AOC Publication

Systematization of Knowledge – Gröbner Basis Algorithms for Arithmetization Oriented Ciphers

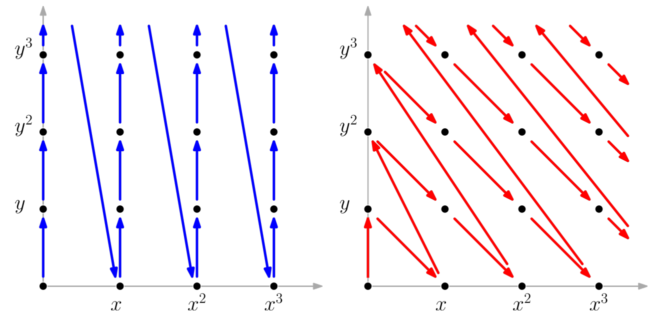
by Jan Ferdinand Sauer   Jun 28, 2021   0 Comment

We have published an introductory paper [0] about Gröbner basis attacks on AOCs. Whether you're looking for an intuitive way into the world of Gröbner basis computations, or want to look up a certain detail about the attack pipeline, or are simply curious to learn a few neat tricks and algorithms, it should be to your liking. A background in computer science probably helps when reading the document, but I encourage you to have a look in any case.

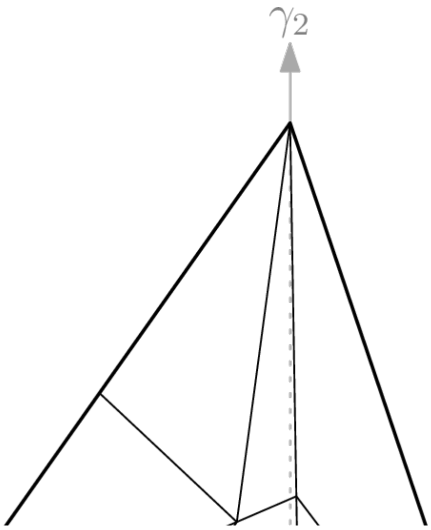
Broadly summarized, the paper

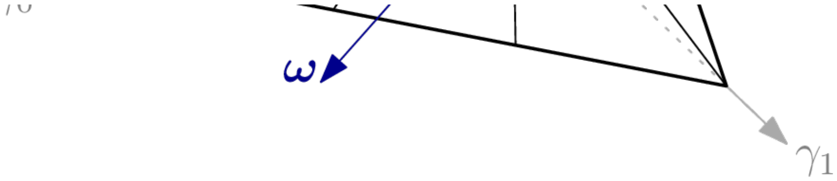
- covers the **basic definitions**.
- shows how **solution readout** works.
- explains **Buchberger's algorithm**, as well as **$\mathbf{F}_4$** and **$\mathbf{F}_5$**.
- describes the XL-family, especially **Mutant XL**.
- goes into great detail about term-order change algorithm **FGLM**.
- intuits the **Gröbner Walk**.
- presents interesting and relevant **open questions**.

The document aims for intuition as opposed to complete rigor, but the many references make it easy to start digging deeper. A major plus: explaining things intuitively often means pictures! For example, did you know what a monomial order looks like when visualized? Below, you can see the orders *lex* and *degrevlex* in blue and red, respectively.



Or how about the Gröbner fan of a particular polynomial ideal? Admittedly, if you already know what a Gröbner fan is, you have probably seen pictures of some. But if you don't yet know, maybe below illustration of a Gröbner Walk piques your curiosity to find out what it is all about.





No matter your motivation or background, I hope the SoK has something for you. And if you have any feedback, don't hesitate to contact us!

[0] https://ia.cr/2021/870

Jan Ferdinand Sauer

Website: https://asdm.gmbh

Leave a Reply

Logged in as Jan Ferdinand Sauer Logout

Comment

Submit