Soundness Proof for Eagen's Proof of Sums of Points

Alp Bassa

Veridise

1 Introduction

In this note we provide a soundness proof for the proof of sums of points proposed by Eagen in [2, Section 3]. Given an elliptic curve E, the aim is to prove that a given set of rational points $P_1, P_2, \ldots, P_N \in E(\mathbb{F}_q)$ sum to zero

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

This is reduced to proving a claim about the existence of regular functions of the affine part of the curve having zeros at the specified points. This reduction is explained in Section 2. It remains to provide a proof that the given function (which is committed to by the prover) has zeros at the specified points. In a first attempt the points and function are projected to a random line chosen by the verifier and the question is reduced to one of vanishing of a univariate polynomial (corresponding to the norm) at the projection points. This can now be established using the Schwartz-Zippel Lemma by evaluating at a random point. A soundness proof for this arguments (with a random choice of line) is given in Theorem 3.

Rather than evaluating the norm of the function at a random coordinate of the randomly chosen line, one can evaluate the initial function at the intersection points of the line with the elliptic curve (this follows from basic properties of the pullback and pushforward of divisors and functions). For ease of computation Eagen suggests restricting the sample space to lines where these points will be rational. This results in a new distribution of the lines. In this case the reduction to a question about points on the projected line is more elaborate, but goes through (see Section 4, Theorem 6). The final Schwarz-Zippel argument however becomes problematic. In particular a finer understanding of the splitting behavior of rational places in random subfields seems to be required. This issue is explained in Section 4 and seems also to be present in the proof alluded to in [2].

To overcome this problem we take a different approach in Section 5. We recast the problem as a problem about the equality of two degree $2N$ functions on the surface $E \times E$. The Schwartz-Zippel argument is now done by evaluating at a random rational points of the surface. To conclude soundness, we use a bound on the number of rational points of projective varieties in terms of their degree given in [1, 3], which corresponds to the Schwartz-Zippel Lemma in this more general context. The corresponding soundness result is given in Theorem 10.

The functions can be replaced by their logarithmic derivative. Doing this for the norm function is a bit subtle, but can be explained easily using the theory of derivations on function fields. This is done in Section 6.

Finally, in Section 7 we describe an alternative approach combining the intuitive idea of projecting to random lines and the evaluation of the norm already using coordinates on the

elliptic curve, without rationality restrictions. This uses basic properties of univariate polynomial resultants.

For details about facts and notions about elliptic curves and algebraic function fields we refer to [5] and [6].

2 Problem Statement

Let E be an elliptic curve in short Weierstrass form over the finite field $\mathbb{F}_q$ given by the equation

$$y^2 = x^3 + a \cdot x + b.$$

We will denote the function field by $\mathbb{F}_q(E)$. Denote by $\mathcal{O}$ the point at infinity. Given rational points $P_1, P_2, \ldots, P_N \in E(\mathbb{F}_q)$ with $P_1 + P_2 + \cdots + P_N = \mathcal{O}$, we want to provide an interactive proof of this fact. For this we will prove the existence of a "witness function" D on the elliptic curve having pole of order N at $\mathcal{O}$ and zeros exactly at the P_i. More precisely, we will use the following characterization of principal divisors of E:

Theorem 1 ([5] Corollary 3.5)**.** *Let E be an elliptic curve and let $D = \sum n_P \cdot P \in \mathrm{Div}(E)$. Then D is a principal divisor if and only if*

$$\sum_{P \in E} n_P = 0 \qquad \textit{and} \qquad \sum_{P \in E} [n_P]P = \mathcal{O}.$$

Clearly, $P_1 + P_2 + \cdots + P_N = \mathcal{O}$ if and only if $P_1 + P_2 + \cdots + P_N - [N] \cdot \mathcal{O} = \mathcal{O}$. Now as the divisor $P_1 + P_2 + \cdots + P_N - N \cdot \mathcal{O}$ has degree 0, this is equivalent to it being principal, by Theorem 1. Hence there exists a function D on E having zeros exactly at the P_i and pole of order N at $\mathcal{O}$. Functions having poles only at $\mathcal{O}$ form the coordinate ring of the affine curve E, which is given by

$$\mathbb{F}_q[E] = \mathbb{F}_q[x, y]/\langle y^2 - (x^3 + A \cdot x + b)\rangle.$$

Its elements can be represented by $D = a(x) - y \cdot b(x)$ with $a(x), b(x) \in \mathbb{F}_q[x]$. As x and y have a pole at $\mathcal{O}$ of order 2 and 3 respectively, we have

$$v_{\mathcal{O}}(D) = v_{\mathcal{O}}(a(x) - y \cdot b(x)) = \max\{2 \cdot \deg a(x), 3 + 2 \deg b(x)\} = N.$$

We have reduced the problem to proving that there exists a function $D \in \mathbb{F}_q(E)$ having zeros exactly at the rational points $P_1, P_2, \ldots, P_N \in E(\mathbb{F}_q)$ and pole at $\mathcal{O}$, i.e.,

$$(D) = P_1 + P_2 + \ldots + P_N - N \cdot \mathcal{O}.$$

The points P_i and the witness function D are fixed before the interaction.

3 A First Attempt

Next, rather than verifying that D vanishes at all the P_i, the protocol proceeds as follows: the verifier chooses a random subfield $\mathbb{F}_q(z)$ of $\mathbb{F}_q(E)$ with $[\mathbb{F}_q(E) : \mathbb{F}_q(z)] = 3$ (in fact the verifier chooses a random $\lambda \in \mathbb{F}_q$ and defines $z = y - \lambda \cdot x$) and checks that $N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D)$ vanishes at $z(P_1), \ldots, z(P_N)$, where $N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(\cdot)$ denotes the field norm for the extension $\mathbb{F}_q(E)/\mathbb{F}_q(z)$. Note that this is a necessary, but not sufficient condition for D to vanish at the P_i.

Note that if D does not vanish at some of the P_i, then $N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D)$ does not vanish at $z(P_i)$ with high probability over the random choice of z:

Theorem 2. *Suppose D vanishes at $Q_1, \ldots, Q_N$ and suppose $P \neq Q_i$ for $i = 1, \ldots, N$. Then the probability that $N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D)(z(P)) = 0$ is at most N/q.*

Proof. As $P \neq Q_i$, we have $x(P) \neq x(Q_i)$ or $y(P) \neq y(Q_i)$. Choosing a random $\lambda \in \mathbb{F}_q$ and letting $z = y - \lambda \cdot x$, the function $N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D)$ has zeros exactly at $z(Q_i) = y(Q_i) - \lambda \cdot x(Q_i)$ for $i = 1, \ldots, N$. We want to estimate the probability that $y(Q_i) - \lambda \cdot x(Q_i) = y(P) - \lambda \cdot x(P)$ for some $i = 1, \ldots, N$. If for some i we have $x(Q_i) = x(P)$, then the above equality cannot hold for any choice of λ, as it would imply $y(Q_i) = y(P)$. For all other i, we need to have

$$\frac{y(P) - y(Q_i)}{x(P) - x(Q_i)} = \lambda$$

for the equality to hold. As there are at most N different possible values for the left hand side, only at most N of the q possible choices for λ will lead to an equality. So the probability is at most N/q. □

Note that the points Q_i are determined by the witness function D. They are exactly the zeroes of D, repeated according to the multiplicity. P is an arbitrary point. We will choose it as one of the committed points P_i later on.

Rather than verifying that the norm vanishes on the $z(P_i)$, i.e., is equal to $\prod_{i=1}^{N} c(z - z(P_i))$ the verifier chooses a random $\mu \in \mathbb{F}_q$ and evaluates both the above product and the norm at μ. By the Schwartz-Zippel Lemma, if the norm and the product do not agree, then their value at μ will be equal with probability at most N/q.

Throughout we will assume that D is monic. More precisely, D will be a polynomial in x and y. The coefficient of the highest degree monomial, where the degree is calculates with weights $\deg(x) = 2$ and $\deg(y) = 3$, is assumed to be 1. Hence the constant c in the factorization of $N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D)$ above is 1. Note that the proof of soundness does hold also for non-monic D. However an honest prover will not be able to provide a convincing proof unless a monic witness function is chosen, because of the form of the right hand side.

Combining this with Theorem 2 we obtain:

Theorem 3. *Given a an element $D \in \mathbb{F}_q[E]$ with leading coefficient 1 and $v_{\mathcal{O}}(D) = N$ and $P_1, \ldots, P_N \in E(\mathbb{F}_q)$. Suppose that $(D)_0 \neq P_1 + \cdots + P_N$. Choose random $\lambda, \mu \in \mathbb{F}_q$. Let $z = y - \lambda \cdot x$. Then the probability that*

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

is at most $2N/q$.

Proof. As $D \in \mathbb{F}_q[E]$ and $v_{\mathcal{O}}(D) = N$, the function D vanishes at N points $Q_1, \ldots, Q_N$. If $(D)_0 \neq P_1 + \cdots + P_N$, then for some $P \in \{P_1, \ldots, P_N\}$ the function D does not vanish at P, i.e. $P \neq Q_i$ for $i = 1, \ldots, N$. In this case by Theorem 2 we will have

$$N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D) = \prod_{i=1}^{N}(z - z(P_i)) \tag{2}$$

with probability at most N/q, and the evaluations at all μ will agree. However with probability at least $1 - N/q$ the polynomials in Equation (2) will be distinct of degree N. Hence their value at the randomly chosen μ will be equal with probability at most N/q. Hence the probability that Equation (1) holds is at most $N/q + (1 - N/q)(N/q) < 2N/q$. □

4 A new sample space

The protocol described in [2] does not utilize a random choice of $\lambda, \mu \in \mathbb{F}_q$ pair, but a random choice of rational points $A_0, A_1 \in E(\mathbb{F}_q)$. The reason for this is to ease the computation of the left hand side of Equation (1). Rather than evaluating the norm of D at the point $z = \mu$, one can compute the expression already on the elliptic curve E.

The extension $\mathbb{F}_q(E)/\mathbb{F}_q(z)$ corresponds to a covering of curves $\phi : E \to \mathbb{P}^1$. In the notation of [5] we have the inclusion $\phi^* : \mathbb{F}_q(z) \to \mathbb{F}_q(E)$ and the norm map $\phi_* = N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)} : \mathbb{F}_q(E) \to \mathbb{F}_q(z)$. We have corresponding maps on the group of divisors of E and $\mathbb{P}^1$:

$$\phi^* : \mathrm{Div}(\mathbb{P}^1) \to \mathrm{Div}(E) \quad \text{and} \quad \phi_* : \mathrm{Div}(E) \to \mathrm{Div}(\mathbb{P}^1)$$

which are defined on points by

$$\phi^*(Q) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P) \cdot P \quad \text{and} \quad \phi_*(P) = \phi(P),$$

and extended to divisors linearly. Here $e_\phi(P)$ denotes the ramification index of P in the covering given by ϕ. For basic properties of ϕ^* and ϕ_* see [5, Section II.3]. For a nonzero rational function f and a divisor $\sum n_P \cdot P$ (with f having neither pole nor zero on points in the support of the divisor) we define

$$f\left(\sum n_P \cdot P\right) = \prod_P f(P)^{n_P}.$$

By [5, Exercise 2.10 (a)] we have for the rational function D on E and the divisor Q of $\mathbb{P}^1$, where Q is the point $(z = \mu)$ on $\mathbb{P}^1$, the equality $D(\phi^*(Q)) = (\phi_*(D))(Q)$. In particular

$$\prod_{P \in f^{-1}(\mu)} D(P)^{e_\phi(P)} = N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D)(\mu). \tag{3}$$

Hence the left hand side of Equation (1) can be computed by evaluating the function D on E at the points of E mapping to the point $Q = (z = \mu)$. The points on E mapping to $Q = (z = \mu)$ might however not all be rational, which would cause problems with their representation. Hence it is useful to restrict the choice of μ to elements in $\mathbb{F}_q$ such that there are exactly three points $A_0, A_1, A_2 \in E$ mapping to the point $(z = \mu)$, and all are rational (they are in $E(\mathbb{F}_q)$). So the place Q splits in the extension $\mathbb{F}_q(E)/\mathbb{F}_q(z)$. The points A_0, A_1, A_2 have z coordinate μ. Using Equation (3), we can rewrite Equation (1) as

$$D(A_0) \cdot D(A_1) \cdot D(A_2) = \prod_{i=1}^{N} (\mu - z(P_i)) \tag{4}$$

As $z = y - \lambda \cdot x$ the points A_0, A_1, A_2 lie on the line $y = \lambda \cdot x + \mu$, so $A_0 + A_1 + A_2 = \mathcal{O}$. Hence a random choice of A_0 and A_1 from $E(\mathbb{F}_q)$ uniquely determines A_2, which will also be a rational point. Moreover, the points A_0, A_1 uniquely determine the line $L = y - \lambda \cdot x - \mu$ (if they are distinct, it is the line through A_0 and A_1, otherwise it is the line tangent to E at $A_0 = A_1$). Hence they also determine λ and μ. So rather than choosing a random λ and subsequently a suitable (i.e., splitting) random μ, we can directly randomly choose A_0, A_1 from $\mathbb{F}_q(E)$.

Randomly choosing A_0 and A_1 from $E(\mathbb{F}_q)$ rather than λ, μ from $\mathbb{F}_q$ changes the sample space and the probability distribution, but does not result in an essential change in the estimations above. In particular, the distribution of the slopes λ of the resulting chord line need not be uniform with each slope having probability $1/q$, but we can obtain good estimates:

Lemma 4. *Randomly choose affine rational points $A_0, A_1 \in E(\mathbb{F}_q)\backslash\mathcal{O}$. For a given $\lambda \in \mathbb{F}_q$ the probability that the the line through A_0 and A_1 has slope λ is at most $2/(\#E(\mathbb{F}_q) - 2)$.*

Proof. Consider all q lines of slope λ. Each of the $\#E(\mathbb{F}_q) - 1$ affine rational points has to be on one of them. Out of these lines, there will be

(i) N_0 many where not all three intersection points with E are rational (at most one is rational),

(ii) N_1 many lines intersecting E at a rational point with multiplicity 3 (this point is a 3-torsion point),

(iii) N_2 many lines intersecting E at two rational points, being tangent to one of them,

(iv) N_3 many lines intersecting E at three rational points.

We have $N_1 + 2 \cdot N_2 + 3 \cdot N_3 \leq \#E(\mathbb{F}_q) - 1$. Considering points with multiplicities, each line in case (i),(ii),(iii) and (iv) has 0, 1, 2 and 3 pairs of rational points, respectively. So for a line in case (i),(ii),(iii) and (iv), for a random choice of $A_0, A_1 \in E(\mathbb{F}_q)\backslash\mathcal{O}$, the line through them (the line tangent to the elliptic curve at the point in case $A_0 = A_1$) will be equal to this line with probability

$$0, \frac{1}{(\#E(\mathbb{F}_q) - 1)^2/2}, \frac{2}{(\#E(\mathbb{F}_q) - 1)^2/2} \text{ and } \frac{3}{(\#E(\mathbb{F}_q) - 1)^2/2}$$

respectively.

Hence for a random choice of $A_0, A_1 \in E(\mathbb{F}_q)\backslash\mathcal{O}$ the probability of them defining a line of slope λ is given by

$$N_1 \frac{1}{(\#E(\mathbb{F}_q) - 1)^2/2} + N_2 \frac{2}{(\#E(\mathbb{F}_q) - 1)^2/2} + N_3 \frac{3}{(\#E(\mathbb{F}_q) - 1)^2/2}$$

$$= \frac{N_1 + 2 \cdot N_2 + 3 \cdot N_3}{(\#E(\mathbb{F}_q) - 1)^2/2} \leq \frac{2}{\#E(\mathbb{F}_q) - 1}$$

□

One potential issue might be that for a random choice of A_0 and A_1 the support of (D) might not be disjoint from $\{A_0, A_1, A_2\}$, the support of $\phi^*(z = \mu)$ for the resulting z and μ. One can adapt the reasoning above to these cases as well. As the resulting implementation would be more cumbersome, it is better to avoid these cases. One way is to just assume this does not happen as the corresponding probability is negligible:

Lemma 5. *The probability that the support for D is not disjoint from $\{A_0, A_1, A_2\}$ is at most $3(N + 1)/\#E(\mathbb{F}_q)$ and hence negligible.*

Proof. D has N zeros and one pole at $\mathcal{O}$.

For one of the A_i to be a pole of D, either A_0 or A_1 have to be $\mathcal{O}$, or we need to have $A_0 + A_1 = \mathcal{O}$, i.e., $A_1 = -A_0$. Each of these three events cases occur with probability $1\ \#E(\mathbb{F}_q)$.

For one of the A_i to be a zero of D: as the points of $E(\mathbb{F}_q)$ form a group and A_0 and A_1 are chosen uniformly random from $E(\mathbb{F}_q)$, the point $A_2 = -A_0 - A_1$ will also follow a uniformly random distribution. Hence for each of them the probability of being a zero of D is given by the probability of being equal to one of the N zeros of D, which is at most $N/\#E(\mathbb{F}_q)$.

The result follows from the union bound. □

Alternatively, the verifier can just sample A_0, A_1 from the set $E(\mathbb{F}_q)\backslash\{\mathcal{O}\}$, compute $A_2 = -A_0 - A_1$ and check that $x(A_0) \neq x(A_1)$ and $D(A_i) \neq 0$ for $i = 0, 1, 2$, resampling if necessary. Hence we can assume that the support of D and L are disjoint.

Adapting Theorem 2 we get

Theorem 6. *Suppose D vanishes at $Q_1, \ldots, Q_N$ and suppose $P \neq Q_i$ for $i = 1, \ldots, N$. Choose random $A_0, A_1 \in E(\mathbb{F}_q)\backslash\mathcal{O}$ with $A_0 \neq -A_1$ and consider the line L defined by them. Then the probability that $N_{\mathbb{F}_q(E)/\mathbb{F}_q(L)}(D)(L(P)) = 0$ is at most $2N/(\#E(\mathbb{F}_q) - 1)$.*

Proof. The random choice of A_0, A_1 will define a line L that is not vertical, as $A_0, A_1 \neq \mathcal{O}$ and $A_0 \neq A_1$. Hence we will have $L = y - \lambda \cdot x - \mu$ for some $\lambda, \mu \in \mathbb{F}_q$. The function $N_{\mathbb{F}_q(E)/\mathbb{F}_q(L)}(D)$ has zeros exactly at $L(Q_i) = y(Q_i) - \lambda \cdot x(Q_i) - \mu$ for $i = 1, \ldots, N$. We want to estimate the probability that $y(Q_i) - \lambda \cdot x(Q_i) - \mu = y(P) - \lambda \cdot x(P) - \mu$ for some $i = 1, \ldots, N$. If for some i we have $x(Q_i) = x(P)$, then the above equality cannot hold for any choice of λ, as it would imply $y(Q_i) = y(P)$. For all other i, we need to have

$$\frac{y(P) - y(Q_i)}{x(P) - x(Q_i)} = \lambda$$

for the equality to hold. As there are at most N different possible values for the left hand side, and by Lemma 4 each of them occurs as the slope of the line L with probability at most $2/(\#E(\mathbb{F}_q) - 2)$, the probability that one of them is the slope of the line defined by the random choice of A_0, A_1 is at most $2N/(\#E(\mathbb{F}_q) - 1)$. □

If we try to mimic Theorem 3, we run into problems. A random choice of A_0, A_1 determines the line $L = y - \lambda \cdot x - \mu$. Letting $z = y - \lambda \cdot x$, we obtain a subfield $\mathbb{F}_q(z)$ and we can consider the norm $N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D)$ of the function D, which is supposed to equal $\prod_{i=1}^{N}(z - z(P_i))$. We know that these two polynomials agree at the point μ. The problem is however that we do not know what other potential value we might have substituted for z, i.e., we do not know from which the set the random evaluation point in the Schwartz-Zippel Lemma is drawn. The corresponds to all possible η values such that the line $y - \lambda \cdot x - \eta$ intersects E in 3 rational points. In other words the place $(z = \eta)$ splits in the extension $\mathbb{F}_q(E)/\mathbb{F}_q(z)$. However the this number depends on the choice of λ and it is difficult to give a lower bound for the number of splitting places independent of λ. Note that in the previous distribution we could choose all values for μ, as we did not have any splitting condition. Tchebotarev Theorem kind of results will only give asymptotic guarantees: we would expect on average a proportion of $1/6$ of the rational points to split, as the Galois group will be in general the group S_3 of order 6. For a fixed elliptic curve E one could count for each λ the number of split places in $\mathbb{F}_q(E)/\mathbb{F}_q(z)$ and obtain explicit bounds.

The idea of first determining the subfield $\mathbb{F}_q(z)$ and then the place $(z = \mu)$ seems difficult (the number of possibilities for μ depend on λ and is difficult to estimate). The idea of reducing the problem to a case where the univariate Schwartz-Zippel Lemma is applicable might not be the easiest one. The right approach to be to taken is to consider the set of all possible (λ, μ) pairs (these are pairs so that the place $L = 0$ splits in $\mathbb{F}_q(E)/\mathbb{F}_q(L)$ where $L = y - \lambda \cdot x - \mu$) simultaneously. For this one has to pass to algebraic surfaces.

5 Soundness Proof Using the Algebraic Surface $E \times E$

For a random choice of $A_0, A_1 \in E(\mathbb{F}_q)\backslash\mathcal{O}$ the probability that $A_0 = \pm A_1$ is $2/(\#E(\mathbb{F}_q) - 1)$, and hence negligible. For simplicity, we will hence assume that $A_0 \neq \pm A_1$. So we do not need to consider tangents $(A_0 \neq A_1)$ and the resulting line L is not vertical $(A_0 \neq -A_1)$.

We consider the surface $E \times E$. The pair (A_0, A_1) of points from $E(\mathbb{F}_q)$ can be seen as a rational point in $(E \times E)(\mathbb{F}_q)$. Let $A_0 = (x_0, y_0)$, $A_1 = (x_1, y_1)$ and let $L = y - \lambda x - \mu$ be the line determined by A_0 and A_1. Suppose $(D)_0 = \sum_{i=1}^{N} Q_i$. As the leading coefficient of D is assumed to be 1, for any choice of A_0, A_1 we have

$$D(A_0) \cdot D(A_1) \cdot D(A_2) = N_{\mathbb{F}_q(E)/\mathbb{F}_q(L)}(D)\Big|_{L=0} = \prod_{i=1}^{N} -(y(Q_i) - \lambda \cdot x(Q_i) - \mu).$$

We have to show that if $\{P_i\} \neq \{Q_i\}$, then with high probability over the choice of A_0, A_1 we have

$$\prod_{i=1}^{N} -(y(Q_i) - \lambda \cdot x(Q_i) - \mu) \neq \prod_{i=1}^{N} -(y(P_i) - \lambda \cdot x(P_i) - \mu)$$

and hence

$$D(A_0) \cdot D(A_1) \cdot D(A_2) \neq \prod_{i=1}^{N} -(y(P_i) - \lambda \cdot x(P_i) - \mu). \tag{5}$$

As $\{P_i\}, \{Q_i\}$ are fixed, $\prod_{i=1}^{N}(y(Q_i) - \lambda \cdot x(Q_i) - \mu) - \prod_{i=1}^{N}(y(P_i) - \lambda \cdot x(P_i) - \mu)$ is a function of λ and μ, which in turn are functions of A_0 and A_1. We have $\lambda = \frac{y_1 - y_0}{x_1 - x_0}$ and $\mu = y_0 - \frac{y_1 - y_0}{x_1 - x_0} x_0$. We want to show that with high probability over the choice of (A_0, A_1),we have

$$\prod_{i=1}^{N}(y(Q_i) - \lambda \cdot x(Q_i) - \mu) - \prod_{i=1}^{N}(y(P_i) - \lambda \cdot x(P_i) - \mu) \neq 0,$$

or equivalently, by interpreting this as a function of x_0, y_0, x_1, y_1 and multiplying by $(x_1 - x_0)^N$ we obtain

$$f(x_0, y_0, x_1, y_1) = \prod_{i=1}^{N}((y(Q_i) - y_0)(x_1 - x_0) - (x(Q_i) - x_0)(y_1 - y_0)) - \prod_{i=1}^{N}((y(P_i) - y_0)(x_1 - x_0) - (x(P_i) - x_0)(y_1 - y_0)) \neq 0.$$

Here $\{P_i\}$ are committed to and $\{Q_i\}$ are determined by D, which is also committed to. Hence $x(P_i), y(P_i), x(Q_i), y(Q_i)$ are fixed elements. Hence we can consider the function

$$f(X_0, Y_0, X_1, Y_1) = \prod_{i=1}^{N}((y(Q_i) - Y_0)(X_1 - X_0) - (x(Q_i) - X_0)(Y_1 - Y_0)) - \prod_{i=1}^{N}((y(P_i) - Y_0)(X_1 - X_0) - (x(P_i) - X_0)(Y_1 - Y_0)).$$

as a function on $E \times E$.

Note that the points $\{P_i\}$ are known and easily verified to be defined over $\mathbb{F}_q$. The points $\{Q_i\}$ however are implicitly given. They are determined as zeros of $D \in \mathbb{F}_q$, but are not necessarily defined over $\mathbb{F}_q$. Hence it is a priori not clear that $f(X_0, Y_0, X_1, Y_1)$ is defined over $\mathbb{F}_q$. This is proven in the following lemma:

Lemma 7. $f(X_0, Y_0, X_1, Y_1) \in \mathbb{F}_q[X_0, Y_0, X_1, Y_1]$.

Proof. As the points P_i are rational, $x(P_i), y(P_i) \in \mathbb{F}_q$. Hence the second product in the definition of f is defined over F_q. The Q_i are zeros of D, which is defined over $\mathbb{F}_q$. So the Q_i come as full Galois orbits. Hence for the first product in the definition of f for each quadratic factor $(y(Q_i) - Y_0)(X_1 - X_0) - (x(Q_i) - X_0)(Y_1 - Y_0)$ all of its Galois conjugates occur as factors in the product as well. Hence the first product is also defined over $\mathbb{F}_q$. □

We want to show that the probability of f vanishing at a random point $(A_0, A_1) \in (E \times E)(\mathbb{F}_q)$ is negligible. This is done by bounding the total number of rational zeros of f on $E \times E$ and showing that it is small compared to $\#(E \times E)(\mathbb{F}_q)$.

The surface $E \times E$, as a product of irreducible degree 3 curves is irreducible and has degree $3 \cdot 3 = 9$. Intersecting it with $f(X_0, Y_0, X_1, Y_1) = 0$ of degree $2N$ we get a curve of degree $2N \cdot 9 = 18N$. To be precise, we have to show that $f(X_0, Y_0, X_1, Y_1)$ does not vanish on $E \times E$:

Lemma 8. *Assume $\sum Q_i \neq \sum P_i$ and $N \ll q$. Then $f(X_0, Y_0, X_1, Y_1)$ does not vanish on $E \times E$*

Proof. As $E \times E$ is irreducible, it suffices to show that non of the factors of f vanishes on all of $E \times E$. As $\sum Q_i \neq \sum P_i$, by reordering the points, we can assume without loss of generality that the divisors differ in their coefficient of $P = P_1 = Q_1$, i.e. $v_P(\sum Q_i) \neq v_P \sum P_i$). Moreover, without loss of generality we may assume that the coefficient in $\sum P_i$ is larger than the coefficient in $\sum Q_i$ (exchanging the roles if necessary). We can a suitable power of the quadratic factor

$$((y(P_i) - Y_0)(X_1 - X_0) - (x(P_i) - X_0)(Y_1 - Y_0)),$$

which will not vanish on $E \times E$ as it is quadratic. So we may assume without loss of generality that P_1 is not in the support of the divisor $\sum Q_i$. Subsitute in $x_0 = x(P_1)$ and $y_0 = y(P_1)$ in $f(X_0, Y_0, X_1, Y_1)$.The second product will be zero. We obtain

$$f(x(P_1), y(P_1), X_1, Y_1) = \prod_{i=1}^{N}((y(Q_i) - y(P_1))(X_1 - x(P_1)) - (x(Q_i) - x(P_1))(Y_1 - y(P_1))).$$

As P_1 is not in the support of the divisor $\sum Q_i$, for each i either $y(Q_i) \neq y(P_1)$ or $x(Q_i) \neq x(P_1)$. So all factors are linear and nonzero. Hence the zero set is a union of at most N lines, each containing at most 3 points of the elliptic curve. As $N \ll q$ by the Hasse–Weil bound $3N < \#E(\mathbb{F}_q)$ and hence $f(x(P_1), y(P_1), X_1, Y_1)$ cannot vanish on all of $E(\mathbb{F}_q) \times \{(x(P_1), y(P_1))\}$. □

We can bound the number of rational points on the curve cut out by $f(x_0, x_1, x_2, x_3)$ from the surface $E \times E$ using the following generalization of the Schwartz-Zippel Lemma:

Theorem 9 ([1, Claim 7.2], [3, Lemma A.3])**.** *Let V be a projective variety of dimension n and degree d. Then*

$$\#V(\mathbb{F}_q) \leq d \cdot q^n.$$

In particular, we obtain for the degree $18N$ curve obtained by intersecting the surface $E \times E$ with the hypersurface $\{f = 0\}$

$$\#\{(A_0, A_1) \in E(\mathbb{F}_q) | f(A_0, A_1) = 0\} \leq 18Nq. \tag{6}$$

Consequently, we obtain the following soundness result:

Theorem 10. *Given a an element $D \in \mathbb{F}_q[E]$ with leading coefficient 1 and $v_{\mathcal{O}}(D) = N$ and $P_1, \ldots, P_N \in E(\mathbb{F}_q)$. Suppose that $(D)_0 \neq P_1 + \cdots + P_N$. Choose random $A_0, A_1 \in E(\mathbb{F}_q)\backslash\mathcal{O}$, with $A_0 \neq \pm A_1$. Let $L = y - \lambda \cdot x - \mu$ be the line defined by A_0, A_1. Then the probability that*

$$N_{\mathbb{F}_q(E)/\mathbb{F}_q(L)}(D)(0) = \prod_{i=1}^{N}(-L(P_i)) \tag{7}$$

is at most $18Nq/\big((\#E(\mathbb{F}_q)-1)^2 - 2(\#E(\mathbb{F}_q)-1)\big) \approx 18N/q$.

Proof. For a random choice of A_0, A_1, equality holds in Equation (7) exactly when $f(A_0, A_1) = 0$. The number of zeros of f on $E \times E$ is bounded by $18Nq$ by (6). As the number of $A_0, A_1 \in E(\mathbb{F}_q)\backslash\mathcal{O}$ pairs with $A_0 \neq \pm A_1$ is given by $(\#E(\mathbb{F}_q)-1)^2 - 2(\#E(\mathbb{F}_q)-1)$, the results follows. By the Hasse bound, we know that $E(\mathbb{F}_q)$ is at the order of q. Hence we get the estimation $18N/q$ for the soundness error. □

Note that assuming a monic or even nonzero function witness is not necessary for soundness. Clearly if the function D is zero, it cannot be a valid witness for the points $P_1, \ldots, P_n$ summing to zero. Moreover, as the polynomial on the right hand side is chosen to be monic, unless a monic witness function (or a witness function whose norm as a polynomial in the corresponding variable is monic) is chosen, the prover will not be able to provide a convincing proof. Hence normalization is required for completeness, but it is not necessary for the soundness argument. We have the following theorem:

Theorem 11. *Given a an element $D \in \mathbb{F}_q[E]$ and points $P_1, \ldots, P_{N_1} \in E(\mathbb{F}_q)$. Choose random $A_0, A_1 \in E(\mathbb{F}_q)\backslash\mathcal{O}$, with $A_0 \neq \pm A_1$. Let $L = y - \lambda \cdot x - \mu$ be the line defined by A_0, A_1. For the random choice of A_0, A_1 denote by $\mathcal{P}$ the probability that*

$$N_{\mathbb{F}_q(E)/\mathbb{F}_q(L)}(D)(0) = \prod_{i=1}^{N}(-L(P_i)). \tag{8}$$

In the following cases $\mathcal{P}$ is negligible:

(i) $D = 0$ *and* $q \gg N_1$,

(ii) $D \neq 0$, $(D)_0 = \sum_{i=1}^{N_2} Q_i$, $\sum_{i=1}^{N_1} P_i \neq \sum_{i=1}^{N_2} Q_i$ *and* $q \gg \max\{N_1, N_2\}$

(iii) $D \neq 0$, $(D)_0 = \sum_{i=1}^{N_2} Q_i$, $\sum_{i=1}^{N_1} P_i = \sum_{i=1}^{N_2} Q_i$, $q \gg N_1$, *but* $\mathrm{lc}(D)^3 \neq 1$, *where* $\mathrm{lc}(D)$ *denotes the leading coefficient of* D.

Proof. (i) If $D = 0$, then

$$D(A_0) \cdot D(A_1) \cdot D(A_2) = N_{\mathbb{F}_q(E)/\mathbb{F}_q(L)}(D)\Big|_{L=0} = 0.$$

We consider the function

$$f(X_0, Y_0, X_1, Y_1) = -\prod_{i=1}^{N_1}((y(P_i) - Y_0)(X_1 - X_0) - (x(P_i) - X_0)(Y_1 - Y_0))$$

on $E \times E$. Let $(A, B) \in E(\mathbb{F}_q)\backslash\{P_1, \ldots, P_{N_1}\}$. Then $f(A, B, X_1, Y_1) = 0$ defines a union of N_1 lines, each intersecting $\{(A, B)\} \times E(\mathbb{F}_q)$ in at most 3 points. Hence f does not vanish on all of $E \times E$. Hence $\#\{(A_0, A_1) \in E(\mathbb{F}_q) | f(A_0, A_1) = 0\} \leq 18N_1 q$. By the Hasse–Weil bound the number of all (A_0, A_1) pairs is at the order of q^2. So the probability for a random (A_0, A_1) pair that $f(A_0, A_1)$ vanishes and hence the right hand side evaluates to zero is bounded by $18N_1/q$.

(ii) If $\sum_{i=1}^{N_1} P_i \neq \sum_{i=1}^{N_2} Q_i$ then

$$D(A_0) \cdot D(A_1) \cdot D(A_2) = N_{\mathbb{F}_q(E)/\mathbb{F}_q(L)}(D)\Big|_{L=0} = c \cdot \prod_{i=1}^{N_2} -(y(Q_i) - \lambda \cdot x(Q_i) - \mu).$$

We need to show that with high probability

$$c \cdot \prod_{i=1}^{N_2} -(y(Q_i) - \lambda \cdot x(Q_i) - \mu) \neq \prod_{i=1}^{N_1} -(y(P_i) - \lambda \cdot x(P_i) - \mu)$$

Let $N = \max\{N_1, N_2\}$. Expressing λ, μ in terms of A_0, A_1 and clearing denominators this reduces to showing that

$$(x_1 - x_0)^{\epsilon_1} \cdot c \cdot \prod_{i=1}^{N_2}((y(Q_i) - y_0)(x_1 - x_0) - (x(Q_i) - x_0)(y_1 - y_0)) \\ - (x_1 - x_0)^{\epsilon_2} \prod_{i=1}^{N_1}((y(P_i) - y_0)(x_1 - x_0) - (x(P_i) - x_0)(y_1 - y_0)) \neq 0.$$

Here ϵ_1 is $N - N_2$ if $N_1 > N_2$ and zero otherwise. Similarly for ϵ_2. Adopting Lemma 8 and Theorem 10 the result follows.

(iii) If the divisors $(D)_0$ and $\sum_{i=1}^{N_1} P_i$ but the leading coefficient of D does not give a monic polynomial when taking the norm, we have to show that

$$c \cdot \prod_{i=1}^{N_2} -(y(Q_i) - \lambda \cdot x(Q_i) - \mu) \neq \prod_{i=1}^{N_2} -(y(Q_i) - \lambda \cdot x(Q_i) - \mu).$$

Here $c \neq 1$. We can rewrite this as

$$(c-1) \cdot \prod_{i=1}^{N_2} -(y(Q_i) - \lambda \cdot x(Q_i) - \mu) \neq 0,$$

which reduces to case (i).

□

Note that having nonzero and normalized witness functions in only required for completeness, but not for soundness. However when implementing one has to exercise care, especially when using the version coming from logarithmic derivatives described below. An ill-conceived implementation might have unexpected vulnerabilities stemming not from the unsoundness of the scheme, but issues with the implementation itself.

6 Logarithmic Derivatives

As is done classically, one can use that equality of the polynomial is equivalent to the equality of the corresponding logarithmic derivatives (see [4, Lemma 3]). Hence one can replace the polynomial in $\mathbb{F}_q[z]$ obtained by the norm of D and the polynomial having zeros at the coordinates of the projected points by the corresponding logarithmic derivatives. Note that logarithmic derivatives of functions differing by a multiplicative constant agree, so this makes considerations

about normalization obsolete. Finding the logarithmic derivative of the norm at the random points requires a bit more care.

Consider again the equation

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

Both sides are elements of $\mathbb{F}_q(z)$. We want to find their derivation with respect to z (see [6, Definition 4.1.5]). This is immediate for the right hand side. For the left hand side, we let x', x'' and y', y'' be the conjugates over $\mathbb{F}_q(z)$ of x and y respectively. The derivation δ_z extends to the Galois closure of $\mathbb{F}_q(E)$ over $\mathbb{F}_q(z)$, i.e., to $\mathbb{F}_q(x, y, x', y', x'', y'')$. We have $N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D) = D(x, y) \cdot D(x', y') \cdot D(x'', y'')$ and hence

$$\begin{aligned}\delta_z\big(N_{\mathbb{F}_q(E)/\mathbb{F}_q(z)}(D)\big) =&\delta_z(D(x, y))D(x', y')D(x'', y'')\\ &+D(x, y)\delta_z(D(x', y'))D(x'', y'')\\ &+D(x, y)D(x', y')\delta_z(D(x'', y'')).\end{aligned}$$

Now as $z = y - \lambda \cdot x$, we have

$$1 = \delta_z(z) = \delta_z(y) - \lambda \cdot \delta_z(x) = (\delta_x(y) - \lambda)\delta_z(x).$$

Similarly $1 = (\delta_{x'}(y') - \lambda)\delta_z(x')$ and $1 = (\delta_{x''}(y'') - \lambda)\delta_z(x'')$.

As $y^2 = x^3 + Ax + B$, we obtain $2y\delta_x(y) = 3x^2 + A$ and similarly $2y'\delta_{x'}(y') = 3x'^2 + A$ and $2y''\delta_{x''}(y'') = 3x''^2 + A$.

Lastly, letting $D(x, y) = a(x) - y \cdot b(x)$, we have

$$\delta_z(D(x, y)) = \delta_x(D(x, y))\delta_z(x) = (a'(x) - y \cdot b'(x) - \delta_x(y) \cdot b(x)) \cdot \delta_z(x).$$

Similarly for the conjugates. Hence for the logarithmic derivative we obtain

$$\frac{\delta_z(D(x, y))}{D(x, y)}\delta_z(x) + \frac{\delta_z(D(x', y'))}{D(x', y')}\delta_z(x') + \frac{\delta_z(D(x'', y''))}{D(x'', y'')}\delta_z(x'') = \sum_{i=1}^{N}\frac{1}{z - z(P_i)}.$$

Evaluating at a place R of the Galois closure above the place $(z = \mu)$ and noting that $A_0 = (x(R), y(R)), A_1 = (x'(R), y'(R)), A_2 = (x''(R), y''(R))$ we obtain Equation (1) in [2].

7 An alternative Approach

Although the interpretation of first reducing to a problem of univariate polynomial equality checking and utilizing the Schwartz-Zippel Lemma as is done in the case where we have a uniform distribution over all λ, μ pairs is more intuitive, it does not directly generalize to the setup where sampling is done from the space of random pairs of rational points on the elliptic curve. It seems however likely that the proof can be extended to this case as well. We have not pursued this approach further, as the proof given in Section 5 using the surface $E \times E$ leads immediately to the desired result.

There is however an alternative approach: the rational behind choosing rational points $A_0, A_1 \in E(\mathbb{F}_q)$ was to be able to evaluate the norm of the witness function D directly on the curve without having to compute the norm. It is possible to do this for a random choice of λ, μ pair as well. In this case the intersection points will not necessarily be rational, but there is

no reason to require this unless one has to do calculations with them directly. Using resultant one can avoid doing any computation with these points and use only the random coefficients λ, μ.

More precisely, picking a random line $y = \lambda \cdot x + \mu$ (i.e., picking random λ, μ), the intuitive approach with soundness proof given in Theorem 3 works. The problem is to compute the left hand side of Equation (1) without having to compute the norm. Using the equation of the line $y = \lambda \cdot x + \mu$ and the elliptic curve $y^2 = x^3 + a \cdot x + b$, we see that the x-coordinates of the three intersection points are given by the roots of the cubic polynomial

$$(\lambda \cdot x + \mu)^2 - (x^3 + a \cdot x + b)$$

and the corresponding y coordinates can be evaluated using the line equation. The value of the norm of D can hence be obtained by using the resultant of this cubic polynomial and the polynomial $D(x, \lambda \cdot x + \mu)$:

$$\mathrm{Res}(a(x) - (\lambda x + \mu) \cdot b(x), (\lambda x + \mu)^2 - (x^3 + ax + b)).$$

This approach can be particularly useful, if choosing rational points on the elliptic curve uniformly at random is difficult.

References

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

[2] 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`.

[3] 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).

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

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

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