Bundesamt
für Sicherheit in der
Informationstechnik

Post-processing algorithms for Markov chain models

Johannes Mittmann

(based on joint work with Maciej Skórski)

Bundesamt für Sicherheit in der Informationstechnik (BSI), Germany

European Cyber Week | November 21, 2024 | Rennes, France

Physical true random number generator

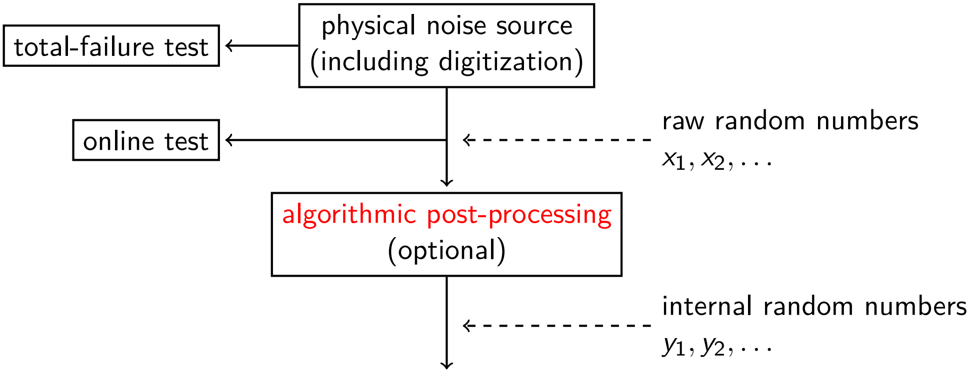


Figure: PTG.2 generator according to AIS 20/31

Algorithmic post-processing

Goal: Increase the entropy per data bit (entropy extraction)

Examples:

- Von Neumann unbiasing
- XOR-ing non-overlapping bits ($\rightarrow$ this talk)
- $\mathbb{F}_2$-linear maps

XOR-ing non-overlapping bits

- Let $x_1, x_2, \ldots \in \{0, 1\}$ be raw random bits and let $n \geq 1$.
- The internal random bits are computed by XOR-ing n non-overlapping bits, i.e.

$$y_j := x_{(j-1)n+1} \oplus \cdots \oplus x_{jn} \in \{0, 1\}, \qquad j \geq 1 .$$

- E.g., for $n = 2$, we have

$$y_1 = x_1 \oplus x_2 , \quad y_2 = x_3 \oplus x_4 , \quad y_3 = x_5 \oplus x_6 , \quad \ldots$$

- Stochastic model: The raw and internal random bits are interpreted as realizations of stochastic processes $X_1, X_2, \ldots$ and $Y_1, Y_2, \ldots$
- Task: Determine a min-entropy lower bound for $Y_1, Y_2, \ldots$

Outline

We consider the following stochastic models for the raw random bits:

1. Bernoulli processes
2. Binary Markov chains

Bernoulli processes

Binary random variables

- A random variable X taking values in $\{0, 1\}$ is called binary.
- It is $B(1, p)$-distributed with parameter $p := \Pr(X = 1) \in [0, 1]$.
- The bias (or imbalance) of X is defined as

$$b := \text{bias}(X) := \mathrm{E}\big((-1)^X\big) = \Pr(X = 0) - \Pr(X = 1) \in [-1, 1] \,.$$

  The parameters p and b are related by $b = 1 - 2p$.
- We have $\mathrm{E}(X) = p$ and $\mathrm{Var}(X) = p(1 - p)$.
- The min-entropy of X is

$$\mathrm{H}_\infty(X) := -\log_2 \max_{x \in \{0,1\}} \Pr(X = x) = -\log_2 \max\{p - 1, p\} = 1 - \log_2(1 + |b|) \,.$$

Bernoulli process

- A Bernoulli process is a sequence of binary random variables $X_1, X_2, \ldots$ that are independent and identically distributed (IID).
- It can be parameterized by $p = \Pr(X_1 = 1)$ or $b = \mathrm{bias}(X_1)$.
- Its min-entropy per bit is

$$\frac{1}{m} \mathrm{H}_\infty(X_1, \ldots, X_m) = \mathrm{H}_\infty(X_1) = 1 - \log_2\big(1 + |b|\big)\,, \qquad m \geq 1\,.$$

XOR-ing independent bits

- Let $X_1, X_2, \ldots$ be a Bernoulli process.
- Let $n \geq 1$ and define

$$Y_j := X_{(j-1)n+1} \oplus \cdots \oplus X_{jn}\,, \qquad j \geq 1\,.$$

- Then $Y_1, Y_2, \ldots$ is again a Bernoulli process.
- It suffices to determine $\text{bias}(Y_1) = \text{bias}(X_1 \oplus \cdots \oplus X_n)$.

Piling-up Lemma for independent bits

Lemma (Matsui 1993)

Let $X_1, \ldots, X_n$ be independent binary random variables. Then

$$\mathrm{bias}(X_1 \oplus \cdots \oplus X_n) = \mathrm{bias}(X_1) \cdots \mathrm{bias}(X_n)\,.$$

Proof: $\mathrm{E}\big((-1)^{X_1 \oplus \cdots \oplus X_n}\big) = \mathrm{E}\big((-1)^{X_1} \cdots (-1)^{X_n}\big) \overset{\text{indep.}}{=} \mathrm{E}\big((-1)^{X_1}\big) \cdots \mathrm{E}\big((-1)^{X_n}\big)$ □

We obtain

$$\frac{1}{m}\,\mathrm{H}_\infty(Y_1, \ldots, Y_m) = \mathrm{H}_\infty(Y_1) = 1 - \log_2\big(1 + |b|^n\big)\,, \qquad m \geq 1\,.$$

Min-entropy of XOR-ed independent bits

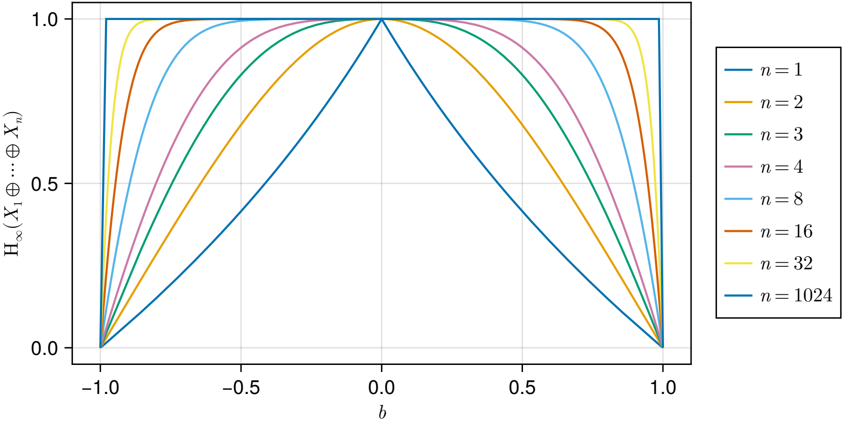


Figure: Min-entropy $H_\infty(Y_1) = H_\infty(X_1 \oplus \cdots \oplus X_n)$ for $b = \text{bias}(X_1)$

Binary Markov chains

Binary Markov chains

- A binary Markov chain is a sequence of binary random variables $X_0, X_1, X_2, \dots$ such that, for all $j \geq 1$ and $x_0, x_1, \dots, x_j \in \{0, 1\}$, we have

$$\Pr(X_j = x_j \mid X_0 = x_0, \dots, X_{j-1} = x_{j-1}) = \Pr(X_j = x_j \mid X_{j-1} = x_{j-1}) \,.$$

- It is determined by
  - the initial distribution $\pi_{x_0} := \Pr(X_0 = x_0)$ and
  - the transition probabilities $P^{(j)}_{x_{j-1},x_j} := \Pr(X_j = x_j \mid X_{j-1} = x_{j-1})$

  and we use the vector/matrix notations

$$\boldsymbol{\pi} = \begin{pmatrix} \pi_0 \\ \pi_1 \end{pmatrix} \qquad \text{and} \qquad \boldsymbol{P}^{(j)} = \begin{pmatrix} P^{(j)}_{0,0} & P^{(j)}_{0,1} \\ P^{(j)}_{1,0} & P^{(j)}_{1,1} \end{pmatrix} .$$

Stationary binary Markov chains

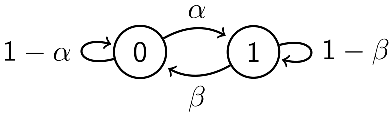
- From now on, let $X_0, X_1, X_2, \ldots$ be a stationary binary Markov chain, i.e. $\boldsymbol{P} := \boldsymbol{P}^{(1)} = \boldsymbol{P}^{(2)} = \ldots$ and $\boldsymbol{\pi}^\top \boldsymbol{P} = \boldsymbol{\pi}^\top$.
- We consider parameters $\alpha, \beta \in (0, 1)$ such that

$$\boldsymbol{\pi} = \frac{1}{\alpha + \beta} \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \qquad \text{and} \qquad \boldsymbol{P} = \begin{pmatrix} 1 - \alpha & \alpha \\ \beta & 1 - \beta \end{pmatrix} .$$

- We define the conditional biases

$$\boldsymbol{b} = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} := \begin{pmatrix} \text{bias}(X_1 \mid X_0 = 0) \\ \text{bias}(X_1 \mid X_0 = 1) \end{pmatrix} = \begin{pmatrix} 1 - 2\alpha \\ 2\beta - 1 \end{pmatrix} .$$

- Graph representation:



Alternative parameterizations

- As before, we define

$$p := \Pr(X_1 = 1) = \frac{\alpha}{\alpha + \beta} \qquad \text{and} \qquad b := \text{bias}(X_1) = \frac{\beta - \alpha}{\alpha + \beta}\,.$$

- Let $\lambda := 1 - \alpha - \beta \in (-1, 1)$.
- We have

$$E(X_j) = p \quad \text{and} \quad \text{Cov}(X_i, X_j) = p(1-p)\lambda^{|i-j|}\,, \qquad i, j \geq 0\,.$$

- A stationary binary Markov chain is a Bernoulli process (IID) iff $\lambda = 0$.

- We can use the parameterizations (α, β), (b_0, b_1), (p, λ), or (b, λ).

Min-entropy rate of Markov chains

- The min-entropy rate of a stationary binary Markov chain is

$$\lim_{m\to\infty} \frac{1}{m} \mathrm{H}_\infty(X_1,\ldots,X_m) = -\log_2 \max\left\{1-\alpha, 1-\beta, (\alpha\beta)^{1/2}\right\}.$$

- The sequence $\left(\frac{1}{m} \mathrm{H}_\infty(X_1,\ldots,X_m)\right)_{m\geq 1}$ is not monotone in general.

Conditional min-entropy

- The (worst-case) conditional min-entropy $\mathrm{H}_\infty(X_m \mid X_0, \ldots, X_{m-1})$ is defined by

$$-\log_2 \max_{x_0,\ldots,x_m \in \{0,1\}} \Pr(X_m = x_m \mid X_0 = x_0, \ldots, X_{m-1} = x_{m-1}) \,.$$

- We have the min-entropy lower bound

$$\frac{1}{m}\mathrm{H}_\infty(X_1, \ldots, X_m) \geq \mathrm{H}_\infty(X_m \mid X_0, \ldots, X_{m-1}) = \mathrm{H}_\infty(X_1 \mid X_0)\,, \quad m \geq 1\,.$$

- We have

$$\mathrm{H}_\infty(X_1 \mid X_0) = -\log_2 \max\{1-\alpha, \alpha, 1-\beta, \beta\} = 1 - \log_2\left(1 + \|\boldsymbol{b}\|_\infty\right)\,,$$

where $\|\boldsymbol{b}\|_\infty = \max\{|b_0|, |b_1|\} = |b(1-\lambda)| + |\lambda|$.

Min-entropy rate vs. conditional min-entropy

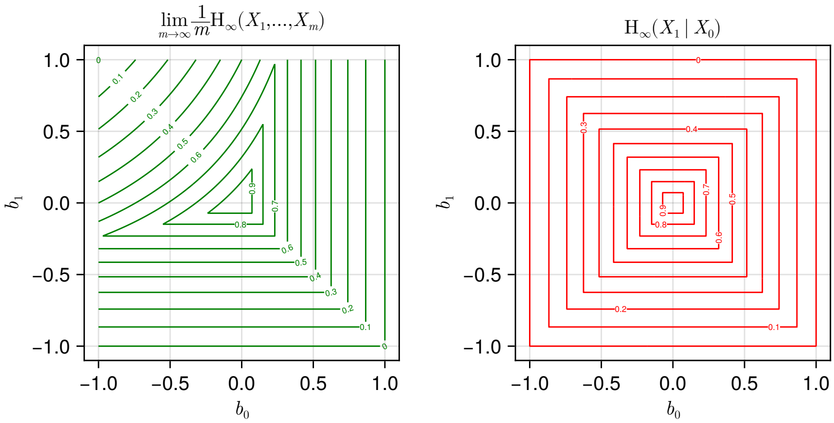


Figure: Contour lines for min-entropy rate and conditional min-entropy

Min-entropy rate vs. conditional min-entropy

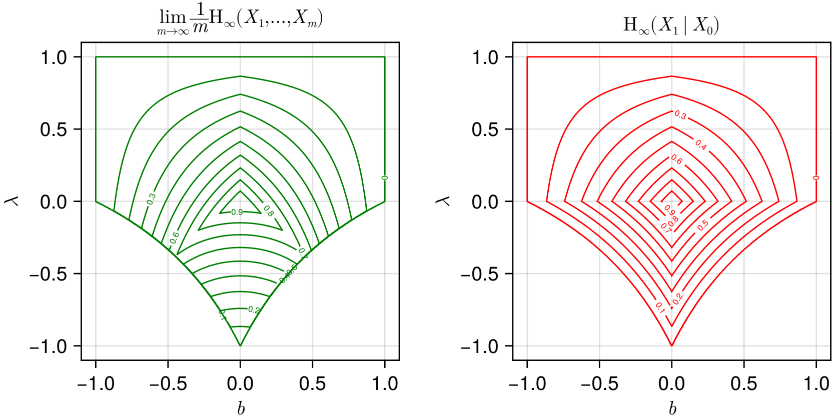


Figure: Contour lines for min-entropy rate and conditional min-entropy

XOR-ing Markovian bits

- Let $X_0, X_1, X_2, \ldots$ be a stationary binary Markov chain.
- Let $n \geq 1$ and define

$$Y_j := X_{(j-1)n+1} \oplus \cdots \oplus X_{jn}\,, \qquad j \geq 1\,.$$

- Then $Y_1, Y_2, \ldots$ is a stationary process, but not Markovian in general.

- Side note: The process $(Y_1, X_n), (Y_2, X_{2n}), \ldots$ is a Markov chain on $\{0,1\}^2$.

Approach for lower bounding the min-entropy of XOR-ed Markovian bits

- We have the min-entropy lower bound

$$\frac{1}{m}\,\mathrm{H}_\infty(Y_1,\ldots,Y_m) \geq \mathrm{H}_\infty(Y_m \mid Y_1,\ldots,Y_{m-1}) \geq \mathrm{H}_\infty(Y_1 \mid X_0)\,, \quad m \geq 1\,.$$

- It suffices to determine

$$\mathrm{H}_\infty(Y_1 \mid X_0) = \mathrm{H}_\infty(X_1 \oplus \cdots \oplus X_n \mid X_0) = 1 - \log_2\bigl(1 + \|\boldsymbol{b}^{(n)}\|_\infty\bigr)\,,$$

where $\boldsymbol{b}^{(n)}$ denotes the conditional biases

$$\boldsymbol{b}^{(n)} := \begin{pmatrix} \mathrm{bias}(X_1 \oplus \cdots \oplus X_n \mid X_0 = 0) \\ \mathrm{bias}(X_1 \oplus \cdots \oplus X_n \mid X_0 = 1) \end{pmatrix}\,.$$

Piling-up Lemma for Markovian bits

Lemma

Let $X_0, X_1, X_2, \ldots$ be a binary Markov chain with initial distribution $\boldsymbol{\pi}$ and transition probabilities $\boldsymbol{P}^{(1)}, \boldsymbol{P}^{(2)}, \ldots$ and denote $\boldsymbol{Z} := \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $\mathbf{1} := \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$.

(a) *We have the conditional biases*

$$\boldsymbol{b}^{(n)} := \begin{pmatrix} \mathrm{bias}(X_1 \oplus \cdots \oplus X_n \mid X_0 = 0) \\ \mathrm{bias}(X_1 \oplus \cdots \oplus X_n \mid X_0 = 1) \end{pmatrix} = \boldsymbol{P}^{(1)} \boldsymbol{Z} \cdots \boldsymbol{P}^{(n)} \boldsymbol{Z} \mathbf{1}\,, \qquad n \geq 0\,.$$

(b) *We have the bias*

$$b^{(n)} := \mathrm{bias}(X_1 \oplus \cdots \oplus X_n) = \boldsymbol{\pi}^\top \boldsymbol{P}^{(1)} \boldsymbol{Z} \cdots \boldsymbol{P}^{(n)} \boldsymbol{Z} \mathbf{1}\,, \qquad n \geq 0\,.$$

This lemma simplifies and generalizes [Simion, 2009].

Min-entropy lower bound for XOR-ed Markovian bits

- We obtain the min-entropy lower bound

$$\frac{1}{m} \mathrm{H}_\infty(Y_1, \dots, Y_m) \geq \mathrm{H}_\infty(Y_1 \mid X_0) = 1 - \log_2\big(1 + \|(\boldsymbol{PZ})^n \mathbf{1}\|_\infty\big) , \quad m \geq 1 .$$

- Special cases:

$$\|\boldsymbol{b}^{(n)}\|_\infty = \|(\boldsymbol{PZ})^n \mathbf{1}\|_\infty = \begin{cases} |b|^n & \text{if } \lambda = 0 \text{ (IID case)} , \\ |\lambda|^{\lfloor (n+1)/2 \rfloor} & \text{if } b = 0 \text{ (unbiased case)} . \end{cases}$$

Further min-entropy lower bounds

- Denote $B_0^{(n)} := \|\boldsymbol{b}^{(n)}\|_\infty = \|(\boldsymbol{PZ})^n\mathbf{1}\|_\infty$.
- Define

$$B_1^{(n)} := \left(|b(1-\lambda)|^2 + \frac{|b(1-\lambda)\lambda|}{|b(1-\lambda)| + |\lambda|} + |\lambda|\right)^m, \qquad \text{if } n = 2m\,,$$

$$B_1^{(n)} := B_1^{(2m)} \cdot \big(|b(1-\lambda)| + |\lambda|\big)\,, \qquad \text{if } n = 2m+1\,.$$

- Define $B_2^{(n)} := \big(\|\boldsymbol{b}\|_\infty\big)^{\lfloor (n+1)/2 \rfloor} = \big(|b(1-\lambda)| + |\lambda|\big)^{\lfloor (n+1)/2 \rfloor}$.
- Then $B_0^{(n)} \leq B_1^{(n)} \leq B_2^{(n)}$ and we obtain the min-entropy lower bounds

$$h_i^{(n)} := 1 - \log_2\big(1 + B_i^{(n)}\big)\,, \qquad i = 0, 1, 2\,,$$

with $h_0^{(n)} \geq h_1^{(n)} \geq h_2^{(n)}$.

Min-entropy lower bounds for XOR-ed Markovian bits

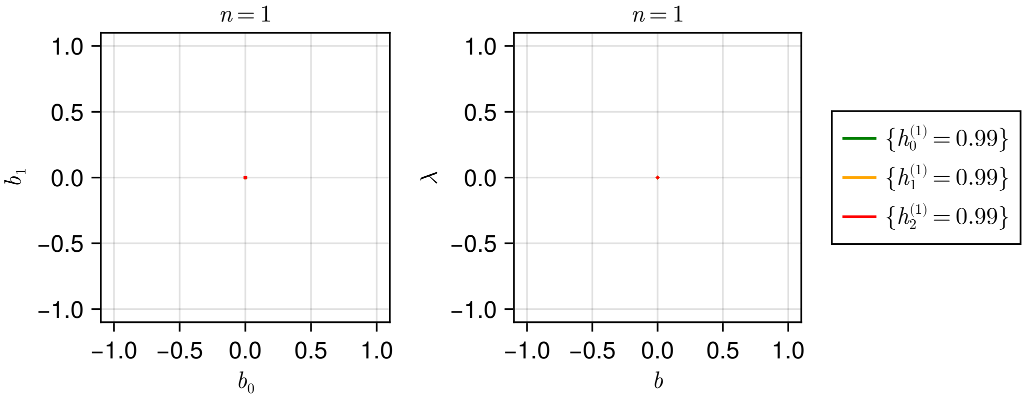


Figure: Contour lines for min-entropy lower bounds of 0.99 bits

Min-entropy lower bounds for XOR-ed Markovian bits

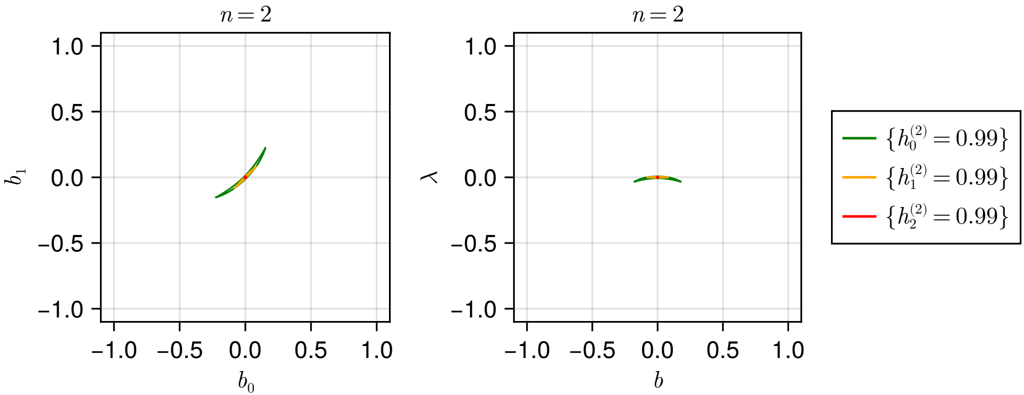


Figure: Contour lines for min-entropy lower bounds of 0.99 bits

Min-entropy lower bounds for XOR-ed Markovian bits

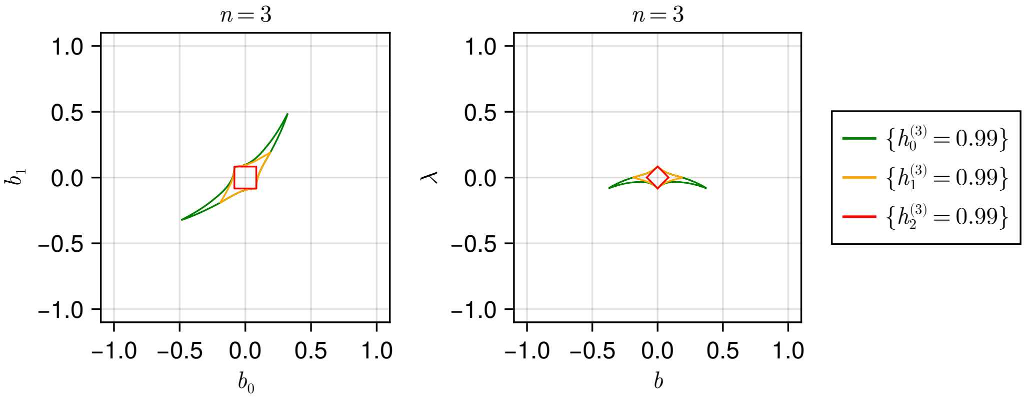


Figure: Contour lines for min-entropy lower bounds of 0.99 bits

Min-entropy lower bounds for XOR-ed Markovian bits

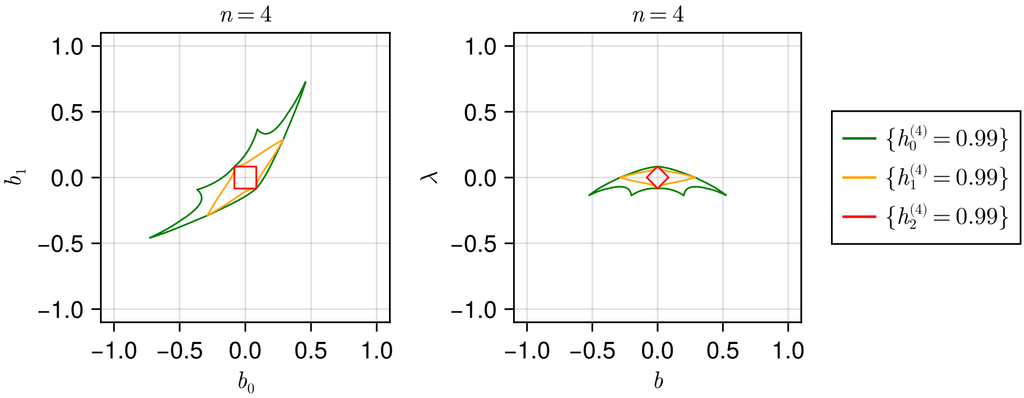


Figure: Contour lines for min-entropy lower bounds of 0.99 bits

Min-entropy lower bounds for XOR-ed Markovian bits

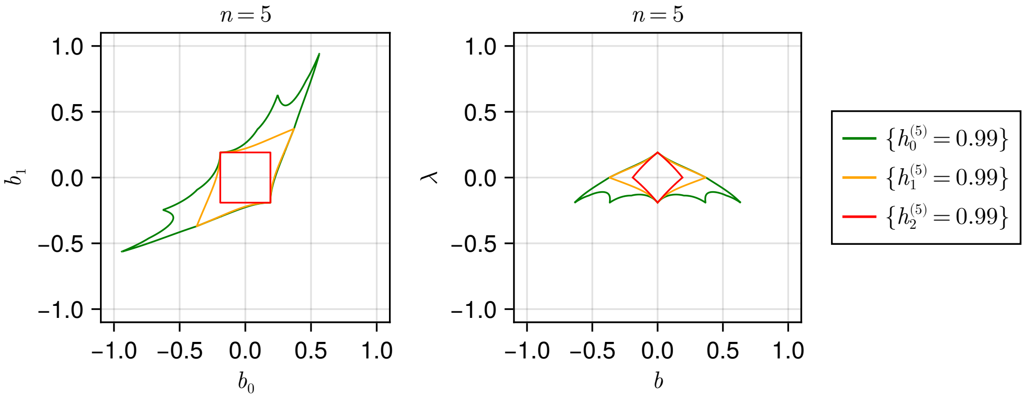


Figure: Contour lines for min-entropy lower bounds of 0.99 bits

Min-entropy lower bounds for XOR-ed Markovian bits

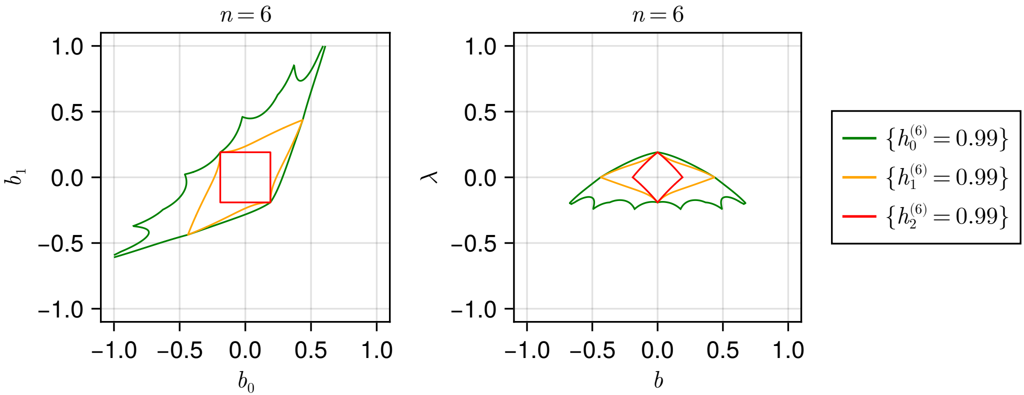


Figure: Contour lines for min-entropy lower bounds of 0.99 bits

Min-entropy lower bounds for XOR-ed Markovian bits

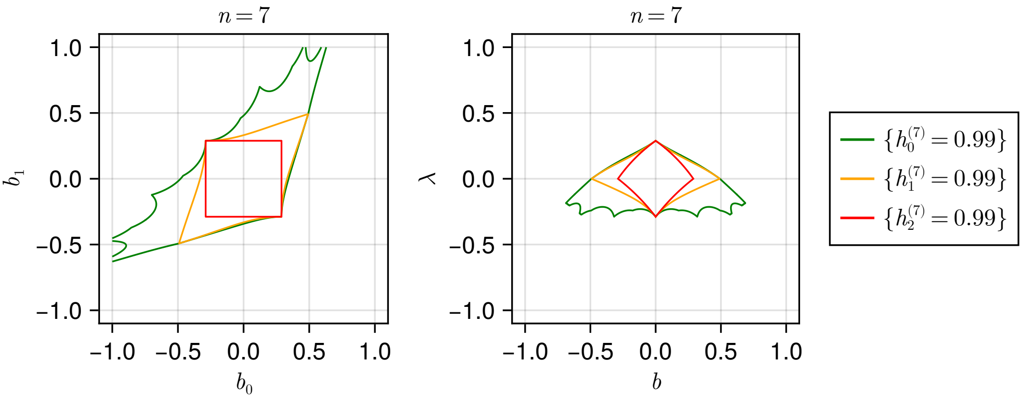


Figure: Contour lines for min-entropy lower bounds of 0.99 bits

Min-entropy lower bounds for XOR-ed Markovian bits

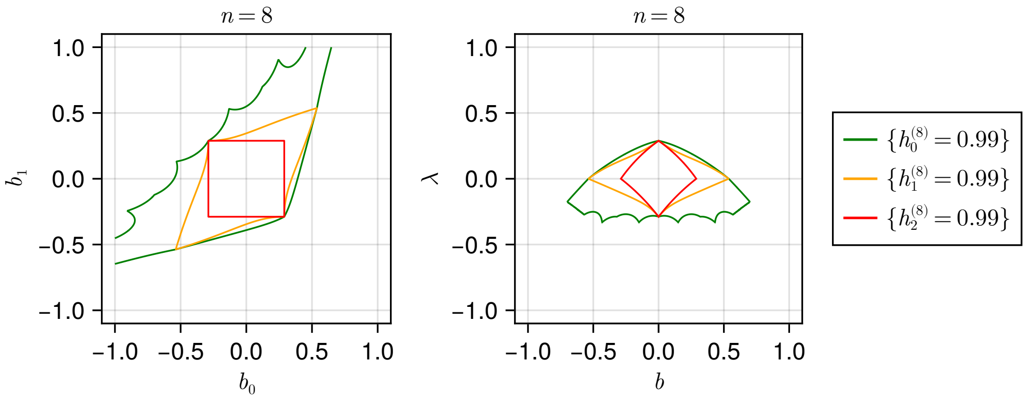


Figure: Contour lines for min-entropy lower bounds of 0.99 bits

Min-entropy lower bounds for XOR-ed Markovian bits

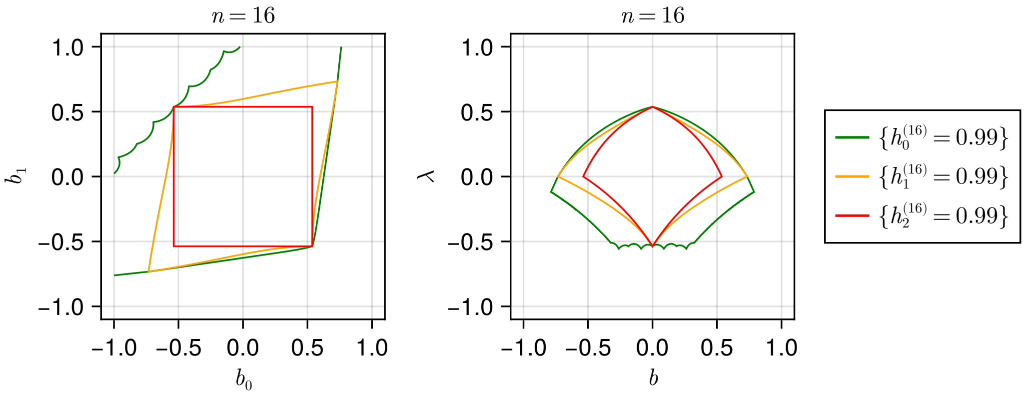


Figure: Contour lines for min-entropy lower bounds of 0.99 bits

Min-entropy lower bounds for XOR-ed Markovian bits

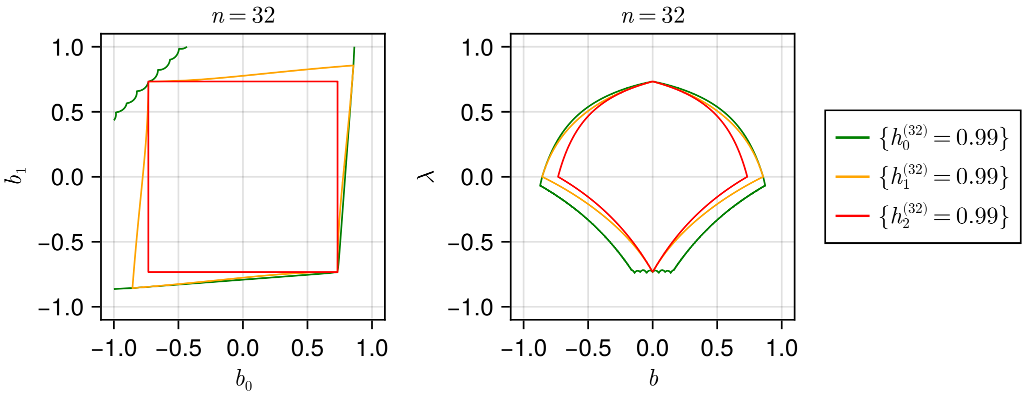


Figure: Contour lines for min-entropy lower bounds of 0.99 bits

Min-entropy lower bounds for XOR-ed Markovian bits

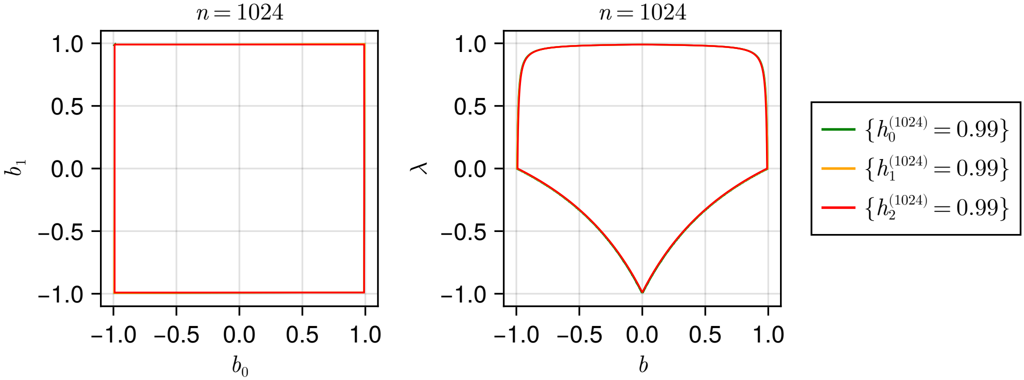


Figure: Contour lines for min-entropy lower bounds of 0.99 bits

Wrap-up

Summary and outlook

- We presented min-entropy lower bounds for XOR-ed Markovian bits.
- The results demonstrate that XOR-ing is robust against small dependencies.

- Work in progress: Generalization for arbitrary $\mathbb{F}_2$-linear post-processing functions

Thank you for your attention!

Questions?

https://www.bsi.bund.de/dok/randomnumbergenerators

ais-20-31@bsi.bund.de

johannes.mittmann@bsi.bund.de