Quick evaluation of polynomials via Strassen's Algorithm

September 14, 2009

1 Introduction

We have already seen that we can evaluate

$$\sum_{0 \le d \le k-1} x^{d^2} \pmod{2, g(x)}$$

quickly if we can perform FFT's quickly in this ring. Unfortunately, it remains to be proved that we have FFTs available (well, we certainly have them available, but whether they can be made to run as fast as we need is the real issue), for various reasons that I don't want to get into.

Earlier today I discovered that, in fact, one can use Strassen's algorithm to do this quickly instead, which is good because Strassen works in any ring. I believe I wrote before that Strassen might come to our aid, and it seems I was right, but the application of it I have in mind is different than what I wrote about before. Furthermore, there may be a way to use the *ideas* in the fast multiplication algorithm from Knuth's book *Seminumerical Algorithms* to improve things well beyond what Strassen gives, to obtain results comparable to FFTs.

2 The basic idea

Basically, here is the idea: let $D := k^{1/3}$, and assume that k is a cube. Let

$$h_0(Y) \ := \ 1 + xY + x^4Y^2 + x^9Y^3 + \cdots + x^{(D-1)^2}Y^D.$$

Then, it is a simple exercise to check that

$$\sum_{0 \le d \le k-1} x^{d^2} \;=\; \sum_{0 \le a,b \le D-1} x^{(aD^2+bD)^2} h_0(x^{2aD^2+2bd}).$$

So, if we can evaluate $h_0(Y)$ quickly at the points in the set

$$\{x^{2aD^2+2bD} \;:\; 0 \le a, b \le D-1\},$$

then we are done.

It is easy to see that these values of $h_0(Y)$ are entries of the following matrix product

$$\begin{bmatrix} 1 & x & x^4 & x^9 & \cdots & x^{(D-1)^2} \\ 1 & x^{2D+1} & x^{4D+4} & x^{6D+9} & \cdots & x^{2(D-1)D+(D-1)^2} \\ 1 & x^{4D+1} & x^{8D+4} & x^{12D+9} & \cdots & x^{4(D-1)D+(D-1)^2} \\ 1 & x^{6D+1} & x^{12D+4} & x^{18D+9} & \cdots & x^{6(D-1)D+(D-1)^2} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x^{2(D-1)D+1} & x^{4(D-1)D+4} & x^{6(D-1)D+9} & \cdots & x^{2(D-1)^2D+(D-1)^2} \end{bmatrix}$$

$$\times \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & x^{2D^2} & x^{4D^2} & x^{6D^2} & \cdots & x^{2(D-1)D^2} \\ 1 & x^{4D^2} & x^{8D^2} & x^{12D^2} & \cdots & x^{4(D-1)D^2} \\ 1 & x^{6D^2} & x^{12D^2} & x^{18D^2} & \cdots & x^{6(D-1)D^2} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x^{2(D-1)D^2} & x^{4(D-1)D^2} & x^{6(D-1)D^2} & \cdots & x^{2(D-1)^2D^2} \end{bmatrix}.$$

And we know that Strassen's method allows us to compute this product in time significantly faster than $D^3 = k$.