Veridise Logarithmic Derivative Review

Rigo Salazar, Freeman Slaughter, Luke Szramowski, Cypher Stack *

March 14, 2025

This report contains a review of a logarithmic derivative technique report from Veridise. As with any such report, it may contain errors and cannot guarantee correctness or security. Further, it cannot guarantee that any particular implementation of the construction is correct, secure, or suitable for intended use cases.

The authors assert no warranty and disclaim liability for its use. The authors further express no endorsement of any kind. This report has not undergone any further formal or peer review

Contents

1 Introduction

We find that the original paper [Bas24] lacks a formal backing for the results used and proven. The mathematics contained in the report are sound, but lack direct reference to the results or do not contain enough justification to be taken at face value.

Within the findings section, we have included a rework of each section of the paper, including citations of results which are invoked, proofs of results which were stated but for which proofs were unavailable, and inclusion of important background information.

It is also of importance that the notation used possess a higher degree of specificity, which will be highlighted in the notation section below.

2 Notation

Throughout this report, the following notation will be used, unless otherwise specified.

- Let F denote the function field over K, where K is perfect and the full constant field of F.

*https://cypherstack.com

- We denote the characteristic of F as prime p.
- Let $F^\times$ denote the multiplicative group of F.
- For a point $P = (a, b)$ on an elliptic curve, we denote $x(P) = a$ and $y(P) = b$.
- For an elliptic curve E, we denote $\mathcal{O}_\infty$ as the point at infinity.
- Let $K[x, y]$ denote the ring of polynomials, in x and y, with coefficients in K and $K(x, y)$ denote the ring of rational functions in x and y.

3 Restructure

3.1 Regarding Derivations

Definition 1. A *derivation* of the quotient field F/K into F is a K-linear map $\delta : F \to F$ such that, for each $f, g \in F$, it holds that $\delta(f \cdot g) = f \cdot \delta(g) + \delta(f) \cdot g$.

Definition 2 ([DF04], 551)**.** The field K is said to be *separable* (or *separably algebraic*) over F if every element of K is the root of a separable polynomial over F. Equivalently, the minimal polynomial over F of every element of K is separable.

Definition 3. A *separating element* of F/K in F is defined as any element for which $F/K(x)$ is a separable algebraic extension.

Definition 4. Let F be a field and K be a finite extension of F. Let $\alpha \in K$ and define the linear transformation $\ell_\alpha : K \to K$ by $\ell_\alpha(x) \mapsto \alpha \cdot x$. Then the *field norm* of α with respect to F/K is defined to be the determinant of ℓ_α.

We recall some properties regarding derivations and separating elements, which are from [Sti09]:

Proposition 1 ([Sti09], Proposition 4.1.4b)**.** For each separating element z, there exists a unique derivation δ_z such that $\delta_z(z) = 1$.

Lemma 1 ([Sti09], Lemma 4.1.6a)**.** For each derivation η and $x \in F$, we have that

$$\eta = \eta(x) \cdot \delta_x.$$

Lemma 2 ([Sti09], Lemma 4.1.6b)**.** Let x and y be separating elements. Then it holds that

$$\delta_y = \delta_y(x) \cdot \delta_x.$$

Lemma 3 ([Sti09], Lemma 4.1.6c)**.** Let $t \in F$. Then $\delta_x(t) \neq 0$ if and only if t is a separating element.

Definition 5. Given a function field F/K and a derivation δ, the *logarithmic derivative* is the map $L : F^\times \to F$ defined as $L(f) = \frac{\delta(f)}{f}$.

In the classical case from calculus, this corresponds to $\frac{\mathrm{d}}{\mathrm{dx}} \ln(f(x))$ for a function $f(x)$. This map defines a group homomorphism, which can be seen by the following:

$$L(f \cdot g) = \frac{\delta(f \cdot g)}{f \cdot g} = \frac{f \cdot \delta(g) + \delta(f) \cdot g}{f \cdot g} = \frac{\delta(f)}{f} + \frac{\delta(g)}{g} = L(f) + L(g).$$

3.2 Characterization of the Kernel

We can use Lemma 3 to characterize the kernel of the logarithmic derivative. In specific,

$$\ker(L) = \{t \in F^\times : L(t) = 0\}.$$

We can first notice that the kernel of L is determined entirely by the kernel of the derivation, since:

$$\begin{aligned} L(t) = 0 &\Leftrightarrow \frac{\delta(t)}{t} = 0 \\ &\Leftrightarrow \delta(t) = 0 \text{ and } t \neq 0. \end{aligned}$$

So, we can note that all non-trivial elements of the kernel of L will be exactly the non-trivial elements of the kernel of δ.

Remark 1. In order to increase readability, it should be noted that when δ is invoked, it is simply δ_a for some separating element a. The particular element is not chosen specifically - nor does it need to be, by Lemma 2, since each derivation is only going to differ by some non-zero scalar.

Lemma 4. Let a, b be separating elements in F. Then:

$$\ker(\delta_a) = \ker(\delta_b).$$

Proof. We shall go about this by subset containment, then conclude by similarity of cases. Let $k \in \ker(\delta_a)$. Since a, b are separating elements, Lemma 2 implies that

$$\delta_a = \delta_a(b) \cdot \delta_b.$$

By Lemma 3, we have that $\delta_a(b) \neq 0$. Taking the evaluation of k on both sides yields:

$$0 = \delta_a(k) = \delta_a(b) \cdot \delta_b(k).$$

Since $\delta_a(b) \neq 0$, it must be the case that $\delta_b(k) = 0$. So, $k \in \ker(\delta_b)$, as desired. It is clear that if we started with $l \in \ker(\delta_b)$ that the same argument would show $l \in \ker(\delta_a)$, therefore we have our desired result. □

The first thing we can notice is that if $k \in K$, then it is not a separating element, and as such, $\delta(k) = 0$, by the equivalence prior stated in Lemma 3. Thus, $K \subset \ker(\delta)$. In essence, elements of K behave the way constant values do in single-variable calculus.

Due to the result from Lemma 3, we can see that the kernel is exactly described as the set of all non-separating elements. An exact characterization of this is given in ([Sti09], Proposition 3.10.2), which allows us to note that:

$$\ker(L) = \{f \in F^\times : f \in K \text{ or } f = u^p \text{ with } u \in F^\times\}.$$

This characterization lends itself nicely to our intuition regarding derivatives from calculus: the kernel clearly contains constant terms, whose derivatives should vanish and all terms that would result in a multiple of p being produced would vanish as well. This characterization is important to the results below, so keep it in mind moving forward.

3.3 Notes on the Degree

Definition 6. For $t \in F \setminus K$, the *degree* of t in F, which we denote as $\deg_F(t)$, is defined as $\deg_F(t) = [F : K(t)]$.

We can note that since the field has characteristic p, the degree of the polynomial is exactly what one would expect. However, since fields don't possess an inherent metric which gives a useful scale to field elements, the workaround is to define such a measure algebraically.

The following quantities are equal:

1. $\deg_F(t)$
2. $\deg(t)_\infty$, which denotes the pole divisor of t in F.
3. $\deg(t)_0$, which denotes the zero divisor of t in F.

We can further note here that if the base field F and the rational function field $K(x)$ coincide, then the usual definition of degree holds. That is, for $a(x), b(x) \in F$, which are relatively prime:

$$\deg_F\left(\frac{a(x)}{b(x)}\right) = \deg_{K(x)}\left(\frac{a(x)}{b(x)}\right) = \max\left\{\deg(a(x)), \deg(b(x))\right\},$$

where the degree contained in the maximum is the standard polynomial degree.

It should be remarked that the degree operation behaves in a logarithmic fashion, in the sense that we can extract powers from it. That is, for $t = u^x$, then it holds that $\deg_F(t) = \deg_F(u^x) = x \cdot \deg_F(u)$, where $u \in F$ and $x \in K$.

With the prior background knowledge in mind, let us consider the following lemma:

Lemma 5. Let $f, g \in F$, where $\deg_F(f), \deg_F(g) < p$. Then $L(f) = L(g)$ if and only if $f = c \cdot g$ for some $c \in K$.

Proof. ($\Leftarrow$) We first establish the backward direction: let $f, g \in F$. Suppose that there exists some $c \in K$ such that $f = c \cdot g$. Using the definition of a derivation, the calculation is as follows:

$$L(f) = \frac{\delta(f)}{f} = \frac{\delta(c \cdot g)}{c \cdot g} = \frac{c \cdot \delta(g) + \delta(c) \cdot g}{c \cdot g} = \frac{c \cdot \delta(g)}{c \cdot g} = L(g)$$

($\Rightarrow$) Now we show the forward direction. We start by assuming that $L(f) = L(g)$, and $\deg_F(f), \deg_F(g) < p$. Let us recall from prior assumption that the ambient field K is perfect; that is, that every polynomial splits into linear factors. As such, we can define f and g as follows:

$$f(x) = a\prod_{i=1}^{p-1}(x - r_i) \quad \text{and} \quad g(x) = b\prod_{i=1}^{p-1}(x - q_i),$$

where $a, b, r_i, q_i \in K$ for all i. Now, taking the logarithmic derivative, we find that

$$L(f(x)) = a\sum_{i=1}^{p-1}\frac{1}{x - r_i} \quad \text{and} \quad L(g(x)) = b\sum_{i=1}^{p-1}\frac{1}{x - q_i}.$$

Given that $L(f) = L(g)$, it must be the case that the functions possess poles at the same locations with the same multiplicity. Specifically, that

$$a\sum_{i=1}^{p-1}\frac{1}{x - r_i} = b\sum_{i=1}^{p-1}\frac{1}{x - q_i},$$

hence there must exist some permutation π such that $r_{\pi(i)} = q_i$. Then it must be the case that the roots of f are precisely the roots of g, where the functions themselves can differ only by a multiplicative constant, as claimed.

□

Remark 2. It should be noted that if K is not a splitting field of F, the proof becomes far more difficult. The inclusion of the perfectness of K is necessary to draw this result.

3.4 Precursory Substitutions

Let us define $\mathbb{F}_q(E)$ to be the function field of the elliptic curve E, given by the equation:

$$y^2 = x^3 + Ax + B,$$

where $A, B \in \mathbb{F}_q$. Let $D(x, y) \in \mathbb{F}_q(E)$. We can recall that $D(x, y)$ will be a polynomial in indeterminate x and y, and we shall only consider the evaluation of $D(x, y)$ on points which fall on the curve. Let us further assume it only possesses poles at the point at infinity. We can explicitly express $D(x, y)$ in the following form, for some natural numbers n, m:

$$D(x, y) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_{i,j} x^i y^j.$$

We can notice that everywhere y^2 (or some power of y^2) appears in the summation, it can be replaced by the equation of the curve. Furthermore, every odd power of y can also undergo this replacement after separating the even component of the power (for example, $y^3 = y^2 \cdot y$). Using this method, we can re-express this as $D(x, y) = a(x) - y \cdot b(x)$ for some polynomials $a(x), b(x) \in \mathbb{F}_q(x)$.

Now, let us consider the substitution $z = y - \lambda \cdot x$ for some $\lambda \in \mathbb{F}_q$. Substituting this into the original curve, we obtain

$$0 = y^2 - x^3 - A \cdot x - B = (z + \lambda \cdot x)^2 - x^3 - A \cdot x - B.$$

Expanding and collecting like terms, we find that

$$x^3 - (\lambda \cdot x)^2 + (2\lambda z + A) \cdot x + (B - z^2) = 0.$$

We can notice that in order to obtain $\mathbb{F}_q(E)$ from $\mathbb{F}_q(z)$, we need to simply adjoin a root of the above polynomial. As it is a third degree polynomial, we can denote the roots of the polynomial as x_0, x_1 and x_2. Let $y_i = z - \lambda \cdot x_i$. We shall use the above substitution in the derivation given in the next subsection.

3.5 Formal Deduction of the Desired Formula

Remark 3. For all the following derivations, we shall include comments on an operation-by-operation basis to reduce confusion, as well as simplify notation where needed.

We wish to find an expression for the logarithmic derivative of the norm of $D(x, y)$. To do this, consider the following steps:

1. Let us begin by symbolically noting that the quantity we wish to derive an expression for is given by
$$L(N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D(x, y))) = \frac{\delta_z(N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D(x, y)))}{N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D(x, y))}.$$

2. By the result given in [[DF04], Exercise 17], we have that

$$N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D(x,y)) = \prod_{i=0}^{2} D(x_i, y_i).$$

3. We can notice that taking the logarithmic derivative will require us to find the derivation of this product. Since the Leibnitz rule holds, we can see that

$$\delta_z\left(\prod_{i=0}^{2} D(x_i, y_i)\right) = \sum_{j=0}^{2} \frac{\prod_{i=0}^{2} D(x_i, y_i)}{D(x_j, y_j)} \delta_z(D(x_j, y_j)).$$

4. So, let us determine an expression for $\delta_z(D(x_j, y_j))$. Starting from $D(x_j, y_j) = a(x_j) - y_j \cdot b(x_j)$, we have that:

$$\delta_z(D(x_j, y_j)) = \delta(x_j) \cdot a'(x_j) - \delta_z(y_j) \cdot b(x_j) - y_j \cdot b'(x_j)\delta_z(x_j),$$

where $a'(x_j)$ and $b'(x_j)$ are the usual derivatives on polynomials.

5. Now, let us recall that $y_j^2 = x_j^3 + A \cdot x_j + B$. Taking δ_{x_j} of both sides and collecting terms yields

$$\delta_{x_j}(y_j) = \frac{3 \cdot x_j^2 + A}{2 \cdot y_j}.$$

6. We re-parameterize the derivation with respect to z, since $\delta_v = \delta_v(w) \cdot \delta_w$ (using Lemma 2), which leaves us with

$$\delta_z(y_j) = \frac{3x_j^2 + A}{2 \cdot y_j} \delta_z(x_j).$$

7. As $z = y_j - \lambda \cdot x_j$, taking the derivation results in $\delta_z(z) = \delta_z(y_j) - \lambda \cdot \delta_z(x_j)$, which paired with the above and 1 gives

$$\left(\frac{3x_j^2 + A}{2 \cdot y_j} - \lambda\right) \cdot \delta_z(x_j) = 1.$$

8. With the above expression, we can solve for $\delta_z(x_j)$:

$$\delta_z(x_j) = \frac{2 \cdot y_j}{3x_j^2 + A - \lambda \cdot 2y_j}.$$

9. We now have all the pieces needed to simplify the expression for the logarithmic derivative of the norm of $D(x, y)$. By definition, we have that

$$L(N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D(x,y))) = \sum_{j=0}^{2} \frac{\delta_z(D(x_j, y_j))}{D(x_j, y_j)}.$$

Applying Item 4 above, we have that

$$L(N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D(x,y))) = \sum_{j=0}^{2} \frac{\delta(x_j) \cdot a'(x_j) - \delta_z(y_j) \cdot b(x_j) - y_j \cdot b'(x_j)\delta_z(x_j)}{D(x_j, y_j)}.$$

Using Item 6 above, we can substitute $\delta_z(y_j)$ to obtain

$$L(N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D(x,y))) = \sum_{j=0}^{2} \frac{\delta(x_j)\cdot a'(x_j) - \left(\frac{3x_j^2+A}{2\cdot y_j}\delta_z(x_j)\right)\cdot b(x_j) - y_j\cdot b'(x_j)\delta_z(x_j)}{D(x_j,y_j)}.$$

Notice that the numerator possesses $\delta_z(x_j)$ in each of its terms, thus it may be factored out as follows

$$L(N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D(x,y))) = \sum_{j=0}^{2} \frac{a'(x_j) - \left(\frac{3x_j^2+A}{2\cdot y_j}\right)\cdot b(x_j) - y_j\cdot b'(x_j)}{D(x_j,y_j)}\delta_z(x_j).$$

Finally, we can then replace the factored term by the expression solved for in Item 8 to find that

$$L(N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D(x,y))) = \sum_{j=0}^{2} \frac{a'(x_j) - \left(\frac{3x_j^2+A}{2\cdot y_j}\right)\cdot b(x_j) - y_j\cdot b'(x_j)}{D(x_j,y_j)}\cdot\frac{2\cdot y_j}{3x_j^2+A-2\lambda\cdot y_j}.$$

This gives us the desired final form of the derivation. We note that in this form it is straightforward to evaluate the logarithmic derivative of the norm at some point, as the summation is taken over only three points.

3.6 A Potential Vulnerability

The first notion that we must approach with care is the multiplicities of the roots of the selected polynomials. As is seen in the above derivation, we have that:

$$\delta_z(N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D(x,y))) = \sum_{i=1}^{k}\frac{n_i}{z-z(P_i)},$$

where the n_i are the multiplicities of the roots found in $D(x,y)$. The immediate danger is that, as this calculation is performed over a finite field of characteristic p, terms could potentially vanish upon modular reduction. For all practical purposes, it can be argued that this issue occurs with only negligible probability, due to the extremely large value of p and the comparatively small degree of the polynomial. As such, selecting a large enough value of p (say, on the order of 2^{252} for example) is sufficient to assuage us of this vulnerability.

A more glaring issue that occurs is that an adversary with knowledge of a single valid proof can forge an arbitrary amount of proofs. Moreover, they may do so in a straightforward fashion. We can recall that the motivation behind this derivation is to give a proof of the following:

$$\sum_{i=1}^{k} n_i\cdot P_i = \mathcal{O}_\infty,$$

where $\mathcal{O}_\infty$ denotes the point at infinity. Since this addition is computed over a field with characteristic p, then for any sequence $\{d_i\}_{i=1}^{k}$ with $d_i\in\mathbb{Z}$ for all i, we have that

$$\sum_{i=1}^{k}(n_i+d_i\cdot p)\cdot P_i \equiv \sum_{i=1}^{k} n_i\cdot P_i.$$

This implies that an adversary can take a valid proof and add on points times integer multiples of p, and this will appear to also have the same valid proof.

The obvious, naive fix to this issue would be to add on a check to guarantee that the committed coefficients are in reduced form modulo p. This would effectively necessitate a range proof, which can be done efficiently with Bulletproofs [BBB+17] for instance, but it is actually not enough to prevent forgeries.

Suppose that an adversary obtains a valid proof that $\sum_{i=1}^{k} n_i \cdot P_i = \mathcal{O}_\infty$, where the n_i coefficients have passed a range proof certifying that $0 \leq n_i < p$ for each i. As $\mathcal{O}_\infty$ behaves like an identity, $\mathcal{O}_\infty = -\mathcal{O}_\infty$. This adversary can take $p \cdot P_1 + \cdots + p \cdot P_k = 0$, then subtract the valid representation, which results in

$$\sum_{i=1}^{k} (p - n_i) \cdot P_i = -\mathcal{O}_\infty = \mathcal{O}_\infty,$$

thus also represents a valid proof. The important feature to note here is that if the n_i coefficients pass a range proof certifying that $0 \leq n_i < p$ for all i, then for each non-zero n_i we also have that $0 \leq p - n_i < p$, which similarly passes the same range proof.

This highlights that a naive implementation of the range proof to check that the coefficients n_i are in $[0, p)$ is insufficient. Indeed, a range proof with an upper bound of $\lfloor p/2 \rfloor$ would be more appropriate to prevent this vulnerability. For security purposes, it may be necessary to require the upper bound of the range proof be even smaller to widen the gap between n_i and $p - n_i$, say $\lfloor p/10 \rfloor$, or perhaps simply set an immutable, predetermined upper bound on a protocol basis that nearly all real-world instances fall under, something like $2^{33} \approx 10^{10}$. Overall, we do not see an immediate way around range proofs, it appears that they are required to prevent adversarial forgeries.

References

[Bas24] Alp Bassa. On the Use of Logarithmic Derivatives in Eagen's Proof of Sums of Points. `https://repo.getmonero.org/-/project/54/uploads/bfe9f49326a843ef1c9466e30a5d42c8/VAR_Monero_Logarithmic_Derivatives_Final.pdf`, 2024. Accessed: 03-Mar-2025.

[BBB+17] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short Proofs for Confidential Transactions and More. Cryptology ePrint Archive, Paper 2017/1066, 2017. `https://eprint.iacr.org/2017/1066`.

[DF04] David S. Dummit and Richard M. Foote. *Abstract Algebra, 3rd Edition.* John Wiley and Sons, Inc., 2004.

[Sti09] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Graduate Texts in Mathematics. Springer, 2009. `https://doi.org/10.1007/978-3-540-76878-4`.