

Title: Random constructions in Quantum Information Theory

Date: Jul 04, 2010 09:15 AM

URL: <http://pirsa.org/10070004>

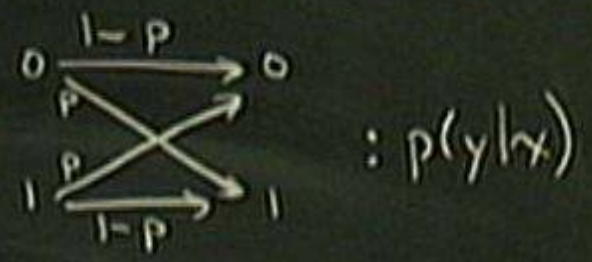
Abstract: TBA

PERIMETER  INSTITUTE FOR THEORETICAL PHYSICS

A VERY FAMOUS RANDOM CONSTRUCTION

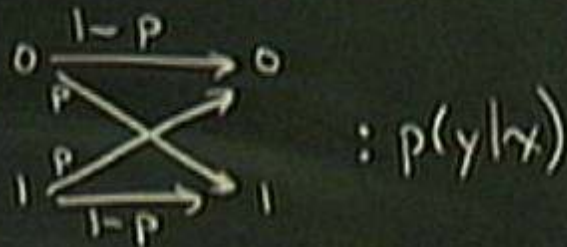
A VERY FAMOUS RANDOM CONSTRUCTION

BINARY
SYMMETRIC
CHANNEL



A VERY FAMOUS RANDOM CONSTRUCTION

BINARY
SYMMETRIC
CHANNEL



MANY USES

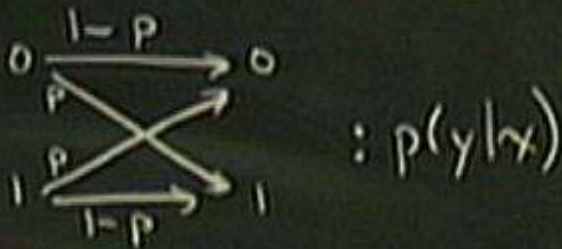
$$p^n(y_1 \dots y_n | x_1 \dots x_n) = \prod_{i=1}^n p(y_i | x_i)$$

$\overset{y^n}{\underbrace{}}$ $\overset{x^n}{\underbrace{}}$

p^n

A VERY FAMOUS RANDOM CONSTRUCTION

BINARY
SYMMETRIC
CHANNEL



$$: p(y|x)$$

MANY USES

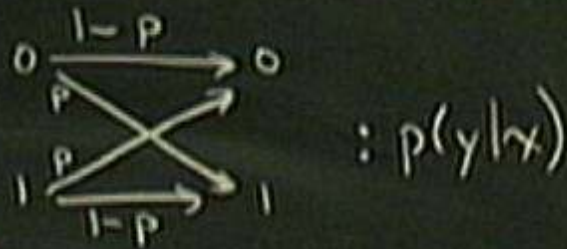
$$p^n(y_1 \dots y_n | x_1 \dots x_n) = \prod_{i=1}^n p(y_i | x_i)$$

$\underbrace{\hspace{10em}}_{y^n}$
 $\underbrace{\hspace{10em}}_{x^n}$



A VERY FAMOUS RANDOM CONSTRUCTION

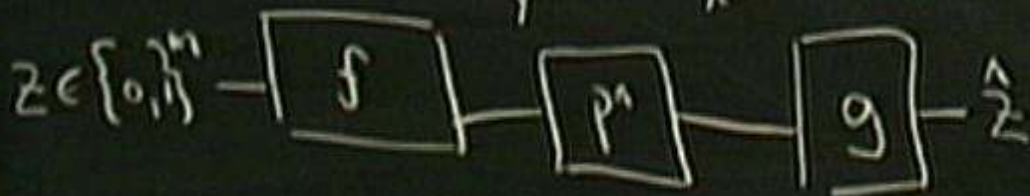
BINARY
SYMMETRIC
CHANNEL



MANY USES

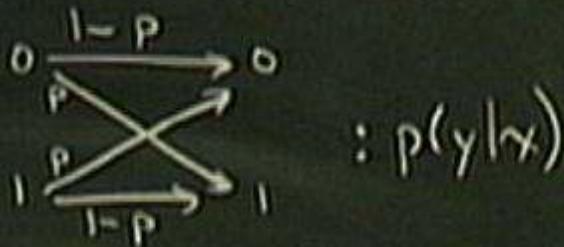
$$p^n(y_1 \dots y_n | x_1 \dots x_n) = \prod_{i=1}^n p(y_i | x_i)$$

$\underbrace{\hspace{10em}}_{y^n} \quad \underbrace{\hspace{10em}}_{x^n}$



A VERY FAMOUS RANDOM CONSTRUCTION

BINARY
SYMMETRIC
CHANNEL

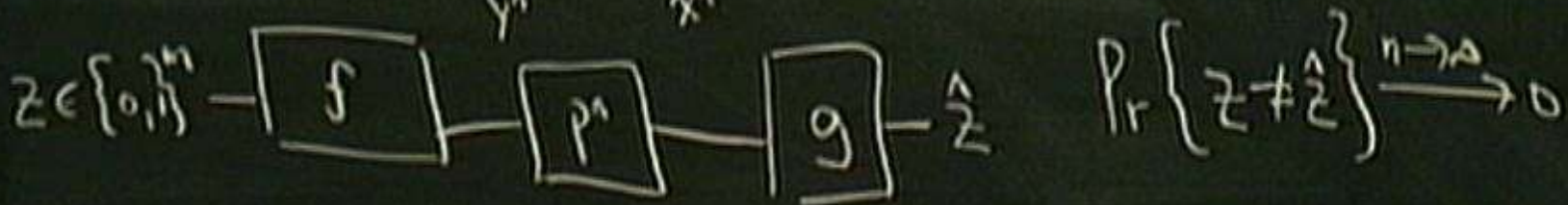


$$: p(y|x)$$

MANY USES

$$p^n(y_1 \dots y_n | x_1 \dots x_n) = \prod_{i=1}^n p(y_i | x_i)$$

$\underbrace{\hspace{10em}}_{y^n}$
 $\underbrace{\hspace{10em}}_{x^n}$



HOW TO FIND NEAR-OPTIMAL f ?

ie $\frac{M}{n} \rightarrow 1 - H(p)$, $H(p) = -p \log p - (1-p) \log (1-p)$

HOW TO FIND NEAR-OPTIMAL f ?

ie $\frac{m}{n} \rightarrow 1 - H(p)$, $H(p) = -p \log p - (1-p) \log (1-p)$

- f FUNCTION WLOG.

HOW TO FIND NEAR-OPTIMAL f ?

ie $\frac{m}{n} \rightarrow 1 - H(p)$, $H(p) = -p \log p - (1-p) \log (1-p)$

- f FUNCTION WLOG.
- CHOOSE $f(z) \in_{\text{unif}} \{0,1\}^n$ iid $\forall z$.

HOW TO FIND NEAR-OPTIMAL f ?

ie $\frac{m}{n} \rightarrow 1 - H(p)$, $H(p) = -p \log p - (1-p) \log (1-p)$

- f FUNCTION WLOG.
- CHOOSE $f(z) \in_{\text{unif}} \{0,1\}^n$ iid $\forall z$
- AVG $\Pr\{z \neq f(z)\}$ (FOR UNIF z) OVER CHOICES OF f .

DICTIONARY

CLASSICAL

UNIT OF INFO

BIT $b \in \{0, 1\}$

CONCATENATE

BITS $b^i \in \{0, 1\}^n$

UNCERTAINTY

PROB DENSITY

CHANNEL

STOCHASTIC MAP
 $P(y|x)$

DISTINGUISHABILITY

$$\|p - q\|_1 = \sum_i |p_i - q_i|$$

DETERMINISTIC
EVOLUTION

FUNCTION

QUANTUM

QUBIT $|\psi\rangle \in \mathbb{C}^2 = \text{span}\{|0\rangle, |1\rangle\}$
 $\langle\psi|\psi\rangle = 1$

QUBITS $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} = \text{span}\{|b^i\rangle; b^i \in \{0, 1\}^n\}$

UNITARY (ISOMETRY) $|\psi\rangle \mapsto U|\psi\rangle$
 $\rho \mapsto U\rho U^\dagger$

DICTIONARY

CLASSICAL

UNIT OF INFO

BIT $b \in \{0, 1\}$

CONCATENATE

BITS $b^i \in \{0, 1\}^n$

UNCERTAINTY

PROB DENSITY

CHANNEL

STOCHASTIC MAP
 $P(y|x)$

DISTINGUISHABILITY

$$\|p - q\|_1 = \sum_i |p_i - q_i|$$

DETERMINISTIC EVOLUTION

FUNCTION

QUANTUM

QUBIT $|i\rangle \in \mathbb{C}^2 = \text{span}\{|0\rangle, |1\rangle\}$
 $\langle i | i \rangle = 1$

QUBITS $|i\rangle \in (\mathbb{C}^2)^{\otimes n} = \text{span}\{|b^i\rangle; b^i \in \{0, 1\}^n\}$

DENSITY OPERATOR

$$\rho \in \text{Den}(A) = \{\rho \in \text{Her}(A); \text{tr} \rho = 1, \rho \geq 0\}$$

UNITARY (ISOMETRY)

$$|i\rangle \mapsto U|i\rangle$$
$$\rho \mapsto U\rho U^\dagger$$

DICTIONARY

CLASSICAL

UNIT OF INFO

BIT $b \in \{0, 1\}$

CONCATENATE

BITS $b^n \in \{0, 1\}^n$

UNCERTAINTY

PROB. DENSITY

CHANNEL

STOCHASTIC MAP
 $P(y|x)$

DISTINGUISHABILITY

$$\|p - q\|_1 = \sum_i |p_i - q_i|$$

DETERMINISTIC
EVOLUTION

FUNCTION

QUANTUM

QUBIT $|1\rangle \in \mathbb{C}^2 = \text{span}\{|0\rangle, |1\rangle\}$
 $\langle 1|1\rangle = 1$

QUBITS $|1\rangle \in (\mathbb{C}^2)^{\otimes n} = \text{span}\{|b\rangle; b^n \in \{0, 1\}^n\}$

DENSITY OPERATOR

$$\rho \in \mathcal{D}(\mathcal{H}) = \{\rho \in \mathcal{H}(\mathcal{H}) \mid \text{tr} \rho = 1, \rho \geq 0\}$$

$$\mathcal{N}: \mathcal{D}(\mathcal{H}(A)) \rightarrow \mathcal{D}(\mathcal{H}(B))$$

UNITARY (ISOMETRY) $|1\rangle \mapsto U|1\rangle$
 $\rho \mapsto U\rho U^\dagger$

DICTIONARY

CLASSICAL

UNIT OF INFO

BIT $b \in \{0, 1\}$

CONCATENATE

BITS $b^n \in \{0, 1\}^n$

UNCERTAINTY

PROB DENSITY

CHANNEL

STOCHASTIC MAP
 $P(y|x)$

DISTINGUISHABILITY

$$\|p - q\|_1 = \sum_i |p_i - q_i|$$

DETERMINISTIC
EVOLUTION

FUNCTION

QUANTUM

QUBIT $|1\rangle \in \mathbb{C}^2 = \text{span}\{|0\rangle, |1\rangle\}$
 $\langle 1|1\rangle = 1$

QUBITS $|1\rangle \in (\mathbb{C}^2)^{\otimes n} = \text{span}\{|b\rangle; b^n \in \{0, 1\}^n\}$

DENSITY OPERATOR

$$\rho \in \text{Den}(A) = \{\rho \in \text{Her}(A); \text{tr} \rho = 1, \rho \geq 0\}$$

$N: \text{Den}(A) \rightarrow \text{Den}(B)$ LINEAR

$$\|\rho - \sigma\|_1 \leftarrow \text{trace norm} = \text{nuclear norm}$$

UNITARY (ISOMETRY) $|1\rangle \mapsto U|1\rangle$
 $\rho \mapsto U\rho U^\dagger$

HOW TO FIND NEAR-OPTIMAL f ?

ie $\frac{m}{n} \rightarrow 1 - H(p)$, $H(p) = -p \log p - (1-p) \log (1-p)$

- f FUNCTION WLOG

- CHOOSE $f(z) \in_{\text{unif}} \{0,1\}^n$ iid $\forall z$

- AVG $\Pr\{z \neq f(z)\}$ (FOR UNIF z) OVER CHOICES OF f .

DIRAC BRAKET NOTATION

$|x\rangle \in A$

$\langle x| = (|x\rangle)^\dagger$

NO
SMOKING
HERE

• AVG $P_{\{z \neq \frac{1}{2}\}}$ (FOR UNIF z) OVER

DIRAC BRAKET NOTATION

$$|\psi\rangle \in A$$

$$\langle\psi| = (|\psi\rangle)^*$$

$$\langle\psi|\psi\rangle$$

INNER PRODUCT

$$|\psi\rangle\langle\psi|$$

A LESS FAMOUS ANALOGUE: QUANTUM ERROR CORRECTION

A LESS FAMOUS ANALOGUE: QUANTUM ERROR CORRECTION

PAULI CHANNEL

$$\mathcal{N}(\rho) = \sum_{i=0}^3 p_i \sigma_i \rho \sigma_i^\dagger$$



A LESS FAMOUS ANALOGUE: QUANTUM ERROR CORRECTION

PAULI CHANNEL

$$p_i \geq 0 \quad \sum_i p_i = 1.$$

$$\mathcal{N}(\rho) = \sum_{i=0}^3 p_i \sigma_i \rho \sigma_i^\dagger$$

$$\sigma_0 = \mathbb{I} \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



PAULI CHANNEL

$$p_i \geq 0 \quad \sum_i p_i = 1.$$

$$\mathcal{N}(\rho) = \sum_{i=0}^3 p_i \sigma_i \rho \sigma_i^\dagger$$

$$\sigma_0 = I \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



PAULI CHANNEL

$$p_i \geq 0 \quad \sum_i p_i = 1.$$

$$\mathcal{N}(\rho) = \sum_{i=0}^3 p_i \sigma_i \rho \sigma_i^\dagger$$

$$\sigma_0 = I$$

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$

$|\psi\rangle \langle \psi|$



$|\varphi\rangle$

PAULI CHANNEL

$$p_i \geq 0 \quad \sum_i p_i = 1$$

$$\mathcal{N}(\rho) = \sum_{i=0}^3 p_i \sigma_i \rho \sigma_i^\dagger$$

$$\sigma_0 = I$$

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$$

$$|\psi\rangle \langle \psi|$$



$$|\varphi\rangle$$

$$\forall |\psi\rangle$$

$$\| |\psi\rangle \langle \psi| - \varphi \| < \epsilon$$

$$\epsilon \xrightarrow{n \rightarrow \infty} 0$$

A LESS FAMOUS ANALOGUE: QUANTUM ERROR CORRECTION

PAULI CHANNEL

$$p_i \geq 0 \quad \sum_i p_i = 1$$

$$\mathcal{N}(\rho) = \sum_{i=0}^3 p_i \sigma_i \rho \sigma_i$$

$$\sigma_0 = I \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\|\rho\|_{\infty} \leq \epsilon$$



$$\forall |\psi\rangle \quad \|\mathcal{N}^{\otimes n}(|\psi\rangle) - |\phi\rangle\| < \epsilon$$

$$\epsilon \xrightarrow{n \rightarrow \infty} 0$$

HOW TO FIND A GOOD \mathcal{E} ?

$\rho \in \mathcal{S}(\mathcal{H})$
 $\rho \geq 0$



A LESS FAMOUS ANALOGUE: QUANTUM ERROR CORRECTION

PAULI CHANNEL

$$p_i \geq 0 \quad \sum_i p_i = 1$$

$$N(\rho) = \sum_{i=0}^3 p_i \sigma_i \rho \sigma_i$$

$$\sigma_0 = I \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$$



$$\forall |\psi\rangle \quad \|\mathcal{E}(|\psi\rangle\langle\psi|) - \varphi\| < \epsilon$$

$$\epsilon \xrightarrow{n \rightarrow \infty} 0$$

HOW TO FIND A GOOD \mathcal{E} ?

- USE ISOMETRY $\mathcal{E}(\cdot) = E \cdot E^\dagger$



A LESS FAMOUS ANALOGUE: QUANTUM ERROR CORRECTION

PAULI CHANNEL

$$p_i \geq 0 \quad \sum_i p_i = 1$$

$$\mathcal{N}(\rho) = \sum_{i=0}^3 p_i \sigma_i \rho \sigma_i^\dagger$$

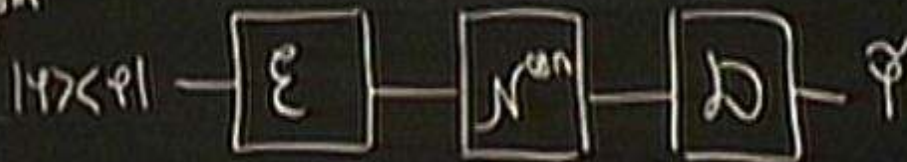
$$\sigma_0 = I$$

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$$



$$\forall |\psi\rangle \quad \|\mathcal{D}(\mathcal{N}^{\otimes n}(\mathcal{E}(|\psi\rangle\langle\psi|))) - |\varphi\rangle\langle\varphi|\| < \epsilon$$

$$\epsilon \xrightarrow{n \rightarrow \infty} 0$$

HOW TO FIND A GOOD \mathcal{E} ?

- USE ISOMETRY $\mathcal{E}(\cdot) = E \cdot E^\dagger$
- CHOOSE E USING UNITARILY INVARIANT MEASURE

• CHOOSE E USING UNITARILY INVARIANT MEASURE

• RATE ACHIEVED THIS WAY:

$\{b \in \mathcal{A}\}$

NO
SMOKING
PLEASE

• CHOOSE E USING UNITARILY INVARIANT MEASURE

• RATE ACHIEVED THIS WAY:

$$\frac{M}{n} \rightarrow$$

• RATE ACHIEVED THIS WAY:

$$\frac{m}{n} \rightarrow 1 - H(p) \quad H(p) = -\sum_i p_i \log p_i$$

• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

$$\frac{m}{n} \rightarrow 1 - H(p) \quad H(p) = -\sum_i p_i \log p_i$$

ANALYSIS BY RANDOM MATRICES.

{a,b}

}



• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

$$\frac{m}{n} \rightarrow 1 - H(p) \quad H(p) = -\sum_i p_i \log p_i$$

ANALYSIS BY RANDOM MATRICES.

$$L, M \cong (\mathbb{C}^2)^{\otimes m}$$

• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

$$\frac{M}{n} \rightarrow 1 - H(p) \quad H(p) = -\sum_i p_i \log p_i$$

ANALYSIS BY RANDOM MATRICES.

$$L, M \cong (\mathbb{C}^2)^{\otimes M}$$

$$|\Phi\rangle = \frac{1}{\sqrt{2^M}} \sum_{b \in \{0,1\}^M}$$

• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

$$\frac{m}{n} \rightarrow 1 - H(p) \quad H(p) = -\sum_i p_i \log p_i$$

ANALYSIS BY RANDOM MATRICES

$$\cong (\mathbb{C}^2)^{\otimes m}$$

$$|\Phi\rangle = \frac{1}{\sqrt{2^m}} \sum_{b \in \{0,1\}^m} |b^m\rangle_L \otimes |b^m\rangle_M$$



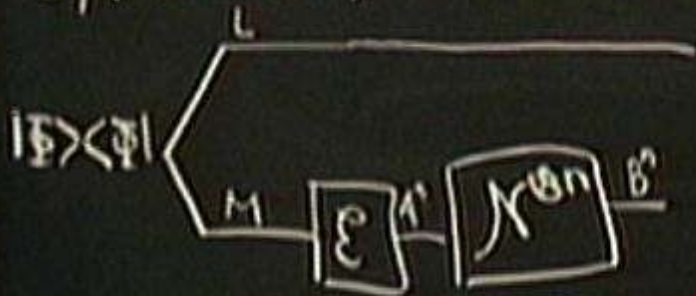
• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

$$\frac{M}{n} \rightarrow 1 - H(p) \quad H(p) = -\sum_i p_i \log p_i$$

ANALYSIS BY RANDOM MATRICES

$$L, M \cong (\mathbb{C}^2)^{\otimes n}$$

$$|\Phi\rangle_M = \frac{1}{\sqrt{2^m}} \sum_{b \in \{0,1\}^m} |b^m\rangle_L \otimes |b^m\rangle_M$$



• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

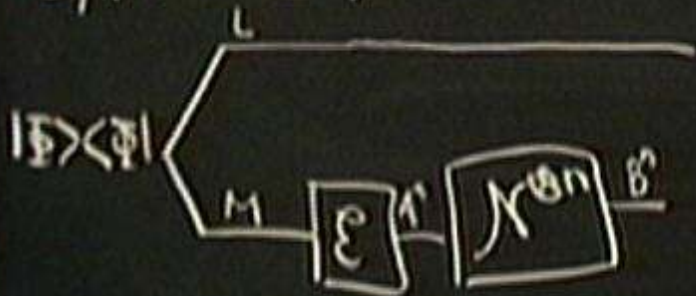
$$\frac{m}{n} \rightarrow 1 - H(p) \quad H(p) = -\sum_i p_i \log p_i$$

ANALYSIS BY RANDOM MATRICES

$$L, M \cong (\mathbb{C}^2)^{\otimes m}$$

$$|\Phi\rangle_{LM} = \frac{1}{\sqrt{2^m}} \sum_{b \in \{0,1\}^m} |b^m\rangle_L \otimes |b^m\rangle_M$$

NOTE: $\chi(p) = \text{tr}_C U_{X^m} P U_{X^m}^*$



$$U: A \rightarrow B \otimes C$$

• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

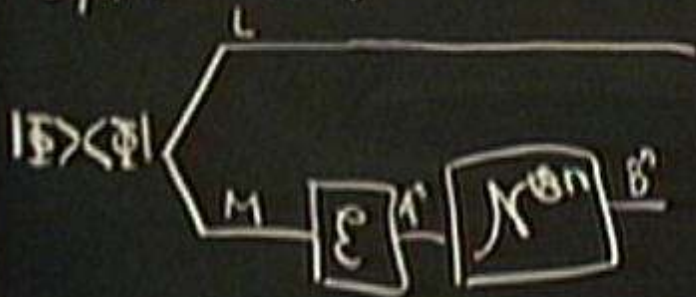
$$\frac{m}{n} \rightarrow 1 - H(p) \quad H(p) = -\sum_i p_i \log p_i$$

ANALYSIS BY RANDOM MATRICES

$$L, M \cong (\mathbb{C}^2)^{\otimes m}$$

$$|\Phi\rangle_{LM} = \frac{1}{\sqrt{2^m}} \sum_{b \in \{0,1\}^m} |b^m\rangle_L \otimes |b^m\rangle_M$$

NOTE: $\chi(p) = \text{tr}_C U_X P U_X^\dagger$



$$U \cdot \Lambda \rightarrow B \otimes C$$

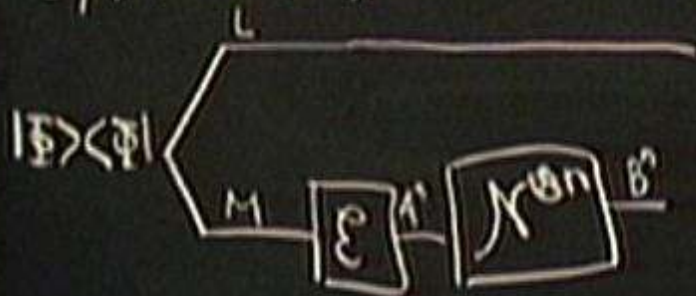
• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

$$\frac{m}{n} \rightarrow 1 - H(p) \quad H(p) = -\sum_i p_i \log p_i$$

ANALYSIS BY RANDOM MATRICES

$$L, M \cong (\mathbb{C}^2)^{\otimes m}$$

$$|\Phi\rangle_{LM} = \frac{1}{\sqrt{2^m}} \sum_{b \in \{0,1\}^m} |b^m\rangle_L \otimes |b^m\rangle_M$$



NOTE: $\chi(p) = \text{tr}_C U_{X^m} \rho U_{X^m}^*$

$$U_{X^m}: A \rightarrow B \otimes C \quad U_{X^m} |i\rangle = \sum_{j=0}^1 \sqrt{p_j} |i\rangle_B \otimes |j\rangle_C$$

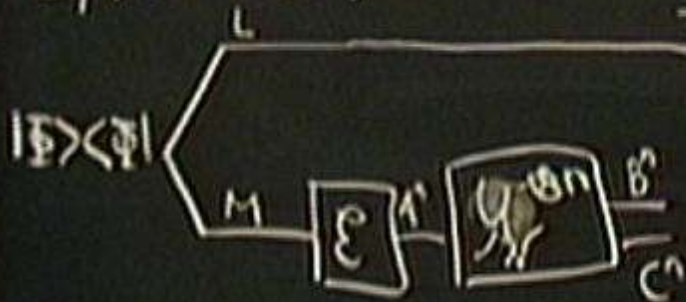
• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

$$\frac{M}{n} \rightarrow 1 - H(p) \quad H(p) = -\sum_i p_i \log p_i$$

ANALYSIS BY RANDOM MATRICES

$$L, M \cong (\mathbb{C}^2)^{\otimes m}$$

$$|\Phi\rangle_m = \frac{1}{\sqrt{2^m}} \sum_{b \in \{0,1\}^m} |b^m\rangle \otimes |b^m\rangle$$



NOTE: $\chi(p) = \sum_{i=0}^n \sqrt{p_i}$

$$\|p - 6\| \leftarrow \text{transformation}$$

GLB/Cⁿ
EXISTENCE OF D

$$\|p - \sigma\|_{L^1(\mathbb{R}^n)}$$

$$G_{LB^*C^n}$$

EXISTENCE OF \mathcal{D} : DEPENDS ON $\sigma_{LC^n} := \text{tr}_{B^n} G_{LB^*C^n}$

$$\|p - \hat{p}\|_1 \leq \text{trace}(m^2)$$

$$G_{LB^*C^n}$$

EXISTENCE OF \mathcal{D} : DEPENDS ON $\sigma_{LC^n} := \text{tr}_{B^n} G_{LB^*C^n}$

ROUGH ESTIMATE: $\text{tr}[(G_{LC^n})^2]$