ENTROPY FOR QUANDLES

Filippo Spoggiari
Charles University Prague

SPIEDini, Florence

23 NOV 2023

Mettere in ordine la camera...

secondo i genitori secondo i bambini

DISORDINE = IMPREVEDIBILITÀ

DISORDINE IN ALGEBRA

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

	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

<u>Quadrato latino</u>

- max disordine
- min prevedibilità

<u>Proiezione</u>

- min disordine
- max prevedibilità.

DEFINIZIONE DI QUANDLE

<u>DEF.</u> Q - insieme non vuoto, $\triangleright : Q^2 \to Q$ - operazione binaria

$(Q, \triangleright)$ è detto <u>quandle</u> se

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

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

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

DEFINIZIONE DI QUANDLE

DEF. Q - insieme non vuoto, $\triangleright : Q^2 \to Q$ - operazione binaria

$(Q, \triangleright)$ è detto quandle se

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

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

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

ES

- $(Q, x \triangleright y = x)$ è un quandle (di proiezione)
- $(\mathbb{Z}_n, x \triangleright y = 2y - x)$ è un quandle (diedrale)

Pensiamo ai quandle come tabelle di moltiplicazione tali che

(1) Diagonale identica

(2) le colonne sono permutazioni

(3) Condizione di compatibilità tra le colonne
(difficile da visualizzare)

<u>OSS</u>: Applicheremo la nozione di entropia ai quandle, ma molto si può generalizzare.

QUANDLE E GRUPPI

<u>OSS</u>. I quandle sono molto lontani dall'essere gruppi:

<u>PROP</u>. $(Q, \triangleright)$ - quandle.

- $(Q, \triangleright)$ ha un elemento neutro $\Rightarrow |Q| = 1$
- $(Q, \triangleright)$ è associativo $\Rightarrow$ $(Q, \triangleright)$ è quandle proiettivo.

Calcolare

$$3+6+4+6+4+6+4+6+4+6+4.$$

LAVORARE SENZA ASSOCIATIVITÀ

Calcolare

$$3+6+4+6+4+6+4+6+4+6+4.$$

Con associatività:

$$3+(6+4)+(6+4)+(6+4)+(6+4)+(6+4)=53$$

Senza associatività:

$$(((\cdots(3+6)+4)+6)+4)+6)+4)+6)+4)+6)+4)= \frown$$

<u>Morale</u>: le cose funzionano ancora, ma è tutto un po' più complicato.

Cominciamo a misurare il disordine (i.e. la prevedibilità) di un quandle.

ENTROPIA

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

l' entropia di p è

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

ENTROPIA

<u>DEF</u>. $p = (p_1, \dots, p_n)$ - DPD $\left(p_i \in [0,1] \, , \, \sum_{i=1}^{n} p_i = 1 \right)$

l'<u>entropia di p</u> è

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

<u>PROP</u>. (1) $h(p) \geq 0$

(2) $h(p) = 0 \iff p_i = 1$ e $p_j = 0 \;\; \forall j \neq i$

(3) $h(p) = \log(n) \iff p = \left(\frac{1}{n}, \dots, \frac{1}{n} \right)$

(4) $0 \leq h(p) \leq \log(n)$.

DEF. $a : \{1, \dots, n\} \to \{1, \dots n\}$ - funzione.

Definiamo la distribuzione di a:

DPD

$$\hat{a} := \left(\frac{|a^{-1}(1)|}{n}, \dots, \frac{|a^{-1}(n)|}{n} \right)$$

e l' entropia della funzione a:

$$h(a) := h(\hat{a})$$

DEF $a : \{1, \dots, n\} \to \{1, \dots, n\}$ - funzione.

Definiamo la <u>distribuzione</u> di a:

$$\hat{a} := \left(\frac{|a^{-1}(1)|}{n}, \dots, \frac{|a^{-1}(n)|}{n} \right)$$

DPD

e l'<u>entropia della funzione a</u>:

$$h(a) := h(\hat{a})$$

PROP (1) $h(a) = 0 \iff a$ è costante

(2) $h(a) = \log(n) \iff a$ è una permutazione

DEF. $(Q,\triangleright)$ - quandle, $L_1,\dots,L_n$ - righe di $(Q,\triangleright)$.

Definiamo l'<u>entropia del quandle $(Q,\triangleright)$</u>

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

DEF. $(Q, \triangleright)$ - quandle, $L_1, \dots, L_n$ - righe di $(Q, \triangleright)$.

Definiamo l'*entropia del quandle* $(Q, \triangleright)$

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

OSS. (1) Perchè abbiamo usato le righe e non le colonne?

(2) Che cosa misura, intuitivamente, $H(Q)$?

DEF. $(Q, \triangleright)$ - quandle, $L_1, \dots, L_n$ - righe di $(Q, \triangleright)$.

Definiamo l'entropia del quandle $(Q, \triangleright)$

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

OSS. (1) Perché abbiamo usato le righe e non le colonne?

(2) Che cosa misura, intuitivamente, $H(Q)$?

PROP. (1) $H(Q) = 0 \iff Q$ quandle di proiezione (max ordine)

(2) $H(Q) = \log(n) \iff Q$ quandle latino (max disordine)

ESEMPI DI ENTROPIA

ES. $(\mathbb{Z}_n, x \triangleright y = 2y - x) =: Q$ – quandle diedrale

$$H(Q) = \begin{cases} \log(n) & n \text{ dispari} \\ \frac{1}{2}\log(n) & n \text{ pari} \end{cases}$$

ESEMPI DI ENTROPIA

ES. $(\mathbb{Z}_n, x \triangleright y = 2y - x) =: Q$ – quandle diedrale

$$H(Q) = \begin{cases} \log(n) & n \text{ dispari} \\ \frac{1}{2}\log(n) & n \text{ pari} \end{cases}$$

DEF. G – gruppo. $(G, x \triangleright y = y x^{-1} y)$ è un quandle detto Core(G)

DEF. G – gruppo. $(G, x \triangleright y = y^{-1} x y)$ è un quandle detto Conj(G)

PROP.

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

PROP.

$$H(\mathrm{Core}(D_n)) = \begin{cases} \log(2n) - \dfrac{n+1}{2n}\log(n+1) & n \text{ dispari} \\[2ex] \log(2n) - \dfrac{1}{2n}\left[\left(\dfrac{n}{2}-1\right)\cdot 2\log 2 + (n+2)\log(n+2)\right] & n \text{ pari} \end{cases}$$

Inoltre, in ogni caso, $\lim\limits_{n\to+\infty}\left\{H(\mathrm{Core}(D_n))\right\} = +\infty$.

PROP.

$$H(\mathrm{Core}(D_n)) = \begin{cases} \log(2n) - \dfrac{n+1}{2n}\log(n+1) & n \text{ dispari} \\[2ex] \log(2n) - \dfrac{1}{2n}\left[\left(\dfrac{n}{2}-1\right)\cdot 2\log 2 + \right. \\ \quad \left. + (n+2)\log(n+2)\right] & n \text{ pari} \end{cases}$$

Inoltre, in ogni caso, $\lim_{n \to +\infty} \{H(\mathrm{Core}(D_n))\} = +\infty$.

PROP.

$$H(\mathrm{Conj}(D_n)) = \begin{cases} \log(2n) - \dfrac{1}{2n}\left[(n+1)\log 2 + n\log n\right] & n \text{ dispari} \\[2ex] \log(2n) - \dfrac{1}{2n}\left[2(n+1)\log 2 + n\log n\right] & n \text{ pari} \end{cases}$$

Inoltre, in ogni caso, $\lim_{n \to +\infty} \{H(\mathrm{Conj}(D_n))\} = +\infty$.

<u>OSS</u>. Abbiamo quandle arbitrariamente grandi con entropia arbitrariamente grande.

<u>OSS.</u> Abbiamo quandle arbitrariamente grandi con entropia arbitrariamente grande.

(1) Possiamo costruire quandle arbitrariamente piccoli con entropia arbitrariamente grande? NO.

OSS. Abbiamo quandle arbitrariamente grandi con entropia arbitrariamente grande.

(1) Possiamo costruire quandle arbitrariamente piccoli con entropia arbitrariamente grande? NO.

(2) Possiamo costruire quandle arbitrariamente grandi con entropia arbitrariamente piccola???

<u>OSS.</u> Abbiamo quandle arbitrariamente grandi con entropia arbitrariamente grande.

(1) Possiamo costruire quandle arbitrariamente piccoli con entropia arbitrariamente grande? NO.

(2) Possiamo costruire quandle arbitrariamente grandi con entropia arbitrariamente piccola???

(3) Quali fattori / proprietà di un quandle regolano la sua entropia?

OSS. Se le righe di Q hanno la stessa frequenza:

$$H(Q) = h(L_1)$$

ES.

	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

$Core(D_3)$

Due elementi diversi e quattro uguali

$$\Downarrow$$

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

DEF. $(Q, \triangleright)$ - quandle. Definiamo le <u>mappe di moltiplicazione a destra e a sinistra</u>

$$R_x : Q \longrightarrow Q \qquad\qquad L_x : Q \longrightarrow Q$$
$$q \longmapsto q \triangleright x \qquad\qquad q \longmapsto x \triangleright q$$

(colonne) (righe)

DEF. $(Q, \triangleright)$ - quandle. Definiamo le **mappe di moltiplicazione a destra e a sinistra**

$$R_x : Q \to Q \qquad\qquad L_x : Q \to Q$$
$$\quad q \mapsto q \triangleright x \qquad\qquad \quad q \mapsto x \triangleright q$$

(colonne) (righe)

Definiamo inoltre

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

$\mathrm{Aut}(Q)$ = gruppo degli automorfismi di Q.

PROP. (1) $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G) \leq \mathrm{Sym}(G)$

(2) $\mathrm{Inn}(G)$ e $\mathrm{Aut}(G)$ agiscono naturalmente su G.

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

(2) $\mathrm{Inn}(Q)$ e $\mathrm{Aut}(Q)$ agiscono naturalmente su Q.

DEF. $(Q, \triangleright)$-quandle.

(1) se $\mathrm{Inn}(Q)$ agisce transitivamente su Q, allora Q e' detto <u>connesso</u>.

(2) se $\mathrm{Aut}(Q)$ agisce transitivamente su Q, allora Q e' detto <u>omogeneo</u>

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

(2) $\mathrm{Inn}(Q)$ e $\mathrm{Aut}(Q)$ agiscono naturalmente su Q.

DEF. $(Q, \triangleright)$ - quandle.

(1) se $\mathrm{Inn}(Q)$ agisce transitivamente su Q, allora Q e' detto <u>connesso</u>.

(2) se $\mathrm{Aut}(Q)$ agisce transitivamente su Q, allora Q e' detto <u>omogeneo</u>

OSS. Q connesso $\Rightarrow$ Q omogeneo.

PROP. (Q, D) – quandle omogeneo. $\Rightarrow$ $H(Q) = h(L_1)$.

PROP. (Q, D) - quadrato omogeneo. $\Rightarrow H(Q) = h(L_1)$.

OSS. L'entropia di Q è influenzata dalla variazione di entropia delle righe, noi poi prendiamo la media. Nei quadrati omogenei questo non avviene: le righe hanno entropia costante.

Stiamo introducendo un fattore che "spinge verso l'ordine" cioè abbassa l'entropia.

Introduciamo ora una proprietà che "spinge al disordine"

<u>DEF</u>. $(Q, \triangleright)$ - quandle. Se $R_x \neq R_y$ per ogni $x \neq y$ diciamo che $(Q, \triangleright)$ è un quandle <u>fedele</u>.

Introduciamo ora una proprietà che "spinge al disordine"

<u>DEF</u>. $(Q, \triangleright)$ - quandle. Se $R_x \neq R_y$ per ogni $x \neq y$ diciamo che $(Q, \triangleright)$ è un quandle <u>fedele</u>.

<u>PROP</u>. $(Q, \triangleright) = (\mathbb{Z}_n, x \triangleright y = 2y - x)$ - quandle diedrale.

(1) n dispari $\Rightarrow$ $(Q, \triangleright)$ è fedele

(2) n pari $\Rightarrow$ $(Q, \triangleright)$ non è fedele.

Introduciamo ora una proprietà che "spinge al disordine"

<u>DEF.</u> $(Q, \triangleright)$ - quandle. Se $R_x \neq R_y$ per ogni $x \neq y$ diciamo che $(Q, \triangleright)$ è un quandle <u>fedele</u>.

<u>PROP.</u> $(Q, \triangleright) = (\mathbb{Z}_n, x \triangleright y = 2y - x)$ - quandle diedrale.

(1) n dispari $\Rightarrow$ $(Q, \triangleright)$ è fedele

(2) n pari $\Rightarrow$ $(Q, \triangleright)$ non è fedele.

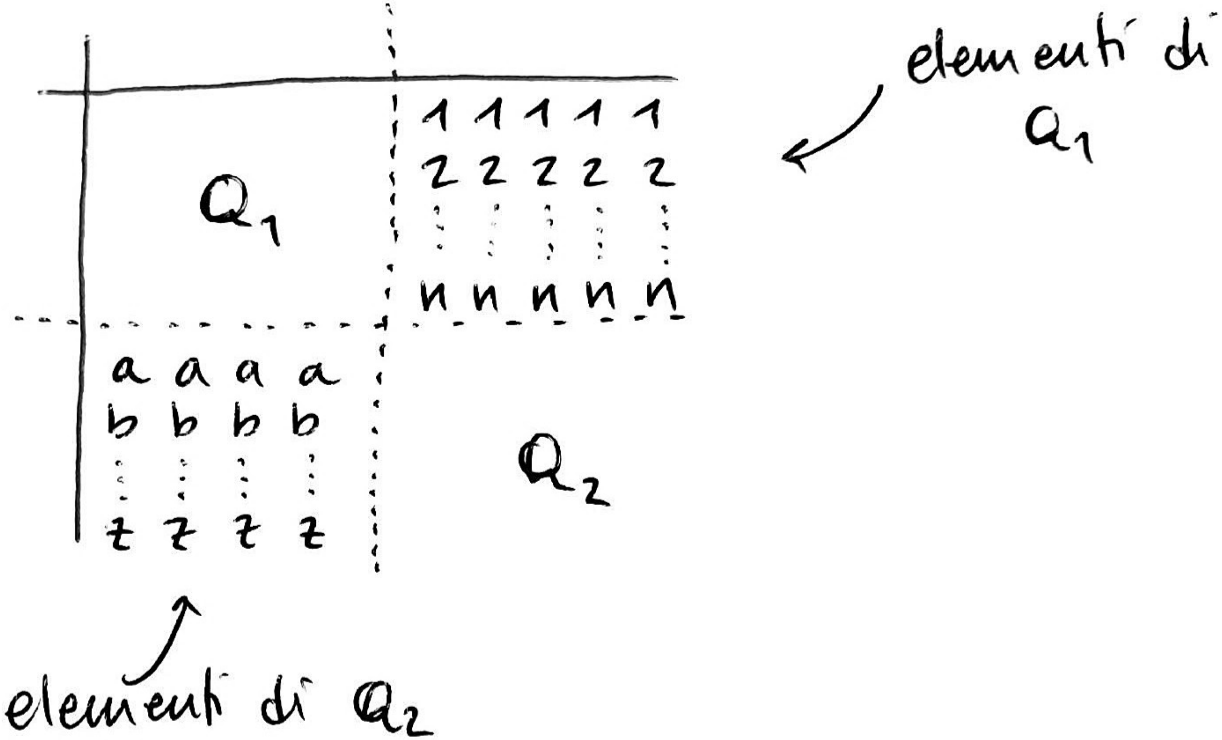
Esiste un "lower bound" per quandle fedeli? Cioè, una entropia minima diversa da zero?

DEF. Q_1, Q_2-quandle. Definiamo la <u>somma di quandle</u>

$$
Q_1 \# Q_2 = \begin{array}{|c|c}
\hline
Q_1 & \begin{matrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ n & n & n & n & n \end{matrix} \\
\hdashline
\begin{matrix} a & a & a & a \\ b & b & b & b \\ \vdots & \vdots & \vdots & \vdots \\ z & z & z & z \end{matrix} & Q_2
\end{array}
$$

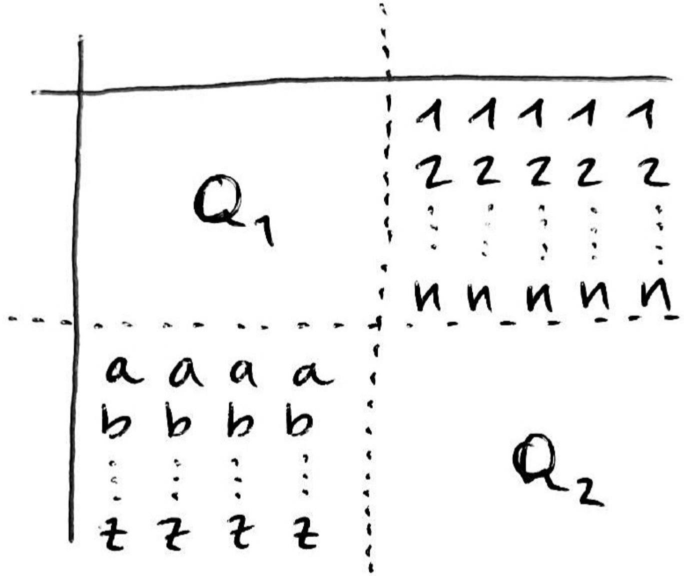
DEF. Q_1, Q_2-quandle. Definiamo la somma di quandle

$Q_1 \# Q_2 =$



DEF. Q_1, Q_2-quandle. Definiamo la <u>somma di quandle</u>

$$Q_1 \# Q_2 =$$



elementi di Q_1

elementi di Q_2

Nello stesso modo, il <u>multiplo di un quandle Q</u>

$$kQ := \underbrace{Q \# Q \# \cdots \# Q}_{k \text{ volte}}$$

PROP. (1) $Q_1 \# Q_2$ è non connesso

(2) Q_1, Q_2 fedeli $\Longrightarrow$ $Q_1 \# Q_2$ fedele

(3) $\#$ è commutativa e associativa

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

PROP. (1) $Q_1 \# Q_2$ è non connesso

(2) Q_1, Q_2 fedeli $\Rightarrow$ $Q_1 \# Q_2$ fedele

(3) $\#$ è commutativa e associativa

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

COR. $H(kQ) \xrightarrow[k \to +\infty]{} 0$.

Dunque, non esiste un lower bound per quandle fedeli.

$\boxed{\text{ENTROPIA E H, S, P}}$

ENTROPIA E H, S, P

$\boxed{P}$ $H(\mathcal{Q}_1 \times \mathcal{Q}_2) = \dots$

(a) $H(\mathcal{Q}_1) + H(\mathcal{Q}_2)$

(b) $H(\mathcal{Q}_1) \cdot H(\mathcal{Q}_2)$

(c) $\max \{ H(\mathcal{Q}_1), H(\mathcal{Q}_2) \}$

$\boxed{\text{ENTROPIA E H, S, P}}$

$\boxed{P}$ $H(\mathcal{Q}_1 \times \mathcal{Q}_2) = \dots$

(a) $H(\mathcal{Q}_1) + H(\mathcal{Q}_2)$

(b) $H(\mathcal{Q}_1) \cdot H(\mathcal{Q}_2)$

(c) $\max\{H(\mathcal{Q}_1), H(\mathcal{Q}_2)\}$

<u>PROP.</u> $H(\mathcal{Q}_1 \times \mathcal{Q}_2) = H(\mathcal{Q}_1) + H(\mathcal{Q}_2)$.

$\boxed{H}$ $Q_1 \twoheadrightarrow Q_2$. Allora

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

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

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

$\boxed{H}$ $Q_1 \twoheadrightarrow Q_2$. Allora

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

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

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

<u>PROP.</u> $Q_1 \twoheadrightarrow Q_2 \implies H(Q_2) \leq H(Q_1)$

<u>COR.</u> $H(Q/\alpha) \leq H(Q)$

$\boxed{5}$ $Q_1 \hookrightarrow Q_2$. Allora

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

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

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

$\boxed{5}$ $Q_1 \hookrightarrow Q_2$. Allora

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

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

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

Purtroppo, nessuna delle precedenti.

<u>ES.</u>

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

Core (D_3)

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

$\boxed{5}$ $Q_1 \hookrightarrow Q_2$. Allora

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

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

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

Purtroppo, nessuna delle precedenti.

<u>ES</u>.

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

Core(D_3)

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

$Q_1 \hookrightarrow Q_2$

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

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

<u>Oss.</u> $Q_1 \leq Q_2 \Rightarrow H(Q_1) \leq H(Q_2)$ non vale neanche per quandle connessi: (SmallQuandle(21,9) in RIG)

<u>OSS.</u> $Q_1 \leq Q_2 \Rightarrow H(Q_1) \leq H(Q_2)$ non vale neanche per quandle connessi: (SmallQuandle(21,9) in RIG)

<u>PROP.</u> $Q_1 \leq Q_2$ quandles, $|Q_1| = m$, $|Q_2| = n$. Allora

$$H(Q_1) \leq \frac{n^2}{m^2} H(Q_2)$$

<u>OSS.</u> È una stima spesso molto larga, ma sembra non si possa fare di meglio...

$\boxed{\#}$ $H(a_1 \# a_2) = \dots$

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

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

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

(d) Nessuna delle precedenti.

$\boxed{\#}$ $H(Q_1 \# Q_2) = \dots$

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

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

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

(d) Nessuna delle precedenti.

Ancora, nessuna delle precedenti.

<u>Prop.</u> Q_1, Q_2 quandles, $|Q_1| = n$, $|Q_2| = m$. Allora

$$H(Q_1 \# Q_2) \leq 1 + \left(\frac{n^2}{m^2+n^2}\right) H(Q_1) + \left(\frac{m^2}{m^2+n^2}\right) H(Q_2)$$

CONCLUSIONI

- l'entropia permette di misurare e verificare alcune proprietà dei quandles, e si comporta relativamente bene rispetto alle costruzioni universali
- Tutto si può generalizzare a tabelle di moltiplicazione. Nei gruppi, quasigruppi e loop è banale.

CONCLUSIONI

- l'entropia permette di misurare e verificare alcune proprietà dei quandles, e si comporta relativamente bene rispetto alle costruzioni universali

- Tutto si può generalizzare a tabelle di moltiplicazione. Nei gruppi, quasigruppi e loop è banale.

Nuovi Orizzonti

- Migliorare le stime di $H(Q_1 \hookrightarrow Q_2)$ e $H(Q_1 \# Q_2)$, dove possibile.

- Esiste un lowerbound di entropia per quandle $\left\{ \begin{array}{l} \text{– connessi} \\ \text{– fedeli} \\ \text{– non latini} \end{array} \right.$?

GRAZIE PER L' ATTENZIONE !

spaggiari@karlin.mff.cuni.cz.

Ringraziamenti

(1) M. Vergoni e UNIFI per l'invito

(2) Prof. D. Stonovský per gli indispensabili colloqui

(3) LateX Beamer per le slides.