THE GEOMETRY MONOID OF AN IDENTITY

Patrick DEHORNOY
Université de Caen

Main idea: For each algebraic identity I, (more generally, for each family of algebraic identity, actually for each equational variety), there exists a specific monoid $\mathcal{M}_I$ that describes the geometry of I.

$\longrightarrow$ Studying $\mathcal{M}_I$ with convenient algebraic tools leads in good cases to results about I and I-systems (= those algebraic systems that satisfy I, typically:

- solving the word problem,
- constructing free I-systems.

$\longrightarrow$ Applies at least to

- $x(yz) = (zy)z$ (Thompson, MacLane, Stasheff);
- $x(yz) = (xy)(xz)$ ($\longrightarrow$ braid applications);
- $x(yz) = (xy)(yz)$ (new)...

Free I-systems:

Suppose I is an algebraic identity involving one binary operation, for instance

$$x * (y * z) = (x * y) * (y * z). \qquad (I)$$

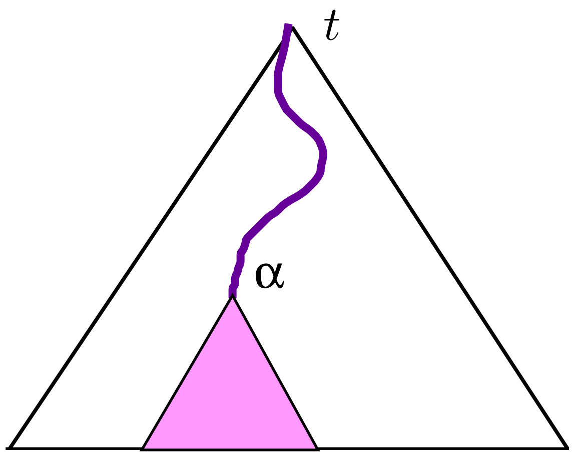
Fix a set of variables X;
Let T_X be the set of all terms constructed from X and a binary operator;
Let $\equiv_I$ be the congruence on (the absolutely free algebra) T_X generated by the instances of I, i.e., the pairs $(t_1 * (t_2 * t_3), (t_1 * t_2) * (t_2 * t_3))$.

Fact: *$T_X/\equiv_I$ is a free I-system based on X.*

$\longrightarrow$ What does "applying I to a term t" mean?
$\longrightarrow$ Iteratively replacing some subterm of t which has the form $t_1 * (t_2 * t_3)$ with the corresponding term $(t_1 * t_2) * (t_2 * t_3)$, or conversely: depends on orientation and on position.

The operators I_a^+ :

Fix an address system in terms :
$\longrightarrow$ view them as binary trees and specify a subterm by describing the path from the root:



the α-th subterm of t

Definition: I_a^+ is the (partial) operator on T_X that maps t to t' iff the α-th subterm of t can be expressed as $t_1 * (t_2 * t_3)$ and t' is obtained from t by replacing this subterm with the corresponding $(t_1 * t_2) * (t_2 * t_3)$ (= "applying I to t at α"); write I_α^- for the inverse of I_a^+.

The geometry monoid of I:

Definition: The geometry monoid $\mathcal{M}_I$ of I is the monoid generated by all operators I_a^+ and I_α^-.

Fact: *Two terms t, t' are $\equiv_I$-equivalent iff some element of $\mathcal{M}_I$ maps t to t':*

$$t' = (t)w,$$

where w is a finite sequence of signed addresses (describing how to transform t to t' using I).

Question: How to use $\mathcal{M}_I$? In particular: Can the study of $\mathcal{M}_I$ solve the word problem of $\equiv_I$?

$\longrightarrow$ difficult, because (i) $\mathcal{M}_I$ is not a group, (ii) there is no uniform connection between $\mathcal{M}_I$, which acts on terms, and terms themselves;

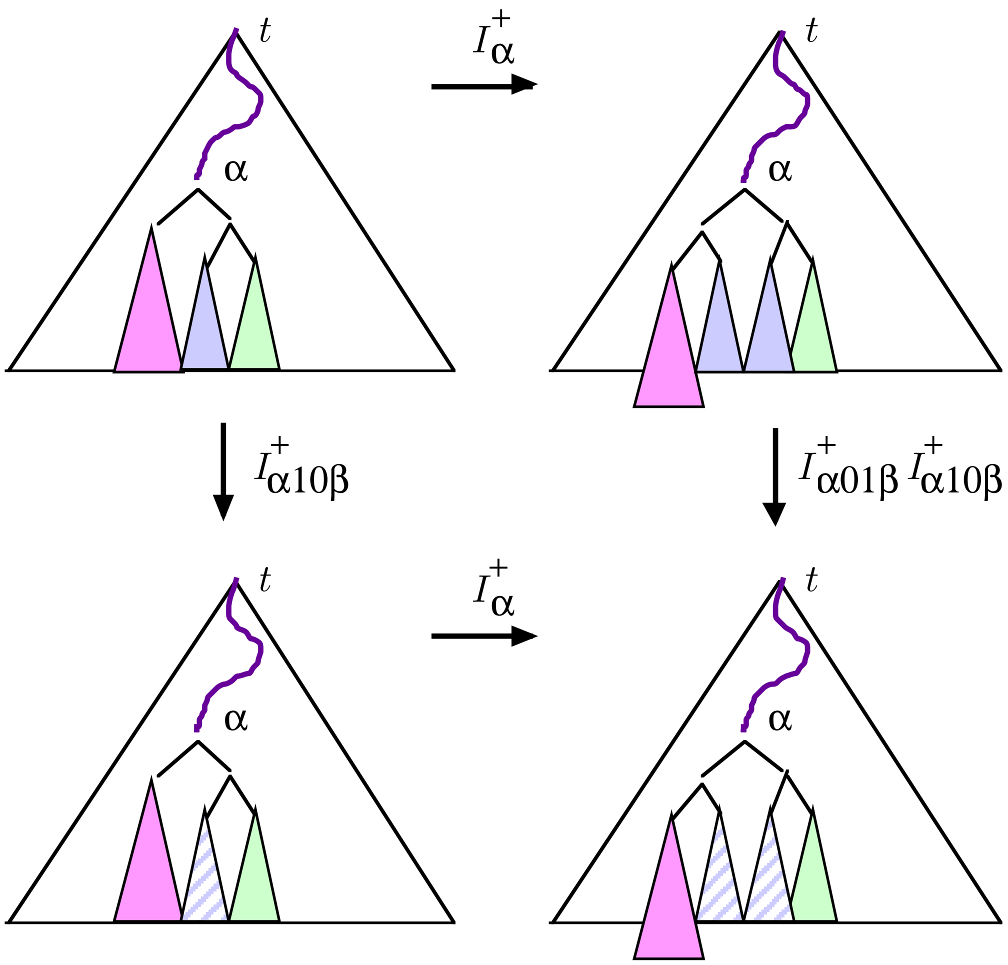
$\longrightarrow$ solution when (i) $\mathcal{M}_I$ can be replaced with a group, (ii) $\mathcal{M}_I$ contains copies of the terms (in some sense...)

The group G_I:

Principle: Guess a presentation of $\mathcal{M}_I$, then introduce the group G_I defined by this presentation:
$\longrightarrow$hopefully: G_I ressembles $\mathcal{M}_I$ enough.

Geometry relations in $\mathcal{M}_I$:

Example: $I^+_{\alpha 10\beta} I^+_{\alpha} = I^+_{\alpha} I^+_{\alpha 01\beta} I^+_{\alpha 10\beta}$, or simply $\alpha 10\beta \cdot \alpha \equiv \alpha \cdot \alpha 01\beta \cdot \alpha 10\beta$.



Definition: The group G_I is the group

$$\langle \alpha \in \{0,1\}^*; R_I \rangle,$$

with R_I the list of all relations:

$$\alpha 0\beta \cdot \alpha 1\gamma = \alpha 1\gamma \cdot \alpha 0\beta,$$
$$\alpha 0\beta \cdot \alpha = \alpha \cdot \alpha 00\beta,$$
$$\alpha 10\beta \cdot \alpha = \alpha \cdot \alpha 01\beta \cdot \alpha 10\beta,$$
$$\alpha 11\beta \cdot \alpha = \alpha \cdot \alpha 11\beta,$$
$$\alpha 1 \cdot \alpha \cdot \alpha 0 = \alpha \cdot \alpha 1 \cdot \alpha.$$

$\longrightarrow$ How to study such a group?

$\longrightarrow$ G_I is the group of fractions of a monoid which admits (right) least common multiples (proving this requires specific algebraic tools, mainly word reversing, reminiscent of Garside's analysis of the braid groups.

The blueprint of a term:

$\longrightarrow$ How to connect the monoid $\mathcal{M}_I$ and the group G_I?
$\longrightarrow$ How to use G_I for studying I?

Fact: *For each t in $T_{\{x\}}$, we have $t^{p+1} \equiv_I t * x^p$ for p large enough.*

Proof: For $t = x$, equality. For $t = t_1 * t_2$:

$$\begin{aligned} x^{p+1} &\equiv_I t_1 * x^p \\ &\equiv_I t_1 * (t_2 * x^{p-1}) \\ &\equiv_I (t_1 * t_2) * (t_2 * x^{p-1}) \\ &\equiv_I (t_1 * t_2) * x^p = t * x^p \end{aligned}$$

for p large enough. □

$\longrightarrow$ Some element of $\mathcal{M}_I$, depending on t, must witness for this term equivalence: use this element, or, rather, its copy in G_I, as the blueprint of t.

Definition: For t in $T_{\{x\}}$, the blueprint of t is the element χ_t of G_I inductively defined by $\chi_x = 1$, and

$$\chi_t = \chi_{t_1} \cdot \mathrm{sh}_1(\chi_{t_2}) \cdot \emptyset \cdot \mathrm{sh}_1(\chi_{t_1}^{-1})$$

for $t = t_1 * t_2$, where $\mathrm{sh}_1 : \alpha \mapsto 1\alpha$ for each address α.

By construction, we have

$$(x^{p+1})\chi_t = t * x^p$$

for p large enough: thus χ_t, which lives in G_I, describes how to construct t from scratch using I. ($\longrightarrow$ not every identity is eligible).

Now, use χ_t as a syntactic counterpart to t:
Assume $t' \equiv_I t$, hence $t' = (t)w$ for some w. Then

$$x^{p+1} \xrightarrow{\chi_{t'}} t' * x^p$$

$$x^{p+1} \xrightarrow{\chi_t} t * x^p \xrightarrow{\mathrm{sh}_0(w)} t' * x^p$$

where $\mathrm{sh}_0 : \alpha \mapsto 0\alpha$:

$\longrightarrow$ if we guessed the relations correctly, we should have $\chi_{t'} \equiv \chi_t \cdot \mathrm{sh}_0(w)$;
$\longrightarrow$ If this is true, this must be checkable by a direct computation.
$\longrightarrow$ This is true.

Proposition: *(solution to the word problem)*
For t, t' in $T_{\{x\}}$, the following are equivalent:
(i) We have $t \equiv_I t'$;
(ii) In the group G_I, the element $\chi_t^{-1}\chi_{t'}$ belongs to the subgroup generated by the elements 0α.

$\longrightarrow$ For which identities does this approach work?
• associativity $\longrightarrow$ Thompson's group F;
• self-distributivity $\longrightarrow$ an extension of Artin's braid group B_∞;
• the current identity $x(yz) = (xy)(xz)$...
$\longrightarrow$ In each case: specific algebraic study (the groups are very different).

References

P. Dehornoy; Braids and Self-Distributivity; Progress in Math. vol. 192, Birkhäuser (2000).

Preprints:
http://www.math.unicaen.fr/∼dehornoy/