

The Dimension Bound for Graph Algebraic Immunity Is Attainable

Alper Ferudun*

21 October 2026

Abstract

Let the graph algebraic immunity of a Boolean map $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ be the least degree of a nonzero reduced Boolean polynomial vanishing on its graph. A dimension count bounds this quantity by the least d for which $\sum_{j=0}^d \binom{n+m}{j} > 2^n$. We prove that this bound is attained for every $n, m \geq 1$. The argument combines translation invariance of low-degree Boolean evaluation spaces with Rado's independent-representative theorem. Averaging translates of a basis gives a rank lower bound for every subset of the cube. Adding independent dummy vectors then produces a basis containing at most one point over each input. Completing these selected points to a graph gives the desired map. This answers the unrestricted existence question recorded by Krause in Oberwolfach Report 31/2007. The proof is self-contained and uses classical matroid ideas. It imposes no balancing or permutation condition.

1 The graph immunity bound

Write

$$B_s = \mathbb{F}_2[z_1, \dots, z_s] / (z_1^2 - z_1, \dots, z_s^2 - z_s).$$

Each element has a unique squarefree algebraic normal form. Its degree is the largest cardinality of a monomial with nonzero coefficient. Denote its degree-at-most- d subspace by $P_d(s)$, and put

$$\Phi_s(d) = \dim P_d(s) = \sum_{j=0}^d \binom{s}{j}, \quad 0 \leq d \leq s.$$

A nonzero element of B_s is a nonzero Boolean function; the field equations themselves are therefore not annihilators in this definition.

For $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, define

$$\text{AI}_{\text{gr}}(f) = \min\{\deg p : 0 \neq p \in B_{n+m}, p(x, f(x)) = 0 \text{ for every } x \in \mathbb{F}_2^n\}.$$

The graph has 2^n points. Hence the evaluation map $P_d(n+m) \rightarrow \mathbb{F}_2^{2^n}$ has nonzero kernel as soon as its domain dimension exceeds 2^n . Consequently

$$\text{AI}_{\text{gr}}(f) \leq d^*(n, m) := \min\{d : \Phi_{n+m}(d) > 2^n\}. \quad (1)$$

For positive m the threshold exists, since $\Phi_{n+m}(n+m) = 2^{n+m} > 2^n$.

*Mercury Software GmbH. Email: alper@mercurycodelab.com. GitHub: [AlperTheKing](https://github.com/AlperTheKing). Unrefereed preprint. Licensed under CC BY 4.0.

Krause’s report, describing joint work with Altendorf and Armknecht, asks whether equality in (1) can always be attained when $1 \leq m \leq n$ [4, pp. 1838–1839]. The same graph-immunity definition and dimension bound appear in Carlet’s author-hosted text [2, pp. 149–151]. Armknecht and Krause had already developed a construction based on matroid union [1]. We use classical independent representatives to prove unconditional existence.

Theorem 1. *For every pair of positive integers n, m , there is a map $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ satisfying*

$$\text{AI}_{\text{gr}}(f) = d^*(n, m).$$

The theorem concerns arbitrary maps. In particular, it does not assert that an extremal map can be balanced or, when $m = n$, a permutation. Graph algebraic immunity is distinct from basic or component algebraic immunity; these distinctions matter for both the definition and the numerical bound.

2 Rank density and independent representatives

A vector configuration will be indexed by a finite set E . Its labels may be different even when their vectors coincide. For $S \subseteq E$ write $\rho(S)$ for the rank of its vectors.

Lemma 2. *Suppose a finite group acts transitively on E and preserves the rank of every subset. If $\rho(E) = r$, then*

$$\rho(S) \geq r \frac{|S|}{|E|} \quad (S \subseteq E).$$

Proof. Fix a labeled basis $B \subseteq E$ of size r . Every translate gB is a basis, and $gB \cap S$ is independent. Thus $|gB \cap S| \leq \rho(S)$. Transitivity implies that a uniformly chosen group element sends B to a set containing any fixed label with probability $r/|E|$. Averaging gives

$$\rho(S) \geq \mathbb{E}_g |gB \cap S| = \frac{r|S|}{|E|}.$$

□

We give the linear form of Rado’s theorem [5], including its standard inductive proof, so that the existence argument needs no external structural result.

Lemma 3 (Independent representatives). *Let $A_1, \dots, A_k$ be finite vector families in a vector space V over a field. They have representatives $a_i \in A_i$ that are linearly independent if and only if*

$$\dim \text{span} \left(\bigcup_{i \in J} A_i \right) \geq |J| \quad \text{for every } J \subseteq \{1, \dots, k\}. \quad (2)$$

Proof. Necessity follows by taking the representatives indexed by J . For sufficiency, induct on k . The cases $k = 0$ and $k = 1$ are immediate.

Suppose first that some nonempty proper subset J is tight in (2). Induction gives independent representatives for these families. They form a basis of

$$W = \text{span} \left(\bigcup_{i \in J} A_i \right), \quad \dim W = |J|.$$

Project the remaining families to V/W . For $K \subseteq \{1, \dots, k\} \setminus J$, the dimension of the span of their images is

$$\dim \operatorname{span} \left(\bigcup_{i \in J \cup K} A_i \right) - |J| \geq |K|.$$

Induction applies in the quotient. Lift its independent representatives and adjoin the chosen basis of W ; the resulting family is independent.

If there is no such tight subset, every nonempty proper J has rank at least $|J| + 1$. Choose a nonzero $a_k \in A_k$, and quotient by the line $\langle a_k \rangle$. For every nonempty $J \subseteq \{1, \dots, k-1\}$, the rank drops by at most one and remains at least $|J|$. Induction supplies representatives independent in this quotient. Together with a_k , their lifts are independent in V . $\square$

Proposition 4. *Suppose the configuration of Lemma 2 is partitioned into N blocks of equal cardinality, and its rank r satisfies $r \leq N$. There is a basis consisting of labels in r different blocks.*

Proof. Put $h = N - r$ and adjoin a direct summand of dimension h . Let D be a basis of this new summand. For block E_i , form A_i by taking its original vectors in the first summand and all vectors of D in the second. When $h = 0$, D is empty.

For a nonempty set J of k blocks, equal cardinalities and Lemma 2 give

$$\begin{aligned} \dim \operatorname{span} \left(\bigcup_{i \in J} A_i \right) &= \rho \left(\bigcup_{i \in J} E_i \right) + h \\ &\geq \frac{rk}{N} + N - r \\ &= k + (N - r) \left(1 - \frac{k}{N} \right) \geq k. \end{aligned}$$

The empty-set inequality is automatic. Lemma 3 supplies N independent representatives, one for each A_i . At most r representatives can be original vectors and at most h can belong to D . Since $r + h = N$, exactly r are original vectors. They form a basis and come from distinct indexed blocks. If a vector has several labels, choose its label in the block it represents. $\square$

Only transitivity of the configuration is used here. The acting group need not preserve the partition. Equal block sizes are what turn the density estimate into every inequality required by Rado's theorem.

3 A basis inside a Boolean graph

Proof of Theorem 1. Set

$$s = n + m, \quad N = 2^n, \quad d = d^*(n, m) - 1, \quad r = \Phi_s(d) \leq N.$$

For each $z \in \mathbb{F}_2^s$, consider the evaluation column

$$v_z = (z^A)_{A \subseteq \{1, \dots, s\}, |A| \leq d} \in \mathbb{F}_2^r.$$

The complete configuration has rank r . Indeed, a linear relation among its rows would be a squarefree polynomial that vanishes on the whole cube. Such a polynomial is zero: write it as $p_0 + z_s p_1$, evaluate at $z_s = 0, 1$, and induct on s .

Translations act transitively on the labels z . Substitution $z_i \mapsto z_i + a_i$ preserves $P_d(s)$, since expansion of a squarefree monomial produces only monomials of no larger degree. The substitution

is invertible, being its own inverse. Its invertible matrix takes the evaluation column v_z to v_{z+a} . Thus translations preserve ranks, and Lemma 2 applies.

Partition the labels into the N fibres

$$E_x = \{(x, y) : y \in \mathbb{F}_2^m\}, \quad x \in \mathbb{F}_2^n.$$

Every fibre has 2^m labels. Proposition 4 gives a basis of r evaluation columns with distinct input coordinates. Define $f(x) = y$ on these chosen pairs and choose $f(x)$ arbitrarily on the remaining inputs.

The evaluation columns indexed by the graph of f contain a basis of $\mathbb{F}_2^r$. Therefore evaluation on the graph is injective on $P_d(s)$: a polynomial vanishing there must have all its coefficients zero. It follows that $\text{AI}_{\text{gr}}(f) \geq d + 1$. The opposite inequality is (1), because $\Phi_s(d + 1) > N$. Hence $\text{AI}_{\text{gr}}(f) = d + 1 = d^*(n, m)$. $\square$

The argument includes the equality case $r = N$, when the selected basis already specifies every output, as well as $d = 0$. Positive n, m ensure $\Phi_s(0) = 1 \leq 2^n$, so that the degree d used in the proof is nonnegative.

Example 5. For $n = 2$, $m = 1$, the threshold is $d^* = 2$, and the map $f(x_1, x_2) = x_1x_2$ attains it. The functions $1, x_1, x_2, f$ on $\mathbb{F}_2^2$ are linearly independent, so no nonzero affine polynomial vanishes on the graph. The reduced polynomial $y + x_1x_2$ is a degree-two annihilator. This is an instance of $r = N = 4$.

4 Exact certificates and scope

The accompanying standard-library Python program supplies exact diagnostics for all 28 pairs $1 \leq m \leq n \leq 7$. For each pair it records a complete function table, verifies that the degree-at-most- $d^* - 1$ graph evaluation matrix has full rank, and produces a nonzero annihilator of degree exactly d^* . All arithmetic is over $\mathbb{F}_2$. Both ordinary and optimized Python execution produce identical outputs; correctness checks do not rely on Python assertions.

For construction in these finite tests, the program packs disjoint input bases for the spaces

$$P_{d-|z|}(n), \quad z \in \mathbb{F}_2^m, \quad |z| \leq d, \quad d = d^* - 1.$$

It uses augmenting exchanges from the classical matroid-union setting [1, 3] and checks independence after every exchange. On the basis indexed by z , it assigns output z . The total required basis size is

$$\sum_{j=0}^{\min(m, d)} \binom{m}{j} \Phi_n(d - j) = \Phi_{n+m}(d)$$

by Vandermonde's identity (with $\Phi_n(t) = 2^n$ for $t \geq n$). Order output words and output monomials by weight. The entry z^β vanishes unless $\beta \subseteq z$, so the resulting square graph submatrix is block triangular; its diagonal blocks are the invertible input evaluation matrices. The program also verifies the final graph rank directly, independently of this block interpretation.

Additional regression tests check all 1024 subset-rank inequalities for the four degree spaces on $\mathbb{F}_2^3$, all 8192 corresponding translation-rank identities, and all 105 partitions of its eight labels into four pairs for $P_1(3)$. These finite certificates test implementations and boundary cases. The all-parameter result rests on the preceding proof, not on a finite search or a claim of formal verification.

The conclusion is solely attainability of the graph-immunity bound for unrestricted maps. It does not certify the cryptographic quality of the resulting functions, supply a succinct formula for all

parameters, or impose bijectivity or balance. The independent-representative theorem and matroid methods used here are classical. This unrefereed note makes no absolute priority claim.

AI assistance was used in developing the argument, drafting, and preparing exact diagnostic code. The mathematical argument and its scope have been subjected to a detailed self-audit; no independent review or machine-checked formal verification is claimed.

References

- [1] F. Armknecht and M. Krause, Constructing Single- and Multi-output Boolean Functions with Maximal Algebraic Immunity, in *Automata, Languages and Programming*, ICALP 2006, Part II, Lecture Notes in Computer Science **4052**, Springer, 2006, 180–191. [doi:10.1007/11787006_16](https://doi.org/10.1007/11787006_16).
- [2] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, author-hosted manuscript, pp. 149–151. [Author-hosted full text](#).
- [3] J. Edmonds and D. R. Fulkerson, Transversals and Matroid Partition, *Journal of Research of the National Bureau of Standards* **69B** (1965), 147–153. [doi:10.6028/jres.069B.016](https://doi.org/10.6028/jres.069B.016).
- [4] M. Krause (joint work with H. Altendorf and F. Armknecht), Constructing Boolean Functions of Maximal Algebraic Immunity, in *Complexity Theory*, Oberwolfach Report 31/2007, 1838–1839. [doi:10.4171/OWR/2007/31](https://doi.org/10.4171/OWR/2007/31).
- [5] R. Rado, A Theorem on Independence Relations, *Quarterly Journal of Mathematics* **os-13** (1942), 83–89. [doi:10.1093/qmath/os-13.1.83](https://doi.org/10.1093/qmath/os-13.1.83).