Lattice Obstructions and Coefficient Alphabets for Homogeneous Boolean Lifts

Luca Blanchi

June 2026

Abstract

We study exact integer presentations of Boolean functions by expanded homogeneous forms and by polynomial interpolation on integer two-point encodings. The main point is that coefficient-height obstructions are preceded by a more basic lattice obstruction: the evaluation lattice depends strongly on the chosen Boolean encoding.

For a product encoding

$$\Omega = \prod_{i=1}^{n} a_i, b_i \subset \mathbb{Z}^n, \qquad m_i = b_i - a_i > 0,$$

we compute the interpolation lattice by finite differences. If $f : \Omega \to \mathbb{Z}$, then its unique multilinear interpolant has coefficients

$$\frac{\Delta_S f}{m_S}, \qquad m_S = \prod_{i \in S} m_i.$$

Consequently the least common denominator needed to interpolate f is

$$D_\Omega(f) = \operatorname{lcm} S \subseteq [n] \frac{m_S}{\gcd(m_S, \Delta_S f)}.$$

For Boolean functions $g : \Omega \to -1, 1$, the universal denominator is exactly

$$D_{\text{univ}}(\Omega) = \frac{\prod_i m_i}{\gcd(2, \prod_i m_i)}.$$

We then classify exactly which Boolean functions on Ω are represented by integer polynomials. If

$$U = i : m_i = 1, \qquad V = i : m_i = 2, \qquad W = i : m_i \geq 3,$$

then such functions are precisely those which are independent of the W-coordinates and, after identifying the V-coordinates with $-1, 1$, restrict on each U-fiber to a signed character. Equivalently they have the form

$$g(x, y, z) = \sigma(x) \prod_{j \in R(x)} y_j.$$

Thus the number of exact-integral Boolean functions is

$$\left(2^{|V|+1}\right)^{2^{|U|}}.$$

We also introduce coefficient alphabets for homogeneous Boolean lifts in the $0, 1$-encoding. For an alphabet $A \subset \mathbb{Z}$, an exact homogeneous degree-d lift exists if and only if every Boolean Möbius coefficient belongs to the corresponding block sumset:

$$\mu_S(g) \in \binom{d}{|S|} A.$$

This gives exact universal criteria for arbitrary alphabets. For odd alphabets

$$A_H^{\mathrm{odd}} = -H, -H+2, \ldots, H, \qquad H \text{ odd},$$

Lucas' theorem produces an arithmetically oscillating universal degree threshold:

$$D_{H,\mathrm{odd}}(n) = Q(n) \left\lceil \frac{D_H(n)}{Q(n)} \right\rceil, \qquad Q(n) = 2^{\lceil \log_2(n+1) \rceil},$$

where

$$D_H(n) = \min \left\{ d : H \binom{d}{n} \geq 2^n \right\}.$$

Finally, for a uniformly random Boolean function G_n, we compute the typical exact ternary sparsity:

$$\Sigma_{\mathrm{ex},H}(G_n) = \left(\frac{1}{H} \sqrt{\frac{2}{\pi}} + o_{\mathbb{P}}(1) \right) (1+\sqrt{2})^n$$

for each fixed $H \geq 1$, in contrast with the parity worst case 3^n.

The results are elementary but exact. They are not coordinate-invariant statements about polynomial threshold functions. They are invariants of explicit integer presentation models.

1 Introduction

The expanded homogeneous model for Boolean functions has a simple but rigid block structure. In the standard $0,1$-encoding, a homogeneous monomial of degree d collapses on the Boolean cube to a unique squarefree monomial. The block corresponding to a support $S \subseteq [n]$ has size

$$\binom{d}{|S|}.$$

Thus coefficient constraints on a homogeneous form become independent constraints on the Boolean Möbius coefficients.

The present note develops two complementary extensions of this observation.

First, before studying coefficient height, one should identify the underlying interpolation lattice. The usual $0,1$-encoding is special because it is unimodular: every integer-valued function on the cube has an integer multilinear representative. Other natural integer encodings, such as $-1,1^n$, are not unimodular. They introduce denominator and congruence obstructions before coefficient-size obstructions appear.

Second, instead of bounding coefficients by an interval, one may prescribe an arbitrary coefficient alphabet

$$A \subset \mathbb{Z}.$$

Then the exact lift problem is governed by sumsets

$$qA = a_1 + \cdots + a_q : a_i \in A.$$

This includes coefficient boxes, ternary coefficients, signed-binary coefficients, and odd alphabets.

The note is self-contained. It deliberately studies presentation-dependent integer models. It does not claim coordinate-invariant lower bounds for polynomial threshold functions.

2 Integer two-point encodings and finite differences

Let

$$\Omega = \prod_{i=1}^{n} a_i, b_i \subset \mathbb{Z}^n, \qquad a_i < b_i,$$

and set

$$m_i = b_i - a_i > 0.$$

For $S \subseteq [n]$, define

$$m_S = \prod_{i \in S} m_i, \qquad m_\varnothing = 1.$$

For $U \subseteq [n]$, let $p_U \in \Omega$ be the point with

$$(p_U)_i = \begin{cases} b_i, & i \in U, \\ a_i, & i \notin U. \end{cases}$$

For a function $f : \Omega \to \mathbb{Z}$, define its finite-difference coefficients by

$$\Delta_S f = \sum_{U \subseteq S} (-1)^{|S|-|U|} f(p_U).$$

Let

$$\phi_S(T) = \prod_{i \in S} (T_i - a_i).$$

The polynomials ϕ_S, $S \subseteq [n]$, form a $\mathbb{Z}$-basis of the module of multilinear integer polynomials in $T_1, \ldots, T_n$. Indeed,

$$\phi_S(T) = \prod_{i \in S} T_i + \text{terms supported on proper subsets of } S,$$

so the change-of-basis matrix from the standard squarefree monomial basis is triangular with diagonal entries 1.

Theorem 2.1. Finite-difference interpolation formula For every $f : \Omega \to \mathbb{Z}$, the unique multilinear polynomial over $\mathbb{Q}$ interpolating f on Ω is

$$P_f(T) = \sum_{S \subseteq [n]} \frac{\Delta_S f}{m_S} \phi_S(T).$$

Consequently, the least positive integer D such that DP_f has integer coefficients is

$$D_\Omega(f) = \operatorname{lcm}_{S \subseteq [n]} \frac{m_S}{\gcd(m_S, \Delta_S f)}.$$

Proof. Let

$$P(T) = \sum_{S \subseteq [n]} c_S \phi_S(T).$$

Evaluating at p_U, we obtain

$$\phi_S(p_U) = \begin{cases} m_S, & S \subseteq U, \\ 0, & S \not\subseteq U. \end{cases}$$

Therefore

$$P(p_U) = \sum_{S \subseteq U} c_S m_S.$$

Thus $P(p_U) = f(p_U)$ for all $U \subseteq [n]$ is equivalent to

$$f(p_U) = \sum_{S \subseteq U} c_S m_S.$$

By Möbius inversion on the Boolean lattice,

$$c_S m_S = \sum_{U \subseteq S} (-1)^{|S|-|U|} f(p_U) = \Delta_S f.$$

Hence

$$c_S = \frac{\Delta_S f}{m_S}.$$

Since the basis ϕ_S is a unimodular $\mathbb{Z}$-basis of the multilinear integer polynomials, DP_f has integer coefficients in the standard squarefree monomial basis if and only if each

$$D\frac{\Delta_S f}{m_S}$$

is an integer. The least such D is the displayed least common multiple. □

3 The evaluation lattice

Let

$$\operatorname{ev}\Omega : \mathbb{Z}[T_1, \ldots, T_n]\mathrm{ml} \to \mathbb{Z}^{\Omega}$$

be the evaluation map from multilinear integer polynomials to integer-valued functions on Ω.

In the basis ϕ_S on the domain and the point basis indexed by $U \subseteq [n]$ on the codomain, the matrix of evaluation is

$$M_{U,S} = \begin{cases} m_S, & S \subseteq U, \\ 0, & S \not\subseteq U. \end{cases}$$

Thus

$$M = Z \operatorname{diag}(m_S),$$

where $Z_{U,S} = 1_{S \subseteq U}$ is the zeta matrix of the Boolean lattice.

The zeta matrix Z is unimodular, with inverse given by Möbius inversion:

$$Z^{-1}_{U,S} = \begin{cases} (-1)^{|U|-|S|}, & S \subseteq U, \\ 0, & S \not\subseteq U. \end{cases}$$

Proposition 3.1. Diagonal form and index The evaluation lattice $\operatorname{ev}\Omega(\mathbb{Z}[T]\mathrm{ml}) \subseteq \mathbb{Z}^\Omega$ is equivalent over $\mathbb{Z}$ to the diagonal lattice with diagonal entries

$$m_S = \prod_{i \in S} m_i, \qquad S \subseteq [n].$$

In particular, its index in $\mathbb{Z}^\Omega$ is

$$[\mathbb{Z}^\Omega : \operatorname{ev}\Omega(\mathbb{Z}[T]\mathrm{ml})] = \prod_{S \subseteq [n]} m_S = \prod_{i=1}^{n} m_i^{2^{n-1}}.$$

Proof. Since Z is unimodular,

$$M = Z \operatorname{diag}(m_S)$$

is equivalent over $\mathbb{Z}$ to $\operatorname{diag}(m_S)$. Therefore the cokernel has order

$$\prod_{S \subseteq [n]} m_S.$$

Finally,

$$\prod_{S \subseteq [n]} m_S = \prod_{S \subseteq [n]} \prod_{i \in S} m_i = \prod_{i=1}^{n} m_i^{|S : S \ni i|} = \prod_{i=1}^{n} m_i^{2^{n-1}}.$$

□ This diagonal form is not necessarily the Smith normal form in invariant-factor order when the m_i have distinct prime factors. It is, however, a diagonal form over $\mathbb{Z}$ sufficient for the interpolation and index computations above.

4 Universal denominators for Boolean functions

Let

$$g : \Omega \to -1, 1.$$

For $S \neq \varnothing$, the finite difference $\Delta_S g$ is a sum of $2^{|S|}$ signs. Hence

$$\Delta_S g \equiv 0 \pmod 2 \qquad (S \neq \varnothing).$$

Let

$$M = \prod_{i=1}^{n} m_i.$$

Theorem 4.1. Universal Boolean denominator The least positive integer D such that every Boolean function

$$g : \Omega \to -1, 1$$

has a multilinear interpolant with coefficients in $D^{-1}\mathbb{Z}$ is

$$D_{\text{univ}}(\Omega) = \frac{M}{\gcd(M, 2)}.$$

Proof. First prove sufficiency.

Let $g : \Omega \to -1, 1$. Its coefficient in the ϕ_S-basis is

$$\frac{\Delta_S g}{m_S}.$$

For $S = \varnothing$, this coefficient is ± 1.

Assume $S \neq \varnothing$. Then $\Delta_S g$ is even. If M is odd, choose $D = M$. Since $m_S \mid M$,

$$D\frac{\Delta_S g}{m_S} \in \mathbb{Z}.$$

If M is even, choose $D = M/2$. Since $\Delta_S g/2 \in \mathbb{Z}$,

$$D\frac{\Delta_S g}{m_S} = \frac{M}{m_S} \cdot \frac{\Delta_S g}{2} \in \mathbb{Z}.$$

Thus

$$D = \frac{M}{\gcd(M, 2)}$$

suffices.

For necessity, choose a Boolean function g whose top finite difference satisfies

$$\Delta_{[n]} g = 2.$$

Such a function exists, because $\Delta_{[n]} g$ is a sum of 2^n independently assignable signs and can attain every value in

$$-2^n, -2^n + 2, \ldots, 2^n.$$

The coefficient of $\phi_{[n]}$ in the interpolating polynomial is then

$$\frac{2}{M}.$$

If all Boolean functions can be represented with coefficients in $D^{-1}\mathbb{Z}$, then

$$D\frac{2}{M} \in \mathbb{Z}.$$

Equivalently,

$$\frac{M}{\gcd(M, 2)} \mid D.$$

This proves minimality. □

Examples

For the standard encoding $0, 1^n$, all $m_i = 1$, so

$$D_{\text{univ}} = 1.$$

Thus every integer-valued function on the cube has an integer multilinear representative. For the sign encoding $-1, 1^n$, all $m_i = 2$, so

$$D_{\text{univ}} = 2^{n-1}.$$

For $0, m^n$, one has

$$D_{\text{univ}} = \frac{m^n}{\gcd(2, m^n)}.$$

5 Exact-integral Boolean functions on two-point encodings

We now classify Boolean functions on Ω that are represented by integer polynomials.

Partition the coordinates as follows:

$$U = i : m_i = 1, \qquad V = i : m_i = 2, \qquad W = i : m_i \geq 3.$$

For $i \in U$, set

$$x_i = T_i - a_i \in 0, 1.$$

For $j \in V$, set

$$y_j = T_j - a_j - 1 \in -1, 1.$$

For $k \in W$, write the coordinate as z_k.

Theorem 5.1. Classification of exact-integral Boolean functions A Boolean function

$$g : \Omega \to -1, 1$$

is represented on Ω by a polynomial in $\mathbb{Z}[T_1, \ldots, T_n]$ if and only if it has the form

$$g(x, y, z) = \sigma(x) \prod_{j \in R(x)} y_j,$$

where

$$\sigma : 0, 1^U \to -1, 1$$

is arbitrary and

$$R(x) \subseteq V$$

is an arbitrary subset depending on x. In particular, g is independent of the W-coordinates.

The number of exact-integral Boolean functions on Ω is therefore

$$\left(2^{|V|+1}\right)^{2^{|U|}}.$$

Proof. Suppose first that g is represented by some polynomial

$$P(T) \in \mathbb{Z}[T_1, \ldots, T_n].$$

Let $k \in W$, so $m_k = b_k - a_k \geq 3$. Fix all coordinates except T_k. We obtain a one-variable integer polynomial

$$Q(t) \in \mathbb{Z}[t]$$

such that

$$Q(a_k), Q(b_k) \in -1, 1.$$

For an integer polynomial, $Q(b_k) - Q(a_k)$ is divisible by $b_k - a_k = m_k$. But

$$Q(b_k) - Q(a_k) \in 0, \pm 2.$$

Since $m_k \geq 3$, this difference must be 0. Thus g is independent of coordinate k. Since $k \in W$ was arbitrary, g is independent of all W-coordinates.

Now fix a value of the U-coordinates. The restriction of P to the remaining V-coordinates becomes an integer polynomial in the variables $y_j \in -1, 1$. Reducing modulo the relations

$$y_j^2 = 1$$

gives a Walsh expansion

$$p(y) = \sum_{R \subseteq V} b_R y_R, \qquad b_R \in \mathbb{Z},$$

where

$$y_R = \prod_{j \in R} y_j.$$

Since $p(y) \in -1, 1$ for all $y \in -1, 1^V$, Parseval's identity for the Walsh characters gives

$$1 = \mathbb{E}_y[p(y)^2] = \sum_{R \subseteq V} b_R^2.$$

Because all b_R are integers, exactly one coefficient is ± 1 and the rest are 0. Hence, on this U-fiber,

$$p(y) = \pm y_R$$

for some $R \subseteq V$. The sign and the subset R may depend on the fixed U-fiber. Thus

$$g(x, y, z) = \sigma(x) y_{R(x)}.$$

Conversely, suppose g has this form. For each $x^0 \in 0, 1^U$, let

$$I_{x^0}(x) = \prod_{\substack{i \in U \\ x_i^0 = 1}} x_i \prod_{\substack{i \in U \\ x_i^0 = 0}} (1 - x_i).$$

This is an integer polynomial and is the indicator of the U-fiber $x = x^0$. Then

$$g(x,y,z) = \sum_{x^0 \in 0,1^U} I_{x^0}(x)\sigma(x^0) \prod_{j \in R(x^0)} y_j$$

is an integer polynomial representing g. This proves the classification.

For each of the $2^{|U|}$ fibers, one may choose independently a sign $\sigma(x)$ and a subset $R(x) \subseteq V$. Thus the number of functions is

$$(2 \cdot 2^{|V|})^{2^{|U|}} = \left(2^{|V|+1}\right)^{2^{|U|}}.$$

□

Corollary 5.2. When are all Boolean functions exact-integral? Every Boolean function

$$g : \Omega \to -1, 1$$

is represented by an integer polynomial if and only if

$$W = \varnothing \qquad \text{and} \qquad |V| \leq 1.$$

Proof. If $W \neq \varnothing$, every exact-integral Boolean function is independent of the W-coordinates by Theorem 5.1, so not all Boolean functions are represented.

Assume $W = \varnothing$. The total number of Boolean functions on Ω is

$$2^{2^{|U|+|V|}}.$$

By Theorem 5.1, the number of exact-integral Boolean functions is

$$2^{(|V|+1)2^{|U|}}.$$

These numbers are equal if and only if

$$(|V|+1)2^{|U|} = 2^{|U|+|V|},$$

i.e.

$$|V| + 1 = 2^{|V|}.$$

This holds exactly for $|V| = 0$ and $|V| = 1$. □

Special cases

For $0, 1^n$, one has $U = [n]$ and $V = W = \varnothing$. Hence all Boolean functions are exact-integral.

For $-1, 1^n$, one has $V = [n]$ and $U = W = \varnothing$. Hence the exact-integral Boolean functions are precisely the 2^{n+1} signed characters

$$\pm y_R.$$

For $0, m^n$ with $m \geq 3$, one has $W = [n]$. Hence the only exact-integral Boolean functions are the two constants.

6 Homogeneous lifts and coefficient alphabets

We now return to the standard $0,1$-encoding.

Let

$$F \in \mathbb{Z}[X_0, \dots, X_n]_d$$

be a homogeneous integer form of degree d. We evaluate it on the Boolean cube by

$$x \mapsto F(1, x_1, \dots, x_n).$$

After reducing by the Boolean relations $x_i^2 = x_i$, every such evaluation has a unique multilinear representative

$$p(x) = \sum_{S \subseteq [n]} a_S x_S.$$

For $S \subseteq [n]$, let

$$q_S(d) = \binom{d}{|S|},$$

with the convention $\binom{d}{s} = 0$ if $s > d$.

A homogeneous monomial of degree d reduces to x_S if and only if its positive variables among $X_1, \dots, X_n$ are precisely the variables indexed by S. The number of such monomials is $q_S(d)$. Thus the homogeneous coefficients split into disjoint blocks indexed by S.

Let

$$A \subseteq \mathbb{Z}$$

be an allowed coefficient alphabet. For $q \geq 1$, define the q-fold sumset

$$qA = a_1 + \cdots + a_q : a_i \in A.$$

Set

$$0A = 0.$$

Theorem 6.1. Exact lift criterion for coefficient alphabets Let

$$p(x) = \sum_{S \subseteq [n]} a_S x_S$$

be an integer multilinear polynomial. There exists a homogeneous degree-d form

$$F \in \mathbb{Z}[X_0, \dots, X_n]_d$$

with all coefficients in A, satisfying

$$F(1, x) = p(x) \qquad \forall x \in 0, 1^n,$$

if and only if

$$a_S \in q_S(d)A \qquad \forall S \subseteq [n].$$

If A is finite, the number of distinct integer-valued functions on the Boolean cube obtained in this way is

$$V_{n,d}(A) = \prod_{S\subseteq[n]} |q_S(d)A| = \prod_{s=0}^{n} \left| \binom{d}{s} A \right|^{\binom{n}{s}}.$$

Proof. The coefficient a_S is the sum of the homogeneous coefficients in the block indexed by S. This block has cardinality

$$q_S(d) = \binom{d}{|S|}.$$

If all homogeneous coefficients lie in A, then a_S must lie in $q_S(d)A$.

Conversely, if $a_S \in q_S(d)A$, then one can choose $q_S(d)$ elements of A whose sum is a_S and assign them to the block indexed by S. Since the blocks are disjoint, these choices can be made independently for all S. This constructs the required homogeneous lift.

If A is finite, the possible values of a_S are exactly the elements of $q_S(d)A$, and the choices for distinct S are independent. Since the multilinear coefficients uniquely determine the function on the Boolean cube, multiplication over all S gives the stated formula. □

7 Universal exact lifts for coefficient alphabets

Let

$$g : 0,1^n \to -1,1.$$

Its Boolean Möbius coefficients are

$$\mu_S(g) = \sum_{T\subseteq S} (-1)^{|S|-|T|} g(1_T).$$

Here $1_T \in 0,1^n$ is the indicator vector of T.

For $|S| = s$, the value $\mu_S(g)$ is a sum of 2^s signs. Conversely, because the values of g on the points 1_T, $T \subseteq S$, can be assigned arbitrarily, the set of possible values of $\mu_S(g)$ is exactly

$$M_s = -2^s, -2^s + 2, \ldots, 2^s - 2, 2^s.$$

For $s = 0$, this is

$$M_0 = -1, 1.$$

Theorem 7.1. Universal alphabet criterion Every Boolean function

$$g : 0,1^n \to -1,1$$

has an exact homogeneous degree-d lift with coefficients in A if and only if

$$M_s \subseteq \binom{d}{s} A \qquad 0 \le s \le n.$$

Proof. If every Boolean function has such a lift, then for any fixed S of size s, every possible value of $\mu_S(g)$ must belong to the block sumset $q_S(d)A = \binom{d}{s}A$. Since the possible values are exactly M_s, this gives necessity.

Conversely, assume

$$M_s \subseteq \binom{d}{s} A \qquad 0 \le s \le n.$$

Let g be arbitrary. For each S, $\mu_S(g) \in M_{|S|}$, hence

$$\mu_S(g) \in \binom{d}{|S|} A.$$

By Theorem 6.1, the multilinear polynomial representing g has a homogeneous degree-d lift with coefficients in A. □

8 Odd alphabets and Lucas oscillations

Fix an odd integer

$$H \ge 1$$

and consider the odd coefficient alphabet

$$A_H^{\mathrm{odd}} = -H, -H+2, \ldots, H-2, H.$$

For $q \ge 1$,

$$qA_H^{\mathrm{odd}} = z \in \mathbb{Z} : |z| \le Hq,\ z \equiv q \pmod 2.$$

Indeed, a sum of q odd integers is congruent to q modulo 2, and every integer of that parity between $-Hq$ and Hq can be obtained by changing summands in steps of 2.

For $s \ge 1$, all values in M_s are even. Hence Theorem 7.1 implies two conditions:

$$H\binom{d}{s} \ge 2^s$$

and

$$\binom{d}{s} \equiv 0 \pmod 2$$

for every $1 \le s \le n$.

Define

$$Q(n) = 2^{\lceil \log_2(n+1) \rceil},$$

the least power of 2 strictly larger than n.

Lemma 8.1. Parity of binomial blocks For an integer $d \geq 0$,

$$\binom{d}{s} \equiv 0 \pmod 2 \qquad \forall, 1 \leq s \leq n$$

if and only if

$$Q(n) \mid d.$$

Proof. By Lucas' theorem modulo 2, $\binom{d}{s}$ is odd if and only if every binary digit equal to 1 in s occurs in a position where d also has binary digit 1.

Let 2^t be the largest power of 2 dividing d, with the convention that $t = \infty$ if $d = 0$. Then all binary digits of d below position t are 0, and the digit in position t is 1 if $d \neq 0$.

If $2^t \leq n$, take

$$s = 2^t.$$

Then the binary support of s is contained in that of d, so $\binom{d}{s}$ is odd.

Conversely, if $2^t > n$, every integer $1 \leq s \leq n$ has some nonzero binary digit below position t, where d has digit 0. Hence no such s has binary support contained in that of d, so $\binom{d}{s}$ is even for every $1 \leq s \leq n$.

The condition $2^t > n$ is equivalent to divisibility of d by the least power of 2 greater than n, namely (Q(n)). □

Define

$$D_H(n) = \min \left\{ d \geq 0 : H\binom{d}{n} \geq 2^n \right\}.$$

The binomial coefficient is understood to be 0 if $d < n$, so $D_H(n) \geq n$.

Theorem 8.2. Universal degree for odd alphabets Let

$$A_H^{\text{odd}} = -H, -H+2, \ldots, H, \qquad H \geq 1 \text{ odd}.$$

The least degree d such that every Boolean function on $0, 1^n$ has an exact homogeneous degree-d lift with coefficients in A_H^{odd} is

$$D_{H,\text{odd}}(n) = Q(n) \left\lceil \frac{D_H(n)}{Q(n)} \right\rceil.$$

Proof. By Theorem 7.1 and the description of qA_H^{odd}, universal exact representation is equivalent to the following two conditions for every $1 \leq s \leq n$:

$$H\binom{d}{s} \geq 2^s,$$

and

$$\binom{d}{s} \equiv 0 \pmod 2.$$

The parity condition is equivalent to $Q(n) \mid d$ by Lemma 8.1.

It remains to reduce the size inequalities to the single top inequality

$$H\binom{d}{n} \geq 2^n.$$

For $d \geq n$, set

$$r_s = \frac{2^s}{\binom{d}{s}}.$$

For $0 \leq s < d$,

$$\frac{r_{s+1}}{r_s} = \frac{2(s+1)}{d-s}.$$

This ratio is increasing in s, so (r_s) is log-convex. Hence its maximum on $0 \leq s \leq n$ occurs at an endpoint. Since $r_0 = 1$, and $H \geq 1$, the inequalities

$$H\binom{d}{s} \geq 2^s \qquad (0 \leq s \leq n)$$

follow from

$$H\binom{d}{n} \geq 2^n.$$

Thus the admissible degrees are precisely the multiples of (Q(n)) that are at least $D_H(n)$. The least such degree is

$$Q(n)\left\lceil \frac{D_H(n)}{Q(n)} \right\rceil.$$

□

Corollary 8.3. Signed-binary coefficients For signed-binary coefficients

$$A = -1, 1,$$

one has

$$D_{\pm}(n) = Q(n)\left\lceil \frac{D_1(n)}{Q(n)} \right\rceil,$$

where

$$D_1(n) = \min\left\{ d : \binom{d}{n} \geq 2^n \right\}.$$

If $c_>1$ is the unique solution of

$$c \log c - (c-1)\log(c-1) = \log 2,$$

then

$$D_1(n) = c_n + O(\log n).$$

Consequently,

$$\liminf_{n\to\infty} \frac{D_\pm(n)}{n} = c_*, \qquad \limsup_{n\to\infty} \frac{D_\pm(n)}{n} = 2c_*.$$

More precisely, the set of subsequential limits of $D_\pm(n)/n$ is the whole interval

$$[c_*, 2c_*].$$

Proof. The formula for $D_\pm(n)$ is Theorem 8.2 with $H = 1$.

Let

$$q_n = \frac{Q(n)}{n}.$$

As n varies, the set of subsequential limits of q_n is ([1,2]). Moreover

$$\frac{D_1(n)}{Q(n)} = \frac{c_*}{q_n} + o(1).$$

Therefore

$$\frac{D_\pm(n)}{n} = q_n \left\lceil \frac{c_*}{q_n} + o(1) \right\rceil.$$

If $q \in (c_*, 2]), the limiting value is(q).If(q \in [1, c_*)$, the limiting value is $2q$. Thus the possible limits contain

$$[c_*, 2] \cup [2, 2c_*] = [c_*, 2c_*].$$

The endpoints are obtained by one-sided choices of q_n tending to c_*. □

9 Typical exact ternary sparsity

Let

$$G_n : 0, 1^n \to -1, 1$$

be uniformly random, with independent values.

For an exact ternary homogeneous lift, i.e. a lift with coefficients in

$$-1, 0, 1,$$

the minimum number of nonzero homogeneous coefficients is, whenever the lift is feasible,

$$\Sigma_{\mathrm{ex},1}(g) = \sum_{S\subseteq[n]} |\mu_S(g)|.$$

Indeed, in the block S, a sum $A = \mu_S(g)$ requires at least (|A|) nonzero coefficients from $-1, 0, 1$, and this is achieved by using (|A|) coefficients equal to $\mathrm{sgn}(A)$, provided the block has size at least (|A|).

More generally, for height $H \geq 1$, with coefficients in

$$[-H, H] \cap \mathbb{Z}$$

and sparsity cost equal to the number of nonzero homogeneous coefficients, the exact sparsity is

$$\Sigma_{\mathrm{ex},H}(g) = \sum_{S \subseteq [n]} \left\lceil \frac{|\mu_S(g)|}{H} \right\rceil$$

whenever the required block capacities are available.

We compute this quantity for a random Boolean function.

Theorem 9.1. Typical exact sparsity For each fixed integer $H \geq 1$,

$$\Sigma_{\mathrm{ex},H}(G_n) = \left(\frac{1}{H}\sqrt{\frac{2}{\pi}} + o_{\mathbb{P}}(1) \right) (1+\sqrt{2})^n.$$

In particular,

$$\Sigma_{\mathrm{ex},1}(G_n) = \left(\sqrt{\frac{2}{\pi}} + o_{\mathbb{P}}(1) \right) (1+\sqrt{2})^n.$$

Proof. First consider $H = 1$.

For $|S| = s$,

$$\mu_S(G_n) = \sum_{T \subseteq S} (-1)^{|S|-|T|} G_n(1_T)$$

is a sum of 2^s independent Rademacher random variables. Let

$$R_N = \varepsilon_1 + \cdots + \varepsilon_N$$

with independent Rademacher signs. Then

$$\mu_S(G_n) \stackrel{d}{=} R_{2^s}.$$

It is standard, by the central limit theorem and uniform integrability, that

$$\mathbb{E}|R_N| = \left(\sqrt{\frac{2}{\pi}} + o(1) \right) \sqrt{N} \qquad (N \to \infty).$$

Thus

$$\mathbb{E}|\mu_S(G_n)| = \left(\sqrt{\frac{2}{\pi}} + o(1) \right) 2^{s/2}$$

as $s \to \infty$.

Therefore

$$\mathbb{E}\Sigma_{\mathrm{ex},1}(G_n) = \sum_{s=0}^{n} \binom{n}{s} \mathbb{E}|R_{2^s}|.$$

Given $\varepsilon > 0$, choose s_0 such that for all $s \geq s_0$,

$$\left| \frac{\mathbb{E}|R_{2^s}|}{2^{s/2}} = \sqrt{\frac{2}{\pi}} \right| < \varepsilon.$$

The contribution of $s < s_0$ is polynomial in n, hence negligible compared with $(1+\sqrt{2})^n$. Consequently

$$\mathbb{E}\Sigma_{\mathrm{ex},1}(G_n) = \left(\sqrt{\frac{2}{\pi}} + o(1) \right) \sum_{s=0}^{n} \binom{n}{s} 2^{s/2}.$$

Since

$$\sum_{s=0}^{n} \binom{n}{s} 2^{s/2} = (1+\sqrt{2})^n,$$

we have

$$\mathbb{E}\Sigma_{\mathrm{ex},1}(G_n) = \left(\sqrt{\frac{2}{\pi}} + o(1) \right) (1+\sqrt{2})^n.$$

It remains to prove concentration. View

$$\Sigma_{\mathrm{ex},1}(G_n) = \sum_{S} |\mu_S(G_n)|$$

as a function of the 2^n independent values $G_n(1_T)$.

If one value $G_n(1_T)$ is changed, then μ_S changes only when $T \subseteq S$. The number of such S is

$$2^{n-|T|}.$$

Each affected $|\mu_S|$ changes by at most 2. Hence the total change is at most

$$c_T = 2 \cdot 2^{n-|T|}.$$

Thus

$$\sum_{T \subseteq [n]} c_T^2 = \sum_{t=0}^{n} \binom{n}{t} 4 \cdot 4^{n-t} = 4 \cdot 5^n.$$

By McDiarmid's bounded differences inequality,

$$\mathbb{P}\left(|\Sigma_{\mathrm{ex},1}(G_n) = \mathbb{E}\Sigma_{\mathrm{ex},1}(G_n)| \geq u \right) \leq 2 \exp\left(-\frac{2u^2}{4 \cdot 5^n} \right).$$

Taking

$$u = \varepsilon (1+\sqrt{2})^n$$

gives an exponent of order

$$-\left(\frac{(1+\sqrt{2})^2}{5} \right)^n.$$

Since

$$(1+\sqrt{2})^2 = 3 + 2\sqrt{2} > 5,$$

this tends to $-\infty$. Hence

$$\Sigma_{\mathrm{ex},1}(G_n) = \left(\sqrt{\frac{2}{\pi}} + o_{\mathbb{P}}(1)\right)(1+\sqrt{2})^n.$$

For general fixed $H \geq 1$,

$$\Sigma_{\mathrm{ex},H}(G_n) = \sum_S \left\lceil \frac{|\mu_S(G_n)|}{H} \right\rceil.$$

Thus

$$\frac{1}{H}\sum_S |\mu_S(G_n)| \leq \Sigma_{\mathrm{ex},H}(G_n) \leq \frac{1}{H}\sum_S |\mu_S(G_n)| + 2^n.$$

Since

$$2^n = o((1+\sqrt{2})^n),$$

the asserted formula follows from the $H = 1$ case. $\square$

Comparison with parity

For parity

$$\mathrm{PAR}_n(x) = (-1)^{x_1+\cdots+x_n},$$

one has

$$|\mu_S(\mathrm{PAR}\, n)| = 2^{|S|}.$$

Therefore

$$\Sigma \mathrm{ex}, 1(\mathrm{PAR}_n) = \sum_{S\subseteq[n]} 2^{|S|} = 3^n.$$

Thus the typical exact ternary sparsity grows like

$$(1+\sqrt{2})^n,$$

whereas the parity worst case grows like

$$3^n.$$

10 Local parity certificates on arbitrary faces

We record a useful local obstruction. It applies to threshold sign-representation by integer polynomials with bounded multilinear coefficients.

Let

$$[n] = R \sqcup J \sqcup K.$$

Consider the face

$$\mathcal{F} = \{x \in 0,1^n : x_j = 1 \ \forall j \in J, \quad x_k = 0 \ \forall k \in K\},$$

whose free coordinates are those in R. Let

$$r = |R|.$$

Suppose

$$g(x) = \sigma(-1)^{\sum_{i \in R} x_i} \qquad (x \in \mathcal{F}),$$

where $\sigma \in -1, 1$.

Let

$$p(x) = \sum_{S \subseteq [n]} a_S x_S$$

be an integer multilinear polynomial sign-compatible with g on $\mathcal{F}$:

$$g(x)p(x) > 0 \qquad (x \in \mathcal{F}).$$

Assume coefficient bounds

$$|a_S| \leq B_S.$$

Proposition 10.1. Local parity certificate Under the assumptions above,

$$\sum_{Q \subseteq J} B_{R \cup Q} \geq 2^r.$$

In the homogeneous height model, where

$$B_S = H\binom{d}{|S|},$$

this becomes

$$H \sum_{q=0}^{|J|} \binom{|J|}{q} \binom{d}{r+q} \geq 2^r.$$

Proof. Restrict p to the face $\mathcal{F}$. Variables in K become 0, variables in J become 1, and variables in R remain free. The coefficient of the top monomial

$$x_R = \prod_{i \in R} x_i$$

in the restricted polynomial is

$$A_R = \sum_{Q \subseteq J} a_{R \cup Q}.$$

The restricted polynomial is integer-valued on $0,1^R$ and sign-represents parity on that r-dimensional cube, up to a global sign. Let its values be

$$v(1_T) = \sigma(-1)^{|T|} c_T, \qquad c_T \in \mathbb{Z}_{\geq 1}.$$

The top Möbius coefficient is

$$A_R = \sum_{T \subseteq R} (-1)^{r-|T|} v(1_T) = \sigma(-1)^r \sum_{T \subseteq R} c_T.$$

Therefore

$$|A_R| \geq 2^r.$$

On the other hand,

$$|A_R| = \left| \sum_{Q \subseteq J} a_{R \cup Q} \right| \leq \sum_{Q \subseteq J} |a_{R \cup Q}| \leq \sum_{Q \subseteq J} B_{R \cup Q}.$$

This proves the first claim.

If p arises from a homogeneous degree-d form of coefficient height at most H, then the coefficient a_S is a sum of $\binom{d}{|S|}$ homogeneous coefficients, each of absolute value at most H. Hence

$$|a_S| \leq H \binom{d}{|S|}.$$

Substituting this into the first inequality gives

$$H \sum_{Q \subseteq J} \binom{d}{|R| + |Q|} \geq 2^r.$$

Grouping by $q = |Q|$ yields

$$H \sum_{q=0}^{|J|} \binom{|J|}{q} \binom{d}{r+q} \geq 2^r.$$

□

11 Scope and limitations

The results above are exact statements about explicit integer presentation models.

They should not be interpreted as coordinate-invariant lower bounds for polynomial threshold functions. The choice of Boolean encoding matters substantially:

In the $0, 1$-encoding, the interpolation lattice is unimodular. In the $-1, 1$-encoding, exact-integral Boolean functions are only signed characters. In general two-point integer encodings, denominator obstructions are governed by the gaps $m_i = b_i - a_i$.

Similarly, the homogeneous lift model is an expanded monomial presentation. Its coefficient height, alphabet, and sparsity are presentation costs, not intrinsic invariants of Boolean functions under arbitrary coordinate changes.

The open threshold problem remains substantially harder than the exact interpolation problem. For exact lifts, one controls the Möbius coefficients of the given Boolean function. For threshold sign-representations, one may replace g by an arbitrary integer-valued function v with the same sign pattern. This becomes a positive-cone rounding or discrepancy problem for the Boolean zeta matrix and is not resolved by the lattice and alphabet methods developed here.

12 Summary of main formulas

For

$$\Omega = \prod_i a_i, b_i, \qquad m_i = b_i - a_i, \qquad m_S = \prod_{i \in S} m_i,$$

the interpolating polynomial of $f : \Omega \to \mathbb{Z}$ is

$$P_f(T) = \sum_{S \subseteq [n]} \frac{\Delta_S f}{m_S} \prod_{i \in S} (T_i - a_i).$$

The least denominator of P_f is

$$D_\Omega(f) = \mathrm{lcm}_{S \subseteq [n]} \frac{m_S}{\gcd(m_S, \Delta_S f)}.$$

The universal Boolean denominator is

$$D_{\mathrm{univ}}(\Omega) = \frac{\prod_i m_i}{\gcd(2, \prod_i m_i)}.$$

If

$$U = i : m_i = 1, \quad V = i : m_i = 2, \quad W = i : m_i \geq 3,$$

then exact-integral Boolean functions are precisely

$$g(x, y, z) = \sigma(x) y_{R(x)}.$$

Their number is

$$\left(2^{|V|+1}\right)^{2^{|U|}}.$$

For homogeneous degree-d lifts in the $0, 1$-encoding with coefficient alphabet A,

$$p(x) = \sum_S a_S x_S$$

has a lift if and only if

$$a_S \in \binom{d}{|S|} A \qquad \forall S.$$

Every Boolean function has such a lift if and only if

$$-2^s, -2^s + 2, \ldots, 2^s \subseteq \binom{d}{s} A \qquad 0 \leq s \leq n.$$

For odd alphabets

$$A_H^{\mathrm{odd}} = -H, -H + 2, \ldots, H,$$

the universal degree is

$$D_{H,\mathrm{odd}}(n) = Q(n) \left\lceil \frac{D_H(n)}{Q(n)} \right\rceil,$$

where

$$Q(n) = 2^{\lceil \log_2(n+1) \rceil}$$

and

$$D_H(n) = \min \left\{ d : H\binom{d}{n} \geq 2^n \right\}.$$

For a uniformly random Boolean function,

$$\Sigma_{\mathrm{ex},H}(G_n) = \left(\frac{1}{H}\sqrt{\frac{2}{\pi}} + o_{\mathbb{P}}(1) \right) (1+\sqrt{2})^n.$$

References

M. Bhargava, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, Journal für die reine und angewandte Mathematik 490 1997, 101–127.

É. Lucas, Théorie des fonctions numériques simplement périodiques, American Journal of Mathematics 1 1878, 184–196, 197–240, 289–321.

R. O'Donnell, Analysis of Boolean Functions, Cambridge University Press, 2014.

R. P. Stanley, Enumerative Combinatorics, Volume 1, Cambridge University Press, 2nd edition, 2011.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work, ChatGPT, by OpenAI, was used to assist with mathematical drafting, formalization, review, and editing. This work is shared as a preliminary AI-assisted mathematical note. The mathematical content may have been only partially reviewed and may contain errors; it should not be treated as peer-reviewed or as a fully verified manuscript.