SEARCHING FOR POINTS WITH THE ELKIES ANTS-IV ALGORITHM

MARK WATKINS

1. General description (due to Stoll and Elkies)

Let V be a (smooth) projective variety in $\mathbf{P}^n$. We want to find $\mathbf{Q}$-rational points on it. Choose a prime p. For each local solution $\vec{s}$ to V over $\mathbf{F}_p$, we determine a $\mathbf{Z}_p$-lattice $\Lambda_p \subseteq \mathbf{Z}^{n+1}$ such that every lift of $\vec{s}$ is in this lattice. Then we look for short vectors in $\Lambda_{\mathbf{R}} \cap \mathbf{Z}^{n+1}$. When we have a curve, the resulting lattice will be represented as a matrix

$$\begin{pmatrix} 1 & \star & \star & \dots & \star \\ 0 & p & p\star & \dots & p\star \\ 0 & 0 & p^2 & \dots & p^2\star \\ \dots & & & \dots & \\ 0 & 0 & 0 & \cdots & p^n \end{pmatrix}$$

where the first row is a lift of the local solution, the second row corresponds to a linear approximation, the third to a quadratic approximation, and so on. The stars are p-adic integers, but we can make the matrix integral via restriction mod p^n and then lifting to $\mathbf{Z}$. In higher dimensions, we have more tangent directions; for instance, with surfaces we have 2 diagonal entries of size p, three of size p^2, four of size p^3, and so on, until we reach the requisite $(n+1)$ rows. For instance, for a curve $f(x,y,z)$ in $\mathbf{P}^2$ we take a local solution $(1 : y_0 : z_0)$, lift it to a mod-p^2 solution $(1 : y_1 : z_1)$, and the second row is $(0 : p : p\xi)$ where ξ is $-(\partial y)f(1,y_1,z_1)/(\partial z)f(1,y_1,z_1)$.

We want to get all linear combinations of the rows of the above matrix (reduced mod p^k for some k) with all entries less than a height bound H, and then test each to see if it corresponds to a global solution; this is efficiently achieved via LLL-reduction on the rows. The resulting reduced matrix will have entries of size $D^{1/(n+1)}$ where D is the determinant, and with this reduced matrix, we will want to take linear combinations of the rows with coefficients bounded by about $H/D^{1/(n+1)}$. To make this quantity a small constant, we take H of size $D^{1/(n+1)}$; for instance, in the example below we have $n = 3$ and $D = p^6$ for a quadric intersection, and take H of size $p^{3/2}$.

2. Quadric Intersections

Let Q be an intersection of two quadrics in $\mathbf{P}^3$ given by

$$F_a(w,x,y,z) = a_{11}W^2 + a_{12}^S WX + a_{13}^S WY + a_{14}^S WZ + \\ a_{22}X^2 + a_{23}^S XY + a_{24}^Z XZ + a_{33}Y^2 + a_{34}^S YZ + a_{44}Z^2 = 0$$

and similarly with b_{ij} for the other quadric. The S-superscript here reminds us that we have symmetrised the 16 coefficients of the symmetric matrix down to just 10 coefficients.

Let p be an auxiliary prime for which the quadric intersection has good reduction. We then find run over all local solutions mod p, and for each such solution get a matrix whose first row is a lift of local solution to mod p^3, and such that any linear combination of its rows is a solution mod p^3. We then apply lattice reduction to this matrix, and search for global solutions of small height. The first difficulty is to generate all local solutions. We could use an iterative resultant method on Q itself, but this leads to slowness in the finding of roots of polynomials mod p. Instead we find one local point and draw lines through it; this yields a ternary cubic, and for this we apply the same trick, thus reducing to solving a quadratic.

2.1. **Parametrisation of local solutions.** Let $(1 : x_0 : y_0 : z_0)$ be a local solution mod p to Q. We parametrise other solutions via $(1 : x_0 + t : y_0 + At : z_0 + Bt)$, taking note that solutions $(1 : x_0 : Y : Z)$ and $(0 : X : Y : Z)$ can easily be handled separately. We note that

$$\begin{aligned}0 &= (f(1, x_0 + t, y_0 + At, z_0 + Bt) - f(1, x_0, y_0, z_0))/t \\ &= [a_{22} + a^S_{23}A + a^S_{24}B + a_{33}A^2 + a^S_{34}AB + a_{44}B^2]t + x_0(2a_{22} + a^S_{23}A + a^S_{24}B)+ \\ &\qquad + y_0(a^S_{23} + a_{33}A + a^S_{34}B) + z_0(a^S_{24} + a^S_{34}A + 2a_{44}B) + (a^S_{12} + a^S_{13}A + a^S_{14}B)\end{aligned}$$

and similarly for g. So we have two linear equations involving t, and equate the solutions to get

$$\begin{aligned}&[a_{22} + a^S_{23}A + a^S_{24}B + a_{33}A^2 + a^S_{34}AB + a_{44}B^2]\cdot \\ &\quad\cdot [x_0(2b_{22} + b^S_{23}A + b^S_{24}B) + y_0(b^S_{23} + b_{33}A + b^S_{34}B)+ \\ &\qquad\qquad + z_0(b^S_{24} + b^S_{34}A + 2b_{44}B) + (b^S_{12} + b^S_{13}A + b^S_{14}B)] = \\ &[b_{22} + b^S_{23}A + b^S_{24}B + b_{33}A^2 + b^S_{34}AB + b_{44}B^2]\cdot \\ &\quad\cdot [x_0(2a_{22} + a^S_{23}A + a^S_{24}B) + y_0(a^S_{23} + a_{33}A + a^S_{34}B)+ \\ &\qquad\qquad + z_0(a^S_{24} + a^S_{34}A + 2a_{44}B) + (a^S_{12} + a^S_{13}A + a^S_{14}B)].\end{aligned}$$

We can write this in terms of a ternary equation as

$$\begin{aligned}h(A, B) = c_{300}A^3 &+ c_{210}A^2B + c_{120}AB^2 + c_{030}B^3 \\ &+ c_{201}A^2 + c_{021}B^2 + c_{111}AB + c_{102}A + c_{012}B + c_{003} = 0\end{aligned}$$

where

$$\begin{gathered}c_{300} = g_Aa_{33} - f_Ab_{33}, \quad c_{030} = g_Ba_{44} - f_Bb_{44}, \quad c_{003} = g_0a_{22} - f_0b_{22}, \\ c_{210} = g_Aa^S_{34} + g_Ba_{33} - f_Ab^S_{34} - f_Bb_{33}, \quad c_{120} = g_Ba^S_{34} + g_Aa_{44} - f_Bb^S_{34} - f_Ab_{44}, \\ c_{201} = g_0a_{33} + g_Aa^S_{23} - f_0b_{33} - f_Ab^S_{23}, \quad c_{021} = g_0a_{44} + g_Ba^S_{24} - f_0b_{44} - f_Bb^S_{24}, \\ c_{102} = g_0a^S_{23} + g_Aa_{22} - f_0b^S_{23} - f_Ab_{22}, \quad c_{012} = g_0a^S_{24} + g_Ba_{22} - f_0b^S_{24} - f_Bb_{22}, \\ \text{and} \quad c_{111} = g_0a^S_{34} + g_Ba^S_{23} + g_Aa^S_{24} - f_0b^S_{34} + f_Bb^S_{23} + f_Ab^S_{24},\end{gathered}$$

where

$$\begin{gathered}f_A = a^S_{13} + a^S_{23}x_0 + 2a_{33}y_0 + a^S_{34}z_0, \quad f_B = a^S_{14} + a^S_{24}x_0 + a^S_{34}y_0 + 2a_{44}z_0, \\ f_0 = a^S_{12} + 2a_{22}x_0 + 2a^S_{23}y_0 + a^S_{24}z_0,\end{gathered}$$

and similarly with g_A, g_B, and g_0. Denote by $(a_0 : b_0)$ a local mod p solution to this cubic equation. Now we parametrise the (A, B) solutions, here by $(a_0 + u, b_0 + uv)$.

We have that $h(a_0+u,b_0+uv)-h(a_0,b_0)$ is divisible by u, and thus for each v mod p we are led to solve the quadratic u-equation

$$\begin{aligned}
&\big[c_{003}v^3+c_{120}v^2+c_{210}v+c_{300}\big]u^2+\\
&\quad+\big[(c_{120}v^2+2c_{210}v+3c_{300})a_0+(c_{210}v^2+2c_{120}v+3c_{003})b_0+\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad (c_{021}v^2+c_{111}v+c_{201})\big]u+\\
&\quad+(c_{210}v+3c_{300})a_0^2+(2c_{120}v+2c_{210})a_0b_0+(3c_{003}v+c_{120})b_0^2+\\
&\qquad\quad+(c_{111}v+2c_{201})a_0+(2c_{021}v+c_{111})b_0+(c_{012}v+c_{102})=0.
\end{aligned}$$

The reduction to finding roots of a quadratic makes this step fast.

2.2. **Lifting the solutions and forming the matrix.** We now have all the local solutions to Q modulo some prime p. We work with these one at a time. Our first step in forming our matrix is to lift this solution $P_1=(1:x_1:y_1:z_1)$ to mod p^3. We let

$$A_2=a_{12}^S+2a_{22}x_1+a_{23}^Sy_1+a_{24}^Sz_1,\qquad A_3=a_{13}^S+a_{23}^Sx_1+2a_{33}y_1+a_{34}^Sz_1,$$

$$A_4=a_{14}^S+a_{24}^Sx_1+a_{34}^Sy_1+2a_{44}z_1,$$

and similarly with B_i. Then by our assumption that P_0 is non-singular, the matrix of derivatives whose rows are $(A_2:A_3:A_4)$ and $(B_2:B_3:B_4)$ has rank 2. We can assume that $A_3B_4-B_3A_4\not\equiv 0 \pmod p$, as else we can just permute variables to ensure this. Writing M for the matrix whose rows are $(A_3:A_4)$ and $(B_3:B_4)$, we then solve the $\vec{v}$-congruence $M(v_a:v_b)\equiv-\big(F_a(P_1):F_b(P_1)\big)/p$. This gives us a point $P_2=(1:x_2:y_2:z_2)=(1:x_1:y_1+v_ap:z_1+v_bp)$ that is a solution mod p^2 to the quadric intersection Q. We then solve $M(v_a:v_b)=\big(F_a(P_2):F_b(P_2)\big)/p$ to get a point $r_1=P_3=(1:x_3:y_3:z_3)=(1:x_2:y_2+v_ap:z_2+v_bp)$ that is a solution mod p^3 to the quadric intersection Q. This solution will eventually be the first row of our matrix.

Now we wish to find a vector $r_2=(0:p:pw_a:pw_b)$ such r_1+r_2 is a solution mod p^3 to the quadric intersection Q. One way of doing this is to take a different lift of P_1, and then subtract it from P_3 and scale to get the desired form. We can do this, for instance, by recomputing the A_i and B_i using P_3 instead of P_1. Then we want yet another vector $r_3=(0:0:p^2:lp^2)$ such that the span of these three vectors contains the set of solutions to Q mod p^3. This can again be achieved via finding a solution not already in the span, and then performing appropriate differencing and scaling. Although this is all just linear algebra, we now give an explicit recipe for achieving this.

To get r_2 we simply let $\tilde{P}_1=P_1+p(0:1:0:0)$ and solve the congruence $M(v_a:v_b)\equiv-\big(F_a(\tilde{P}_1):F_b(\tilde{P}_1)\big)$, and then lift the obtained solution to mod p^3 in the same manner. This gives us a second point, and we subtract P_1 from it to get r_2. To get r_3 we could take $\tilde{P}_1=P_1-p(0:1:0:0)$ as before, but since we have all lifts mod p^2 in the span of r_1 and r_2, we can instead reduce (r_1-r_2) mod p^2 and then lift it just once to give us a new solution mod p^3. In fact, we need only get the $(v_a:v_b)$ vector from the lifting, and then the third row is $r_3=(0:0:p^2:lp^2)$ where $l\equiv v_b/v_a$ (we simply switch columns when v_a is zero).

2.3. **Using the matrix.** We now have a matrix

$$M = \begin{pmatrix} 1 & x_3 & y_3 & z_3 \\ 0 & p & pw_a & pw_b \\ 0 & 0 & p^2 & lp^2 \\ 0 & 0 & 0 & p^3 \end{pmatrix}$$

such that any linear combination of its rows is a solution to $Q \bmod p^3$. Obviously the determinant of M is p^6. We now perform lattice reduction on the rows of M, giving us a new matrix N. Our final step is to loop over the rows of N, taking small linear combinations, and testing if the result is a global solution to Q. Given a height bound H, we expect the number of such tests to be an amount proportional to H^4/p^6. However, if we have a long skinny lattice, it might be superior to intersect it with a hyperplane rather than looping over small points.

To find points of height H it suffices to loop over $|u_i| \le B_i$ where B_i is the sum of the absolute values of the entries in the ith row of the inverse matrix of N. For each such (u_1, u_2, u_3, u_4) we test if $\sum_i u_i N_i$ is a global solution, where N_i is the ith row of N. We can essentially gain a factor of 2 by associating the u-vector with its negative. We assume for simplicity that $B_1 \ge B_2 \ge B_3 \ge B_4$. If both B_3 and B_4 are less than 1, we probably want to operate differently, as in this case B_1 and B_2 might both be quite large. If B_2 is also less than 1, we need only check $(1,0,0,0)$. Otherwise, we take $A_{11} = N_1^T Q_a N_1$ and similarly with A_{12} and A_{22} and with the B's, where Q_a and Q_b are the quadric intersections written as matrices; we then take $x = A_{12}B_{11} - B_{12}A_{11}$ and $y = B_{22}A_{11} - A_{22}B_{11}$ and test if $xN_1 + yN_2$ is a global solution (having tested N_1 and N_2 individually beforehand).

The searching takes H^4/p^6 time for each local solution, while lifting the local solution and doing LLL takes essentially constant time for each local solution. Since, by the Hasse-Weil bound, there are about p local solutions, we get a total time of $p + H^4/p^5$, which is minimised by taking p of size $H^{2/3}$.

3. Example

Let Q be given by the symmetric matrices

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & -2 & -6 \\ 0 & -2 & -1 & -1 \\ 0 & -6 & -4 & -4 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 & 1 & 2 \\ 1 & 1 & -3 & -4 \\ 1 & -3 & 5 & -4 \\ 2 & -4 & -4 & 4 \end{pmatrix}.$$

This quadric intersection corresponds to the elliptic curve E given by the minimal model $[0, -1, 1, -7772, -261137]$. A point on this curve is $(-203/4, 17/8)$. Via analytic computations, we are led to expect that the curve has rank 2 and the second generator has height around 225. So we expect to find a point with H around $\exp(225/8) \approx 1.6 \cdot 10^{12}$. Though our experience with such curves leads us to believe that we could use a smaller bound [we actually find a point whose coordinates are bounded by $1.25 \cdot 10^{11}$], for the sake of example we take $H = 2 \cdot 10^{12}$ and $p = 158740123$.

A local solution mod p to Q is given by $(1 : 1 : 44401206 : 112879317)$, from which we get the cubic

$$\begin{aligned} &126946254A^3 + 114334385A^2B + 96113346AB^2 + 29906951B^3 + 48241743A^2 + \\ &\quad + 11402293AB + 107562232B^2 + 102569588A + 140907608B + 45234610 = 0. \end{aligned}$$

and this has $(2, 51052649)$ as a solution.

Running over values of v, with $v = 106920807$ we find the solution $u = 104700759$ from which we get $A = 104700761$ and $B = 11304648$ and so $t = 103958427$, from which we have $P_1 = (1 : 103958428 : 56894077 : 84932273)$ as a local solution mod p. We then get $M = \begin{pmatrix} 94214203 & 22874125 \\ 59432635 & 275598640 \end{pmatrix}$ from which $(v_a, v_b) = (59308178, 141708512)$, and then $(v_a, v_b) = (34330977, 51121936)$ for the second lift, giving us

$$r_1 = (1 : 103958428 : 865086589975390559895875 : 1288192351801212761113864)$$

as a solution of Q mod p^3. We then work with $P_1 + p(0 : 1 : 0 : 0)$, and get $(v_a, v_b) = (31387949, 23742203)$ then $(v_a, v_b) = (11909346, 116976846)$ so that

$$s_2 = (1 : 262698551 : 300096761415227742152309 : 2947632452256208375931247)$$

is another solution mod p^3, so that we have

$$r_2 = (0 : 158740123 : 3435011517276066316497301 : 1659440100454995614817383)$$

We then lift the mod-p^2-reduction of $r_1 - r_2$ to mod p^3, where here we get that $(v_a, v_b) = (33514091, 120434226)$, so that the third row of the matrix is given by $r_3 = (0 : 0 : p^2 : 58123626p^2)$. So the matrix is

$$\begin{pmatrix} 1 & 103958428 & 865086589975390559895875 & 1288192351801212761113864 \\ 0 & 158740123 & 3435011517276066316497301 & 1659440100454995614817383 \\ 0 & 0 & 25198426650055129 & 1464623926396237197377754 \\ 0 & 0 & 0 & 4000001345836229134240867 \end{pmatrix}$$

and the LLL-reduction on its rows is

$$\begin{pmatrix} 56881359698 & -124389272966 & -42276224810 & 14138702493 \\ 1022189646293 & 828711803877 & -1170524846811 & 345826325149 \\ -2224045783902 & -187105486324 & -626773352561 & 4819171954601 \\ -7406789624477 & -1342133389496 & -7568052767254 & -4601377145302 \end{pmatrix}.$$

From the LLL-reduction of this matrix, we find the point

$$(56881359698 : -124389272966 : -42276224810 : 14138702493)$$

on Q, and this maps back to the point on our model of E whose x-coordinate is

29766285663295131895027138976061006262940198775445003671410529300211707811066720167161909112316153/
180691271602398954814106043213357677335232321513682898324688282299457871778826785268845537187856.

This computation only took about a day. Indeed, using this method a fast computer will take about a week to find points of height around 250.