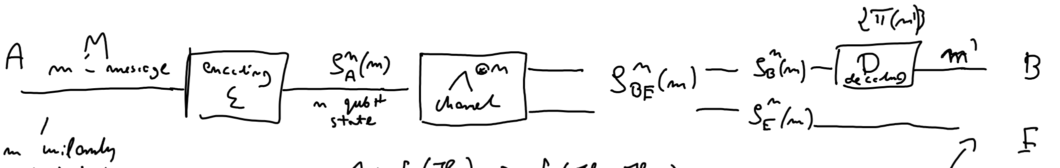
13 - Devetak-Winter

12 grudnia 2010
15:02

We look for a quantum version of Csiszar-Körner theorem this will (finally) allow us to analyze security against collective (unfortunately not coherent) attacks



$\Lambda : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B \otimes \mathcal{H}_E)$

$(\forall_m \ \varrho_E(m) \approx \varrho_E)$

code $[|M|, n]$

<u>Def</u> R is achievable rate of secret communication via channel Λ iff there exists sequence of codes $[2^{nR}, n]$ for which

$$p_e = \max_m \left(1 - \mathrm{Tr}\, \Pi(m)\, \varrho_B^n(m)\right) \xrightarrow{n\to\infty} 0$$

prob of error

and $\chi(\{\varrho_E(m)\}) = S\left(\frac{1}{2^{nR}}\sum_m \varrho_E(m)\right) - \frac{1}{2^{nR}}\sum_m S(\varrho_E(m)) \to 0$

Holevo quantity

<u>Def:</u> C_s is the highest R

<u>Theorem</u> (Devetak, Winter, Cai, Yeung, 2004)

$$C_s \geq \max_{p,\varrho_A} \left(\chi_{AB} - \chi_{AE}\right)$$

$A \to B$

$\varrho_A^x \to \mathrm{Tr}_E\, \Lambda(\varrho_A^x) = \varrho_B^x$

$A \to E$

$\varrho_A^x \to \mathrm{Tr}_B\, \Lambda(\varrho_A^x) = \varrho_E^x$

$$\chi_{AB} = S\left(\sum_x p_x \varrho_B^x\right) - \sum_x p_x S(\varrho_B^x)$$

$$\chi_{AE} = S\left(\sum_x p_x \varrho_E^x\right) - \sum_x p_x S(\varrho_E^x)$$

Unfortunately unlike in classical case there is no single letter upper bound

<u>Proof</u>

we will present explicit construction achieving rate $\chi_{AB} - \chi_{AE}$.

s we construct the code

$$|M| = 2^{nR} \quad M \xrightarrow{\text{privacy amplification}} (J, M) \xrightarrow{\text{coding}} \varrho_A^n \to (\varrho_B^n, \varrho_E^n)$$

J - uniformly distributed random variable $j = 1 \ldots |J|$

$$m \xrightarrow{\mathcal{E}} \varrho_A^n(j, m)$$

coarser structure (j) — finer structure (m)

Our code: we generate $|J| \cdot |M|$ random states $\varrho_1 \otimes \ldots \otimes \varrho_n$ where each ρ_i is chosen randomly from a set $\{S_x\}$ with probabilities p_x

From HSW theorem we know we can take $|J|\cdot|M| = 2^{n(\chi_{AB} - \varepsilon)}$ to have errorfree communication. We take $|J| = 2^{n(\chi_{AE} - \varepsilon)}$ so we will have $|M| = 2^{n(\chi_{AB} - \chi_{AE})}$.

We need to show that $\chi(\{\rho_E^n(m)\}) \to 0$

$$\rho_E^n(m) = \frac{1}{|J|}\sum_j \rho_E^n(j,m) = \frac{1}{|J|}\sum_j \mathrm{Tr}_B \Lambda(\rho_A^n(j,m))$$

Now we need a lemma which would be „law of large numbers" for operators:

L.1 Quantum Chernoff bound (Ahlswede, Winter 2000)

X_i - random variables with values in operators on d dimensional Hilbert space

$$0 \le X_i \le \mathbb{1}$$

$$\Pr\left[\frac{1}{M}\sum_i^M X_i \notin [(1-\eta)\langle x\rangle, (1+\eta)\langle x\rangle]\right] \le 2d\, e^{-\frac{M\alpha\eta^2}{2\ln 2}}$$

there seem to be a mistake in original paper factor „$2\ln 2$" is not correct, seems one should take „3" instead

where $\langle x\rangle = E(X_i)$,

and α is such that $\langle x\rangle \ge \alpha\cdot\mathbb{1}$

Probability that mean on the sample differs from the true mean by η goes exponentially down with increasing number of samples m

Classically the same, just put $d=1$

L.2 „Tender operator"

Let ρ be a state and $X \le \mathbb{1}$ a positive operator such that $\mathrm{Tr}(\rho X) \ge 1-\varepsilon$ then

$$\|\rho - \sqrt{X}\rho\sqrt{X}\|_1 \le \sqrt{8\varepsilon}$$

Proof:

$$\|\ldots\|_1^2 = \mathrm{Tr}(|\rho - \sqrt{X}\rho\sqrt{X}|)^2 = \qquad Y = \sqrt{X}, \quad \rho = \sum p_i \Pi_i$$

projection on eigenstates (1D)

$$= \mathrm{Tr}\left(\left|\sum_i p_i(\Pi_i - Y\Pi_i Y)\right|\right)^2 \le \sum_i p_i \mathrm{Tr}(|\Pi_i - Y\Pi_i Y|)^2$$

$$\left(\mathrm{Tr}(\sqrt{A^\dagger A})\right)^2 \le \mathrm{rank}(A^\dagger A)\cdot \mathrm{Tr}(A^\dagger A)$$

$$\left(\sum_{i=1}^m \lambda_i\right)^2 \le m\left(\sum_{i=1}^m \lambda_i^2\right)$$

arithmetic mean $\le$ quadratic mean

In our case $A = \Pi_i - Y\Pi_i Y$ rank $A^\dagger A \le 4$

$$\le 4\sum_i p_i \mathrm{Tr}(\Pi_i + Y\Pi_i Y^2 \Pi_i Y - 2\Pi_i Y \Pi_i Y)$$

$$\mathrm{Tr}(\Pi_i Y^2 \Pi_i Y^2) \le \mathrm{Tr}(\Pi_i Y \Pi_i Y)$$

$)$

$\leq 4 \left(1 - \sum_i p_i \, \mathrm{Tr}(\Pi_i Y \Pi_i Y) \right)$

$\Big\} \quad 1 - x^2 \leq 2(1-x)$

$\leq 8 \left(1 - \sum_i \mathrm{Tr}\, \Pi_i Y \right) \leq 8 \left(1 - \sum_i \mathrm{Tr}\, \Pi_i X \right) \leq 8 \varepsilon$ ∎

Lemma 3

Let $x \to \rho_x$ be $c \to q$ channel, $\rho = \sum_x p_x \rho_x$, $\rho_x \in \mathcal{L}(\mathcal{H})$, $\dim \mathcal{H} = d$

Let T_n^ε be set of typical sequences x^n,

$$\rho^n = \frac{1}{|T_n^\varepsilon|} \sum_{x^n \in T_n^\varepsilon} \underset{\rho_{x_1} \otimes \dots \otimes x_n}{\underset{\shortparallel}{\rho_{x^n}}}$$

And ρ_i^n be randomly chosen ρ_{x^n} with $x^n \in T_n^\varepsilon$ (uniform distribution on typical sets)

$$\Pr\left[\left| \frac{1}{M} \sum_i^M \rho_i^n - \rho^n \right|_1 \geq \varepsilon \right] \leq 2 \cdot 2^{n(S(\rho)+\delta)} e^{- \frac{M 2^{-n(\chi(\{\rho_x\})+\delta)} \left(\frac{\varepsilon}{5d}\right)^2}{2 \ln 2}}$$

this factor is not really important

which shows it is enough to take $M \geq 2^{(\chi(\rho_x)+\delta)\cdot n}$ to have a mean of the sample close to the mean operator

Proof:

$\rho_x = \sum_k \lambda_x^k |e_k^x\rangle\langle e_k^x|$ $\qquad \rho_i^n = \sum_{\{k\}} \underbrace{\lambda_{i_1}^{k_1} \cdots \lambda_{i_n}^{k_n}}_{\lambda_i^{\{k\}}} |e_{k_1}^{i_1}\rangle\langle e_{k_1}^{i_1}| \otimes \dots \otimes |e_{k_n}^{i_n}\rangle\langle e_{k_n}^{i_n}|$

$|e_{\{k\}}^i\rangle = |e_{k_1}^{i_1}\rangle \otimes \dots \otimes |e_{k_n}^{i_n}\rangle$

Define: $P^i = \sum_{\{k\} \in T_k^i} |e_{\{k\}}^i\rangle\langle e_{\{k\}}^i|$ where T_k^i is a set of sequences $\{k\}$ for which

$$\left| -\frac{1}{n} \log\left(\lambda_i^{\{k\}}\right) - \bar{S} \right| < \delta, \text{ where}$$

$\bar{S} = \sum_x p_x S(\rho_x)$

Now let $\rho = \sum_x p_x \rho_x = \sum_k \lambda_k |e_k\rangle\langle e_k|$ and define

$P = \sum_{\{k\} \in T_k} |e_{\{k\}}\rangle\langle e_{\{k\}}|$, where T_k is a set of sequences $\{k\}$ such that:

$$\left| -\frac{1}{n} \log(\lambda_{\{k\}}) - S \right| < \delta \quad \text{where}$$

$S = S(\rho)$

Let us define:

$\tilde{\rho}_i^m = P P^i \rho_i^m P^i P$, we know that $\tilde{\rho}_i^m \leq 1\!\!1\, 2^{-m(\bar{S}-\delta)}$
and that it is supported on $\leq 2^{m(S+\delta)}$ dimensional space

Let $\tilde{\rho}^m = \frac{1}{|T_m^\epsilon|}\sum_{x^m \in T_m^\epsilon} \tilde{\rho}_{x^m}$ $\quad \tilde{\rho}^m = \sum_k \lambda_k |\rho_k\rangle\langle\rho_k|$ - eigendecomposition

Let $\tilde{\Pi} = \sum_{k \in \tilde{T}} |\rho_k\rangle\langle\rho_k|$ where $\tilde{T}$ contains these k for which
$\left|-\frac{1}{m}\log\lambda_k - S(\rho)\right| \leq \delta$

Now we are sure that $\tilde{\Pi}\tilde{\rho}_i^m\tilde{\Pi} \leq 1\!\!1\cdot 2^{-m(\bar{S}-\delta)}$ and $\tilde{\Pi}\tilde{\rho}^m\tilde{\Pi} \geq 2^{-m(S+\delta)}1\!\!1$
We can define:
$$\hat{\rho}_i^m = \tilde{\Pi}\tilde{\rho}_i^m\tilde{\Pi}\, 2^{m(\bar{S}-\delta)} \quad \text{and} \quad \hat{\rho}^m = 2^{m(\bar{S}-\delta)}\cdot\tilde{\Pi}\tilde{\rho}^m\tilde{\Pi}$$
and apply Lema 1 to them:
$$\Pr\left[\frac{1}{M}\sum_j \hat{\rho}_i^m \notin \left[(1\pm\varepsilon)\hat{\rho}^m\right]\right] \leq 2\cdot 2^{m(S+\delta)} e^{-\frac{M\cdot 2^{-m(S-\bar{S}+2\delta)}\varepsilon^2}{2\ln 2}}$$

if $\frac{1}{M}\sum_j \hat{\rho}_i^m \in [(1\pm\varepsilon)\hat{\rho}^m]$ then this implies
$$\left|\frac{1}{M}\sum_i \hat{\rho}_i^m - \hat{\rho}^m\right|_1 \leq \varepsilon 2^{m(\bar{S}-\delta)} \Rightarrow \left|\frac{1}{M}\sum_i \tilde{\Pi}\tilde{\rho}_i^m\tilde{\Pi} - \tilde{\Pi}\tilde{\rho}^m\tilde{\Pi}\right|_1 \leq \varepsilon.$$

We know that for m large enough $\mathrm{Tr}(\tilde{\rho}^m\tilde{\Pi}) \geq 1-\frac{\varepsilon^2}{8}$
which means $|\tilde{\rho}^m - \tilde{\Pi}\tilde{\rho}^m\tilde{\Pi}|_1 \leq \varepsilon$ by tender measurement, so by
triangle: $\left|\frac{1}{M}\sum_i \tilde{\Pi}\tilde{\rho}_i^m\tilde{\Pi} - \tilde{\rho}^m\right| \leq 2\varepsilon$
Analogously $\mathrm{Tr}\left(\tilde{\Pi}\,\frac{1}{M}\sum_i \tilde{\rho}_i^m\right) \geq 1-\frac{\varepsilon^2}{8}$ so
$\left|\frac{1}{M}\sum_i \tilde{\rho}_i^m - \tilde{\rho}^m\right|_1 \leq 3\varepsilon$ and again to get rid of "~"
$\left|\frac{1}{M}\sum_i \rho_i^m - \rho^m\right| \leq 5\varepsilon$

So we see that if we take $|J| > 2^{m\chi(\{\rho_x\})}$ we will
have $\rho_E^m(m) = \frac{1}{|J|}\sum_j \rho_E^m(j,m) \approx \rho_E^{\otimes m}$ in the sense of $|\ |_1$ norm

What remains to be shown is that this implies that
$S(\rho_E^m(m)) \approx S(\rho_E^{\otimes m})$ this assumes

Fannes inequality

Let ρ, σ be two density matrices on d dimensional space
Such that $|\rho - \sigma|_1 \leq \eta \leq \frac{1}{e}$
$$|S(\rho) - S(\sigma)| \leq \eta\log d - \eta\log\eta$$

In our case this means
$S(\rho_E^m(m)) - S(\rho_E^{\otimes m}) \leq \varepsilon\cdot m\bar{S}$ but we can always take
$\varepsilon \sim e^{-\Theta m\delta^2}$ for some constant Θ, for m large enough

$\varepsilon \sim e^{-\Theta n \delta^2}$ for some constant Θ, for n large enough
since all "typical" properties have this characteristic error tails.
So we can indeed make $\chi(\{\varrho^n_E(m)\}) \to 0$ ∎

Encoding vs Postprocessing

Similarly as in classical Csiszar-Körner we can look equivalently at a situation of extracting secret key from CQQ correlations (classically we had CCC correlation)

There is a CQQ state:

$$\varrho_{ABE} = \sum_x p_x |x\rangle\langle x| \otimes \varrho^x_{BE} \quad \text{and } ABE$$

share $\varrho_{ABE}^{\otimes n}$, A bits are in X^n while B and E perform measurements to learn X^n, after that A sends error-correction information publicly and A & B introduce some randomness. In effect, number of secret bits is equal to:

$$K = n \cdot (\chi_{AB} - \chi_{AE})$$