Veridise

# On the Use of Logarithmic Derivatives in Eagen's Proof of Sums of Points

Alp Bassa

Veridise

## 1 Background

Consider an elliptic curve over the finite field $\mathbb{F}_q$ given by the equation

$$y^2 = x^3 + A \cdot x + B.$$

Eagen ([3, Section 3]) provides an interactive prove that given rational points $P_1, P_2, \ldots, P_N$ of the elliptic curve sum to zero.

$$P_1 + P_2 + \cdots + P_N = \mathcal{O}.$$

The idea is to provide as witness a rational function $D(x, y)$ on the elliptic curve (regular outside $\infty$), which vanishes precisely at these points. An argument for the vanishing of the function at the points is obtained by taking a random line $\ell$, projecting the points onto $\ell$, and showing that the pushforward (norm) of $D(x, y)$ vanishes at the projected points. More precisely, a line given by $y - \lambda \cdot x = 0$ defines a map $(x, y) \mapsto y - \lambda \cdot x =: z$ and hence gives a subfield $\mathbb{F}_q(z)$ of the function field $E = \mathbb{F}_q(x, y)$ of the elliptic curve. The task is reduced to showing that

$$N_{\mathbb{E}/\mathbb{F}_q(z)}(D(x, y))$$

vanishes precisely at the points $z(P_1), z(P_2), \ldots, z(P_N)$. Here $N_{E/\mathbb{F}_q(z)}(\cdot)$ denotes the field norm from $E$ to $\mathbb{F}_q(z)$ (e.g. see [7, Chapter VI, Section 5]). So we have to provide a proof for

$$N_{\mathbb{E}/\mathbb{F}_q(z)}(D(x, y)) = \prod_{i=1}^{N}(z - z(P_i)).$$

Note that both sides are functions of $z$, the coordinate on the line. This is done by evaluating both sides of above equations at a random point $z = \mu$ on the line, by the use of the Schwartz-Zippel Lemma ([8, 11]). A soundness proof for this fact was given in [1]. Rather than first obtaining the norm of $D(x, y)$ and evaluating it at $\mu$, by the relation between pushforward and pullback of functions and divisors, one can evaluate $D(x, y)$ at the pullback of the divisor $(z = \mu)$ on $E$ (at the points on $E$ mapping to the point $z = \mu$). There is another small modification concerning the choice of the random line $y = \lambda \cdot x$ and the random evaluation point $\mu$. As $D(x, y)$ is evaluated at the points on $E$ mapping to a random point $\mu$ on a random line $\ell$, rather than choosing the line $\ell$ and the point $\mu$, we can randomly choose three collinear points $A_0, A_1, A_2$ on $E$ and use the line they define for the projection. As three collinear points on $E$ add up to $\infty$, the choice of $A_0$ and $A_1$ uniquely determine $A_2$. The choice of $A_0, A_1$ gives a slightly different probability distribution than a choice $\lambda$ (defining $\ell$) and a consecutive choice of $\mu$, but a similar soundness argument applies. For further details see [1].

As a further simplification, Eagen [3] utilizes logarithmic derivatives, the use of which will be detailed and formalized in this note.

## 2 Derivations and the Logarithmic Derivative

For further details on derivations and their relation to differentials, see [10, Chapter 4]. For their cryptographic use see [4, 6]. Let $F$ be a function field over $K$ (assume $K$ is perfect and it is the full constant field of $F$). A derivation of $F/K$ into $F$ is a $K$-linear map $\delta : F \to F$ satisfying the Leibniz rule for products

$$\delta(f \cdot g) = f \cdot \delta(g) + \delta(f) \cdot g$$

for all $f, g \in F$.

If $z \in F$ is a separating element of $F/K$ (i.e. $F/K(z)$ is finite and separable), then any derivation $\delta : F \to F$ of $F/K$ is uniquely determined by $\delta(z)$ ([10, Proposition 4.1.4]). Moreover, there exists a derivation $\delta : F \to F$ of $F/K$ with $\delta(z) = 1$. This derivation is unique by above and it is called the derivation with respect to $z$. It is denoted by $\delta_z$. On $K(z)$ it corresponds to the formal derivative with respect to $z$.

For a derivation $\eta : F \to F$ we have

$$\eta = \eta(z) \cdot \delta_z.$$

This can be easily seen by the uniqueness result above and the fact that both sides agree on the separating element $z$. In particular, for another separating element $y$ of $F/K$ we have

$$\delta_y = \delta_y(z) \cdot \delta_z,$$

which corresponds to the chain rule.

It can be shown that for a separating element $z \in F$ and for $t \in F$ we have

$$\delta_z(t) \neq 0 \Leftrightarrow t \text{ is a separating element.}$$

In particular $\delta_z(t) = 0$ if and only if $t \in K$ or $t = u^p$ for some $u \in F$, where $p$ is the characteristic. Note that this agrees with our intuition that constants should have zero derivatives and for $t = u^p$ we have $t' = p \cdot u^{p-1} \cdot u' = 0$ in characteristic $p$. Here primes indicate derivatives.

Given a function field $F/K$ and a derivation $\delta : F \to F$ of $F/K$, we can define the map $L : F^\times \to F$ by

$$f \mapsto \frac{\delta(f)}{f}.$$

This map is called the logarithmic derivative, as in the classical case it corresponds to taking the derivative of the function $\log(f)$. Using the Leibniz rule, we have

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

Hence $L$ is a homomorphism from the multiplicative group $F^\times$ to the additive group $F$. By the characterization of elements $t \in F$ satisyfing $\delta(t) = 0$, the kernel of $L$ is given by

$$\ker(L) = \{t \in F^\times | t \in K \text{ or } t = u^p \text{ for some } u \in F\}.$$

For $t \in F \backslash K$ we can define $\deg_F(t) = [F : K(t)] = \deg(t)_\infty = \deg(t)_0$, where $(t)_\infty$ and $(t)_0$ denote the pole divisor and the zero divisor of $t$ in $F$, respectively. Note that for $F = K(x)$, the rational function field, we recover the usual definition

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

for $a(x)$ and $b(x)$ relatively prime. Here deg on the right hand side denotes the usual degree as a polynomial. Raising an element to a power $n$ multiplies its degree by $n$, hence if $t = u^p$, then $\deg_F(t) = \deg_F(u^p) = p \cdot \deg_F(u)$. Hence for large $p$ we obtain an easy way of checking $t \neq u^p$ for any $u \in F$:

**Lemma 1.** *Suppose $t \in \ker(L)$ and $\deg_F t < p$. Then $t \in K$, i.e. the only elements in the kernel of the logarithmic differential of low degree are constants. In particular for nonzero $f, g$ of degree $< p$ we have $L(f) = L(g)$ if and only if $f = c \cdot g$ for some constant $c \in K$.*

# 3 Verifying the Divisor Witness

Our aim is to establish

$$N_{E/\mathbb{F}_q(z)}(D(x,y)) = \prod_{i=1}^{N}(z - z(P_i)). \tag{1}$$

We assume both sides have degree smaller than the characteristic $p$. Hence showing that their logarithmic derivatives agree and one of the coefficients is equal suffices to conclude equality. Alternatively, without comparing coefficients we can conclude that they differ by a multiplicative constant. Hence assume $\deg D, N \ll p$. This will ensure that both the norm of $D$ and the term on the right have small degree. By Lemma 1, if their logarithmic derivatives agree, we can conclude that they differ by a multiplicative constant.

Now the logarithmic derivative (with respect to $z$) of the term on the right can be easily computed by the Leibniz rule:

$$\frac{\delta_z\left(\prod_{i=1}^{N}(z - z(P_i))\right)}{\prod_{i=1}^{N}(z - z(P_i))} = \sum_{i=1}^{N}\frac{1}{z - z(P_i)}.$$

Evaluating this at the point $z = \mu$ gives

$$\sum_{i=1}^{N}\frac{1}{\mu - z(P_i)}. \tag{2}$$

The logarithmic derivative of the norm is a bit more involved. It can in fact be expressed in terms of the values of $D(x,y)$ at the points $A_0, A_1, A_2$ in the support of the pullback of the divisor $(z = \mu)$. The computation is done in the next section.

# 4 Formulas for the Logarithmic Derivative of the Norm

Let $E = \mathbb{F}_q(x,y)$ be the function field of the elliptic curve given by the equation

$$y^2 = x^3 + A \cdot x + B, \tag{3}$$

with $A, B \in \mathbb{F}_q$. Assume $D(x,y) \in E$ has only poles at $\infty$. Using Equation (3) we can write $D(x,y)$ in the form $D(x,y) = a(x) - y \cdot b(x)$ for $a(x), b(x) \in \mathbb{F}_q[x]$.

Let $\lambda \in \mathbb{F}_q$ and let

$$z = y - \lambda \cdot x. \tag{4}$$

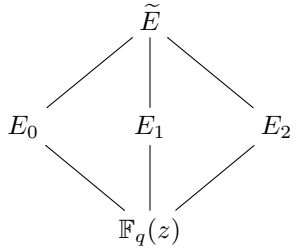
Consider the subfield $\mathbb{F}_q(z) \subseteq E$. We have $[E : \mathbb{F}_q(z)] = 3$. Let $\widetilde{E}$ be the Galois closure of $E/\mathbb{F}_q(z)$. Solving Equation (4) for $y$ and substituting into Equation (3), we obtain

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

So $E$ can be obtained from $\mathbb{F}_q(z)$ by adjoining a root of the polynomial

$$T^3 - \lambda^2 \cdot T^2 + (2\lambda z + A) \cdot T + (B - z^2).$$

Let the roots of this polynomial be given by $x_0, x_1, x_2$ and let $y_i = z - \lambda \cdot x_i$ for $i = 0, 1, 2$. Consider the subfields $E_i = \mathbb{F}_q(x_i, y_i)$ for $i = 0, 1, 2$. We obtain the following diagram of fields:




Note that all extension $E_i/\mathbb{F}_q(z)$, $\widetilde{E}/E_i$ and $\widetilde{E}/\mathbb{F}_q(z)$ are separable. In particular $z$ is a separating element of $\widetilde{E}/\mathbb{F}_q$

Consider the derivation $\delta_z$ of $\widetilde{E}$ with respect to $z$, i.e., the unique derivation $\delta_z : \widetilde{E} \to \widetilde{E}$ with $\delta_z(z) = 1$. Note that its restriction to $\mathbb{F}_q(z)$ corresponds to the formal derivative of the rational function field.

We want to find an expression for the logarithmic derivative of the norm, i.e. $L\big(N_{E/\mathbb{F}_q(z)}(D(x,y))\big)$. For this we first compute the derivation $\delta_z(\cdot)$.

We have

$$N_{E/\mathbb{F}_q(z)}(D(x,y)) = D(x_0,y_0) \cdot D(x_1,y_1) \cdot D(x_2,y_2). \tag{5}$$

We can find the derivation of each of the factors:

$$\delta_z\big(D(x_i,y_i)\big) = \delta_z\big(a(x_i) - y_i \cdot b(x_i)\big) = a'(x_i)\delta_z(x_i) - \delta_z(y_i)b(x_i) - y_i b'(x_i)\delta_z(x_i).$$

Note that $a'$ and $b'$ denote the usual derivatives of the polynomials $a$ and $b$. As $y_i^2 = x_i^3 + A \cdot x_i + B$, by applying $\delta_{x_i}$ and using the chain rule we obtain $2y_i\delta_{x_i}(y_i) = 3x_i^2 + A$, i.e. $\delta_{x_i}(y_i) = (3x_i^2 + A)/(2y_i)$ and hence

$$\delta_z(y_i) = \frac{3x_i^2 + A}{2y_i}\delta_z(x_i). \tag{6}$$

Substituting this above we get

$$\delta_z\big(D(x_i,y_i)\big) = \underbrace{\Big(a'(x_i) - \frac{3x_i^2 + A}{2y_i}b(x_i) - y_i b'(x_i)\Big)}_{\frac{\mathrm{d}D(x_i,y_i)}{\mathrm{d}x_i}}\delta_z(x_i).$$

Hence using Equation (5) we get for the derivation of the norm

$$\begin{aligned}\delta_z\big(N_{E/\mathbb{F}_q(z)}(D(x,y))\big) = {} & \delta_z\big(D(x_0,y_0)\big) \cdot D(x_1,y_1) \cdot D(x_2,y_2) \\ & + D(x_0,y_0) \cdot \delta_z\big(D(x_1,y_1)\big) \cdot D(x_2,y_2) \\ & + D(x_0,y_0) \cdot D(x_1,y_1) \cdot \delta_z\big(D(x_2,y_2)\big).\end{aligned}$$

Hence we get for the logarithmic derivative

$$\begin{aligned} L\big(N_{E/\mathbb{F}_q(z)}(D(x,y))\big) &= \frac{\delta_z\big(N_{E/\mathbb{F}_q(z)}(D(x,y))\big)}{N_{E/\mathbb{F}_q(z)}(D(x,y))} \\ &= \sum_{i=0}^{2} \frac{\frac{\mathrm{d}D(x_i,y_i)}{\mathrm{d}x_i}}{D(x_i,y_i)} \cdot \delta_z(x_i) \\ &= \sum_{i=0}^{2} \frac{\big(a'(x_i) - \frac{3x_i^2+A}{2y_i} b(x_i) - y_i b'(x_i)\big)}{D(x_i,y_i)} \cdot \delta_z(x_i) \end{aligned}$$

To find an expression for $\delta_z(x_i)$, we use Equations (4) and (6). Applying $\delta_z(\cdot)$ to both sides we obtain

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

and hence

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

We obtain

$$L\Big(N_{E/\mathbb{F}_q(z)}(D(x,y))\Big) = \sum_{i=0}^{2} \frac{\big(a'(x_i) - \frac{3x_i^2+A}{2y_i} b(x_i) - y_i b'(x_i)\big)}{D(x_i,y_i)} \cdot \frac{2y_i}{3x_i^2 + A - \lambda \cdot 2y_i}.$$

Finally we want to evaluate this expression at the point $z = \lambda$. We can do this by evaluating above expression at $(x_i, y_i) = A_i$. More precisely, let $Q$ be a place of $\widetilde{E}$ lying above $P = (z = \mu)$. Then we have $x_i(Q) = x(A_i)$, $y_i(Q) = y(A_i)$ and $z(Q) = z(P) = \mu$. Hence

$$\begin{aligned} &L\Big(N_{E/\mathbb{F}_q(z)}(D(x,y))\Big)(P) \\ &\quad = \sum_{i=0}^{2} \frac{\big(a'(x(A_i)) - \frac{3x(A_i)^2+A}{2y(A_i)} b(x(A_i)) - y(A_i) b'(x(A_i))\big)}{D(x(A_i),y(A_i))} \cdot \frac{2y(A_i)}{3x(A_i)^2 + A - \lambda \cdot 2y(A_i)}. \end{aligned}$$

# 5 Conclusion

We have recovered the expression for the logarithmic derivative of the norm and its evaluation in terms of points on the pullback as given by [3]. As mentioned in the Background Section above, the slightly different probability distribution in the choice of randomness causes some additional difficulties for the soundness argument. However the soundness proof given in [1] for the interactive protocol verifying Equation (1) can be adapted to this case as well. In particular, one obtains bounds on the soundness error by considering the surface $E \times E$ and using results [2, 5] on the number of rational points of projective varieties in terms of their degree. This would correspond to the Schwartz-Zippel Lemma in this more general context.

# 6 An Implicit Assumption and a Potential Vulnerability

Our aim is to obtain an argument for

$$n_1 \cdot P_1 + \cdots + n_k \cdot P_k = \infty. \tag{7}$$

Note that here the coefficients (multiplicities) $n_i$ are integers. The above process reduces this to a claim about

$$\sum_{i=1}^{k} \frac{n_i}{z - z(P_i)}, \tag{8}$$

namely that it is equal to

$$\delta_z\big(N_{E/\mathbb{F}_q(z)}(D(x,y))\big),$$

see Equation (1). Note that in the original Equation (7) the $n_i$ were integers, whereas in expression (8) they are elements of the finite field $\mathbb{F}_p$. Hence there is a loss of information. This is caused by the use of logarithmic derivatives, which turns integer exponents into coefficients in the finite field. Hence we have to be cautious.

Above we have assumed that both sides of Equation (1) have degree smaller than $p$. We used the fact that the logarithmic derivative is a homomorphism from $F^\times$ to $F$ to conclude that if the logarithmic derivatives of both sides agree, then they differ by at most a nonzero multiplicative constant. This was sufficient for us, as multiplying a function by a nonzero constant does not change its divisor. If the condition about the degrees does not hold, the two sides might differ by $t = u^p$, the $p$-th power of a non-constant element $u \in F$, but still have equal logarithmic derivatives.

The left hand side of Equation (1) is a polynomial, and in the argument the prover commits to its coefficients. Hence the degree is under control and cannot be very large. As $p$ is classically very large, committing to the coefficients of this polynomial would even not be possible if its degree would be larger than $p$.

The right hand side however consists of $k$ points with multiplicities $n_1, \ldots, n_k$. In the protocol the points are fixed (either their are public or they are committed to), hence multiplication by a $p$-th power will necessarily correspond only to changing the multiplicities in a restricted way: suppose

$$\prod_{i=1}^{k} (z - z(P_i))^{n_i} = \prod_{i=1}^{k} (z - z(P_i))^{m_i} \cdot u^p.$$

Here we can assume with high probability that the $z(P_i)$ are distinct. Then we have

$$n_i \equiv m_i \pmod{p}, \text{ for } i = 1, \ldots, k.$$

So a proof that

$$n_1 \cdot P_1 + \cdots + n_k \cdot P_k = \infty$$

will necessarily also provide an argument that

$$m_1 \cdot P_1 + \cdots + m_k \cdot P_k = \infty,$$

as the logarithmic derivatives of the expression on the right hand side of Equation (1) agree in this case. This is the only ambiguity that can arise.

Hence we implicitly make the assumption that $0 \leq n_i < p$ for $i = 1, \ldots, k$. No additional constraints need to be added, but the user of the argument for sums of points has to be aware of this implicit assumption, which is easy to miss in applications. A particular danger is to use the argument to prove that a divisor with negative coefficients sums to zero. Given a valid proof for $\sum n_i \cdot P_i = \infty$ with $0 \leq n_i < p$, a malicious prover can replace some of the coefficients $n_i$ by the corresponding negative numbers $-(p - n_i)$ (congruent modulo $p$ to $n_i$) and obtain an argument which the verifier will accept.

# References

[1] Bassa, A., *Soundness Proof for Eagen's Proof of Sums of Points*, Veridise Technical Report.

[2] Dvir, Zeev; Kollár, János; Lovett, Shachar, *Variety evasive sets*, Comput. Complexity 23, No. 4, 509-529 (2014).

[3] Eagen, Liam, *Zero Knowledge Proofs of Elliptic Curve Inner Products from Principal Divisors and Weil Reciprocity*, Cryptology ePrint Archive, Paper 2022/596, `https://eprint.iacr.org/2022/596`.

[4] Eagen, Liam; Kanjalkar, Sanket; Ruffing, Tim; Nick, Jonas, *Bulletproofs++: Next Generation Confidential Transactions via Reciprocal Set Membership Arguments*, Advances in Cryptology – EUROCRYPT 2024, Lecture Notes in Computer Science, vol 14655, Springer Verlag.

[5] Ellenberg, Jordan S.; Oberlin, Richard; Tao, Terence, *The Kakeya set and maximal conjectures for algebraic varieties over finite fields*, Mathematika 56, No. 1, 1-25 (2010).

[6] Haböck, Ulrich, *Multivariate lookups based on logarithmic derivatives*, Cryptology ePrint Archive, Paper 2022/1530, `https://eprint.iacr.org/2022/1530`.

[7] Lang, Serge, *Algebra*, 3rd ed., Graduate Texts in Mathematics 211, Springer Verlag, 2002.

[8] Schwartz, Jacob T., *Fast probabilistic algorithms for verification of polynomial identities*, J. ACM, 27(4):701–717, 1980.

[9] Silverman, Joseph H., *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics 106, Springer Verlag, 2009.

[10] Stichtenoth, Henning, *Algebraic function fields and codes*, 2nd ed., Graduate Texts in Mathematics 254, Springer Verlag, 2009.

[11] Zippel, Richard, *Probabilistic algorithms for sparse polynomials*, in Edward W. Ng, editor, EUROSAM, volume 72 of Lecture Notes in Computer Science, pages 216–226. Springer, 1979.