Constructive and Nonconstructive Methods in Combinatorics and TCS

Lectures 5-6: Applications of the Combinatorial Nullstellensatz

April 9-11, 2018

Lecturer: Andy Drucker *Scribe: Chris Jones*

Today we study the Combinatorial Nullstellensatz (CNSS) in a little more detail.

1 Kouba's proof of the Nullstellensatz

We'll start with an alternate proof of the Nullstellensatz. It's possible this proof could be useful for formulating a constructive version of the Nullstellensatz. The proof is "duality-based": from evaluations of P on a cube $S_1 \times S_2 \times \cdots \times S_n$, we can infer the leading term's coefficient. This is linear in the sense that if P is entirely 0 on the cube, we will show the leading term is also 0 (hence arguing contrapositively, if we have a nonzero leading term, P must be nonzero somewhere on the cube).

Theorem (Combinatorial Nullstellensatz)**.** *Let $\mathbb{F}$ be a field, $P(x_1, \ldots, x_n) \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ a polynomial, and $S_1 \times S_2 \times \cdots \times S_n \subseteq \mathbb{F}^n$. Suppose there's a nonzero leading term $\vec{x}^{\vec{\alpha}}$ with $\vec{\alpha}$ strictly dominated by $(|S_1|, |S_2|, \ldots, |S_n|)$ i.e. $\alpha_i < |S_i|$ for every i.*

Then $P(\vec{x}) \neq 0$ for some $\vec{x} \in S_1 \times S_2 \times \cdots \times S_n$.

Proof (from [Kou09]). Idea for interpolating the $\vec{\alpha}$ coefficient of P: start from simple interpolation in one variable, then bootstrap to multiple variables.

Say $S_i \subseteq \mathbb{F}$ is of size $d_i + 1$. We look at the vector space $\mathbb{F}^{\leq d_i}[x]$ of univariate polynomials of degree at most d_i. Abstractly, for $t \in S_i$ we have linear maps

$$\begin{aligned} \text{eval}_t : \quad & \mathbb{F}^{\leq d_i}[x] \to \mathbb{F} \\ & P \mapsto P(t) \\ \text{coef}_l : \quad & \mathbb{F}^{\leq d_i}[x] \to \mathbb{F} \\ & P \mapsto l\text{-th coefficient of } P \end{aligned}$$

These are linear, hence they live in the dual space $\mathbb{F}^{\leq d_i}[x]^*$. Moreover, $\{\text{eval}_t\}$ is a basis for the space $\mathbb{F}^{\leq d_i}[x]^*$:

- $\{\text{eval}_t\}$ span the space: any tuple of values from $\mathbb{F}$ is possible as a tuple of eval's on some poly p (via Lagrange interpolation). This says the linear map

$$\begin{aligned} \mathbb{F}^{\leq d_i}[x] &\to \mathbb{F}^{S_i} \\ P &\mapsto (\text{eval}_{s_1}(P), \text{eval}_{s_2}(P), \ldots, \text{eval}_{s_{d_i+1}}(P)) \end{aligned}$$

  is surjective and has rank at least $d_i + 1$, and hence so does the dual/transpose map.

- They're necessarily linearly independent in $\mathbb{F}^{\leq d_i}[x]^*$ by their dimension (and because the dimension of a space is the same the dimension of its dual, which is $d_i + 1$).

$\{\text{coef}_l : l = 0, 1 \ldots, d_i\}$ is another basis; indeed it's the dual basis of the standard basis for $\mathbb{F}^{\leq d_i}[x]$. The key corollary is that there are coefficients that change the basis:

$$\text{coef}_l = \sum_{t \in S_i} \lambda_t^l \cdot \text{eval}_t$$

Time to generalize. Say we want to interpolate the $\vec{\alpha}$-th coefficient of a multivariate polynomial P. Define the following weird map,

$$\Phi : \mathbb{F}[x_1, x_2, \ldots, x_n] \to \mathbb{F}$$
$$\Phi(P) \mapsto \sum_{t_1 \in S_1} \sum_{t_2 \in S_2} \cdots \sum_{t_n \in S_n} \lambda_{t_1}^{\alpha_1} \lambda_{t_2}^{\alpha_2} \cdots \lambda_{t_n}^{\alpha_n} P(t_1, t_2, \ldots, t_n)$$

Note that Φ is only properly defined if we have $\alpha_i < |S_i|$. It looks ugly, but we should think of Φ as "lifting" the univariate polynomial coefficient formula to multivariate polynomials. It has some redeeming properties:

- Φ is linear.
- The action of Φ on monomials should be nice.

Lemma.

$$\Phi(\vec{x}^{\vec{\beta}}) = \begin{cases} 1 & \text{if } \vec{\beta} = \vec{\alpha} \\ 0 & \text{if } \beta_i \leq d_i, \beta_i \neq \alpha_i \text{ for some } i \\ ? & \text{otherwise} \end{cases}$$

Proof of lemma.

$$\begin{aligned} \Phi(x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}) &= \sum_{t_1 \in S_1} \sum_{t_2 \in S_2} \cdots \sum_{t_n \in S_n} \lambda_{t_1}^{\alpha_1} \lambda_{t_2}^{\alpha_2} \cdots \lambda_{t_n}^{\alpha_n} t_1^{\beta_1} t_2^{\beta_2} \cdots t_n^{\beta_n} \\ &= \left(\sum_{t_1 \in S_1} \lambda_{t_1}^{\alpha_1} t_1^{\beta_1} \right) \left(\sum_{t_2 \in S_2} \lambda_{t_2}^{\alpha_2} t_2^{\beta_2} \right) \cdots \left(\sum_{t_n \in S_n} \lambda_{t_n}^{\alpha_n} t_n^{\beta_n} \right) \end{aligned}$$

The basis inversion via $\lambda_{t_i}^{\alpha_i}$ is only defined up to degree d_i. For those $\beta_i \leq d_i$, the above are

$$\text{coef}_{\alpha_i}(x_i^{\beta_i})$$

This is zero if any $\beta_i \neq \alpha_i$ in this range, completing the proof of the lemma. □

Thus Φ will extract the coefficient of a leading term $\vec{x}^{\vec{\alpha}}$ of P as the other terms will necessarily be killed off. In fact, this completes the proof of the theorem: if P vanishes on the cube $S_1 \times S_2 \times \cdots \times S_n$, then looking at the definition of Φ we would have that the coefficent of $\vec{x}^{\alpha}$ is 0. □

Note. *The basic CNSS requires we exhibit a nonzero leading term. This proof goes through if we exhibit a nonzero non-dominated term. Michałek's proof also only requires this assumption.*

Note. *This proof seems to require that $\mathbb{F}$ be a field, whereas Michałek's proof shows the CNSS holds if $\mathbb{F}$ is only assumed to be an integral domain. Kouba's strategy has also been applied to prove the CNSS over integral domains [Hei]. Forms of the Nullstellensatz also exist for non-integral domains, if we're willing to make assumptions about the sets S_i.*

2 Hilbert's Nullstellensatz

The original Hilbert Nullstellensatz provides the start of a "dictionary" between algebra and geometry.

Theorem. *Let $\mathbb{F}$ be algebraically closed, $f, g_1, g_2, \ldots g_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. If $V(f) \supseteq V(g_1, \ldots, g_m)$, then there is k and $h_i \in \mathbb{F}[x_1, \ldots x_n]$ with*

$$f^k = \sum_{i=1}^{m} h_i g_i$$

This is the "correct" converse to the fact that if $f = \sum h_i g_i$, then $V(f) \supseteq V(g_1, \ldots, g_m)$. Note that the straight converse is false e.g. $f = x, g = x^2$.

It seems like Alon found the CNSS by considering simple special cases where the varieties are subcubes:

$$g_i = \prod_{s \in S_i} (x_i - s)$$

It's clear that $V(g_i) = \mathbb{F} \times \cdots \times \mathbb{F} \times S_i \times \mathbb{F} \times \cdots \times \mathbb{F}$, so $V(g_1, g_2, \ldots, g_n) = S_1 \times S_2 \times \cdots \times S_n$. Now if $f(x) = 0$ on this cube, what can we say about f? If $\mathbb{F}$ is algebraically closed, we could apply the Nullstellensatz. If we let $\mathbb{F}$ be arbitrary, the Nullstellensatz doesn't apply directly, but we might still conjecture the following:

Theorem (Theorem 1.1 in [Alo99])**.** *In the situation above,*

$$f = \sum_{i=1}^{n} h_i g_i$$

for some $h_i \in \mathbb{F}[x_1, \ldots, x_n]$, $\deg(h_i) \leq \deg(f) - \deg(g_i)$.

The degree bound is optimal. We can get $k = 1$ in the above because the g_i are particularly simple and univariate. This theorem was used by Alon to prove the CNSS.

From a complexity theory viewpoint, the above theorem states the completeness of a proof system for certifying $f \equiv 0$ on $S_1 \times \cdots \times S_n$: the proof consists of the polynomials h_i. However, the algorithmic problem of "given f and S_i, is f nonzero somewhere on $S_1 \times \cdots \times S_n$?" is not even in co-NP via this proof system because the polynomials h_i could have too many monomials.

2.1 An application of Theorem 1.1: k-coloring

Alon and others have produced many examples of certifying nonexistence of solutions to combinatorial problems via Theorem 1.1. Here is an example from Alon and Tarsi,

Lemma. *Let G be an undirected, simple graph. Define the graph polynomial*

$$f_G(\{x_u\}_{u \in V}) \stackrel{def}{=} \prod_{e=(u,v)} (x_u - x_v)$$

Then G is non-k-colorable $\Leftrightarrow$ f_G lies in $\mathbb{C}$-ideal generated by $\{x_u^k - 1\}$.

Proof. Name the polynomials $P_u = x_u^k - 1$.

($\Leftarrow$) Suppose $f_G \in \langle P_u \rangle$. Assume for the sake of contradiction that G is k-colorable via $\phi : V \to [k]$, we define

$$\begin{aligned} \chi : V &\to \mathbb{C} \\ v &\mapsto \omega^{\phi(v)} \end{aligned}$$

for ω a k-th root of unity. But $f_G(\{\chi(u)\}) \neq 0$ while $P_u(\chi(u)) = 0$.

($\Rightarrow$) If G isn't k-colorable, $f_G \equiv 0$ on $S_1 \times \cdots \times S_n$ for $S_i = \{\omega, \omega^2, \ldots, \omega^k\}$. By Theorem 1.1 above, $f_G = \sum h_u P_u$ so it lies in the ideal. □

Incidentally, we can think of $\chi : V \to \mathbb{C}$ in this case as a "nontrivial character" of the graph.

Note. *If we had some way to quickly check ideal membership, we could solve k-COLOR. We probably can't do that, but some modern research involves trying to solve special cases.*

3 Some applications of the CNSS

3.1 Finding regular subgraphs

There are several interesting theorems that revolve around finding regular structures (e.g. a 3-regular subgraph, not necessarily spanning or induced) inside of irregular graphs.

Theorem (Corollary of AFK ideas below)**.** *Every 4-regular graph contains a 3-regular subgraph.*

Theorem (Requires more work)**.** *If $k \geq 4r$, then k-regular H contains an r-regular subgraph.*

Theorem ([PRS95])**.** *If G has $200n \log n$ edges, then G contains a 3-regular subgraph.*
There is a matching lower bound of $\Omega(n \log \log n)$.

Theorem ([AFK84])**.** *Let G be a loopless graph and p prime. Suppose $\overline{\deg}(G) > 2p - 2$ and $\Delta(G) \leq 2p - 1$ i.e. the degree is concentrated around $2p - 1$.*
Then G has a p-regular subgraph.

Proof. (uses CNSS) Define the following polynomial over $\mathbb{F}_p$,

$$F(\{x_e\}) = \prod_v \left(1 - \left(\sum_{e \ni v} x_e\right)^{p-1}\right) - \prod_e (1 - x_e)$$

Raising the inner summation to the $(p-1)$-th power "booleanizes" the result to be either 0 or 1, by Fermat's Little Theorem.

Degree of the first term: $(p-1) \cdot n < m$ by assumption on $\overline{\deg}$ and the handshaking lemma.

Degree of the second term: m

The leading term comes from the second term, implying its coefficient is either ± 1 and it's multilinear. By CNSS on $\{0,1\}^n$, there are $y_e \in \{0,1\}$ such that $F(\{y_e\}) \neq 0$. This inspires the choice of subgraph,

$$H = \{\text{edges with } y_e = 1\}$$

Some $y_{e^*} = 1$ because $F(\vec{0}) = 0$, and this ensures the second term is zero on $\{y_e\}$. The first term can't be zero, so for every v

$$\sum_{e \ni v} y_e \equiv 0 \qquad \mod p$$

$\Delta(G) \leq 2p - 1$ implies the H-degrees are either 0 or p; the nonzero ones form our p-regular subgraph. □

3.2 Finding f-factors in graphs

Classically, a t-factor is a t-regular spanning subgraph of G. For $t = 1$, this is a perfect matching, and for $t = 2$ this is a collection of cycles. Modernly, an f-factor is a vast generalization. Given a function $f : V \to 2^{\{0,1,\ldots,d(v)\}}$, a spanning subgraph H is an f-factor if

$$\deg_H(v) \in f(v) \qquad \text{for every } v$$

That is, we're given a set of allowable vertex degrees at each vertex, and we must find a graph meeting all degree requirements.

Should we expect the Lovasz Local Lemma to apply? Early work in this area may have done this. If G is d-regular, and f includes all but one of of the degrees, we might expect it to. To apply LLL, under a random choice of subgraph we need the failure probabilities to be significantly less than $1/d$,

$$\Pr[v \text{ has illegal degree}] \leq \frac{1}{ed}$$

If the illegal degree is 75, say, then by Chernoff the failure probabilities are like $\exp(-d)$, which is small enough. But if the illegal degree is 50, we attain it with probability like $1/\sqrt{d}$, which is not small enough for LLL. This discrepancy perhaps suggests that LLL is not the right tool for this problem.

Theorem ([SV08])**.** *If $f(v)$ includes enough values, then G has an f-factor.*

Specifically, we require $|f(v)| \geq \left\lceil \frac{d(v)}{2} \right\rceil$.

This theorem is tight (but we may not show this in this course).

Proof. In this case, finding the right polynomial is easy, but arguing that its leading term is nonzero is the hard part. Define (over $\mathbb{R}$)

$$P(\{x_e\}) = \prod_v \prod_{a \in f(v)^c} \left(\sum_{e \ni v} x_e - a \right)$$

where $f(v)^c$ denotes the complement of $f(v)$ in $\{0, \ldots, d(v)\}$. We want to find a nonzero point $\vec{x} \in \{0,1\}^E$, hence to apply CNSS we must exhibit a leading multilinear term. The f-factor will just take those edges e with $x_e = 1$.

The degree of the function is clear from its representation. Every leading term will necessarily be a sum of 1's by multiplying. So, in order to show that there's a leading multilinear term, it suffices to create a function $g(v, a) = e \ni v$ that is injective. Intuitively, we want to orient edges to associate edges to endpoints. This suggests constructing an Euler tour, which is one way to "consistently orient" the edges.

The original graph may not have an Euler tour. To fix this, add a new vertex v^* connected to all odd-degree vertices. Let C be the Euler tour. Define

$$S_v = \{\text{non-fictitious edges in } C \text{ directed towards } v\}$$

where "non-fictitious" means "not incident to v^*". Facts about S_v:

- $S_u \cap S_v = \emptyset$ for distinct vertices u, v.
- $|S_v| = \begin{cases} \frac{d(v)}{2} & d(v) \text{ even} \\ \geq \frac{d(v)-1}{2} & d(v) \text{ odd} \end{cases} \geq |f(v)|^c$ by assumption on f.

Since $|S_v| \geq |f(v)|^c$, we can associate each $a \notin f(v)$ to a unique edge. □

3.3 Permanent Lemma

One more algebraic topic, then it's on to some complexity theory.

Define the permanent of a matrix,

$$\begin{aligned} \operatorname{per} A : \mathbb{F}^{n \times n} &\to \mathbb{F} \\ A &\mapsto \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)} \end{aligned}$$

The formula is the same as det without the $\operatorname{sign}(\sigma)$ term. Here are some facts about the permanent; before that, here's the definition of the complexity class #P:

Definition. #P *is the class of functions* $f : \{0,1\}^* \to \mathbb{N}$ *such that there is a polytime Turing machine* M *and a polynomial function* $t(n)$ *with*

$$f(x) = \left|\{y \in \{0,1\}^{t(|x|)} \mid M(x, y) = 1\}\right|$$

Example problems in #P are counting solutions to a 2SAT instance, counting perfect matchings in a graph, and counting the number of topological sorts of a digraph. It is a theorem of Toda that a Turing machine with an oracle for #Pcan decide every problem in PH (winnability of k-round games). #P also admits worst-case to average-case reductions: if we can solve 1% of inputs to a #P-hard problem, we can solve every instance to that problem with high probability.

- Lemma (Valiant's original paper defining permanent). Computing the permanent of a 0-1 matrix is #P-hard.
- $\mathbb{N}$-permanent is #P-complete
- $\mathbb{Z}$-permanent is #P-hard (and is complete under slightly more robust definitions)
- $\mathbb{Z}_3$-permanent is hard for the mod 3 version of #P

Back to the combinatorial lemma on per which is a useful theorem to know about:

Lemma. *Assume* $\operatorname{per}(A) \neq 0$ *for an* $n \times n$ *matrix* A. *Let* $S_1, S_2, \ldots, S_n \subseteq \mathbb{F}$ *of size 2.*

Then the vector $A\vec{x}$ *is still pretty unpredictable on the domain* $\vec{x} \in S_1 \times S_2 \times \cdots \times S_n$ *in the sense that*

$$\forall b \in \mathbb{F}^n. \quad \exists \vec{x} \in S_1 \times \cdots \times S_n. \quad \forall i \in [n]. \quad (A\vec{x})_i \neq b_i$$

Proof. Apply the CNSS.

$$P(\vec{x}) = \prod_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} x_j - b_i \right)$$

We want to show the polynomial P is nonzero on $S_1 \times \cdots \times S_n$. As usual, what are the leading coefficients? They're degree n, and $\operatorname{coef}(x_1 x_2 \cdots x_n) = \operatorname{per}(A) \neq 0$ by assumption. □

3.3.1 Application of the Permanent Lemma: Erdös-Ginzburg-Ziv

Theorem (Erdös-Ginzburg-Ziv)**.** *Let* p *be a prime,* $a_1, \ldots a_{2p-1} \in \mathbb{Z}_p$. *Then there is a subset* S *of exactly* p *elements such that*

$$\sum_{i \in S} a_i \equiv 0 \mod p$$

Proof. It's a cute one! WLOG $0 \leq a_1 \leq \cdots a_{2p-1} \leq p-1$.

If there is an i such that $a_i \equiv a_{i+p-1}$ then a_i through a_{i+p-1} are all the same and will work. Otherwise, we can "pair" a_i with a_{i+p-1}. Consider the $(p-1) \times (p-1)$ matrix of all 1's, and call it A. Then

$$\operatorname{per} A = (p-1)! \not\equiv 0 \mod p$$

because p is a prime (Wilson's theorem). Let $S_i = \{a_i, a_{i+p-1}\}$. Question: which values b to avoid in the statement of the permanent lemma? Let

$$b_1, \ldots, b_{p-1} = \mathbb{Z}_p \setminus \{-a_{2p-1}\}$$

By the lemma, there is x with $Ax \neq b$. But $(Ax)_i$ is the same for every i, equal to $\sum x_j$. The only possible value for this sum is then

$$\sum_j x_j \equiv -a_{2p-1}$$

This is a sum of $p-1$ elements up to a_{2p-2} with sum $-a_{2p-1}$, so adding in a_{2p-1} sums to 0. □

4 Computational complexity of CNSS problems

The next goal is to explore the complexity of some related problems. The most basic problem is the following:

Problem: Given an arithmetic circuit C, find x such that $C(x) \neq 0$.

When the degree of the circuit is small relative to the field size, the Schwarz-Zippel lemma tells us that there are many nonzero points (then a random x is likely to work, assuming C is not uniformly zero). Derandomizing this construction would imply new circuit lower bounds [KI04]. Even if the total degree of the circuit is not small, if the degree of each variable is small relative to the field size, then the CNSS tells us at least one nonzero point exists; however, it's not clear how to produce such an x.

Note that an easy reduction shows this problem is NP-hard: arithmetize a boolean circuit (that uses $O(1)$ occurrences of each variable), then finding a nonzero x solves CIRCUIT-SAT. In these cases, the field size is 2, while the degree of each variable is $O(1) > 2$, so the NP-hardness reduction is not immediately an obstruction to a potential CNSS constructivization. However, [Alo] noted that there is a family of "hard examples" for constructive CNSS based on one-way permutations.

Definition. *A one-way permutation (OWP) is a family of functions* $\{f_n\}, f_n : \{0,1\}^n \to \{0,1\}^n$ *such that*

- f_n *is a permutation*
- f_n *is polytime computable*
- *Any probabilistic polytime Turing machine cannot compute* $f^{-1}(x)$ *on random* x*.*

Let $\mathbb{F} = \mathbb{F}_2$, say $\{C_n\}$ compute $\{f_n\}$. Arithmetize these to arithmetic circuits $\{A_n\}$, and define the polynomials

$$P_y(x_1, \ldots, x_n) = \prod_{i=1}^{n} (A_{n,i}(x) \oplus y_i \oplus 1)$$

Here $y \in \mathbb{F}_2^n$ is fixed to an element of our choosing. The point is that P_y has a unique nonzero input in $\mathbb{F}_2^n$ at $x = f_n^{-1}(y)$. When reduced to a multilinear polynomial, P_y has full degree, as this is the only way for a multilinear boolean function to have odd support size. Hence if we had a constructive version of the CNSS, we could produce this x and break the one-way permutation.

This is a little unsatisfying of an example, because the function P_y is only semantically multilinear, and not syntactically so.

4.1 The Chevalley-Warning problem and PPA

Let's just restrict ourselves to the case $\mathbb{F}_2$ for the moment, and review the statements of the CNSS and Chevalley-Warning theorem in this setting.

- (CNSS_2) If $P \in \mathbb{F}_2[x_1, \ldots, x_n]$ is multilinear and $\deg(P) = n$, then there is $a \in \{0,1\}^n$ such that $P(a) = 1$.
- ($\text{Chevalley-Warning}_2$) If $\deg(P) < n$ and $P(a) = 0$, then there is $b \neq a$ such that $P(b) = 0$.

Over $\mathbb{F}_2$, the statements are easily mutually reducible:

Proof. [$\text{CNSS}_2 \implies \text{CW}_2$] Define

$$Q(x_1, \ldots x_n) = P(x) \oplus (x_1 \oplus a_1 \oplus 1)(x_2 \oplus a_2 \oplus 1) \cdots (x_n \oplus a_n \oplus 1) \oplus 1$$

Q has degree n, so apply CNSS_2 to Q to find b with $Q(b) = 1$. We must have $b \neq a$ and $P(b) = 0$.

[$\text{CW}_2 \implies \text{CNSS}_2$] If $P(\vec{1}) = 1$, then we're done! Otherwise, let

$$Q(x_1, \ldots, x_n) = P(x) \oplus x_1 x_2 \cdots x_n \oplus 1$$

$Q(\vec{1}) = 0$ by assumption, and apply CW_2 to produce another zero. The degree of Q is strictly less than n because the n-degree term of P is killed off. □

The statement of the Chevalley-Warning theorem suggests certain circuits

$$P(x) = \prod_{i=1}^{m} (1 + P_i(x))$$

and a certain computational problem (introduced by [Pap94]) that we shall call the "$\mathbb{F}_2$ Chevalley problem":

Problem: Given P as above and a such that $P(a) \neq 0$, find $b \neq a$ such that $P(b) \neq 0$.

By the Chevalley-Warning theorem such a b always exists. It isn't immediately obvious how to produce b, however. There are actually several related questions depending on how the polynomials P_i are specified (for example, as a list of monomials or as small arithmetic circuits).

In the next lecture, we'll show how to reduce the Chevalley problem to the language of graph theory. That is, we'll show how to reduce it to following trivial-looking combinatorial property of graphs:

Problem: Given a graph G and an odd degree vertex, find another odd degree vertex.

This problem in turn reduces to the problem of finding a second leaf in a graph with degrees at most 2, given a first leaf. These problems are members of the class PPA (Polynomial Parity Argument), and the existence of this reduction informally implies that we can prove the Chevalley-Warning theorem over $\mathbb{F}_2$ using the handshaking lemma on a certain graph.

References

[AFK84] Noga Alon, Shmuel Friedland, and Gil Kalai. Regular subgraphs of almost regular graphs. *Journal of Combinatorial Theory, Series B*, 37(1):79–91, 1984.

[Alo] Noga Alon. Discrete mathematics: methods and challenges.

[Alo99] Noga Alon. Combinatorial nullstellensatz. *Combinatorics, Probability and Computing*, 8(1-2):7–29, 1999.

[Hei] Peter Christian Heinig. Proof of the combinatorial nullstellensatz over integral domains in the spirit of kouba.

[KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *computational complexity*, 13(1-2):1–46, dec 2004.

[Kou09] Omran Kouba. A duality based proof of the combinatorial nullstellensatz. *the electronic journal of combinatorics*, 16(1):9, 2009.

[Pap94] Christos H. Papadimitriou. On the complexity of the parity argument and other inefficient proofs of existence. *Journal of Computer and System Sciences*, 48(3):498–532, jun 1994.

[PRS95] László Pyber, Vojtech Rodl, and Endre Szemerédi. Dense graphs without 3-regular subgraphs. *Journal of Combinatorial Theory, Series B*, 63(1):41–54, 1995.

[SV08] Hamed Shirazi and Jacques Verstraëte. A note on polynomials and f-factors of graphs. *the electronic journal of combinatorics*, 15(1):22, 2008.