Counterexamples to the Low-Norm Nullstellensatz Hypothesis

Alex Lombardi
Princeton

May 29, 2026

Abstract

We give several examples of families of polynomials $p_1, \ldots, p_t \in \mathbb{R}[x_1, \ldots, x_n]/\langle x_i^d - 1\rangle_i$ on which the Low-Norm Nullstellensatz Hypothesis of [Devadas-Hopkins-Kalai-Kothari-Lombardi-Mathialagan, STOC 2026] fails to hold. That is, we prove the existence of polynomials $f \in \langle p_1, \ldots, p_t\rangle$ with coefficient L^1 norm $||f||_1 = 1$ but such that every decomposition $f = \sum_i p_i \cdot q_i$ has cost $\sum_i ||q_i||_1 = 2^{\Omega(n)}$. Our examples include one with $d = 2$, the regime originally studied by [Devadas et al.], as well as generalizations that would also have sufficed for their purposes.

Our counterexamples highlight an important class of polynomials for (potentially) falsifying the LNNH: for prime d, functions $f(x) = f_C(x) = \frac{1}{|C|}\sum_{c\in C} x^c$ that are indicator functions for the input $x \in \mu_d^n \simeq \mathbb{Z}_d^n$ belonging to a linear subspace $C^\perp \subset \mathbb{Z}_d^n$, or more generally a coset $C^\perp + \sigma$.

Contents

1 Introduction **3**
- 1.1 Our Results . . . 3
- 1.2 Implications and Open Questions . . . 4

2 Dual Certificates for Nullstellensatz **5**

3 Counterexample Polynomials: (Dual) Subspace Membership **6**

4 Combinatorial Rectangles of Side Length $d-1$ **6**
- 4.1 The Dual Certificate . . . 7

5 Counterexample with $d=2$ **8**

6 Counterexample using a rectangle with smaller side length **9**

1 Introduction

Let $p_1, \ldots, p_t \in \mathbb{C}[x_1, \ldots, x_n]/\langle x_i^d - 1\rangle_i$ be multivariate polynomials with exponents taken modulo d. This polynomial ring is equivalent to the ring of functions mapping $\mu_d \to \mathbb{C}$, where μ_d denotes the set of dth roots of unity. When specialized to this ring, Hilbert's Nullstellensatz implies that any f vanishing on the common zero set of $p_1, \ldots, p_t$ must lie in the ideal $\langle p_1, \ldots, p_t\rangle$, meaning that there exist polynomials $q_1, \ldots, q_t$ such that

$$f = \sum_i p_i \cdot q_i$$

over the ring. When $d = 2$, or whenever $p_1, \ldots, p_t$ have real coefficients, it is also reasonable to consider the question restricted to $\mathbb{R}[x_1, \ldots, x_n]/\langle x_i^d - 1\rangle_i$, where the same statement holds.

Recently, a work of Devadas et al. [DHK+26] asked whether such decompositions (in the case $d = 2$) have to be *small*. Their metric was the coefficient L^1 norm, denoted $||f||_1$, defined to be the sum of the absolute values of the coefficients. Namely, they defined the ideal basis $p_1, \ldots, p_t$ to be "Nullstellensatz-friendly" if for all $f \in \langle p_1, \ldots, p_t\rangle$, there exists a decomposition $f = \sum_i p_i \cdot q_i$ such that

$$\sum_i ||q_i||_1 \leq \mathsf{poly}(n) \cdot ||f||_1.$$

For any such collection $p_1, \ldots, p_t$, the **low-norm Nullstellensatz hypothesis** (LNNH) is precisely the conjecture that such decompositions exist.

[DHK+26] are interested in the LNNH because of applications to the construction of succinct non-interactive arguments (SNARGs) for NP. They prove [DHK+26, Theorem 5.4] that in the special case $d = 2$, a SNARG for NP can be constructed under standard cryptographic assumptions provided the existence of a family of polynomials $p_1, \ldots, p_t$ satisfying the LNNH along with a couple of additional properties:

- The polynomials $p_i(x)$ have constant locality and constant L^1 norm.
- A certain computational problem $k\mathsf{Lin}(\mathcal{C})$ (where $\mathcal{C}$ is the vanishing set of $p_1, \ldots, p_t$) is NP-hard.

In fact, while it is not explicitly stated in the paper, an analogous result holds for larger values of d.[1]

Thus, we are highly motivated to understand whether and when the LNNH is true. Thus far, extremely little was known:

- It was observed in [DHK+26] (following, e.g., [CMS20]) that if the polynomials $p_i(x)$ are all monomials (defining linear constraints modulo d) then the LNNH holds, but these families are not cryptographically useful.
- A recent work of Potechin and Zhang [PZ24] give a counterexample where $\langle p_1, \ldots, p_t\rangle = \langle 1\rangle$ is the entire ring (the p_j have empty common zero set), but in a significantly different setting:
  - they work over the ring of polynomials modulo $\langle x_i^2 - x\rangle$ (i.e., $\{0, 1\}$-input rather than $\{\pm 1\}$), and
  - their polynomials p_j have superconstant locality.

1.1 Our Results

In this work, we *refute* the low-norm Nullstellensatz for several polynomial families of interest. In particular, we highlight the following examples:

1. Take $d = 3$, and let $p_1, \ldots, p_n \in \mathbb{R}[x_1, \ldots x_n]/\langle x_i^3 - 1\rangle_i$ be defined as $p_i(x) = \frac{1}{3}(1 + x_i + x_i^2)$. That is, $p_i(x)$ is the indicator function for $x_i = 1 \in \{1, \omega, \omega^2\}$. The common vanishing set is $\{\omega, \omega^2\}^n$.

[1] Essentially, all that is required in their construction is replacing the $\mathbb{Z}_2$ linearity test with the analogous $\mathbb{Z}_d$ linearity test.

2. Take $d = 5$, and let $p_1, \ldots, p_n \in \mathbb{R}[x_1, \ldots, x_n]/\langle x_i^5 - 1\rangle_i$ be defined as $p_i(x) = \chi(x_i \in \{\omega, \omega^{-1}\}) = \frac{1}{5}\sum_{k=0}^{4}(\omega^k + \omega^{-k})x_i^k$ for a 5th root of unity ω. The common zero set is $\{1, \omega^2, \omega^3\}^n$.
3. Take $d = 2$, and work with $2n$ variables $x_1, \ldots, x_n, y_1, \ldots, y_n$. Define $p_i(x, y) = \frac{1}{4}(1+x_i)(1+y_i)$, which is 1 if and only if $x_i = y_i = 1$. The common vanishing set is $\{(1,-1),(-1,1),(-1,-1)\}^n$.

We emphasize that any of these examples would have been cryptographically useful, and indeed examples (1) and (3) are extremely natural alternatives to the "AND code" highlighted by [DHK+26]. Unfortunately, we prove:

Theorem 1.1. *The sets of polynomials in examples (1), (2), and (3) above do not satisfy the low-norm Nullstellensatz hypothesis. In fact, there exist polynomials $f \in \langle p_1, \ldots, p_n\rangle$ such that $||f||_1 = 1$ but for any Nullstellensatz decomposition $f = \sum_i p_i \cdot q_i$, we have that $\sum_i ||q_i||_1 \geq 2^{\Omega(n)}$.*

Moreover, our proof technique suggests that in general, when $p_1, \ldots, p_t$ are defined on *disjoint* sets of variables, counterexamples are likely to exist.

Concurrent work. In concurrent and independent work, Jin [Jin26] falsifies the low-norm Nullstellensatz hypothesis for the AND code highlighted by [DHK+26]. In contrast, our counterexamples are for alternative polynomial systems that (if LNNH were true) would also have sufficed for the purposes of [DHK+26].

In another concurrent work, Bloom and Kim [BK26] independently discovered a counterexample for system (1) and an alternative generalization (involving side length 2 rectangles) to what is in Section 4.

1.2 Implications and Open Questions

Theorem 1.1 refutes several low-norm Nullstellensatz hypotheses for natural candidate polynomial systems of interest for SNARG constructions [DHK+26]. In conjunction with [Jin26], this casts doubt on the LNNH more broadly. However, it remains wide open to attack the LNNH in full generality. Outside of "trivial" examples such as linear subspaces, is there some fundamental reason why LNNH cannot hold? Or is there a more clever choice of $p_1, \ldots, p_t$ for which LNNH does hold?

In fact, we can ask this question even about a specific sub-problem of the LNNH, based on the structure of our counterexample polynomials f. For d prime and for any linear subspace $C \subset \mathbb{Z}_d^n$, define the dual code membership polynomial

$$f_C(x_1, \ldots, x_n) = \frac{1}{|C|}\sum_{c \in C} x_1^{c_1} \ldots x_n^{c_n},$$

which computes the indicator function of $C^\perp = \{a \in \mathbb{Z}_d^n : a \cdot c = 0 \text{ for all } c \in C\}$ on the exponent of $x = \omega_d^a$. We informally ask

Question 1.2. Do there exists non-trivial examples of $p_1, \ldots, p_t$ such that the LNNH holds for all polynomials of the form f_C?

Technically, this restriction of LNNH is vacuous if $V = V(p_1, \ldots, p_t)$ contains 1^n because $f_C(1^n) = 1$ for all C. However, one can ask the same question for *coset* polynomials

$$f_{C,\sigma}(x_1, \ldots, x_n) = \frac{1}{|C|}\sum_{c \in C} \omega_d^{-c\cdot\sigma} x^c,$$

which computes the indicator function for the coset $C^\perp + \sigma$.

Finally, we remark that in [DHK+26], the LNNH was used to prove the non-signaling soundness of an exponential length probabilistically checkable proof for NP (which in turn guarantees the computational soundness of a candidate SNARG). Our refutations of LNNH do not appear to extend to attacks on the corresponding candidate nsPCPs, and thus it also remains wide open to analyze the non-signaling soundness of these very simple candidate nsPCPs. While polynomial-length PCPs cannot even have non-trivial (< 1)

non-signaling soundness error [KRR14], [DHK+26] proved that the Hadamard PCP does have soundness error strictly less than 1. The question is if such PCPs have non-signaling soundness error $1 - 1/\mathsf{poly}(n)$.

We now proceed to prove Theorem 1.1.

2 Dual Certificates for Nullstellensatz

Throughout, we work over the ring

$$\mathcal{R}_{d,\mathbb{C}} = \mathbb{C}[x_1, \ldots, x_n]/\langle x_i^d - 1\rangle_i,$$

whose monomials are indexed by exponent vectors

$$a = (a_1, \ldots, a_n) \in (\mathbb{Z}/d\mathbb{Z})^n, \qquad x^a = x_1^{a_1} \cdots x_n^{a_n},$$

or the real coefficient analogue

$$\mathcal{R}_{d,\mathbb{R}} = \mathbb{R}[x_1, \ldots, x_n]/\langle x_i^d - 1\rangle_i.$$

For a polynomial $f = \sum_a \widehat{f}(a)x^a$, we write $\|f\|_1 = \sum_a |\widehat{f}(a)|$ for the coefficient L^1 norm (also known as the Fourier L^1 norm).

Definition 2.1 (Nullstellensatz Certificate Complexity)**.** Fix some polynomials $p_1, \ldots p_t \in \mathcal{R}$. For any $f \in \langle p_1, \ldots, p_t\rangle$, define its Nullstellensatz certificate complexity by

$$\Phi(f) := \inf\left\{\sum_j \|q_j\|_1 : f = \sum_j p_j q_j\right\}.$$

Using a form of (weak) convex program duality (LP duality in the case of real coefficients), we can define a *dual certificate* that guarantees a lower bound on $\Phi(f)$.

Definition 2.2 (Dual Nullstellensatz Certificate)**.** For any $f \in \langle p_1, \ldots, p_t\rangle$, we say that a polynomial $g \in \mathcal{R}$ certifies that $\Phi(f) \geq v$ if the following two conditions hold:

- For every $j \in [t]$, $||\overline{p_j} \cdot g||_\infty \leq 1$, where $||\cdot||_\infty$ denotes the infinity norm of the coefficient vector.
- The real part of $\langle g, f\rangle = \mathop{\mathbb{E}}_{x \leftarrow \mu_d^n}\left[\overline{f(x)} \cdot g(x)\right]$ is at least v.

To see that such a g indeed certifies that $\Phi(f) \geq v$, suppose that $f = \sum_i p_i \cdot q_i$. Then, we have that

$$\mathrm{Re}\langle g, f\rangle \leq |\langle g, f\rangle| = \left|\sum_j \langle g, p_j \cdot q_j\rangle\right| = \left|\sum_j \langle g \cdot \overline{p_j}, q_j\rangle\right| \leq \sum_j ||g \cdot \overline{p_j}||_\infty ||q_j||_1 \leq \Phi(f).$$

We remark that this dual certificate applies in both the real and complex coefficient cases. In the real case, the conditions simplify to:

- for every $j \in [t]$, $||p_j \cdot g||_\infty \leq 1$, and
- $\langle g, f\rangle = \mathop{\mathbb{E}}_{x \leftarrow \mu_d^n}\left[f(x) \cdot g(x)\right] \geq v$.

Indeed, in the event that all p_j have real coefficients, the real and complex optimization problems are *equivalent* (we omit the proof for brevity and because it is not needed).

3 Counterexample Polynomials: (Dual) Subspace Membership

Let d be a prime, and let $C \subset \mathbb{Z}_d^n$ denote a linear subspace of dimension m; we will also refer to C as a linear code. Define the dual subspace (or dual code)

$$C^\perp = \{a \in \mathbb{Z}_d^n : \langle a, c\rangle = 0 \text{ for all } c \in C\}.$$

Then, define the dual subspace membership polynomial

$$f_C(x) = \frac{1}{|C|}\sum_{c\in C} x^c,$$

which computes the function $(\omega_d^{a_1}, \ldots, \omega_d^{a_n}) \mapsto \chi(a \in C^\perp)$.

Our counterexamples will use *random* dual subspace membership polynomials.

Lemma 3.1. *Let $p_1, \ldots, p_t$ have common zero set $V \subset \mu_d^n$, and suppose that $1^n \notin V$. Then, if C is a uniformly random m dimensional subspace of $\mathbb{Z}_d^n$, we have that*

$$\Pr\Big[f_C \text{ vanishes on } V\Big] \geq 1 - \frac{|V|}{d^m}.$$

Proof. For any $V \subset \mu_d^n$, let $W \subset \mathbb{Z}_d^n$ be the corresponding set of exponent vectors. Then, f_C vanishes on V if and only if $W \cap C^\perp = \emptyset$. Each element of W is nonzero and thus is an element of $C^\perp$ with probability exactly d^{-m}. The result follows by a union bound. □

For an appropriate choice of m, f_C will indeed vanish on V, and it has L^1 norm equal to 1. Thus, to produce counterexamples, it now suffices to prove exponential lower bounds on $\Phi(f)$.

4 Combinatorial Rectangles of Side Length $d-1$

We first consider polynomials in $\mathbb{R}[x_1, \ldots, x_n]/\langle x_i^d - 1\rangle$ of the following form:

$$p_i(x) = \frac{1}{d}\sum_{a=1}^{d} x_i^a.$$

This polynomial computes the function $\omega_d^a \mapsto \chi(a = 0)$. Thus, the common vanishing set $V = V(p_1, \ldots, p_n) = \{\omega_d, \ldots, \omega_d^{d-1}\}^n$ has $(d-1)^n$ out of d^n points.

As a result, we have that a random f_C vanishes on V with high probability whenever

$$(d-1)^n \ll d^m,$$

i.e.,

$$m \geq \frac{\log(d-1)}{\log d}\cdot n + O(\frac{1}{\log d}).$$

Indeed, let us set $m = \frac{\log(d-1)}{\log d}\cdot n + O(\frac{1}{\log d})$ to be slightly larger than $\frac{\log(d-1)}{\log d}\cdot n$. In the rest of this section, we prove lower bounds on $\Phi(f)$ in terms of the *minimum distance* $\Delta(C)$ of the linear code $C \subset \mathbb{Z}_d^n$, i.e.,

$$\Delta(C) = \min_{c\in C}\Big[||c||_H\Big],$$

or the minimum Hamming weight of a codeword. For this setting of parameters, standard results from coding theory tell us that with high probability over C, asymptotically

$$H_d\Big(\frac{\Delta(C)}{n}\Big) \geq 1 - \frac{m}{n} \approx 1 - \frac{\log(d-1)}{\log d},$$

where H_d denotes the d-ary entropy function. Thus, for any constant d, C will typically have minimum distance $\Omega(n)$.

4.1 The Dual Certificate

Recall that a polynomial $g \in \mathcal{R}_{d,\mathbb{R}}$ is dual-feasible if for all $i \in [n]$,

$$||p_i \cdot g||_\infty \leq 1.$$

To understand this, we observe that multiplication p_i induces the following transformation on coefficient vectors:

$$\widehat{p_i g}(a_1, \ldots, a_n) = \frac{1}{d} \sum_{r=0}^{d-1} \widehat{g}(a_1, \ldots, a_{i-1}, a_i - r, a_{i+1}, \ldots, a_n),$$

so coefficients are averaged across exponent vectors with varying a_i.

Theorem 4.1 (Exponential lower bound from minimum distance). *Let $\Delta = \Delta(C)$ and let $R = \lfloor \frac{\Delta}{2} \rfloor - 1$. Then,*

$$\Phi(f_C) \geq d \cdot (d-1)^R = d^{\Omega(R)}.$$

In particular, if $\Delta(C) = \Omega(n)$, then

$$\Phi(f_c) \geq d^{\Omega(n)}.$$

Proof. By construction, we have that C satisfies the following property.

Claim 4.2. *For every a within Hamming distance R of the code C, let $\delta = \delta(a) \leq R$ denote the distance from a to C. Then, for every $i \in [n]$, the points $\{(a_1, \ldots, a_{i-1}, a_i - r, a_{i+1}, \ldots, a_n)\}_r$ either all have distance $\{\delta, \delta - 1\}$ from C or all have distance $\{\delta, \delta + 1\}$ from C.*

Moreover, the smaller of the two distances occurs exactly once within this set.

Proof. Let c be the nearest codeword to a. Then either $a_i = c_i$ or $a_i \neq c_i$. Because $\delta(a) \leq R \leq \frac{\Delta}{2} - 1$, the nearest codeword to the shifts of a is also c. In the first case, all of the shifts have distance $\delta + 1$, while in the second case, all of the shifts have distance δ except for one (which has distance $\delta - 1$). □

This structure will allow us to define a good dual certificate. For $0 \leq \delta \leq R$, define the amplitude

$$\phi_\delta = (-1)^\delta \cdot d \cdot (d-1)^{R-\delta}$$

for $\delta \leq R$, and $\phi_\delta = 0$ otherwise. We define the polynomial g to have coefficients

$$\widehat{g}(a) = \phi_{\delta(a)}.$$

We now claim that g is a valid dual certificate.

Claim 4.3. *For all $i \in [n]$, $||p_i \cdot g||_\infty \leq 1$.*

Proof. We begin with the formula

$$\widehat{p_i g}(a) = \frac{1}{d} \sum_{r=0}^{d-1} \widehat{g}(a_1, \ldots, a_{i-1}, a_i - r, a_{i+1}, \ldots, a_n).$$

We want to show that $|\widehat{p_i g}(a)| \leq 1$ for all i and all a. To see this, we note that for all i and all a with distance δ from C, the vectors in the sum have distances either $(\delta - 1, \delta, \ldots, \delta)$ or $(\delta, \delta + 1, \ldots, \delta + 1)$ from C. Thus, every coefficient of $p_i g$ can be expressed as

$$\frac{1}{d} \cdot (\phi_\delta + (d-1) \cdot \phi_{\delta+1})$$

for some non-negative integer δ.

We now break into cases.

- If $\delta > R$, then the coefficient is 0.
- If $\delta = R$, then the coefficient is
$$\frac{1}{d}\phi_R = (-1)^R.$$
- If $\delta \leq R$, then the coefficient is
$$\frac{1}{d}(\phi_\delta + (d-1)\phi_{\delta+1}) = 0.$$ □

Dual Certificate Value. Finally, on each codeword $c \in C$ we have $\widehat{g}(c) = \phi_0$, so the dual certificate value is given by
$$\langle g, f\rangle = \frac{1}{|C|}\sum_{c\in C}\widehat{g}(c) = \phi_0 = d\cdot(d-1)^R.$$
This completes the proof of Theorem 4.1. □

Thus, we conclude that with high probability over C, f_C vanishes on V, $||f||_1 = 1$, but $\Phi(f_C) = d^{\Omega(n)}$.

5 Counterexample with $d = 2$

Our first counterexample gives an exponential lower bound for a family of polynomials for every prime $d \geq 3$. For our second counterexample, we work over the ring
$$\mathbb{R}[x_1, y_1, \ldots, x_n, y_n]/(x_i^2 - 1, y_i^2 - 1)$$
and define
$$p_i(x, y) = \frac{1}{4}(1 + x_i)(1 + y_i),$$
which on input $((-1)^a, (-1)^b)$ computes the function $\chi((a_i, b_i) = (0, 0))$. The vanishing set V is then $\{(-1, 1), (1, -1), (-1, -1)\}^n$ and has 3^n out of 4^n possible points.

We will build our counterexample very similarly to the previous section. Sample a random subspace $C \subset \mathbb{Z}_2^{2n}$ of dimension m. Then, we know that f_C vanishes on V with probability at least $1 - \frac{3^n}{4^m}$, so we will set m slightly larger than $\log_4(3)\cdot n$.

The only difference from the previous section is that each polynomial p_i involves *two* variables rather than one, and thus multiplication by p_i mixes four coefficients rather than $d = 2$. However, the p_i still act on disjoint variable sets. Thus, the relevant metric in this section is the *block distance*
$$\Delta = \Delta_{\{0,1\}^2}(C),$$
which is the minimum Hamming weight of a codeword $c \in \mathbb{Z}_2^{2n} \simeq (\{0, 1\}^2)^n$, where C is identified as a code with block length n over an alphabet $\Sigma = \{0, 1\}^2$.

By another standard calculation from coding theory, we know that asymptotically,
$$H_4(\Delta_{\{0,1\}^2}(C)/n) \geq 1 - \frac{m}{n},$$
so for our choice of m we will have that $\Delta = \Omega(n)$ with high probability.

Thus, we will again set $R = \lfloor \frac{\Delta}{2} \rfloor - 1$, define amplitudes
$$\phi_\delta = (-1)^\delta \cdot 4 \cdot 3^{R-\delta},$$
(with $\phi_\delta = 0$ for $\delta > R$) and define dual certificate g with the coefficients
$$\widehat{g}(a) = \phi_{\delta(a)},$$

where $\delta(a)$ is now defined to be the block distance from a to C. The dual value of g can again be calculated as

$$\langle g, f \rangle = \phi_0 = 4 \cdot 3^R.$$

Moreover, we will again have that $||p_i \cdot g||_\infty \leq 1$, because every coefficient of $p_i \cdot g$ will have the form

$$\frac{1}{4}(\phi_\delta + 3 \cdot \phi_{\delta+1}),$$

which is upper bounded by 1 in absolute value by the same calculation as in the previous section.

As we have $R = \Omega(n)$ with high probability, we have thus proved the lower bound

$$\Phi(f_C) = 2^{\Omega(n)}$$

with high probability over C.

6 Counterexample using a rectangle with smaller side length

Finally, we give an example where each local polynomial cuts out a set of two symbols rather than one symbol. The proof is similar in spirit to the previous two sections, but a somewhat more careful choice of dual certificate g is required.

Let ω be a primitive fifth root of unity. We work over

$$\mathbb{C}[x_1, \ldots, x_n]/\langle x_i^5 - 1 \rangle_i$$

and define

$$p_i(x) = \frac{1}{5} \sum_{k=0}^{4} (\omega^k + \omega^{-k}) x_i^k.$$

If $x = \omega^a$, then

$$p_i(\omega^a) = \chi(a_i \in \{1, 4\}).$$

Thus the common zero set is

$$V = \{1, \omega, \omega^2\}^n.$$

Notice that $1^n \in V$. Therefore the unshifted polynomial f_C from the previous sections cannot vanish on V, since $f_C(1^n) = 1$. For this reason we use code *coset* polynomials in this section.

Let $C \subset \mathbb{Z}_5^n$ be a linear subspace of dimension m and let $\sigma \in \mathbb{Z}_5^n$. Define

$$f_{C,\sigma}(x) = \frac{1}{|C|} \sum_{c \in C} \omega^{-\sigma \cdot c} x^c.$$

On the input $x_i = \omega^{a_i}$, this polynomial computes the indicator of the coset $\sigma + C^\perp$:

$$f_{C,\sigma}(\omega^a) = \chi(a \in \sigma + C^\perp).$$

Therefore $f_{C,\sigma}$ vanishes on V exactly when

$$(\sigma + C^\perp) \cap \{0, 2, 3\}^n = \emptyset.$$

For a fixed C of dimension m and a random shift σ, each point of $\{0, 2, 3\}^n$ lies in $\sigma + C^\perp$ with probability 5^{-m}. Hence, by a union bound,

$$\Pr_\sigma \left[(\sigma + C^\perp) \cap \{0, 2, 3\}^n \neq \emptyset \right] \leq \frac{3^n}{5^m}.$$

Thus, if m is slightly larger than $\log_5(3)n$, then a random shift makes $f_{C,\sigma}$ vanish on V with high probability. As discussed in Section 4, for such choices of m, a random linear code C also has minimum distance $\Delta(C) = \Omega(n)$ with high probability.

We now prove that these $f_{C,\sigma}$ have large certificate complexity whenever C has large minimum distance. The only new ingredient is the following single-variable polynomial.

Claim 6.1. *Let the univariate polynomial $h(z)$ be defined as*

$$h(z) = \frac{1}{\sqrt{5}} \cdot (\sqrt{5} - z + z^2 + z^3 - z^4)$$

Then

$$h(\omega) = h(\overline{\omega}) = 0,$$

which implies that

$$h(x_i) \cdot p_i(x) = 0.$$

Proof. Since h has real coefficients, it suffices to check that $h(\omega) = 0$. To see this, observe that

$$\omega + \omega^4 = 2\cos(2\pi/5), \qquad \omega^2 + \omega^3 = 2\cos(4\pi/5),$$

and so

$$h(\omega) = \frac{1}{\sqrt{5}} \cdot (\sqrt{5} - (\omega + \omega^4) + (\omega^2 + \omega^3)) = \frac{1}{\sqrt{5}} \cdot (\sqrt{5} - 2\cos(2\pi/5) + 2\cos(4\pi/5)) = 0.$$

For the final conclusion, we recall that $p_i(\omega^a)$ computes the function $\chi(a_i \in \{1, 4\})$, so $h(x_i) \cdot p_i(x)$ indeed vanishes on all inputs in μ_5^n. □

Next, we produce a polynomial $g_0(x_1, \ldots, x_n)$ with an exponentially large constant term, but such that $||p_i \cdot g_0||_\infty \leq 1$. To do this, let $R = \lfloor \frac{\Delta}{2} \rfloor - 1$ as before.

Then, define

$$g_0(x_1, \ldots, x_n) = \sqrt{5}^{R-1} \cdot \Big(\prod_{i=1}^{n} h(x_i) \Big)|_{||a||_H \leq R}.$$

By this, we mean we take the polynomial $\sqrt{5}^{R-1} \cdot \prod_{i=1}^{n} h(x_i)$ and remove all monomials with exponent vectors $a \in \mathbb{Z}_5^n$ with Hamming weight larger than R.

We claim that

$$||p_j \cdot g_0||_\infty \leq ||p_j||_1 = O(1).$$

To prove this, we use the fact that $p_j(x) \cdot \prod_{i=1}^{n} h(x_i) = 0$. Therefore,

$$p_j(x) \cdot g(x) = -p_j \cdot \Big((\sqrt{5})^R \cdot \prod_{i=1}^{n} h_i(x) \Big)|_{||a||_H > R}.$$

By construction, every coefficient of $\Big((\sqrt{5})^{R-1} \cdot \prod_{i=1}^{n} h_i(x) \Big)|_{||a||_H > R}$ has absolute value at most $\frac{1}{5}$. Thus, we have that

$$||p_i \cdot g_0||_\infty \leq ||p_i||_1.$$

Finally, to construct our dual certificate, we simply take

$$g(x) = g_0(x) \cdot \sum_{c \in C} \omega^{-c \cdot \sigma} x^c.$$

The key feature of this example, just as was the case for our previous certificates, was that the coefficients of $p_i(x) \cdot g_0(x) \cdot \sum_{c \in C} \omega^{-c \cdot \sigma} x^c$ associated with different codewords c do not interact (because of the cutoff of coefficients of $g_0(x)$ at Hamming weight $R \leq \Delta/2 - 1$). Thus, we have that

$$||p_i \cdot g||_\infty = ||p_i \cdot g_0||_\infty = O(1).$$

On the other hand, by construction, we have that

$$\langle g, f_{C,\sigma} \rangle = \widehat{g}_0(0) = \sqrt{5}^{R-1}.$$

Thus, rescaling g by a constant, we have proved that

$$\Phi(f_{c,\sigma}) = \sqrt{5}^{\Omega(R)} = 2^{\Omega(n)}$$

with high probability over (C, σ), as claimed.

Acknowledgements

A.L. thanks Lali Devadas, Sam Hopkins, Yael Kalai, Pravesh Kothari, and Surya Mathialagan for many helpful discussions. A.L. also thanks Violet Bloom and Gwanho Kim for helpful discussions and for sharing a write-up proving some special cases of the AND code LNNH.

AI Assistance. The counterexample polynomials and dual certificates presented here were generated interactively in a dialogue with ChatGPT 5.5 Pro. In particular, the counterexample polynomials were proposed generalizations of a particular example polynomial

$$f(x_1, x_2, x_3, x_4) = \frac{1}{9} \sum_{\substack{c \in \mathrm{Span}\{(1,1,1,0),\\ (2,1,0,1)\}}} x^c$$

which was generated via a (symmetrized) exhaustive search over the vertices of the convex polytope

$$P_V = \{f \in \mathbb{R}[x_1, x_2, x_3, x_4]/\langle x_i^3 - 1 \rangle : ||f||_1 \leq 1 \text{ and } f(V) \equiv 0\} \subset \mathbb{R}^{81}.$$

for the vanishing set $V = \{\omega, \omega^2\}^4 \subset \{1, \omega, \omega^2\}^4$. Over P_V, this polynomial has the globally maximal Nullstellensatz certificate complexity and generalizes to give our first family of counterexamples.

References

[BK26] Violet Bloom and Gwanho Kim, 2026. Personal communication. 4

[CMS20] Alessandro Chiesa, Peter Manohar, and Igor Shinkar. On local testability in the non-signaling setting. In Thomas Vidick, editor, *ITCS 2020*, volume 151, pages 26:1–26:37. LIPIcs, January 2020. 3

[DHK+26] Lalita Devadas, Samuel B Hopkins, Yael Tauman Kalai, Pravesh K Kothari, Alex Lombardi, and Surya Mathialagan. Snargs for np and non-signaling pcps, revisited. *Cryptology ePrint Archive*, 2026. 3, 4, 5

[Jin26] Zhengzhong Jin. Low-norm nullstellensatz hypothesis for the and code is false, 2026. Personal communication. 4

[KRR14] Yael Tauman Kalai, Ran Raz, and Ron D. Rothblum. How to delegate computations: the power of no-signaling proofs. In David B. Shmoys, editor, *46th ACM STOC*, pages 485–494. ACM Press, May / June 2014. 5

[PZ24] Aaron Potechin and Aaron Zhang. Bounds on the total coefficient size of nullstellensatz proofs of the pigeonhole principle. In Karl Bringmann, Martin Grohe, Gabriele Puppis, and Ola Svensson, editors, *ICALP 2024*, volume 297 of *LIPIcs*, pages 117:1–117:20. Schloss Dagstuhl, July 2024. 3