POLYNOMIALS IN DISCRETE MATHEMATICS

NOGA ALON, TEL AVIV

I. COMBINATORIAL NULLSTELLENSATZ

HILBERT'S NULLSTELLENSATZ:

IF F IS AN ALGEBRAICALLY CLOSED FIELD, AND

$f, g_1, g_2, \ldots, g_m \in F[x_1, x_2, \ldots, x_n]$,

AND

$g_1(\underline{x}) = \ldots = g_m(\underline{x}) = 0 \Rightarrow f(\underline{x}) = 0$,

THEN

$\exists k \geq 1$, $h_1(\underline{x}), \ldots, h_m(\underline{x}) \in F[x_1, \ldots, x_n]$

SO THAT

$$f^k = \sum_{i=1}^{m} h_i(\underline{x})\, g_i(\underline{x}).$$

C.N. A SPECIAL CASE:

$m = n$, $g_i = \prod_{a \in S_i} (x_i - a)$ WHERE $S_i \subset F$

CLAIM: IN THIS CASE, IF

$$g_1(\underline{x}) = \ldots = g_n(\underline{x}) = 0 \Rightarrow f(\underline{x}) = 0$$

THEN

$$\exists\, h_1(\underline{x}), \ldots, h_n(\underline{x}) \in F[x_1, x_2, \ldots, x_n]$$

SATISFYING

$$\deg h_i \leq \deg f - \deg g_i$$

AND

$$f = \sum_{i=1}^{n} h_i(\underline{x})\, g_i(\underline{x}).$$

HENCE: IF F IS A FIELD,

$f(\underline{x}) \in F[x_1, x_2, \ldots, x_n]$,

$\deg f = \sum_{i=1}^{n} t_i$ AND $\operatorname{COEF}_f \prod_{i=1}^{n} x_i^{t_i} \neq 0$,

AND IF

$S_1, \ldots, S_n \subset F$, $|S_i| > t_i$

THEN

$\exists\, s_1 \in S_1, \ldots, s_n \in S_n$

SUCH THAT

$f(s_1, s_2, \ldots, s_n) \neq 0$.

THEOREM (CAUCHY AND DAVENPORT)

IF

p IS A PRIME, AND

$$\emptyset \neq A, B \subset \mathbb{Z}_p$$

THEN

$$|A+B| = |\{a+b : a \in A, b \in B\}|$$
$$\geq \text{MIN}(p, |A|+|B|-1).$$

REMARK: THIS IS TIGHT.

A+ NATHANSON + RUZSA (94):

THIS CAN BE PROVED BY APPLYING C. N. TO

$$\prod_{c \in C} (x+y-c),$$

WHERE $C \supseteq A+B$, $|C| = |A|+|B|-2$,

$S_1 = A$, $S_2 = B$, $t_1 = |A|-1$, $t_2 = |B|-1$.

THE SAME TECHNIQUE GIVES:

<u>THEOREM (ANR):</u> IF p IS A PRIME, $\emptyset \neq A_1, A_2, \ldots, A_{k_2} \subseteq Z_p$, $|A_i| \neq |A_j| \ \forall\, i \neq j$

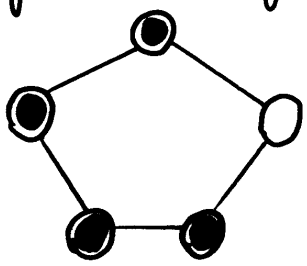
THEN

$$|A_1 \oplus A_2 \oplus \ldots \oplus |A_{k_2}|$$
$$= |\{a_1 + a_2 + \ldots + a_{k_2} \mid a_i \in A_i,\ a_i \neq a_j\}|$$
$$\geq \text{MIN}\left(p,\ \sum_{i=1}^{k_2} |A_i| - \binom{k_2+1}{2} + 1\right).$$

<u>REMARK:</u> THIS IS TIGHT, FOR ALL POSSIBLE CARDINALITIES OF $|A_i|$.

GRAPH COLORING (MATIYASEVICH (74), A+TARSI (92)):

DEFINITIONS: IF $G=(V,E)$ IS A GRAPH, $V=\{1,2,\ldots,n\}$, A PROPER COLORING OF G IS $c: V \to Z$ (= THE INTEGERS) WITH $c(i) \neq c(j)$ $\forall ij \in E$.



THE CHROMATIC NUMBER $\chi(G)$ OF G IS

$\text{MIN}\{k:$ $\exists$ A PROPER COLORING $c: V \to Z$ OF G WITH $c(V)=\{1,2,\ldots,k\}\}$.

IF $G=(V,E)$, $V=\{1,2,\ldots,n\}$, THE GRAPH POLYNOMIAL f_G OF G (INTRODUCED BY SYLVESTER, PETERSEN (1891)) IS:

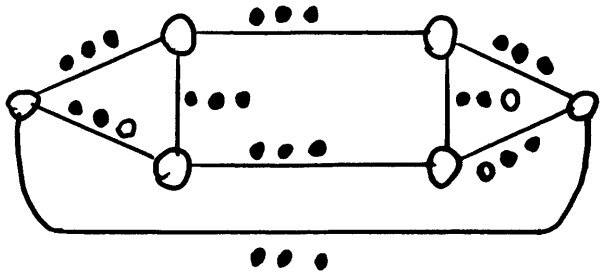
$$f_G(x_1,x_2,\ldots,x_n)=\prod_{\substack{i,j\in E\\ i>j}}(x_i-x_j)$$

NOTE THAT: FOR $S_1,S_2,\ldots,S_n\subset\mathbb{Z}$ $\exists$ A PROPER COLORING $c:V\to\mathbb{Z}$ WITH $c(i)\in S_i$ $\forall i$, IFF $\exists\, a_i\in S_i$ SO THAT

$$f_G(a_1,\ldots,a_n)\neq 0.$$

USING TAIT (1880), VIGNERON (46), 4CT, A+ TARSI (92), JAEGER AND C.N, THIS GIVES:

FOR ANY ASSIGNMENT OF A LIST $S(e)$ OF 3 COLORS TO EACH EDGE e OF A 2-CONNECTED, CUBIC, PLANAR G, THERE IS A COLORING ASSIGNING TO EACH EDGE A COLOR FROM ITS LIST, WITH ADJACENT EDGES GETTING DISTINCT COLORS.



[THIS EXTENDS THE 4CT].

II. THE RANK ARGUMENT

GRAPH POWERS.

IF $G=(V,E)$, $H=(V',E')$ ARE GRAPHS, THEIR (AND) PRODUCT $G\times H$ IS THE GRAPH ON $V(G\times H)=V\times V'$ IN WHICH $(u,u')\sim(v,v')$ IFF $(u=v$ OR $uv\in E)$ AND $(u'=v'$ OR $u'v'\in E')$ [BUT $(u,u')\neq(v,v')$].

THE n'TH POWER OF G, G^n IS

$$G^n = \underbrace{G\times G\times \cdots \times G}_{n \text{ TIMES } G}$$

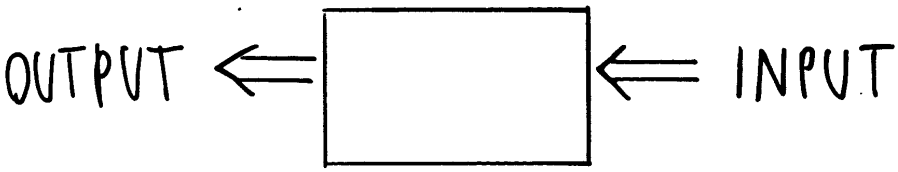
SHANNON CAPACITY

LET $\alpha(G^n)$ DENOTE THE INDEPENDENCE NUMBER OF G^n.

THE SHANNON CAPACITY OF G IS:

$$c(G) = \lim_{n\to\infty} \left[\alpha(G^n)\right]^{1/n} \left(= \sup \left[\alpha(G^n)\right]^{1/n}\right).$$

MOTIVATION



A CHANNEL HAS AN INPUT SET X, AN OUTPUT SET Y, AND A FAN-OUT SET $S_x \subseteq Y \quad \forall x \in X$.

THE GRAPH OF THE CHANNEL IS $G=(X,E)$, WHERE $xx' \in E \Leftrightarrow S_x \cap S_{x'} \neq \emptyset$ (THAT IS: x, x' CAN BE CONFUSED).

$\alpha(G)$ = MAXIMUM NUMBER OF DISTINCT MESSAGES THE CHANNEL CAN COMMUNICATE IN A SINGLE USE (WITH NO ERRORS).

$\alpha(G^n)$ = MAXIMUM NUMBER OF DISTINCT MESSAGES THE CHANNEL CAN COMMUNICATE IN n USES

$C(G)$ = MAXIMUM NUMBER OF DISTINCT MESSAGES PER USE THE CHANNEL CAN COMMUNICATE.

∃ UPPER BOUNDS FOR THE SHANNON CAPACITY [SHANNON (56), LOVÁSZ (79), HAEMERS (79)

A RECENT BOUND:

F = A LINEAR SPACE OF POLYNOMIALS IN r VARIABLES OVER A FIELD F.

A REPRESENTATION OF $G=(V,E)$ OVER F IS A SET $(f_v, C_v)_{v\in V}$, WITH $f_v \in F$, $C_v \in F^r$ AND

(i) $f_v(C_v) \neq 0 \quad \forall v \in V$

(ii) $f_v(C_u) = 0 \quad \forall u \neq v, uv \notin E$

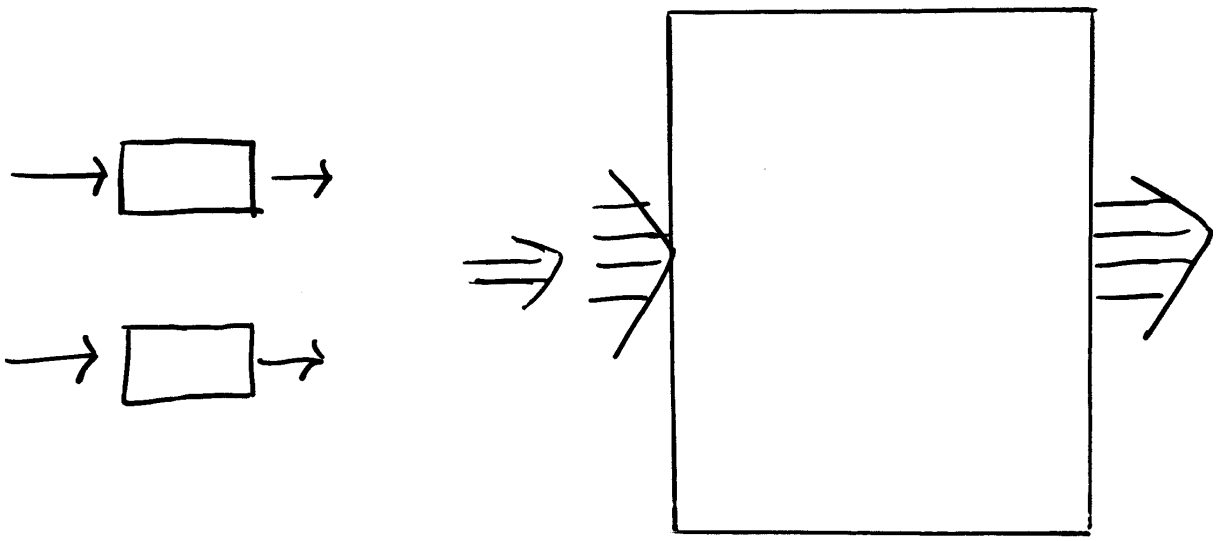
THEOREM: IF G HAS A REPRESENTATION OVER F, THEN

$$c(G) \leq \dim(F).$$

THEOREM: $\forall k \quad \exists\, G, H$ WITH $c(G), c(H) \leq k$, AND YET $c(G+H) \geq k^{\Omega(\log k / \log\log k)}$.

($G+H$ = THE DISJOINT UNION OF G AND H)

[THIS ANSWERS A PROBLEM OF SHANNON]



III AN OPEN PROBLEM:

IF $c(G), c(H) \leq \aleph_2$, HOW LARGE CAN $c(G+H)$ BE?