BLACKBOARD PROOFS

CSE202 – WEEK 4

1. Quadratic convergences

1. For the inverse.
Start from

$$y_{n+1} = y_n + y_n(1 - ay_n).$$

Multiplying by $-a$ and adding 1 yields

$$1 - ay_{n+1} = 1 - ay_y - ay_n(1 - ay_n) = (1 - ay_n)^2.$$

Dividing by a concludes that

$$\frac{1}{a} - y_{n+1} = a\left(\frac{1}{a} - y_n\right)^2.$$

2. For the square root.
Start from the Newton iteration

$$y_{n+1} = \frac{1}{2}\left(y_n + \frac{a}{y_n}\right),$$

subtract $\sqrt{a}$ and factor, to get

$$\begin{aligned} y_{n+1} - \sqrt{a} &= \frac{1}{2}\left(y_n - 2\sqrt{a} + \frac{a}{y_n}\right), \\ &= \frac{1}{2y_n}\left(y_n^2 - 2\sqrt{a}y_n + a\right), \\ &= \frac{\left(y_n - \sqrt{a}\right)^2}{2y_n}. \end{aligned}$$

2. How can one reduce division to 3 multiplications?

The question "Why $3\,\mathrm{Mul}(n/2)$?" in the slide corresponds to a refinement of the algorithm that is not the one described in the previous slide. In order to get a complexity as low as these $3\,\mathrm{Mul}(n/2)$ operations, two observations need to be made:

(1) the first multiplication $a \times s$ is a multiplication of a polynomial of degree k (the value of s obtained recursively) by a polynomial of degree n (a). In order to perform this multiplication, it is sufficient to rewrite a as $a_0 + X^k a_1$ with $\deg a_0$ and $\deg a_1$ smaller than k, compute both products $a_0 \times s$ and $a_1 \times s$ and conclude in $O(n)$ operations;
(2) by design, $a \times s = 1 + O(X^k)$, which means that there is a polynomial $\tilde{a}$ *of degree at most* k such that $1 - as = X^k\tilde{a}$. Thus in order to compute the first n coefficients of $s \times (1 - as)$, it is sufficient to compute the first k coefficients of $s \times \tilde{a}$, which costs only $\mathrm{Mul}(n/2)$ operations.

3. Complexity of Euclidean division

The algorithm starts by reverting lists of coefficients, which does not use any arithmetic operation on the coefficients. Next, it computes the inverse of a power series at precision $\deg A - \deg B + 1$, so that when $\deg A = cn$ and $\deg B = n$, this is precision $(c-1)n+1$ and by the result on inversion of power series this has complexity $O(\mathrm{Mul}((c-1)n)$. By the second inequality on Mul, this is $O(\mathrm{Mul}(n))$. The next operation is a multiplication by $\tilde{A}$, again in $\mathrm{Mul}(n)$ operations on the coefficients. Reversing the coefficients of $\tilde{Q}$ to recover Q does not cost any arithmetic operation. Finally, the computation of the remainder R uses one multiplication in degree n, in $\mathrm{Mul}(n)$ and one subtraction in $O(n)$ operations. Summing up the costs of these individual operations gives a complexity in $O(\mathrm{Mul}(n))$ operations.