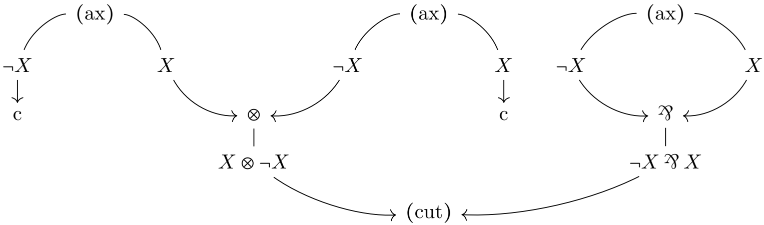
Proofs, rings, and ideals

Daniel Murfet, William Troiani

University of Melbourne, University of Sorbonne Paris Nord

2022

Geometry of Interaction



Permutations	Operators	Rings
$(12)(34)(56)$	$[\![\pi]\!] = \begin{pmatrix} 0 & 0 & p & q \\ 0 & qp^* + qp^* & 0 & 0 \\ p^* & 0 & 0 & 0 \\ q^* & 0 & 0 & 0 \end{pmatrix}$	?

Formulas

Definition (Formulas)

- *Unoriented atoms* $X, Y, Z, \ldots$
- *An oriented atom* (or *atomic proposition*) is a pair $(X, +)$ or $(X, -)$ where X is an unoriented atom.

Pre-formulas:

- Any atomic proposition is a preformula.
- If A, B are pre-formulas then so are $A \otimes B$, $A \parr B$.
- If A is a pre-formula then so is $\neg A$.

Formulas: quotient of pre-formulas:

$$\neg(A \otimes B) \sim \neg B \parr \neg A \qquad \neg(A \parr B) \sim \neg B \otimes \neg A$$

$$\neg(X, +) \sim (X, -) \qquad \neg(X, -) \sim (X, +)$$

Polynomial ring of a proof structure

Definition (Sequence of (un)oriented atoms)

Let A be a formula with sequence of oriented atoms $\big((X_1, x_1), \dots, (X_n, x_n)\big)$. The *sequence of unoriented atoms* of A is $(X_1, \dots, X_n)$ and the *set of unoriented atoms* of A is the disjoint union $\{X_1\} \coprod \cdots \coprod \{X_n\}$.

Definition (Polynomial ring P_A of a formula A)

P_A is the free commutative k-algebra on the set of unoriented atoms of A:

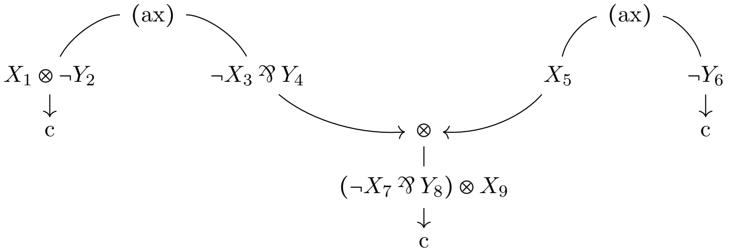
$$P_A = k[X_1, \dots, X_n]$$

Let π be a proof structure with edge set E and denote by A_e the formula labelling edge $e \in E$. The *polynomial ring* of π, denoted P_π is the following, where U_e is the set of unoriented atoms of A_e.

$$P_\pi := \bigotimes_{e \in E} P_{A_e} \cong k[\coprod_{e \in E} U_e]$$

Polynomial ring example

Let π denote the following proof net.



$P_\pi =$

$$k\Big[\{X\} \coprod \{Y\} \coprod \{X\} \coprod \{Y\} \coprod \{X\} \coprod \{Y\} \coprod \{X\} \coprod \{Y\} \coprod \{X\}\Big]$$

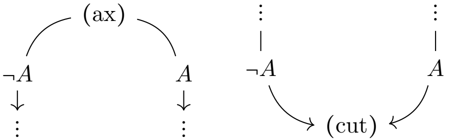
$$= k[X_1, Y_2, X_3, Y_4, X_5, Y_6, X_7, Y_8, X_9]$$

But what about the links?

Links

Definition (Link ideal I_l, link coordinate ring R_l)

Axiom/Cut link l:

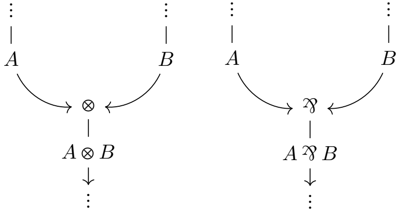


$\big((X_1, x_1), \ldots, (X_n, x_n)\big)$ is the sequence of oriented atoms of A, and $\big((Y_1, y_1), \ldots, (Y_m, y_m)\big)$ is that of B.

$$I_l \subseteq P_A \otimes P_{\neg A}$$
$$I_l = (X_i - X_i')_{i=1}^n = (X_i \otimes 1 - 1 \otimes X_i)_{i=1}^n \qquad R_l := P_A \otimes P_{\neg A} / I_l$$

Tensor/Par links

Tensor/Par link l:



Let $\boxtimes = \otimes$ if l is a tensor link, and $\boxtimes = \parr$ if l is a par link.

$$I_l \subseteq P_A \otimes P_B \otimes P_{A \boxtimes B}$$
$$I_l = (\{X_i - X_i'\}_{i=1}^n \cup \{Y_j - Y_j'\}_{j=1}^m)$$
$$= (\{X_i \otimes 1 \otimes 1 - 1 \otimes 1 \otimes X_i\}_{i=1}^n \cup \{1 \otimes Y_j \otimes 1 - 1 \otimes 1 \otimes Y_j\}_{j=1}^m)$$

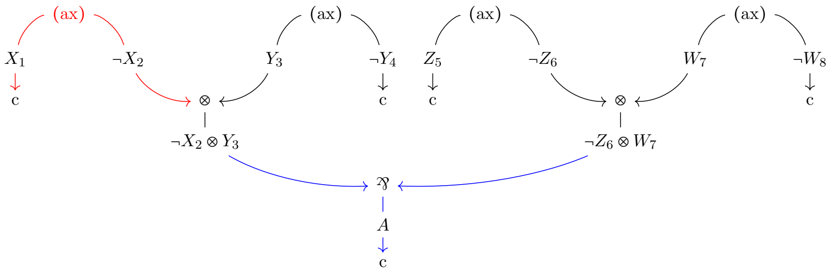
$$R_l = P_A \otimes P_B \otimes P_{A \boxtimes B} / I_l$$

Definition (Defining ideal I_π, coordinate ring R_π)

$I_\pi := \sum_l I_l \subseteq P_\pi$ where l ranges over all links of π. $R_\pi := P_\pi / I_\pi$.

Example of coordinate ring of a link

Let $A := (\neg X_2 \otimes Y_3) \parr (\neg Z_6 \otimes W_7)$.



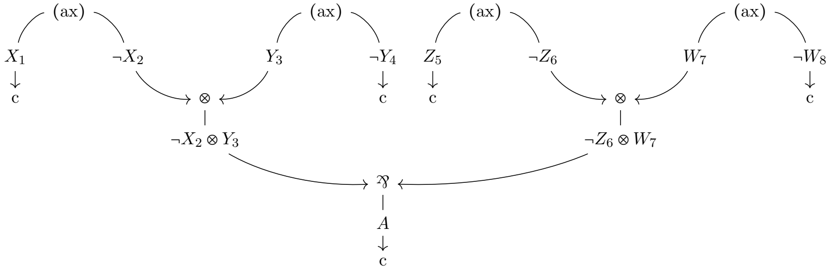
Let l denote the red axiom link, and l' denote the blue par link.

$$I_l = (X_1 - X_2) \subseteq k[X_1, X_2] \qquad R_l = k[X_1, X_2]/I_l \cong k[X_1]$$

$$I_{l'} = (X_2 - X_2', Y_3 - Y_3', Z_6 - Z_6', W_7 - W_7') \qquad R_{l'} = k[X_2, X_2', Y_3, Y_3', Z_6, Z_6', W_7, W_7']/I_{l'} \cong k[X_2, Y_3, Z_6, W_7]$$

Example of coordinate ring of a proof structure

$$A := (\neg X_2 \otimes Y_3) \parr (\neg Z_6 \otimes W_7)$$



$$\begin{aligned}
P_\pi &= k[X_1, X_2, X_2', X_2'', Y_3, Y_3', Y_3'', Y_4, Z_5, Z_6, Z_6', Z_6'', W_7, W_7', W_7'', W_8] \\
I_\pi &= (X_1 - X_2) + (Y_3 - Y_4) + (Z_5 - Z_6) + (W_7 - W_8) \\
&\quad + (X_2 - X_2', Y_3 - Y_3') + (Z_6 - Z_6', W_7 - W_7') \\
&\quad + (X_2' - X_2'', Y_3' - Y_3'', Z_6' - Z_6'', W_7' - W_7'') \\
R_\pi &= P_\pi / I_\pi \cong k[X, Y, Z, W]
\end{aligned}$$

Persistent walks

$$\begin{tikzcd}
 & (\mathrm{ax}) \arrow[dl, dash, bend right] \arrow[dr, dash, bend left] & \\
A \arrow[d] & & \neg A \arrow[d] \\
\vdots & & \vdots \\
X_1 \amalg \cdots \amalg X_n \arrow[rr, leftrightarrow, "J"] & & Y_1 \amalg \cdots \amalg Y_n
\end{tikzcd}
\qquad
\begin{tikzcd}
X_1 \amalg \cdots \amalg X_n \arrow[rr, leftrightarrow, "J"] & & Y_1 \amalg \cdots \amalg Y_n \\
\vdots & & \vdots \\
A \arrow[u] & & \neg A \arrow[u] \\
 & (\mathrm{cut}) \arrow[ul, dash, bend left] \arrow[ur, dash, bend right] &
\end{tikzcd}$$

$$\begin{tikzcd}
 & \vdots & & \vdots & \\
X_1 \amalg \cdots \amalg X_n \arrow[ddddrr, "I^1"] & A \arrow[u, dash] \arrow[dr, bend right] & & B \arrow[u, dash] \arrow[dl, bend left] & Y_1 \amalg \cdots \amalg Y_m \arrow[ddddll, "I^2"'] \\
 & & \boxtimes & & \\
 & & A \boxtimes B \arrow[u, dash] \arrow[d] & & \\
 & & \vdots & & \\
 & & X_1 \amalg \cdots \amalg X_n \amalg Y_1 \amalg \cdots \amalg Y_m & &
\end{tikzcd}$$

Persistent walks

$$\text{(ax)}, \text{(cut)} \qquad X_1 \amalg \cdots \amalg X_n \xleftrightarrow{\;J\;} Y_1 \amalg \cdots \amalg Y_n$$

$$\otimes, \parr \qquad X_1 \amalg \cdots \amalg X_n \xrightarrow{I^1} X_1 \amalg \cdots \amalg X_n \amalg Y_1 \amalg \cdots \amalg Y_m \xleftarrow{I^2} Y_1 \amalg \cdots \amalg Y_m$$

Definition

Let π be a proof structure admitting a conclusion A. Choose also an unoriented atom X in A. A **persistent walk** of X is a walk ν in π satisfying the following conditions.

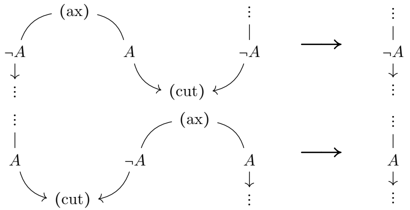
1. The formula A labels some edge e, the first edge e_1 of ν is e.
2. If $i > 1$ then X uniquely determines an edge $e_i \neq e_{i-1}$ adjacent with e_{i-1} via J, I^1, I^2.

Theorem

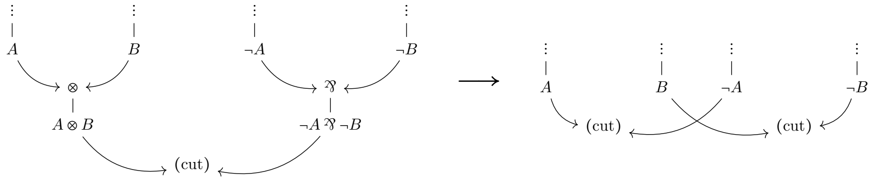
The coordinate ring of a proof structure π is isomorphic to a polynomial ring in n indeterminants, where the number of persistent walks in π is equal to $2n$.

Cut reduction

a-redexes:



m-redex:



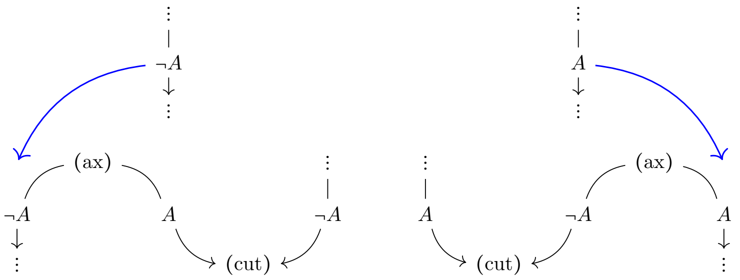
Modelling cut-reduction

Definition

Let $\gamma : \pi \longrightarrow \pi'$ be a reduction, there exists homomorphisms.

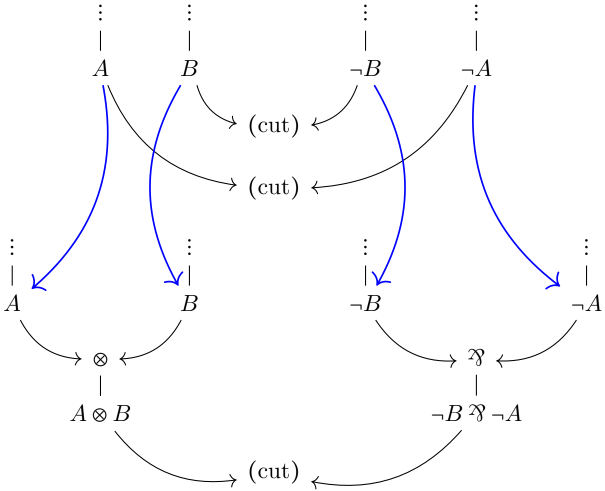
$$\begin{tikzcd} P_{\pi'} \arrow[r, bend left, "T_\gamma"] & P_\pi \arrow[l, bend left, "S_\gamma"] \end{tikzcd}$$

T_γ, γ reducing an a-redex:



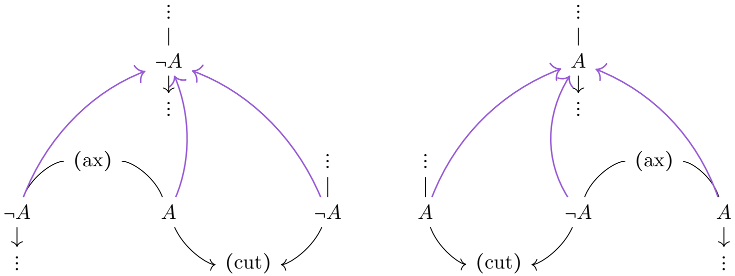
Modelling cut reduction

T_γ, γ reducing an m-redex:



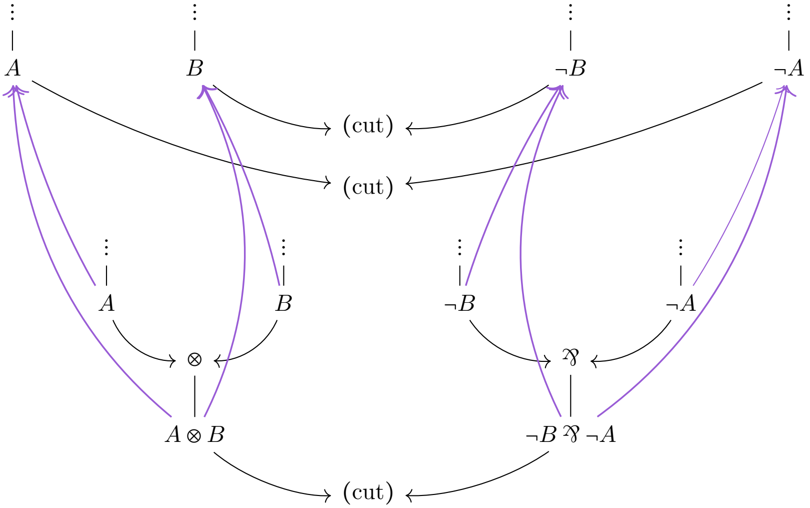
Modelling cut reduction

S_γ, γ reducing an a-redex.



Modelling cut reduction

S_γ, γ reducing an m-redex.



Cut elimination on the level of the coordinate rings

Proposition

Let γ be any reduction, we have $T_\gamma(I_{\pi'}) \subseteq I_\pi, S_\gamma(I_\pi) \subseteq I_{\pi'}$ and the induced morphisms of k-algebras $\overline{T}_\gamma, \overline{S}_\gamma$ making the following diagram commute, are mutually inverse isomorphisms. In the following, $p : P_\pi \twoheadrightarrow R_\pi$ and $p' : P_{\pi'} \twoheadrightarrow R_{P_{\pi'}}$ are projection maps.

$$\begin{tikzcd}
I_\pi \arrow[r] & P_\pi \arrow[r, two heads, "p"] \arrow[d, bend right, "S_\gamma"'] & R_\pi \arrow[d, bend right, "\overline{S}_\gamma"'] \\
I_{\pi'} \arrow[r, tail] & P_{\pi'} \arrow[r, two heads, "p'"] \arrow[u, bend right, "T_\gamma"'] & R_{\pi'} \arrow[u, bend right, "\overline{T}_\gamma"']
\end{tikzcd}$$

Permutation

Proposition

Let π be a proof net with single conclusion A with oriented atoms $\big((U_1, u_1), ..., (U_n, u_n)\big)$. Then $n = 2m$ is even, and there is a subsequence $i_1 < \cdots < i_m$ with complement $j_1 < \cdots < j_m$ in $\{1, \cdots, n\}$ such that $u_{i_a} = +, u_{j_a} = -$ for $1 \le a \le m$ and if we write $X_a = U_{i_a}, Y_a = U_{j_a}$ for $1 \le a \le m$ then β_+, β_- in the following diagram are isomorphisms.

$$\begin{tikzcd}
k[X_1, ..., X_m] \arrow[d] \arrow[dr, "\beta_+"] & \\
P_\pi \arrow[r, two heads] & R_\pi \\
k[Y_1, ..., Y_m] \arrow[u] \arrow[ur, "\beta_-"'] &
\end{tikzcd}$$

Furthermore, the composite $\beta_-^{-1}\beta_+ : k[X_1, .., X_m] \longrightarrow k[Y_1, ..., Y_m]$ is given for some permutation σ_π of $\{1, ..., m\}$ by:

$$\beta_-^{-1}\beta_+(X_i) = Y_{\sigma_\pi(i)}, \quad 1 \le i \le m$$

Proofs as permutations

Definition (The *essence* $\mathrm{Ess}\,\pi$ of π)

Let π admit no m-redexes and assume all conclusions of all axiom links are atomic. $\mathrm{Ess}\,\pi$ is the disjoint union of the unoriented atoms appearing as conclusions to axiom links which are not premise to cut links.

Definition

Let d_i denote the least integer such that

$$(\alpha_\pi \circ \gamma_\pi)^{d_i}(X) \in \mathrm{Ess}\,\pi$$

Notice that such an integer d_i always exists as π is a proof net. Define for any unoriented atom appearing in the conclusion to any axiom link in π:

$$\delta_\pi(X) = (\alpha_\pi \circ \gamma_\pi)^{d_i}(X)$$

Comparison

$$\begin{tikzcd}
k[X_1, ..., X_m] \arrow[d] \arrow[dr, two heads, "\beta_+"] & \\
P_\pi \arrow[r, two heads] & R_\pi \\
k[Y_1, ..., Y_m] \arrow[u] \arrow[ur, two heads, "\beta_-"'] &
\end{tikzcd}$$

$$\delta_\pi(X) = (\alpha_\pi \circ \gamma_\pi)^{d_i}(X) \qquad \beta_-^{-1}\beta_+(X_i) = Y_{\sigma(i)}$$

Proposition

Let π be a proof net with single conclusion A with sequence of oriented atoms given by: $\big((U_1, u_1), ..., (U_n, u_n)\big)$. Then for all $i = 1, ..., n$ we have:

$$\delta_\pi(U_i) = U_{\sigma(i)}$$

Division algorithm for polynomials in multiple variables

Choose an order $x_1 < \cdots < x_n$, this induces lexicographic order on the monic monomials of $k[x_1, ..., x_n]$ with respect to the degrees. Consider $\mathbb{C}[x > y]$.

$$y < xy < x^2 < x^2y^{10} < x^3 < \cdots$$

Now, divide according to leading terms!

$$
\begin{array}{ll}
q_0 : & \qquad\quad xy^2 \\
q_1 : & \qquad\quad y^2 \\
x^2y & \overline{)x^3y^3 + xy^2 - y} \\
x + y & \\
 & \;x^3y^3 \\
\hline
 & \qquad\quad xy^2 - y \\
 & \qquad\quad xy^2 + y^3 \\
\hline
 & \qquad\qquad -y - y^3
\end{array}
$$

Leading terms

Given polynomials $f_1, \ldots, f_n$ we have the following inclusion, where $\langle g_1, \ldots, g_m \rangle$ denotes the ideal generated by the polynomials $g_1, \ldots, g_m$.

$$\langle \mathrm{LT}\, f_1, \cdots, \mathrm{LT}\, f_n \rangle \subseteq \langle \mathrm{LT} \langle f_1, \ldots, f_n \rangle \rangle$$

This reverse inclusion does *not* hold in general. Indeed, consider the polynomial ring $k[x, y]$ with $y < x$. Let f_1, f_2 respectively denote the polynomials $x^3 - 2xy$ and $x^2 y - 2y^2 + x$. We have:

$$\{\mathrm{LT}\, f_1, \mathrm{LT}\, f_2\} = \{x^3, x^2 y\}$$

however, the following polynomial is in the ideal generated by $\{f_1, f_2\}$.

$$y(x^3 - 2xy) - x(x^2 y - 2y^2 + x) = -x^2$$

Hence, x^2 is in the leading ideal. However, x^2 is not in the ideal generated by the polynomials $x^3, x^2 y$.

Gröbner bases

Definition

A set of polynomials $\{f_1, \ldots, f_n\}$ satisfying the following:

$$\langle \mathrm{LT}\, f_1, \cdots \mathrm{LT}\, f_n \rangle = \langle \mathrm{LT}\{f_1, \ldots, f_n\} \rangle$$

is a *Gröbner basis* for the ideal $\langle f_1, \ldots, f_n \rangle$ generated by $f_1, \ldots, f_n$.

Definition

The S*-polynomial* of polynomials $g, h \in k[x_1, \ldots, x_n]$ is defined to be the following, where $\beta = (\beta_1, \ldots, \beta_n)$ where $\beta_i = \max\big((\deg g)_i, (\deg h)_i\big)$..

$$S(g, h) := \frac{x^\beta}{\mathrm{LT}\, g} g - \frac{x^\beta}{\mathrm{LT}\, h} h$$

This is indeed a polynomial, and is designed to obtain cancellation of leading terms.

Buchberger Algorithm

Definition

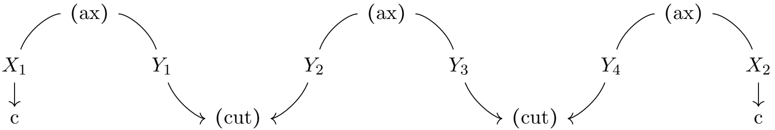
Given a finite sequence $G = (f_1, ..., f_m)$ of polynomials in $k[x_1, ..., x_n]$ we define the *Buchberger algorithm* as follows.

Algorithm

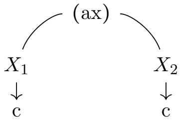
On input G.

1. For all $i < j$ calculate $S(f_i, f_j)$.
2. Consider the lexicographic order on the set of pairs (i, j) where $i, j \in \{1, ..., m\}$. From smallest to largest, with respect to this order, divide $S(i, j)$ by G. If the remainder is 0 for all pairs (i, j) then terminate the algorithm and return the sequence G. Otherwise, let (i', j') be the least pair such that division of $S(i', j')$ by G results in a non-zero remainder r.
3. Append the polynomial r to the end of the sequence G and return to Step (1).

Let π denote the following proof net.



π reduces to π':

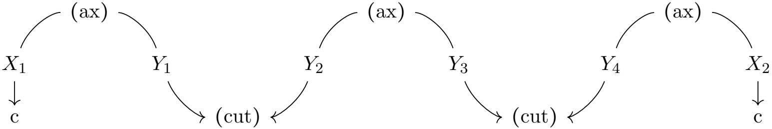


We now consider the sets of generators of the defining ideals of π and π'.

$$G_\pi := \{X_1 - Y_1, Y_1 - Y_2, Y_2 - Y_3, Y_3 - Y_4, Y_4 - X_2\}, \quad G_{\pi'} := \{X_1 - X_2\}$$

$$Y_1 > Y_2 > Y_3 > Y_4 > X_1 > X_2$$

There *is* something to do



$$G_\pi = \{f_1 = X_1 - Y_1,\ f_2 = Y_1 - Y_2,\ f_3 = Y_2 - Y_3,\ f_4 = Y_3 - Y_4,\ f_5 = Y_4 - X_2\}$$

$$Y_1 > Y_2 > Y_3 > Y_4 > X_1 > X_2$$

The leading terms of $f_1, \ldots, f_5$ respectively are $-Y_1, Y_1, Y_2, Y_3, Y_4$ and the leading term of $f_1 + \cdots + f_5$ is X_1. Hence:

$$X_1 \in \mathrm{LT}\langle G_\pi \rangle, \qquad X_1 \notin \langle \mathrm{LT}\, G_\pi \rangle$$

Thus, G_π is *not* Gröbner basis.

We now calculate the 10 S-polynomials which arise from G_π.

$$S(f_1, f_2) = Y_2 - X_1 \qquad S(f_1, f_3) = Y_1Y_3 - Y_2X_1 \qquad S(f_1, f_4) = Y_1Y_4 - X_1X_3$$

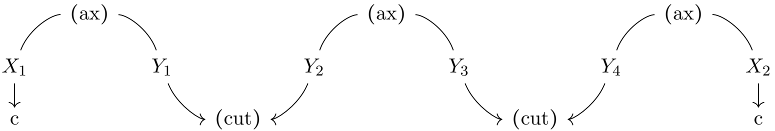
$$S(f_1, f_5) = Y_1X_2 - X_1Y_4 \qquad S(f_2, f_3) = Y_1Y_3 - Y_2^2 \qquad S(f_2, f_4) = Y_1Y_4 - Y_2Y_3$$

$$S(f_2, f_5) = Y_1X_2 - Y_2Y_4 \qquad S(f_3, f_4) = Y_2Y_4 - Y_2^2 \qquad S(f_3, f_5) = Y_2X_2 - Y_3Y_4$$

$$S(f_4, f_5) = Y_3X_2 - Y_4^2$$

For each $i > j$, $i, j \in \{1, ..., 5\}$ we now divide $S(f_i, f_j)$ by G. In fact, this always gives a remainder zero except for the particular case when $(i, j) = (1, 2)$, which we show on the next slide.

Division



$$G_\pi = \{f_1 = X_1 - Y_1,\ f_2 = Y_1 - Y_2,\ f_3 = Y_2 - Y_3,\ f_4 = Y_3 - Y_4,\ f_5 = Y_4 - X_2\}$$

$$
\begin{array}{rl}
 & (0,0,1,1,1) \\
G_\pi & \overline{)\,Y_2 - X_1} \\
 & \quad Y_2 - Y_3 \\
\hline
 & \qquad\quad Y_3 - Y_4 \\
 & \qquad\quad Y_3 - X_1 \\
\hline
 & \qquad\qquad\qquad Y_4 - X_1 \\
 & \qquad\qquad\qquad Y_4 - X_2 \\
\hline
 & \qquad\qquad\qquad\qquad X_2 - X_1
\end{array}
$$

$$\big(G_\pi \cup \{X_2 - X_1\}\big) \cap k[X_1, X_2] = G_{\pi'}$$

Summary

- We defined a new Geometry of Interaction model and showed how it fits into the existing literature (GoI 0, GoI 1).
- We related "plugging of formulas" to an already existing algorithm.

Next steps:

- More algebraic structure, eg, Koszul Complexes.
- Extend this model to MELL.
- Use this as a foundation for more exotic models of MLL/MELL.
  - Quantum error correction codes.
  - Landau-Ginzburg models, the bicategory of hypersurface singularities.

Thank you

Questions?

(Bonus frame) Proof sketch

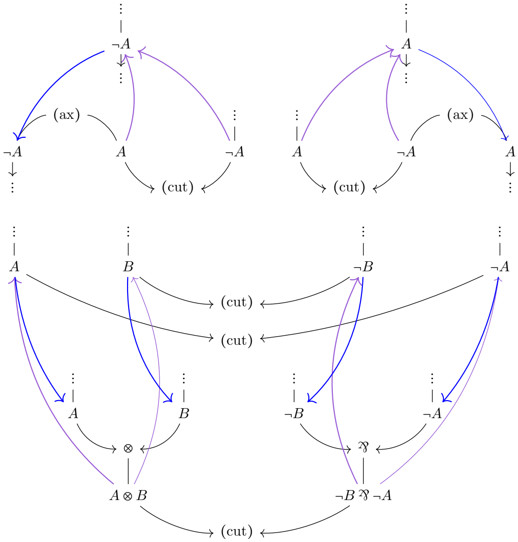
$$\begin{tikzcd} I_\pi \arrow[r] & P_\pi \arrow[r, two heads, "p"] \arrow[d, bend right, "S_\gamma"'] & R_\pi \arrow[d, bend right, "\overline{S}_\gamma"'] \\ I_{\pi'} \arrow[r, tail] & P_{\pi'} \arrow[r, two heads, "p'"] \arrow[u, bend right, "T_\gamma"'] & R_{\pi'} \arrow[u, bend right, "\overline{T}_\gamma"'] \end{tikzcd}$$

Existence: easy. $\overline{T}_\gamma, \overline{S}_\gamma$ isomorphisms: suffices to show:

$$\overline{T}_\gamma \overline{S}_\gamma p = p$$
$$\overline{S}_\gamma \overline{T}_\gamma p' = p'$$

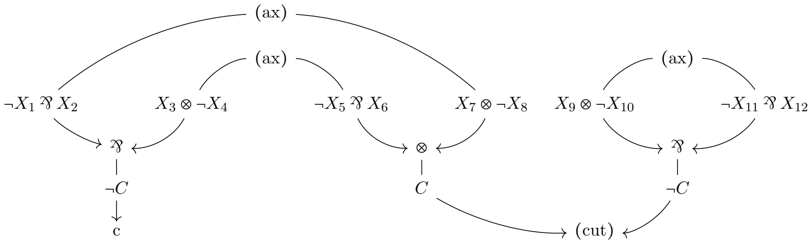
as p, p' are surjective. This is equivalent to $p' S_\gamma T_\gamma = p', p T_\gamma S_\gamma = p$, or $p'(S_\gamma T_\gamma - 1) = 0, p(T_\gamma S_\gamma - 1) = 0$. It suffices to check this on generators, ie, on unoriented atoms. It is clear that $S_\gamma T_\gamma = 1$, however we have $T_\gamma S_\gamma \neq 1$. The circumstances where this is the case is indicated schematically on the next slide.

(Bonus frame) Proof continued

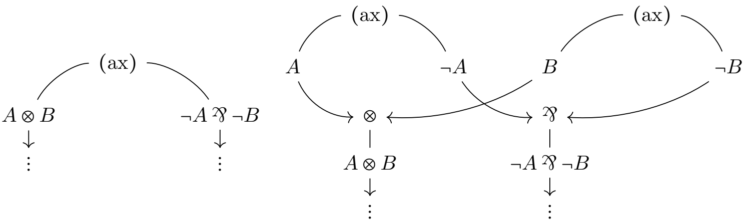


(Bonus frame) Example of Proposition

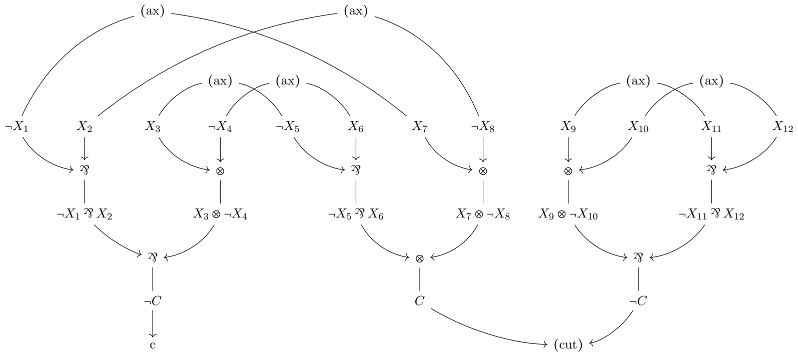
Let π denote the following proof net.



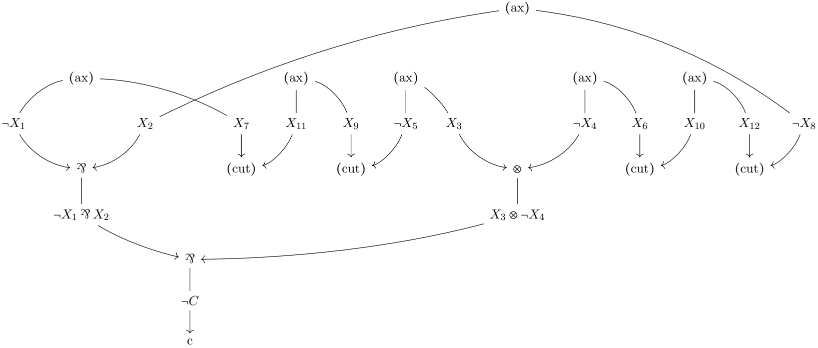
We apply η-expansion:



(Bonus frame) After η-expansion



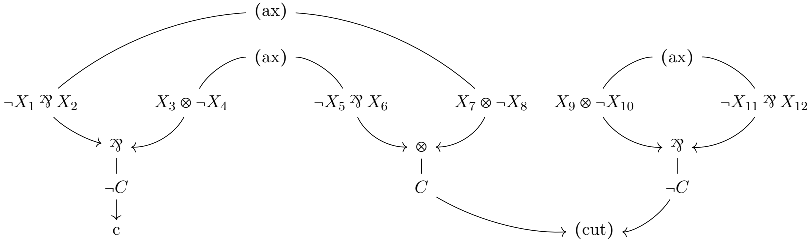
(Bonus frame) After reducing m-redexes



$$\delta(X_1) = X_3 \quad \delta(X_3) = X_1 \quad \delta(X_4) = X_2 \quad \delta(X_2) = X_4$$

(Bonus frame) Comparison continued

Returning to π:



The following are elements of the defining ideal I_π of π.

$$X_2 - X_8 \quad X_8'' - X_{12}'' \quad X_{12} - X_{10} \quad X_{10}'' - X_6'' \quad X_6 - X_4$$

and so are $X_i - X_i', X_i' - X_i''$ for $i = 2, 4, 6, 10, 12$. Hence $\sigma(2) = 4$ and $\sigma(4) = 2$. Similarly, $\sigma(1) = 3$ and $\sigma(3) = 1$.

$$\delta(X_1) = X_3 \quad \delta(X_3) = X_1 \quad \delta(X_4) = X_2 \quad \delta(X_2) = X_4$$