Föreläsn. 8 Olov 17/4-05

Schwartz-Zippel lemma

Sats

Låt $\mathbb{F}$ vara ett legeme och $S \subseteq \mathbb{F}$ en ändlig mängd. Ett polynomium $P(X_1, \ldots, X_n) \in \mathbb{F}[X_1, \ldots, X_n]$, $\deg(P) = d \geq 0$ har högst $|S|^{n-1} d$ nollpunkter i $S^n = \underbrace{S \times \cdots \times S}_{n \text{ gånger}}$.

Bevis: Induktion efter n.

Basfallet $n = 1$ Resultat välkänt

Induktionssteget

Antag satsen gäller för alla polynomier i $n-1$ variabler. Vi skall visa att så också för polynomier i n variabler.

Skriv $P(X_1, \ldots, X_n) = \sum_{s=0}^{d} X_1^s P_s(X_2, \ldots X_n)$

Låt $i = S$ vara.

största indeks så $P_i(X_2, \ldots, X_n) \neq 0$.

alltså låt $i = \deg_{X_i}(P)$.

Vi har $i \geq 0$

1) För hvert tuppel $(r_2, \ldots, r_n)$ så

$P_i(r_2, \ldots, r_n) \neq 0$ är $\deg(P(X_1, r_2, \ldots, r_n)) = i$

Så därför är det högst i $r \in S$ så

$P(r, r_2, \ldots, r_n) = 0$. alltså i alt

3/8

højst $i\|S\|^{n-1}$ $(r, r_2, \dots, r_n) \in S^n$

så $P(r, r_2, \dots, r_n) = 0$ og

$P_i(r_2, \dots, r_n) \neq 0$.

2)

Der er højst $\deg P_i \cdot \|S\|^{n-2} < (d-i)\|S\|^{n-2}$

tupler $(r_2, \dots, r_n)$ så $P_i(r_2, \dots, r_n) = 0$

og dermed højst

$$\|S\| \cdot (d-i)\|S\|^{n-2} = (d-i)\|S\|^{n-1}$$

tupler $(r, r_2, \dots, r_n) \in S^n$

så $P(r, r_2, \dots, r_n) = 0$ og

$P_i(r_2, \dots, r_n) = 0$.

1)+2)

I alt er der højst $i\|S\|^{n-1} + (d-i)\|S\|^{n-1}$

$= d\|S\|^{n-1}$

multipunkter for $P : S^n$ □