Channel Resolvability Codes based on Sparse Random Linear Coding

Rana Ali Amjad
joint work with Gerhard Kramer

Jan 30, 2015
Channel Resolvability

- **Aim:** Approximate Random number generation at the output of a channel.
- **Appr. Measures** Informational divergence, Normalized informational divergence, Variational distance.
- **Applications:** Secrecy, Stealth, Coordination.
Achievability and Converse

A rate $R$ is said to be achievable if there exists an encoder such that

$$\mathbb{D}(P_{Y^n} \parallel Q_{Y}^n) \xrightarrow{n \to \infty} 0$$

- **Converse:** No rate $R < I(X; Y)$ achievable.
- **Achievability:** Any $R > I(X; Y)$ achievable.
  - Proved using random coding arguments.
  - Code design with reasonable complexity is still largely an open problem.
Random Linear Coding (RLC)

Encoder Operation

\[ X^n = UG \oplus V^n \]

\( G \) is a \( nR \times n \) random binary matrix.

- We showed that any \( R > I(X; Y) \) is achievable using RLC.
- The encoding complexity is \( \mathcal{O}(n^2) \).
Sparse Random Linear Coding

Encoder Operation:

\[ X^n = W G_L \oplus V^n \]
\[ W = U G_D. \]

\( G_L \) is a known \( nR \times f \) binary matrix, \( G_L \) is a \( f \times n \) sparse random binary matrix.

- We showed that any \( R > I(X; Y) \) is achievable using sparse RLC.
- Encoding complexity \( \mathcal{O}(n \log n) \) is achievable.
Thank you