Appendix to Section S

Procedure `eigen`. Let ℓ be a prime and let $1 \le \gamma < \ell$. Suppose that the goal is to decide whether γ is the eigevalue of a Frobenius endomorphism when the latter is restricted to $E[\ell]$. It is assumed that $\mathrm{char}(K)$ does not divide ℓ. Therefore $E[\ell] \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ is a vector space over $\mathbb{Z}_\ell$ that is of dimension two.

To decide whether there exists $P = (\alpha, \beta) \in E[\ell]^*$ such that $\varphi(P) = [\gamma]P$ rests upon the possibility to express $[\gamma]P$ as $(\alpha - c_\gamma(\alpha)/d_\gamma(\alpha), \beta r_\gamma(\alpha)/s_\gamma(\alpha))$, where c_γ, d_γ, r_γ and s_γ are polynomials in variable x.

The existence of $P \in E[\ell]^*$ for which $\varphi(P)$ and $[\gamma]P$ coincide in the first coordinate depends upon

$$\tilde{g}_\ell = \gcd(d_\gamma x^q - x d_\gamma + c_\gamma, \bar{f}_\ell).$$

If $\tilde{g}_\ell \neq 1$, then for each root α of $\tilde{g}_\ell$ there exists $P = (\alpha, \beta) \in E[\ell]^*$ such that α^q, which is the first coordinate of $\varphi(P)$, is equal to $\alpha - c_\gamma(\alpha)/d_\gamma(\alpha)$, which is the first coordinate of $[\gamma](P)$. If $\tilde{g}_\ell = 1$, then γ is not an eigenvalue. Assume $\tilde{g}_\ell \neq 1$.

To see if for any α which is a root of $\tilde{g}_\ell$ there exists β such that $P = (\alpha, \beta) \in E[\ell]$ and $\varphi(P)$ agrees with $[\gamma]P$ in the second coordinate too, the equation $\beta^q = \beta r_\gamma(\alpha)/s_\gamma(\alpha))$ has to be verified. Since $\beta^{q-1} = (\alpha^3 + a\alpha + b)^{(q-1)/2}$, the verification of γ being an eigenvalue finishes by the test of

$$\gcd((x^3 + ax + b)^{\frac{q-1}{2}} s_\gamma(x) - r_\gamma(x), \tilde{g}_\ell).$$

Degree of $\tilde{g}_\ell$. Suppose that γ is an eigenvalue. Then the number of roots of $\tilde{g}_\ell$ is twice the number of $P \in E[\ell]^*$ such that $\varphi(P) = [\pm\gamma]P$. The characteristic polynomial $T^2 - t_\ell T + q_\ell$ may be equal to $(T - \gamma)^2$. In such a case $\tilde{g}_\ell = \bar{f}_\ell$ since every element of $E[\ell]^*$ is mapped by φ to $[\gamma]P$.

Let $T^2 - t_\ell T + q_\ell \neq (T - \gamma)^2$. Then φ possesses besides γ another eigenvalue, say λ. The existence of $P \in E[\ell]^*$ with $\varphi(P) = [-\gamma]P$ is thus equivalent to $\lambda = -\gamma$. Since $\lambda \neq \gamma$, the eigenspaces of λ and γ are of dimension one. Hence $\deg(\tilde{g}_\ell) = (q-1)/2$ if $\lambda \neq -\gamma$ and $\deg(\tilde{g}_\ell) = q - 1$ if $\lambda = -\gamma$.

In Schoof's algorithm the situation $\lambda = -\gamma$ does not occur since in such a case the characteristic polynomial is equal to $(T - \gamma)(T + \gamma) = T - \gamma^2$, and that implies $t_\ell = 0$. However, the procedure `eigen` is called in Schoof's algorithm only after it has been verified that $t_\ell \neq 0$.

Two approaches to the procedure `tyzero`. The procedure is called in the situation when it is known that there exists $P = (\alpha, \beta) \in E[\ell]^*$ such that $\varphi^2(P)$ and $[q_\ell]P$ agree in the first coordinate. The equality $t_\ell = 0$ takes place if and only if $\varphi^2(P) = [-q_\ell]P$ for each $P \in E[\ell]$. However, for this to hold it suffices to find just one $P \in E[\ell]^*$ for which $\varphi^2(P) = [-q_\ell]P$.

If $\varphi^2(P)$ and $[-q_\ell]P$ always agree, then $-\beta^{q^2} = \beta r_{q_\ell}(\alpha)/s_{q_\ell}(\alpha)$ for each $P = (\alpha, \beta) \in E[\ell]^*$. The respective polynomial has to be thus divisible by $\bar{f}_\ell$. If that divisibility takes place, then the second coordinate of $\varphi^2(P)$ and $[-q_\ell](P)$ agrees for all $P \in E[\ell]^*$, and thus also for an element P for which the first coordinate of $\varphi^2(P)$ and $[-q_\ell](P)$ agrees. Since the existence of such P is known, $t_\ell = 0$, and $\varphi^2(P) = [-q_\ell]P$ for every $P \in E[\ell]$. However, to make this conclusion requires that $\bar{f}_\ell$ divides the polynomial that expresses the agreement in the second coordinate. In this case it does not suffice to verify the existence of a nontrivial common divisor.

An alternative approach is to store $\gcd(\bar{s}_\ell, \bar{f}_\ell)$. Denote it by g_ℓ, like in the main text. If $\deg(g_\ell) < \deg(\bar{f}_\ell)$, then $t_\ell \neq 0$ because roots of g_ℓ are those α for which there exists β such that $P = (\alpha, \beta) \in E[\ell]^*$ and $\varphi^2(P)$ agrees with $[q_\ell]P$ in the first coordinate. If $t_\ell = 0$, then the agreement is true for all $P \in E[\ell]$.

However, the test $\deg(g_\ell) < \deg(\bar{f}_\ell)$ does not have to be done. The main idea of the alternative approach is that instead of testing the divisibility of the polynomial that expresses the agreement of $\varphi^2(P)$ and $[-q_\ell](P)$ in the second coordinate, it suffices to test the existence of a common nontrivial divisor of that polynomial with g_ℓ. Indeed, for each root α of such a common divisor there exists β such that $P = (\alpha, \beta)$ is in $E[\ell]$, and $\varphi^2(P)$ agrees with $[-q_\ell](P)$ in both coordinates.

Why $\tilde{g}_\ell$ and g_ℓ agree. Suppose that $g_\ell = \gcd(\bar{s}_\ell, \bar{f}_\ell) > 1$ and $t_\ell \neq 0$. In such a case τ is chosen so that $\tau^2 \equiv 4q_\ell \bmod \ell$. Set $\gamma = 2q_\ell/\tau$. As has been explained in Section I, either γ or $-\gamma$ is an eigenvalue of φ (relative to $E[\ell]$). At this point of Schoof's algorithm it is already known that $t_\ell \neq 0$. Hence only one of γ and $-\gamma$ is the eigenvalue.

Roots of $\tilde{g}_\ell$ (which is defined with respect to the eigenvalue $\pm\gamma$) are those α, for which there exists β such that $P = (\alpha, \beta) \in E[\ell]^*$ and $\varphi[P]$ agrees with $[\pm\gamma]P$ in the first coordinate. If this happens, then $\varphi^2(P) = [\gamma^2]P = [4q_\ell^2/\tau^2]P = [q_\ell]P$. Hence α is also a root of g_ℓ, and $\tilde{g}_\ell$ divides g_ℓ.

Indeed, roots of g_ℓ are those α for which there exists $P = (\alpha, \beta) \in E[\ell]^*$ such that $\varphi^2(P)$ and $[q_\ell]P$ agree in the first coordinate. This means that $\varphi^2(P) = [\pm q_\ell]P$. Since $t_\ell \neq 0$, there is no P with $\varphi^2(P) = [-q_\ell]P$. Hence only the case of $\varphi^2(P) = [q_\ell]P$ may take place. If $\varphi(P) = [\pm\gamma]P$ for every $P \in E[\ell]$, then $\varphi^2(P) = [q_\ell]P$ for every $P \in E[\ell]$. In such a case $\tilde{g}_\ell = g_\ell = \bar{f}_\ell$. For the rest we may thus assume the existence of an eigenvalue $\lambda \neq \pm\gamma$. Hence $\lambda^2 \neq \gamma^2$. Both λ^2 and $\gamma^2 = q_\ell$ are eigenvalues of $\varphi^2(P)$. There cannot be $\lambda^2 = -\gamma^2$ since $\varphi^2(P) = [-q_\ell]P$ never takes place. Therefore both q_ℓ and $\bar{q}_\ell$ are of degree $(q-1)/2$. That implies that they are equal (up to a scalar multiple).