Black boxes

November 23, 2023 9:18 AM

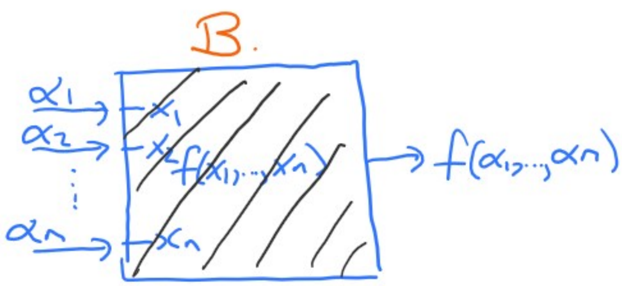
Assignment #6 due 11pm Monday Nov. 27th
Assignment #7 due 11pm Monday Dec 4th.

The "Black-box" representation for polynomials.

Let $f \in R[x_1, \dots, x_n]$, R an integral domain eg. $\mathbb{Z}, \mathbb{Q}(\alpha), \mathbb{F}_q$.

Sparse representation : $f = \sum_{i=1}^{t} a_i \cdot M_i(x_1, \dots, x_n)$ $\quad a_i \in R \setminus \{0\}$.
↑ monomials

Black-box representation : $B : R^n \to R$ is a computer program that on input of $\alpha \in R^n$ computes $f(\alpha)$ i.e. $B(\alpha) = f(\alpha)$.



We cannot see inside B.
All we can do is evaluate B at a point $\alpha \in R^n$.
We "probe" the black-box at a point $\alpha \in R^n$.

Let $d = \deg(f)$, $t = \#f$, for $R = \mathbb{Z}$ let $h = \|f\|_\infty = \max_{1 \le i \le t} |a_i|$.
We may or may not know bounds $D \ge d$, $T \ge t$, $H \ge h$.

Example.

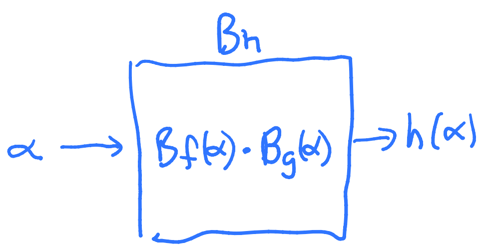
$$f = \det(T_3) = \det\left(\begin{bmatrix} u & v & w \\ v & u & v \\ w & v & u \end{bmatrix}\right) \in \mathbb{Z}[u,v,w].$$

Notice $\deg(f) \le 3 = D$
$\#f \le 3! = T$
$\|f\|_\infty \le 3! = H$

```
B := proc( alpha :: list(integer))
    local T3, i, j;
    uses LinearAlgebra;
    T3 := Matrix(3,3);
    for i to 3 do for j to 3 do
        T3[i,j] := alpha[abs(i-j)+1];
    od; od;
```

```
    Determinant(T3);
end;
```

How can we multiply two polynomials $f, g \in R[x_1, \ldots, x_n]$ given by black boxes $B_f : R^n \to R$ and $B_g : R^n \to R$? Let $h = f \cdot g$.

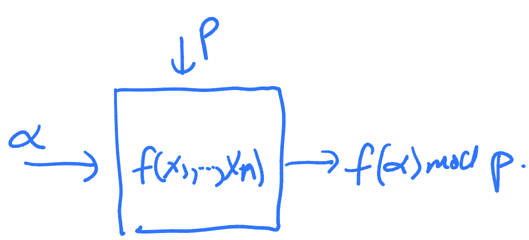



```
BBmultiply := proc( Bf, Bg)
        proc(α) Bf(α) · Bg(α) end
end
```

This costs $O(1)$.

For $R = \mathbb{Z}$ it is useful to use the Chinese remainder theorem.

A <u>modular black-box</u> representation for $f \in \mathbb{Z}[x_1, \ldots, x_n]$ is a black-box $B : (\mathbb{Z}_p^n, p)$ that for $\alpha \in \mathbb{Z}_p^n$ computes $f(\alpha) \bmod p$.




```
B := proc( alpha :: list(integer), p::prime)
    local T;
    uses LinearAlgebra;
    T := ToeplitzMatrix(alpha, symmetric);
    Det(T) mod p;
end;
```

Given a black-box $B : R^n \to R$ for $f \in R[x_1, \ldots, x_n]$

Is $f = 0$?

What is $\deg(f)$? $\boxed{\deg(f, x_i)?}$

What is $t = \#f$?

What is $LT(f)$?

Interpolate f, i.e., find $a_i \in R$ and $M_i(x_1, \ldots, x_n)$.