Probabilistic properties of modular addition

Victoria Vysotskaya

JSC "InfoTeCS",
NPK "Kryptonite"

CTCrypt'19 / June 4, 2019

vysotskaya.victory@gmail.com

Definitions

Definition

The table P_n of shape $2^n \times 2^n$ indexed by Δx and Δf with elements $(P_n)_{\Delta x, \Delta f} = P_n(\Delta x, \Delta f)$, where

$$P_n(\Delta x, \Delta f) = \frac{1}{2^{2n}} \left| \{(x, y) \in \mathbb{Z}_{2^n}^2 : \Delta f = f(x \oplus \Delta x, y) \oplus f(x, y)\} \right|$$

and

$$f(x, y) = x \boxplus_n y$$

is called *Differential Distribution Table (DDT)*.

DDT has the following form

$$P_n = \begin{array}{c|ccccc} \Delta x \backslash \Delta f & 0 & \dots & j & \dots & 2^n-1 \\ \hline 0 & \ddots & & \vdots & & \\ \vdots & & \ddots & \vdots & & \\ i & \dots & \dots & P_n(i,j) & & \\ \vdots & & & & & \\ 2^n-1 & & & & & \end{array}$$

$$P_n(i,j) = \frac{1}{2^{2n}} \left| \left\{ (x,y) : j = \left((x \oplus i) \boxplus_n y \right) \oplus \left(x \boxplus_n y \right) \right\} \right|.$$

Previous results [1]

Lemma

Let matrix P_n have the form

$$P_n = \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right].$$

Then matrix P_{n+1} has the form

$$P_{n+1} = \frac{1}{2}\left[\begin{array}{cc|cc} 2A & B & 0 & B \\ C & D & C & D \\ \hline 0 & B & 2A & B \\ C & D & C & D \end{array}\right].$$

[1] Vysotskaya V., Some properties of modular addition (Extended abstract), Cryptology ePrint Archive https://eprint.iacr.org/2018/1103, 2018.

Problem statement

Question

How for a given Δx can we determine the minimum cardinality $K_c(\Delta x)$ of the set of numbers $\Delta f_1, \ldots, \Delta f_{K_c(\Delta x)}$ such that

$$\sum_{i=1}^{K_c(\Delta x)} P_n(\Delta x, \Delta f_i) \geqslant c, \quad 0 < c \leqslant 1 \quad ?$$

Note

Attacker searches for a row with a small value K_c.

Definition

The entropy in i-th row of matrix P_n is defined as

$$H_n^i = -\sum_{j=0}^{2^n-1} P_n(i,j)\log_2 P_n(i,j),\ \ i = 0,\ldots,2^n-1.$$

Hypothesis

$$K_{\frac{1}{2}}(i) \leqslant 2^{H_n^i} \text{ for all } P_n \text{ rows indices } i \in \{0,\ldots,2^n-1\}.$$

Idea

Let's consider value $2^{H_n^i}$ instead of $K_{\frac{1}{2}}(i)$.

Lemma

$$H_{n+1}^i = \begin{cases} H_n^{i \bmod 2^n} + 1, & \text{if } i \in [2^{n-1}, 2^n - 1] \cup [3 \cdot 2^{n-1}, 2^{n+1} - 1], \\ H_n^{i \bmod 2^n} + \beta_n^{i \bmod 2^n}, & \text{if } i \in [0, 2^{n-1} - 1] \cup [2^n, 3 \cdot 2^{n-1} - 1], \end{cases}$$

where

$$\beta_n = \Big[0, \underbrace{\frac{1}{2^{n-1}}}_{1}, \underbrace{\frac{1}{2^{n-2}}, \frac{1}{2^{n-2}}}_{2}, \ldots, \underbrace{\frac{1}{8}, \ldots, \frac{1}{8}}_{2^{n-4}}, \underbrace{\frac{1}{4}, \ldots, \frac{1}{4}}_{2^{n-3}}, \underbrace{\frac{1}{2}, \ldots, \frac{1}{2}}_{2^{n-2}}\Big].$$

Theorem

$$\mathbb{E}H_n = \frac{2}{3}n + O(1) \text{ as } n \to \infty.$$

Corollary

$$\mathbb{E}2^{qH_n} = \Omega\left(2^{\frac{2}{3}nq}\right).$$

Theorem

There exist two sequences of recurrence relations

$$\check{F}_k(n) = \sum_{\ell=1}^{k+1} \check{\alpha}_{k,\ell} \check{F}_k(n-\ell) \quad \textit{and} \quad \hat{F}_k(n) = \sum_{\ell=1}^{k+1} \hat{\alpha}_{k,\ell} \hat{F}_k(n-\ell)$$

and two sequences of positive numbers $\check{c}_k, \hat{c}_k$ *such that:*

$$\check{F}_k(n) \lesssim \mathbb{E}2^{qH_n} \lesssim \hat{F}_k(n) \quad \textit{as} \quad n \to \infty$$

and

$$\lim_{n\to\infty} \frac{|\log \check{F}_k(n) - \log \check{F}_k(n)|}{n} \to 0 \quad \textit{as} \quad k \to \infty.$$

Lemma

Characteristic polynomials $\check{H}_k(\lambda)$ *and* $\hat{H}_k(\lambda)$ *of these recurrences:*

1. *have no root in the annulus* $1 < |\lambda| \leqslant 2$, *if* $q = 1$;
2. *have no root* λ *such that* $|\lambda| = 2^{q-1} + 1$, *if* $q > 1$,
3. *have exactly one root* λ *such that* $|\lambda| > 2^{q-1} + 1$, *if* $q > 1$.

Note

Both functions $\hat{H}_k(\lambda)$ *and* $\check{H}_k(\lambda)$ *have a real root on the segment* $[2^q + 1, 3 \cdot 2^q]$ *which can be found by halving the segment. In this case, for* m *steps the root can be found with an accuracy* $O(2^{-m})$.

Lemma

$$\breve{F}_k(n) = \breve{\gamma}_k \breve{y}_k^n + \breve{\rho}_k(n),$$
$$\widehat{F}_k(n) = \widehat{\gamma}_k \widehat{y}_k^n + \widehat{\rho}_k(n),$$

where $\breve{y}_k, \widehat{y}_k$ *are maximum (by the absolute value) roots of polynomials* $\breve{H}_k(\lambda)$ *and* $\widehat{H}_k(\lambda)$ *respectively, and*

$$\breve{\rho}_k(n) = \begin{cases} O(1), & \text{if } q = 1, \\ O\left(\left[2^{q-1}+1\right]^n\right), & \text{otherwise} \end{cases} \quad \text{as } n \to \infty$$

(the same holds for $\widehat{\rho}_k(n)$*).*

Lemma

$$\lim_{k\to\infty} (\widehat{y}_k - \breve{y}_k) = 0.$$

Example

For $0 < \varepsilon < 10^{-4}$

$$\breve{\alpha}_1 \cdot 2^{(0.7265-\varepsilon)n} \lesssim \mathbb{E}2^{H_n} \lesssim \hat{\alpha}_1 \cdot 2^{(0.7265+\varepsilon)n},$$

$$\breve{\alpha}_2 \cdot 2^{(1.5361-\varepsilon)n} \lesssim \mathbb{D}2^{H_n} \lesssim \hat{\alpha}_2 \cdot 2^{(1.5361+\varepsilon)n}.$$

Example

By Chebyshev's inequality

$$\mathbb{P}\left(\left|2^{H_n} - \mathbb{E}2^{H_n}\right| \geqslant u^n \sqrt{\mathbb{D}2^{H_n}}\right) \leqslant \frac{1}{u^{2n}} \to 0 \text{ as } n \to \infty, u > 1.$$

Thus with probability tending to one

$$2^{H_n} \leqslant \mathbb{E}2^{H_n} + u^n \cdot \sqrt{\mathbb{D}2^{H_n}}$$

or, for example,

$$2^{H_n} = o\left(2^{0.76807n}\right) \text{ as } n \to \infty.$$

Note

Last year we proved [1] that matrix' P_n rows are divided into classes of equivalence. Entropy is one and the same for all members of a class.

Lemma

Compact (of size $O(n)$) representations of classes of equivalence may be generated in time proportional to their number. This is

$$\frac{e^{\pi\sqrt{\frac{2n}{3}}}}{2\sqrt{2}\pi\sqrt{n}} = O\left(2^{3,7007\sqrt{n}}\right) \text{ as } n \to \infty.$$

Theorem

For each number i the row of DDT-matrix with this number belongs to the equivalence class of size

$$\rho_i = 2 \cdot C_K^{s-1} C_{s-1}^{c_1} C_{s-1-c_1}^{c_2} \dots C_{s-1-c_1-\dots-c_{r-2}}^{c_{r-1}},$$

where

1. *K is the number of 1's in binary representation of i,*
2. *s is the number of groups of 0's and 1's in i,*
3. *$c_1, c_2, \dots$ is the number of 0's of size $1, 2, \dots$.*

Note

Usually one needs $\Omega(2^{3n})$ *operations to calculate* H_n.
For $n = 32$ *it is* 2^{96} $(\sim 6,4 \cdot 10^{19}$ *sec.*$)$,
for $n = 64$ *it is* 2^{192} $(\sim 4 \cdot 10^{48}$ *sec.*$)$.

But using our approach
for $n = 32$ *it takes 0,1 sec. and*
for $n = 64$ *it takes 62 sec. on a laptop.*

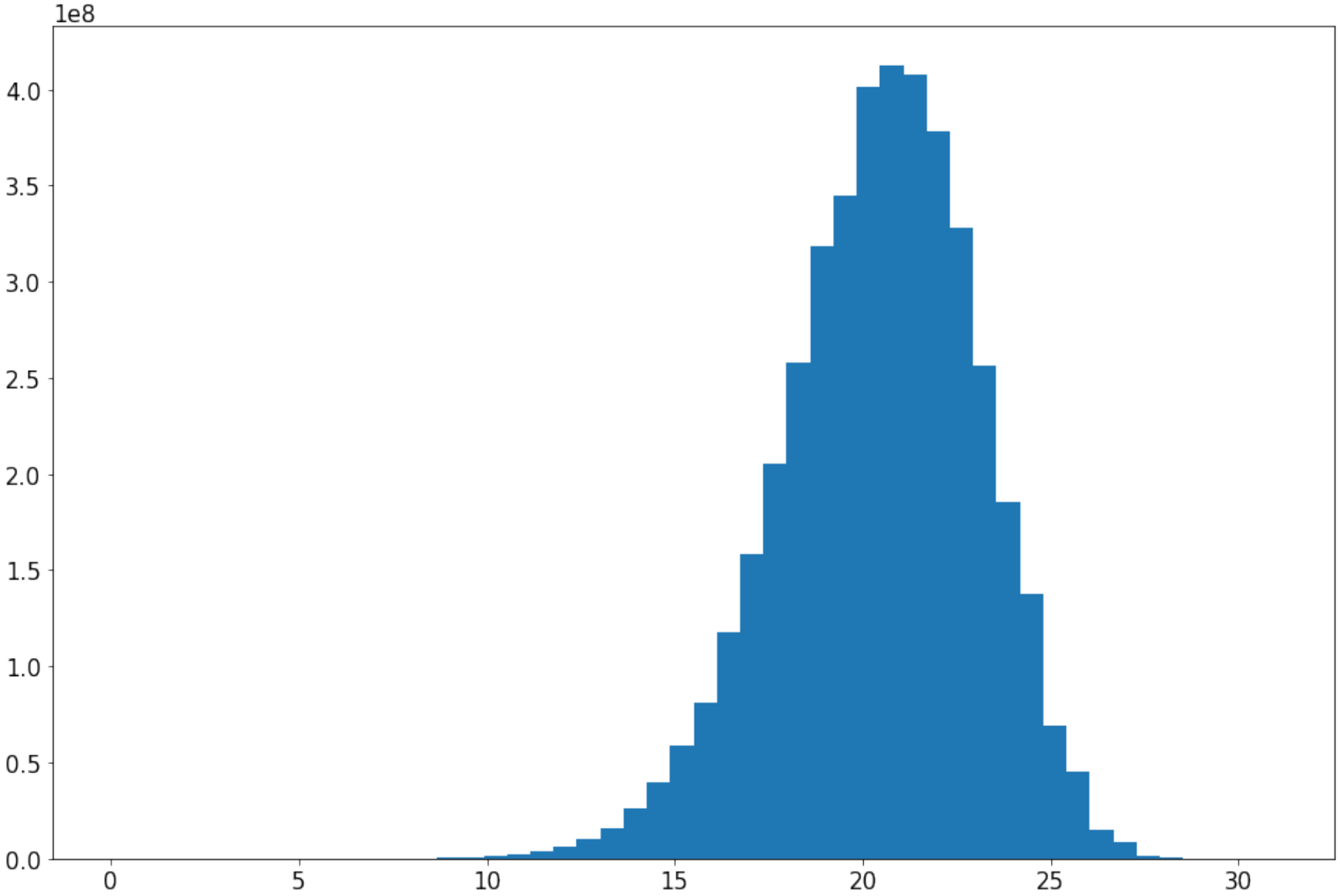

Figure: Distribution of H_{32}

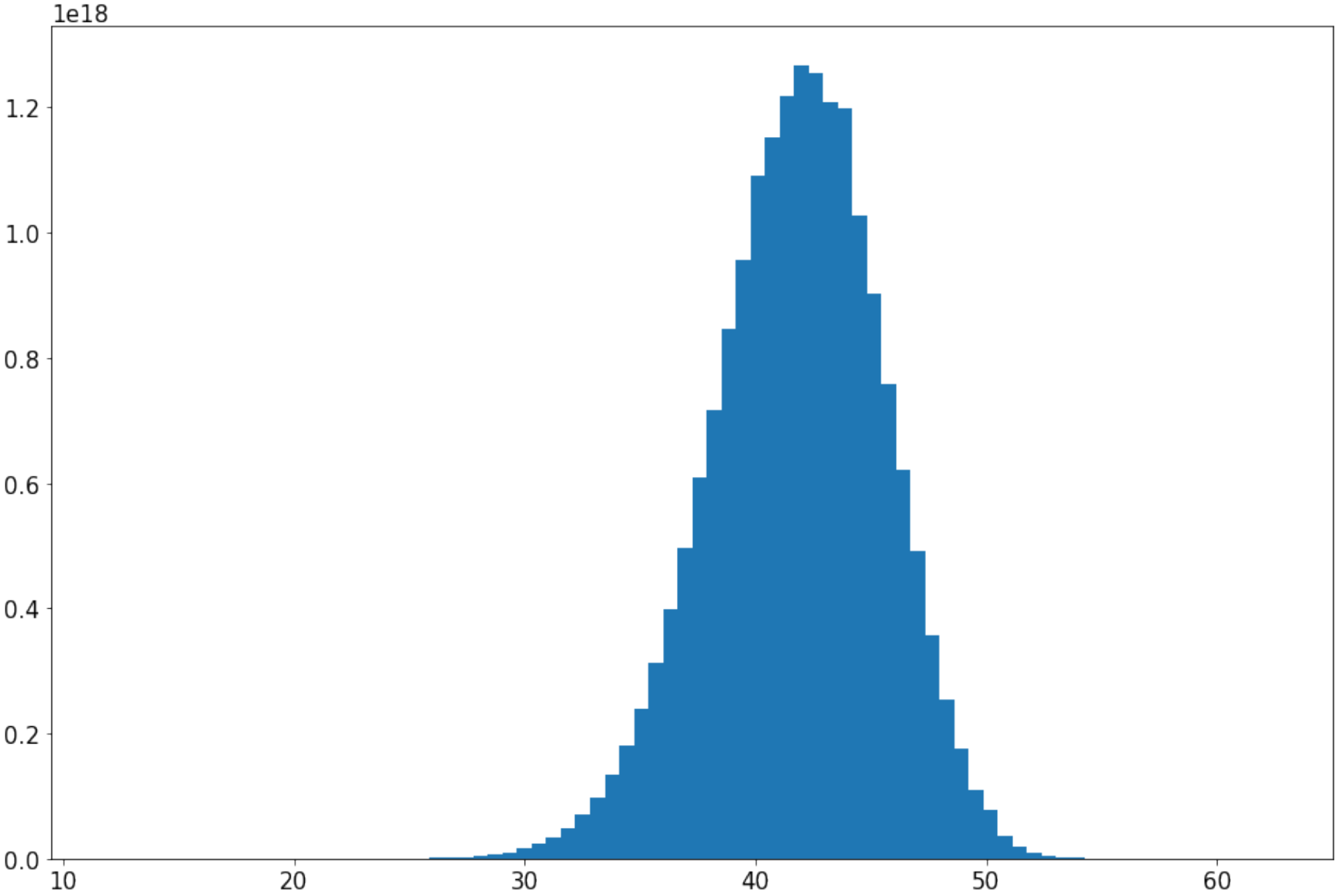

Figure: Distribution of H_{64}

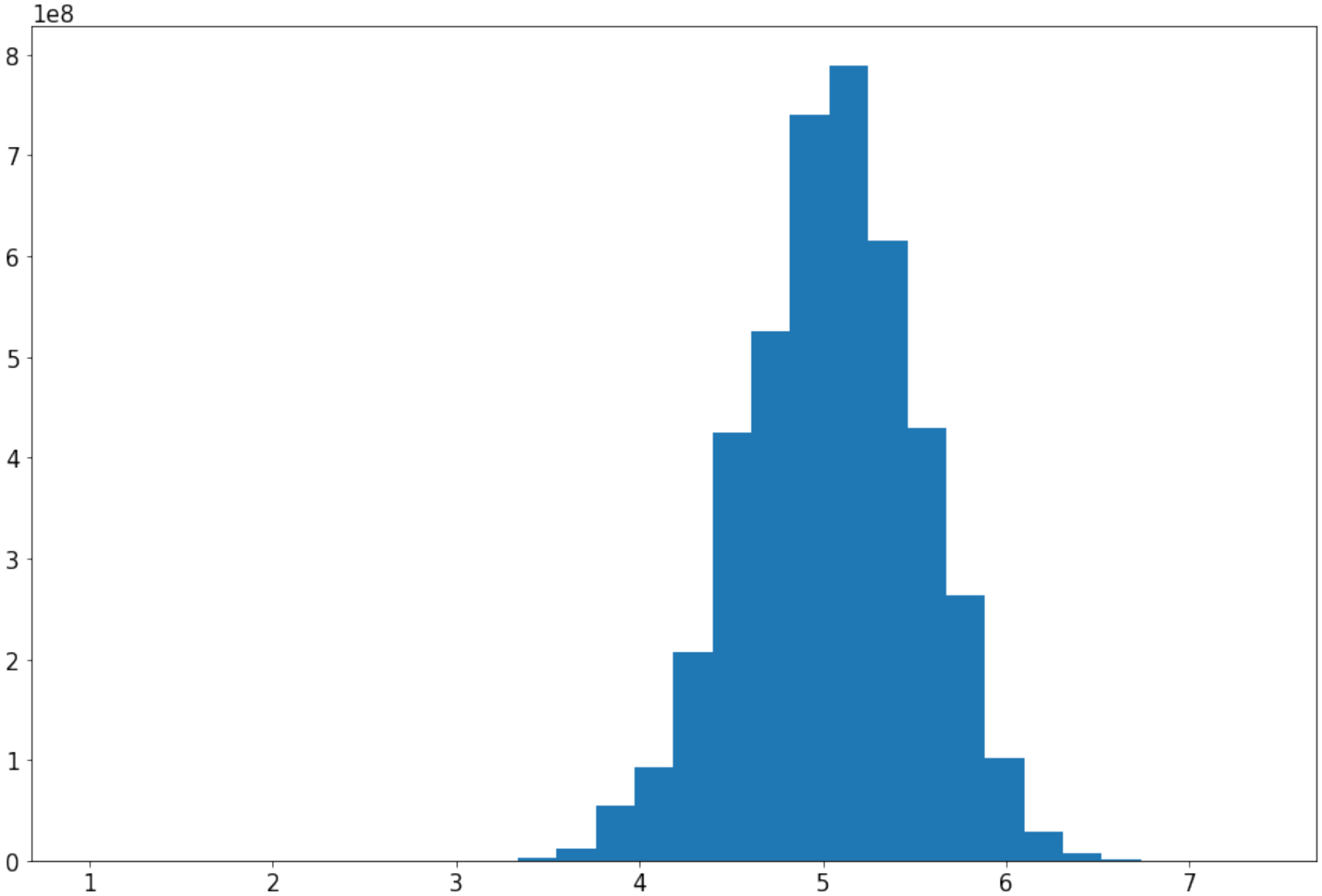

Figure: Distribution of $2^{H_{32}}/K_{\frac{1}{2}}$.

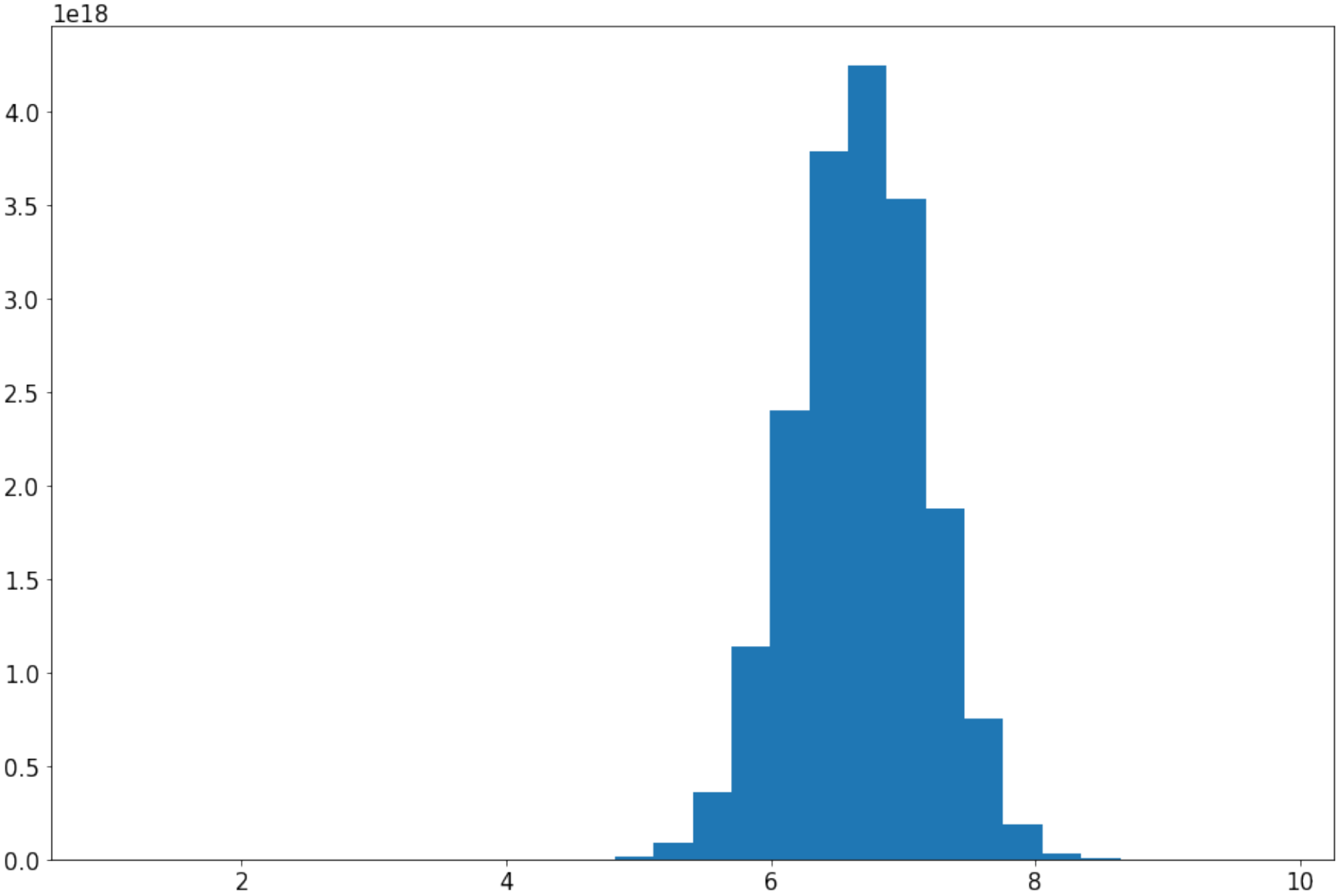

Figure: Distribution of $2^{H_{64}}/K_{\frac{1}{2}}$.

Note

For $n = 32$

theoretical $\mathbb{E}2^{H_n} \sim 9,96 \cdot 10^6$,
computed $\mathbb{E}2^{H_n} \sim 5,40 \cdot 10^6$.

So real value is only 1,8 times smaller than calculated one.

Note

For $n = 32$ *and* $n = 64$ *we showed that*

$$K_{\frac{1}{2}}(i) \leqslant 2^{H_n^i}$$

so our hypothesis is true for them. Besides, the relation

$$2^{H_n^i}/K_{\frac{1}{2}}(i)$$

is small.

Conclusion

In this work we

1. obtained an estimate (accurate up to an additive constant) of expected value of entropy H_n in rows of DDT,
2. proved asymptotic inequalities describing the behavior of values $\mathbb{E}2^{H_n}$ and $\mathbb{D}2^{H_n}$ as long as other moments as $n \to \infty$,
3. checked all results for $n = 32$ and $n = 64$.

Questions?