Trivial is (Sometimes) Best: Distributed Hypothesis Testing via Linear Codes

Adway Girish

joint work with Robinson Cung and Emre Telatar

January 30, 2026
LIDS student conference

Binary hypothesis testing

- $\mathcal{H} \in \{0, 1\} \,:\, Z \sim \mathsf{P}_Z^{\mathcal{H}}$

Binary hypothesis testing

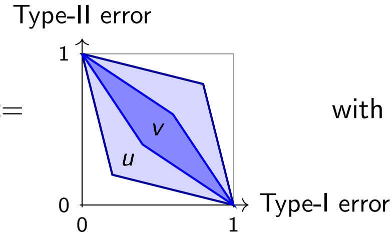
- $\mathcal{H} \in \{0, 1\} : Z \sim \mathsf{P}_Z^{\mathcal{H}}$; observe Z, declare $\hat{\mathcal{H}} \in \{0, 1\}$ as function of Z

Binary hypothesis testing

- $\mathcal{H} \in \{0,1\} : Z \sim \mathrm{P}_Z^{\mathcal{H}}$; observe Z, declare $\hat{\mathcal{H}} \in \{0,1\}$ as function of Z
- Type-I error $= \mathrm{P}_Z^0\{\hat{\mathcal{H}} = 1\}$ and Type-II error $= \mathrm{P}_Z^1\{\hat{\mathcal{H}} = 0\}$

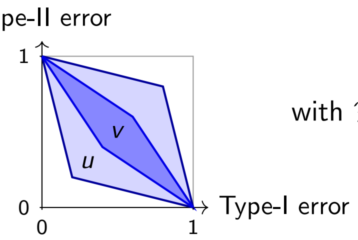
Binary hypothesis testing, Blackwell order

- $\mathcal{H} \in \{0,1\} : Z \sim \mathrm{P}_Z^{\mathcal{H}}$; observe Z, declare $\hat{\mathcal{H}} \in \{0,1\}$ as function of Z
- Type-I error $= \mathrm{P}_Z^0\{\hat{\mathcal{H}} = 1\}$ and Type-II error $= \mathrm{P}_Z^1\{\hat{\mathcal{H}} = 0\}$
- $u(Z) \succeq v(Z) \;:=$



with $\hat{\mathcal{H}}$ function of $u(Z), v(Z)$ resp.

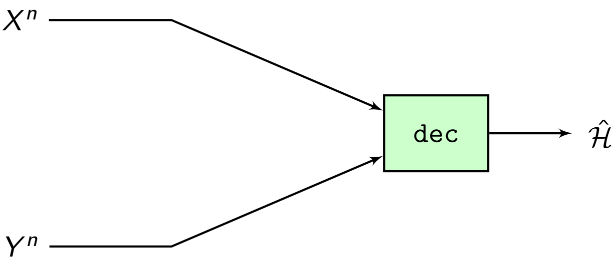
Binary hypothesis testing, Blackwell order

- $\mathcal{H} \in \{0,1\} : Z \sim \mathsf{P}_Z^{\mathcal{H}}$; observe Z, declare $\hat{\mathcal{H}} \in \{0,1\}$ as function of Z
- Type-I error $= \mathsf{P}_Z^0\{\hat{\mathcal{H}} = 1\}$ and Type-II error $= \mathsf{P}_Z^1\{\hat{\mathcal{H}} = 0\}$
- $u(Z) \succeq v(Z) \;:=$ 

with $\hat{\mathcal{H}}$ function of $u(Z), v(Z)$ resp.
- $u(Z) \succeq v(Z) \iff$ there exists $\mathsf{P}_{V|U}$ such that $\mathsf{P}_{u(Z)}^{\mathcal{H}} \xrightarrow{\mathsf{P}_{V|U}} \mathsf{P}_{v(Z)}^{\mathcal{H}}$ for both $\mathcal{H} = 0, 1$

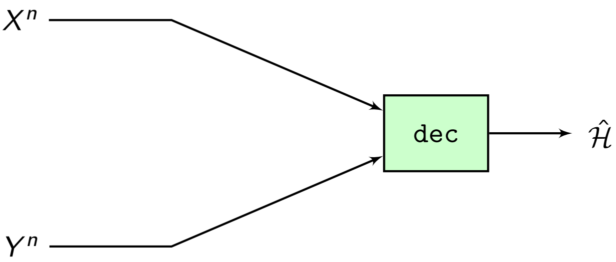
(Centralized) hypothesis testing

$\mathcal{H} \in \{0, 1\} : (X_i, Y_i) \overset{\text{i.i.d.}}{\sim} \mathsf{P}^{\mathcal{H}}$



(Centralized) hypothesis testing

$\mathcal{H} \in \{0,1\} : (X_i, Y_i) \overset{\text{i.i.d.}}{\sim} \mathrm{P}^{\mathcal{H}}$



$$(X^n, Y^n) \succeq f(X^n, Y^n) \quad \text{for any } f$$

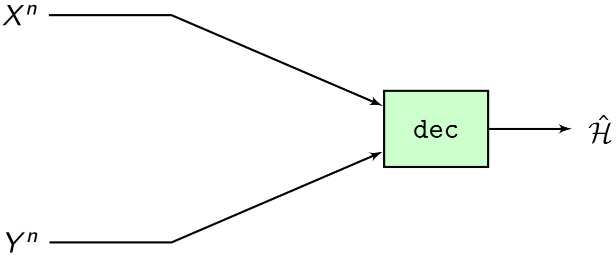
(Centralized) hypothesis testing: binary inputs

$\mathcal{H} \in \{0,1\} : (X_i, Y_i) \overset{\text{i.i.d.}}{\sim} \mathsf{P}^{\mathcal{H}}$

$X_i, Y_i \in \{0,1\}$ w.p. $1/2$

$\mathsf{P}^{\mathcal{H}}\{X_i \neq Y_i\} = p_{\mathcal{H}}$

$\text{corr}_{\mathcal{H}}(X_i, Y_i) = \rho_{\mathcal{H}} = 1 - 2p_{\mathcal{H}}$



$(X^n, Y^n) \succeq f(X^n, Y^n)$ for any f

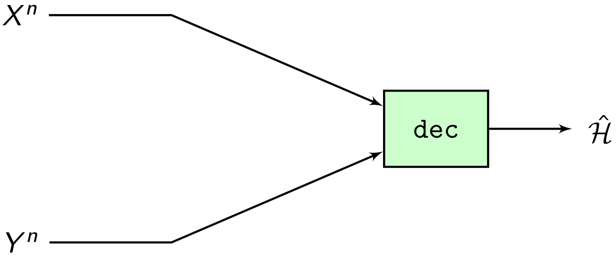
(Centralized) hypothesis testing: binary inputs

$\mathcal{H} \in \{0,1\} : (X_i, Y_i) \overset{\text{i.i.d.}}{\sim} \mathrm{P}^{\mathcal{H}}$

$X_i, Y_i \in \{0,1\}$ w.p. $1/2$

$\mathrm{P}^{\mathcal{H}}\{X_i \neq Y_i\} = p_{\mathcal{H}}$

$\mathrm{corr}_{\mathcal{H}}(X_i, Y_i) = \rho_{\mathcal{H}} = 1 - 2p_{\mathcal{H}}$



$X^n \oplus Y^n$ sufficient, $\quad X^n \oplus Y^n \succeq (X^n, Y^n) \succeq f(X^n, Y^n)$ for any f

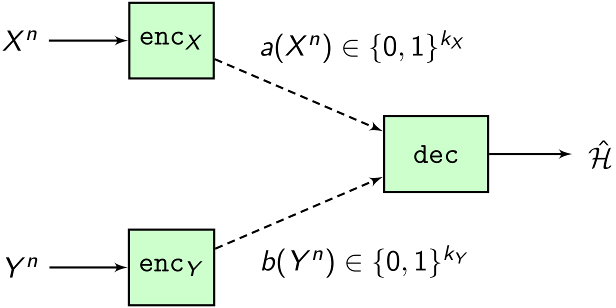
Distributed hypothesis testing: binary inputs

$\mathcal{H} \in \{0,1\} : (X_i, Y_i) \overset{\text{i.i.d.}}{\sim} \mathrm{P}^{\mathcal{H}}$

$X_i, Y_i \in \{0,1\}$ w.p. $1/2$

$\mathrm{P}^{\mathcal{H}}\{X_i \neq Y_i\} = p_{\mathcal{H}}$

$\mathrm{corr}_{\mathcal{H}}(X_i, Y_i) = \rho_{\mathcal{H}} = 1 - 2p_{\mathcal{H}}$



$X^n \oplus Y^n$ sufficient, $\quad X^n \oplus Y^n \succeq (X^n, Y^n) \succeq f(X^n, Y^n)$ for any f

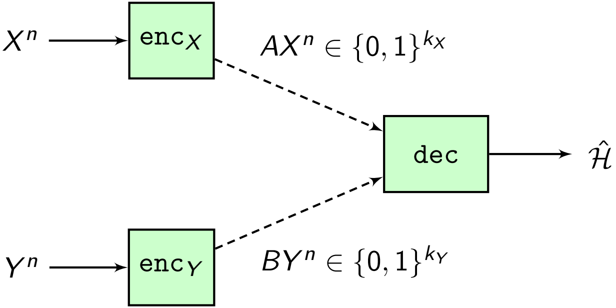
Distributed hypothesis testing: binary inputs, linear codes

$\mathcal{H} \in \{0,1\} : (X_i, Y_i) \overset{\text{i.i.d.}}{\sim} \mathrm{P}^{\mathcal{H}}$

$X_i, Y_i \in \{0,1\}$ w.p. $1/2$

$\mathrm{P}^{\mathcal{H}}\{X_i \neq Y_i\} = p_{\mathcal{H}}$

$\mathrm{corr}_{\mathcal{H}}(X_i, Y_i) = \rho_{\mathcal{H}} = 1 - 2p_{\mathcal{H}}$

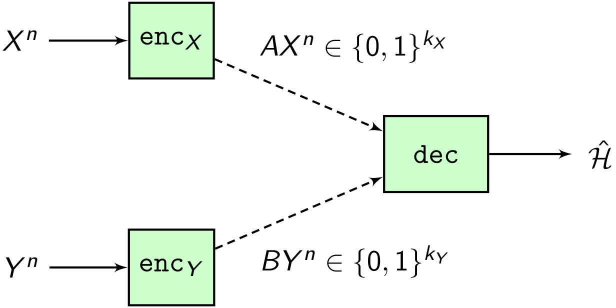


$X^n \oplus Y^n$ sufficient, $\quad X^n \oplus Y^n \succeq (X^n, Y^n) \succeq f(X^n, Y^n)$ for any f

Distributed hypothesis testing: binary inputs, linear codes

$\mathcal{H} \in \{0,1\} : (X_i, Y_i) \overset{\text{i.i.d.}}{\sim} \mathrm{P}^{\mathcal{H}}$

$X_i, Y_i \in \{0,1\}$ w.p. $1/2$
$\mathrm{P}^{\mathcal{H}}\{X_i \neq Y_i\} = p_{\mathcal{H}}$
$\mathrm{corr}_{\mathcal{H}}(X_i, Y_i) = \rho_{\mathcal{H}} = 1 - 2p_{\mathcal{H}}$



$X^n \oplus Y^n$ sufficient, $\quad X^n \oplus Y^n \succeq (X^n, Y^n) \succeq f(X^n, Y^n)$ for any f

Is there a “best” linear code?

Truncation is sometimes the best linear code

Truncation is sometimes the best linear code

- $AX^n \oplus AY^n \succeq (AX^n, AY^n) \succeq (AX^n, BY^n)$ for any A, B, for any ρ_0, ρ_1 ✓

Truncation is sometimes the best linear code

- $AX^n \oplus AY^n \succeq (AX^n, AY^n) \succeq (AX^n, BY^n)$ for any A, B, for any ρ_0, ρ_1 ✓
  (same linear code + modulo-2 sum sufficient)

Truncation is sometimes the best linear code

- $AX^n \oplus AY^n \succeq (AX^n, AY^n) \succeq (AX^n, BY^n)$ for any A, B, for any ρ_0, ρ_1 ✓
  (same linear code + modulo-2 sum sufficient)

- $X^k \oplus Y^k \succeq AX^n \oplus AY^n$ for (1) $\rho_0 = 0$ or $\rho_1 = 0$, (3) $\rho_1 = -\rho_0$ ✓

Truncation is sometimes the best linear code

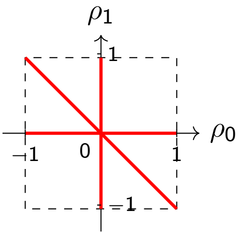
- $AX^n \oplus AY^n \succeq (AX^n, AY^n) \succeq (AX^n, BY^n)$ for any A, B, for any ρ_0, ρ_1 ✓
  (same linear code + modulo-2 sum sufficient)

- $X^k \oplus Y^k \succeq AX^n \oplus AY^n$ for (1) $\rho_0 = 0$ or $\rho_1 = 0$, (3) $\rho_1 = -\rho_0$ ✓
  (linear codes “bad” — only as good as simple truncation — for some parameters)

Truncation is sometimes the best linear code

- $AX^n \oplus AY^n \succeq (AX^n, AY^n) \succeq (AX^n, BY^n)$ for any A, B, for any ρ_0, ρ_1 ✓
  (same linear code + modulo-2 sum sufficient)

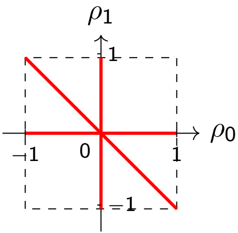
- $X^k \oplus Y^k \succeq AX^n \oplus AY^n$ for (1) $\rho_0 = 0$ or $\rho_1 = 0$, (3) $\rho_1 = -\rho_0$ ✓
  (linear codes "bad" — only as good as simple truncation — for some parameters)



Truncation is sometimes the best linear code

- $AX^n \oplus AY^n \succeq (AX^n, AY^n) \succeq (AX^n, BY^n)$ for any A, B, for any ρ_0, ρ_1 ✓
  (same linear code + modulo-2 sum sufficient)

- $X^k \oplus Y^k \succeq AX^n \oplus AY^n$ for (1) $\rho_0 = 0$ or $\rho_1 = 0$, (3) $\rho_1 = -\rho_0$ ✓
  (linear codes "bad" — only as good as simple truncation — for some parameters)

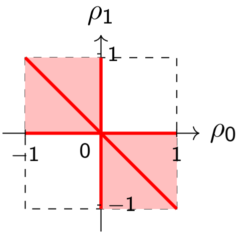


- conjecture: $X^k \oplus Y^k \succeq AX^n \oplus AY^n$ for all ρ_0, ρ_1 of opposite signs ?

Truncation is sometimes the best linear code

- $AX^n \oplus AY^n \succeq (AX^n, AY^n) \succeq (AX^n, BY^n)$ for any A, B, for any ρ_0, ρ_1 ✓
  (same linear code + modulo-2 sum sufficient)

- $X^k \oplus Y^k \succeq AX^n \oplus AY^n$ for (1) $\rho_0 = 0$ or $\rho_1 = 0$, (3) $\rho_1 = -\rho_0$ ✓
  (linear codes "bad" — only as good as simple truncation — for some parameters)

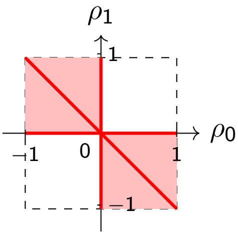


- conjecture: $X^k \oplus Y^k \succeq AX^n \oplus AY^n$ for all ρ_0, ρ_1 of opposite signs ?

Truncation is sometimes the best linear code

- $AX^n \oplus AY^n \succeq (AX^n, AY^n) \succeq (AX^n, BY^n)$ for any A, B, for any ρ_0, ρ_1 ✓
  (same linear code + modulo-2 sum sufficient)

- $X^k \oplus Y^k \succeq AX^n \oplus AY^n$ for (1) $\rho_0 = 0$ or $\rho_1 = 0$, (3) $\rho_1 = -\rho_0$ ✓
  (linear codes "bad" — only as good as simple truncation — for some parameters)



- conjecture: $X^k \oplus Y^k \succeq AX^n \oplus AY^n$ for all ρ_0, ρ_1 of opposite signs ?
  (linear codes "bad" for testing any positive vs. negative correlation)

Proof

Proof

- recall: $u(Z) \succeq v(Z) \iff$ there exists $\mathrm{P}_{V|U}$ such that $\mathrm{P}^{\mathcal{H}}_{u(Z)} \xrightarrow{\mathrm{P}_{V|U}} \mathrm{P}^{\mathcal{H}}_{v(Z)}$

Proof

- recall: $u(Z) \succeq v(Z) \iff$ there exists $\mathsf{P}_{V|U}$ such that $\mathsf{P}^{\mathcal{H}}_{u(Z)} \xrightarrow{\mathsf{P}_{V|U}} \mathsf{P}^{\mathcal{H}}_{v(Z)}$
- explicitly construct channel (that does not depend on $\mathcal{H}$) so that

$$\begin{aligned} &\mathsf{P}^{\mathcal{H}}_{AX^n \oplus AY^n} \longrightarrow \mathsf{P}^{\mathcal{H}}_{(AX^n, BY^n)} && \text{for any } \rho_0, \rho_1 \\ &\mathsf{P}^{\mathcal{H}}_{X^k \oplus Y^k} \longrightarrow \mathsf{P}^{\mathcal{H}}_{AX^n \oplus AY^n} && \text{for (1) } \rho_1 = 0 \text{ or } \rho_0 = 0, \text{ (3) } \rho_1 = -\rho_0 \end{aligned}$$

Proof

- recall: $u(Z) \succeq v(Z) \iff$ there exists $\mathrm{P}_{V|U}$ such that $\mathrm{P}^{\mathcal{H}}_{u(Z)} \xrightarrow{\mathrm{P}_{V|U}} \mathrm{P}^{\mathcal{H}}_{v(Z)}$

- explicitly construct channel (that does not depend on $\mathcal{H}$) so that

$$\mathrm{P}^{\mathcal{H}}_{AX^n \oplus AY^n} \longrightarrow \mathrm{P}^{\mathcal{H}}_{(AX^n, BY^n)} \quad \text{for any } \rho_0, \rho_1$$

$$\mathrm{P}^{\mathcal{H}}_{X^k \oplus Y^k} \longrightarrow \mathrm{P}^{\mathcal{H}}_{AX^n \oplus AY^n} \quad \text{for (1) } \rho_1 = 0 \text{ or } \rho_0 = 0, \text{ (3) } \rho_1 = -\rho_0$$

- conjecture:

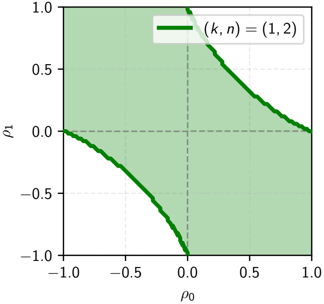
Proof

- recall: $u(Z) \succeq v(Z) \iff$ there exists $\mathsf{P}_{V|U}$ such that $\mathsf{P}^{\mathcal{H}}_{u(Z)} \xrightarrow{\mathsf{P}_{V|U}} \mathsf{P}^{\mathcal{H}}_{v(Z)}$
- explicitly construct channel (that does not depend on $\mathcal{H}$) so that

$$\mathsf{P}^{\mathcal{H}}_{AX^n \oplus AY^n} \longrightarrow \mathsf{P}^{\mathcal{H}}_{(AX^n, BY^n)} \quad \text{for any } \rho_0, \rho_1$$

$$\mathsf{P}^{\mathcal{H}}_{X^k \oplus Y^k} \longrightarrow \mathsf{P}^{\mathcal{H}}_{AX^n \oplus AY^n} \quad \text{for (1) } \rho_1 = 0 \text{ or } \rho_0 = 0, \text{ (3) } \rho_1 = -\rho_0$$

- conjecture:



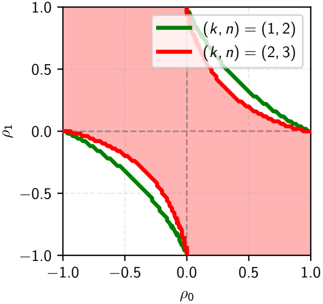
Proof

- recall: $u(Z) \succeq v(Z) \iff$ there exists $\mathsf{P}_{V|U}$ such that $\mathsf{P}^{\mathcal{H}}_{u(Z)} \xrightarrow{\mathsf{P}_{V|U}} \mathsf{P}^{\mathcal{H}}_{v(Z)}$
- explicitly construct channel (that does not depend on $\mathcal{H}$) so that

$$\mathsf{P}^{\mathcal{H}}_{AX^n \oplus AY^n} \longrightarrow \mathsf{P}^{\mathcal{H}}_{(AX^n, BY^n)} \quad \text{for any } \rho_0, \rho_1$$

$$\mathsf{P}^{\mathcal{H}}_{X^k \oplus Y^k} \longrightarrow \mathsf{P}^{\mathcal{H}}_{AX^n \oplus AY^n} \quad \text{for (1) } \rho_1 = 0 \text{ or } \rho_0 = 0\text{, (3) } \rho_1 = -\rho_0$$

- conjecture:



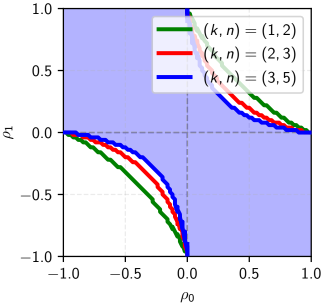
Proof

- recall: $u(Z) \succeq v(Z) \iff$ there exists $\mathsf{P}_{V|U}$ such that $\mathsf{P}^{\mathcal{H}}_{u(Z)} \xrightarrow{\mathsf{P}_{V|U}} \mathsf{P}^{\mathcal{H}}_{v(Z)}$
- explicitly construct channel (that does not depend on $\mathcal{H}$) so that

$$\mathsf{P}^{\mathcal{H}}_{AX^n \oplus AY^n} \longrightarrow \mathsf{P}^{\mathcal{H}}_{(AX^n, BY^n)} \quad \text{for any } \rho_0, \rho_1$$

$$\mathsf{P}^{\mathcal{H}}_{X^k \oplus Y^k} \longrightarrow \mathsf{P}^{\mathcal{H}}_{AX^n \oplus AY^n} \quad \text{for (1) } \rho_1 = 0 \text{ or } \rho_0 = 0, \text{ (3) } \rho_1 = -\rho_0$$

- conjecture:



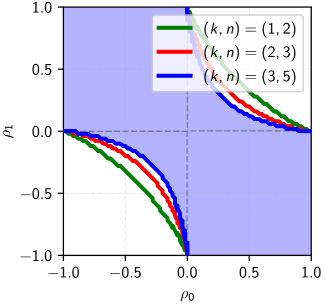
Proof

- recall: $u(Z) \succeq v(Z) \iff$ there exists $\mathrm{P}_{V|U}$ such that $\mathrm{P}^{\mathcal{H}}_{u(Z)} \xrightarrow{\mathrm{P}_{V|U}} \mathrm{P}^{\mathcal{H}}_{v(Z)}$
- explicitly construct channel (that does not depend on $\mathcal{H}$) so that

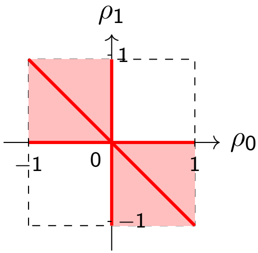
$$\mathrm{P}^{\mathcal{H}}_{AX^n \oplus AY^n} \longrightarrow \mathrm{P}^{\mathcal{H}}_{(AX^n, BY^n)} \quad \text{for any } \rho_0, \rho_1$$

$$\mathrm{P}^{\mathcal{H}}_{X^k \oplus Y^k} \longrightarrow \mathrm{P}^{\mathcal{H}}_{AX^n \oplus AY^n} \quad \text{for (1) } \rho_1 = 0 \text{ or } \rho_0 = 0, \text{ (3) } \rho_1 = -\rho_0$$

- conjecture:



$\xrightarrow[n\to\infty]{?}$



Summary

Summary

- truncation is the best linear code for testing:

  (1) for/against independence

  (2) opposite correlations of same magnitude

Summary

- truncation is the best linear code for testing:

  (1) for/against independence

  (2) opposite correlations of same magnitude

- conjecture: also for testing opposite correlations of any magnitude

Summary

- truncation is the best linear code for testing:
  (1) for/against independence
  (2) opposite correlations of same magnitude

- conjecture: also for testing opposite correlations of any magnitude

arXiv:2601.10526

Thank you!