

# FACTORING POLYNOMIALS OVER FUNCTION FIELDS

OSÉ FELIPE VOLOCH

ABSTRACT. If  $K/k$  is a function field in one variable of positive characteristic, we describe a general algorithm to factor one-variable polynomials with coefficients in  $K$ . The algorithm is flexible enough to find factors subject to additional restrictions, e.g., to find all roots that belong to a given finite dimensional  $k$ -subspace of  $K$  more efficiently. It also provides a deterministic polynomial time irreducibility test in small characteristic. We also discuss some applications.

## 1. INTRODUCTION

Let  $K/k$  be a function field in one variable, that is, a finitely generated extension of transcendence degree one with  $k$  algebraically closed in  $K$ . Let  $G(T)$  be a polynomial in one variable over  $K$ . The algorithmic problem of finding the irreducible factors of  $G(T)$  in  $K[T]$  and, in particular its roots in  $K$ , is a much-studied problem with many applications, see e.g. [vzGK85, Poh05, BvHKS09] and the references therein. A noteworthy special case is the case where  $K = k(x)$ , the rational function field, and the coefficients of  $G(T)$  are in  $k[x]$ . This case corresponds to factoring polynomials in two variables with coefficients in  $k$ .

Many of the applications of the above problem actually require the solution of a more restricted problem. For instance, given  $G(T)$  and a finite dimensional  $k$ -subspace  $V$  of  $K$ , find the roots of  $G(T)$  in  $V$ . An example of an application where this restricted problem suffices is the Guruswami-Sudan list-decoding algorithm. See [GS00] for a comprehensive discussion.

Throughout this paper  $k$  has characteristic  $p > 0$  and we make the assumption that the polynomial  $G(T)$  to be factored is squarefree. The reduction to this case is a standard first step in all algorithms and is presented in the above cited papers. We also assume  $G(0) \neq 0$ .

The purpose of this paper is to describe an algorithm that solves the general problem of factoring a squarefree  $G(T)$  and also has the additional feature of improved performance when applied a more restricted problem, such as above. Indeed, we will describe an algorithm that finds a factor of  $G(T)$  of prescribed degree whose coefficients are on prescribed finite dimensional  $k$ -subspaces of  $K$ . We prove that, up to a final step, the algorithm runs in deterministic polynomial time for small characteristics and, in particular, provides a deterministic polynomial time absolute irreducibility test in this setting. See Theorem 2.2 and Remark 2.3 below for a precise statement and discussion. We do not try to obtain specific running times as, in practice, these will not be better than the heuristic running times of existing algorithms. We also discuss some other applications of the ideas in this paper in Section 4. The approach is novel and relies on a linear independence criterion over  $k$  using Wronskian matrices.

---

2010 *Mathematics Subject Classification*. Primary: 12Y05 ; Secondary: 11R09.

*Key words and phrases*. Polynomial factorization, function fields, irreducibility test.

Our algorithm, like most standard algorithms, needs at the beginning, a place of the function field  $K$  with a few additional properties. In our presentation of the main part of the algorithm, in Section 2, we just assume its existence. In the subsequent Section 3 we discuss how to find such a place. While, in some cases (e.g.  $k$  finite,  $K = k(x)$ ) this is easy, it can be difficult in the generality we work with and some of the literature seems to gloss over this point.

Most of the standard algorithms then proceed to compute a complete factorization of the image of the polynomial when specialized to residue field of the place just discussed (see the description of a generic factorization algorithm in [Poh05]). The factorization step in the residue field is often easy in practice but can be difficult in certain circumstances. These algorithms also often have a bottleneck reconstructing global factorizations from local ones. In contrast, our algorithm does not need to compute this factorization at the beginning, nor tries to reconstruct global factorizations from local ones. Instead, it may do a partial factorization during intermediate steps using easy gcd computations. At the end, our algorithm may need to further factor some of these partial factors. If the objective is an irreducibility criterion, it does not require finding such a factorization at all.

We also mention the algorithm of [Rup99, Gao03] that uses a certain first order partial differential equation and shares some of the advantages of our approach. It only applies however when  $K$  is a rational function field. One application of this approach [Rup99] is to bound the size of the largest prime  $p$  for which an irreducible polynomial in  $\mathbb{Z}[x, y]$  factors modulo  $p$ . Our approach allows us to obtain similar bounds in full generality when  $k$  itself is a global field.

## 2. THE MAIN ALGORITHM

We begin with presenting some concepts and results from [Sch39, SV86]. See also [GV87] which proves stronger versions of the main results of [Sch39] and may be more accessible and also [Hes02] which presents relevant algorithms. Let  $K/k$  be a function field. The usual higher derivatives do not work well in small characteristics. A suitable replacement for higher derivatives that work in general are the Hasse derivatives. We denote by  $D^{(i)}, i = 0, 1, \dots$ , the Hasse derivatives with respect to some separating variable on  $K$ . These are  $k$ -linear operators on  $K$  satisfying:

$$D^{(i)} \circ D^{(j)} = \binom{i+j}{j} D^{(i+j)},$$

$$D^{(i)}(uv) = \sum_{j=0}^i D^{(j)}(u) D^{(i-j)}(v).$$

By [Sch39, Satz 2],  $f_0, \dots, f_m \in K$  are linearly independent over  $k$  if and only if the Wronskian matrix  $(D^{(i)}(f_j))$  has maximal rank  $m + 1$ . In this case, there is a minimal list of integers  $0 = \varepsilon_0 < \dots < \varepsilon_m$  such that the matrix  $(D^{(\varepsilon_i)}(f_j))$  has maximal rank  $m + 1$ . Also, to a place  $v$  of  $K$ , we can associate a minimal list of integers  $0 = j_0 < \dots < j_m$  such that the matrix  $(D^{(j_i)}(f_j))$  evaluated at  $v$  has maximal rank  $m + 1$ . If  $K$  is the function field of an algebraic curve  $Y$ , then the morphism  $(f_0 : \dots : f_m) : Y \rightarrow \mathbb{P}^m$  has some degree  $\Delta$ , then we can take  $\varepsilon_i \leq j_i \leq \Delta$  when the  $f_i$  are linearly independent ([SV86, Section 2]). On the other hand, if the Wronskian matrix has rank  $m$  and  $a_0, \dots, a_m \in K$  satisfy

$\sum_{j=0}^m a_j D^{(i)}(f_j) = 0, i = 0, 1, 2, \dots$  and  $a_0 = 1$ , then  $a_j \in k, j = 0, 1, \dots, m$  as follows from the proof of [Sch39, Satz 1].

Consider a monic, squarefree polynomial

$$G(T) = \sum_{j=0}^s a_j T^j, a_j \in K, a_s = 1 \quad (2.1)$$

Let  $R = K[T]/G(T)$  and  $t$  the image of  $T$  in  $R$ . We extend the operators  $D^{(i)}, i \geq 0$  to  $R$ . We need an expression for  $D^{(i)}(t)$ . We have that

$$0 = D^{(i)}(G(t)) = \sum_{j_1+2j_2+\dots+ij_i \leq i} A_{j_1, \dots, j_i} (D^{(1)}(t))^{j_1} \dots (D^{(i)}(t))^{j_i} \quad (2.2)$$

where the  $A_{j_1, \dots, j_i}$  are polynomials in  $t$  and, in particular,  $A_{0, \dots, 0, 1} = G'(t)$  which is invertible in  $R$  and this determines  $D^{(i)}(t)$  uniquely, by induction. They can be computed more efficiently by the algorithms of [Hes02]. If  $v$  is a place of  $K$  with ring of integers  $\mathcal{O}$  and maximal ideal  $\mathfrak{m}$  such that  $G \pmod{v}$  is well-defined (i.e.  $G$  has coefficients in  $\mathcal{O}$ ) and separable, then the operators  $D^{(i)}, i < q$  defined using an uniformizer for  $\mathfrak{m}$ , induce operators in  $R_1 = (\mathcal{O}/\mathfrak{m}^q)[T]/(G(T))$  by the same formulas, for any  $q$  power of  $p$ .

The ring  $R_1 = (\mathcal{O}/\mathfrak{m}^q)[T]/(G(T))$  is an Artinian ring and, thus, a direct sum of Artinian local rings. These summands correspond to irreducible factors of  $G(T)$  which, in turn, correspond to irreducible factors of  $G(T) \in (\mathcal{O}/\mathfrak{m})[T]$ , which is assumed separable. The standard factorization version of Hensel's lemma gives an algorithmic way to go from the latter to the former. In the process of algorithm 1 below, we will decompose  $R_1$  as a direct sum but we may not go all the way to the full decomposition as a sum of Artinian local rings. Since we are in an equicharacteristic setting, for any Artinian local summand  $S$  of  $R_1$ , the residue field of  $S$  is isomorphic to a unique subring of  $S$  (in the present setting, the image of  $x \mapsto x^q$ ) and we refer to the elements of this subring as constants.

The input of our general algorithm is the following:

- The function field  $K/k$
- The polynomial  $G(T) \in K[T]$  monic, squarefree, of degree  $s$  with discriminant  $f \neq 0$ .
- A place  $v$  of  $K/k$ , with with ring of integers  $\mathcal{O}$  and maximal ideal  $\mathfrak{m}$  with  $G(T) \in \mathcal{O}[T]$  and  $v(f) = 0$  and an uniformizer of  $v$  used to define the  $D^{(i)}$ .
- Finite dimensional  $k$ -vector spaces  $V_i \subset K, i = 0, \dots, r-1$ , with  $1 \in V_0$ , together with a  $k$ -basis  $\{h_{ij}\}$  for each  $V_i$ , where  $r < s$ . Put  $h_{r1} = 1$ .

The output is either a monic factor of  $G(T)$  of the form  $H(T) = \sum_{i=0}^r b_i T^i, b_i \in V_i, i < r, b_r = 1$  or a proof that such a factor does not exist.

To obtain a full factorization algorithm, the following lemma (a variant of [Poh05, Lemma 4.1]) provides bounds for the valuations of the coefficients of the potential factors of  $G(T)$  and these bounds can be used to define suitable  $V_i$  as Riemann-Roch spaces.

**Lemma 2.1.** *Let  $t$  be a root of  $G(T) = \sum_{i=0}^s a_i T^i$  in some finite extension  $L/K$  and  $H(T) = \sum_{i=0}^r b_i T^i$  its monic minimal polynomial over  $K$ . Then, for any place  $v$  of  $L$*

$$v(t) \geq \min_{0,1,\dots,s-1} v(a_i)/(s-i)$$

and, for any place  $v$  of  $K$ ,

$$v(b_i) \geq (r-i) \min_{0,1,\dots,s-1} v(a_i)/(s-i).$$

---

**Algorithm 1** Find factor of  $G(T)$  with restricted coefficients

---

- 1:  $R = K[T]/(G(T))$ .
  - 2:  $\Phi \in R^{m+1}$  the row vector with entries  $h_{ij}t^i \in R$  in some order.
  - 3: Find bound  $\Delta$  for  $j_i, \varepsilon_i$  for maps to  $\mathbb{F}^m$  given by specializations of  $\Phi$ .
  - 4: Compute  $q$ , smallest power of  $p$  with  $q > \Delta$  (so  $q \leq p\Delta$ ).
  - 5: Find place  $v$  of  $K$  with  $G \pmod{v}$  well-defined and separable.
  - 6:  $R_1 = (\mathcal{O}/\mathfrak{m}^q)[T]/(G(T))$ ,  $R_0 = (\mathcal{O}/\mathfrak{m})[T]/(G(T))$ .
  - 7: Compute matrix  $M$  with rows  $D^{(i)}(\Phi)$ ,  $i = 0, \dots, q-1$ , working in  $R_1$ .
  - 8: Attempt to do Gaussian elimination on  $M$ , working in  $R_0$ .
  - 9: **if** Some pivot  $P(T) \in R_0$  is not invertible **then**
  - 10:     Compute  $H_0(T) = \gcd(G(T), P(T))$  and  $E_0(T) = G(T)/H_0(T)$  in  $R_0$ .
  - 11:     Lift factorization  $G(T) = H_0(T)E_0(T)$  in  $R_0$  to factorization  $G(T) = H(T)E(T)$  in  $R_1$  and replace  $G(T)$  by  $H(T)$  and  $E(T)$  in step 6.
  - 12: **end if**
  - 13: **if**  $M$  has full rank  $m+1$  **then**
  - 14:     **return**  $G(T)$  has no factor of required form.
  - 15: **else if**  $M$  has rank  $m$  **then**
  - 16:     **return** Solution  $u_{ij}$  of  $\sum_{ij} u_{ij}D^{(\ell)}(h_{ij}t^i) = 0$ ,  $u_{r1} = 1$ ,  $\ell = 0, 1, \dots, q-1$ .
  - 17: **else**
  - 18:     Go back to 2 and remove an entry from  $\Phi$ .
  - 19: **end if**
- 

*Proof.* Recall that we assume throughout that  $G(0) \neq 0$ , so  $t \neq 0$ . If  $iv(t) + v(a_i) > sv(t)$  for all  $i < s$ , then  $\infty = v(G(t)) = \min\{iv(t) + v(a_i)\} = sv(t)$ , contradiction. This gives the first part of the lemma.

We have that  $b_i$  is the  $(r-i)$ -th symmetric function on the conjugates of  $t$  so the second part follows from the first by extending  $v$  to a valuation of the splitting field of  $H$ .  $\square$

It follows that, without any further restriction on the valuations of the elements of  $V_i$ , that we can take

$$\Delta = -r \sum_v \min\{0, \min_{0,1,\dots,s-1} v(a_i)/(s-i)\} \quad (2.3)$$

as a bound for the  $j_i, \varepsilon_i$ . Such a bound can be improved if additional restrictions are put in the  $V_i$ .

**Theorem 2.2.** *Given the above input, algorithm 1 runs in deterministic polynomial time in  $p, s, \Delta$  (measured in number of operations in the field  $\mathcal{O}/\mathfrak{m}$ ) and outputs either a certificate that  $G(T)$  has no factor of the required form or a decomposition of  $R_1$  as a direct sum of at most  $s$  rings  $R'$ . Moreover, for each summand  $R'$ , the algorithm outputs elements  $u_{ij}$  of  $R'$  that are constant in each summand of the decomposition of  $R'$  into local rings and from which a factor of  $G(T)$  of the required form can be constructed or a certificate that this summand does not yield such a factor. In particular, the algorithm provides a deterministic polynomial time absolute irreducibility test in characteristic  $p$  for  $p$  polynomially bounded in  $s, \Delta$ .*

*Proof.* By induction on  $m$ . Assume  $m = 1$ . Since  $1 \in V_0$ ,  $\Phi = (1, t^r)$  and  $M$  has rank 1 or 2. If the rank is 2 in  $R'$ , it is clear there is no factor of the required form. If the rank is 1 in  $R'$ , this means that  $D^{(i)}(t^r) = 0$ ,  $i = 1, \dots, q-1$ , so  $t^r$  is constant in any local summand

of  $R'$ , the solution of the linear system is  $u_{01} = -t, u_{r1} = 1$  and  $H(T) = T - t$  is a factor of  $G(T)$  of the required form.

As mentioned above, step 3 is dealt with in general by equation 2.3 unless there is a better bound available.

For step 5, we compute the discriminant of  $G(T)$  and find a place for which it is a unit. Some power of  $\Delta$  provides a bound for the number of bad places.

As mentioned above, the operators  $D^{(i)}, i < q$  act on  $R_1$  and the computation of the matrix  $M$  in step 7 is polynomial in operations in  $R_1$  but  $\dim_{\mathcal{O}/\mathfrak{m}} R_1 \leq sq$  giving a bound in terms of the number of operations in  $\mathcal{O}/\mathfrak{m}$ .

In the process of Gaussian elimination (whose running time is polynomial in the size of the matrix), for each candidate pivot in the ring  $R_0$ , the factorization from steps 10 and 11 we can write  $R_1$  as a direct sum of two rings for which the pivot is invertible in one factor and zero in the other. In the first factor, we use the pivot as in the usual Gaussian elimination and, in the second factor, we look for a new pivot. The work done before splitting  $R_1$  is reused. At the end of steps 1-12, we arrive at a decomposition of  $R$  as a sum of at most  $s$  rings and the image of  $M$  in each of these is put in row echelon form by the Gaussian elimination process.

Those summands of  $R_1$  where  $M$  has full rank  $m+1$  yield no factor of  $G(T)$  of the required form. For other factors  $R'$  where  $M$  has rank  $m$ , we compute the  $u_{ij}$  as described in step 16. It follows from the proof of [GV87, Theorem 1] that the  $u_{ij}$  are constant in each local factor of the decomposition of  $R'$ . Since  $\sum u_{ij}h_{ij}t^i = 0$ , it follows, since  $u_{ij}$  are constants and  $G(t) = 0$ , that the image of  $\sum u_{ij}h_{ij}T^i$  in each such local factor yields a factor of  $G(T)$  of the required form. For the factors  $R'$  where  $M$  has rank smaller than  $m$ , we decrement  $m$ , rerun the algorithm and are done by induction.  $\square$

**Remark 2.3.** *What Theorem 2.2 does not do is identify the  $u_{ij}$  with specific elements of  $k$ , necessarily. For that, we need to further factor the factor of  $G(T)$  corresponding to the ring  $R'$  as a product of irreducibles to obtain the full decomposition of  $R'$  as a sum of local rings and identify the  $u_{ij}$  with constants in each summand.*

*As mentioned in the introduction, the first step in most standard factoring algorithms for  $K[T]$  is to fully factor  $G(T) \in (\mathcal{O}/\mathfrak{m})[T]$  and how it is performed depends on the nature of the field  $k$ . One advantage of our method is that this step may not be required at all (if  $G(T)$  has no factors, or a single irreducible factor, of the required form) or it may only be needed for a proper factor of  $G(T)$ .*

We will discuss an example but, beforehand, here is a non-example. If  $G(T) \in k[T]$ , that is, has constant coefficients, then  $D^{(i)}(t) = 0, i > 0$ , the matrix  $M$  has always rank one and the algorithm unravels to the base case  $m = 1$ . The polynomial  $T - t$  is a factor of  $G(T)$  for  $G(t) = 0$  and we are left with the task of factoring  $G(T)$  over the constant field  $k$ .

For a more representative example consider

$$G(T) = T^4 + (x+1)T^3 + (x^2+1)T^2 + (x^3+x^2+1)T + (x^2+x) \in \mathbb{F}_2(x)[T].$$

We look for factors of  $G(T)$  of the form  $T+ax+b$ , so  $r = 1$ ,  $V_0$  is spanned by  $1, x$ ,  $\Phi = (1, x, T)$  and  $m = 2$ . Modulo the ideal  $(x+1)$ ,  $G(T)$  reduces to  $T^4 + T$ . We find that

$$D^{(2)}(T) = (xT^5 + (x^2+x)T^4 + x^5T + (x^6+x^5))/G'(T)^3.$$

The gcd of  $G(T)$  and the numerator of the last expression is  $H(T) = T^2 + T + x^2 + x$  and, in the ring  $R_1 = (k[x]/(x+1)^4)[T]/(H(T))$ , we solve the system  $t + ax + b = D(t) + a = 0$ , so  $a = D(t), b = t + D(t)x$ . We find that  $D(t) = 1$ , so  $a = 1, b = x + t$ . Now, modulo the ideal  $(x+1)$ , we have  $H(T) = T^2 + T = T(T+1)$  and we lift this factorization to  $R_1$  and find  $H(T) = (T+x)(T+x+1)$ . Now,  $R_1$  is a direct sum of two rings from this factorization and  $b = 0, 1$  respectively in each of the factors. Consequently,  $G(T)$  has the factors  $T+x, T+x+1$  of the required form.

**Remark 2.4.** *If the characteristic is zero or large, we need to replace  $R_1$ . We could work with the ring  $(\mathcal{O}/\mathfrak{m}^n)[T]/(G(T))$  for suitable  $n$ , but the Hasse derivatives do not preserve this ring. Instead, we can consider  $D^{(i)} : (\mathcal{O}/\mathfrak{m}^n)[T]/(G(T)) \rightarrow (\mathcal{O}/\mathfrak{m}^{n-i})[T]/(G(T))$ . We have not worked out the full details of this possibility.*

### 3. A SUITABLE PLACE

As discussed above, given a function field  $K/k$  and  $f \in K, f \neq 0$ , we need to construct a place  $v$  of the function field  $K$  such that  $v(f) = 0$ , as well as an uniformizer for this place. While, in some cases (e.g.  $k$  finite,  $K = k(x)$ ) this is easy, it can be difficult in the generality we work with and some of the literature seems to gloss over this point (but see [GS00, Algorithm 3.2]). Without loss of generality, we assume that  $k$  is finitely generated over its prime field. We can also assume that  $f \notin k$ , for otherwise the condition  $v(f) = 0$  is automatic and we can replace  $f$  by an element of  $K \setminus k$  in order to produce the place  $v$ . Under this additional hypothesis, there are only at most  $2[K : k(f)]$  places of  $K$  with  $v(f) \neq 0$  and to find  $v$  it suffices to generate enough places of  $K$ .

Assume first that  $k$  is a finite field. We need also to be able to take  $p$ -th roots in  $K$  and, by taking successive  $p$ -th roots of  $f$ , we assume  $K/k(f)$  separable. Then  $K = k(f, g)$  for some  $g \in K$  and there is  $P(x, y) \in k[x, y], P(f, g) = 0$ . We then find  $\alpha \neq 0$  in  $k$  or in an extension field such that  $P(\alpha, y)$  is separable. There is a place of  $K$  corresponding to each irreducible factor of  $P(\alpha, y)$  over  $k(\alpha)$  and, if  $m(x)$  is the minimal polynomial of  $\alpha$  over  $k$ , then  $m(f)$  is an uniformizer for any such place, as  $m(f)$  is an uniformizer for the corresponding place of  $k(f)$  which, by construction, is unramified in  $K$ . While this procedure is straightforward enough, it is worth pointing out that we may not have a suitable place with residue field  $k$  or even an extension of  $k$  of small degree as we can see by considering a simple example such as  $T^p - (x^{p^n} - x) + 1 \in \mathbb{F}_p(x)[T]$ . It is possible to ensure that a suitable place with residue field  $k$  exists if  $\#k$  is large enough in terms of  $[K : k(f)]$  and the genus of  $K$ .

The case where  $k$  is not algebraic over its prime field can be tackled as follows. Let  $k_0$  be the algebraic closure in  $k$  of its prime field. Then  $K$  and  $k$  are respectively the function field of varieties  $X, Y$  over  $k_0$  with a map  $X \rightarrow Y$  of relative dimension 1. We realize  $X$  as a subvariety of projective space and intersect  $X$  with random hypersurfaces. As long as these hypersurfaces intersect  $X$  in an irreducible subset that is not a component of the divisor of  $f$  and is transversal to the fibers of the map  $X \rightarrow Y$ , such a hypersurface will define a place of  $K/k$  satisfying our requirements and the equation of the hypersurface is the uniformizer we need. The version of Bertini's theorem over finite fields from [CP16] guarantees that, for high enough degree, most hypersurfaces satisfy our conditions. Checking that they do can be done using the main algorithm of this paper.

## 4. OTHER APPLICATIONS

As mentioned in the introduction, [Rup99] has a bound on the size of the largest prime  $p$  for which an irreducible polynomial in  $\mathbb{Z}[x, y]$  factors modulo  $p$ . We substantially extend this result. We will consider polynomials in  $K[T]$  where  $K/k$  is a function field and  $k$  itself is a global field. We impose no restriction on the characteristic of  $k$ . We can associate a height to elements of  $k$  in the usual way. If we represent  $K$  as a finite extension of  $k(x)$  for some transcendental element  $x$  of  $K$ , we can talk about the coefficients of an element of  $K$  and their height. Given  $G(T) \in K[T]$ , for all but finitely primes  $\mathfrak{p}$  of  $k$ , we can consider the reduction of  $G(T)$  modulo  $\mathfrak{p}$ .

**Theorem 4.1.** *Let  $k$  be a global field,  $K/k$  a function field and  $G(T) \in K[T]$  an irreducible polynomial, as in equation 2.1 and define  $\Delta$  as in equation 2.3. Let  $H$  be the maximum height of the coefficients of the  $a_i$ . The norm  $N(\mathfrak{p})$  of the primes  $\mathfrak{p}$  of  $k$  for which the reduction of  $G(T)$  modulo  $\mathfrak{p}$  is either undefined or reducible satisfies  $N(\mathfrak{p}) = O(H^{(\Delta+1)^3})$ , where the implied constant depends on  $s, \Delta$ .*

*Proof.* Since  $G(T)$  is assumed irreducible, the matrix  $M$  in Algorithm 1 has maximal rank and so a maximal minor has non-zero determinant. Note that  $\Delta + 1$  is a bound for the number of columns (hence also of rows) of  $M$ . We now compute  $M$  with entries in  $R$  (with no restriction on the characteristic of  $k$ ). It follows from equation 2.2 that the height of the coefficients of  $D^{(i)}(t)$  is  $O(H^i)$ , hence the the height of the coefficients of the (non-zero) determinant of a maximal minor of  $M$  is  $O(H^{(\Delta+1)^3})$  and the result follows.  $\square$

In the case where  $k = \mathbb{F}_q(Z)$ , the approach of the previous theorem is used in [EKR+] to prove a proximity gap statement (in the sense of [BSCI+20, BN20]) for Algebraic Geometry codes.

A different application concerns the the Guruswami-Sudan list-decoding algorithm for Reed-Solomon or Algebraic Geometry codes [GS00]. If one has a fixed code, there are fixed finite dimensional  $k$ -vector spaces  $V_0, W_0, \dots, W_{s-1} \subset K$  and, for each received message, a polynomial  $G(T) \in K[T]$  is constructed with coefficients  $a_i \in W_i$  (the precise construction is irrelevant at the moment), for which we want to know its roots in  $V_0$ . That is precisely the problem we dealt with above, with  $r = 1$ . In this situation, we can take advantage of the fact that the vector spaces above are fixed and construct a set of differential operators  $\mathcal{D}$  on  $K$  such that  $\mathcal{D}(t) = 0$  for a root  $t$  of  $G(T)$  if and only if  $t \in V_0$  (e.g. if  $V_0$  consists of polynomials in  $x$  of degree  $< n < p$ , then  $\mathcal{D} = d^n/dx^n$ ). The construction of  $\mathcal{D}$  is independent of the received message and the construction of  $G(T)$  can be done by viewing the coordinates of the message as independent variables and running the algorithm 1 by extending scalars from  $k$  to some field of rational functions over  $k$ . In this way, the calculation needs to be performed once and reused for each invocation of the Guruswami-Sudan algorithm.

## ACKNOWLEDGEMENTS

This work was supported by MBIE. I would also like to thank the other authors of [EKR+] for questions that motivated this research.

## 5. REFERENCES

- [BvHKS09] Karim Belabas, Mark van Hoeij, Jürgen Klüners, and Allan Steel, *Factoring polynomials over global fields*, J. Théor. Nombres Bordeaux **21** (2009), no. 1, 15–39. [↑1](#)

- [BSCI<sup>+</sup>20] Eli Ben-Sasson, Dan Carmon, Yuval Ishai, Swastik Kopparty, and Shubhangi Saraf, *Proximity Gaps for Reed-Solomon Codes* (2020). Cryptology ePrint Archive, Report 2020/654. [↑7](#)
- [BN20] Sarah Bordage and Jade Nardi, *Interactive Oracle Proofs of Proximity to Algebraic Geometry Codes* (2020). arXiv:2011.04295. [↑7](#)
- [CP16] François Charles and Bjorn Poonen, *Bertini irreducibility theorems over finite fields*, J. Amer. Math. Soc. **29** (2016), no. 1, 81–94. [↑6](#)
- [EKR<sup>+</sup>] Muhammed Esgin, Veronika Kuchta, Sushmita Ruj, Amin Sakzad, Ron Steinfeld, and José Felipe Voloch. in preparation. [↑7](#)
- [GS00] Shuhong Gao and M. Amin Shokrollahi, *Computing roots of polynomials over function fields of curves*, Coding theory and cryptography (Annapolis, MD, 1998), Springer, Berlin, 2000, pp. 214–228. [↑1](#), [6](#), [7](#)
- [Gao03] Shuhong Gao, *Factoring multivariate polynomials via partial differential equations*, Math. Comp. **72** (2003), no. 242, 801–822. [↑2](#)
- [GV87] Arnaldo García and José Felipe Voloch, *Wronskians and linear independence in fields of prime characteristic*, Manuscripta Math. **59** (1987), no. 4, 457–469. [↑2](#), [5](#)
- [vzGK85] J. von zur Gathen and E. Kaltofen, *Factorization of multivariate polynomials over finite fields*, Math. Comp. **45** (1985), no. 171, 251–261. [↑1](#)
- [Hes02] Florian Hess, *An algorithm for computing Weierstrass points*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 357–371. [↑2](#), [3](#)
- [Poh05] Michael E. Pohst, *Factoring polynomials over global fields. I*, J. Symbolic Comput. **39** (2005), no. 6, 617–630. [↑1](#), [2](#), [3](#)
- [Rup99] Wolfgang M. Ruppert, *Reducibility of polynomials  $f(x, y)$  modulo  $p$* , J. Number Theory **77** (1999), no. 1, 62–70. [↑2](#), [7](#)
- [Sch39] Friedrich Karl Schmidt, *Die Wronskische Determinante in beliebigen differenzierbaren Funktionenkörpern*, Mathematische Zeitschrift **45** (1939), no. 1, 62–74. [↑2](#), [3](#)
- [SV86] Karl-Otto Stöhr and José Felipe Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) **52** (1986), no. 1, 1–19. [↑2](#)

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF CANTERBURY, PRIVATE BAG 4800, CHRISTCHURCH 8140, NEW ZEALAND

*Email address:* felipe.voloch@canterbury.ac.nz

*URL:* <http://www.math.canterbury.ac.nz/~f.voloch>