d) Asymptotic protocols

Single-copy conversion: not reversible,

→ at least two numbers to quantify ent.:

\# ebits needed to build state

\# extractable ebits.

Can we do better w/ more copies?

$$|\chi\rangle^{\otimes 2} = \left(\sqrt{\tfrac{2}{3}}\,|00\rangle + \sqrt{\tfrac{1}{3}}\,|11\rangle\right)^{\otimes 2} \longleftrightarrow |\phi^+\rangle^{\otimes ?}$$

$|\phi^+\rangle^{\otimes 2} \to |\chi\rangle^{\otimes 2}$:

$$\left(\tfrac{4}{9}, \tfrac{2}{9}, \tfrac{2}{9}, \tfrac{1}{9}\right) \succ \left(\tfrac{1}{4}, \tfrac{1}{4}, \tfrac{1}{4}, \tfrac{1}{4}\right)$$

$p=1$ & best possible as Schmidt rank cannot be increased by POVM.

$|\chi\rangle^{\otimes 2} \to |\phi^+\rangle^{\otimes ?}$.

$$\left(\tfrac{4}{9}, \tfrac{2}{9}, \tfrac{2}{9}, \tfrac{1}{9}\right) \prec \underbrace{p\left(\tfrac{1}{4}, \tfrac{1}{4}, \tfrac{1}{4}, \tfrac{1}{4}\right) + q\left(\tfrac{1}{2}, \tfrac{1}{2}, 0, 0\right) + (1-p-q)(1,0,0,0)}$$

Optimum: $p = \tfrac{2}{3}$, $q = \tfrac{1}{9}$:

$$\downarrow$$

$$\left(\tfrac{4}{9}, \tfrac{2}{9}, \tfrac{1}{6}, \tfrac{1}{6}\right).$$

$\left.\begin{array}{l} p = \frac{2}{3} : 2 \text{ ebits} \\ q = \frac{1}{9} : 1 \text{ ebit} \end{array}\right\}$ avg. yield <u>per copy</u> of $|\chi\rangle$:

$$\frac{2 \times \frac{2}{3} + 1 \times \frac{1}{9}}{2} = \frac{2}{3} + \frac{1}{18} > \frac{2}{3} \ !$$

$\Rightarrow$ Improved yield as compared to 1-copy protocol!

How good can we get by using $N \to \infty$ copies?

<u>Requirements</u> for <u>asymptotic protocols</u>:

$\to$ convert $|\phi^+\rangle^{\otimes m} \longleftrightarrow |\chi\rangle^{\otimes n}$ with

<u>rate</u> $\frac{n}{m} \to R > 0$ for $n, m \to \infty$

$\to$ success prob. $p \to 1$ for $n \to \infty$

$\to$ Conversion need not be perfect: sufficient if distance from correct state $\delta \to 0$ as $n \to \infty$.

<u>How to measure error δ?</u>

Use $\delta = 1 - F$ ~ "fidelity" $F = |\langle\psi|\phi\rangle|^2$

δ bounds error on <u>any</u> observable O:

$$|\langle\psi|O|\psi\rangle - \langle\phi|O|\phi\rangle| \leq 2\sqrt{\delta}\, \|O\|_\infty \qquad (\to \text{Homework})$$

i.e.: $\delta \to 0 \Rightarrow$ states indistinguishable by <u>any</u> measurement!

Now consider $|\chi\rangle = \sum \sqrt{p(x)}\,|x\rangle_A |x\rangle_B\,,\ x=1,\dots,d$

$$|\chi\rangle^{\otimes n} = \sum_{x_1 - x_n} \sqrt{p(x_1)\cdots p(x_n)}\ |x_1,\dots,x_n\rangle|x_1,\dots,x_n\rangle$$

sequence $x_1,\dots,x_n$ are indep. & identically distributed (i.i.d.) random variables w/ prob. $p(x_i)$

<u>Law of large numbers (L.L.N.)</u>

$$\forall\varepsilon>0\ \ \forall\delta>0\ \ \exists N\ \ \forall n\geq N\ \ p\left(\left|\frac{1}{n}\sum_{i=1}^{n} x_i - E(X)\right| \geq \varepsilon\right) \leq \delta$$

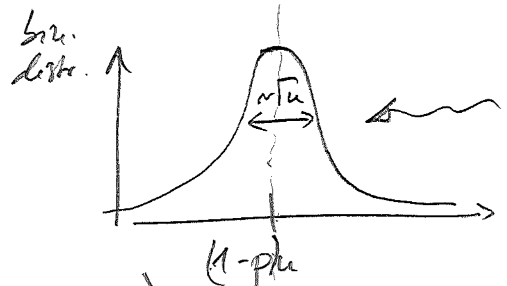
with $E(X) = \sum_x p(x)\,x$.

(i.e., $p(|\dots| \geq \varepsilon) \to 0\ \ \forall\varepsilon$)

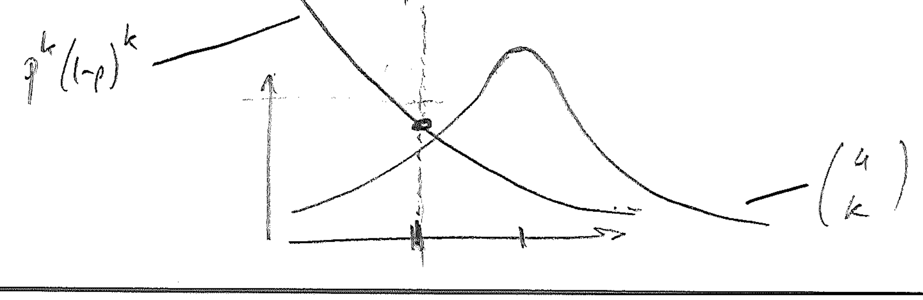
What is the <u>typical output</u> of an i.i.d. source?

<u>E.g.:</u> $x=0,1$; $P_0 \equiv p$; $P_1 = 1-p$.

$\rightarrow$ Binomial distr. $p^k(1-p)^{n-k}\binom{n}{k}$.



$\leftarrow$ <u>rel.</u> width $\rightarrow 0$ as $n\to\infty$ (L.L.N.)



Typ. output: expect output x $\; n \cdot p(x)$ times.

$$\Rightarrow \quad p(x_1, \dots, x_n) = p(x_1) \cdot \ldots \cdot p(x_n) \approx p(1)^{np(1)} \cdot \ldots \cdot p(d)^{np(d)}$$

base 2

$$\Rightarrow \quad -\log p(x_1, \dots, x_n) \approx n \cdot \underbrace{\left(-\sum_x p(x) \log p(x) \right)}_{=:\, H(p)}$$

$=: H(p)$ Shannon entropy of p.

$\Rightarrow$ expect typically $p(x_1, \dots, x_n) \approx 2^{-nH(p)}$,

and there are about $2^{nH(p)}$ such typical sequences.

More precisely:

Def.: We say that $x_1, \dots, x_n$ is a ε-typical sequence if

$$2^{-n(H(p)+\varepsilon)} \leq p(x_1, \dots, x_n) \leq 2^{-n(H(p)+\varepsilon)}$$

Denote the set of ε-typ. seq. by $T(n, \varepsilon)$.

Theorem:

1. $\forall \varepsilon > 0 \; \forall \delta > 0 \; \exists N \; \forall n \geq N$: a random sequence of len. n is ε-typical w/ prob. $\geq 1 - \delta$.

2. $\forall \varepsilon > 0 \; \forall \delta > 0 \; \exists N \; \forall n \geq N$:

$$(1-\delta)\, 2^{n(H(p)-\varepsilon)} \leq |T(n, \varepsilon)| \leq 2^{n(H(x)+\varepsilon)}$$

Proof:

1. $-\log p(x_i)$ is i.i.d. variable.

L.L.N. $\Rightarrow \forall \varepsilon, \delta\ \exists N\ \forall n \geq N\ \ p\Big(\Big|\underbrace{\frac{1}{n}\sum_{i=1}^{n} -\log p(x_i)}_{= -\log p(x_1,\dots,x_n)} - \underbrace{E(-\log p(x))}_{= H(p)}\Big| \geq \varepsilon\Big) \leq \delta$

$\Rightarrow\ \ p\left(\left|-\frac{1}{n}\log p(x_1,\dots,x_n) - H(p)\right| \geq \varepsilon\right) \leq \delta$

$\Rightarrow$ w prob. $\geq 1-\delta$, $\ -n(H(p)+\varepsilon) \leq \log p(x_1,\dots,x_n) \leq -n(H(p)-\varepsilon)$

$\boxtimes$

2. $1 \geq \sum_{x_1 \dots x_n \in T(n,\varepsilon)} p(x_1,\dots,x_n) \geq \sum_{T(n,\varepsilon)} 2^{-n(H(p)+\varepsilon)} = |T(n,\varepsilon)| \cdot 2^{-n(H(p)+\varepsilon)}$

$1-\delta \leq \sum_{T(n,\varepsilon)} p(x_1,\dots,x_n) \leq |T(n,\varepsilon)|\ 2^{-n(H(p)-\varepsilon)}$

$\boxtimes$

<u>In brief</u>: ε-Typ. sequence $\Leftrightarrow$ $\frac{\log p(x_1,\dots,x_n)}{n}$ ε-close to $H(p)$.

Asympt., a sequence is <u>ε-typical w/ $p \to 1$</u>,

and there are <u>$\sim 2^{nH(p)}$ ε-typ. seq.</u>.

Application to ent conversion:

$$|\chi\rangle = \sum_x \sqrt{p(x)}\, |x\rangle_A |x_B\rangle$$

$$\Rightarrow \quad |\chi\rangle^{\otimes n} = \sum \sqrt{p(x_1)\cdots p(x_n)}\, |x_1,\dots,x_n\rangle |x_1,\dots,x_n\rangle$$

Fix $\varepsilon > 0$.

Define $$|\vartheta_n\rangle := \sum_{x_1,\dots,x_n \in T(n,\varepsilon)} \sqrt{p(x_1)\cdots p(x_n)}\, |x_1,\dots,x_n\rangle |x_1,\dots,x_n\rangle$$

and $$|\hat{\vartheta}_n\rangle := \frac{|\vartheta_n\rangle}{\sqrt{\langle\vartheta_n|\vartheta_n\rangle}}$$

We have

$$\langle\hat{\vartheta}_n|\chi^{\otimes n}\rangle = \frac{\overbrace{\sum_{\varepsilon\text{-typ.}} p(x_1,\dots,x_n)}^{\geq 1-\delta \text{ for suff. large } n}}{\sqrt{\sum_{\varepsilon\text{-typ.}} p(x_1,\dots,x_n)}} \xrightarrow{n\to\infty} 1$$

and $\left|T(n,\varepsilon)\right| \leq 2^{n(H(p)+\varepsilon)}$ for n large enough.

Protocol: A prepares $|\hat{\vartheta}_n\rangle$ locally & teleports Bob's part to Bob. $\Rightarrow$ uses $m = \log|T(n,\varepsilon)| = n(H(p)+\varepsilon)$ ebits.

$$\Rightarrow \quad \frac{m}{n} \longrightarrow H(p)+\varepsilon \quad \text{"entanglement dilution rate".}$$

Can be realized for any $\varepsilon > 0 \Rightarrow$ asymptotic rate $H(p)$.

Conversely: Distill ebits from $|\chi\rangle^{\otimes n}$:

- Use $|\hat{\vartheta}_n\rangle$ instead since fidelity $\to 1$.
- $|\vartheta_n\rangle$: max. Schmidt coeff. $2^{-n(H(p)-\varepsilon)}$

$\Rightarrow$ $|\hat{\vartheta}_n\rangle$: max. Schmidt coeff. $\frac{1}{1-\delta}\, 2^{-n(H(p)-\varepsilon)}$

Choose m s.th. $\frac{2^{-n(H(p)-\varepsilon)}}{1-\delta} \leq 2^{-m}$

$\Rightarrow$ $(2^{-m}, 2^{-m}, \dots) \succ$ (Schmidt coeffs. of $|\hat{\vartheta}_n\rangle$)

$\Rightarrow$ can convert $|\hat{\vartheta}_n\rangle$ to m ebits by LOCC.

Protocol: (1) A projects onto ε-typ. subspace $\to |\hat{\vartheta}_n\rangle$

(i.e.: POVM $\{ M_0 = \Pi_{\varepsilon\text{-typ}};\ M_1 = 1 - \Pi_0 \}$)

| success prob. $1-\delta \to 1$

(2) A & B convert $|\hat{\vartheta}_n\rangle$ to m ebits.

$\to$ works for any $m \leq n(H(p)-\varepsilon) - \log(1-\delta)$

$\Rightarrow$ Rate $\frac{m}{n} \to H(p) - \varepsilon \ \forall \varepsilon$

$\Rightarrow$ asymptotic "entanglement distillation rate" $H(p)$.

Asymptotically:

Distillation rate = Dilution rate $= H(p)$.

Optimal? — Yes. Otherwise we could use protocol to increase # of Bell pairs by going in circles.

Remark: Instead of $H(p)$, we typ. use the von Neumann entropy $S(\rho) = -\mathrm{tr}(\rho \log \rho)$, i.e.,

$$H(p) = S(\mathrm{tr}_B |\psi\rangle\langle\psi|) = S(\mathrm{tr}_A |\psi\rangle\langle\psi|).$$

Protocol allows us to convert between any two states $|\psi\rangle^{\otimes n}$ and $|\phi\rangle^{\otimes m}$, provided $n S(\mathrm{tr}_B |\psi\rangle\langle\psi|) = m S(\mathrm{tr}_B |\phi\rangle\langle\phi|)$. (by going via max. ent. states).

Result: The entropy of entanglement

$$E(|\psi\rangle) = S(\mathrm{tr}_A |\psi\rangle\langle\psi|) = S(\mathrm{tr}_B |\psi\rangle\langle\psi|)$$

uniquely quantifies the amount of entanglement in a pure bipartite state.