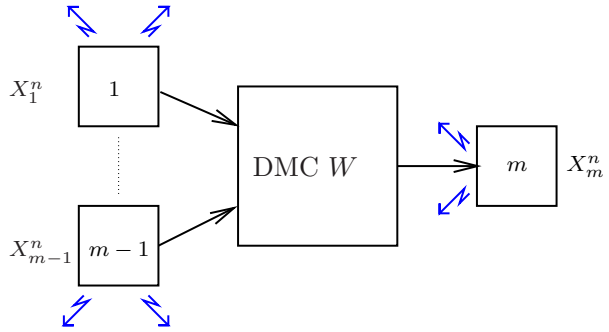
- If $(R, \ldots, R) \in \mathcal{C}$, $\exists$
  - mutually independent rvs $K_i,\ i \in \{1, \ldots, m-1\}$, with each $K_i \sim$ unif. $\mathcal{K}$;
  - encoders $f_i : \mathcal{K} \ \to \ \mathcal{X}_i^n,\ i \in \{1, \ldots, m-1\}$ with $|\mathcal{K}| \cong \exp(nR)$;
  - and a decoder $\phi : \mathcal{X}_m^n \ \to \ \mathcal{K} \times \cdots \times \mathcal{K}$,

  such that ϕ recovers the rvs $K_i,\ i \in \{1, \ldots, m-1\}$ from the MAC output X_m^n w.p. $\to 1$ as $n \to \infty$.
- Arbitrarily fix $i_1 \in \{1, \ldots, m-1\}$. Terminal m broadcasts $K_{i_1} + K_i \mod |\mathcal{K}|,\ i \in \{1, \ldots, m-1\} \backslash \{i_1\}$.
- All the terminals recover K_{i_1}, and $K_{i_1} \ \perp\!\!\!\perp \ \left(K_{i_1} + K_i \mod |\mathcal{K}|\right)_{i \in \{1,\ldots,m-1\}\backslash\{i_1\}}$.
- $\implies$ K_1 is a SK of rate R. $\square$

$$\boxed{\textbf{OP: Is } C_S \ = \ \max\Big\{R : (R, \ldots, R) \in \mathcal{C}\Big\}?}$$

We have examples where equality holds, but know of no counterexample.

Channel with Single Output: SK Capacity and MAC Capacity Region



Theorem 2: $C_S > 0$ iff $\exists\ (R_1, \ldots, R_{m-1}) \in \mathcal{C}$ such that $R_i > 0$ for each $i \in \{1, \ldots, m-1\}$.

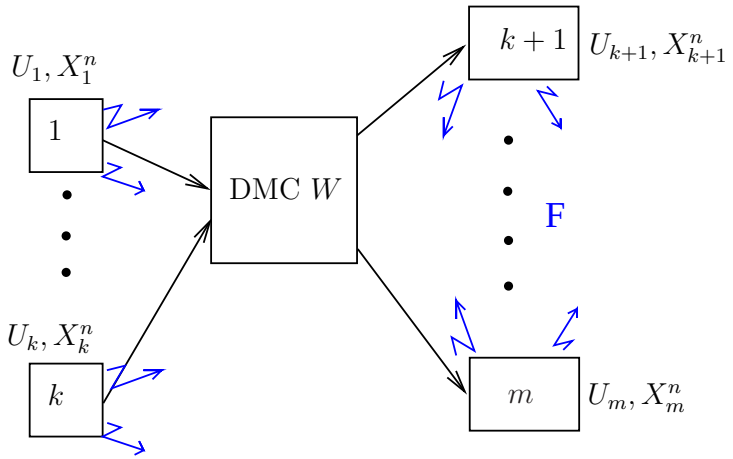
Proof: $\Leftarrow$ Sufficiency is clear by the previous Theorem.

$\Rightarrow$ Suppose that no $(R_1, \ldots, R_{m-1})$ as above exists.

- Then, by the convexity of $\mathcal{C}$, for some $i_1 \in \{1, \ldots, m-1\}$, we must have that $R_{i_1} = 0$ for every $(R_1, \ldots, R_{m-1}) \in \mathcal{C}$.
- $\Rightarrow W(x_m | x_1, \ldots, x_{m-1})$ does not depend on i_1.
- $\Rightarrow$ SK capacity is 0 even if the terminals in $\mathcal{M} \backslash \{i_1\}$ were allowed to operate as a consolidated team. $\square$

Remark: Theorem 2 does not extend to DMCs with ≥ 2 outputs even if there is only one input.

General Lower Bound for SK Capacity: Source Emulation



- *Simple source emulation:* One way to generate an SK is to emulate a "source model" obtained by the input terminals $1, \ldots, k$ transmitting over the DMC W, n i.i.d. repetitions of the rvs $X_1, \ldots, X_k$, with $P_{X_{[1,k]}} = \prod_{i=1}^{k} P_{X_i}$.

- *General source emulation:* Let V be an auxiliary rv with values in a finite set $\mathcal{V}$, and such that

$$V \multimap X_{[1,k]} \multimap X_{[k+1,m]}, \quad P_{X_{[1,k]}|V} = \prod_{i=1}^{k} P_{X_i|V}.$$

  One of the input terminals generates and reveals n i.i.d. repetitions of the rv V, and the input terminals $1, \ldots, k$ transmit over the DMC W, n independent versions of conditionally independent rvs as above.

- The SK capacity for a source model, even with additional secrecy from the revealed V-sequence, is known [C-N 2004].

General Lower Bound for SK Capacity: General Source Emulation

Theorem 3:

$$\begin{aligned} C_S &\geq \max_{P_{V,X_{[1,k]}} \text{as above}} \Big[\text{SK capacity of general source emulation model}\Big] \\ &= \max_{P_{V,X_{[1,k]}} \text{as above}} \Big[\min_{\lambda\in\Lambda}\Big(H(X_{\mathcal{M}}|V) \; - \; \sum_{B\in\mathcal{B}} \lambda_B H(X_B|X_{B^c},V)\Big)\Big]. \end{aligned}$$

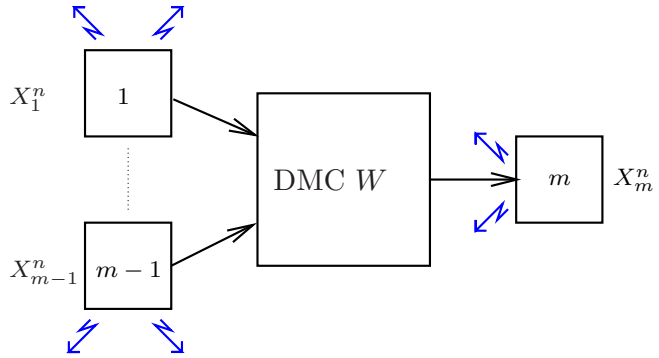
The right side above is achievable by a simple "noninteractive communication" protocol, i.e., with the input terminals not sending any public messages, and with each output terminal sending at most one public message based only on its observed (output) sequence.

Remarks: (i) General source emulation can yield larger SK rates than simple source emulation.

(ii) For a channel model with a *single input*, simple source emulation suffices to achieve SK capacity.

OP: Does general source emulation attain SK capacity?

Single Output Channel: Source Emulation and MAC Capacity Region



Consider a MAC with a single output whose capacity region is $\mathcal{C}$.

- Have seen that $(R, \ldots, R) \in \mathcal{C}$ is sufficient for R to be an achievable SK rate; it is unclear if this condition is necessary.
- However, larger SK rates cannot be achieved by general source emulation ...

Theorem 4: For a MAC $W : \mathcal{X}_1 \times \cdots \times \mathcal{X}_{m-1} \to \mathcal{X}_m$, a necessary and sufficient condition for R to be an achievable SK rate by general source emulation is that $(R, \ldots, R) \in \mathcal{C}$.

General Upper Bound for SK Capacity: Two Technical Lemmas

Let $X_{\mathcal{M}} = (X_1, \ldots, X_m)$. For every family $\mathcal{B} = \{B : B \subset \mathcal{M}, B \neq \emptyset\}$, and numbers $\lambda_B \geq 0$, $B \in \mathcal{B}$, that satisfy $\sum_{B \in \mathcal{B}: B \ni i} \lambda_B = 1$ for each $i \in \mathcal{M}$, the following hold.

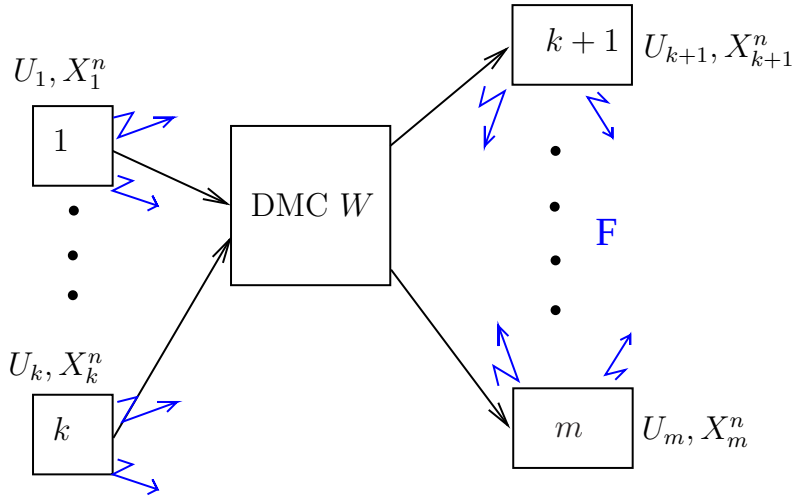
Lemma 5: (*Converse*) Let K, Y be rvs such that K is ϵ-recoverable from (X_i, Y) for each $i \in \mathcal{M}$. Then,

$$H(K|Y) \;\leq\; H(X_{\mathcal{M}}|Y) - \sum_{B \in \mathcal{B}} \lambda_B H(X_B|X_{B^c}, Y) + (m+1)(\epsilon \log |\mathcal{K}| + h(\epsilon)).$$

Lemma 6: (*Interactive communication*) For interactive communication F of the terminals $i \in \mathcal{M}$, with terminal $i \in \mathcal{M}$ possessing "initial" knowledge X_i,

$$H\left(F\right) \geq \sum_{B \in \mathcal{B}} \lambda_B H\left(F|X_{B^c}\right).$$

General Upper Bound for SK Capacity



Theorem 7:

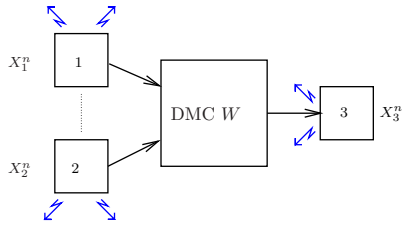
$$C_S \leq \max_{P_{V,X_{[1,k]}}} \min_{\lambda\in\Lambda} \left[\begin{array}{c} \left\{ H(X_{\mathcal{M}}|V) - \sum_{B\in\mathcal{B}} \lambda_B H(X_B|X_{B^c},V) \right\} \\ - \left\{ H(X_{[1,k}|V) - \sum_{B\in\mathcal{B}} \lambda_B H(X_{[1,k]\cap B}|X_{[1,k]\cap B^c},V) \right\} \end{array} \right],$$

where V –○– $X_{[1,k]}$ –○– $X_{[k+1,m]}$, but $P_{X_{[1,k]}|V}$ *need not be* $\prod_{i=1}^k P_{X_i|V}$.

Remark: For a channel model with a *single input*, the upper bound on SK capacity is tight (coinciding with the lower bound in Theorem 3).

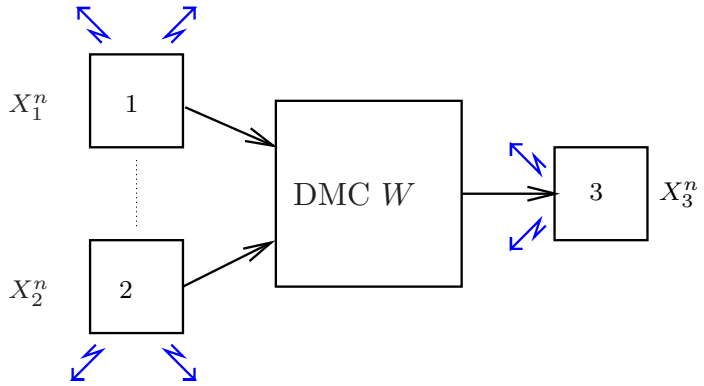
OP: What is the single letter formula for SK capacity?

Example: Binary Adder Channel with $\mathcal{M} = \{1, 2, 3\}$



- Consider the DMC $W : \{0,1\} \times \{0,1\} \to \{0,1\}$ given by $x_3 = x_1 \oplus x_2$.
- *Achievability:*
  - For the MAC W, the rate pair $(0.5, 0.5)$ lies on the boundary of the capacity region $\mathcal{C} = \{(R_1, R_2) : 0 \le R_1 + R_2 \le 1\}$ so that by Theorem 1, $C_S \ge 0.5$, and entails public communication only by the output terminal.
  - By simple source emulation in Theorem 3, $C_S \ge 0.5$.
  - *Alternative scheme for SK generation with* $n = 2$: As DMC inputs, terminal 1 transmits $X_{11} = 0$ or 1 w.p. $(0.5, 0.5)$ and $X_{12} = 0$, while terminal 2 independently transmits $X_{21} = 0$ and $X_{22} = 0$ or 1 w.p. $(0.5, 0.5)$. The output terminal 3 then communicates publicly $X_{31} \oplus X_{32}$. All the terminals recover X_{11}, which is independent of the public communication $\mathbf{F} = X_{31} \oplus X_{32}$, and is uniform on $\{0,1\}$. Hence, X_{11} is a *perfect* SK of rate $\frac{1}{2} H(X_{11}) = 0.5$.
- *Converse:* The upper bound in Theorem 7 yields $C_S \le 0.5$.

Example: Binary "Noisy" Adder Channel with $\mathcal{M} = \{1, 2, 3\}$



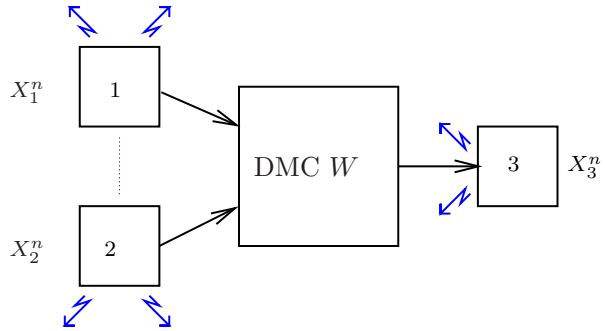
- Consider the DMC $W : \{0,1\} \times \{0,1\} \to \{0,1\}$ given by

$$W(0|x_1, x_2) = W(1|x_1, x_2) = 0.5, \quad \text{if} \quad x_1 = x_2 = 1,$$

$$W(x_3|x_1, x_2) = \mathbf{1}\left(x_3 = x_1 \oplus x_2\right) \quad \text{otherwise.}$$

- *Achievability:*
  - The capacity region of the MAC W is $\mathcal{C} = \{(R_1, R_2) : 0 \leq R_1 + R_2 \leq 1\}$ so that by Theorem 1, $C_S \geq 0.5$, and entails public communication only by the output terminal.
  - By Theorem 4, an SK rate of 0.5 is achievable also by general source emulation. However, it is *not* achievable by simple source emulation.
- *Converse:* The upper bound in Theorem 7 yields $C_S \leq 0.5$.

Example: Arithmetic Adder Channel with $\mathcal{M} = \{1, 2, 3\}$



- Consider the DMC $W : \{0, 1\} \times \{0, 1\} \to \{0, 1, 2\}$ given by $x_3 = x_1 + x_2$.
- *Achievability:*
  - For the MAC W, the rate pair $(0.75, 0.75)$ lies on the boundary of the capacity region $\mathcal{C} = \{(R_1, R_2) : \quad R_1 \leq 1, R_2 \leq 1, R_1 + R_2 \leq 1.5\}$. So, by Theorem 1, 0.75 is an achievable SK rate for the terminals $1, 2, 3$, and requires public communication *only* by the DMC output terminal.
  - Alternatively, by *simple* source emulation in Theorem 3, we get $C_S \geq 0.75$.
- *Converse:* The upper bound in Theorem 7 yields $C_S \leq 0.5 \log 3 = 0.78$.

OP: What is the SK capacity for this simple channel model?!