Parametrizované rozdutie supereliptických kriviek

RNDr. Martina Bátorová

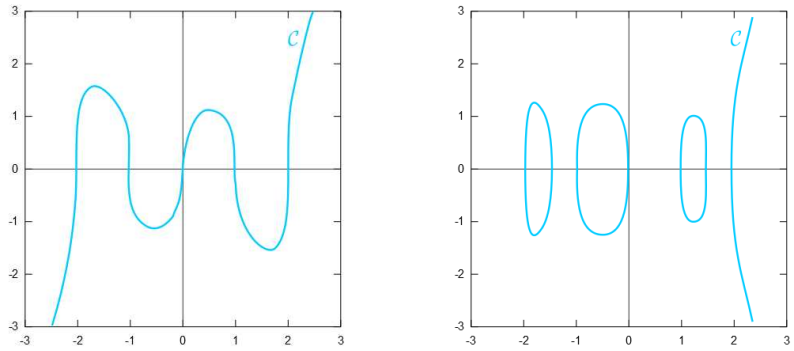
Katedra algebry, geometrie a didaktiky matematiky,
Fakulta matematiky, fyziky a informatiky,
Univerzita Komenského v Bratislave

Deformácie algebraických variet sú jednou zo základných metód algebraickej geometrie. V prípade algebraických kriviek vhodne zvolená deformácia poskytuje mnoho užitočných informácií napr. o vnútornej štruktúre singularít danej krivky.

V našom príspevku sa zameriavame na *supereliptické krivky* definované nad poľom komplexných čísel rovnicou

$$f(x,y): y^k = a_n x^n + \ldots + a_0 = a(x-x_1)\ldots(x-x_n)$$

spĺňajúcou ďalšie podmienky, a ich podtriedu *hypereliptických kriviek (k=2)*. Obe triedy kriviek sa tešia veľkej pozornosti najmä v šifrovaní a elektronickej bezpečnosti (pri uvažovaní poľa konečnej charakteristiky).



Obr.1: Supereliptická krivka pre *(k,n)=(3,5)* (vľavo) a *(k,n)=(4,7)* (vpravo).

Pri vhodne zvolenej súradnicovej sústave môžeme singularitu v nekonečne odstrániť konečným počtom aplikácií metódy lokálneho rozdutia – pôvodne singulárnu krivku nahradíme jej regulárnym biracionálnym ekvivalentom, čo je krivka bez viacnásobných bodov.

Nás zaujíma dopad parametrizácie koreňov na proces desingularizácie rozdúvaním. Konkrétne uvažujeme *r*-parametrickú ($1 \leq r \leq n$) deformáciu krivky zadanú predpisom

$$F(x,y,t_1,\ldots,t_r): y^k = (x-(x_1+t_1))\ldots(x-(x_r+t_r))g(x)$$

s reálnymi resp. komplexnými hodnotami parametrov t_i, $i=1,\ldots,r$. Takto deformovanú krivku normalizujeme a pozorujeme závislosť vnútornej štruktúry singularity na rôznych konfiguráciách koreňov, napr. zmeny v počte potrebných rozdutí na dosiahnutie rozkladu. Vyslovíme dokázané tvrdenie o stálosti vnútornej štruktúry supereliptických kriviek a procesu ich desingularizácie od konfigurácie koreňov pri takto zvolených deformáciách.

Celú konštrukciu ilustrujeme názornými príkladmi a obrázkami. Na záver načrtávame postup ďalšej práce v oblasti topológie singularít supereliptických kriviek s vyššími hodnotami *k,n*.