Large deviation type evaluation in information theoretic security

arXiv:1202.0322, etc

& new results

Masahito Hayashi

Graduate School of Mathematics, Nagoya University

Centre for Quantum Technologies, National University of Singapore

Two streams for finite-length problem

1. Constant error constraint
   - One-shot setting
   - Information spectrum
     - Asymptotic theory for general information sources
     - Classical case (Han, Verdu)
     - Quantum case (Nagaoka MH)
   - Second order analysis (Strassen, Polyanskiy etal, MH)
   - It can be extend to Markovian case (MH)
2. Constraint for decreasing rate
   - Error exponent (Gallager etc)
   - The case when we focus on too small error probability.
   - It can be extend to Markovian case

Relation between information spectrum and one-shot setting

A) Information spectrum (IS)
- Asymptotic setting (It cannot be directly applied to real case.)
- Equality (Direct and Converse parts) is required
- Requirement and formulation are rigorous.
- Many results has been essentially obtained via one-shot result. (Many papers concerning IS contain one-shot result.)

B) One-shot setting (OS)
- Non asymptotic setting (It can be directly applied to real case.)
- Only inequality is obtained and required.
- How to guarantee tightness?
- It is better to require that the bound can yield first and/or second order asymptotics in the iid case.
- Is the obtained bound computable?

My contributions for stream 1

1. Nagaoka & MH, “An Information-Spectrum Approach to Classical and Quantum Hypothesis Testing for Simple Hypotheses” *IEEE IT* (2007)
2. MH “Optimal sequence of quantum measurements in the sense of Stein's lemma in quantum hypothesis testing” JPA (2002)
3. MH & Nagaoka “General formulas for capacity of classical-quantum channels” *IEEE IT* (2003)
4. MH “General formulas for fixed-length quantum entanglement concentration” *IEEE IT* (2006)
5. MH *Quantum Information: An Introduction*, Springer (2006); Japanese version in 2004.
6. MH “General non-asymptotic and asymptotic formulas in channel resolvability and identification capacity and its application to wire-tap channel” *IEEE IT* (2006)
7. MH “Second-Order Asymptotics in Fixed-Length Source Coding and Intrinsic Randomness” *IEEE IT* (2008)
8. MH “Error exponent in asymmetric quantum hypothesis testing and its application to classical-quantum channel coding” *PRA* (2007)
9. MH “Information Spectrum Approach to Second-Order Coding Rate in Channel Coding” *IEEE IT* (2009)
10. Tomamichel & MH “A Hierarchy of Information Quantities for Finite Block Length Analysis of Quantum Tasks”arXiv:1208.1478.

Quantum Information: An Introduction, Springer (2006); Japanese version in 2004

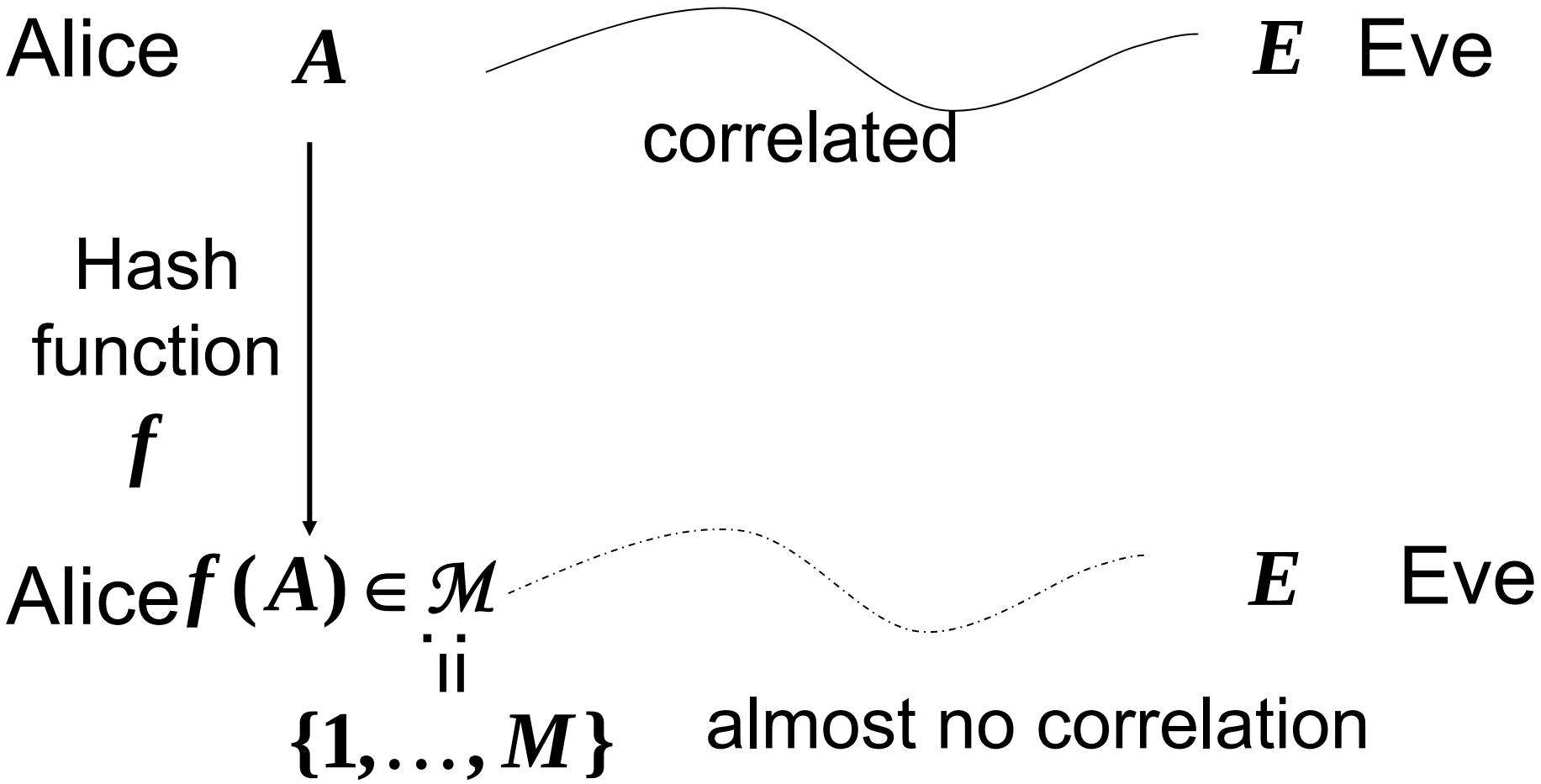
1. "Quantum" Translation of T. S. Han, *Information-Spectrum Methods in Information Theory,* (Springer, Berlin Heidelberg New York, 2002) (Japanese version in 1998).
2. ***Nagaoka's dream*** "Many things can be understood with hypothesis testing via information spectrum"(1999).
   - Ogawa & Nagaoka, "Making good codes for classical-quantum channel coding via quantum hypothesis testing", *IEEE IT* (2007). (Main part in 1999)
   - M. Hayashi "Hypothesis testing approach to quantum information theory," *COE Symposium on Quantum Information Theory (Satellite-workshop of EQIS2003)*, Kyoto, pp.15-16 (2003).
3. The following topics are treated with a one-shot bound via hypothesis testing or a test $\{\rho - a\sigma > 0\}$.
   - c-q channel coding, q-source coding
   - entanglement concentration (pure), entanglement dilution (pure)
   - entanglement distillation (mixed, converse)
   - channel resolvability (direct), wire-tap channel coding (direct)
   - reverse Shannon theorem (classical, direct)

Contents

- Classical case
  - Renyi entropy
  - Analysis with modified mutual information
  - Analysis with universal composability
    - Without leaked information
    - With leaked information
  - Numerical comparison with information spectrum approach (constant constraint approach)
  - Extension to Markovian case
- Quantum case
  - Renyi entropy and conditional Renyi entropy
  - Analysis with universal composability with leaked information
  - Extension to Markovian case

Security in Classical case

Leaked quantum information



Ensemble of Hash functions

For simplicity of analysis, we employ ensemble of Hash functions instead of a single hash function.

$$f_X : \mathcal{A} \rightarrow \{1, \ldots, M\}$$

X :Random variable deciding Hash function

Universal2 Condition

$$\Pr\{ f_X(a_1) = f_X(a_2)\} \leq \frac{1}{M} \qquad \forall a_1 \neq \forall a_2 \in \mathcal{A}$$

Example : Toeplitz Matrix

$\boldsymbol{A_X}$: m × n Matrix with n-1 elements $\boldsymbol{X = (a_1, \cdots, a_{n-1}) \in \mathbb{F}_2^{n-1}}$

$$\boldsymbol{A_X : \mathbb{F}_2^n \to \mathbb{F}_2^m}$$

$$\boldsymbol{A_X} := \begin{pmatrix} a_m & a_{m+1} & \cdots & a_{n-2} & a_{n-1} & 1 & & \\ a_{m-1} & a_m & \cdots & a_{n-3} & a_{n-2} & & 1 & \\ \vdots & \vdots & \ddots & \vdots & \vdots & & & \ddots \\ a_2 & a_3 & \cdots & a_{n-m} & a_{n-m+1} & 0 & & 1 \\ a_1 & a_2 & \cdots & a_{n-m-1} & a_{n-m} & & & 1 \end{pmatrix}$$

$\boldsymbol{\{A_X\}}$ is universal2 hash functions

This method requires small amount of calculation.

Entropy

$P^{AE}(a,e)$:joint distribution

$$H(A,E \mid P) := \sum_{a,e} -P^{AE}(a,e) \log P^{AE}(a,e)$$

$$H(E \mid P) := \sum_{e} -P^{E}(e) \log P^{E}(e)$$

Conditional entropy

$$H(A \mid E \mid P) := \sum_{e} P^{E}(e) H(A \mid P^{A|E=e})$$

$$= H(A,E \mid P) - H(E \mid P)$$

Mutual information

$$I(A:E) = H(E) + H(A) - H(A,E)$$

$$= H(A) - H(A \mid E) = D(P^{AE} \| P^{A} \times P^{E})$$

$$D(P \| Q) := \sum_{x} P(x)(\log P(x) - \log Q(x))$$

Security criterion

$P^{AE}(a,e)$:joint distribution

(1) Universal composability

$$d_1'(A \mid E \mid P) := \left\| P^{AE} - P_U^A \times P^E \right\|_1$$

$$\left\| P^{f_X(A),E,X} - P_U^{f_X(A)} \times P^{E,X} \right\|_1$$

$$= E_X \left\| P^{f_X(A),E} - P_U^{f_X(A)} \times P^E \right\|_1$$

P_U^A :Uniform distribution on $\mathcal{A}$

(2) Modified mutual information

$$I'(A:E) := D(P^{AE} \| P_U^A \times P^E)$$
$$= D(P^{AE} \| P^A \times P^E) + D(P^A \| P_U^A)$$
$$\geq d_1'(A|E|P)^2$$

$$I'(f_X(A):E,X) = E_X I'(f_X(A):E)$$

$$D(P\|Q) := \sum_x P(x)(\log P(x) - \log Q(x))$$

Renyi Entropies and Min entropies

$$H_{1+s}(A \mid P) := \frac{-1}{s} \log \sum_a P^A(a)^{1+s}$$

$$H_{\min}(A \mid P) := -\log \max_a P^A(a)$$

$$H_{1+s}(A \mid E \mid P) := \frac{-1}{s} \log \sum_{a,e} P^E(e) P^{A|E}(a \mid e)^{1+s}$$

$$H_{\min}(A \mid E \mid P) := -\log \max_{a,e} P^{A|E}(a \mid e)$$

Monotone decreasing for s

$$\lim_{s \to 0} H_{1+s}(A \mid E \mid P) = H(A \mid E \mid P)$$

$$H(A \mid E \mid P) \geq H_{1+s}(A \mid E \mid P) \geq H_{\min}(A \mid E \mid P) \qquad s > 0$$

Additivity properties

$$H(A \mid P^n) = nH(A \mid P)$$

$$H_{1+s}(A \mid P^n) = nH_{1+s}(A \mid P)$$

$$H_{\min}(A \mid P^n) = nH_{\min}(A \mid P)$$

$$H(A \mid E \mid P^n) = nH(A \mid E \mid P)$$

$$H_{1+s}(A \mid E \mid P^n) = nH_{1+s}(A \mid E \mid P)$$

$$H_{\min}(A \mid E \mid P^n) = nH_{\min}(A \mid E \mid P)$$

Analysis with modified mutual information

f_X : Universal2 hash functions

$$\mathbf{E}_X I'(f_X(A):E) \le \frac{M^s e^{-sH_{1+s}(A|E|P^{A,E})}}{s}$$

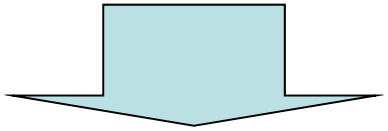
$s=1$: Bennett et al IEEE IT 1995

$0<s<1$: MH IEEE IT 2011

I.I.D. case

When $M = e^{nR}$,

$$E_X I'(f_X(A) \mid E \mid P^n) \leq \frac{e^{-sn(H_{1+s}(A|E|P)-R)}}{s}$$



$$R < H(A \mid E \mid P)$$

$$\exists s \in (0,1] \quad \text{s.t.} \quad H_{1+s}(A \mid E \mid P) > R$$

$E_X I'(f_X(A) \mid E \mid P^n)$ goes to zero exponentially.

Analysis with universal composability: Case without leaked information

$$d_1'(A|P) := \left\| P^A - P_U^A \right\|_1$$

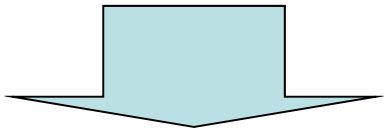
$$d_2(A|P) := \sum_a \left(P^A(a) - P_U^A(a) \right)^2$$

Schwarz inequality yields

$$d_1'(A|P) \le \sqrt{|\mathcal{A}|}\sqrt{d_2(A|P)}$$

Leftover hashing lemma

$$E_X d_2(f_X(A)|P) \le e^{-H_2(A|P)}$$



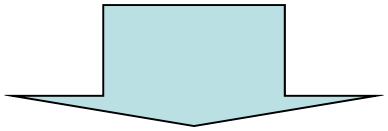
$$E_X d_1'(f_X(A)|P) \le M^{1/2} e^{-\frac{1}{2}H_2(A|P)}$$

Renner(2005)

Weakness of $E_X d_1'(f_X(A)|P) \le M^{1/2} e^{-\frac{1}{2}H_2(A|P)}$

When $M = e^{nR}$ with i.i.d. case,

$$E_X d_1'(f_X(A)|P^n) \le e^{-\frac{n}{2}(H_2(A|P)-R)}$$



When $R < H_2(A|P)$,

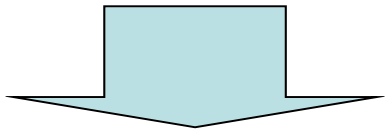
$E_X d_1'(f_X(A)|P^n)$ goes to zero exponentially.

When $R \in (H_2(A|P), H(A|P))$,

we cannot derive a similar conclusion.

Smoothing method

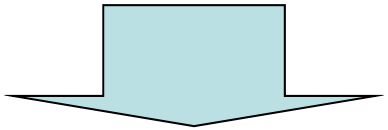
$$E_X d_1'(f_X(A)|P) \leq M^{1/2} e^{-\frac{1}{2}H_2(A|P)}$$



P' : sub-distribution

$$E_X d_1'(f_X(A)|P) \leq 2\left\|P - P'\right\|_1 + M^{1/2} e^{-\frac{1}{2}H_2(A|P')}$$

Renner(2005)



By choosing suitable P'

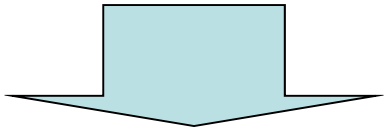
$$E_X d_1'(f_X(A)|P) \leq 3M^{s/1+s} e^{-\frac{s}{1+s}H_{1+s}(A|P)}$$

$$= 3M^{s/1+s}\left(\sum_a P^A(a)^{1+s}\right)^{\frac{1}{1+s}}$$

MH2010

When $M = e^{nR}$ with i.i.d. case,

$$E_X d_1'(f_X(A) \mid P^n) \le e^{-\frac{sn}{1+s}(H_{1+s}(A|P)-R)}$$



When $R < H(A \mid P)$,

$E_X d_1'(f_X(A) \mid P^n)$ goes to zero exponentially.

Derivation of

$$E_X d_1'(f_X(A)\,|\,P) \le 3M^{s/1+s} e^{-\frac{s}{1+s}H_{1+s}(A|P)}$$

MH 2010

$$P'(a) := 1_{\{P(a)\le 1/M'\}} P(a)$$

$$\|P' - P\|_1 = 2 \sum_{a:P(a)>1/M'} P(a) \le 2 \sum_{a:P(a)M'>1} P(a)^{1+s} M'^{s} \le 2M'^{s} e^{-sH_{1+s}(A|P)}$$

&

$$Me^{-H_2(A|P')} = M \sum_{a:P(a)\le 1/M'} P(a)^2$$

$$\le M \sum_{a:(P(a)M')^{-1}\ge 1} P(a)^{2-(1-s)} M'^{-(1-s)} \le \frac{M}{M'} M'^{s} e^{-sH_{1+s}(A|P)}$$

$$E_X d_1'(f_X(A)\,|\,P) \le 2\|P - P'\|_1 + M^{1/2} e^{-\frac{1}{2}H_2(A|P')}$$

$$E_X d_1'(f_X(A)\,|\,P) \le 2M'^{s/2} e^{-sH_{1+s}(A|P)} + \sqrt{\frac{M}{M'} M'^{s} e^{-sH_{1+s}(A|P)}}$$

$$M' := M^{\frac{1}{1+s}} e^{-\frac{s}{1+s}H_{1+s}(A|P)}$$

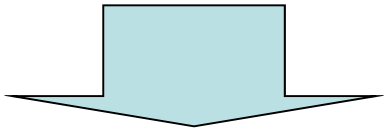
$$E_X d_1'(f_X(A)\,|\,P) \le 3M^{s/1+s} e^{-\frac{s}{1+s}H_{1+s}(A|P)}$$

Optimality of exponent

MH2010

When $M = e^{nR}$,

$$E_X d_1'(f_X(A)|P^n) \le 3\exp[(-n\frac{s(H_{1+s}(A|P)-R)}{1+s}]$$



$$\lim_{n\to\infty} -\frac{\log E_X d_1'(f_X(A)|P^n)}{n} \ge \max_{0\le s\le 1} \frac{s(H_{1+s}(A|P)-R)}{1+s}$$

When f_X is completely random,

$$\lim_{n\to\infty} -\frac{\log E_X d_1'(f_X(A)|P^n)}{n} = \max_{0\le s\le 1} \frac{s(H_{1+s}(A|P)-R)}{1+s}$$

A variant of Gallager function

$$\phi(s \mid P) := \log \sum_e P^E(e) \left(\sum_a P^{A|E}(a \mid e)^{1/(1-s)} \right)^{1-s}$$

$$= \log \left(\sum_e \left(\sum_a P^{AE}(a,e)^{1/(1-s)} \right)^{1-s} \right.$$

Properties

$$\left. \frac{d\phi(s \mid P)}{ds} \right|_{s=0} = -H(A \mid E \mid P)$$

$$sH_{1+s}(A \mid E \mid P) \geq -\phi(s \mid P)$$

$$e^{\phi\left(\frac{s}{1+s} \mid P\right)} = \sum_e P^E(e) e^{-\frac{s}{1+s} H_{1+s}\left(A \mid P^{A|E=e}\right)}$$

$$\phi(s \mid P^n) = n\phi(s \mid P)$$

Case with leaked information

Taking the expectation concerning E ,

$$E_X d_1'(f_X(A)|E|P)$$

$$= E_X \sum_e P^E(e) d_1'(f_X(A)|P^{A|E=e})$$

$$= \sum_e P^E(e) E_X d_1'(f_X(A)|P^{A|E=e})$$

$$\leq \sum_e P^E(e) 3M^{s/1+s} e^{-\frac{s}{1+s} H_{1+s}(A|P^{A|E=e})}$$

$$= 3M^{\frac{s}{1+s}} e^{\phi(\frac{s}{1+s}|P)}$$

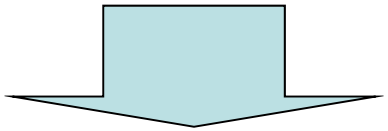
MH2010

I.I.D. case

MH2010

When $M = e^{nR}$, $t = \dfrac{s}{1+s}$

$$E_X d_1'(f_X(A) \mid E \mid P^n) \le 3\exp[n(tR + \phi(t \mid P))]$$



$$\lim_{n\to\infty} -\frac{\log E_X d_1'(f_X(A) \mid E \mid P)}{n}$$

$$\ge \max_{0\le t\le 1/2} -tR - \phi(t \mid P)$$

Bound for extactable length

$$\ell_U(\varepsilon \mid P_{AE})$$

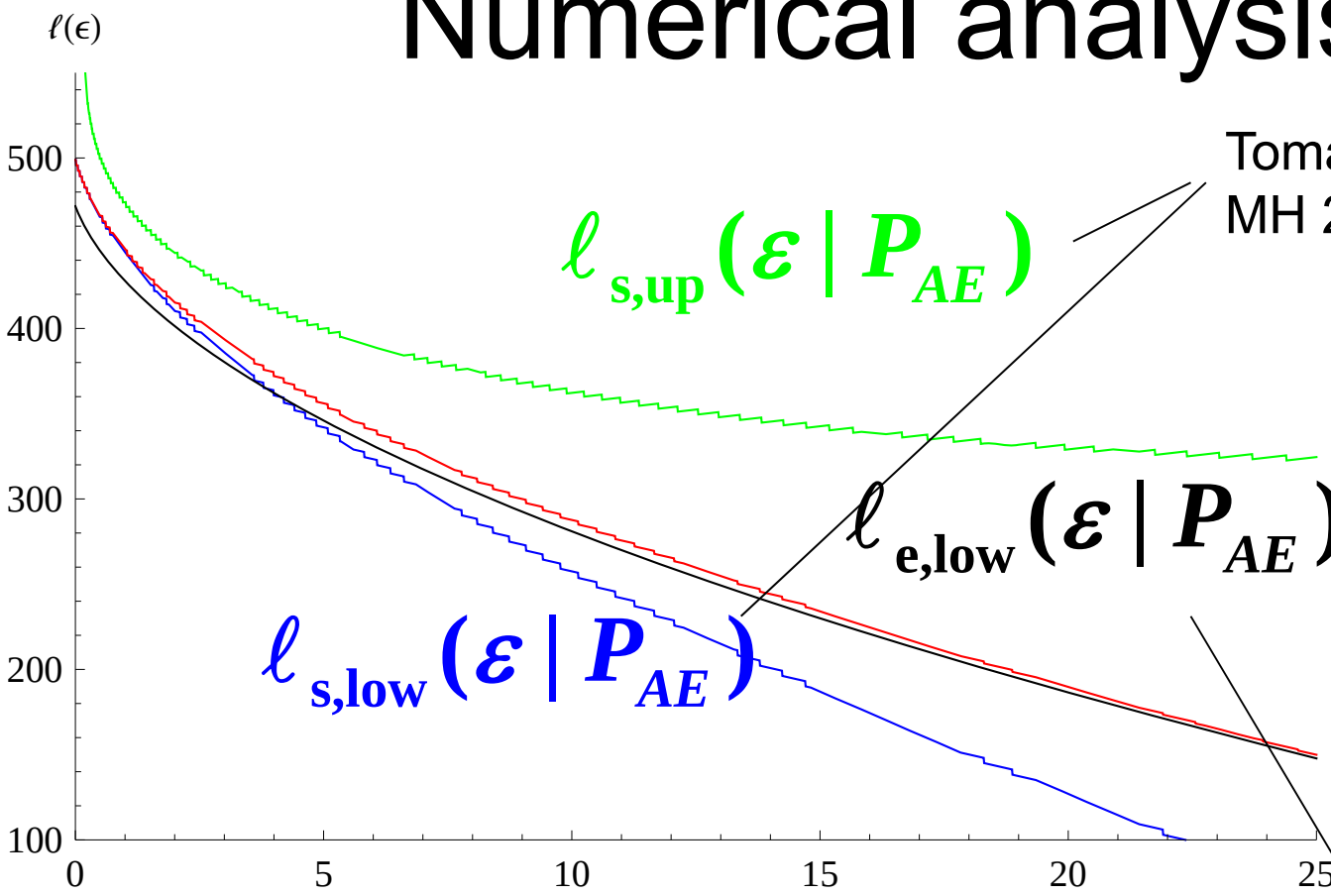
$$:= \max_{M} \left\{ \log M \;\middle|\; \begin{array}{l} \forall f : \mathcal{A} \to \{1,\ldots,M\} \\ \text{Universal2 hash functions} \\ \mathrm{E}_X d(f_X(A) \mid E \mid P_{AE}) \le \varepsilon \end{array} \right\}$$

$$\ge \ell_{\mathrm{e,low}}(\varepsilon \mid P_{AE})$$

S Watanabe & MH 2012

$$:= \sup_{\theta \in (0,1]} \frac{\theta H_{1+\theta}(A \mid E) + (1+\theta)\log \frac{2\varepsilon}{3}}{\theta} - 1$$

Numerical analysis



Tomamichel & MH 2012

When n is smaller than ε, Exponential type evaluation is better than information spectrum type one.

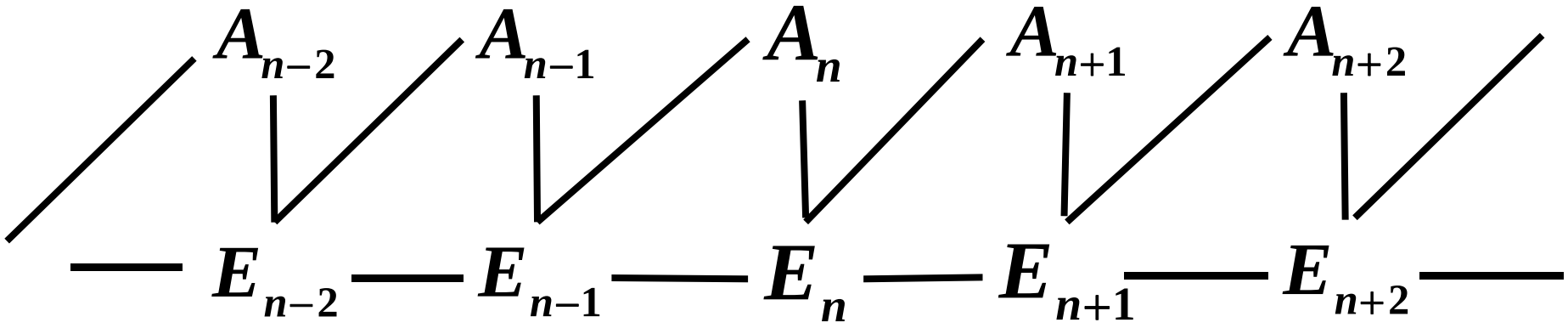
S Watanabe & MH 2012

$$P_{AE}(a,e) = \begin{cases} q/2 & if\ a \neq e \\ (1-q)/2 & f\ a = e \end{cases}$$

$$\mathcal{A} = \mathcal{E} = \{0,1\}$$

n = 1000, q=0.11

Markovian case



Assume

$$P_{A_n E_n | A_{n-1} E_{n-1}}(a, e \mid a', e') = P_{AE|E'}(a, e \mid e')$$

Markovian case

Assume

$$P_{A_n E_n | A_{n-1} E_{n-1}}(a,e|a',e') = P_{AE|E'}(a,e|e')$$

Define matrix

$$X_{e,e'} := \sum_a P_{AE|E'}(a,e|e')^{1/(1-s)}$$

Assume

$X_{e,e'}$ is irreducible, i.e., $\forall e \forall e' \exists n$

$(X^n)_{e,e'} > 0$

$\exists 1$ eigenvalue $\lambda_s > 0$ s.t. eigenvector p_s

$p_s(e) \geq 0$ Perron-Frobenius Theorem

Theorem

$$\phi(s) := \lim_{n\to\infty} \frac{1}{n}\phi(s \mid P^n) = (1-s)\log \lambda_s$$

Then

$$\lim_{n\to\infty} - \frac{\log E_X d_1'(f_X(A) \mid E \mid P)}{n} \geq \max_{0\leq s\leq 1/2} - sR - \phi(s)$$

$$\phi'(0)$$

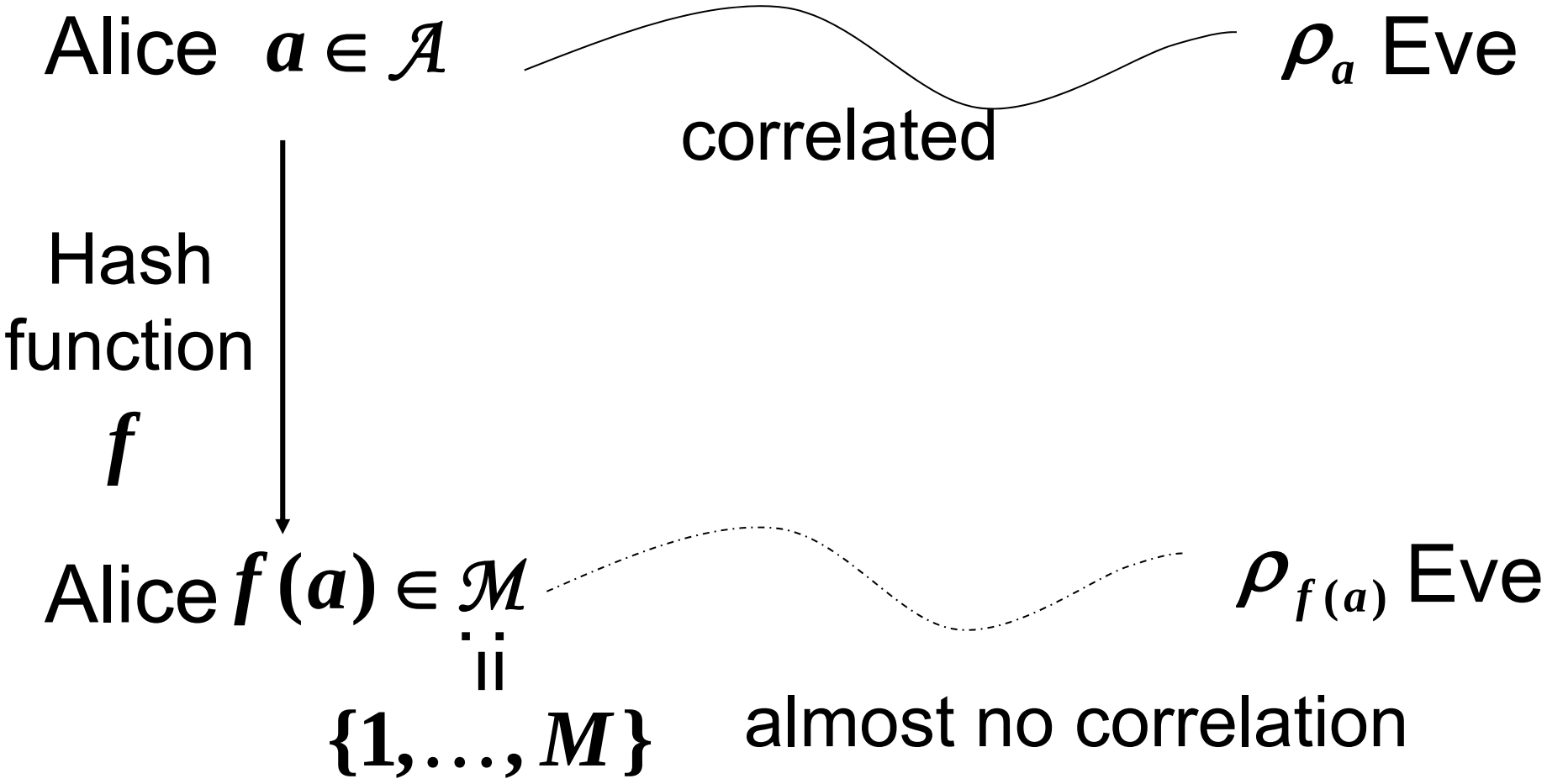
$$= \sum_{e'} P_0(e')(H(AE \mid P_{AE|E'=e'}) - H(E \mid P_{E|E'=e'}))$$

Key generation rate is greater than

$$\sum_{e'} P_0(e')(H(AE \mid P_{AE|E'=e'}) - H(E \mid P_{E|E'=e'}))$$

Extension to Quantum Case

Leaked quantum information



Total density matrix $\rho = \sum_a P(a) |a\rangle\langle a| \otimes \rho_a$

Entropy

$$\rho = \sum_a P(a)\left|a\right\rangle\left\langle a\right| \otimes \rho_a$$

$$H(A,E \mid \rho) := -\mathrm{Tr}\rho \log \rho$$

$$H(E \mid \rho) := -\mathrm{Tr}\rho_E \log \rho_E$$

Conditional entropy

$$H(A \mid E \mid \rho) := H(A,E \mid \rho) - H(E \mid \rho)$$

Quantum mutual information

$$I(A:E \mid \rho) = H(E \mid \rho) + H(A \mid \rho) - H(A,E \mid \rho)$$

$$= H(A \mid \rho) - H(A \mid E \mid \rho) = D(\rho \| \rho_A \otimes \rho_E)$$

$$D(\rho \| \sigma) := \mathrm{Tr}\rho(\log \rho - \log \sigma)$$

Two security criteria

$$\rho = \sum_a P(a)\left|a\right\rangle\left\langle a\right| \otimes \rho_a$$

(1)Universal composability

$$d_1'(A \mid E \mid \rho) := \left\| \rho - \rho_{A,\mathrm{mix}} \otimes \rho_E \right\|_1$$

(2)Modified quantum mutual information

$$I'(A:E \mid \rho) := D(\rho \left\| \rho_{A,\mathrm{mix}} \otimes \rho_E \right.)$$

$$= D(\rho \left\| \rho_A \otimes \rho_E \right.) + D(\rho_A \left\| \rho_{A,\mathrm{mix}} \right.)$$

$$\geq \left\| \rho - \rho_{A,\mathrm{mix}} \otimes \rho_E \right\|_1^2$$

$$D(\rho \left\| \sigma \right.) := \mathrm{Tr}\rho(\log \rho - \log \sigma)$$

Conditional Renyi Entropies

$$H_{1+s}(A|E|\rho) := \frac{-1}{s}\log \mathrm{Tr}\rho^{1+s}\rho_E^{-s}$$

$$\overline{H}_{1+s}(A|E|\rho) := \frac{-1}{s}\log \mathrm{Tr}(\rho^{\frac{1+s}{2}}\rho_E^{-s/2})^2$$

$I_A \otimes \rho_E$ is simplified to ρ_E

Properties

Monotone decreasing for s

$$\lim_{s\to 0} H_{1+s}(A|E|\rho) = \lim_{s\to 0} \overline{H}_{1+s}(A|E|\rho) = H(A|E|\rho)$$

$$H(A|E|\rho) \geq \overline{H}_{1+s}(A|E|\rho) \geq H_{1+s}(A|E|\rho)$$

$$\geq H_{\min}(A|E|\rho) := -\log\left\|\rho_E^{-1/2}\rho\rho_E^{-1/2}\right\| \qquad s\in(0,1]$$

Relative conditional Renyi Entropies

$$H_{1+s}(A \mid E \mid \rho \| \sigma) := \frac{-1}{s} \log \mathrm{Tr} \rho^{1+s} \sigma^{-s}$$

$$\overline{H}_{1+s}(A \mid E \mid \rho \| \sigma) := \frac{-1}{s} \log \mathrm{Tr} (\rho^{\frac{1+s}{2}} \sigma^{-s/2})^2$$

σ:arbitrary state on $\mathcal{H}_E$

Monotone decreasing for s>0

$$\overline{H}_{1+s}(A \mid E \mid \rho \| \sigma) \geq H_{1+s}(A \mid E \mid \rho \| \sigma)$$

$$\geq H_{\min}(A \mid E \mid \rho \| \sigma) := -\log \left\| \sigma^{-1/2} \rho \sigma^{-1/2} \right\|$$

$$s \in (0, 1]$$

Important function

$$\phi(s\,|\,\rho) := \log \mathrm{Tr}_E \left(\mathrm{Tr}_A \rho^{1/(1-s)}\right)^{1-s}$$

$$\left.\frac{d\phi(s\,|\,\rho)}{ds}\right|_{s=0} = -H(A\,|\,E\,|\,\rho)$$

$$\phi(s\,|\,\rho^{\otimes n}) = n\phi(s\,|\,\rho)$$

Theorem

$$\max_{\sigma} sH_{1+s}(A\,|\,E\,|\,\rho\|\sigma) = -(1+s)\phi\left(\frac{s}{1+s}\,|\,\rho\right)$$

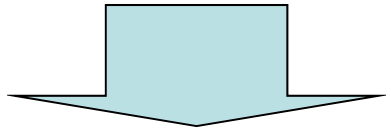
Maximum can be attained by $c\left(\mathrm{Tr}_A \rho^{1+s}\right)^{1/(1+s)}$

$$sH_{1+s}(A\,|\,E\,|\,\rho) \geq -\phi(s\,|\,\rho)$$ MH 2012

Leftover hashing lemma

Renner(2005)

$$E_X d_1'(f_X(A)|E|\rho) \le M^{1/2} e^{-\frac{1}{2}\overline{H}_2(A|E|\rho\|\sigma)}$$



$$E_X d_1'(f_X(A)|E|\rho)$$

$$\le 2\|\rho-\rho'\|_1 + M^{1/2} e^{-\frac{1}{2}\overline{H}_2(A|E|\rho'\|\sigma)}$$

ρ' : sub-state

However, he did not give an explicit choice of ρ'.

Our contribution

MH 2012

By choosing suitable ρ'

$$E_X d_1'(f_X(A)|E|\rho) \le (4+\sqrt{v}) M^{s/2} e^{-\frac{s}{2} H_{1+s}(A|E|\rho\|\sigma)}$$

v: Number of eigenvalues of σ

By setting $\sigma = c(\mathrm{Tr}_A \rho^{1+s})^{1/(1+s)}$

$$E_X d_1'(f_X(A)|E|\rho) \le (4+\sqrt{v}) M^{s/2} e^{\frac{1+s}{2}\phi(\frac{s}{1+s}|\rho)}$$

When $M = e^{nR}$ with i.i.d. case,

$$E_X d_1'(f_X(A)|E|\rho^{\otimes n})$$

$$\le (4+(n+1)^{(d-1)/2}) e^{n(\frac{1+s}{2}\phi(\frac{s}{1+s}|\rho)+\frac{sR}{2})}$$

Derivation of

$$E_X d_1'(f_X(A)|E|\rho) \le (4+\sqrt{v})M^{s/2}e^{-\frac{s}{2}\overline{H}_{1+s}(A|E|\rho\|\sigma)}$$

MH 2012

$\sigma := \sum_i s_i P_i$:Spectrum decomposition of σ

$$\mathcal{E}(\rho) := \sum_i P_i \rho P_i \quad P := \left\{ \mathcal{E}(\rho) - \frac{\sigma}{M} \le 0 \right\} \quad \{X \le 0\} := \sum_{x_i \ge 0} E_i \quad \text{with } X = \sum_i x_i E_i$$

$$\left\| P\rho P - \rho \right\|_1 \le 2\sqrt{\mathrm{Tr}\rho(I-P)}$$

&

$$\mathrm{Tr}\rho(I-P) = \mathrm{Tr}\rho\mathcal{E}(I-P) = \mathrm{Tr}\mathcal{E}(\rho)(I-P)$$

$$\le \mathrm{Tr}\mathcal{E}(\rho)^{1+s} M^s \sigma^{-s}(I-P) \le \mathrm{Tr}\mathcal{E}(\rho)^{1+s} M^s \sigma^{-s}$$

$$= M^s e^{-sH_{1+s}(A|E|\mathcal{E}(\rho)\|\sigma)} \le M^s e^{-sH_{1+s}(A|E|\rho\|\sigma)}$$

$$E_X d_1'(f_X(A)|E|\rho) \le 2\left\|\rho - \rho'\right\|_1 + M^{1/2} e^{-\frac{1}{2}\overline{H}_2(A|E|\rho'\|\sigma)}$$

$$E_X d_1'(f_X(A)|E|\rho) \le 4M^{s/2} e^{-\frac{1}{2}\overline{H}_{1+s}(A|E|\rho\|\sigma)} + M^{1/2} e^{-\frac{1}{2}\overline{H}_2(A|E|P\rho P\|\sigma)}$$

MH, 2012

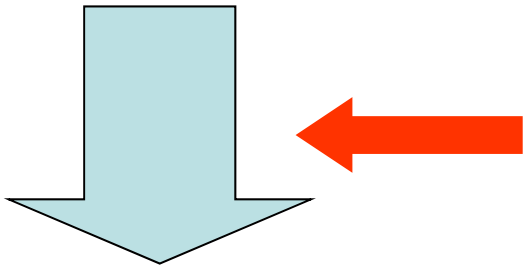
Evaluation of $Me^{-\overline{H}_2(A|E|P\rho P\|\sigma)}$

$$Me^{-\overline{H}_2(A|E|P\rho P\|\sigma)} = M\mathrm{Tr}P\rho P\sigma^{-1/2}P\rho P\sigma^{-1/2}$$

$$\le Mv\mathrm{Tr}\mathcal{E}(\rho)\sigma^{-1/2}P\rho P\sigma^{-1/2} = Mv\mathrm{Tr}\mathcal{E}(\rho)^2\sigma^{-1}P$$

$$\le vM^s\mathrm{Tr}\mathcal{E}(\rho)^{1+s}\sigma^{-s}P \le vM^s\mathrm{Tr}\mathcal{E}(\rho)^{1+s}\sigma^{-s}$$

$$= vM^s e^{-H_{1+s}(A|E|\mathcal{E}(\rho)\|\sigma)} \le vM^s e^{-H_{1+s}(A|E|\rho\|\sigma)}$$



$$E_X d_1'(f_X(A)|E|\rho)$$

$$\le 4M^{s/2}e^{-\frac{1}{2}\overline{H}_{1+s}(A|E|\rho\|\sigma)} + M^{1/2}e^{-\frac{1}{2}\overline{H}_2(A|E|P\rho P\|\sigma)}$$

$$E_X d_1'(f_X(A)|E|\rho) \le (4+\sqrt{v})M^{s/2}e^{-\frac{s}{2}\overline{H}_{1+s}(A|E|\rho\|\sigma)}$$

Improvement of polynomial factor

In i.i.d. case, $v = O(n^{d-1}) \le (n+1)^{d-1}$

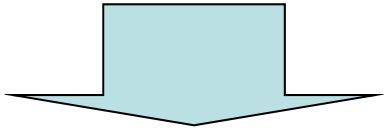
Improvement

λ: Logarithm of the ratio between maximal and minimal eigenvalues of σ

$$E_X d_1'(f_X(A)|E|\rho)$$

$$\le (4+\sqrt{\lceil \lambda \rceil}) M^{s/2} e^{-\frac{s}{2} H_{1+s}(A|E|\rho\|\sigma)+\frac{s}{2}}$$

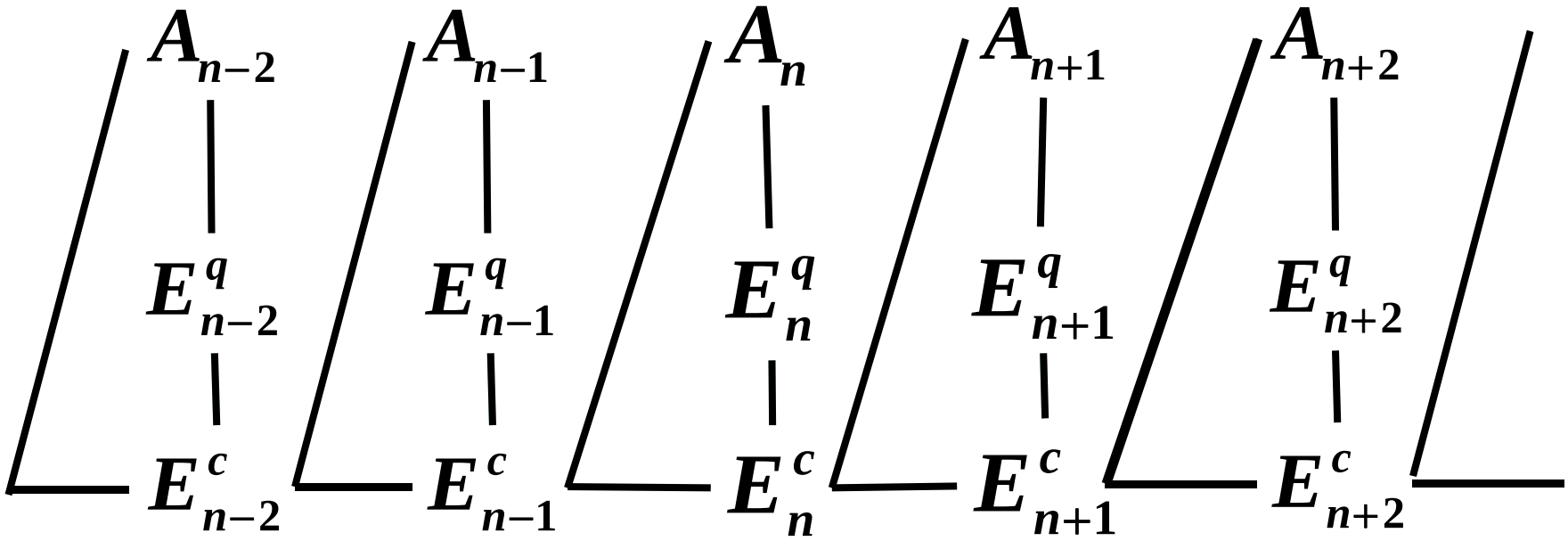
In i.i.d. case, $\lambda = n + C$



By setting $\sigma = c(\mathrm{Tr}_A \rho^{1+s})^{1/(1+s)}$

$$E_X d_1'(f_X(A)|E|\rho) \le (4+\sqrt{\lceil \lambda \rceil}) M^{s/2} e^{\frac{1+s}{2}\phi(\frac{s}{1+s}|\rho)+\frac{s}{2}}$$

Q-Markovian case



Assume

$$P_{A_n E_n^c | A_{n-1} E_{n-1}^c}(a,e|a',e') = P_{AE|E'}(a,e|e')$$

n-th state

$$\rho_{AE|E'=e'} := \sum_{a,e} P_{AE^c|E^c}(a,e|e') \left|a,e\right\rangle\left\langle a,e\right| \otimes \rho^E_{a,e}$$

Q-Markovian case

Define matrix

$$X_{e,e'} := \mathrm{Tr} \sum_{a} P_{A_n E_n^c | E_{n-1}^c}(a,e|e')^{1/(1-s)} (\rho_{a,e}^{E})^{1/(1-s)}$$

Assume

$X_{e,e'}$ is irreducible, i.e., $\forall e \forall e' \exists n$

$(X^n)_{e,e'} > 0$

$\exists 1$ eigenvalue $\lambda_s > 0$ s.t. eigenvector p_s

$p_s(e) \geq 0$ Perron-Frobenius Theorem

Theorem

$$\phi(s) := \lim_{n\to\infty} \frac{1}{n}\phi(s \mid \rho^n) = (1-s)\log \lambda_s$$

Then,

$$\lim_{n\to\infty} - \frac{\log E_X d_1'(f_X(A) \mid E \mid \rho^n)}{n} \geq \max_{0\leq s\leq 1/2} -sR - \phi(s)$$

$$\phi'(0)$$

$$= \sum_{e'} P_0(e')(H(AE \mid \rho_{AE|E'=e'}) - H(E \mid \rho_{E|E'=e'}))$$

Key generation rate is greater than

$$\sum_{e'} P_0(e')(H(AE \mid P_{AE|E'=e'}) - H(E \mid P_{E|E'=e'}))$$

Applications and related topics

- Security analysis for secure key distillation
- Generalization of Leftover hashing lemma (ε-almost dual univesal2 hash functions)
- Security analysis for wire-tap channel with ordinary code (for regular channel)
- Security analysis for Broadcast Channel with Confidential code.
- Universal code for wire-tap channel
- Application to QKD

Conclusion

- We have derived an upper bound for security parameter by smoothing conditional Renyi entropy of order 2 when we applied universal2 hash function.
- The upper bound has a simpler form and goes to zero when the generation rate is smaller than $\boldsymbol{H(A|E|\rho)}$.
- This result can be extended to the Markovian case.

References

- Renner, Ph.D thesis(2005)
- MH, arXiv:1010.1358 (2010).
- MH, arXiv:1012.0322 (2012).
- MH, arXiv:1012.0601 (2012).
- MH, IEEE Trans. IT (2011).
- S. Watanabe, MH, arXiv:1211.5252.
- PPT containing the related topics is available at http://www.quantumlah.org/events/workshops/JSW2012_program.php