Contemporary algebraic and geometric techniques
in coding theory and cryptography
Summer school — July 18-22, 2022
Università degli Studi della Campania "Luigi Vanvitelli"

Computing Riemann–Roch spaces for algebraic geometry codes

Elena Berardini

Affiliation: Eindhoven University of Technology
The Netherlands

Abstract

Reed–Solomon codes are a well–known technique to represent data in the form of vectors, such that the data can be recovered even if some vector coordinates are corrupted. These codes have many properties. Their parameters are optimal. They allow reconstructability of coordinates that have been erased. They ensure the privacy of the data against an adversary learning many coordinates. They are compatible with the addition and multiplication of data. Nevertheless, they suffer from some limitations. For instance, the storage size of vector coordinates grows logarithmically with the number of coordinates: in order to have *long* Reed–Solomon codes, one must work on *large* finite fields. So–called algebraic geometry (AG) codes are a generalization of Reed–Solomon codes that enjoy the same properties, while being free of these limitations. Therefore, the use of AG codes provides complexity gains and turns out to be useful in several applications such as distributed storage [4], distributed computation on secrets [7], and zero–knowledge proofs [5].

Algebraic geometry codes are constructed by evaluating vector spaces of functions, called Riemann–Roch spaces, at the rational points on a curve. It follows that the computation of these spaces is crucial for the implementation of AG codes. However, computing large Riemann–Roch spaces for projective curves still constitutes a major algorithmic and practical challenge. Recently, an algorithm for the computation of Riemann–Roch spaces of plane curves with so–called *ordinary* singularities has been proposed [2]. Until now, no complexity exponent for curves with so–called *non–ordinary* singularities was known. Nevertheless, a generic singular curve admits non–ordinary singularities. Moreover, the models of curves used to build AG codes with good parameters, *e.g.* modular curves, have non–ordinary singularities [10]. The goal of this paper is to present a new efficient algorithm to

compute Riemann–Roch spaces of *every* plane curves, including the non–ordinary ones. This is a joint work with S. Abelard, A. Couvreur and G. Lecerf, published at Journal of Complexity [1].

Our work is in the vein of the fundamental theory conceived by Brill and Noether [6], often called the *geometric* method. Let $\mathscr{C}$ be a projective plane curve defined over a perfect field $\mathbb{K}$. A divisor on $\mathscr{C}$ is a formal sum of points on the curve. It is said to be *smooth* if all points in its decomposition are smooth points of the curve and *non–smooth* otherwise. The aim is to compute a basis of the Riemann–Roch space associated with a smooth divisor D, denoted $L(D)$. The input $\mathbb{K}$–rational divisor D is decomposed into $D = D_+ - D_-$, where D_+ and D_- are *effective* divisors with disjoint supports. To the curve $\mathscr{C}$ is associated a so–called adjoint divisor, denoted $\mathscr{A}$, related to the singularities of $\mathscr{C}$. The Brill–Noether method is mainly divided into two parts, as follows. First, one computes a homogeneous polynomial H that can serve as the common denominator of a basis of $L(D)$. Brill and Noether gave sufficient conditions on such a polynomial in terms of $\mathscr{A}$ and D, that is

$$Div(H) \geq \mathscr{A} + D_+.$$

For reasons of efficiency, it is of practical interest that H is of degree d as small as possible. Then, one computes the polynomials $G_1, ..., G_\ell$ of degree d such that G_i/H for $i = 1, ..., \ell$ form a basis of $L(D)$. These polynomials are obtained as a basis of homogeneous polynomials of degree d which satisfy

$$Div(G) \geq Div(H) - D.$$

Let us mention that to deal with the computation of Riemann–Roch spaces of curves, one can also use another family of algorithms, called *arithmetic*. The most advanced algorithm of this family is due to Hess [8] and is implemented in the computer algebra systems MAGMA and SINGULAR. However, the complexity exponent of this algorithm has not been analysed so far, and recent work based on Brill and Noether's theory seems to confirm that the geometric method is the most efficient in terms of complexity.

An ordinary curve admits a local factorization around each singular point which allows to write its adjunction divisor $\mathscr{A}$ very simply. This local factorisation does not hold as soon as we consider a non–ordinary singularity, hence the need to find new tools to write the adjunction divisor.

First, we propose the rewriting of the adjunction divisor $\mathscr{A}$ in terms of the Puiseux series. We can then exploit the fast algorithms recently developed for the computation of Puiseux expansions at the germs of curves [11].

Then, we give an optimal upper bound for the degree d of the homogeneous polynomial H which serves as the common denominator of a basis of the Riemann–Roch space, namely (see [1, Proposition 12])

$$d \geq \frac{(\delta-1)(\delta-2)+\deg D_+}{2},$$

where δ denotes the degree of the curve. The computation of the denominator H and the numerators G_i can therefore be approached using classical linear algebra methods, by solving linear systems whose number of equations depends on D and $\mathscr{A}$. However, by reformulating this problem in terms of structured linear algebra, we benefit from generally faster algorithms [9]. *In sum*, we obtain the following main result.

Theorem ([1, Theorem 3])**.** *Let $\mathbb{K}$ be a perfect field. Let $F \in \mathbb{K}[x,y,z]$ be a homogeneous and absolutely irreducible polynomial of degree δ, that defines a curve $\mathscr{C}$. Let D be a smooth $\mathbb{K}$–rational divisor of $\mathscr{C}$. Suppose that the characteristic of $\mathbb{K}$ is zero or bigger than δ. Then, a basis of $L(D)$ can be computed with a probabilistic algorithm of Las Vegas type with an expected number of*

$$\tilde{O}((\delta^2+\deg D_+)^{\omega})$$

operations in $\mathbb{K}$, where $2 \leq \omega \leq 3$ is a feasible exponent for linear algebra.

The curves used in the construction of AG codes were for the most part limited to those for which the Riemann–Roch bases were already known. This new work and the ones that will follow will allow the construction of AG codes from more general curves.

Let us conclude with two open questions for future works. First, the use of Puiseux series developments, a fundamental tool for writing the adjunction condition in our work, is less well adapted to finite fields, and limits the computation of Riemann–Roch spaces presented here to curves defined over fields of characteristic zero or bigger than the degree of the curve. It is therefore necessary to find new tools to replace Puiseux series, free from this limitation. Identifying the tool which is best suited to the context and adapting to it what has already been developed for non–ordinary curves in the present paper constitutes the major problem to be faced.

The second question concerns the computation of Riemann–Roch spaces of surfaces. The geometric construction of codes from curves is valid on higher dimensional varieties, and some work has been undertaken on surfaces [3]. One of the motivations for studying codes from surfaces is based on the number of rational points of the latter: while a curve defined over a

finite field $\mathbb{F}_q$ has $O(q)$ rational points, a surface has $O(q^2)$ rational points. Therefore, the use of surfaces yields codes that are generally longer than codes from curves, and consequently allows to work on smaller finite fields, where the arithmetic is faster. In contrast with the situation of curves, algorithms for computing Riemann–Roch spaces of surfaces have been very little studied and, to our knowledge, no complexity exponent is known in this context. Proposing a geometric method and conceiving an algorithm for the efficient computation of Riemann–Roch spaces of surfaces will pave the way to the construction of completely new families of AG codes from surfaces.

Keywords: Algebraic curves, Riemann–Roch spaces, Algebraic Geometry codes, Algorithms

References

[1] S. Abelard, E. Berardini, A. Couvreur and G. Lecerf, *Computing Riemann-Roch spaces via Puiseux expansions*, J. Complexity, 10166, 2022.

[2] S. Abelard, A. Couvreur and G. Lecerf, *Efficient computation of Riemann-Roch spaces for plane curves with ordinary singularities*, preprint 2021.

[3] Y. Aubry, E. Berardini, F. Herbaut and M. Perret, *Bounds on the minimum distance of algebraic geometry codes defined over some families of surfaces*, Contemp. Math. 770, 2021.

[4] A. Barg, K. Haymaker, E. W. Howe, G. L. Matthews and A. Várilly–Alvarado, *Locally recoverable codes from algebraic curves and surfaces*, Algebraic geometry for coding theory and cryptography, Assoc. Women Math. Ser., 9, 95–127, Springer, Cham, 2017.

[5] S. Bordage, M. Lhotel, J. Nardi and H. Randriam, *Interactive Oracle Proofs of Proximity to Algebraic Geometry Codes*, preprint, 2022.

[6] A. Brill and M. Noether, *Ueber die algebraischen Functionen und ihre Anwendung in der Geometrie*, Math. Ann. 7.2, p. 269-310, 1874.

[7] R. Cramer, M. Rambaud and C. Xing, *Asymptotically-Good Arithmetic Secret Sharing over $Z/p^{\ell}Z$ with Strong Multiplication and Its Applications to Efficient MPC*, Springer-Verlag, 2021.

[8] F. Hess, *Computing Riemann–Roch spaces in algebraic function fields and related topics*, J. Symb. Comput. 33 (4), 425–445, 2022.

[9] C.-P. Jeannerod, V. Neiger, É. Schost and G. Villard, *Computing minimal interpolation bases*, J. Symb. Comput. 83, 46 272–314, 2017.

[10] A. Klyachko and O. Kara, *Singularities of the modular curve*, Finite Fields Appl. 7 (3), 415–420, 2001.

[11] A. Poteaux and M. Weimann, *Computing Puiseux series: a fast divide and conquer algorithm*, Ann. Henri Lebesgue 5, 20 1061–1102, 2021.