

A Three-Polynomial Counterexample to the Generalized Effective Hypercube Nullstellensatz

Yuran Xiu
 IIIS, Tsinghua University
 xiuyr23@mails.tsinghua.edu.cn

15 October 2026

Abstract

We give a counterexample to the proposed extension of the effective Hypercube Nullstellensatz from two polynomials to an arbitrary fixed number of polynomials. For every $n \geq 1$, we construct three real polynomials in $2n + 1$ variables, of degrees 2, 2, 1, respectively. Each is nonzero as a function on the Boolean cube, their product vanishes on the cube, and they have no common Boolean zero. Nevertheless, every polynomial certificate $\sum_{i=1}^3 h_i g_i = 1$ on the cube satisfies $\deg \overline{h_1 g_1} \geq n + 1$, where the bar denotes multilinearization. The construction applies a fresh selector variable to the hard pair of Kothari, Kovacs-Deak, Wang, and Yang. Thus its new ingredient is a short transfer of their existing degree obstruction to the product-zero setting. The full unbounded-degree counterexample has been formalized and checked in Lean 4.

1 Introduction

Let $g_1, \dots, g_m$ be real polynomials with no common zero on the Boolean cube $\{0, 1\}^N$. There are polynomial multipliers $h_1, \dots, h_m$ such that

$$\sum_{i=1}^m h_i(x) g_i(x) = 1 \quad (x \in \{0, 1\}^N). \quad (1)$$

Indeed, at each point one may choose a nonzero $g_i(x)$, assign its multiplier the reciprocal value and all other multipliers zero, and interpolate these functions on the finite cube. The effective question is whether such a certificate can be chosen with low degree.

For a polynomial p , write $\bar{p}$ for its unique multilinear representative modulo the relations $X_j^2 = X_j$. We consider the degrees of the *separate reduced products* $\overline{h_i g_i}$. These are distinct from the unreduced product degrees and from the degree of the sum in (1).

Kothari, Kovacs-Deak, Wang, and Yang proved an effective theorem for two generators under the additional hypothesis that their product vanishes on the cube [1, Theorem 10]. They proposed that, for every fixed $m \geq 2$, the same hypotheses should give a bound on $\max_i \deg \overline{h_i g_i}$ polynomial in the input degrees [1, Conjecture 1]. We disprove this extension already for $m = 3$, with a fixed tuple of input degrees.

Theorem 1.1. *For $n \geq 1$, use variables $t, X_1, \dots, X_n, Y_1, \dots, Y_n$ and set*

$$A(X) = \sum_{j=1}^n X_j, \quad B(X, Y) = \sum_{j=1}^n X_j + \sum_{j=1}^n Y_j - (n + 1), \quad (2)$$

$$g_1 = tA, \quad g_2 = tB, \quad g_3 = 1 - t. \quad (3)$$

The ordinary degrees of g_1, g_2, g_3 are 2, 2, 1. Each is nonzero on the Boolean cube. Their product vanishes on the cube, and they have no common Boolean zero. For all real polynomial multipliers h_1, h_2, h_3 , the identity (1) on $\{0, 1\}^{2n+1}$ implies

$$\deg \overline{h_1 g_1} \geq n + 1. \quad (4)$$

Corollary 1.2. *There is no finite real-valued bound depending only on $(\deg g_1, \deg g_2, \deg g_3)$ for the maximum reduced-product degree of a certificate, even when the three generators are nonzero as Boolean functions, have no common Boolean zero, and have product identically zero on the cube. In particular, Conjecture 1 of [1] is false.*

Attribution and scope. The pair A, B in (2) and its degree obstruction are exactly the example in [1, Fact 7]. Their argument shows why removing the product-zero hypothesis fails for two generators. We use that existing example and its symmetrization proof. The observation here is that adjoining a selector t and the third generator $1 - t$ imposes the product-zero hypothesis while preserving the obstruction on the face $t = 1$. This is a negative-answer note about the stated multigenerator conjecture. It does not contradict the two-generator theorem or the main rational-degree theorem of [1].

2 Multilinearization and the known hard pair

A multilinear polynomial in N variables has the form $\sum_{S \subseteq [N]} c_S \prod_{j \in S} X_j$. Replacing every positive exponent in a monomial by one and then collecting coefficients gives $\bar{p}$. It agrees with p on $\{0, 1\}^N$ and cannot have larger total degree. Uniqueness follows by induction on N : write a multilinear polynomial as $P_0 + X_N P_1$ and evaluate first at $X_N = 0$ and then at $X_N = 1$. A polynomial vanishing on the entire cube is therefore zero if it is multilinear. We use this observation also on coordinate faces.

The following form of the hard-pair obstruction is the claim proved in [1, proof of Fact 7]. We give the proof to make the transfer self-contained.

Lemma 2.1 (Hard-pair obstruction). *Suppose a real multilinear polynomial $R(X, Y)$ satisfies*

$$R(0, y) = 0 \quad (y \in \{0, 1\}^n), \quad (5)$$

$$R(x, y) = 1 \quad (x, y \in \{0, 1\}^n, |x| + |y| = n + 1). \quad (6)$$

Then $\deg R \geq n$.

Proof. Suppose, to the contrary, that $d := \deg R < n$. Average R independently over permutations of its X coordinates and of its Y coordinates. The value of this average on a Boolean input of weights (u, v) is given by a bivariate polynomial $S(U, V)$ of total degree at most d . Here is a direct construction. For a multilinear monomial using a distinct X coordinates and b distinct Y coordinates, its average at weights (u, v) is

$$\frac{\binom{u}{a} \binom{v}{b}}{\binom{n}{a} \binom{n}{b}}. \quad (7)$$

This is the probability that a uniformly chosen set of u positions contains the prescribed a positions, times the analogous probability for the other block. Interpret $\binom{U}{a}$ as the falling-factorial polynomial $U(U-1)\cdots(U-a+1)/a!$, with $\binom{U}{0} = 1$. The denominators in (7) are positive because $a, b \leq n$.

Expanding R by monomials and replacing each monomial by this polynomial defines S . Each contributing term has degree $a + b \leq d$.

Both boundary conditions are constant on the relevant weight layers, so averaging preserves them. In particular,

$$S(0, v) = 0 \quad (0 \leq v \leq n), \quad S(u, n+1-u) = 1 \quad (1 \leq u \leq n).$$

The univariate polynomial $S(0, V)$ has degree at most $d < n$ and has $n+1$ distinct zeros. Thus it is identically zero. Also

$$H(U) := S(U, n+1-U) - 1$$

has degree at most $d < n$ and vanishes at $1, \dots, n$. It too must be identically zero. But $H(0) = S(0, n+1) - 1 = -1$, a contradiction. $\square$

The argument applies to arbitrary real coefficients. Neither symmetry of R nor any sign restriction is assumed; symmetrization is used only inside the proof.

3 The selector transfer

Proof of Theorem 1.1. Since $n \geq 1$, both tA and tB have nonzero degree-two monomials, and $1-t$ has degree one. These generators are also nonzero as functions on the cube: for g_1 take $t = 1$, $X_1 = 1$ and the remaining coordinates zero; for g_2 take $t = 1$ and $X = Y = 0$; for g_3 take $t = 0$. Their product has a factor $t^2(1-t)$, which vanishes at both Boolean values of t .

There is no common zero. If $t = 0$, then $g_3 = 1$. If $t = 1$ and $g_1 = 0$, all the Boolean X coordinates are zero. In that case $B = |Y| - (n+1) \leq -1$, so $g_2 \neq 0$.

Now take any certificate (1) and put $P = \overline{h_1 g_1}$. Since g_1 vanishes on the face $t = 0$, $P(0, x, y) = 0$ for every Boolean (x, y) . Write the multilinear polynomial P uniquely as

$$P(t, X, Y) = P_0(X, Y) + tR(X, Y).$$

Multilinear uniqueness on the face implies $P_0 = 0$. Hence $P = tR$.

On $t = 1$ and $X = 0$, the first generator is zero, so $R(0, y) = P(1, 0, y) = 0$. On $t = 1$ and $|X| + |Y| = n+1$, the second and third generators are zero. The certificate then forces $R(x, y) = P(1, x, y) = 1$. Thus R satisfies the two conditions of Lemma 2.1, and $\deg R \geq n$.

In particular $R \neq 0$; the second condition has witnesses for every $n \geq 1$, for example $|X| = n$ and $|Y| = 1$. Since t is a fresh variable, multiplication by t increases every nonzero monomial degree by one and causes no cancellation. Therefore

$$\deg \overline{h_1 g_1} = \deg(tR) = 1 + \deg R \geq n+1.$$

$\square$

Proof of Corollary 1.2. Let F be any proposed real-valued function of the three input degrees. Choose an integer $n \geq 1$ with $n+1 > F(2, 2, 1)$. The generators of Theorem 1.1 satisfy all the hypotheses, but every certificate has a reduced product of degree greater than $F(2, 2, 1)$. This excludes every such function F , and hence every polynomial bound. $\square$

Remark 3.1. For more than two generators, requiring the product to vanish means that at least one generator vanishes at each point. It does not require at most one generator to be nonzero. On the face $t = 1$, the third generator vanishes identically while the first two retain the original hard pair. This distinction is what permits the transfer. The individual nonzero Boolean-function witnesses above ensure that the construction does not rely on adding a generator that vanishes everywhere on the cube.

4 Formal verification

The associated Lean development proves the all- n lower bound and its dimension-independent consequence. Its multilinearization operator replaces positive monomial exponents by one and collects coefficients; the equality of Boolean evaluations, uniqueness, and degree properties are proved. The multipliers range over all real multivariate polynomials. There are no symmetry, coefficient-sign, or multiplier-degree restrictions.

The principal declarations are in namespace `HypercubeNS`:

- `selector_certificate_degree` proves Theorem 1.1’s certificate lower bound for every $n \geq 1$.
- `unbounded_certificate_degree` gives a triple in an ordinary finite indexed variable space exceeding every prescribed natural degree threshold. The formal proof includes the variable-renaming equivalence.
- `no_dimension_independent_bound` proves Corollary 1.2, for every real-valued function of the three input degrees.

The generator hypotheses and exact degrees are proved separately and included in the final counterexample. The hard-pair lemma is proved from layer counting and univariate root bounds, rather than introduced as an axiom. The development does not assert a matching upper certificate degree or a general theorem about exact selector degree shifts.

Verification used Lean 4.27.0 and mathlib commit

`a3a10db0e9d66acbebf76c5e6a135066525ac900`.

A separate reproduction rebuilt all twelve local modules, including the aggregate statement and axiom audit, from saved sources. The associated records preserve the dependency manifest, source hashes, successful build logs, and transitive axiom reports. From the formal artifact’s root, `sh lean/verify.sh` performs the local-source rebuild; the saved helper paths must be configured for the pinned compiler and dependency cache on another machine. The accepted main declarations depend only on `propext`, `Classical.choice`, and `Quot.sound`. No admitted lemma, additional mathematical axiom, native decision procedure, or unchecked numerical certificate is used. The reproduction reused the pinned compiler and dependency caches; it did not rebuild Lean or all of mathlib. The checked statements concern the counterexample and do not constitute a formal audit of the entire cited paper.

References

- [1] Robin Kothari, Matt Kovacs-Deak, Daochen Wang, and Rain Zimin Yang. Rational degree is polynomially related to degree. arXiv:2601.08727v3, 28 September 2026. Section 5.1, Theorem 10, Conjecture 1, and Fact 7.