Proposal to Study the Point Operation Formulae for Elliptic Curves on Projective Coordinates

Min “Jason” Shin
Perm#: 5081542
Date: 4/30/2014
CS 190g

Introduction
Point Operations in elliptic curve over GF(p) involve several multiplications, squarings, and inversions on the affine coordinate system. It is always a crucial objective to shorten the amount of computing time because it directly translates to the cost of operations. Inversion is a costly operation in the affine coordinate system, and the projective coordinate system can serve as a cheaper and more effective operation technique by eliminating the inversion operation.

Proposal
Over the remaining quarter, I will study various point operation formulae for elliptic curves on projective coordinates. I will research and explain the following:

i) The mathematical concept behind projective geometry
ii) The transformation from affine to projective coordinate system.
iii) The advantages in point operation formulae over projective coordinates.
iv) The different kinds of existing formulae for short Weierstrass curves.

For part iv), I will focus on the Jacobian coordinates with various parameters of $\alpha$ on a Weierstrass curve; e.g. $y^2 = x^3 + \alpha x + b$ for $\alpha = 0, -1, -2$, etc., and explain how to formulate the third variable $z$.

I will also demonstrate a thorough example problem with detailed explanations of each components of the operation. This example problem will also illustrate part iii), by comparing the time of computation with computations performed using affine coordinate system.