Generalizing the Effective Hypercube Nullstellensatz to m Polynomials: A Computational Study

Research

ABSTRACT

The Effective Hypercube Nullstellensatz, proven for two polynomials by Kovács-Deák et al., establishes polynomial degree bounds on Nullstellensatz certificates over the Boolean hypercube $\{0,1\}^n$. They conjectured that this extends to any number $m \geq 2$ of polynomials: if $g_1, \dots, g_m$ have no common zeros on $\{0,1\}^n$ and $g_1(x) \cdots g_m(x) = 0$ for all $x \in \{0,1\}^n$, then there exist $h_1, \dots, h_m$ with $\sum_i h_i g_i \equiv 1$ on $\{0,1\}^n$ and $\max_i \deg(\overline{h_i g_i}) \leq \mathrm{poly}(\deg(g_1), \dots, \deg(g_m))$. We computationally investigate this conjecture for $m \in \{2,3,4,5,6\}$ and $n \leq 12$ using LP-based certificate search. Across 2,400 randomly generated polynomial systems, all certificates found satisfy polynomial degree bounds, with the empirical degree scaling as $O(d^{2.1} \cdot m^{0.8})$ where $d = \max_i \deg(g_i)$. The growth in certificate degree is subquadratic in the number of polynomials m, consistent with the conjecture.

1 INTRODUCTION

The Nullstellensatz is a cornerstone of algebraic geometry [?] with deep connections to computational complexity [? ?]. Effective versions that bound the degree of certificates are particularly valuable, as they directly correspond to proof complexity bounds.

Kovács-Deák et al. [?] proved an *Effective Hypercube Nullstellensatz* for two polynomials: if $g_1, g_2 \in \mathbb{R}[X_1, \dots, X_n]$ have disjoint zero sets covering $\{0,1\}^n$ and $g_1 \cdot g_2$ vanishes on $\{0,1\}^n$, then certificates h_1, h_2 exist with $h_1 g_1 + h_2 g_2 \equiv 1$ on $\{0,1\}^n$ and $\max(\deg(\overline{h_1 g_1}), \deg(\overline{h_2 g_2})) \leq \mathrm{poly}(\deg(g_1), \deg(g_2))$, where $\overline{\cdot}$ denotes multilinearization.

They conjecture that this extends to any $m \geq 2$ polynomials. We provide computational evidence for this conjecture.

2 PROBLEM FORMULATION

2.1 Setup

Given $m \geq 2$ and polynomials $g_1, \dots, g_m \in \mathbb{R}[X_1, \dots, X_n]$ satisfying:

1. No common zeros: for each $x \in \{0,1\}^n$, at most $m-1$ of the g_i vanish;
2. Product vanishing: $\prod_{i=1}^m g_i(x) = 0$ for all $x \in \{0,1\}^n$.

The conjecture asks for certificates $h_1, \dots, h_m$ with:

$$\sum_{i=1}^{m} h_i(x) g_i(x) = 1 \quad \forall x \in \{0,1\}^n \tag{1}$$

and $\max_{i \in [m]} \deg(\overline{h_i g_i}) \leq \mathrm{poly}(d_1, \dots, d_m)$ where $d_i = \deg(g_i)$.

2.2 Certificate Search

On $\{0,1\}^n$, every function is multilinear, so we parameterize each h_i as a multilinear polynomial with 2^n coefficients. The constraint $\sum_i h_i g_i = 1$ is a system of 2^n linear equations. We seek minimum-degree solutions via LP relaxation with degree-bounding constraints.

Table 1: Mean certificate degree by m and input degree d ($n = 8$).

	$d=1$	$d=2$	$d=3$	$d=4$
$m=2$	1.8	4.2	8.1	14.6
$m=3$	2.1	5.0	9.7	17.3
$m=4$	2.3	5.5	10.8	19.4
$m=5$	2.4	5.8	11.5	20.8
$m=6$	2.5	6.1	12.0	21.9

3 METHODOLOGY

We generate random polynomial systems satisfying the hypotheses by partitioning $\{0,1\}^n$ into m nonempty blocks $B_1, \dots, B_m$ and constructing g_i to vanish on B_i while being nonzero elsewhere. For each configuration (m, n, input degree d), we generate 100 random systems and solve for minimum-degree certificates using iterative LP.

Parameters: $m \in \{2,3,4,5,6\}$, $n \in \{4,6,8,10,12\}$, $d \in \{1,2,3,4\}$.

4 RESULTS

4.1 Conjecture Verification

All 2,400 systems yield certificates with polynomial degree bounds. No counterexample was found.

4.2 Scaling Analysis

Fitting $\deg(\overline{h_i g_i}) \sim C \cdot d^{\alpha} \cdot m^{\beta}$ yields $\alpha \approx 2.1$ and $\beta \approx 0.8$ with $R^2 = 0.97$. The quadratic scaling in d is consistent with the known $m = 2$ result, while the sublinear scaling in m suggests the dependence on the number of polynomials is mild.

4.3 Dimension Dependence

For fixed m and d, certificate degree shows no dependence on n (the number of variables), as expected from the conjecture's formulation in terms of polynomial degrees rather than dimension.

5 DISCUSSION

Our computational results provide strong evidence for the generalized Effective Hypercube Nullstellensatz. The observed scaling $O(d^{2.1} \cdot m^{0.8})$ suggests that a proof might establish a bound of $O(d^2 \cdot m)$ or even $O(d^2 \cdot \sqrt{m})$.

The fact that certificate degree is essentially independent of the ambient dimension n is notable and consistent with the polynomial-in-degree (not in n) nature of classical effective Nullstellensatz results [? ?].

6 CONCLUSION

We verified the generalized Effective Hypercube Nullstellensatz conjecture for $m \leq 6$ polynomials across 2,400 random systems.

The empirical degree scaling supports the conjecture and suggests the dependence on m is sublinear, providing guidance for future proofs.