From: (b) (6)
To: Perlner, Ray A. (Fed)
Subject: More on UOV
Date: Saturday, September 25, 2021 6:22:16 PM

Hi, Ray,

I've been thinking about why this UOV with more equations than oil subspace bothers me. I want to re-address this point a bit.

If we have an oil subspace of dimension m and we have m equations and n variables, then when we project to a codim p subspace we end up with still m equations, but then n-p variables and an m-p dimensional oil subspace.

If we have an oil subspace of dimension o and we have m equation and n variables, then when we project to a codim p subspace we end up with still m equations, but then n-p variables and an o-p dimensional oil subspace.

In either case, it may be easy to recover AN oil subspace, but perhaps you might need to project further in the first case and then get a bunch of extraneous oil subspaces that don't correspond to the real one.

I did a quick experiment with the magma online calculator. (I could only do extremely small examples because of the memory limit. I didn't try to program the poly-time algorithm for this.) What I found is that when I use o+1 equations and n is large enough for the polytime algorithm to work, I get extraneous solutions. So it doesn't seem that it works directly to solve. I didn't check for intersections, but it seems unlikely.

That algorithm works beyond the bound I mentioned for n smaller by Binomial(b,2) at a superpolynomial cost in b. So there is some hope that using a number of equations that is slightly above the bound and maybe intersecting different solutions can result in something. I think it's worth looking. I'm going to need access to actual magma, though...

My experiments show that when I choose o+3 equations, then every subset of that many equations uniquely corresponds to the actual oil subspace. The problem is that this is for a number of variables for which you would only expect an oil subspace of size o+1, so that means that in the case of n=74, you would need something like 13 equations or so. Still, that is only Binomial(7,2) smaller than the number of variables you would need to solve with m=13. So the complexity of that algorithm is O(g(b)m^3n^wlg(q)^2), where g(b) is the complexity of solving a quadratic system of b variables and equations. Here b=7, it seems. So it looks like it is feasible to solve for 11-dimensional oil subspaces for sets of 13 equations, and if it turns out that these are essentially unique, then intersecting even two of them should give us the correct oil subspace and break the scheme.

I just need real magma now...

Cheers,
Daniel