Proofs as coordinate rings (talk)

William Troiani

May 30, 2022

1 Introduction

Computation, considered as an invisible mental process, is a naive stance. The crucial point is that there are genuine mathematical and physical properties of computation which are independent of the choice of implementation.

A historically significant indication that this might be the case, was the thought experiment often referred to as *Maxwell's Demon*, where it appears as though heat is being transfered from a cooler body to a warmer body, which contradicts the second law of thermodynamics. This thought experiment includes an onlooker (the demon) who stands idle and makes decisions. A proposed solution was that the decision process inside the demon's mind was to be included as part of the physical system. That is, the *computation* being performed by the Demon was a *physically* relevant part of the experiment.

So it makes sense to ask about the inherrent *physical* properties of computation, but what about the inherrent *mathematical* properties of computation? Can one dream of a *geometric* theory of computation? What about an *algebraic* one?

Today's talk presents a humble step in this direction. I introduce a fresh perspective on Girard's *Geometry of interaction program*, which modelled linear logic as operators upon a Hilbert space. There, each proof was associated to a bounded linear operator, here, each proof will be associated to a *coordinate ring*, that is, a quotient of a polynomial ring.

2 Proofs

Definition 2.0.1 (Formulas)**.**

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

Pre-formulas:

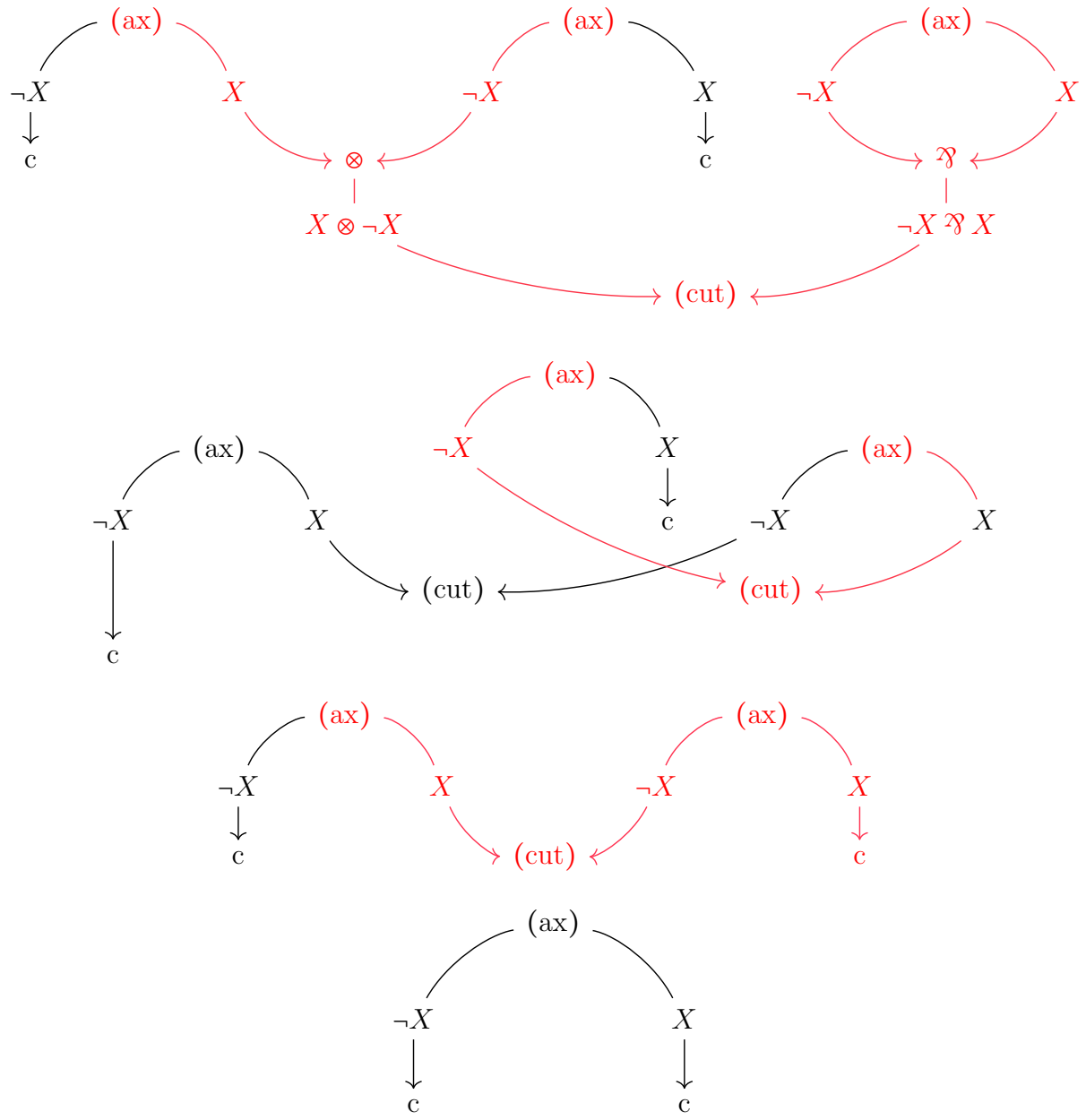
- Any atomic proposition is a preformula.
- If A, B are pre-formulas then so are $A \otimes B$, $A \parr B$.
- If A is a pre-formula then so is $\neg A$.

Formulas: quotient of pre-formulas:

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

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

Example 2.0.2.



3 Elimination Theory

The problem of finding the defining equations of images of algebraic sets under algebraic maps is a classical area of algebraic geometry called *elimination theory*, of which we will use only the most elementary parts.

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!

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

Given polynomials $f_1, ..., f_n$ generating an ideal I.

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

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 $x^2y - 2y^2 + x$. We have:

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

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

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

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

Definition 3.0.1. A generating set $f_1, \ldots, f_n$ for an ideal I is a *Gröbner basis* if

$$\langle \mathrm{LT}\, f_1, \ldots, \mathrm{LT}\, f_n \rangle = \langle \mathrm{LT}\, I \rangle \tag{1}$$

Definition 3.0.2. The *S-polynomial* of polynomials $g, h \in k[x_1, ..., x_n]$ is defined to be the following, where $\beta = (\beta_1, ..., \beta_n)$ 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.

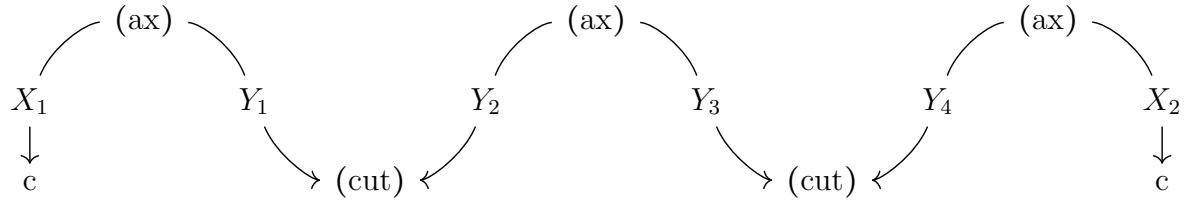
BUCHBERGER'S ALGORITHM.

4 Combining the two

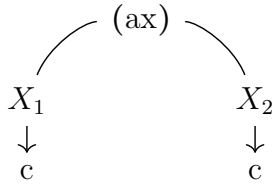
Definition 4.0.1 (Sequence of (un)oriented atoms)**.** Let A be a formula with sequence of oriented atoms $\big((X_1, x_1), ..., (X_n, x_n)\big)$. The *sequence of unoriented atoms* of A is $(X_1, ..., X_n)$ and the *set of unoriented atoms* of A is the disjoint union $\{X_1\} \coprod \cdots \coprod \{X_n\}$.

EXAMPLE OF A COORDINATE RING. USE THE EXAMPLE BLOW, *NOT* OUR FAVOURITE EXAMPLE.

Example 4.0.2. Let π denote the following proof net. We assume that X is an atomic formula, and we include artificial labels for clarity, in the following, X_1, Y_2, Y_4 all denote the formula $\neg X$ and Y_1, Y_3, X_2 denote the formula X.



The proof net π is equivalent under cut elimination to the following proof net, which we denote by π'.



We define a total order $>$ on the monomials in $k[Y_1, Y_2, Y_3, Y_4, X_1, X_2]$ via lexicographic order with respect to the following.

$$Y_1 > Y_2 > Y_3 > Y_4 > X_2 > X_1 \tag{2}$$

We now consider the sequences of generators $\mathcal{G}_\pi$, $\mathcal{G}_{\pi'}$ respectively of the defining ideals of π, π'.

$$\mathcal{G}_\pi \coloneqq (Y_1 - Y_2, Y_1, -X_1, Y_2 - Y_3, Y_3 - Y_4, Y_4 - X_2), \quad \mathcal{G}_{\pi'} \coloneqq (X_2 - X_1) \tag{3}$$

To ease the notation, we respectively let f_1, f_2, f_3, f_4, f_5 denote the polynomials $Y_1 - Y_2, X_1 - Y_1, Y_2 - Y_3, Y_3 - Y_4, Y_4 - X_2$. We make the observation that $\mathcal{G}_\pi$ is *not* a Gröbner basis. To see this, we notice that the leading terms of $f_1, ..., f_5$ respectively are Y_1, Y_1, Y_2, Y_3, Y_4 and the leading term of $f_1 + \ldots + f_5$ is X_1. Since X_1 is not in the ideal generated by Y_1, Y_1, Y_2, Y_3, Y_4, the underlying set of $\mathcal{G}_\pi$ cannot be a Gröbner basis.

The Buchberger Algorithm will calculate $S(f_1, f_2) = Y_2 - X_1$ and then divide this by the sequence $\mathcal{G}_\pi$.

$$\begin{array}{rl} & (0,0,1,1,1) \\ (f_1, f_2, f_3, f_4, f_5) & \overline{)Y_2 - X_1} \\ & \underline{\quad Y_2 - Y_3} \\ & \quad Y_3 - X_1 \\ & \quad \underline{Y_3 - Y_4} \\ & \quad\quad Y_4 - X_1 \\ & \quad\quad \underline{Y_4 - X_2} \\ & \quad\quad\quad X_2 - X_1 \end{array} \tag{4}$$

We thus append the polynomial $X_2 - X_1$ to the end of $\mathcal{G}_\pi$, this results is a sequence with underlying set a Gröbner basis so this sequence is $\overline{\mathcal{G}_\pi}$.

The Elimination Theorem (Thorem 2 of [**?**, §3.1]) states that $|\overline{\mathcal{G}_\pi}| \cap k[X_1, X_2] = \{X_2 - X_1\}$ is a Gröbner basis for the elimination ideal corresponding to eliminating the variables Y_1, Y_2, Y_3, Y_4. We notice that this set $\{X_2 - X_1\}$ is the underlying set of $\mathcal{G}_{\pi'}$.

Consider the following system of equations.

$$x_1 = x_2 \tag{5}$$
$$x_2 = y_1 \tag{6}$$
$$y_1 = y_2 \tag{7}$$
$$y_2 = x_3 \tag{8}$$

If we wish to eliminate the variables y_1, y_2, then we can substitute (6) into (7), and then the result of this into (8), obtaining the following system.

$$x_1 = x_2 \tag{9}$$
$$x_2 = x_3 \tag{10}$$

This successfully eliminates the variables y_1, y_2, but the Buchberger Algorithm would not arrive at these equations, instead a further substitution of (5) into (10) will be performed in order to arrive at the following equations.

$$x_1 = x_2 \tag{11}$$

$$x_1 = x_3 \tag{12}$$

We will define the Lazy Division Algorithm wway!!!!(Algorithm **??**) which is an adaptation to the Division Algorithm, and use this adaptation inside the Buchberger Algorithm (the resulting algorithm we call the Elimination Algorithm) which avoids some of these inefficiencies. This adaptation is what will be related to cut-elimination.