Tail Exponents of Conditional Guesswork via the Method of Types

Adway Girish

joint work with Andreina Motter and Emre Telatar





November 11, 2026
2026 IEEE ITW

Guessing



Alice



Bob

Guessing

- P_X known to Bob

X



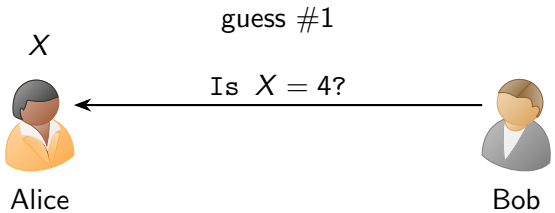
Alice



Bob

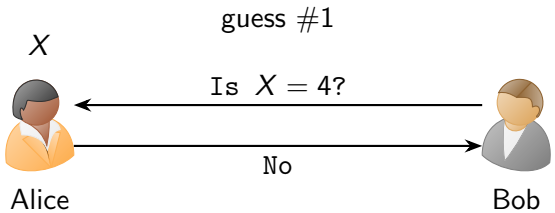
Guessing

- P_X known to Bob



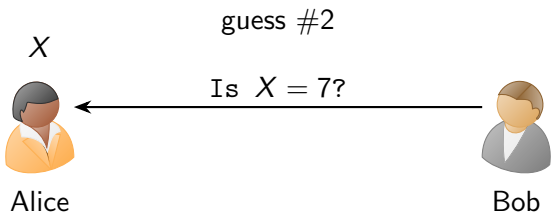
Guessing

- P_X known to Bob



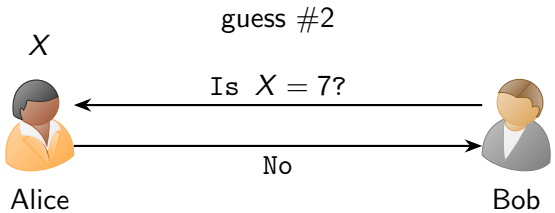
Guessing

- P_X known to Bob



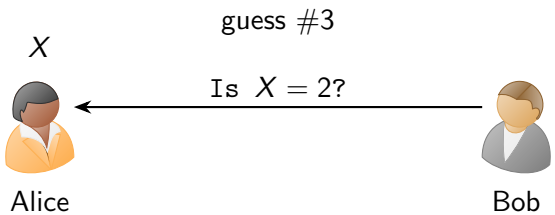
Guessing

- P_X known to Bob



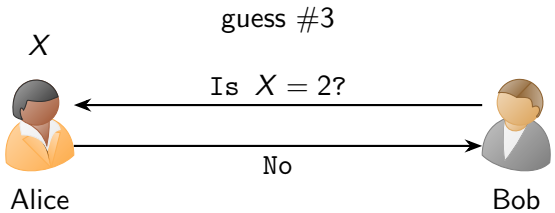
Guessing

- P_X known to Bob



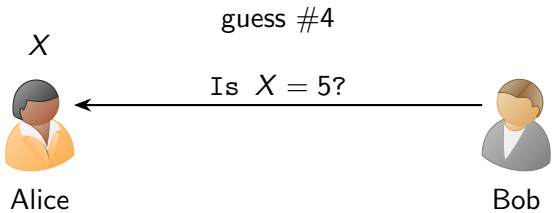
Guessing

- P_X known to Bob



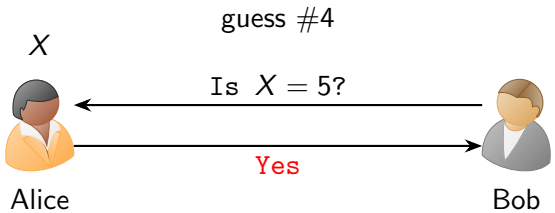
Guessing

- P_X known to Bob



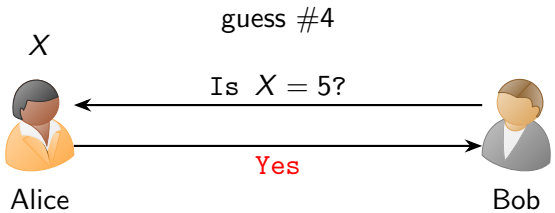
Guessing

- P_X known to Bob



Guessing

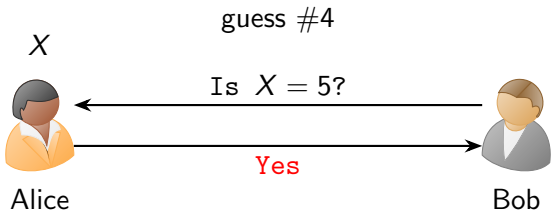
- P_X known to Bob



- $G(x) =$ no. of guesses to get `Yes` when $X = x$

Guessing

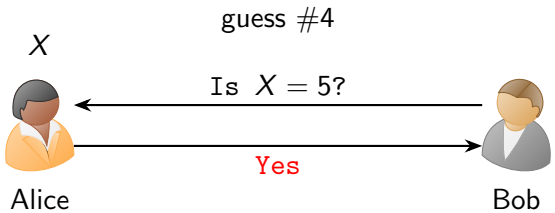
- P_X known to Bob



- $G(x) =$ no. of guesses to get `Yes` when $X = x$
- obvious "optimal" scheme G^*:

Guessing

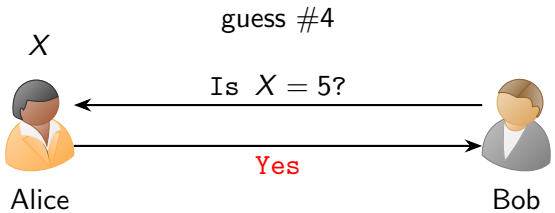
- P_X known to Bob



- $G(x) =$ no. of guesses to get `Yes` when $X = x$
- obvious "optimal" scheme G^*: guess x_1 before x_2 if $P_X(x_1) > P_X(x_2)$

Guessing

- P_X known to Bob



- $G(x) =$ no. of guesses to get `Yes` when $X = x$
- obvious "optimal" scheme G^*: guess x_1 before x_2 if $P_X(x_1) > P_X(x_2)$
- $G^*(x) \approx$ no. of x' with $P_X(x') > P_X(x)$

Guessing with side-information

- P_{XY} known to Bob; Y observed by Bob



Alice



Bob

- $G(x) =$ no. of guesses to get `Yes` when $X = x$
- obvious "optimal" scheme G^*: guess x_1 before x_2 if $P_X(x_1) > P_X(x_2)$
- $G^*(x) \approx$ no. of x' with $P_X(x') > P_X(x)$

Guessing with side-information

- P_{XY} known to Bob; Y observed by Bob



Alice



Bob

- $G(x \mid y)$ = no. of guesses to get `Yes` when $X = x, Y = y$
- obvious "optimal" scheme $G^*(\cdot \mid y)$: guess x_1 before x_2 if $P_{X|Y}(x_1 \mid y) > P_{X|Y}(x_2 \mid y)$
- $G^*(x \mid y) \approx$ no. of x' with $P_{X|Y}(x' \mid y) > P_{X|Y}(x \mid y)$

Guessing vectors with side-information

- $P_{\boldsymbol{X}\boldsymbol{Y}}$ known to Bob; $\boldsymbol{Y}$ observed by Bob

$$\boldsymbol{X} = (X_1, \ldots, X_n)$$
$$\boldsymbol{Y} = (Y_1, \ldots, Y_n)$$

$\boldsymbol{X}$



Alice

$\boldsymbol{Y}$



Bob

- $G(\boldsymbol{x} \mid \boldsymbol{y})$ = no. of guesses to get `Yes` when $\boldsymbol{X} = \boldsymbol{x}$, $\boldsymbol{Y} = \boldsymbol{y}$
- obvious "optimal" scheme $G^*(\cdot \mid \boldsymbol{y})$: guess $\boldsymbol{x}_1$ before $\boldsymbol{x}_2$ if $P_{\boldsymbol{X}|\boldsymbol{Y}}(\boldsymbol{x}_1 \mid \boldsymbol{y}) > P_{\boldsymbol{X}|\boldsymbol{Y}}(\boldsymbol{x}_2 \mid \boldsymbol{y})$
- $G^*(\boldsymbol{x} \mid \boldsymbol{y}) \approx$ no. of $\boldsymbol{x}'$ with $P_{\boldsymbol{X}|\boldsymbol{Y}}(\boldsymbol{x}' \mid \boldsymbol{y}) > P_{\boldsymbol{X}|\boldsymbol{Y}}(\boldsymbol{x} \mid \boldsymbol{y})$

Guessing vectors with side-information

- $P_{\boldsymbol{X}\boldsymbol{Y}}$ known to Bob; $\boldsymbol{Y}$ observed by Bob

$$\boldsymbol{X} = (X_1, \ldots, X_n)$$
$$\boldsymbol{Y} = (Y_1, \ldots, Y_n)$$



Alice



Bob

- $G(\boldsymbol{x} \mid \boldsymbol{y})$ = no. of guesses to get `Yes` when $\boldsymbol{X} = \boldsymbol{x}$, $\boldsymbol{Y} = \boldsymbol{y}$
- obvious "optimal" scheme $G^*(\cdot \mid \boldsymbol{y})$: guess $\boldsymbol{x}_1$ before $\boldsymbol{x}_2$ if $P_{\boldsymbol{X}|\boldsymbol{Y}}(\boldsymbol{x}_1 \mid \boldsymbol{y}) > P_{\boldsymbol{X}|\boldsymbol{Y}}(\boldsymbol{x}_2 \mid \boldsymbol{y})$
- $G^*(\boldsymbol{x} \mid \boldsymbol{y}) \approx$ no. of $\boldsymbol{x}'$ with $P_{\boldsymbol{X}|\boldsymbol{Y}}(\boldsymbol{x}' \mid \boldsymbol{y}) > P_{\boldsymbol{X}|\boldsymbol{Y}}(\boldsymbol{x} \mid \boldsymbol{y})$

what are $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) > t\}$ and $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) < t\}$?

Guessing vectors with side-information

- $P_{\boldsymbol{X}\boldsymbol{Y}}$ known to Bob; $\boldsymbol{Y}$ observed by Bob

$\boldsymbol{X} = (X_1, \ldots, X_n)$
$\boldsymbol{Y} = (Y_1, \ldots, Y_n)$

$\boldsymbol{X}$



Alice

$\boldsymbol{Y}$



Bob

$(X_i, Y_i) \overset{\text{i.i.d.}}{\sim} P_{XY}$

- $G(\boldsymbol{x} \mid \boldsymbol{y}) =$ no. of guesses to get `Yes` when $\boldsymbol{X} = \boldsymbol{x}$, $\boldsymbol{Y} = \boldsymbol{y}$
- obvious "optimal" scheme $G^*(\cdot \mid \boldsymbol{y})$: guess $\boldsymbol{x}_1$ before $\boldsymbol{x}_2$ if $P_{\boldsymbol{X}|\boldsymbol{Y}}(\boldsymbol{x}_1 \mid \boldsymbol{y}) > P_{\boldsymbol{X}|\boldsymbol{Y}}(\boldsymbol{x}_2 \mid \boldsymbol{y})$
- $G^*(\boldsymbol{x} \mid \boldsymbol{y}) \approx$ no. of $\boldsymbol{x}'$ with $P_{\boldsymbol{X}|\boldsymbol{Y}}(\boldsymbol{x}' \mid \boldsymbol{y}) > P_{\boldsymbol{X}|\boldsymbol{Y}}(\boldsymbol{x} \mid \boldsymbol{y})$

what are $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) > t\}$ and $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) < t\}$?

Previous work

what are $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) > t\}$ and $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) < t\}$?

Previous work

what are $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) > t\}$ and $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) < t\}$?

- Arikan (1996)*: $\rho > 0$, $\mathbb{E}[G^*(\boldsymbol{X} \mid \boldsymbol{Y})^\rho] \approx \exp\left\{n\,\rho H_{1/(1+\rho)}(X \mid Y) + o(n)\right\}$

* "An inequality on guessing and its application to sequential decoding", *IEEE Transactions on Information Theory*, 1996

Previous work

what are $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) > \exp(nh)\}$ and $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) < \exp(nh)\}$?

- Arikan (1996)*: $\rho > 0$, $\mathbb{E}[G^*(\boldsymbol{X} \mid \boldsymbol{Y})^\rho] \approx \exp\left\{n\,\rho H_{1/(1+\rho)}(X \mid Y) + o(n)\right\}$

* "An inequality on guessing and its application to sequential decoding", *IEEE Transactions on Information Theory*, 1996

Previous work

what are $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) > \exp(nh)\}$ and $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) < \exp(nh)\}$?

- Arikan (1996)*: $\rho > 0$, $\mathbb{E}[G^*(\boldsymbol{X} \mid \boldsymbol{Y})^\rho] \approx \exp\left\{n\,\rho H_{1/(1+\rho)}(X \mid Y) + o(n)\right\}$
- Christiansen and Duffy (2013)†: $\{\frac{1}{n}\log G^*(\boldsymbol{X})\}$ satisfies LDP under CGF assumptions

* "An inequality on guessing and its application to sequential decoding", *IEEE Transactions on Information Theory*, 1996

† "Guesswork, large deviations, and Shannon entropy", *IEEE Transactions on Information Theory*, 2013

Previous work

what are $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) > \exp(nh)\}$ and $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) < \exp(nh)\}$?

- Arikan (1996)*: $\rho > 0$, $\mathbb{E}[G^*(\boldsymbol{X} \mid \boldsymbol{Y})^\rho] \approx \exp\left\{n\,\rho H_{1/(1+\rho)}(X \mid Y) + o(n)\right\}$
- Christiansen and Duffy (2013)†: $\{\frac{1}{n}\log G^*(\boldsymbol{X})\}$ satisfies LDP under CGF assumptions
- Beirami et al. (2019)‡: closed-form exponents of $\Pr\{G^*(\boldsymbol{X}) \gtrless \exp(nh)\}$ (i.i.d.)

* "An inequality on guessing and its application to sequential decoding", *IEEE Transactions on Information Theory*, 1996

† "Guesswork, large deviations, and Shannon entropy", *IEEE Transactions on Information Theory*, 2013

‡ "A characterization of guesswork on swiftly tilting curves", *IEEE Transactions on Information Theory*, 2019

Previous work

what are $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) > \exp(nh)\}$ and $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) < \exp(nh)\}$?

- Arikan (1996)*: $\rho > 0$, $\mathbb{E}[G^*(\boldsymbol{X} \mid \boldsymbol{Y})^\rho] \approx \exp\left\{n\,\rho H_{1/(1+\rho)}(X \mid Y) + o(n)\right\}$
- Christiansen and Duffy (2013)†: $\{\frac{1}{n}\log G^*(\boldsymbol{X})\}$ satisfies LDP under CGF assumptions
- Beirami et al. (2019)‡: closed-form exponents of $\Pr\{G^*(\boldsymbol{X}) \gtrless \exp(nh)\}$ (i.i.d.)
- Li (2019)§: $\{\frac{1}{n}\log G^*(\boldsymbol{X} \mid \boldsymbol{Y})\}$ satisfies LDP under CGF assumptions

* "An inequality on guessing and its application to sequential decoding", *IEEE Transactions on Information Theory*, 1996

† "Guesswork, large deviations, and Shannon entropy", *IEEE Transactions on Information Theory*, 2013

‡ "A characterization of guesswork on swiftly tilting curves", *IEEE Transactions on Information Theory*, 2019

§ "Large deviations for conditional guesswork", *Statistics & Probability Letters*, 2019

Previous work

what are $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) > \exp(nh)\}$ and $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) < \exp(nh)\}$?

- Arikan (1996)*: $\rho > 0$, $\mathbb{E}[G^*(\boldsymbol{X} \mid \boldsymbol{Y})^\rho] \approx \exp\left\{n\,\rho H_{1/(1+\rho)}(X \mid Y) + o(n)\right\}$
- Christiansen and Duffy (2013)†: $\{\frac{1}{n}\log G^*(\boldsymbol{X})\}$ satisfies LDP under CGF assumptions
- Beirami et al. (2019)‡: closed-form exponents of $\Pr\{G^*(\boldsymbol{X}) \gtrless \exp(nh)\}$ (i.i.d.)
- Li (2019)§: $\{\frac{1}{n}\log G^*(\boldsymbol{X} \mid \boldsymbol{Y})\}$ satisfies LDP under CGF assumptions
- this work: closed-form exponents of $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) \gtrless \exp(nh)\}$ via type-counting (i.i.d.)

* "An inequality on guessing and its application to sequential decoding", *IEEE Transactions on Information Theory*, 1996

† "Guesswork, large deviations, and Shannon entropy", *IEEE Transactions on Information Theory*, 2013

‡ "A characterization of guesswork on swiftly tilting curves", *IEEE Transactions on Information Theory*, 2019

§ "Large deviations for conditional guesswork", *Statistics & Probability Letters*, 2019

Tilted distributions

- $\lambda > 0$

Tilted distributions

- $\lambda > 0$, assume $P_{XY} : P_X, P_{X|Y}(\cdot \mid y)$ have full support and unique maximizer

Tilted distributions

- $\lambda > 0$, assume $P_{XY} : P_X, P_{X|Y}(\cdot \mid y)$ have full support and unique maximizer
- $P_X^{(\lambda)}(x) = \dfrac{P_X(x)^\lambda}{\sum_{x'} P_X(x')^\lambda}$

Tilted distributions

- $\lambda > 0$, assume $P_{XY} : P_X, P_{X|Y}(\cdot \mid y)$ have full support and unique maximizer
- $P_X^{(\lambda)}(x) = \dfrac{P_X(x)^\lambda}{\sum_{x'} P_X(x')^\lambda}$
- $P_X^{(0)} =$ uniform on $\mathrm{supp}(P_X)$

Tilted distributions

- $\lambda > 0$, assume $P_{XY} : P_X, P_{X|Y}(\cdot \mid y)$ have full support and unique maximizer
- $P_X^{(\lambda)}(x) = \dfrac{P_X(x)^\lambda}{\sum_{x'} P_X(x')^\lambda}$
- $P_X^{(0)} =$ uniform on $\mathrm{supp}(P_X)$, $P_X^{(1)} = P_X$

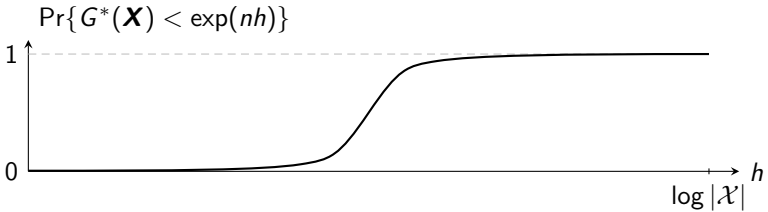
Tilted distributions

- $\lambda > 0$, assume $P_{XY} : P_X, P_{X|Y}(\cdot \mid y)$ have full support and unique maximizer
- $P_X^{(\lambda)}(x) = \dfrac{P_X(x)^\lambda}{\sum_{x'} P_X(x')^\lambda}$
- $P_X^{(0)} =$ uniform on $\mathrm{supp}(P_X)$, $P_X^{(1)} = P_X$, $P_X^{(\infty)} = \delta_{\arg\max P_X}$

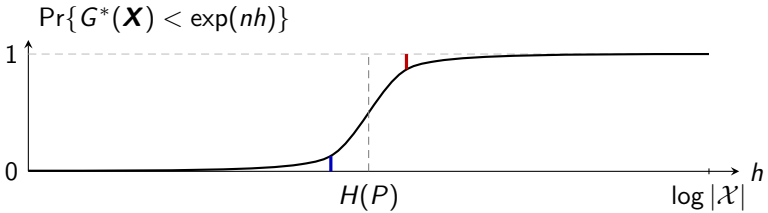
Tilted distributions

- $\lambda > 0$, assume $P_{XY} : P_X, P_{X|Y}(\cdot \mid y)$ have full support and unique maximizer
- $P_X^{(\lambda)}(x) = \dfrac{P_X(x)^\lambda}{\sum_{x'} P_X(x')^\lambda}$
- $P_X^{(0)} = \text{uniform on } \mathrm{supp}(P_X),\ P_X^{(1)} = P_X,\ P_X^{(\infty)} = \delta_{\arg\max P_X}$
- $P_{X|Y}^{(\lambda)}(x \mid y) = \dfrac{P_{X|Y}(x \mid y)^\lambda}{\sum_{x'} P_{X|Y}(x' \mid y)^\lambda}$

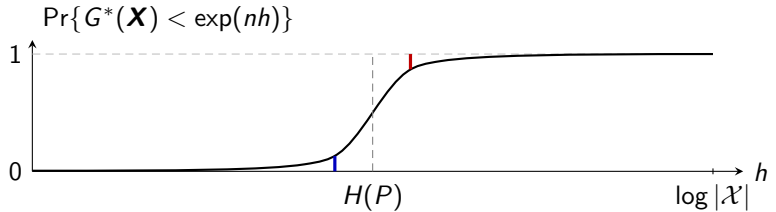
Tail exponents for unconditional guesswork



Tail exponents for unconditional guesswork



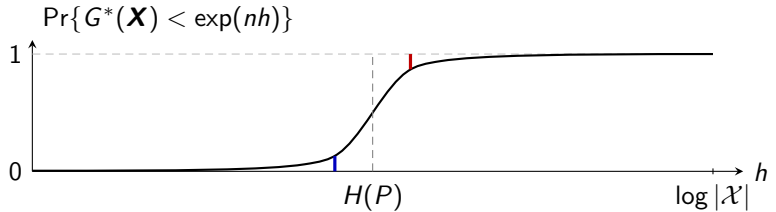
Tail exponents for unconditional guesswork



Theorem (no side-information)

Let $0 < h < \log|\mathcal{X}|$ *and* $\lambda_h > 0 : H(P_X^{(\lambda_h)}) = h$.

Tail exponents for unconditional guesswork



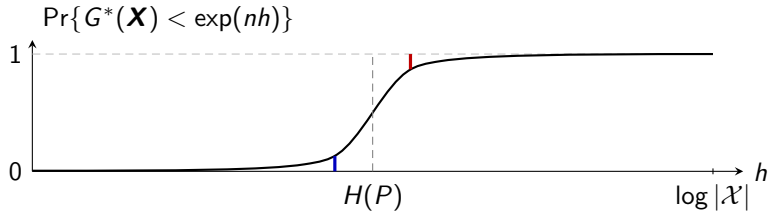
Theorem (no side-information)

Let $0 < h < \log|\mathcal{X}|$ *and* $\lambda_h > 0 : H(P_X^{(\lambda_h)}) = h$. *Then*

$$\text{for } h > H(P_X) \quad \Pr\{G^*(\boldsymbol{X}) > \exp(nh)\}$$

$$\text{for } h < H(P_X) \quad \Pr\{G^*(\boldsymbol{X}) < \exp(nh)\}$$

Tail exponents for unconditional guesswork

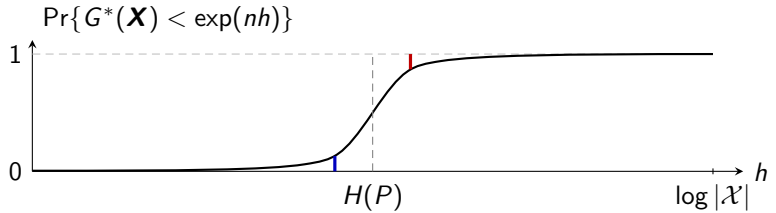


Theorem (no side-information)

Let $0 < h < \log|\mathcal{X}|$ *and* $\lambda_h > 0 : H(P_X^{(\lambda_h)}) = h$. *Then*

$$\left.\begin{array}{ll} \text{for } h > H(P_X) & \Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \\ \text{for } h < H(P_X) & \Pr\{G^*(\boldsymbol{X}) < \exp(nh)\} \end{array}\right\} = \exp\Big\{-nD(P_X^{(\lambda_h)} \,\|\, P_X) + o(n)\Big\}$$

Tail exponents for unconditional guesswork



Theorem (no side-information)

Let $0 < h < \log|\mathcal{X}|$ *and* $\lambda_h > 0 : H(P_X^{(\lambda_h)}) = h \gtrless H(P_X)$. *Then*

$$\Pr\{G^*(\boldsymbol{X}) \gtrless \exp(nh)\} \quad = \exp\Big\{-nD(P_X^{(\lambda_h)} \,\|\, P_X) + o(n)\Big\}$$

Tail exponents for conditional guesswork

$0 < h < \log|\mathcal{X}|, \quad Q_{\boldsymbol{y}} = \text{type of } \boldsymbol{y}$

Tail exponents for conditional guesswork

$0 < h < \log|\mathcal{X}|, \quad Q_{\boldsymbol{y}} = \text{type of } \boldsymbol{y}$

Theorem ("quenched" side-information)

$$\cdots \qquad = h \gtrless \cdots$$

$$\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) \gtrless \exp(nh) \mid \boldsymbol{Y} = \boldsymbol{y}\} = \cdots$$

Theorem ("annealed" side-information)

$$\cdots \qquad = h \gtrless \cdots$$

$$\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) \gtrless \exp(nh)\} = \cdots$$

Tail exponents for conditional guesswork

$0 < h < \log|\mathcal{X}|, \quad Q_{\boldsymbol{y}} = \text{type of } \boldsymbol{y}$

Theorem ("quenched" side-information)

$\lambda_{h,\boldsymbol{y}} > 0 : \quad \cdots \qquad = h \gtrless \cdots$

$$\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) \gtrless \exp(nh) \mid \boldsymbol{Y} = \boldsymbol{y}\} = \exp\Big\{-nD\Big(P_{X|Y}^{(\lambda_{h,\boldsymbol{y}})} \,\|\, P_{X|Y} \mid Q_{\boldsymbol{y}}\Big) + o(n)\Big\}$$

Theorem ("annealed" side-information)

$\cdots \qquad = h \gtrless \cdots$

$$\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) \gtrless \exp(nh)\} = \cdots$$

Tail exponents for conditional guesswork

$0 < h < \log|\mathcal{X}|, \quad Q_{\boldsymbol{y}} = \text{type of } \boldsymbol{y}$

Theorem ("quenched" side-information)

$$\lambda_{h,\boldsymbol{y}} > 0: \quad H_{Q_{\boldsymbol{y}} P_{X|Y}^{(\lambda_{h,\boldsymbol{y}})}}(X \mid Y) = h \gtrless H_{Q_{\boldsymbol{y}} P_{X|Y}}(X \mid Y)$$

$$\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) \gtrless \exp(nh) \mid \boldsymbol{Y} = \boldsymbol{y}\} = \exp\Big\{-nD\Big(P_{X|Y}^{(\lambda_{h,\boldsymbol{y}})} \,\|\, P_{X|Y} \mid Q_{\boldsymbol{y}}\Big) + o(n)\Big\}$$

Theorem ("annealed" side-information)

$$\cdots \qquad\qquad = h \gtrless \cdots$$

$$\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) \gtrless \exp(nh)\} = \cdots$$

Tail exponents for conditional guesswork

$0 < h < \log|\mathcal{X}|, \quad Q_{\boldsymbol{y}} = \text{type of } \boldsymbol{y}$

Theorem ("quenched" side-information)

$\lambda_{h,\boldsymbol{y}} > 0: \quad H_{Q_{\boldsymbol{y}} P_{X|Y}^{(\lambda_{h,\boldsymbol{y}})}}(X \mid Y) = h \gtrless H_{Q_{\boldsymbol{y}} P_{X|Y}}(X \mid Y)$

$$\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) \gtrless \exp(nh) \mid \boldsymbol{Y} = \boldsymbol{y}\} = \exp\Big\{-nD\Big(P_{X|Y}^{(\lambda_{h,\boldsymbol{y}})} \,\|\, P_{X|Y} \mid Q_{\boldsymbol{y}}\Big) + o(n)\Big\}$$

Theorem ("annealed" side-information)

$Q_{Y,\lambda}(y) \propto \cdots$

$\lambda_h > 0: \quad \cdots \qquad\qquad = h \gtrless \cdots$

$$\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) \gtrless \exp(nh)\} = \exp\Big\{-nD\Big(Q_{Y,\lambda_h} P_{X|Y}^{(\lambda_h)} \,\|\, P_{XY}\Big) + o(n)\Big\}$$

Tail exponents for conditional guesswork

$0 < h < \log|\mathcal{X}|, \quad Q_{\boldsymbol{y}} = \text{type of } \boldsymbol{y}$

Theorem ("quenched" side-information)

$$\lambda_{h,\boldsymbol{y}} > 0: \quad H_{Q_{\boldsymbol{y}} P_{X|Y}^{(\lambda_{h,\boldsymbol{y}})}}(X \mid Y) = h \gtrless H_{Q_{\boldsymbol{y}} P_{X|Y}}(X \mid Y)$$

$$\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) \gtrless \exp(nh) \mid \boldsymbol{Y} = \boldsymbol{y}\} = \exp\Big\{-nD\Big(P_{X|Y}^{(\lambda_{h,\boldsymbol{y}})} \,\|\, P_{X|Y} \mid Q_{\boldsymbol{y}}\Big) + o(n)\Big\}$$

Theorem ("annealed" side-information)

$$Q_{Y,\lambda}(y) \propto P_Y(y) \left(\sum_x P_{X|Y}(x \mid y)^\lambda\right)^{1/\lambda}$$

$$\lambda_h > 0: \quad H_{Q_{Y,\lambda_h} P_{X|Y}^{(\lambda_h)}}(X \mid Y) = h \gtrless H(X \mid Y)$$

$$\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) \gtrless \exp(nh)\} = \exp\Big\{-nD\Big(Q_{Y,\lambda_h} P_{X|Y}^{(\lambda_h)} \,\|\, P_{XY}\Big) + o(n)\Big\}$$

Tail exponents for conditional guesswork

$0 < h < \log|\mathcal{X}|, \quad Q_{\boldsymbol{y}} = \text{type of } \boldsymbol{y}$

Theorem ("quenched" side-information)

$$\lambda_{h,\boldsymbol{y}} > 0: \quad H_{Q_{\boldsymbol{y}} P_{X|Y}^{(\lambda_{h,\boldsymbol{y}})}}(X \mid Y) = h \gtrless H_{Q_{\boldsymbol{y}} P_{X|Y}}(X \mid Y)$$

$$\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) \gtrless \exp(nh) \mid \boldsymbol{Y} = \boldsymbol{y}\} = \exp\Big\{-nD\Big(P_{X|Y}^{(\lambda_{h,\boldsymbol{y}})} \,\|\, P_{X|Y} \mid Q_{\boldsymbol{y}}\Big) + o(n)\Big\}$$

Theorem ("annealed" side-information)

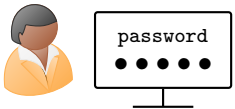
$$Q_{Y,\lambda}(y) \propto P_Y(y) \left(\sum_x P_{X|Y}(x \mid y)^{\lambda}\right)^{1/\lambda} \qquad \longrightarrow \text{dominating } Y\text{-type}$$

$$\lambda_h > 0: \quad H_{Q_{Y,\lambda_h} P_{X|Y}^{(\lambda_h)}}(X \mid Y) = h \gtrless H(X \mid Y)$$

$$\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) \gtrless \exp(nh)\} = \exp\Big\{-nD\Big(Q_{Y,\lambda_h} P_{X|Y}^{(\lambda_h)} \,\|\, P_{XY}\Big) + o(n)\Big\}$$

Application: security against password guessing

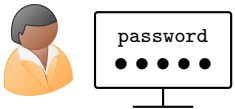
x



Application: security against password guessing

$$X$$

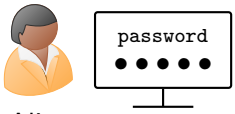
$$P_X(x_i) \propto i^{-0.8} \text{ on } |\mathcal{X}| = 100$$



Application: security against password guessing

$$X$$

$$P_X(x_i) \propto i^{-0.8} \text{ on } |\mathcal{X}| = 100$$



Alice



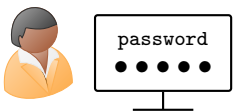
Bob

Application: security against password guessing

$P_{Y|X}$ = erase w.p. $1/2$

X ---------- Y

$P_X(x_i) \propto i^{-0.8}$ on $|\mathcal{X}| = 100$



Alice



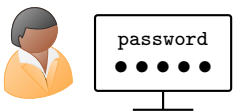
Bob

Application: security against password guessing

d9ZYbLzB $\quad P_{Y|X} =$ erase w.p. $1/2$ $\quad$ _9ZYb__B

X ----------> Y

$P_X(x_i) \propto i^{-0.8}$ on $|\mathcal{X}| = 100$

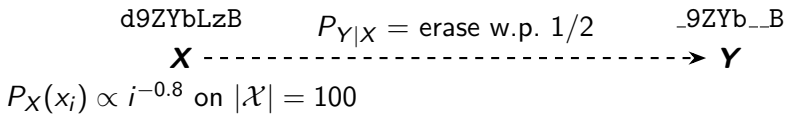


Alice

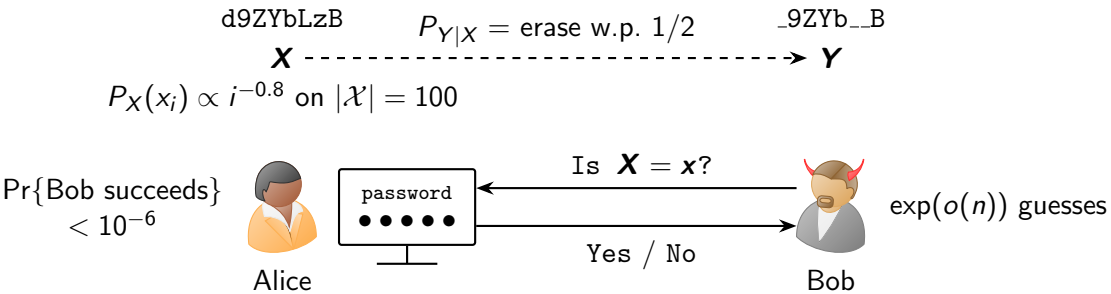


Bob

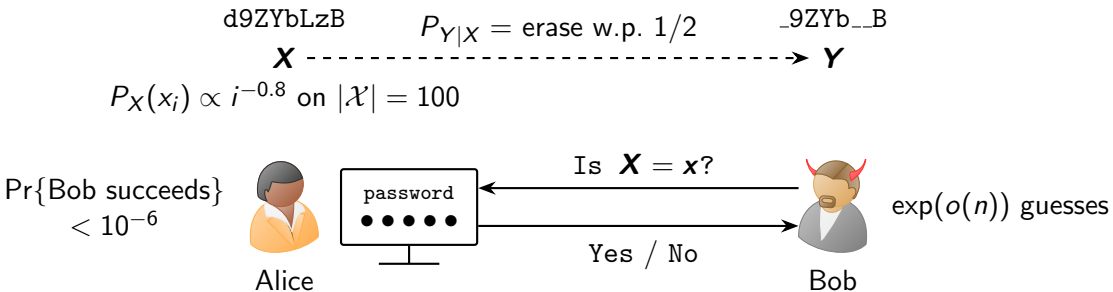
Application: security against password guessing



Application: security against password guessing

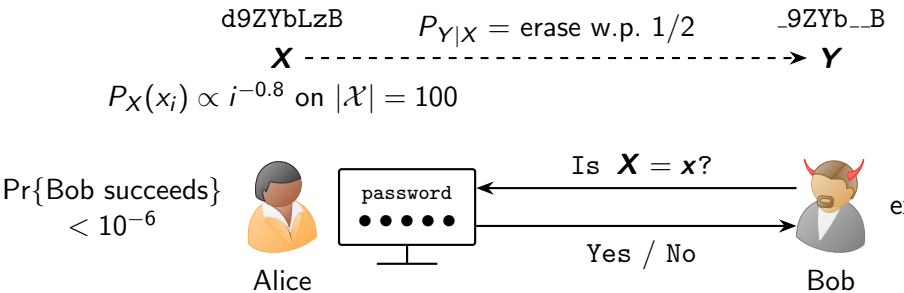


Application: security against password guessing



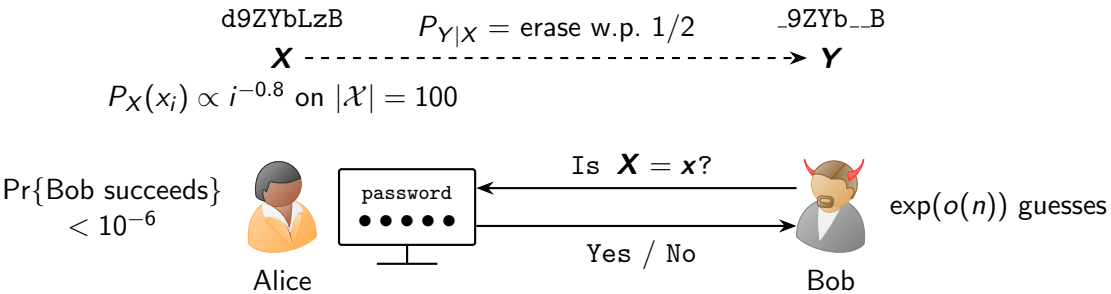
- $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) < \exp(n \cdot 0^+)\} \leq 10^{-6}$ needs $n \gtrsim 24$

Application: security against password guessing



- $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) < \exp(n \cdot 0^+)\} \leq 10^{-6}$ needs $n \gtrsim 24$
- $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) < \exp(n \cdot 0^+) \mid \boldsymbol{Y} = \boldsymbol{y}\} \leq 10^{-6}$ for $Q_{\boldsymbol{y}}(_) = 1/2$ needs $n \gtrsim 14$

Application: security against password guessing



- $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) < \exp(n \cdot 0^+)\} \leq 10^{-6}$ needs $n \gtrsim 24$
- $\Pr\{G^*(\boldsymbol{X} \mid \boldsymbol{Y}) < \exp(n \cdot 0^+) \mid \boldsymbol{Y} = \boldsymbol{y}\} \leq 10^{-6}$ for $Q_{\boldsymbol{y}}(_) = 1/2$ needs $n \gtrsim 14$
- reason: Q_{Y,λ_0} = "dominating $Q_{\boldsymbol{y}}$" has $\sim 89\%$ chars. revealed, not 50%

Proof sketch for unconditional guesswork

- for $h > H(P_X)$, $\Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \approx \exp\Big\{-nD(P_X^{(\lambda_h)} \,\|\, P_X)\Big\}$ at $H(P_X^{(\lambda_h)}) = h$

Proof sketch for unconditional guesswork

- for $h > H(P_X)$, $\Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \approx \exp\Big\{-nD(P_X^{(\lambda_h)} \,\|\, P_X)\Big\}$ at $H(P_X^{(\lambda_h)}) = h$
- type properties:
  - $P_X^n(\boldsymbol{x}) = \exp\{-n[D(Q_{\boldsymbol{x}}\|P_X) + H(Q_{\boldsymbol{x}})]\}$

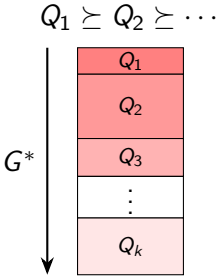
Proof sketch for unconditional guesswork

- for $h > H(P_X)$, $\Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \approx \exp\Big\{-nD(P_X^{(\lambda_h)} \,\|\, P_X)\Big\}$ at $H(P_X^{(\lambda_h)}) = h$
- type properties:
  - $P_X^n(\boldsymbol{x}) = \exp\{-n[D(Q_{\boldsymbol{x}}\|P_X) + H(Q_{\boldsymbol{x}})]\}$

- $Q_i \succeq Q_j : D(Q_i\|P_X) + H(Q_i) \leq D(Q_j\|P_X) + H(Q_j)$

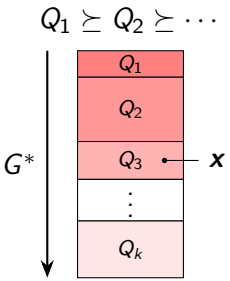
Proof sketch for unconditional guesswork

- for $h > H(P_X)$, $\Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \approx \exp\Big\{-nD(P_X^{(\lambda_h)} \,\|\, P_X)\Big\}$ at $H(P_X^{(\lambda_h)}) = h$
- type properties:
  - $P_X^n(\boldsymbol{x}) = \exp\{-n[D(Q_{\boldsymbol{x}}\|P_X) + H(Q_{\boldsymbol{x}})]\}$
- $Q_i \succeq Q_j : D(Q_i\|P_X) + H(Q_i) \leq D(Q_j\|P_X) + H(Q_j)$



Proof sketch for unconditional guesswork

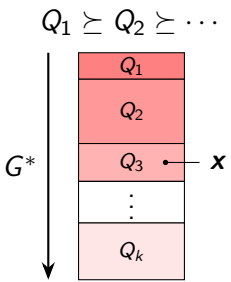
- for $h > H(P_X)$, $\Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \approx \exp\Big\{-nD(P_X^{(\lambda_h)} \,\|\, P_X)\Big\}$ at $H(P_X^{(\lambda_h)}) = h$
- type properties:
  - $P_X^n(\boldsymbol{x}) = \exp\{-n[D(Q_{\boldsymbol{x}}\|P_X) + H(Q_{\boldsymbol{x}})]\}$



- $Q_i \succeq Q_j : D(Q_i\|P_X) + H(Q_i) \leq D(Q_j\|P_X) + H(Q_j)$
- $G^*(\boldsymbol{x}) \approx \sum_{Q' \succeq Q_{\boldsymbol{x}}} |\mathcal{T}_{Q'}^n|$

Proof sketch for unconditional guesswork

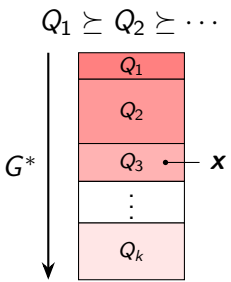
- for $h > H(P_X)$, $\Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \approx \exp\Big\{-nD(P_X^{(\lambda_h)} \,\|\, P_X)\Big\}$ at $H(P_X^{(\lambda_h)}) = h$
- type properties:
  - $P_X^n(\boldsymbol{x}) = \exp\{-n[D(Q_{\boldsymbol{x}}\|P_X) + H(Q_{\boldsymbol{x}})]\}$
  - $|\mathcal{T}_Q^n| \approx \exp\{nH(Q)\}, \quad \#\{\text{types}\} = \text{poly}(n)$



- $Q_i \succeq Q_j : D(Q_i\|P_X) + H(Q_i) \le D(Q_j\|P_X) + H(Q_j)$
- $G^*(\boldsymbol{x}) \approx \sum_{Q' \succeq Q_{\boldsymbol{x}}} |\mathcal{T}_{Q'}^n|$

Proof sketch for unconditional guesswork

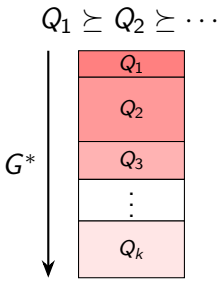
- for $h > H(P_X)$, $\Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \approx \exp\Big\{-nD(P_X^{(\lambda_h)} \,\|\, P_X)\Big\}$ at $H(P_X^{(\lambda_h)}) = h$
- type properties:
  - $P_X^n(\boldsymbol{x}) = \exp\{-n[D(Q_{\boldsymbol{x}}\|P_X) + H(Q_{\boldsymbol{x}})]\}$
  - $|\mathcal{T}_Q^n| \approx \exp\{nH(Q)\}, \quad \#\{\text{types}\} = \text{poly}(n)$



- $Q_i \succeq Q_j : D(Q_i\|P_X) + H(Q_i) \le D(Q_j\|P_X) + H(Q_j)$
- $G^*(\boldsymbol{x}) \approx \sum_{Q' \succeq Q_{\boldsymbol{x}}} |\mathcal{T}_{Q'}^n| \approx \exp\Big\{n \max_{Q' \succeq Q_{\boldsymbol{x}}} H(Q')\Big\}$

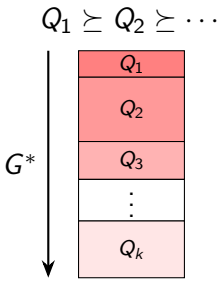
Proof sketch for unconditional guesswork

- for $h > H(P_X)$, $\Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \approx \exp\Big\{-nD(P_X^{(\lambda_h)} \,\|\, P_X)\Big\}$ at $H(P_X^{(\lambda_h)}) = h$
- type properties:
  - $P_X^n(\boldsymbol{x}) = \exp\{-n[D(Q_{\boldsymbol{x}}\|P_X) + H(Q_{\boldsymbol{x}})]\}$
  - $|\mathcal{T}_Q^n| \approx \exp\{nH(Q)\}, \quad \#\{\text{types}\} = \text{poly}(n)$
  - $\Pr\{\boldsymbol{X} \in \mathcal{T}_Q^n\} \approx \exp\{-nD(Q\|P_X)\}$
- $Q_i \succeq Q_j : D(Q_i\|P_X) + H(Q_i) \le D(Q_j\|P_X) + H(Q_j)$
- $G^*(\boldsymbol{x}) \approx \sum_{Q' \succeq Q_{\boldsymbol{x}}} |\mathcal{T}_{Q'}^n| \approx \exp\Big\{n \max_{Q' \succeq Q_{\boldsymbol{x}}} H(Q')\Big\}$



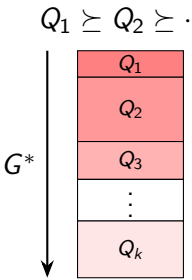
Proof sketch for unconditional guesswork

- for $h > H(P_X)$, $\Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \approx \exp\Big\{-nD(P_X^{(\lambda_h)} \,\|\, P_X)\Big\}$ at $H(P_X^{(\lambda_h)}) = h$
- type properties:
  - $P_X^n(\boldsymbol{x}) = \exp\{-n[D(Q_{\boldsymbol{x}}\|P_X) + H(Q_{\boldsymbol{x}})]\}$
  - $|\mathcal{T}_Q^n| \approx \exp\{nH(Q)\}, \quad \#\{\text{types}\} = \text{poly}(n)$
  - $\Pr\{\boldsymbol{X} \in \mathcal{T}_Q^n\} \approx \exp\{-nD(Q\|P_X)\}$
- $Q_i \succeq Q_j : D(Q_i\|P_X) + H(Q_i) \le D(Q_j\|P_X) + H(Q_j)$
- $G^*(\boldsymbol{x}) \approx \sum_{Q' \succeq Q_{\boldsymbol{x}}} |\mathcal{T}_{Q'}^n| \approx \exp\Big\{n \max_{Q' \succeq Q_{\boldsymbol{x}}} H(Q')\Big\}$
- $-\frac{1}{n}\log \Pr\{G^*(\boldsymbol{X}) > \exp(nh)\}$



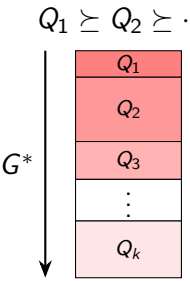
Proof sketch for unconditional guesswork

- for $h > H(P_X)$, $\Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \approx \exp\Big\{-nD(P_X^{(\lambda_h)} \,\|\, P_X)\Big\}$ at $H(P_X^{(\lambda_h)}) = h$
- type properties:
  - $P_X^n(\boldsymbol{x}) = \exp\{-n[D(Q_{\boldsymbol{x}}\|P_X) + H(Q_{\boldsymbol{x}})]\}$
  - $|\mathcal{T}_Q^n| \approx \exp\{nH(Q)\}, \quad \#\{\text{types}\} = \text{poly}(n)$
  - $\Pr\{\boldsymbol{X} \in \mathcal{T}_Q^n\} \approx \exp\{-nD(Q\|P_X)\}$
- $Q_i \succeq Q_j : D(Q_i\|P_X) + H(Q_i) \le D(Q_j\|P_X) + H(Q_j)$
- $G^*(\boldsymbol{x}) \approx \sum_{Q' \succeq Q_{\boldsymbol{x}}} |\mathcal{T}_{Q'}^n| \approx \exp\Big\{n \max_{Q' \succeq Q_{\boldsymbol{x}}} H(Q')\Big\}$
- $-\frac{1}{n}\log \Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \approx \min D(Q\|P_X)$ over $Q : \max_{Q' \succeq Q} H(Q') \ge h$



Proof sketch for unconditional guesswork

- for $h > H(P_X)$, $\Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \approx \exp\Big\{-nD(P_X^{(\lambda_h)} \,\|\, P_X)\Big\}$ at $H(P_X^{(\lambda_h)}) = h$
- type properties:
  - $P_X^n(\boldsymbol{x}) = \exp\{-n[D(Q_{\boldsymbol{x}}\|P_X) + H(Q_{\boldsymbol{x}})]\}$
  - $|\mathcal{T}_Q^n| \approx \exp\{nH(Q)\}, \quad \#\{\text{types}\} = \text{poly}(n)$
  - $\Pr\{\boldsymbol{X} \in \mathcal{T}_Q^n\} \approx \exp\{-nD(Q\|P_X)\}$
- $Q_i \succeq Q_j : D(Q_i\|P_X) + H(Q_i) \le D(Q_j\|P_X) + H(Q_j)$
- $G^*(\boldsymbol{x}) \approx \sum_{Q' \succeq Q_{\boldsymbol{x}}} |\mathcal{T}_{Q'}^n| \approx \exp\Big\{n \max_{Q' \succeq Q_{\boldsymbol{x}}} H(Q')\Big\}$

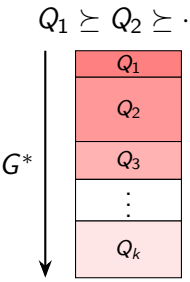


- $-\frac{1}{n}\log\Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \approx \min D(Q\|P_X)$ over $Q : \max_{Q' \succeq Q} H(Q') \ge h$

  $= \min D(Q\|P_X)$ over $Q : H(Q) \ge h$

Proof sketch for unconditional guesswork

- for $h > H(P_X)$, $\Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \approx \exp\Big\{-nD(P_X^{(\lambda_h)} \,\|\, P_X)\Big\}$ at $H(P_X^{(\lambda_h)}) = h$
- type properties:
  - $P_X^n(\boldsymbol{x}) = \exp\{-n[D(Q_{\boldsymbol{x}}\|P_X) + H(Q_{\boldsymbol{x}})]\}$
  - $|\mathcal{T}_Q^n| \approx \exp\{nH(Q)\}, \quad \#\{\text{types}\} = \text{poly}(n)$
  - $\Pr\{\boldsymbol{X} \in \mathcal{T}_Q^n\} \approx \exp\{-nD(Q\|P_X)\}$
- $Q_i \succeq Q_j : D(Q_i\|P_X) + H(Q_i) \le D(Q_j\|P_X) + H(Q_j)$
- $G^*(\boldsymbol{x}) \approx \sum_{Q' \succeq Q_{\boldsymbol{x}}} |\mathcal{T}_{Q'}^n| \approx \exp\Big\{n \max_{Q' \succeq Q_{\boldsymbol{x}}} H(Q')\Big\}$



- $-\frac{1}{n}\log\Pr\{G^*(\boldsymbol{X}) > \exp(nh)\} \approx \min D(Q\|P_X)$ over $Q : \max_{Q' \succeq Q} H(Q') \ge h$
  $= \min D(Q\|P_X)$ over $Q : H(Q) \ge h$
  $= D(P_X^{(\lambda_h)} \,\|\, P_X)$

In short

- method of types gives exponent immediately as a projection problem

In short

- method of types gives exponent immediately as a projection problem
- to solve: instead consider a relaxed version that has the same solution

In short

- method of types gives exponent immediately as a projection problem
- to solve: instead consider a relaxed version that has the same solution, tilted distribution

In short

- method of types gives exponent immediately as a projection problem
- to solve: instead consider a relaxed version that has the same solution, tilted distribution
- hence event $\{G^*(\boldsymbol{X}) \geqslant \exp(nh)\}$ is dominated by $\boldsymbol{x}$ sequences of type $P_X^{(\lambda_h)}$

In short

- method of types gives exponent immediately as a projection problem
- to solve: instead consider a relaxed version that has the same solution, tilted distribution
- hence event $\{G^*(\boldsymbol{X}) \gtrless \exp(nh)\}$ is dominated by $\boldsymbol{x}$ sequences of type $P_X^{(\lambda_h)}$
- similar (but more involved) expressions and interpretation for conditional case

In short

- method of types gives exponent immediately as a projection problem
- to solve: instead consider a relaxed version that has the same solution, tilted distribution
- hence event $\{G^*(\boldsymbol{X}) \gtrless \exp(nh)\}$ is dominated by $\boldsymbol{x}$ sequences of type $P_X^{(\lambda_h)}$
- similar (but more involved) expressions and interpretation for conditional case
- expressions useful, e.g., in password security application

In short

- method of types gives exponent immediately as a projection problem
- to solve: instead consider a relaxed version that has the same solution, tilted distribution
- hence event $\{G^*(\boldsymbol{X}) \gtrcurlyeq \exp(nh)\}$ is dominated by $\boldsymbol{x}$ sequences of type $P_X^{(\lambda_h)}$

- similar (but more involved) expressions and interpretation for conditional case
- expressions useful, e.g., in password security application

Thank you!

arXiv:2608.17949