

ENTROPY FOR QUANDLES

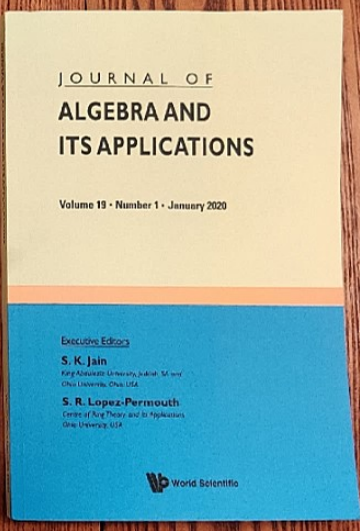
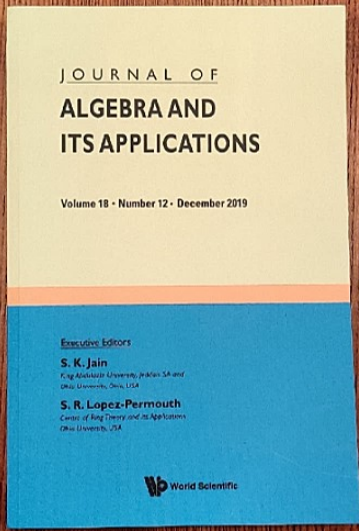
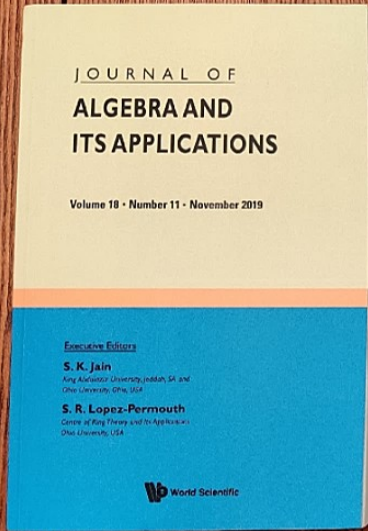
Filippo Spoggiari
Charles University Prague

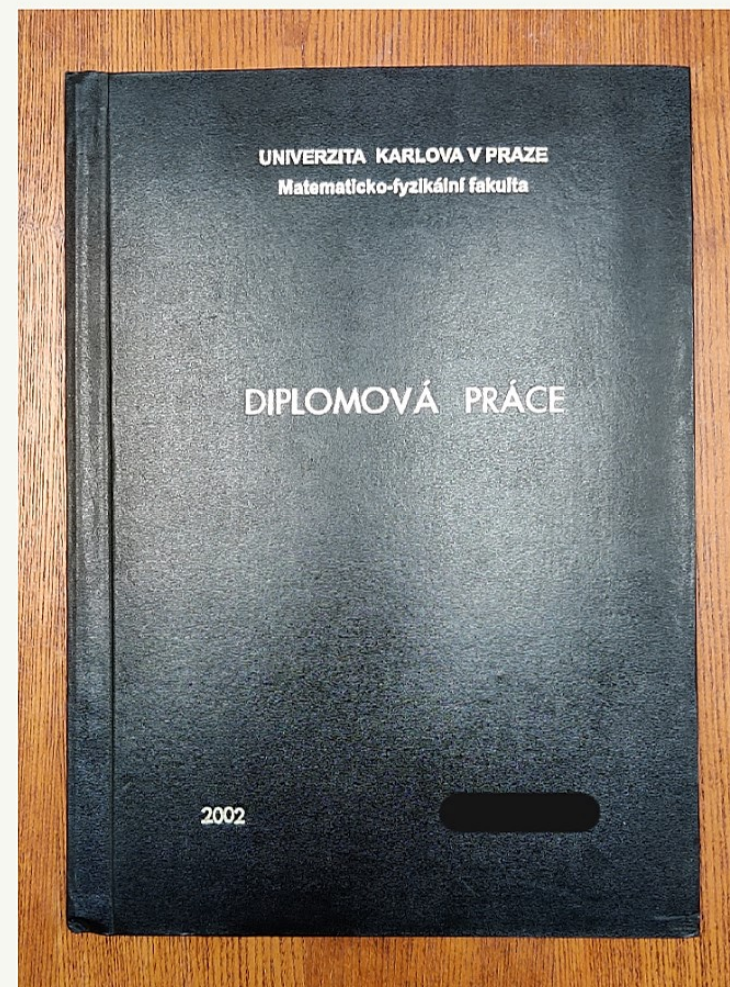
FALL SCHOOL
OF ALGEBRA

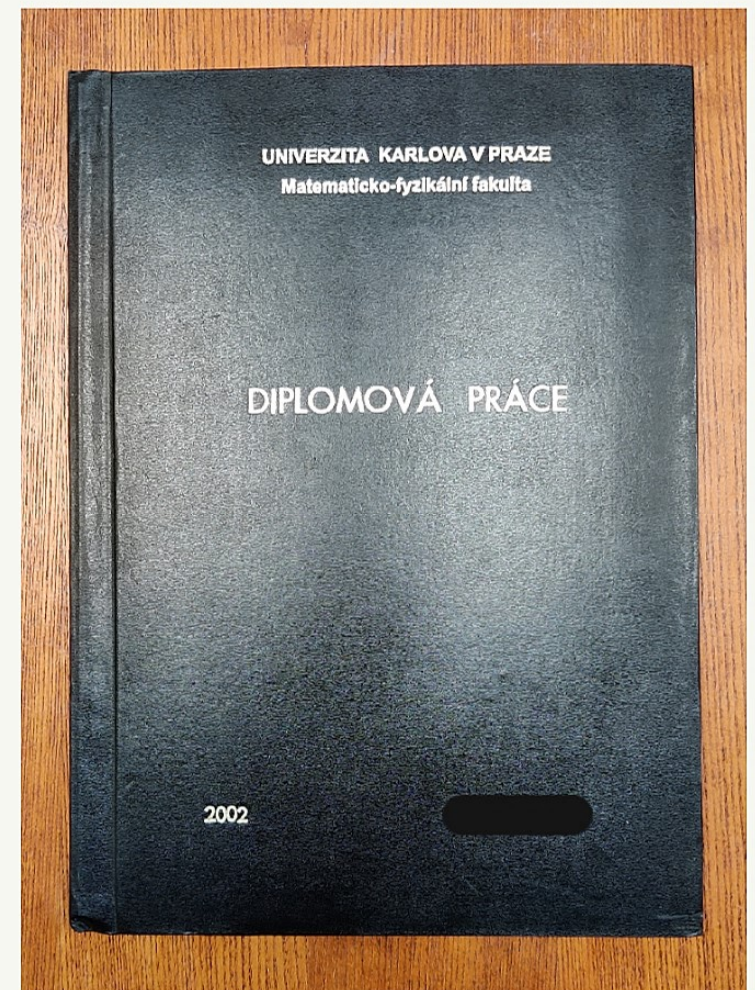
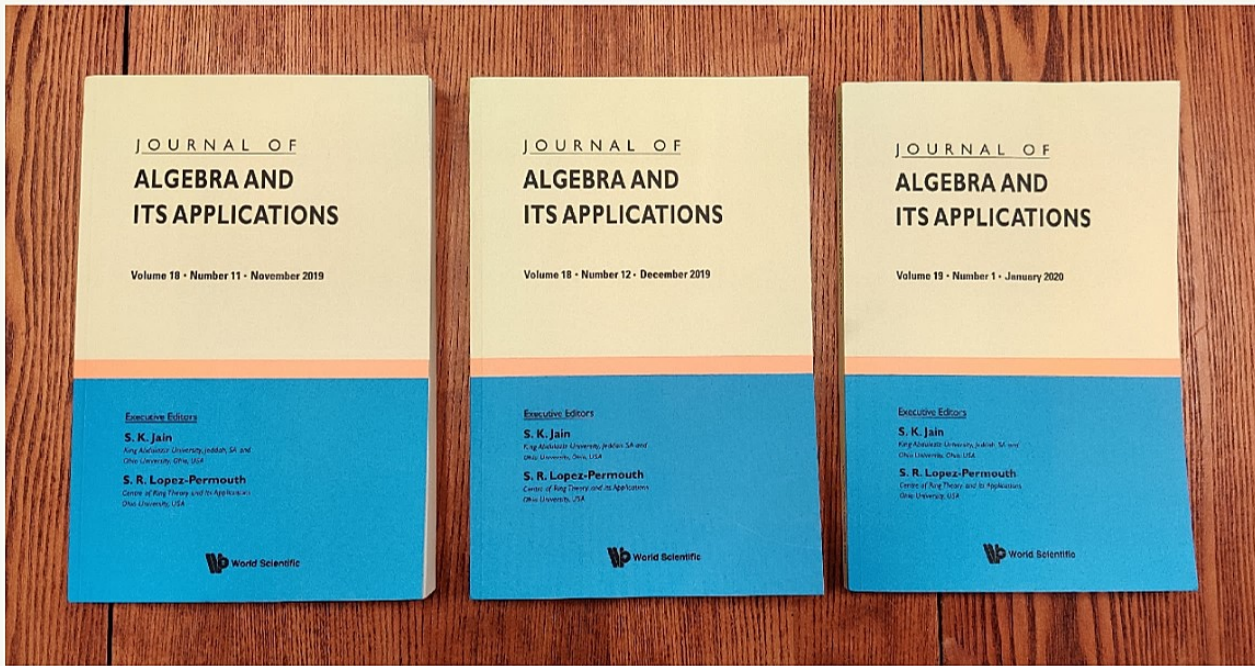
30 NOV - 3 DIC
2023

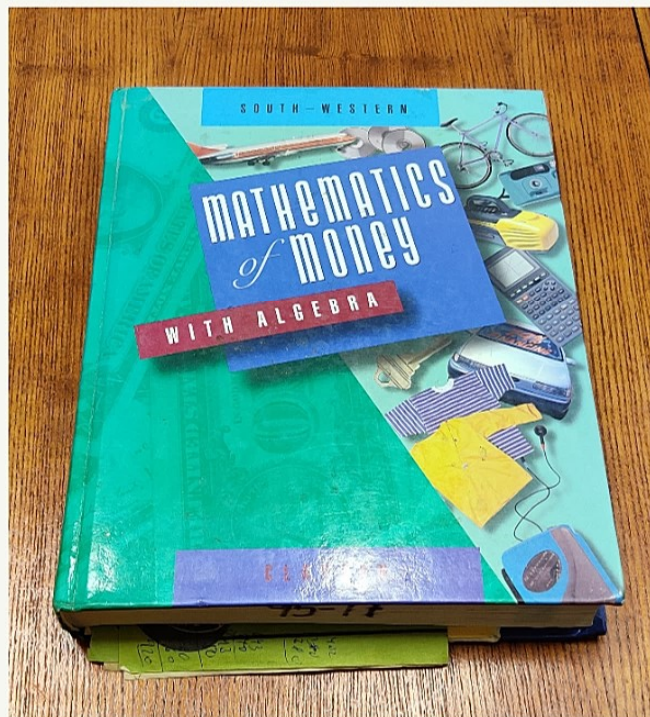
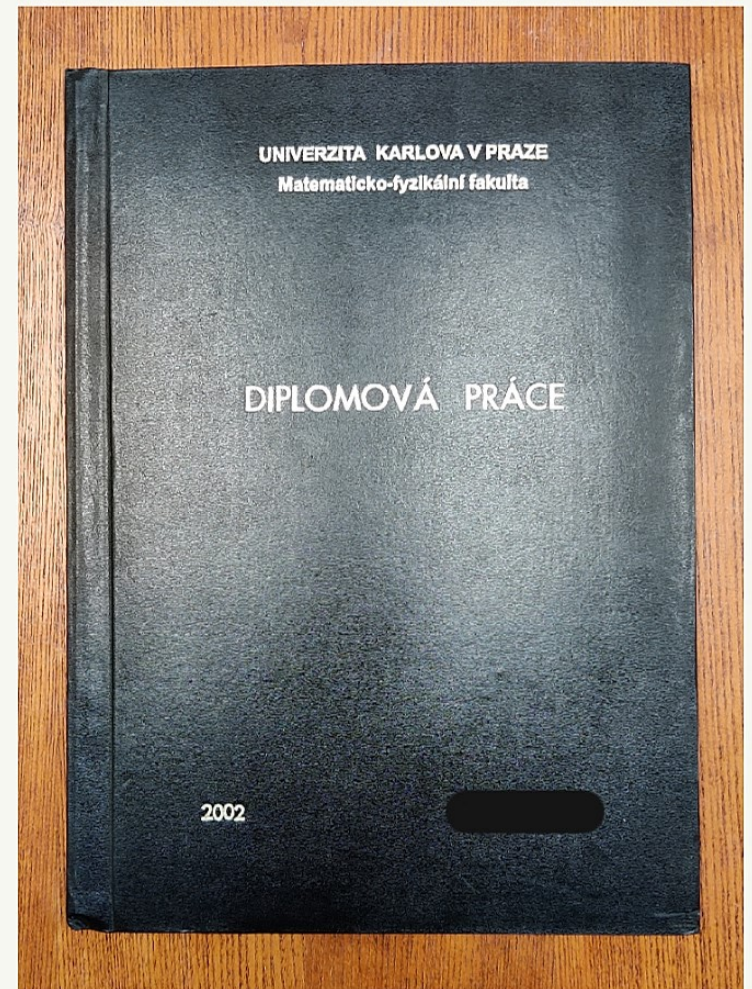
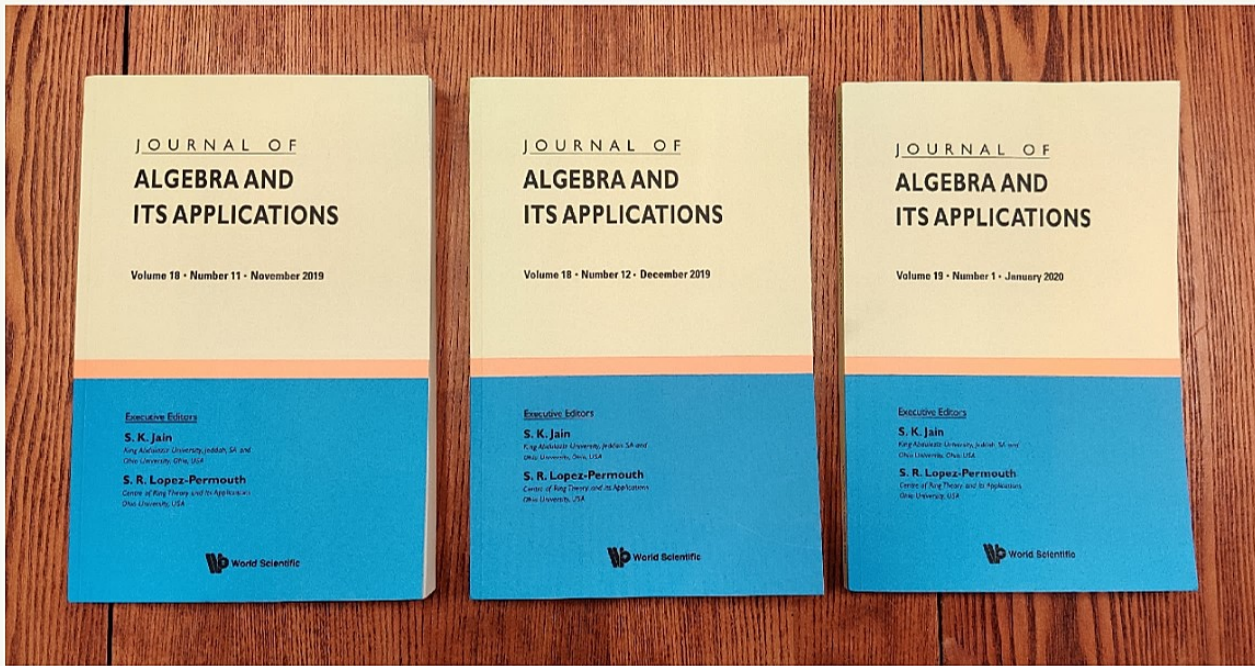


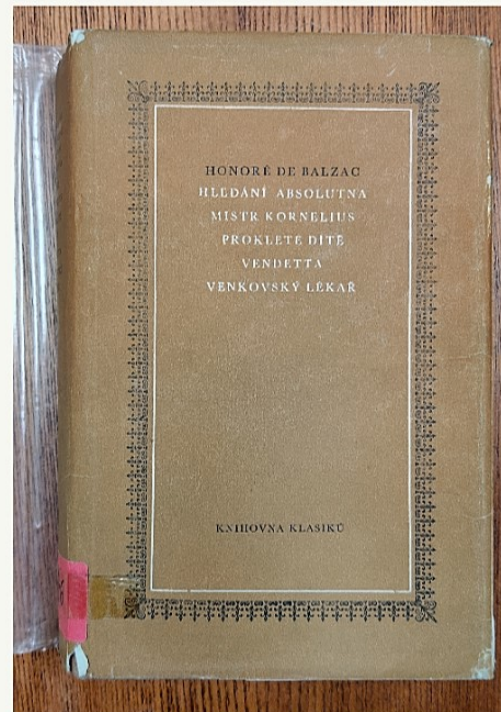
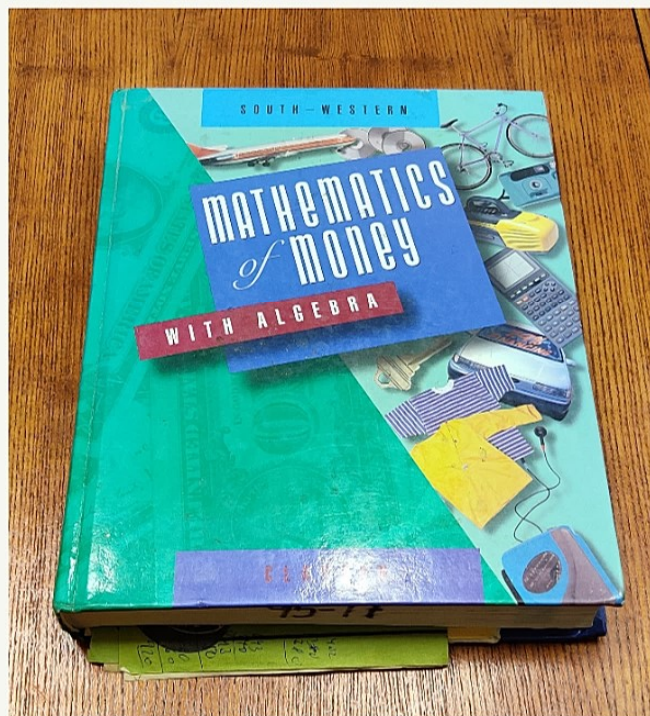
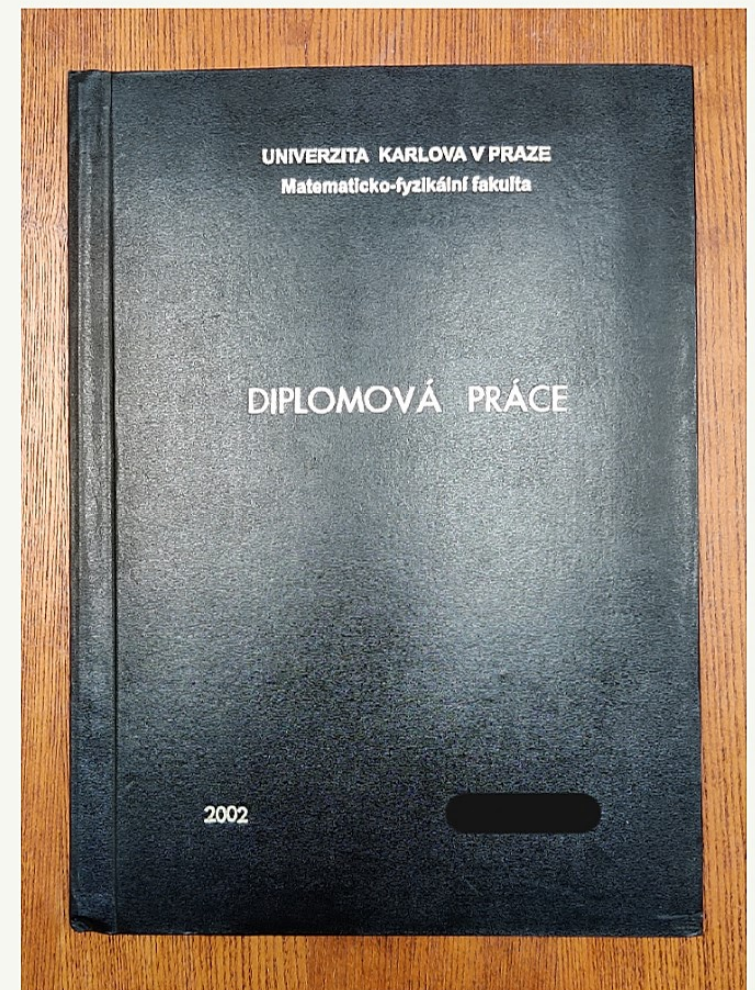
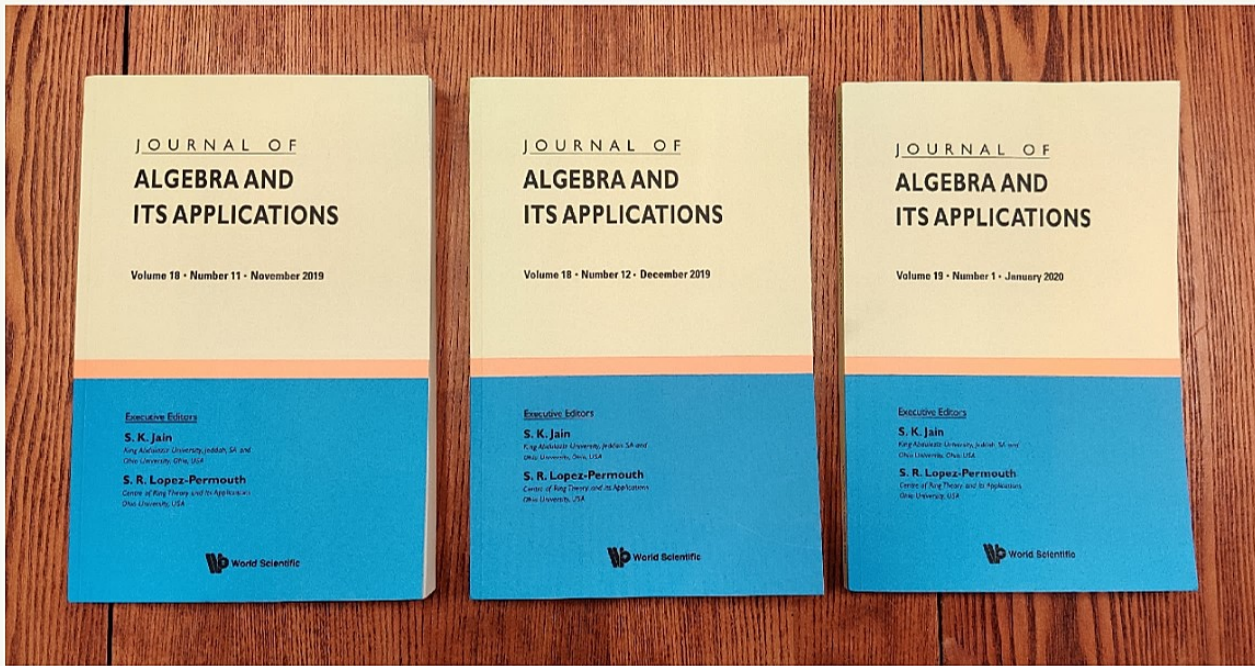
Small Seminar Room - Department of Algebra,
Charles University Prague

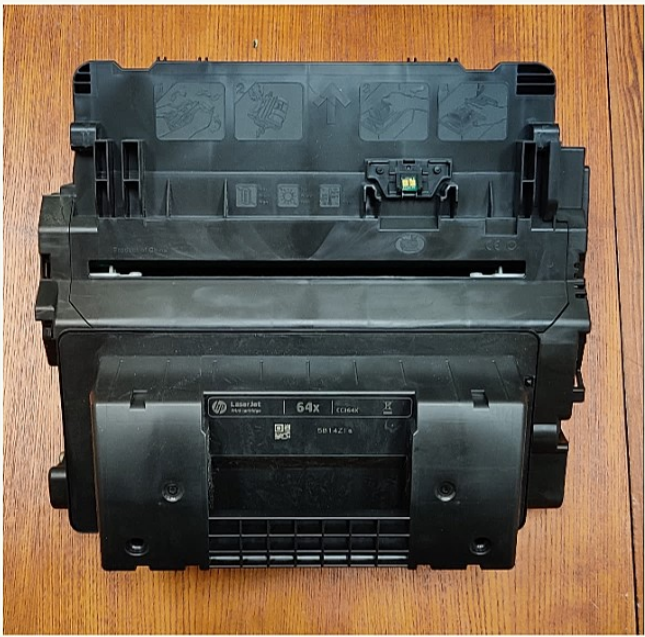


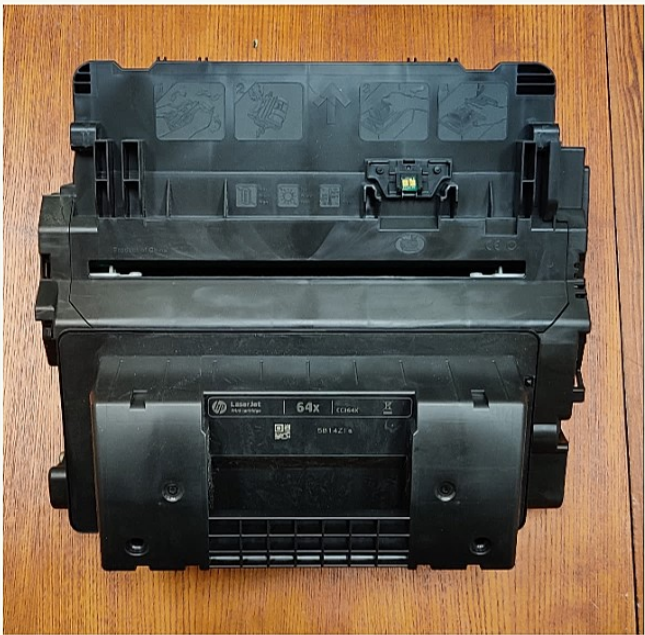


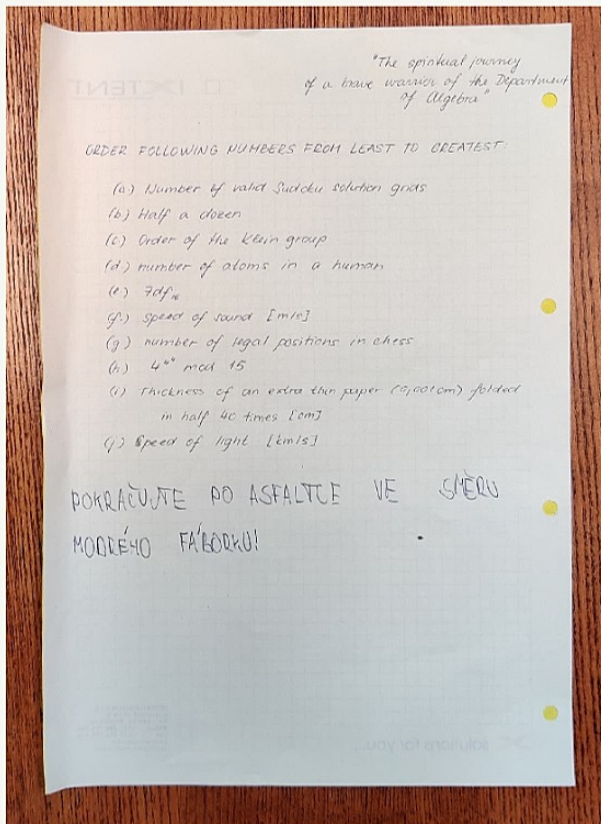
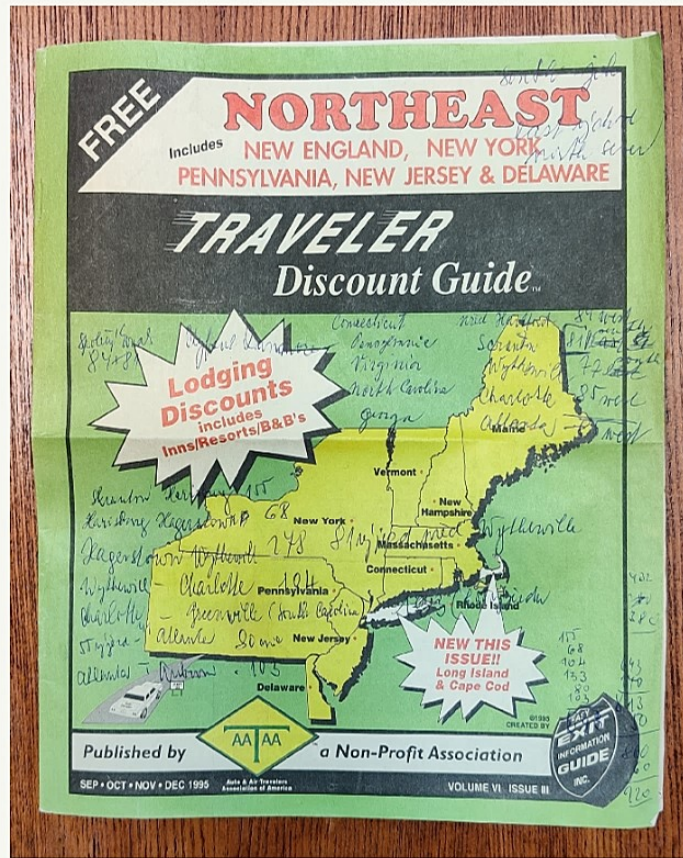
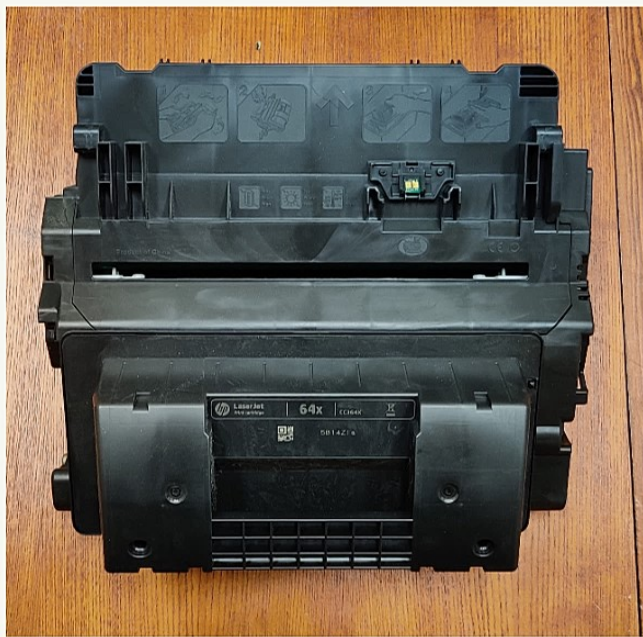


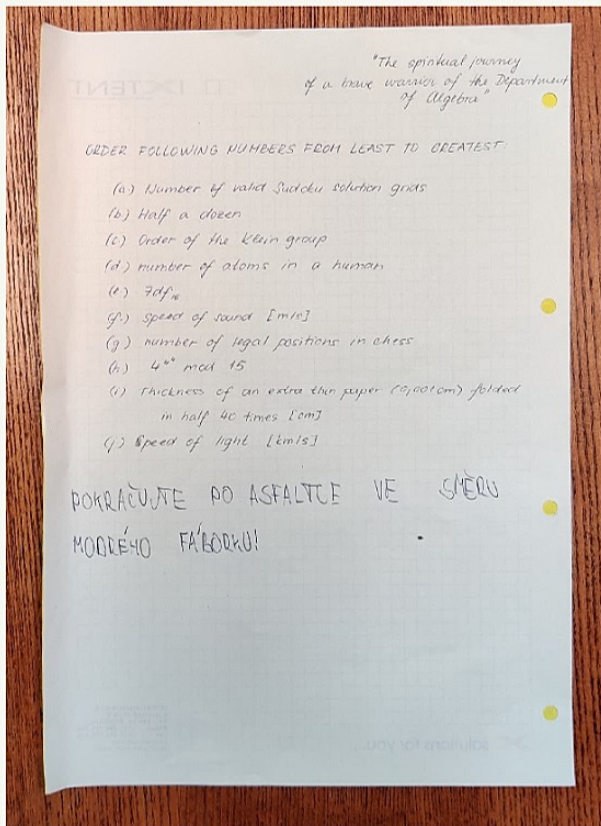
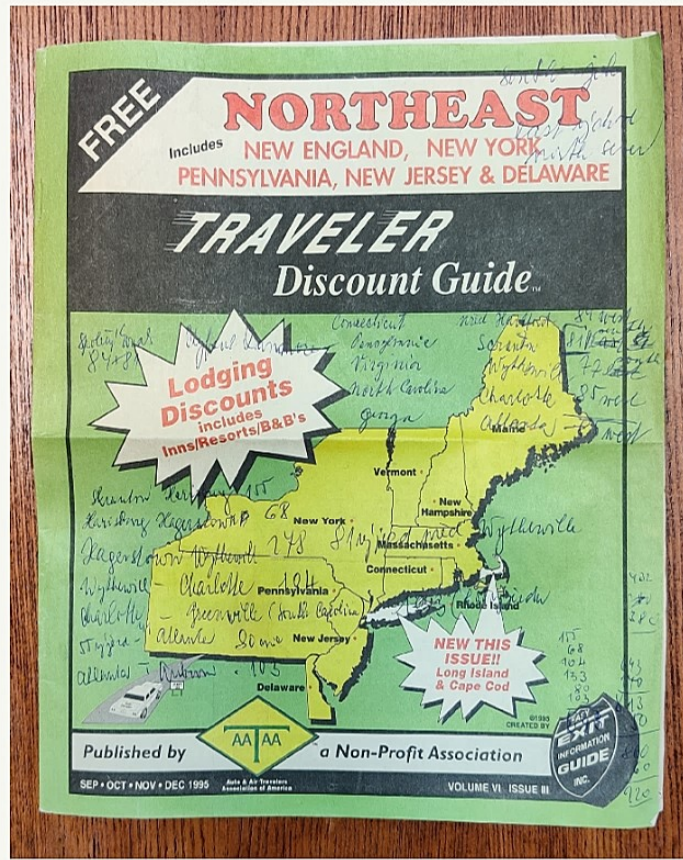
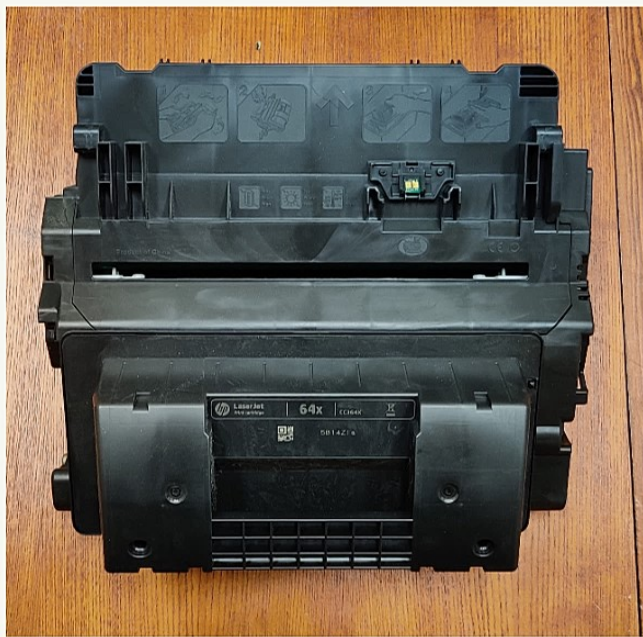






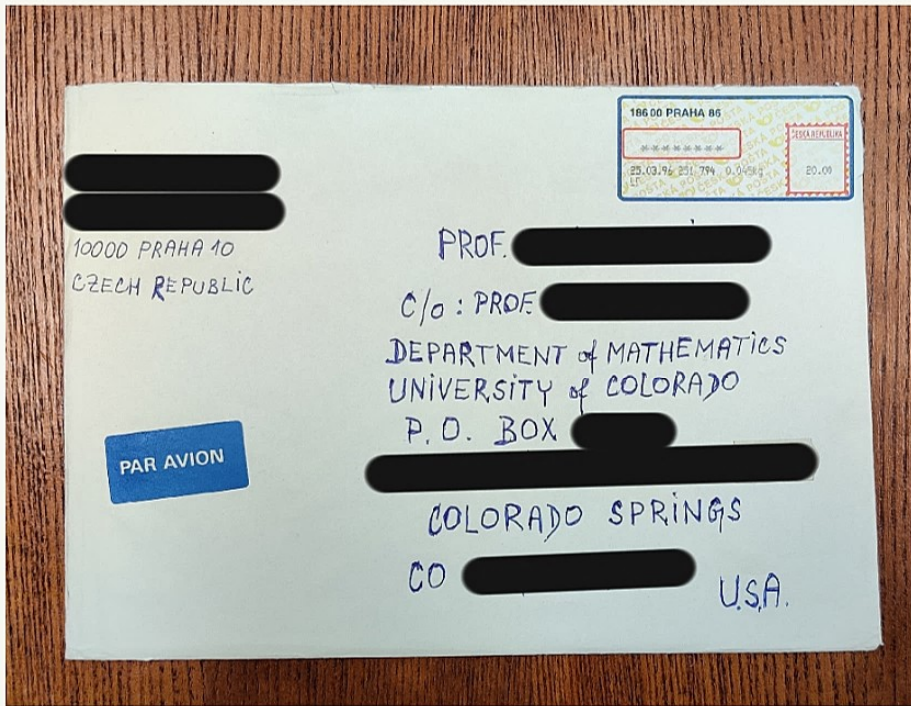


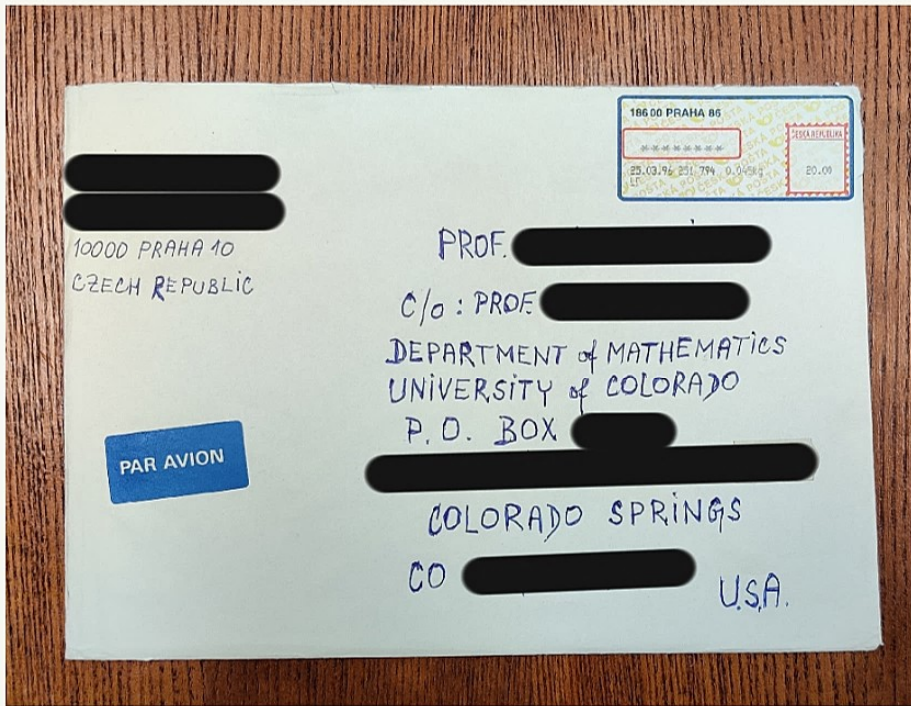


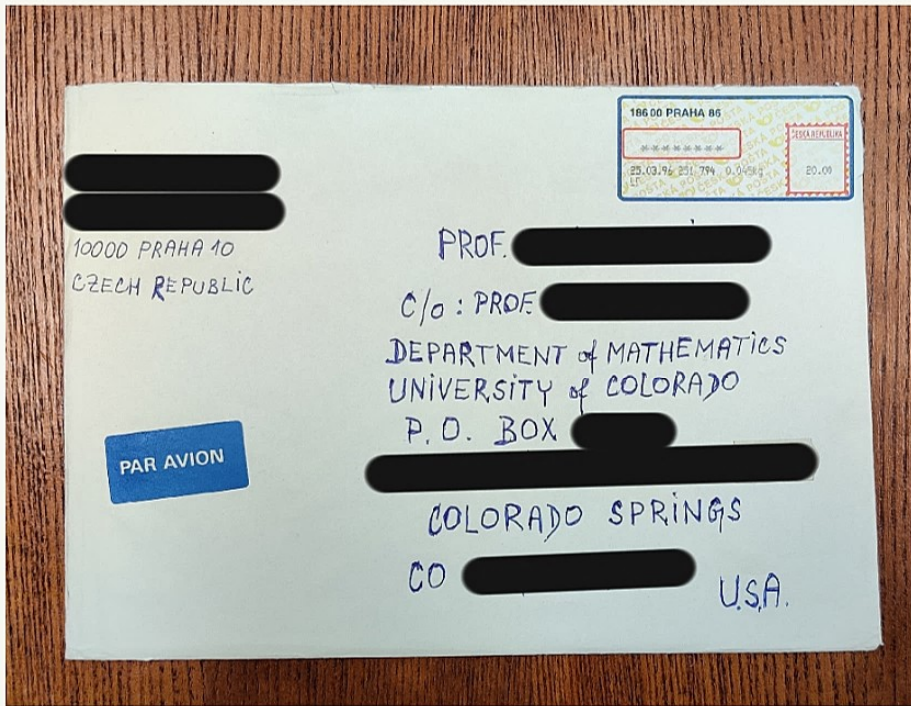
























DISORDER = UNPREDICTABILITY

DISORDER IN ALGEBRA

	1	2	3	4	5
1	1	3	5	2	4
2	5	2	4	1	3
3	4	1	3	5	2
4	3	5	2	4	1
5	2	4	1	3	5

LATIN SQUARE

- max disorder
- min predictability

	1	2	3	4	5
1	1	1	1	1	1
2	2	2	2	2	2
3	3	3	3	3	3
4	4	4	4	4	4
5	5	5	5	5	5

PROJECTION

- min disorder
- max predictability

QUANDLES

DEF. Q - non empty set, $\triangleright: Q^2 \rightarrow Q$ - binary operation.

(Q, \triangleright) is a quandle if

$$(1) \quad \forall x \in Q: x \triangleright x = x$$

$$(2) \quad \forall x, y \in Q \exists! z \in Q: z \triangleright x = y$$

$$(3) \quad \forall x, y, z \in Q: (x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$$

QUANDLES

DEF. Q - non empty set, $\triangleright: Q^2 \rightarrow Q$ - binary operation.

(Q, \triangleright) is a quandle if

$$(1) \quad \forall x \in Q: x \triangleright x = x$$

(diagonal = identity)

$$(2) \quad \forall x, y \in Q \exists! z \in Q: z \triangleright x = y$$

(columns are permutations)

$$(3) \quad \forall x, y, z \in Q: (x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$$

(compatibility condition)

QUANDLES

DEF. Q - non empty set, $\triangleright: Q^2 \rightarrow Q$ - binary operation.

(Q, \triangleright) is a quandle if

$$(1) \quad \forall x \in Q: x \triangleright x = x$$

(diagonal = identity)

$$(2) \quad \forall x, y \in Q \exists! z \in Q: z \triangleright x = y$$

(columns are permutations)

$$(3) \quad \forall x, y, z \in Q: (x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$$

(compatibility condition)

EX. $(Q, x \triangleright y = x)$ is a projection quandle.

$(\mathbb{Z}_n, x \triangleright y = 2y - x)$ is a dihedral quandle.

QUANDLES AND GROUPS

PROP. (Q, \triangleright) - quandle

(1) (Q, \triangleright) has a neutral element $\rightarrow |Q| = 1$.

(2) (Q, \triangleright) is associative $\rightarrow (Q, \triangleright)$ is a projection quandle.

QUANDLES AND GROUPS

PROP. (Q, \triangleright) - quandle

(1) (Q, \triangleright) has a neutral element $\rightarrow |Q| = 1$.

(2) (Q, \triangleright) is associative $\rightarrow (Q, \triangleright)$ is a projection quandle.

RMK. Quandles are very far from being groups!

Compute : $3 + 6 + 4 + 6 + 4 + 6 + 4 + 6 + 4 + 6 + 4$.

WORKING WITHOUT ASSOCIATIVITY

Compute : $3 + 6 + 4 + 6 + 4 + 6 + 4 + 6 + 4 + 6 + 4$.

With associativity : $3 + (6 + 4) + (6 + 4) + (6 + 4) + (6 + 4) + (6 + 4) = 53$.

Without associativity : $((\dots (3 + 6) + 4) + 6) + 4) + 6) + 4) + 6) + 4) + 6) + 4) =$



WORKING WITHOUT ASSOCIATIVITY

Compute : $3 + 6 + 4 + 6 + 4 + 6 + 4 + 6 + 4 + 6 + 4$.

With associativity : $3 + (6 + 4) + (6 + 4) + (6 + 4) + (6 + 4) + (6 + 4) = 53$.

Without associativity : $(((((3 + 6) + 4) + 6) + 4) + 6) + 4) + 6) + 4) + 6) + 4) =$



MORAL OF THE STORY: Things still work, but everything is much more clunky.

ENTROPY - DPD

(discrete probability distribution)

DEF. $p = (p_1, \dots, p_n)$ - DPD $(p_i \in [0, 1] \forall i, \sum_{i=1}^n p_i = 1)$.

The (Shannon) entropy of p is

$$h(p) = - \sum_{i=1}^n p_i \log(p_i).$$

ENTROPY - DPD

(discrete probability distribution)

DEF. $p = (p_1, \dots, p_n)$ - DPD $(p_i \in [0, 1] \forall i, \sum_{i=1}^n p_i = 1)$.

The (Shannon) entropy of p is

$$h(p) = - \sum_{i=1}^n p_i \log(p_i).$$

PROP. (1) $h(p) \geq 0$

(2) $0 \leq h(p) \leq \log(n)$

(3) $h(p) = 0 \iff p_i = 1$ and $p_j = 0 \forall j \neq i$ (min disorder - max predictability)

(4) $h(p) = \log(n) \iff p_i = \frac{1}{n} \forall i$ (max disorder - min predictability)

ENTROPY - FUNCTIONS

DEF. $a: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ - function.

(1) The distribution of a is $\hat{a} = \left(\frac{|a^{-1}(1)|}{n}, \dots, \frac{|a^{-1}(n)|}{n} \right)$.

(It is a DPD)

(2) The entropy of a is $h(a) := h(\hat{a})$.

ENTROPY - FUNCTIONS

DEF. $a: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ - function.

(1) The distribution of a is $\hat{a} = \left(\frac{|a^{-1}(1)|}{n}, \dots, \frac{|a^{-1}(n)|}{n} \right)$.

(It is a DPD)

(2) The entropy of a is $h(a) := h(\hat{a})$.

PROP. (1) $h(a) = 0 \iff a$ is constant

(2) $h(a) = \log(n) \iff a$ is a permutation

ENTROPY - QUANDLES

DEF. (Q, \triangleright) - quandle, L_1, \dots, L_n - rows of (Q, \triangleright) .

The entropy of (Q, \triangleright) is

$$H(Q) := \frac{1}{n} \sum_{i=1}^n h(L_i)$$

ENTROPY - QUANDLES

DEF. (Q, \triangleright) - quandle, L_1, \dots, L_n - rows of (Q, \triangleright) .

The entropy of (Q, \triangleright) is

$$H(Q) := \frac{1}{n} \sum_{i=1}^n h(L_i)$$

RMK. (1) Why did we use the rows and not the columns?

(2) What does $H(Q)$ actually measure?

ENTROPY - QUANDLES

DEF. (Q, \triangleright) - quandle, L_1, \dots, L_n - rows of (Q, \triangleright) .

The entropy of (Q, \triangleright) is

$$H(Q) := \frac{1}{n} \sum_{i=1}^n h(L_i)$$

RMK. (1) Why did we use the rows and not the columns?

(2) What does $H(Q)$ actually measure?

PROP. (1) $H(Q) = 0 \iff Q$ is a projection quandle

(2) $H(Q) = \log(n) \iff Q$ is a latin quandle \leftarrow (A quandle whose table is a latin square)

EXAMPLES OF ENTROPY

EX. $\mathcal{Q} = (\mathbb{Z}_n, x \triangleright y = zy - x)$ - dihedral quandle.

$$H(\mathcal{Q}) = \begin{cases} \log(n) & n \text{ odd} \\ \frac{1}{2} \log(n) & n \text{ even.} \end{cases}$$

EXAMPLES OF ENTROPY

EX. $Q = (\mathbb{Z}_n, x \triangleright y = zy - x)$ - dihedral quandle.

$$h(a) = \begin{cases} \log(n) & n \text{ odd} \\ \frac{1}{2} \log(n) & n \text{ even.} \end{cases}$$

DEF. G -group. $\text{Core}(G) := (G, x \triangleright y = yx^{-1}y)$ is a core quandle.

EXAMPLES OF ENTROPY

EX. $Q = (\mathbb{Z}_n, x \triangleright y = zy - x)$ - dihedral quandle.

$$H(Q) = \begin{cases} \log(n) & n \text{ odd} \\ \frac{1}{2} \log(n) & n \text{ even.} \end{cases}$$

DEF. G -group. $\text{Core}(G) := (G, x \triangleright y = yx^{-1}y)$ is a core quandle.

$$H(\text{Core}(D_n)) = \begin{cases} \log(2n) - \frac{n+1}{2n} \log(n+1) & n \text{ odd} \\ \log(2n) - \frac{1}{2n} \left[\left(\frac{n}{2} - 1 \right) \cdot 2 \log 2 + (n+2) \log(n+2) \right] & n \text{ even.} \end{cases}$$

DEF. G -group. $\text{Conj}(G) := (G, x \triangleright y = y^{-1}xy)$ is a conjugation quandle.

DEF. G -group. $\text{Conj}(G) := (G, x \triangleright y = y^{-1}xy)$ is a conjugation quandle.

$$H(\text{Conj}(D_n)) = \begin{cases} \log(2n) - \frac{1}{2n} [(n+1) \log 2 + n \log n] & n \text{ odd} \\ \log(2n) - \frac{1}{2n} [2(n+1) \log 2 + n \log n] & n \text{ even.} \end{cases}$$

DEF. G -group. $\text{Conj}(G) := (G, x \triangleright y = y^{-1}xy)$ is a conjugation quandle.

$$H(\text{Conj}(D_n)) = \begin{cases} \log(2n) - \frac{1}{2n} [(n+1)\log 2 + n \log n] & n \text{ odd} \\ \log(2n) - \frac{1}{2n} [2(n+1)\log 2 + n \log n] & n \text{ even.} \end{cases}$$

Moreover, in any case

$$\lim_{n \rightarrow +\infty} H(\text{Core}(D_n)) = +\infty$$

$$\lim_{n \rightarrow +\infty} H(\text{Conj}(D_n)) = +\infty.$$

RMK. We have arbitrarily large quandles with arbitrarily high entropy.

(1) Can we have arbitrarily small quandles with arbitrarily high entropy?

RMK. We have arbitrarily large quandles with arbitrarily high entropy.

(1) Can we have arbitrarily small quandles with arbitrarily high entropy? NO

(2) Can we have arbitrarily large quandles with arbitrarily low entropy?

RMK. We have arbitrarily large quandles with arbitrarily high entropy.

(1) Can we have arbitrarily small quandles with arbitrarily high entropy? NO

(2) Can we have arbitrarily large quandles with arbitrarily low entropy? NOT EASY TO GUESS

RMK. We have arbitrarily large quandles with arbitrarily high entropy.

(1) Can we have arbitrarily small quandles with arbitrarily high entropy? NO

(2) Can we have arbitrarily large quandles with arbitrarily low entropy? NOT EASY TO GUESS

(3) What quandle properties regulate its entropy?

RMK. If the rows of Q have the same frequency : $H(Q) = h(L_1)$.

RMK. If the rows of Q have the same frequency : $H(Q) = h(L_1)$.

Ex.

	1	2	3	4	5	6
1	1	1	5	1	3	1
2	2	2	2	2	6	4
3	5	3	3	3	1	3
4	4	6	4	4	4	2
5	3	5	1	5	5	5
6	6	4	6	2	6	6

Core (D_3)

RMK. If the rows of Q have the same frequency : $H(Q) = h(L_1)$.

Ex.

	1	2	3	4	5	6
1	1	1	5	1	3	1
2	2	2	2	2	6	4
3	5	3	3	3	1	3
4	4	6	4	4	4	2
5	3	5	1	5	5	5
6	6	4	6	2	6	6

Four equal elements and
two different in every row

$$H(Q) = h([1, 1, 5, 1, 3, 1])$$

Core (D_3)

DEF. (Q, \triangleright) - quandle. We define

(1) Right multiplication maps: $R_x : Q \rightarrow Q, q \mapsto q \triangleright x$ (columns)

(2) Left multiplication maps: $L_x : Q \rightarrow Q, q \mapsto x \triangleright q$ (rows)

Moreover

$$\text{Im}(Q) = \langle R_x \cdot x \in Q \rangle \leq \text{Sym}(Q)$$

$\text{Aut}(Q) =$ group of automorphisms of (Q, \triangleright) .

DEF. (Q, \triangleright) - quandle. We define

(1) Right multiplication maps: $R_x : Q \rightarrow Q, q \mapsto q \triangleright x$ (columns)

(2) Left multiplication maps: $L_x : Q \rightarrow Q, q \mapsto x \triangleright q$ (rows)

Moreover

$$\text{Inn}(Q) = \langle R_x : x \in Q \rangle \leq \text{Sym}(Q)$$

$\text{Aut}(Q)$ = group of automorphisms of (Q, \triangleright) .

PROP. (1) $\text{Inn}(Q) \leq \text{Aut}(Q) \leq \text{Sym}(Q)$

(2) $\text{Inn}(Q)$ and $\text{Aut}(Q)$ act naturally on Q .

DEF. (Q, \triangleright) - quonolle

(1) If the action of $\text{Inn}(Q)$ on Q is transitive, then Q is connected.

(2) If the action of $\text{Aut}(Q)$ on Q is transitive, then Q is homogeneous.

DEF. (Q, \triangleright) - quonolle

(1) If the action of $\text{Inn}(Q)$ on Q is transitive, then Q is connected.

(2) If the action of $\text{Aut}(Q)$ on Q is transitive, then Q is homogeneous.

RMK. (1) Q connected $\rightarrow Q$ homogeneous.

(2) Q homogeneous $\rightarrow H(Q) = h(L_1)$.

DEF. (Q, \triangleright) - quonolle

(1) If the action of $\text{Inn}(Q)$ on Q is transitive, then Q is connected.

(2) If the action of $\text{Aut}(Q)$ on Q is transitive, then Q is homogeneous.

RMK. (1) Q connected $\rightarrow Q$ homogeneous.

(2) Q homogeneous $\rightarrow H(Q) = h(L_1)$.

Being homogeneous "pushes towards being ordered" (the entropy is constant on the rows).

DEF. (Q, \triangleright) -quandle. If $R_x \neq R_y$ whenever $x \neq y$, then (Q, \triangleright) is faithful.

DEF. (Q, \triangleright) - quandle. If $R_x \neq R_y$ whenever $x \neq y$, then (Q, \triangleright) is faithful.

EX. $Q = (\mathbb{Z}_n, x \triangleright y = 2y - x)$ - dihedral quandle.

(1) n odd $\Rightarrow Q$ is faithful

(2) n even $\Rightarrow Q$ is not faithful

DEF. (Q, \triangleright) -quandle. If $R_x \neq R_y$ whenever $x \neq y$, then (Q, \triangleright) is faithful.

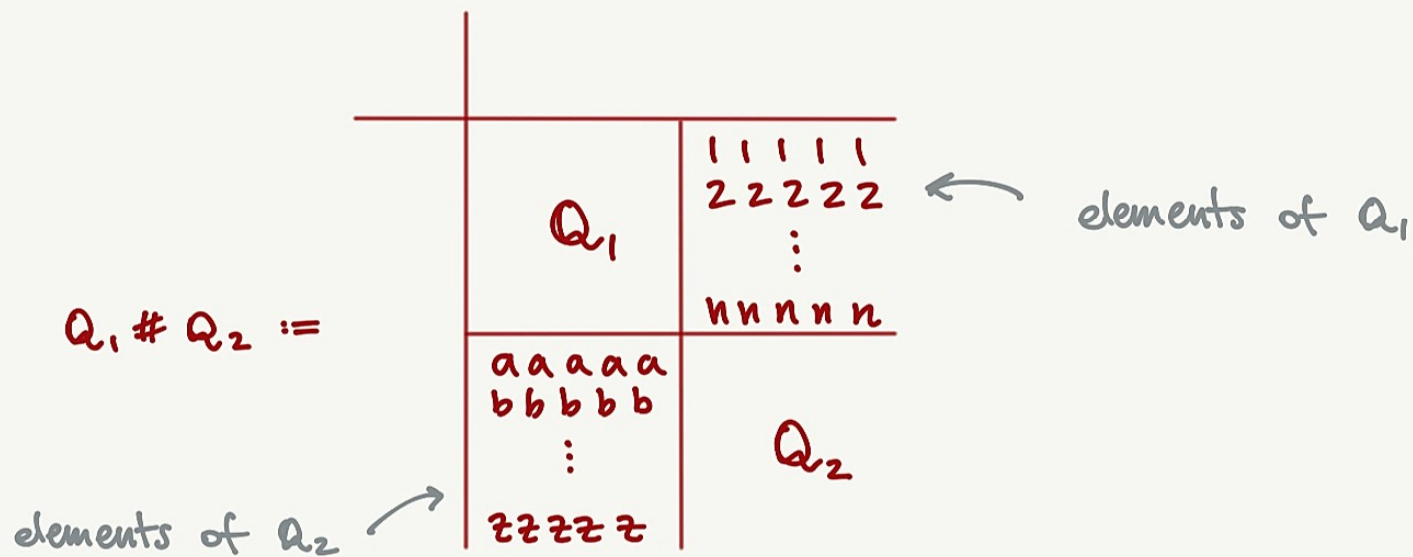
EX. $Q = (\mathbb{Z}_n, x \triangleright y = 2y - x)$ - dihedral quandle.

(1) n odd $\Rightarrow Q$ is faithful

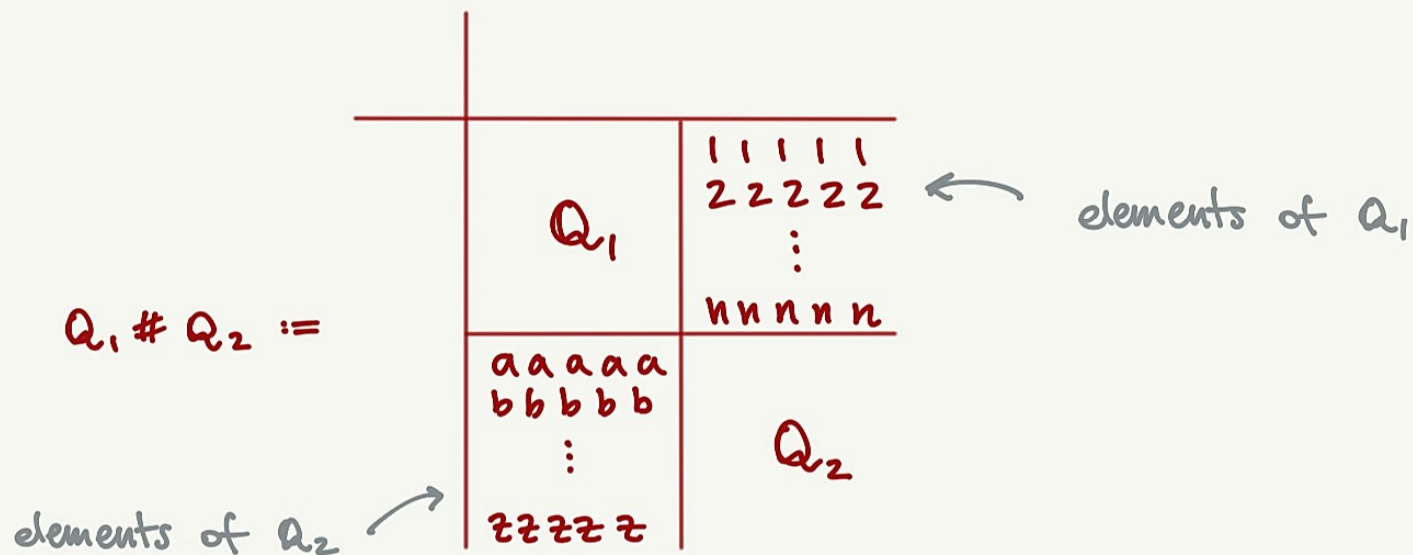
(2) n even $\Rightarrow Q$ is not faithful

Being faithful "pushes towards being disordered". Does it exist a lower bound for the entropy of faithful quandles?

DEF. Q_1, Q_2 - quandles. We define the sum of quandles.



DEF. Q_1, Q_2 - quandles. We define the sum of quandles.



and the k^{th} multiple of a quandle Q : $kQ := \underbrace{Q \# Q \# \dots \# Q}_{k \text{ times}}$

Prop. (1) $\#$ is commutative and associative

(2) $\mathcal{A}_1 \# \mathcal{A}_2$ is a not connected quandle

(3) $\mathcal{A}_1, \mathcal{A}_2$ faithful $\rightarrow \mathcal{A}_1 \# \mathcal{A}_2$ faithful

(4) $H(k\mathcal{A}) \leq \log\left(1 + \frac{1}{k-1}\right) + \frac{1}{k} [H(\mathcal{A}) + \log(k|\mathcal{A}|)]$.

PROP. (1) $\#$ is commutative and associative

(2) $\mathcal{A}_1 \# \mathcal{A}_2$ is a not connected quandle

(3) $\mathcal{A}_1, \mathcal{A}_2$ faithful $\rightarrow \mathcal{A}_1 \# \mathcal{A}_2$ faithful

$$(4) H(k\mathcal{A}) \leq \log\left(1 + \frac{1}{k-1}\right) + \frac{1}{k} [H(\mathcal{A}) + \log(k|\mathcal{A}|)].$$

COR. $\lim_{k \rightarrow \infty} H(k\mathcal{A}) = 0.$

PROP. (1) $\#$ is commutative and associative

(2) $Q_1 \# Q_2$ is a not connected quandle

(3) Q_1, Q_2 faithful $\rightarrow Q_1 \# Q_2$ faithful

(4) $H(kQ) \leq \log\left(1 + \frac{1}{k-1}\right) + \frac{1}{k} [H(Q) + \log(k|Q|)]$.

COR. $\lim_{k \rightarrow \infty} H(kQ) = 0$.

RMK. There is no lower bound for the entropy of faithful quandles.

ENTROPY AND H,S,P OPERATORS

SURVEY

□ $H(Q_1 \times Q_2) = \dots$

(a) $H(Q_1) + H(Q_2)$

(b) $H(Q_1) \cdot H(Q_2)$

(c) $\max \{ H(Q_1), H(Q_2) \}$

ENTROPY AND H,S,P OPERATORS

SURVEY

□ $H(Q_1 \times Q_2) = \dots$

~~(a)~~ $H(Q_1) + H(Q_2)$

(b) $H(Q_1) \cdot H(Q_2)$

(c) $\max \{ H(Q_1), H(Q_2) \}$

PROP. $H(Q_1 \times Q_2) = H(Q_1) + H(Q_2)$

□

$a_1 \rightarrow a_2$. Then

(a) $H(a_1) \leq H(a_2)$

(b) $H(a_1) \geq H(a_2)$

(c) $H(a_1) = H(a_2)$

SURVEY

\square $a_1 \rightarrow a_2$. Then

(a) $H(a_1) \leq H(a_2)$

~~(b) $H(a_1) \geq H(a_2)$~~

(c) $H(a_1) = H(a_2)$

PROP. $a_1 \rightarrow a_2 \rightarrow H(a_2) \leq H(a_1)$

COR. $H(a/\emptyset) \leq H(a)$.

□ $Q_1 \leftrightarrow Q_2$. Then

(a) $H(Q_1) \leq H(Q_2)$

(b) $H(Q_1) \geq H(Q_2)$

(c) $H(Q_1) = H(Q_2)$

SURVEY

5 $Q_1 \leftrightarrow Q_2$. Then

SURVEY

(a) $H(Q_1) \leq H(Q_2)$

(b) $H(Q_1) \geq H(Q_2)$

(c) $H(Q_1) = H(Q_2)$

Unfortunately, none of the above.

Q_1	1	3	5
1	1	5	3
3	5	3	1
5	3	1	5



Core (D_3)

Q_2	1	2	3	4	5	6
1	1	1	5	1	3	1
2	2	2	2	2	6	4
3	5	3	3	3	1	3
4	4	6	4	4	4	2
5	3	5	1	5	5	5
6	6	4	6	2	6	6

□ $Q_1 \leftrightarrow Q_2$. Then

SURVEY

(a) $H(Q_1) \leq H(Q_2)$

(b) $H(Q_1) \geq H(Q_2)$

(c) $H(Q_1) = H(Q_2)$

Unfortunately, none of the above.

Q_1	1	3	5
1	1	5	3
3	5	3	1
5	3	1	5

$$H(Q_1) = \log 3$$



Core (D_3)

Q_2	1	2	3	4	5	6
1	1	1	5	1	3	1
2	2	2	2	2	6	4
3	5	3	3	3	1	3
4	4	6	4	4	4	2
5	3	5	1	5	5	5
6	6	4	6	2	6	6

$$H(Q_2) = \log 3 - \frac{1}{2} \log 2$$

RMK. $Q_1 \leftrightarrow Q_2 \Rightarrow H(Q_1) \leq H(Q_2)$ is false even if Q_1 and Q_2 are both connected.

(SmallQuondle (21, 9) in RIG).

RMK. $Q_1 \leftrightarrow Q_2 \Rightarrow H(Q_1) \leq H(Q_2)$ is false even if Q_1 and Q_2 are both connected.

(Small Quandle $(21, 9)$ in RIG).

PROP. Q_1, Q_2 quandles, $|Q_1| = n$, $|Q_2| = m$, $Q_1 \leftrightarrow Q_2 \Rightarrow H(Q_1) \leq \frac{n^2}{m^2} \cdot H(Q_2)$

$H(Q_1 \# Q_2) = \dots$

(a) $H(Q_1) + H(Q_2)$

(b) $H(Q_1) \cdot H(Q_2)$

(c) $\max \{ H(Q_1), H(Q_2) \}$

(d) None of the above

SURVEY

$H(a_1 \# a_2) = \dots$

(a) $H(a_1) + H(a_2)$

(b) $H(a_1) \cdot H(a_2)$

(c) $\max \{ H(a_1), H(a_2) \}$

~~(d)~~ None of the above

Prop. a_1, a_2 quonelles, $|a_1| = n$, $|a_2| = m$.

$$H(a_1 \# a_2) \leq 1 + \left(\frac{n^2}{m^2 + n^2} \right) H(a_1) + \left(\frac{m^2}{m^2 + n^2} \right) H(a_2)$$

CONCLUSIONS

(*) The entropy function measures some properties of quandles and it behaves relatively well with respect to Universal Algebraic constructions.

CONCLUSIONS

(*) The entropy function measures some properties of quandles and it behaves relatively well with respect to Universal Algebraic constructions.

(*) Everything can be generalized to groupoids (for groups, loops and quasigroups it is trivial).

CONCLUSIONS

(*) The entropy function measures some properties of quandles and it behaves relatively well with respect to Universal Algebraic constructions.

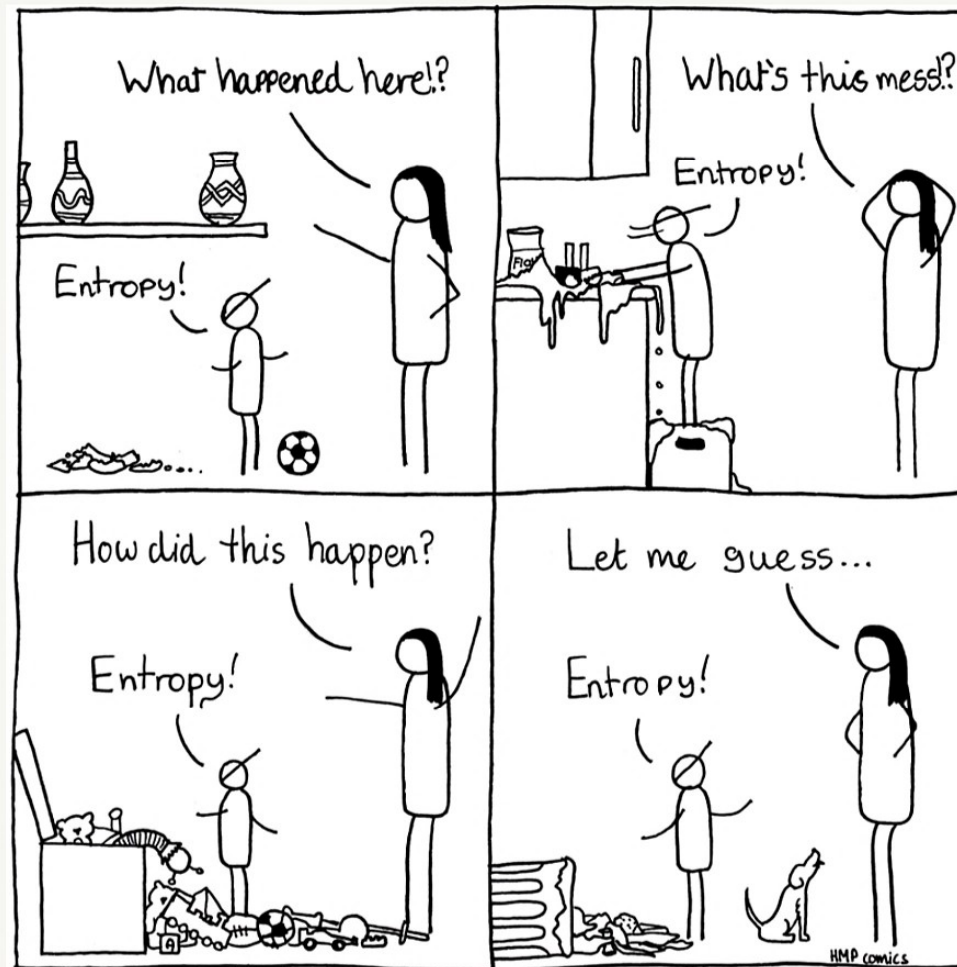
(*) Everything can be generalized to groupoids (for groups, loops and quasigroups it is trivial).

NEW HORIZONS :

(?) lower bound for connected, faithful, non-latin quandles.

THANKS FOR YOUR ATTENTION!

spaggiari @ karlin.mff.cuni.cz



This is why we don't teach our children about entropy until much later...