General adversarial channels

When do large codes exist?

Sidharth "Sid" Jaggi

The Chinese University of Hong Kong

joint work with

Xishi Wang

Amitalok J. Budkuley

Andrej Bogdanov

A new "fact" about random variables...

- Given a joint p.m.f. $P_{X,X'}$ over alphabet $\mathcal{X} \times \mathcal{X}$, when is it possible to create a "long" sequence $\{X_1, X_2, \ldots, X_m\}$ such that each (ordered) pair (X_i, X_j) is (ϵ-approximately) distributed as $P_{X,X'}$?

A new “fact” about random variables...

- Given a joint p.m.f. $P_{X,X'}$ over alphabet $\mathcal{X} \times \mathcal{X}$, when is it possible to create a “long” sequence $\{X_1, X_2, \ldots, X_m\}$ such that each (ordered) pair (X_i, X_j) is (ϵ-approximately) distributed as $P_{X,X'}$?
- If $P_{X,X'}(x, x') = \sum_u P_U(u) P_{X|u}(x) P_{X|u}(x')$, can construct arbitrarily long sequences.

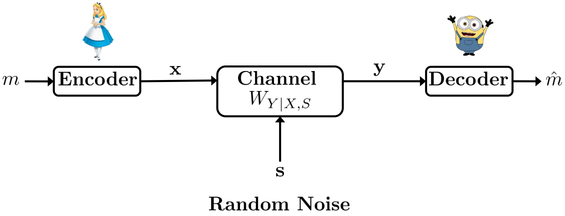
A new "fact" about random variables...

- Given a joint p.m.f. $P_{X,X'}$ over alphabet $\mathcal{X} \times \mathcal{X}$, when is it possible to create a "long" sequence $\{X_1, X_2, \ldots, X_m\}$ such that each (ordered) pair (X_i, X_j) is (ϵ-approximately) distributed as $P_{X,X'}$?
- If $P_{X,X'}(x,x') = \sum_u P_U(u) P_{X|u}(x) P_{X|u}(x')$, can construct arbitrarily long sequences.
- Set of such $P_{X,X'}$ called *completely positive distributions*, have been studied in convex optimization. Forms a convex set.

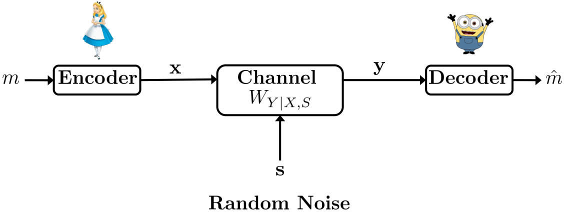
A new "fact" about random variables...

- Given a joint p.m.f. $P_{X,X'}$ over alphabet $\mathcal{X} \times \mathcal{X}$, when is it possible to create a "long" sequence $\{X_1, X_2, \ldots, X_m\}$ such that each (ordered) pair (X_i, X_j) is (ϵ-approximately) distributed as $P_{X,X'}$?
- If $P_{X,X'}(x, x') = \sum_u P_U(u) P_{X|u}(x) P_{X|u}(x')$, can construct arbitrarily long sequences.
- Set of such $P_{X,X'}$ called *completely positive distributions*, have been studied in convex optimization. Forms a convex set.
- If $P_{X,X'}$ is at least ϵ-far from being completely positive, then can only exist sequences of length $\mathcal{O}\left(\exp\left(\frac{1}{\epsilon}\right)\right)$.

A *standard* communication scenario...

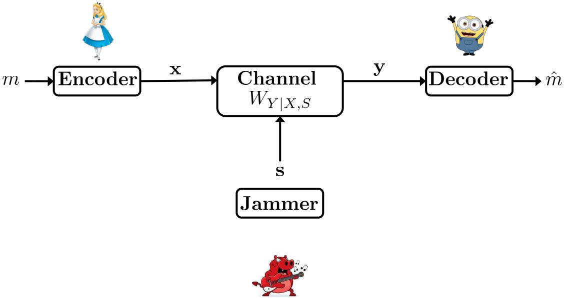


A *standard* communication scenario...

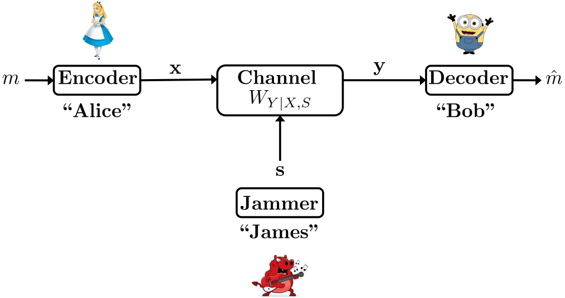


Aim: To communicate a 'large' message 'reliably' to the receiver over the *random* noise channel.

An *adversarial* communication scenario...

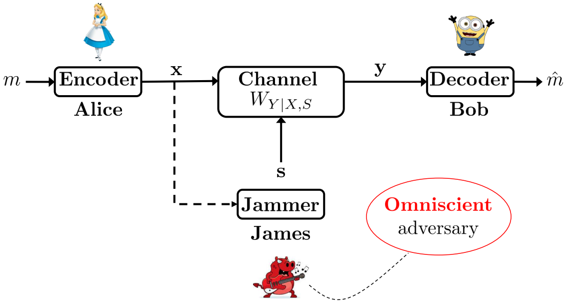


An *adversarial* communication scenario...



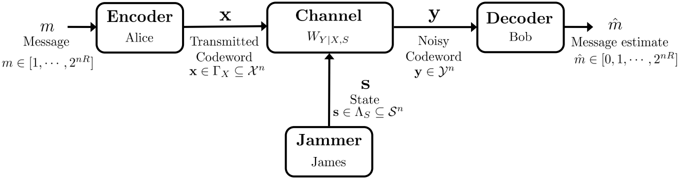
Aim: To communicate a 'large' message 'reliably' to the receiver over the *adversarial* noise channel .

An *adversarial* communication scenario...

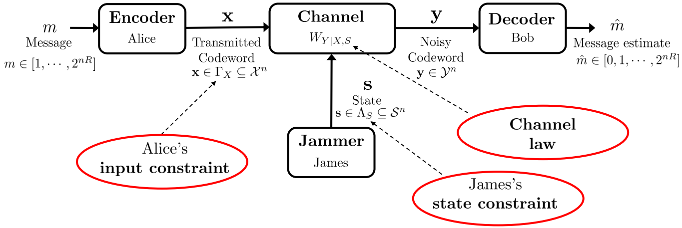


Aim: To communicate a 'large' message 'reliably' to the receiver over the *adversarial* noise channel .

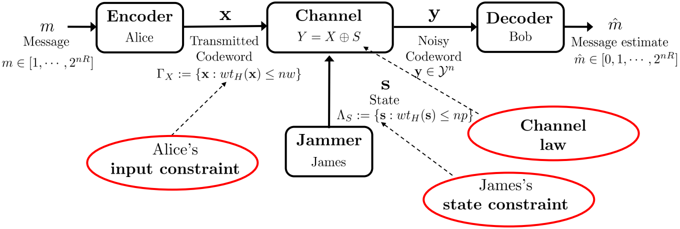
The *adversarial communication* problem setup



The *adversarial communication* problem setup

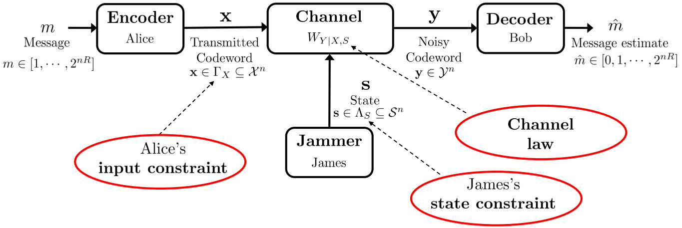


Example: The *Binary* communication setup

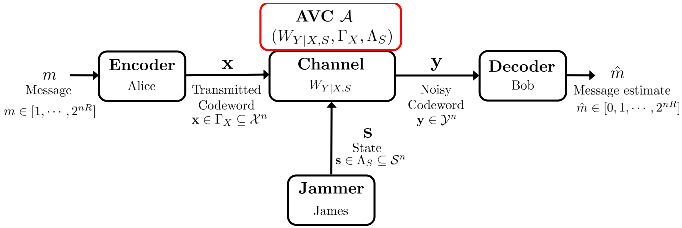


- Channel $W_{Y|X,S}$ is *state-deterministic* with output $Y = X \oplus S$.
- Alice's input constraint $\Gamma_X = \{\mathbf{x} : wt_H(\mathbf{x}) \leq nw\}$, $0 \leq w \leq 1/2$.
- James' state constraint $\Lambda_S = \{\mathbf{s} : wt_H(\mathbf{s}) \leq np\}$, $0 \leq p \leq 1/2$.
- Denoted A-BSC(p)

The *Adversarial Communication* problem setup



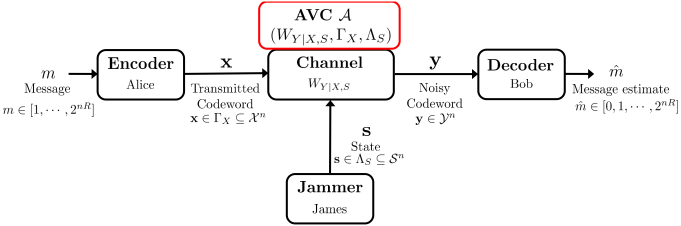
The *Adversarial Communication* problem setup



In this talk, only *symbolwise, state-deterministic* channels $W_{Y|X,S}$.

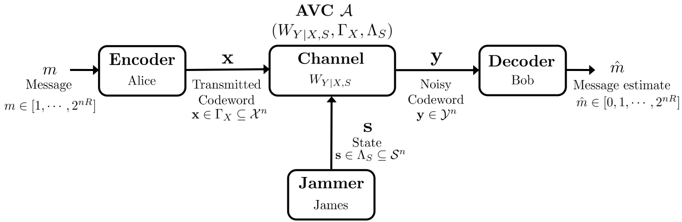
- **Symbolwise** channel: y_i depends only on x_i, s_i.
  - Example: A-BSC(p) channel shown before, with $y_i = x_i \oplus s_i$.
  - Non-example: Deletion channels
- **State-deterministic** channel: y_i is a deterministic function of x_i and s_i.
  - Example: A-BSC(p) channel shown before, with $y_i = x_i \oplus s_i$.
  - Non-example: $W_{Y|X,S}(y|x,s) = \begin{cases} x \oplus s & \text{with probability 1-q} \\ x \oplus s \oplus 1 & \text{with probability q} \end{cases}$

The *Adversarial Communication* problem setup



- Three key parameters: the *channel*, Alice's *input constraints* and James' *state constraints*.
  - *Arbitrarily Varying Channel (AVC)* is specified by $\mathcal{A} = (W_{Y|X,S}, \Gamma_X, \Lambda_S)$.
- User/Adversary strategies:
  - Alice & Bob pick a feasible (acc. to Γ_X) codebook $\mathcal{C}$.
  - James picks a feasible (acc. to Λ_S) jamming sequence $\mathbf{s}$ (as a function of $\mathcal{C}$ and $\mathbf{x}$).
  - *Private* randomization turns out not to benefit any of Alice/Bob/James.

The *Adversarial Communication* problem setup



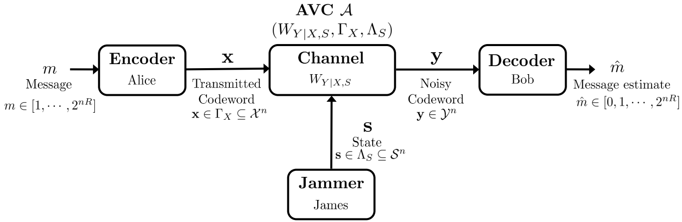
- AVC $\mathcal{A}$ *reliability* criterion: Zero error (requiring vanishing-error turns out not to change the problem for state-deterministic AVCs)

$$\forall m,\ \forall \mathbf{s},\ \ \hat{m} = m$$

- Principal metric of interest: optimum throughput or *capacity*

$$C := \sup\{R : \text{`coding rate'} R \text{ is `achievable'}\}.$$

The *Adversarial Communication* problem setup



- AVC $\mathcal{A}$ *reliability* criterion: Zero error (requiring vanishing-error turns out not to change the problem for state-deterministic AVCs)

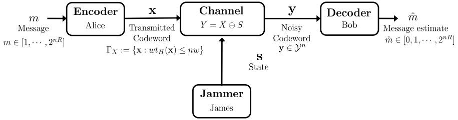
$$\forall m, \ \forall \mathbf{s}, \ \hat{m} = m$$

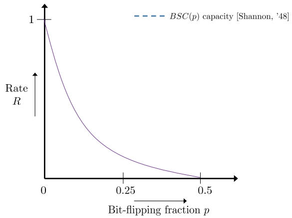
- Principal metric of interest: optimum throughput or *capacity*

$$C := \sup\{R : \text{'coding rate'} R \text{ is 'achievable'}\}.$$

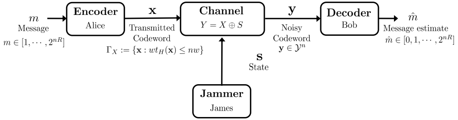
- In this talk, just want to understand precisely when $R > 0$ is possible.

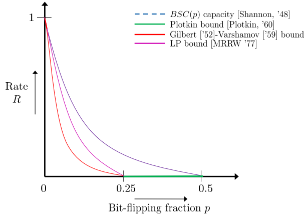
Example: Capacity for the *Binary* communication setup



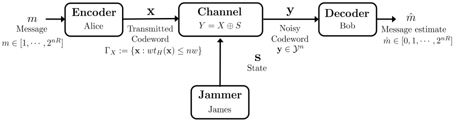


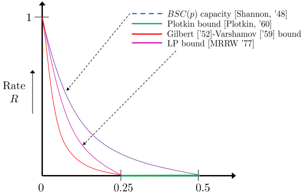
Example: Capacity for the *Binary* communication setup





Example: Capacity for the *Binary* communication setup

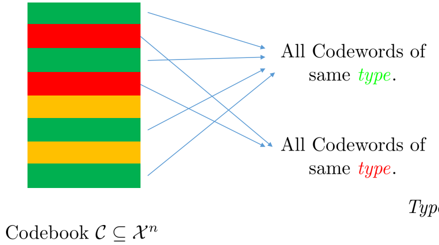




Key Fact

Capacity for A-BSC(p) is 'strictly' smaller than for standard BSC(p)!!

Observation: *Constant Composition* codes suffice



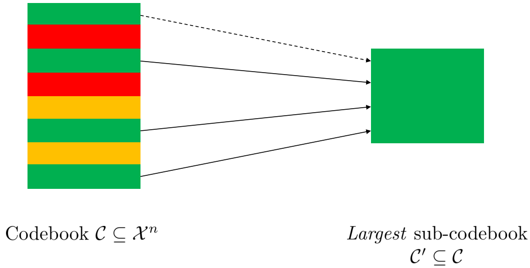
Type:= Empirical distribution of a vector

Ex.: $\underline{x} = (12213133)$

Type $T_{\underline{x}} = (\frac{3}{8}, \frac{2}{8}, \frac{3}{8})$

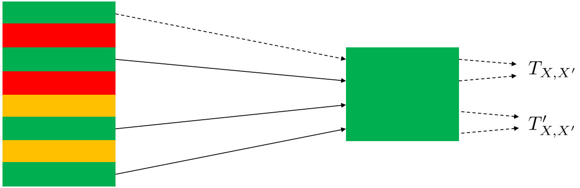
- Constant composition (CC) code: All codewords of the same type.
- Fact: Number of types polynomial in n (at most $(n+1)^{|\mathcal{X}|}$).
- Sub-codebook of largest size $\mathcal{C}' \subseteq \mathcal{C}$: *essentially* of same rate.
  - Vanishing (in n) rate loss in $\mathcal{C}'$ vis-à-vis $\mathcal{C}$.
  - Codebook $\mathcal{C}$ robust to errors $\Rightarrow$ sub-codebook $\mathcal{C}'$ *also* robust to errors.
- So we henceforth analyze only constant composition codes.

Observation: *Constant Composition* codes suffice



- Constant composition (CC) code: All codewords of the same type.
- Fact: Number of types polynomial in n (at most $(n+1)^{|\mathcal{X}|}$).
- Sub-codebook of largest size $\mathcal{C}' \subseteq \mathcal{C}$: *essentially* of same rate.
  - Vanishing (in n) rate loss in $\mathcal{C}'$ vis-à-vis $\mathcal{C}$.
  - Codebook $\mathcal{C}$ robust to errors $\Rightarrow$ sub-codebook $\mathcal{C}'$ *also* robust to errors.
- So we henceforth analyze only constant composition codes.

Joint types or *Couplings*



Codebook $\mathcal{C} \subseteq \mathcal{X}^n$

Largest sub-codebook
$\mathcal{C}' \subseteq \mathcal{C}$

- Important: Properties of joint pair types of codewords in $\mathcal{C}' \subseteq \mathcal{C}$.

Definition (Couplings/Self-couplings)

- The joint type of a pair of vectors or a pair-type is called a coupling.
- A coupling $T_{X,X'}$ with $T_X = T_{X'}$ is called a self-coupling.

Example: Coupling

$$|\mathcal{X}| = 3$$

$\mathbf{x}$: 0 1 1 0 0 2 2 1 0 0 2 0 1 1 0 1 2 0 1 0 2 1 1 0 2

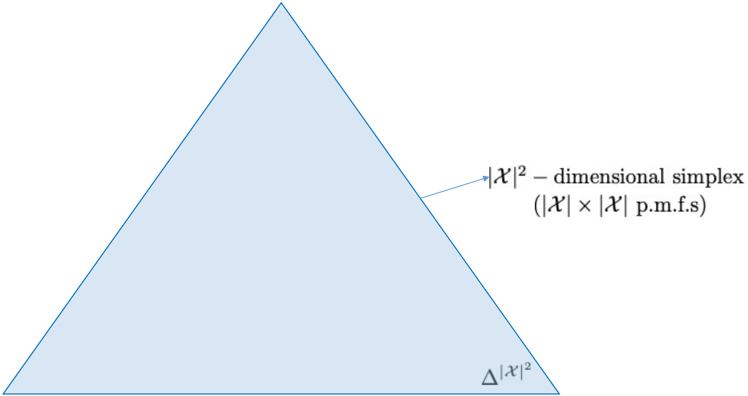
$\mathbf{x}'$: 0 1 0 0 2 2 0 1 2 2 1 0 0 1 0 2 0 1 0 2 1 0 1 1 1

=3

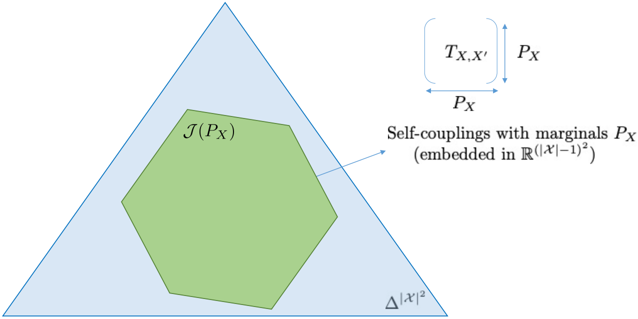
$$T_X = T_{X'} = \left(\frac{10}{25}, \frac{9}{25}, \frac{6}{25}\right), \qquad T_{X,X'} = \frac{1}{25}\begin{bmatrix} 4 & 2 & 4 \\ 4 & 4 & 1 \\ 2 & 3 & 1 \end{bmatrix}$$

- $C_{Hamming} \triangleq \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \Rightarrow d_H(\mathbf{x}, \mathbf{x}') = n \langle C_{Hamming}, T_{X,X'} \rangle$
- $C_{\ell_1} \triangleq \begin{bmatrix} 0 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix} \Rightarrow d_1(\mathbf{x}, \mathbf{x}') \triangleq \sum_{i=1}^{n} |x_i - x'_i| = n \langle C_1, T_{X,X'} \rangle$

Geometry of Sets



Geometry of Sets



$$\text{Row constraints: } \forall i \in [|\mathcal{X}|],\ \sum_{j=1}^{|\mathcal{X}|} (T_{X,X'})_{i,j} = P_X(i),$$

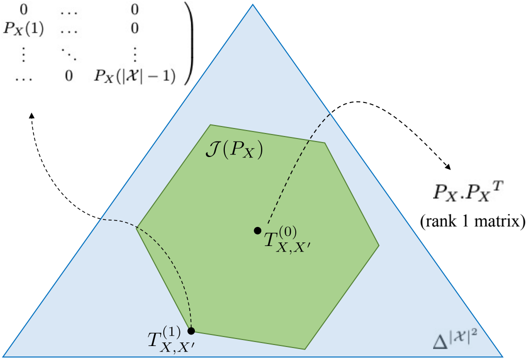
$$\text{Column constraints: } \forall j \in [|\mathcal{X}|],\ \sum_{i=1}^{|\mathcal{X}|} (T_{X,X'})_{i,j} = P_X(j),$$

$2|\mathcal{X}| - 1$ linearly independent constraints.

$\mathcal{J}(P_X)$ is a polytope.

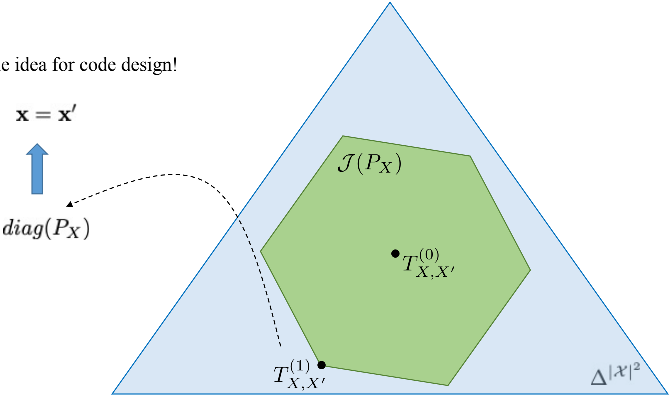
Geometry of Sets

$$diag(\mathbf{P}_X) \triangleq \begin{pmatrix} P_X(0) & 0 & \dots & 0 \\ 0 & P_X(1) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & P_X(|\mathcal{X}|-1) \end{pmatrix}$$

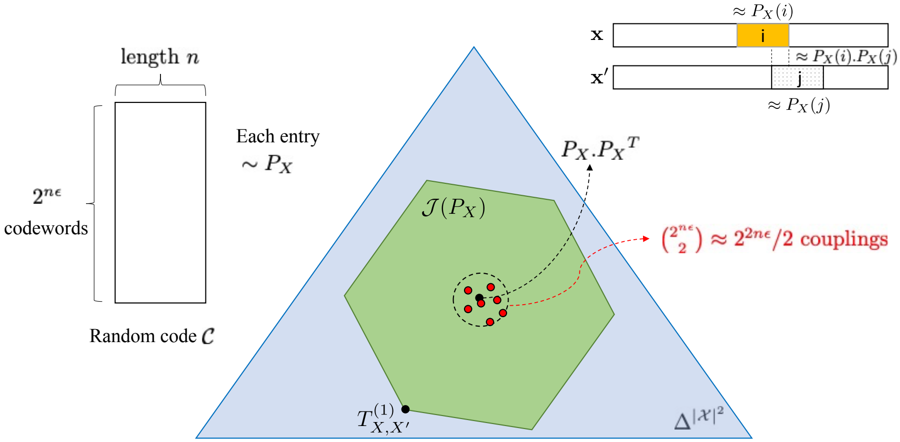


Geometry of Sets

Terrible idea for code design!

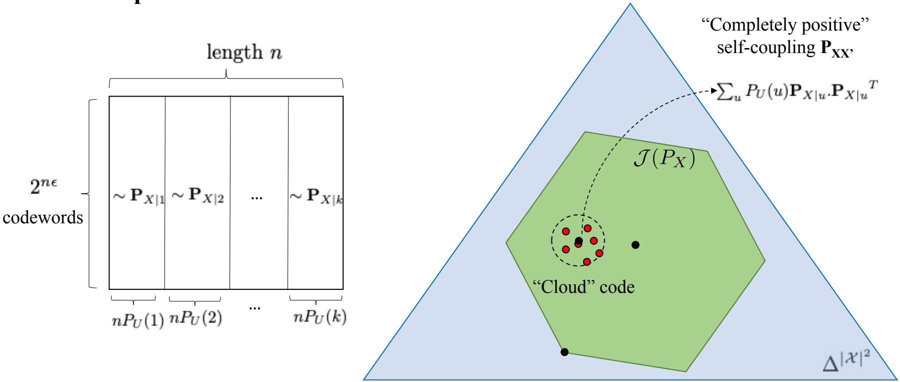


Geometry of Sets



Geometry of Sets

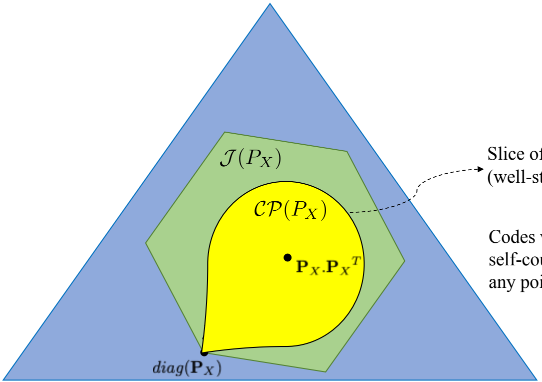
What else is possible?



Example:

$$\mathbf{P}_{XX'} = \begin{pmatrix} 1/8 & 1/8 & 0 \\ 1/8 & 1/4 & 1/8 \\ 0 & 1/8 & 1/8 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1/2 \\ 1/2 \\ 0 \end{pmatrix}\begin{pmatrix} 1/2 & 1/2 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 \\ 1/2 \\ 1/2 \end{pmatrix}\begin{pmatrix} 0 & 1/2 & 1/2 \end{pmatrix}$$

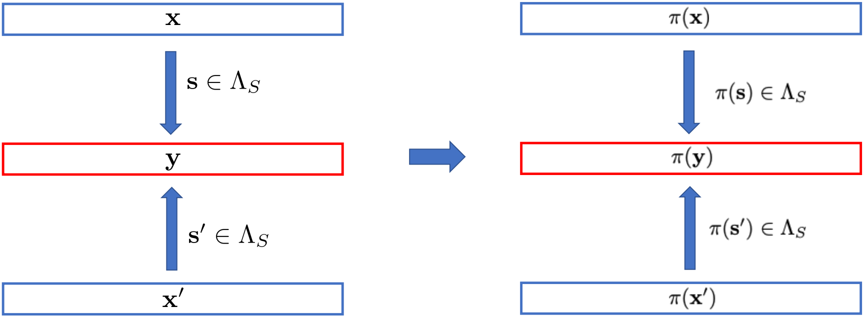
Geometry of Sets



Slice of the "Completely positive cone"
(well-studied object in convex analysis)

Codes with positive rate, and self-couplings concentrated around any point in *CP(P_X)* possible.

What about the adversary?

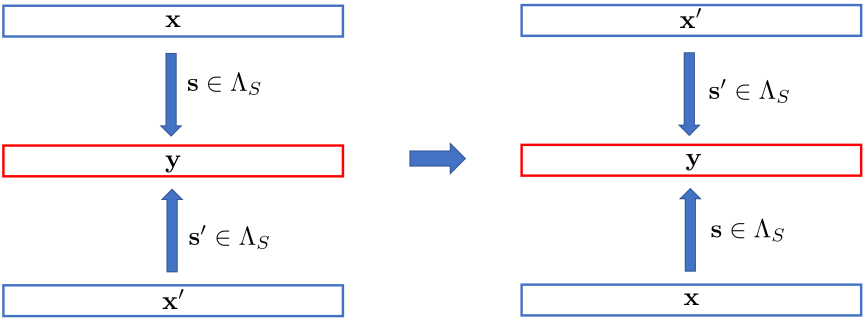


Observation 1:

- If $(\mathbf{x}, \mathbf{x}')$ "confusable" by $\mathcal{A}$, for any permutation π, $(\pi(\mathbf{x}), \pi(\mathbf{x}'))$ *also* confusable by $\mathcal{A}$. Hence $(\mathbf{x}, \mathbf{x}')$ confusable $\Leftrightarrow T(\mathbf{x}, \mathbf{x}')$ confusable

- Not necessarily true if channel not symbolwise, for instance for deletion channels.

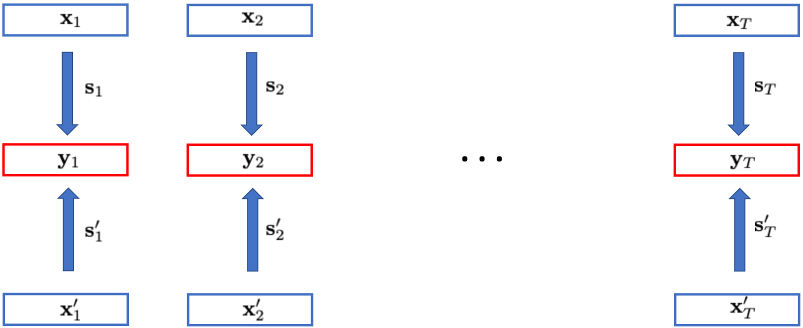
What about the adversary?



Observation 2:

- If $T(\mathbf{x}, \mathbf{x}')$ "confusable" by $\mathcal{A}, T(\mathbf{x}, \mathbf{x}')$ *also* confusable by $\mathcal{A}$.

What about the adversary?



Observation 3 (Convexity):

- By time-sharing, the set (denoted $\mathcal{K}(\mathcal{A})$) of confusable self-couplings is *convex*

What about the adversary?

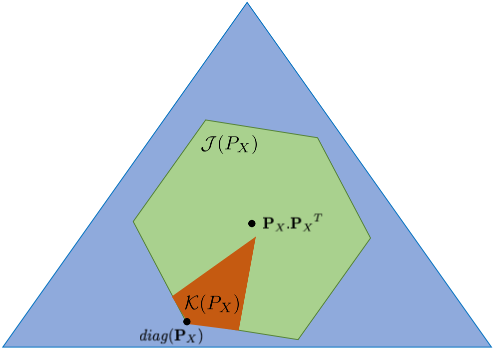
Observation 4: (Constraints from $\mathcal{A}$)

$T_{XX'}$ confusable $\Rightarrow \exists\ T_{XX'SS'Y}$ such that

- *(Consistency with $T_{XX'}$)*:
  $\forall (x,x') \in \mathcal{X} \times \mathcal{X},\ \sum_{s,s',y} T_{XX'SS'Y}(x,x',s,s',y) = T_{XX'}(x,x')$.
- *(Consistency with input constraints Λ_S)*:
  $T_S \triangleq \sum_{x,x',s',y} T_{XX'SS'Y}(x,x',s,s',y)$ satisfies $T_S \in \Lambda_S$,
  $T_{S'} \triangleq \sum_{x,x',s,y} T_{XX'SS'Y}(x,x',s,s',y)$ satisfies $T_{S'} \in \Lambda_S$.
- *(Consistency with channel $W_{Y|X,S}$)*:
  $T_{XSY} \triangleq \sum_{x',s'} T_{XX'SS'Y}(x,x',s,s',y)$ compatible with $W_{Y|X,S}$,
  $T_{X'S'Y} \triangleq \sum_{x,s} T_{XX'SS'Y}(x,x',s,s',y)$ compatible with $W_{Y|X,S}$.

- All constraints linear, hence checking to see if a given $T_{XX'}$ is in the confusability set $\mathcal{K}$ is a computationally efficient convex optimization problem (given membership oracle for Λ_S).
- If Λ_S is a polytope (common in many classical models – e.g. noise weight $\leq pn$) then $\mathcal{K}$ also a polytope.

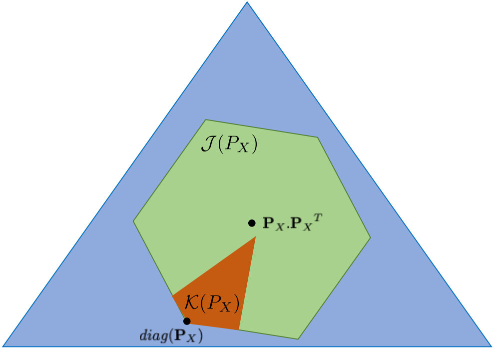
Achievability



Confusability set properties:

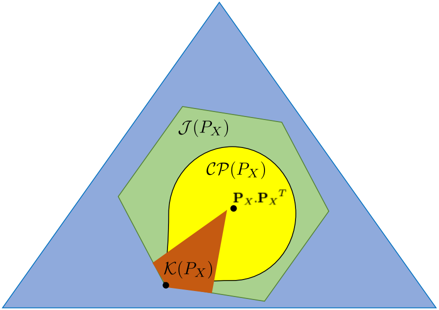
- Characterized by subset $\mathcal{K}(\mathcal{A})$ of self-couplings $\mathcal{J}(P_X)$.
- Convex.
- Transpositionally symmetric.
- Efficiently computable.
- $diag(P_X)$ always in $\mathcal{K}(\mathcal{A})$
- Polytope, if Λ_S a polytope.

Achievability



- Can construct AVCs $\mathcal{A}$ and $\bar{\mathcal{A}}$ that are distinct (for instance, with different output alphabets $\mathcal{Y}$), but with the same confusability polytope $\mathcal{K}$.
- Hence good codes for $\mathcal{A}$ also good for $\bar{\mathcal{A}} \Rightarrow$ capacity regions the same.
- Confusability polytopes fundamentally characterize capacities of state-deterministic AVCs!
- **Not** true for non-state-deterministic AVCs. Can construct non-SD AVCs with the same confusability polytope, but provably different capacities.

Achievability

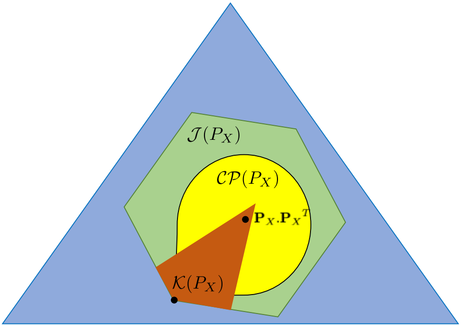


- So if the completely positive slice $\mathcal{CP}(P_X)$ contains self-couplings outside the confusability set $\mathcal{K}(\mathcal{A})$, a positive rate is possible.
- For instance, if $\mathbf{P}_X.\mathbf{P}_X{}^T \notin \mathcal{K}(\mathcal{A})$, then a positive rate is possible.
  - Indeed, in this case, a more careful analysis shows a "Gilbert-Varshamov (GV) type" (greedy packing) achievable rate (matching GV bound in known cases):

$$\max_{P_X \in \Gamma_X} \min_{P_{XX'} \in \mathcal{K}(\mathcal{A})} I(X; X')$$

  - Same rate also achievable via random coding + expurgation. Rate governed by large-deviations exponent.

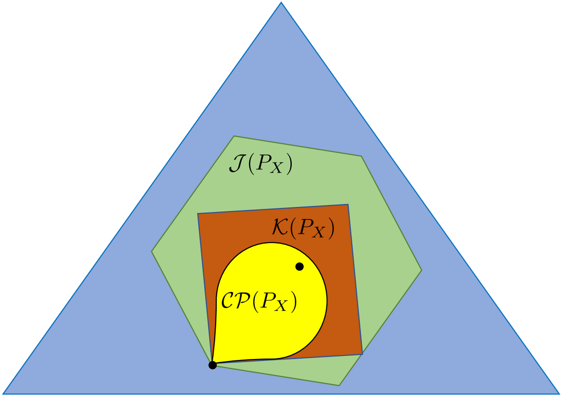
Achievability



- If $\mathbf{P}_X.\mathbf{P}_X{}^T \in \mathcal{K}(\mathcal{A})$, GV-type rate $= 0$.
- However, if $\exists$ completely positive distribution $P_{XX'} = \sum_u P_U(u)\mathbf{P}_{X|u}.\mathbf{P}_{X|u}{}^T$ s.t. $P_{XX'} \notin \mathcal{K}(\mathcal{A})$, positive rate still possible via cloud codes.
- Can construct examples of such AVCs $\Rightarrow$ GV codes $\subsetneq$ cloud codes.
  - GV-type rate for cloud codes:

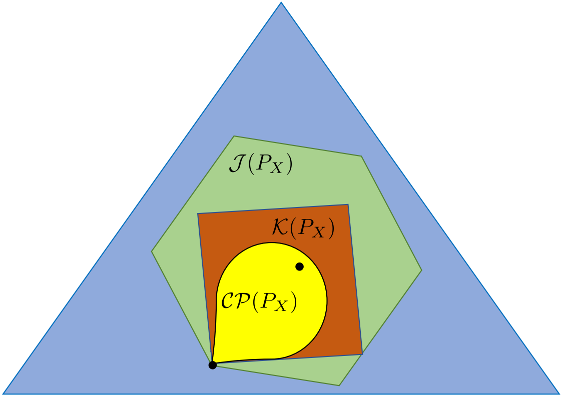
$$\max_{\substack{P_X \in \Gamma_X, \\ P_{XX'} \in \mathcal{CP}(P_X)}} \min_{P_{XX'} \in \mathcal{K}_U(\mathcal{A})} I(X; X'|U)$$

Achievability



- If all completely positive couplings always within the confusability polytope, i.e., for $P_X \in \Gamma_X$, $\mathcal{CP}(P_X) \subseteq \mathcal{K}(\mathcal{A})$, then prior arguments do not give positive rate.

Achievability



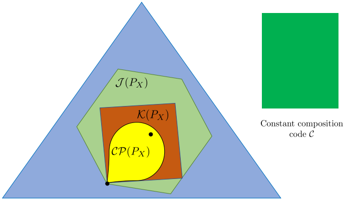
- If all completely positive couplings always within the confusability polytope, i.e., for $P_X \in \Gamma_X$, $\mathcal{CP}(P_X) \subseteq \mathcal{K}(\mathcal{A})$, then prior arguments do not give positive rate.
- Indeed, other half of main result shows no positive rate possible in this scenario.

Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}'$, $T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\mathcal{C}'|))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$

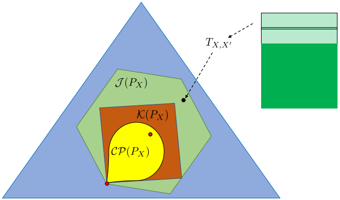
Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}', \; T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\mathcal{C}'|))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



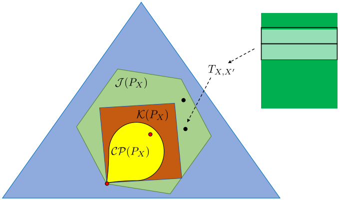
Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}',\ T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\mathcal{C}'|))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



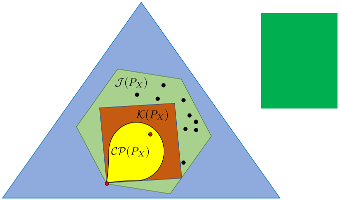
Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}'$, $T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\ \mathcal{C}'\ |))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



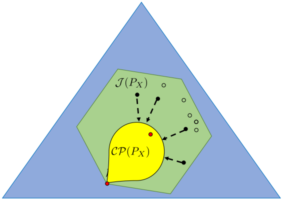
Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}',\ T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\mathcal{C}'|))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



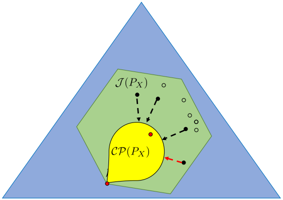
Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}',\ T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\mathcal{C}'|))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



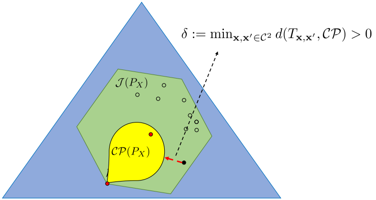
Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}', \ T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\mathcal{C}'|))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



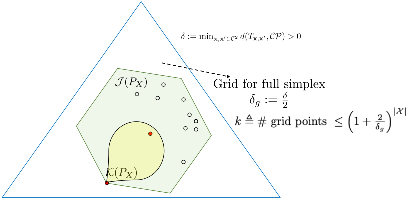
Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}'$, $T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\mathcal{C}'|))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



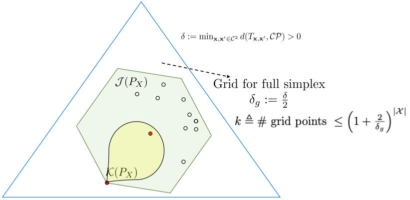
Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}'$, $T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
  - $\mathcal{C}'$ self-couplings $\{T_{\mathbf{x},\mathbf{x}'}\}$ have a 'δ-gap' from $\mathcal{CP}$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\mathcal{C}'|))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



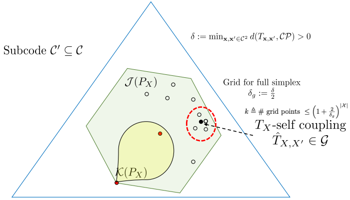
Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}'$, $T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
  - $\mathcal{C}'$ self-couplings $\{T_{\mathbf{x},\mathbf{x}'}\}$ have a 'δ-gap' from $\mathcal{CP}$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\mathcal{C}'|))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



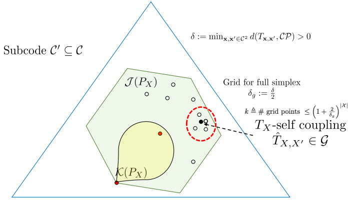
Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}'$, $T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
  - $\mathcal{C}'$ self-couplings $\{T_{\mathbf{x},\mathbf{x}'}\}$ have a 'δ-gap' from $\mathcal{CP}$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\ \mathcal{C}'\ |))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



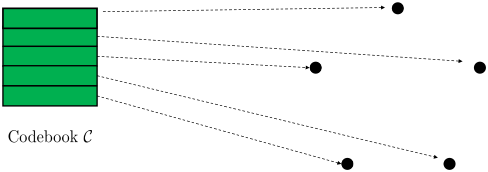
Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}',\ T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
  - $\mathcal{C}'$ self-couplings $\{T_{\mathbf{x},\mathbf{x}'}\}$ have a 'δ-gap' from $\mathcal{CP}$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\ \mathcal{C}'\ |))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



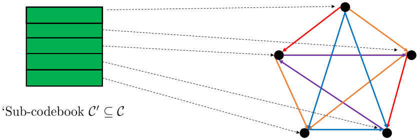
Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}'$, $T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
  - $\mathcal{C}'$ self-couplings $\{T_{\mathbf{x},\mathbf{x}'}\}$ have a 'δ-gap' from $\mathcal{CP}$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\mathcal{C}'|))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



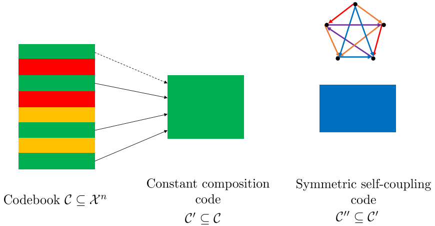
Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}',\ T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
  - $\mathcal{C}'$ self-couplings $\{T_{\mathbf{x},\mathbf{x}'}\}$ have a 'δ-gap' from $\mathcal{CP}$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\ \mathcal{C}'\ |))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



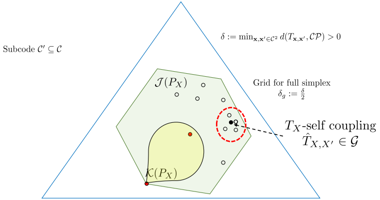
Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}'$, $T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
  - $\mathcal{C}'$ self-couplings $\{T_{\mathbf{x},\mathbf{x}'}\}$ have a 'δ-gap' from $\mathcal{CP}$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\mathcal{C}'|))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



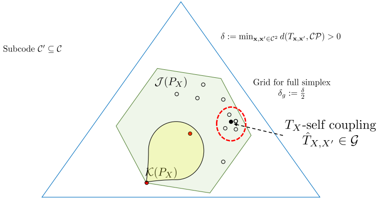
Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}',\ T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
  - $\mathcal{C}'$ self-couplings $\{T_{\mathbf{x},\mathbf{x}'}\}$ have a 'δ-gap' from $\mathcal{CP}$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\ \mathcal{C}'\ |))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



Converse

- Recall constant composition codes only $\Rightarrow \forall \mathbf{x} \in \mathcal{C}'$, $T_{\mathbf{x}} = T_X$.
- For converse, 'good' $\mathcal{C}' \Rightarrow \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}'$, the self coupling $T_{\mathbf{x},\mathbf{x}'} \notin \mathcal{K}(T_X)$.
  - $\mathcal{C}'$ self-couplings $\{T_{\mathbf{x},\mathbf{x}'}\}$ have a 'δ-gap' from $\mathcal{CP}$.
- Construct a δ_g-net $\mathcal{G} \subseteq \Delta$; $|\mathcal{G}|$ depends on $\mathcal{X}$ but *independent of n*
- There exists 'sufficiently large' $\mathcal{C}'' \subseteq \mathcal{C}'$; $\forall \mathbf{x}, \mathbf{x}' \in \mathcal{C}''$, $T_{\mathbf{x},\mathbf{x}'} \approx \hat{T}_{X,X'} \in \mathcal{G}$.
  - Proof uses Ramsey theory $\Rightarrow$ Given code $\mathcal{C}$ with k "covering couplings", $\exists$ subcode $\mathcal{C}'$ (monochromatic clique) of size $\Omega((\log(|\mathcal{C}'|))^{1/(k+1)})$.
- $\hat{T}_{X,X'}$ corresp. to $\mathcal{C}'$ may be symmetric or asymmetric
  - Need *separate* analysis for symmetric (generalized-Plotkin) and asymmetric (Fourier-analytic) $\hat{T}_{X,X'}$



Symmetric Self-Couplings
Classical Plotkin bound for binary codes/Hamming distance

- Code $\mathcal{C} \subseteq \{0,1\}^n$, $d_{min}(\mathcal{C}) \geq \frac{n(1+\epsilon)}{2}$, $\epsilon > 0$, $\quad \Rightarrow \quad |\mathcal{C}| \in \mathcal{O}\left(\frac{1}{\epsilon}\right)$.

"Geometric" proof:

- Map $\mathcal{C} \in \{0,1\}^n$ to $\bar{\mathcal{C}} \in \{-1,1\}^n$.
- $d_{min}(\mathcal{C}) \geq \frac{n(1+\epsilon)}{2} \;\Rightarrow\; \langle \bar{\mathbf{x}}, \bar{\mathbf{x}}' \rangle \leq -\epsilon n$.
  - Codewords $\bar{\mathbf{x}} \neq \bar{\mathbf{x}}'$ make obtuse angles w.r.t. each other over $\mathbb{R}^n$.

$$0 \underbrace{\leq}_{1} \left\langle \left(\sum_{\bar{\mathbf{x}}\in\bar{\mathcal{C}}} \bar{\mathbf{x}}\right), \left(\sum_{\bar{\mathbf{x}}\in\bar{\mathcal{C}}} \bar{\mathbf{x}}\right)^T \right\rangle = \underbrace{\left(\sum_{\bar{\mathbf{x}}\in\bar{\mathcal{C}}} \left\langle \bar{\mathbf{x}}, \bar{\mathbf{x}}^T \right\rangle\right)}_{\leq n|\bar{\mathcal{C}}| \;\; 2} + \underbrace{\left(\sum_{\substack{\bar{\mathbf{x}},\bar{\mathbf{x}}' \in \bar{\mathcal{C}} \\ \bar{\mathbf{x}} \neq \bar{\mathbf{x}}'}} \left\langle \bar{\mathbf{x}}, \bar{\mathbf{x}}^T \right\rangle\right)}_{\leq -\epsilon n \frac{|\bar{\mathcal{C}}|(|\bar{\mathcal{C}}-1|)}{2} \;\; 3}$$

Symmetric Self-Couplings

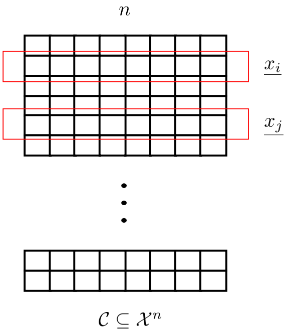
Generalized Plotkin bound

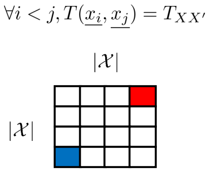
Useful "facts" [Hall '62]:

- Let CoP denote the set of *co-positive* matrices, i.e. symmetric matrices Q such that for any non-negative vector $\mathbf{x}$, $\mathbf{x}^T Q\mathbf{x} \geq 0$.
- The cone CoP of copositive matrices is dual to the cone CP of completely positive matrices.
- Ignoring the (controllable) δ_g quantization deviation due to the grid, suppose $\mathcal{C}''$ s.t. all self-couplings exactly $\hat{T} \notin CP \;\Rightarrow$ $\exists Q \in CoP$ s.t. $||Q||_F = 1$, $\left\langle Q, \hat{T} \right\rangle \leq -\epsilon$.

$$0 \underbrace{\leq}_{Q\in CoP, (1)} \sum_{\mathbf{x},\mathbf{x}'\in\mathcal{C}''} \langle Q, T(\mathbf{x},\mathbf{x}')\rangle = \underbrace{\sum_{\mathbf{x}\in\mathcal{C}''} \langle diag(P_X), Q\rangle}_{\substack{\leq n|\mathcal{C}''| \; (2) \\ (||Q||_F = 1, \\ diag(P_X) \in CP)}} + \underbrace{\sum_{\substack{\mathbf{x},\mathbf{x}' \in \mathcal{C}'' \\ \mathbf{x} \neq \mathbf{x}'}} \left\langle \hat{T}, Q \right\rangle}_{\leq -\epsilon n \frac{|\mathcal{C}''|(|\mathcal{C}''-1|)}{2} \; (3)}$$

Asymmetric Self-Couplings





- Constant composition codes with asymmetric joint types:
  - Constant composition codes $\mathcal{C}$: $T(\underline{x}_i) = T(\underline{x}_j), \forall i, j$
  - Asymmetric joint type: $\forall i < j$, $T(\underline{x}_i, \underline{x}_j) = T_{XY}$. T_{XY} is asymmetric.

Asymmetric Self-Couplings
Example

Let $\Sigma = \mathbb{Z}_3 = \{0,1,2\}$, $N = 3$, and $(X_1, X_2, X_3) = (U, U + A, U + B)$, where U is uniform and (A, B) are independent of U, jointly distributed as:

a	b	$\Pr[A = a, B = b]$
0	1	2/7
1	1	2/7
1	0	1/7
1	2	1/7
2	0	1/7

- The pairs (X_1, X_2), (X_1, X_3) and (X_2, X_3) are identically distributed as T
  - $T = \frac{1}{21}\begin{bmatrix} 2 & 4 & 1 \\ 1 & 2 & 4 \\ 4 & 1 & 2 \end{bmatrix}$
- Asymmetry:
  $\mathrm{asymm}(X, Y) \triangleq \max_{x,y\in\Sigma} \Pr[X = x, Y = y] - \Pr[X = y, Y = x] = 3/21.$

Asymmetric Self-Couplings

Can find code with asymmetric couplings via LP

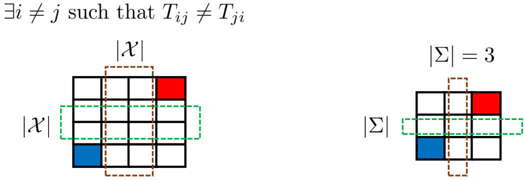
- Suppose we want to find the largest $asymm(X, Y)$ for $N \geq 3$ random variables $X_1, \cdots, X_N$ with each taking value from a size 3 alphabet $\mathcal{X}$.
- We can formulate the problem as a linear program.

$$\begin{array}{ll} \text{maximize} & P_{X_1X_2}(1,2) - P_{X_1X_2}(2,1) \\ \text{subject to} & P_{X_1} = P_{X_i}, \forall i \in [N] \\ & P_{X_1X_2} = P_{X_jX_k}, \forall j < k \\ \text{variables} & P_{X_1X_2\cdots X_N} \in \Delta(|\mathcal{X}|^N) \end{array}$$

- The number of variables is exponential in N.

Asymmetric Self-Couplings

$|\Sigma| = 3$ w.l.o.g.



- Given any asymmetric joint type over finite alphabet $\mathcal{X}$
  - Find $i \neq j$ such that $T_{ij} \neq T_{ji}$.
  - Combine all other symbols in $\mathcal{X} \backslash \{i, j\}$ into a single symbol
  - W.l.o.g. for tradeoff between code-size and asymmetry, assume $|\Sigma| = 3$.

Asymmetric Self-Couplings

When N is large, the asymmetry must go to zero. More precisely,

Theorem

Assume $\mathrm{asymm}(X, Y) > \epsilon$. *Let* $X_1, \ldots, X_N$ *is a sequence of random variables such that for every* $1 \le i < j \le N$, *the joint type of* (X_i, X_j) *is statistically* $\epsilon/2$*-close to* (X, Y). *Then* $N \le \exp K/(\mathrm{asymm}(X, Y) - \epsilon)$ *for some universal constant* K.

Asymmetric Self-Couplings

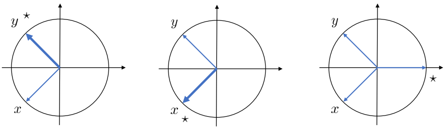
Lemma

There is an embedding $\rho\colon \Sigma \to \mathbb{C}_3^\times$ *such that*

$$\operatorname{Im} \mathbb{E}[\rho(X)\overline{\rho(Y)}] \geq \frac{\sqrt{3}}{2} \cdot \operatorname{asymm}(X, Y).$$

Asymmetric Self-Couplings

Proof:



ρ_1 ρ_2 ρ_3

$\mathrm{Im}\left[\rho_i(X)\overline{\rho_i(Y)}\right]$

	x	$\star$	y
x	0	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{3}}{2}$
$\star$	$-\frac{\sqrt{3}}{2}$	0	0
y	$-\frac{\sqrt{3}}{2}$	0	0

	x	$\star$	y
x	0	0	$\frac{\sqrt{3}}{2}$
$\star$	0	0	$\frac{\sqrt{3}}{2}$
y	$-\frac{\sqrt{3}}{2}$	$-\frac{\sqrt{3}}{2}$	0

	x	$\star$	y
x	0	$-\frac{\sqrt{3}}{2}$	$\frac{\sqrt{3}}{2}$
$\star$	$\frac{\sqrt{3}}{2}$	0	$-\frac{\sqrt{3}}{2}$
y	$-\frac{\sqrt{3}}{2}$	$\frac{\sqrt{3}}{2}$	0

- We show that at least one of the following embeddings $\rho_1, \rho_2, \rho_3 \colon \{x, y, \star\} \to \mathbb{C}_3^\times$ satisfies the claim:

	x	$\star$	y
ρ_1	$\bar{\zeta}$	ζ	ζ
ρ_2	$\bar{\zeta}$	$\bar{\zeta}$	ζ
ρ_3	$\bar{\zeta}$	1	ζ

Asymmetric Self-Couplings

Proof:

- Observe that

$$\mathbb{E}_{X,Y}\,\mathbb{E}_{i\sim\{1,2,3\}}[\operatorname{Im}\rho_i(X)\overline{\rho_i(Y)}] = \frac{\sqrt{3}}{2}\cdot(\Pr[X=x,Y=y]-\Pr[X=y,Y=x]).$$

- By linearity of the $\mathbb{E}$ and Im operators the desired inequality must hold for at least one of ρ_1, ρ_2, ρ_3.

Definition (Zero-sum game G_N)

- Alice chooses a function $f\colon \{1, \ldots, N\} \to \mathbb{C}_3^\times = \{1, \zeta, \overline{\zeta}\}$, where $\mathbb{C}_3^\times$ consists of cube roots of unity.
- Bob chooses a pair of indices $1 \leq I < J \leq N$.
- Bob pays Alice $\mathrm{im} f(I)\overline{f(J)}$ dollars.

Asymmetric Self-Couplings
A Game

Observations about the game:

- This game has a unique value (by von Neumann's min-max theorem).
- For every N the value G_N can be shown to be strictly positive.
  - Alice can ensure an expected payout of $\Omega(1/(N-1))$ by playing the following mixed strategy:
$$f(x) = \begin{cases} \zeta, & \text{if } x \leq K \\ 1, & \text{otherwise,} \end{cases}$$
    where the cutoff K is chosen uniformly at random from $\{1, \ldots, N-1\}$.

Asymmetric Self-Couplings

A Game

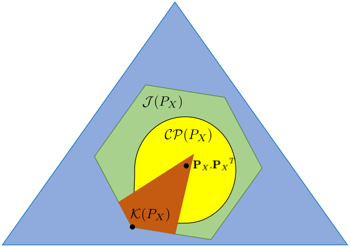
Lemma

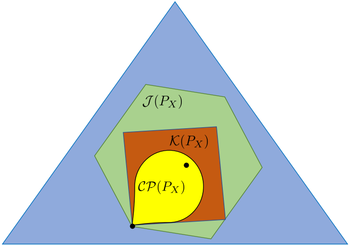
The value of G_N is at most $O(1/\log N)$.

Proof via:

- Fourier analysis over the Boolean hypercube
- Gibbs phenomenon

In Conclusion





Rate and Review!