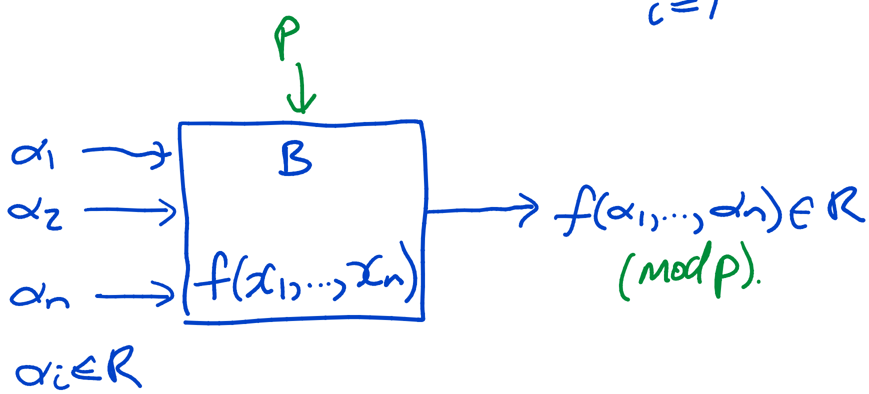
The Black Box representation for polynomials

October 14, 2021 12:18 PM

Kaltofen.

Let $f \in R[x_1, \ldots, x_n]$.

Sparse representation: $f = \sum_{i=1}^{t} a_i M_i(x_1, \ldots, x_n)$ $a_i \neq 0$.



All we can do is evaluate f at $\alpha \in R^n$ (possibly mod p).

B is a program that computes f.

Example. $f = \det(T_4) = \det\left(\begin{bmatrix} x & y & z & w \\ y & x & y & z \\ z & y & x & y \\ w & z & y & x \end{bmatrix}\right) \in \mathbb{Z}[x, y, z, w]$.

```
Bf := proc( α :: list(integer), p)
        n := nops(α);
        Tn := Matrix(n,n);
        for i to n do
            for j to n do
                Tn[i,j] := α[abs(i-j)+1];
            od;
        od;
        Det(Tn) mod p;
    end;
```

matrix of integers α.

Is $f = 0$? What is $\deg(f)$? $\deg(f, x_i)$?

If f and h are given by black boxes B_f and B_g a black box for the product of $f \times h$ is given by.

```
BBmult := proc( Bf :: procedure, Bh :: procedure, p)
```

```
proc( α :: list(integer), p)
    Bf(α, p) * Bn(α, p) mod p;
end;
end;
```

$g = f \times h \qquad g(\alpha) = f(\alpha) \cdot h(\alpha).$

$B_{fh} := BBmult(Bf, Bh, p);$ $\qquad$ $Bfh(\alpha, p);$

Lemma Schwarz-Zippel.

Let $f \in D[x_1, \ldots, x_n]$, D an integral domain, $f \neq 0$.

Let S be a finite subset of D.

If $\alpha_1, \alpha_2, \ldots, \alpha_n$ are chosen at random from S then

$$\mathrm{Prob}[\, f(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0 \,] \leq \frac{\deg(f)}{|S|}.$$

Let B be a black box for $f \in \mathbb{Z}_p[x_1, \ldots, x_n]$

What is $\deg(f, x_1)$?

Suppose $d \geq \deg(f) \Rightarrow d \geq \deg(f, x_1)$.

To compute $\deg(f, x_1)$

① Pick $\alpha_2, \ldots, \alpha_n$ from $\mathbb{Z}_p$ at random and pick $\beta_0, \beta_1, \ldots, \beta_d$ from $\mathbb{Z}_p$.

$f = (x_2 - \alpha_2) x_1^{d_1} + \boxed{}.$

② Idea. Let $\boxed{g(z) = f(z, \alpha_2, \ldots, \alpha_n)}$. Interpolate $g(z)$ knowing $\deg(g(z)) \leq d$.

Compute $y_i \leftarrow B(\beta_i, \alpha_2, \ldots, \alpha_n)$ for $0 \leq i \leq d$.

③ Interpolate $g(z)$ from y_i, β_i $[\, g(\beta_i) = y_i \,]$.

④ Output $\deg g(z)$. // $= \deg(f, x_1)$.

What's $\text{Prob}[\deg(g(z)) < \deg(f, x_1)]$?

Suppose $f = \sum_{i=0}^{d_1} a_i(x_2, \dots, x_n) \cdot x_1^i$ where $d_1 = \deg(f, x_1)$.

$= a_{d_1}(x_2, x_3, \dots, x_n) x_1^{d_1} + \cdots$

we chose these randomly

$\text{Prob}[\deg(g(z)) < d_1] = \text{Prob}[a_d(\underbrace{\alpha_2, \dots, \alpha_n}) = 0]$

By S-Z $\leq \dfrac{\deg(a_d)}{p} \leq \dfrac{\deg(f) = d}{p}$.

We needed $d+1$ values. We need $d = \deg(f)$.

Exercise: How to get d?

Hint: interpolate $g(y) = f(y+\alpha_1, y+\alpha_2, \dots, y+\alpha_n)$