
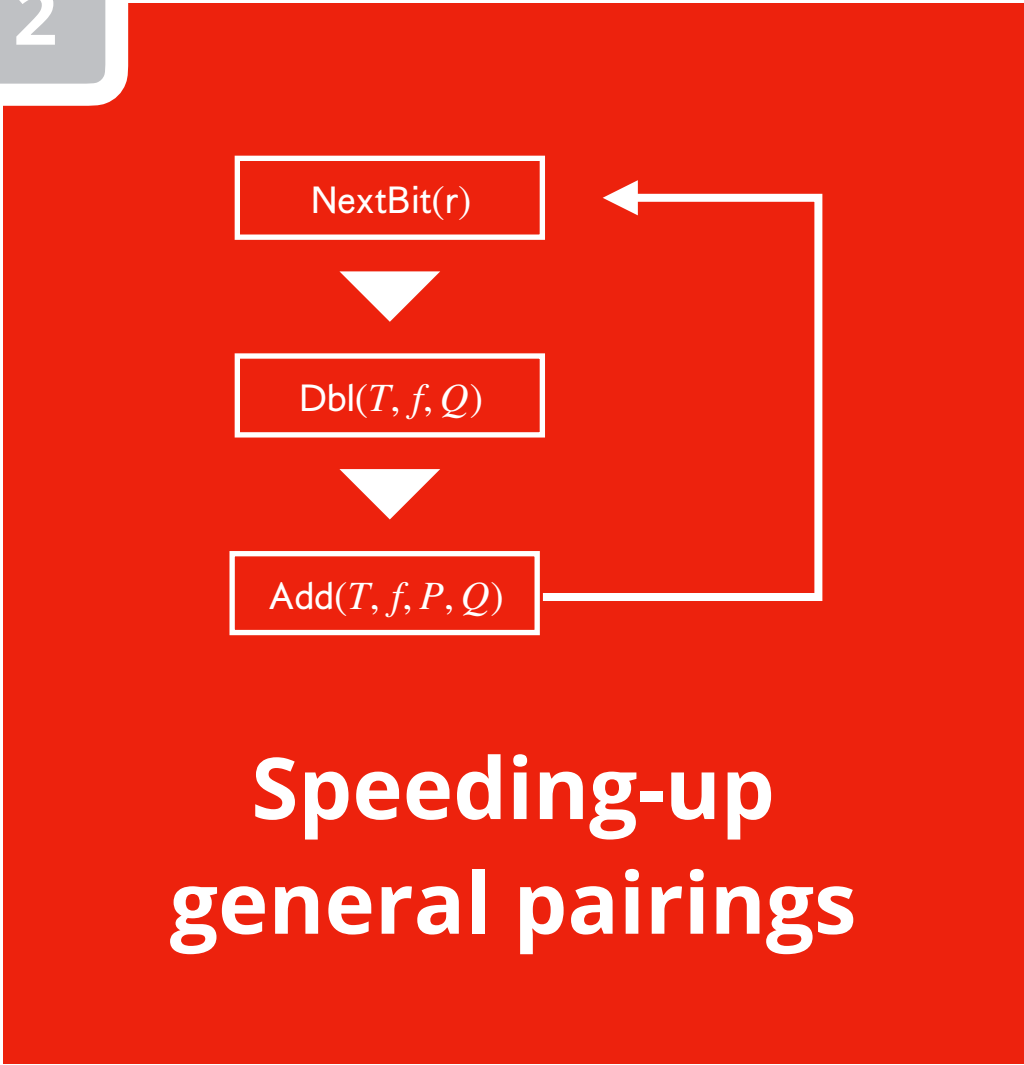


2



general notice

Computing pairings fast is quite technical.
Better suited for papers than slides




core idea

For $P \in E(\mathbb{F}_p)$ and $Q \in E^t(\mathbb{F}_p)$,
don't use curve arithmetic
but pairing $e(P, Q)$ to get
overlap in orders!


core idea

For $P \in E(\mathbb{F}_p)$ and $Q \in E^t(\mathbb{F}_p)$,
don't use curve arithmetic
but pairing $e(P, Q)$ to get
overlap in orders!



 **general approach**

Instead I describe the general approach,
and leave all details out

 **general approach**

Instead I describe the general approach,
and leave all details out

0

take some literature

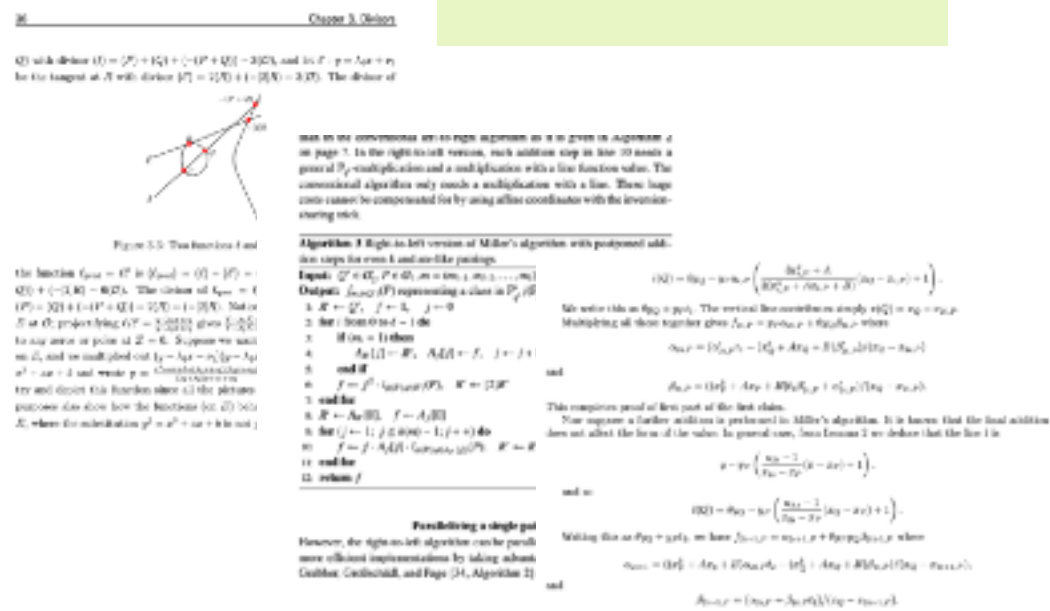
1

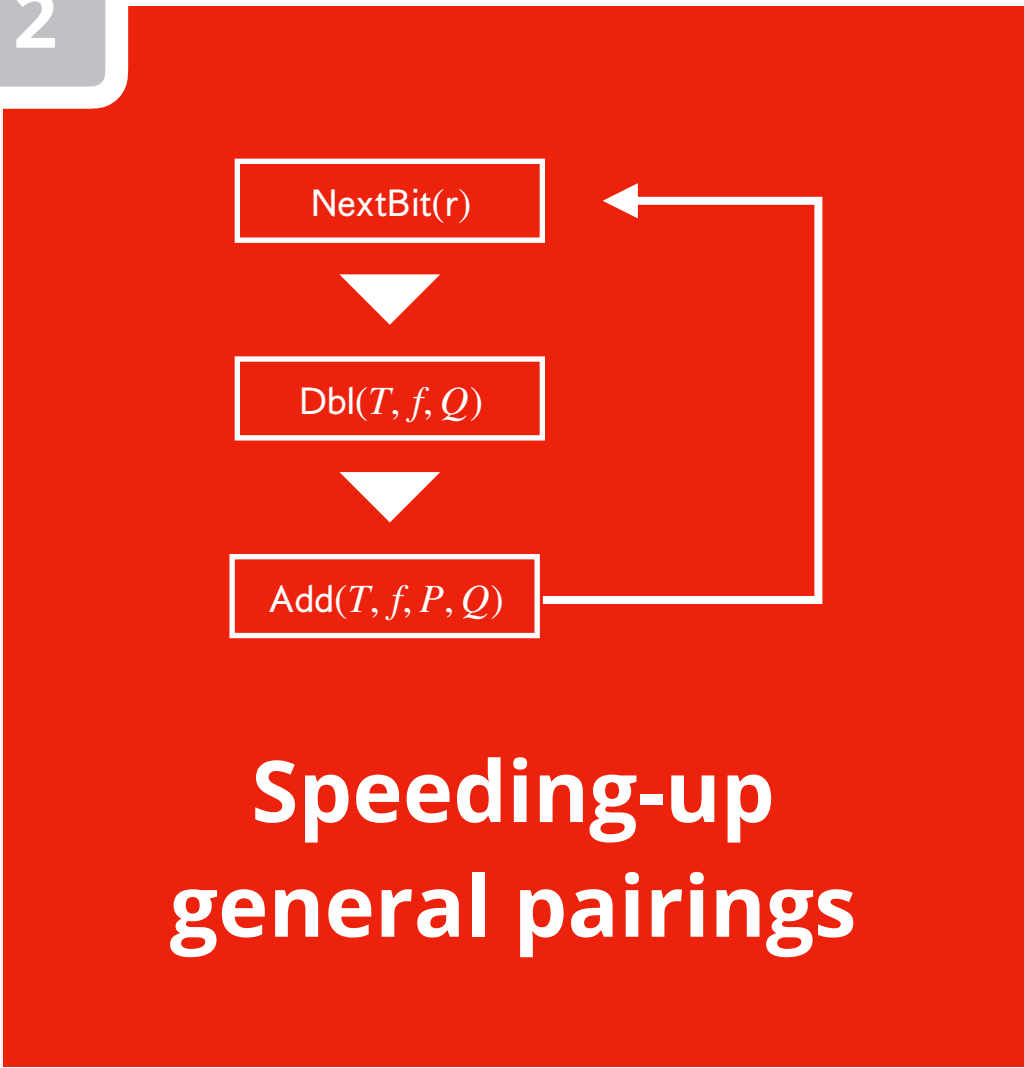
1
implement all tricks
that apply

2

2 benchmark speed and finetune

3





!


general notice

Computing pairings fast is quite technical.
Better suited for papers than slides

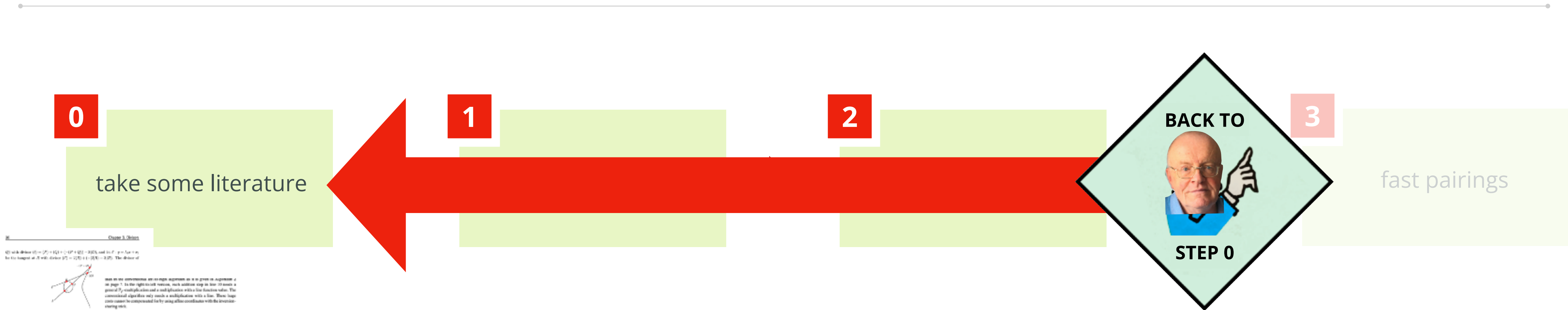
✓

core idea

For $P \in E(\mathbb{F}_p)$ and $Q \in E^t(\mathbb{F}_p)$,
don't use curve arithmetic
but pairing $e(P, Q)$ to get
overlap in orders!

 **general approach**

Instead I describe the general approach,
and leave all details out



Chapter 3. Division

Q) with division $U = (P^2 + Q^2) + (-P^2 + Q^2) - 3Q^2$, and in \mathcal{F} , $p = 5a + 7a$ for its longest α with division $\beta^2 = 2(Q^2 + 1) - 3(Q^2 - 3Q^2)$. The divisor of

Figure 3.5.5: Two functions U and Q

the

Q)

Q) with division

for its longest α with division

β^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

α^2

seen on the environment are to-right segments on α as given in segment α on page 7. In the right-to-left version, each addition step on line 10 needs a point multiplication and a multiplication with a line function value. The computational algorithm only needs a multiplication with a line function. These large steps can be compensated for by using affine coordinates with the inversion-saving trick.

Algorithm 3 Right to left version of Miller's algorithm with postponed add:

Chapter 3. Division

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

then in \mathcal{F} with

$$(x_2) = (x_2 - x_1) \cdot \text{norm}_E \left(\frac{y_2 - y_1}{(x_2 - x_1)^2 + (y_2 - y_1)^2} \right)$$

We note this as $\text{div}_2 = \text{div}_1$. The vertical line function is simply $\text{div}_2(x) = y_2 - y_1$.