David Bozarth
CES 512 – Spring 2005
Sonoma State University

Hw 3.1 : Squaring a polynomial by mimicking Karatsuba's algorithm

A polynomial

$$p(x) = c_0*x^0 + c_1*x^1 + \ldots + c_{n-1}*x^{n-1}$$

can be separated in two groups of coefficients: those with even order, and those with odd order. Let y = x2. Without loss of generality, suppose p(x) has an even number of terms, and let polynomials A and B be defined as:

$$A = c_0*y^0 + c_2*y^2 + \ldots + c_{(n/2)-1}*y^{(n/2)-1}$$ … the even coefficients from p(x)

$$B = c_1*y^1 + c_3*y^3 + \ldots + c_{(n/2)}*y^{(n/2)}$$ … the odd coefficients from p(x)

Then

$$p(x) = A + x*B$$

$$[p(x)]^2 = A^2 + x2*B^2 + 2*x*A*B$$

An identity is

$$2*A*B = (A + B)^2 - (A^2 + B^2)$$

Thus

$$([p(x)]^2 = A^2 + x^2*B^2 + x*[(A + B)^2 - (A^2 + B^2)]$$

In this manner the coefficients of a squared polynomial can be obtained, without having to perform any polynomial multiplication.

Since A and B are polynomials in y, it is convenient to first obtain the atomic expressions in A and B; then perform the polynomial arithmetic inside the square brackets; then convert all the polynomials in y, to polynomials in x.

Then the multiplications by powers of x can be done, followed by the addition of the 3 resulting polynomials.

David Bozarth
CES 512 – Spring 2005
Sonoma State University

Application

The squared polynomial can be squared again, and so on. For example,

$$(2 + 3*x)^{32} = (((((2 + 3*x)^2)^2)^2)^2)^2$$

When polynomial multiplication is required to obtain a power of a polynomial, use of this technique can simplify the process:

$$(2 + 3*x)^{29} = (2 + 3*x)^{16} * (2 + 3*x)^8 * (2 + 3*x)^4 * (2 + 3*x)^1$$

In this homework I left out polynomial multiplication, and found the coefficients of $(2 + 3*x)^{32}$.

Algorithm: SquarePoly

Input p(x)

A = (even order coefficients)

B = (odd order coefficients)

Find A^2, B^2, $(A^2 + B^2)$, $(A + B)^2$ by recursive calls to SquarePoly.

Find $(A + B)^2 – (A^2 + B^2)$

Convert y-polynomials to x-polynomials.

Perform these x-multiplications by shifting right: x^2*B^2, $x * [(A + B)^2 – (A^2 + B^2)]$

Output the sum $A^2 + x^2*B^2 + x*[(A + B)^2 - (A^2 + B^2)]$

Results:

p(x):

2.0
3.0

{[p(x)]^2}^5 :

4.294967296E9
2.06158430208E11
4.793183502336E12
7.189775253504E13
7.8188805881856E14
6.567859694075904E15
4.4333052935012352E16
2.46998437780783104E17
1.1578051770974208E18
4.6312207083896832E18
1.5977711443944407E19
4.793313433183322E19
1.258244776210622E20
2.9036417912552817E20
5.9109850750554E20
1.063977313509969E21
1.6957138434065165E21
2.3939489553974333E21
2.992436194246794E21
3.3074294778517206E21
3.224743740905426E21
2.7640660636332227E21
2.073049547724917E21
1.35198883547277E21
7.604937199534341E20
3.650369855776488E20
1.4741878263712696E20
4.913959421237651E19
1.3162391306886062E19
2.7232533738382234E18
4.084880060755241E17
3.9531097367298048E16
1.853020188851841E15