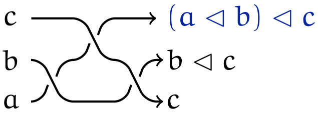
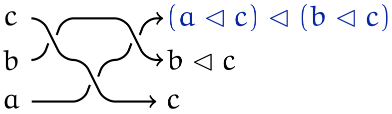
More algebraic connections: SD and the Yang–Baxter equation, Leibniz algebras etc.

Victoria LEBED, Trinity College Dublin (Ireland)

Denver, July 2017



$\overset{\text{RIII}}{\sim}$



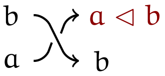
Part 1:

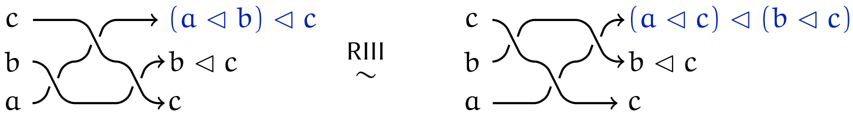
Self-Distributivity and Representations of Braid Groups

1 Coloring invariants for positive braids

Self-distributivity: $\boxed{(a \lhd b) \lhd c = (a \lhd c) \lhd (b \lhd c)}$

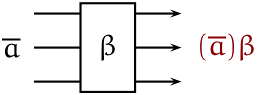
Diagram colorings by $(S, \lhd)$
for positive braids:





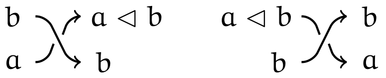
$\mathrm{End}(S^n) \leftarrow B_n^+$	RIII	$(a \lhd b) \lhd c = (a \lhd c) \lhd (b \lhd c)$

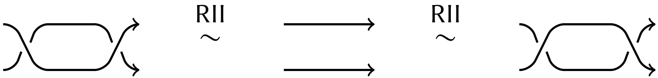
B_n^+ is the monoid of positive braids.



2 Coloring invariants for braids

Diagram colorings by $(S, \triangleleft)$
for braids:





$\mathrm{End}(S^n) \leftarrow B_n^+$	RIII	$(a \triangleleft b) \triangleleft c = (a \triangleleft c) \triangleleft (b \triangleleft c)$	shelf
$\mathrm{Aut}(S^n) \leftarrow B_n$	& RII	$\forall b,\ a \mapsto a \triangleleft b$ invertible	rack
$S \hookrightarrow (S^n)^{B_n}$		$a \triangleleft a = a$	quandle

$a \mapsto (a, \ldots, a)$

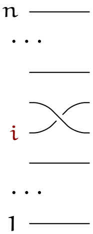
B_n is the group of braids.

3 Recovering familiar B_n-representations

$\mathrm{End}(S^n) \leftarrow B_n^+$	RIII	$(a \triangleleft b) \triangleleft c = (a \triangleleft c) \triangleleft (b \triangleleft c)$	shelf
$\mathrm{Aut}(S^n) \leftarrow B_n$	& RII	$\forall b,\ a \mapsto a \triangleleft b$ invertible	rack
$S \hookrightarrow (S^n)^{B_n}$ $a \mapsto (a, \dots, a)$		$a \triangleleft a = a$	quandle

Examples:

S	$a \triangleleft b$	$(S, \triangleleft)$ is a	in braid theory
${}_{\mathbb{Z}[t^{\pm 1}]}\mathrm{Mod}$	$ta + (1-t)b$	quandle	(red.) Burau: $B_n \to GL_n(\mathbb{Z}[t^{\pm}])$

$\rho_B($ 

$) = I_{i-1} \oplus \begin{pmatrix} 1-t & 1 \\ t & 0 \end{pmatrix} \oplus I_{n-i-1}$

3 Recovering familiar B_n-representations

$\mathrm{End}(S^n) \leftarrow B_n^+$	RIII	$(a \triangleleft b) \triangleleft c = (a \triangleleft c) \triangleleft (b \triangleleft c)$	shelf
$\mathrm{Aut}(S^n) \leftarrow B_n$	& RII	$\forall b,\ a \mapsto a \triangleleft b$ invertible	rack
$S \hookrightarrow (S^n)^{B_n}$		$a \triangleleft a = a$	quandle

$a \mapsto (a, \ldots, a)$

Examples:

S	$a \triangleleft b$	$(S, \triangleleft)$ is a	in braid theory
${}_{\mathbb{Z}[t^{\pm 1}]}\mathrm{Mod}$	$ta + (1-t)b$	quandle	(red.) Burau: $B_n \to GL_n(\mathbb{Z}[t^{\pm}])$
group	$b^{-1}ab$	quandle	Artin: $B_n \hookrightarrow \mathrm{Aut}(F_n)$
twisted linear quandle			Lawrence–Krammer–Bigelow
$\mathbb{Z}$	$a+1$	rack	$\lg(w), \mathrm{lk}_{i,j}$
free shelf			Dehornoy: order on B_n
Laver tables			???

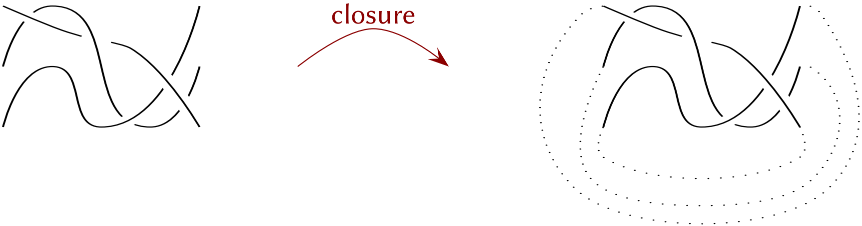
4 Coloring counting invariants for knots

Theorem (*Joyce & Matveev* '82):

✓ The number of colorings of a diagram D of a knot K by a quandle $(S, \triangleleft)$ yields a knot invariant.

✓ $\#\operatorname{Col}_{S,\triangleleft}(D) = \#\operatorname{Hom}_{\mathsf{Quandle}}(Q(K), S) = \operatorname{Tr}(\rho_S(\beta))$

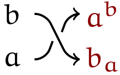
- $Q(K)$ = fundamental quandle of K
  (a weak universal knot invariant);
- $\operatorname{closure}(\beta) = K$;
- $\rho_S \colon B_n \to \operatorname{Aut}(S^n)$ is the S-coloring invariant for braids.



Part 2:

Self-Distributivity and the Yang–Baxter Equation

5 Upper strands matter!

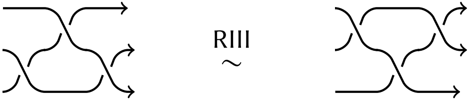
Diagram colorings by (S, σ): 

$\sigma(a, b) = (b_a, a^b)$

Ex.: $\sigma_{SD}(a, b) = (b, a \lhd b)$

RIII-compatibility $\iff$ set-theoretic Yang–Baxter equation:

$\boxed{\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 \colon S^{\times 3} \to S^{\times 3}}$ $\qquad \sigma_1 = \sigma \times \mathrm{Id}_S,\ \sigma_2 = \mathrm{Id}_S \times \sigma$



In particular,

$$\boxed{\text{YBE for } \sigma_{SD} \quad \iff \quad \text{self-distributivity for } \lhd}$$

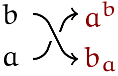
Drinfel′d ’92:

Set-theoretic solutions $\overset{\text{linearize}}{\rightsquigarrow}$ $\overset{\text{deform}}{\rightsquigarrow}$ linear solutions.

Example: $\sigma(a, b) = (b, a)$ $\rightsquigarrow$ R-matrices.

6 YBE as a unifying framework

Diagram colorings by (S, σ):



$\sigma(a, b) = (b_a, a^b)$

Ex.: $\sigma_{\triangleleft}(a, b) = (b, a \triangleleft b)$

RIII-compatibility $\iff$ set-theoretic Yang–Baxter equation:

$\boxed{\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 : S^{\times 3} \to S^{\times 3}}$ $\quad \sigma_1 = \sigma \times \mathrm{Id}_S,\ \sigma_2 = \mathrm{Id}_S \times \sigma$

Exotic example: $\sigma(a, b) = (b, a)$ $\rightsquigarrow$

$\sigma_{Lie}(a \otimes b) = b \otimes a + \hbar 1 \otimes [a, b]$, where $[1, a] = [a, 1] = 0$:

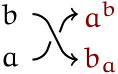
YBE for σ_{Lie}	$\iff$	Leibniz relation for $[\,]$

Very exotic example: $\sigma_{Ass}(a, b) = (a * b, 1)$, where $1 * a = a$:

YBE for σ_{Ass}	$\iff$	associativity for $*$

7 YBE and braids and knots

Diagram colorings by (S, σ):



$\sigma(a, b) = (b_a, a^b)$

Ex.: $\sigma_{\triangleleft}(a, b) = (b, a \triangleleft b)$

RIII	$\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$	YB operator
& RII	σ invertible & $\forall b,\ a \mapsto a^b$ and $a \mapsto a_b$ invertible	birack
& RI	$\exists$ a bijection t such that $\sigma(t(a), a) = (t(a), a)$	biquandle

Result: Coloring invariants of braids and knots.

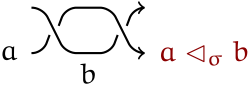
Bad news: These invariants give nothing new!

Unrelated question: Describe free biracks and biquandles.

8 From biracks to racks

Thm (*Soloviev & Lu–Yan–Zhu* '00, *L.–Vendramin* '17):

✓ Birack (S,σ) $\quad\rightsquigarrow\quad$ its structure rack $(S,\lhd_\sigma)$:



✓ This is a projection **Birack** $\twoheadrightarrow$ **Rack** along involutive biracks:

- $\lhd_{\sigma_\lhd} = \lhd$;
- $\lhd_\sigma$ trivial $\quad\Longleftrightarrow\quad$ $\sigma^2 = \mathrm{Id}$.

✓ The structure rack remembers a lot about the birack:

- $(S,\lhd_\sigma)$ quandle $\quad\Longleftrightarrow\quad$ (S,σ) biquandle;
- σ and $\lhd_\sigma$ induce isomorphic B_n-actions on S^n

$\Longrightarrow$ same braid and knot invariants.

⚠ $(S,\sigma) \ncong (S,\sigma_{\lhd_\sigma})$ as biracks!

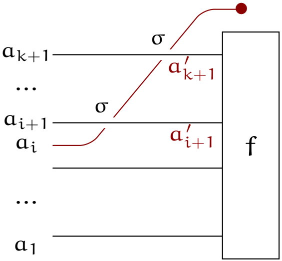
9 Braided cohomology

Carter–Elhamdadi–Saito '04 & *L.* '13:

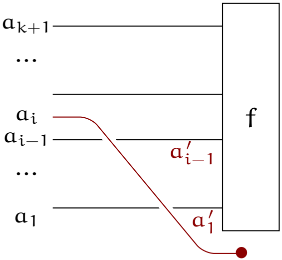
$$C^k_{\mathrm{Br}}(S,\mathbb{Z}_n) = \mathrm{Map}(S^{\times k},\mathbb{Z}_n),$$

$$(d^k_{\mathrm{Br}} f)(a_1,\ldots,a_{k+1}) = \sum_{i=1}^{k+1} (-1)^{i-1}\big(f(a_1,\ldots,a_{i-1},(a_{i+1},\ldots,a_{k+1})_{a_i}) - f((a_1,\ldots,a_{i-1})^{a_i},a_{i+1},\ldots,a_{k+1})\big)$$

$= \sum (-1)^{i-1} \Big($



$-$



$\Big)$

$\rightsquigarrow$ Braided cohomology $H^k_{\mathrm{Br}}(S,\mathbb{Z}_n)$.

10 Why I like braided cohomology

① (Higher) braid and knot invariants:

$$d^2_{\mathrm{Br}}\phi = 0 \implies \phi \text{ refines (positive) braid coloring invariants,}$$
$$\phi = d^1_{\mathrm{Br}}\psi \implies \text{the refinement is trivial.}$$

Question: New invariants?

Answer: I don't know!

② $d^2_{\mathrm{Br}}\phi = 0 \implies$ diagonal deformations of σ:

$$\sigma_q(a,b) = q^{\phi(a,b)}\sigma(a,b).$$

(*Freyd–Yetter* '89, *Eisermann* '05)

10 Why I like braided cohomology

③ Unifies cohomology theories for

✓ self-distributive structures $\sigma_{SD}(a,b) = (b \lhd a, a)$

✓ associative structures $\sigma_{Ass}(a,b) = (a * b, 1)$

✓ Lie algebras $\sigma_{Lie}(a \otimes b) = b \otimes a + 1 \otimes [a,b]$

....

+ explains parallels between them,

+ suggests theories for new structures.

10 Why I like braided cohomology

④ For certain σ, computes the group cohomology of

$$\boxed{\mathrm{As}(S,\sigma) = \langle\, S \mid ab = b_a\, a^b,\ \text{where } \sigma(a,b) = (b_a\,,\ a^b)\ \rangle}$$

Example: $\mathrm{As}(S,\sigma_{SD}) = \langle\, S \mid a\,b = b\,(a \triangleleft b)\ \rangle = \mathrm{As}(S,\triangleleft)$.

$$\begin{tikzcd}
\boxed{\text{YB world}} \arrow[r, bend right, "\text{examples}"'] & \boxed{\text{ass. world}} \arrow[l, bend right, "\text{methods}"']
\end{tikzcd}$$

Applications: Cohomology of factorized groups & plactic monoids.

Rmk: Structure racks know a lot about structure groups.

Part 3:

Self-Distributivity and

Leibniz Algebras

11 Leibniz algebras and their cohomology

Bloh '65, *Loday & Cuvier* '91: A Leibniz algebra is a vector space V endowed with a bracket $[,]$ satisfying the Leibniz identity

$$[v,[w,u]] = [[v,w],u] - [[v,u],w].$$

It is a Lie algebra if $[,]$ is antisymmetric: $[v,w] = -[w,v]$.

Leibniz (Loday) cohomology:

$$\begin{tikzcd}
\mathbf{Lei} \arrow[d, shift left, two heads, "\text{anti-symm.}"] & V \arrow[r, mapsto] & (\mathrm{Hom}(T(V),X), d^*_{Lei}) \arrow[d, two heads, "\text{anti-symm.}"] & \text{Cuvier–Loday} \\
\mathbf{Lie} \arrow[u, shift left, hook] & V \arrow[u, mapsto] \arrow[r, mapsto] & (\mathrm{Hom}(\Lambda(V),X), d^*_{CE}) & \text{Chevalley–Eilenberg}
\end{tikzcd}$$

$$d^{k-1}_{Lei} f(v_1 \dots v_k) = \sum_{1 \leqslant i < j \leqslant k} (-1)^{j-1} f(v_1 \dots v_{i-1}[v_i, v_j]v_{i+1} \dots \widehat{v_j} \dots v_k)$$

Leibniz (Loday) cohomology:

$$\begin{tikzcd}
\mathbf{Lei} \arrow[d, shift left, "\text{anti-symm.}"] & V \arrow[r, mapsto] & (\mathrm{Hom}(T(V), X), d^*_{Lei}) \arrow[d, "\text{anti-symm.}"] & \text{Cuvier–Loday} \\
\mathbf{Lie} \arrow[u, hook, shift left] & V \arrow[u, mapsto] \arrow[r, mapsto] & (\mathrm{Hom}(\Lambda(V), X), d^*_{CE}) & \text{Chevalley–Eilenberg}
\end{tikzcd}$$

$$d^{k-1}_{Lei} f(v_1 \dots v_k) = \sum_{1 \leqslant i<j \leqslant k} (-1)^{j-1} f(v_1 \dots v_{i-1} [v_i, v_j] v_{i+1} \dots \widehat{v_j} \dots v_k)$$

Remark: This is the braided cohomology of

$$\sigma_{Lie}(a \otimes b) = b \otimes a + 1 \otimes [a, b],$$

where $[1, a] = [a, 1] = 0$. Also, recall that

$$\boxed{\text{YBE for } \sigma_{Lie} \quad \Longleftrightarrow \quad \text{Leibniz relation for } [\,]}$$

This is one of the explanations of the choice of the Leibniz lift of the Jacobi identity for Lie algebras.

12 Coquecigrue problem

Question (*Loday* '93): $\dfrac{\text{Lie groups}}{\text{Lie algebras}} = \dfrac{???}{\text{Leibniz algebras}}$.

Suggestion (*Kinyon* '07): ??? = Lie rack (= smooth rack).

Criterion 1 Lie's third theorem:

$$\begin{tikzcd}
\mathbf{LeiAlg} \arrow[r, shift left, "\text{integration (1)}"] & \mathbf{LieRack} \arrow[l, shift left, "\text{tangent (2)}"] \\
\mathbf{LieAlg} \arrow[u, hook] \arrow[r, shift left, "\text{integration}"] & \mathbf{LieGroup} \arrow[l, shift left, "\text{tangent}"] \arrow[u, "\text{Conj}"']
\end{tikzcd}$$

(2) *Kinyon* '07;

(1) *Covez* '10: locally,
Bordemann–Wagemann '16: globally, not functorially.

13 Coquecigrue problem

Question (*Loday* '93): $\frac{\text{Lie groups}}{\text{Lie algebras}} = \frac{???}{\text{Leibniz algebras}}$.

Suggestion (*Kinyon* '07): ??? = Lie rack (= smooth rack).

Criterion 2 Cohomological:

(*Loday* '95): A graded algebra morphism, which is iso in degree 1:

$$H^*_{CE}(\mathfrak{g}, X) \to H^*_{Lei}(\mathfrak{g}, X).$$

(*Covez* '12): A graded algebra morphism, injective in degree 1:

$$H^*_{G}(G, X) \to H^*_{R}(\mathrm{Conj}(G), X).$$

Part 4:

Self-Distributivity and

Cryptography

SD-based authentication scheme

Dehornoy '06: For certain shelves $(S, \triangleleft)$, it is difficult to reconstruct b from $(a\,,\ a \triangleleft b)$.

$\rightsquigarrow$ Authentication scheme:

✓ Adam's private key: $s \in S$.

✓ Public key: $(p, p') \in S \times S$, satisfying $p' = p \triangleleft s$.

✓ Procedure: Adam chooses $r \in S$, and sends to Eve

$x = p \triangleleft r,$
$x' = p' \triangleleft r,$
$y = s \triangleleft r.$

Eve checks $x' = x \triangleleft y$, i.e.,

$$(p \triangleleft s) \triangleleft r = (p \triangleleft r) \triangleleft (s \triangleleft r).$$

15 Multi-distributivity

Multi-shelf = set S + operations $(\lhd_i)_{i \in I}$ satisfying

$$(a \lhd_i b) \lhd_j c = (a \lhd_j c) \lhd_i (b \lhd_j c). \tag{MD}$$

Kalka–Teicher '13: SD-based key establishment protocol.

Take $I_A, I_B \subseteq I$ and $S_A, S_B \subseteq S$.

✓ Adam chooses a private key $(a, c, j) \in S \times S_A \times I_A$, and sends to Eve $a \lhd_j c$ and $x_\beta \lhd_j c$ for generators x_β of S_B.

✓ Eve chooses a private key $(b, i) \in S_B \times I_B$, and sends to Adam $x_\alpha \lhd_i b$ for generators x_α of S_A.

✓ Both compute the key (MD).

Suitable types of multi-shelves: S is a group, $f_i, g_i, h_i \in \mathrm{End}(G)$, $a_i \in G$

1) $y \lhd_i x = f_i(x^{-1}) g_i(y) h_i(x)$,
2) $y \lhd_i x = x f_i(y) a_i f_i(x^{-1})$.