Journées Codage et Cryptographie, 2012 à Dinard
Soumission de:

Hamish IVEY-LAW
Institut de Mathématiques de Luminy
hlaw@iml.univ-mrs.fr

Titre:
Bases explicites d'espaces de sections globales des diviseurs sur un produit symétrique d'une courbe hyperelliptique

Nous considerons un genre de « problème de Riemann-Roch » pour certaines surfaces algébriques, soit les produits ou produits symétriques d'une courbe hyperelliptique de genre arbitraire sur un corps (presque) quelconque. Nous présentons une solution théorique à la question de la structure et la dimension de l'espace de sections globales d'une classe de diviseur quelconque et aussi un algorithme pratique pour produire une base d'un tel espace de sections. On applique ses résultats pour dériver des plongements explicites des produits symétriques d'une courbe hyperelliptique et, en particulier, nous redériverons le plongement bien connu de la jacobienne d'une courbe de genre deux dans $\mathbb{P}^{15}$ donné pour la première fois par Cassels [1] and Flynn [3] (voir aussi Flynn [4] et Cassels and Flynn [2]). Nous expliquerons comment cela nous permet d'évaluer l'application $C \times C \to J$ (lorsque $g = 2$) sur les pointes p-adiques sans perte de précision, qui a quelques applications aux algorithmes p-adique de comptage de points sur une jacobienne. Qui plus est, ces nouvelles méthodes explicites ouvre la possibilité d'étudier le codage sur les surfaces provenant des produits ou produits symétriques d'une courbe hyperelliptique.

Plus de détails: Soit C une courbe hyperelliptique de genre g et soit $\mathrm{Sym}^2(C)$ le produit symétrique de C. Soient V et H les diviseurs vertical et horizontal sur $C \times C$ et soit ∇ le diviseur anti-diagonal sur $C \times C$. Soit $\gamma = g - 1$ et soient $m > \gamma$ et $r \geqslant 0$. Dans la partie théorique de cet exposé nous prouverons (modulo certains conditions légères) qu'il y a une décomposition

$$H^0(C \times C, m(V+H) + r\nabla) \cong H^0(C^2, m(V+H)) \oplus \bigoplus_{i=1}^{r} H^0(C, (m - \gamma i)D_\infty)$$

où $D_\infty = 2(\infty)$ ou $D_\infty = (\infty^+) + (\infty^-)$ (selon que la courbe a un modèle pair ou impair). On obtient comme corollaires la formule

$$\dim H^0(C \times C, m(V+H) + r\nabla) = (m-\gamma)^2 + 4mr - \gamma r(r+2).$$

ainsi qu'une décomposition similaire pour $H^0(\mathrm{Sym}^2(C), m\Theta_S + r\nabla_S)$ (où Θ_S et ∇_S sont les images de $V+H$ et ∇ sous l'application quotient $C \times C \to \mathrm{Sym}^2(C)$) et la formule

$$\dim H^0(\mathrm{Sym}^2(C), m\Theta_S + r\nabla_S) = \binom{m-\gamma+1}{2} + r(m+1) - \gamma\binom{r+1}{2}.$$

Dans la partie explicite de cet exposé nous décrirons une décomposition de $H^0(C \times C, m(V + H))$ par rapport à sa structure en tant que D_4-module et cette information sera utilisée pour développer un algorithme qui produit une base explicite de $H^0(\mathrm{Sym}^2(C), m\Theta_S + r\nabla)$. Pour terminer, on redérivera la base de Cassels [1] et Flynn [3] ainsi de montrer comment adapter la méthode pour permettre l'évaluation de l'application $C \times C \to J$ (lorsque $g = 2$) sur les pointes p-adiques sans perte de précision.

References

[1] J. W. S. Cassels. Arithmetic of curves of genus 2. In *Number theory and applications (Banff, AB, 1988)*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 27–35. Kluwer Acad. Publ., Dordrecht, 1989.

[2] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[3] E. V. Flynn. The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field. *Math. Proc. Cambridge Philos. Soc.*, 107(3):425–441, 1990.

[4] E. V. Flynn. The group law on the Jacobian of a curve of genus 2. *J. Reine Angew. Math.*, 439:45–69, 1993.