Electronic Colloquium on Computational Complexity, Report No. 139 (2026)

# Fine-Grained $\mathsf{AC}^0$ Lower Bounds for $k$-OV, $k$-XOR, and $k$-SUM via Colored Subgraph Isomorphism

Haoxing LIN*

National University of Singapore

haoxingl@comp.nus.edu.sg

**Abstract**

We prove lower bounds for $k$-$\mathsf{OV}$, $k$-$\mathsf{XOR}$, and $k$-$\mathsf{SUM}$ in nonuniform $\mathsf{AC}^0$, tracking how the circuit-size exponent scales with $k$ and using no running-time hypothesis. Our framework gives depth-zero projections from colored subgraph isomorphism to the three targets at dimension, row count, or bit width $O(k \log n)$, without increasing depth or size, and preserving gate orientation. For every fixed depth and every sufficiently large fixed $k$, we obtain unconditional bounds $n^{\Omega(k)}$ for $k$-$\mathsf{OV}$ and $(n/k)^{\Omega(k)}$ for $k$-$\mathsf{XOR}$ and $k$-$\mathsf{SUM}$, with an absolute exponent-rate constant independent of both $k$ and the depth, while the onset threshold may depend on $(d, k)$. For growing $k = n^{o(1)}$, we obtain, for every fixed depth $d$, the unconditional floor $n^{\Omega_d(\min\{\sqrt{k}, \log n\})}$. This strengthens to $n^{\Omega(k)}$ at depth two for both top-gate orientations, i.e., top conjunction and top disjunction. Assuming a pattern-uniform strengthening of the Li–Razborov–Rossman source lower bound, the same projections complete the subpolynomial frontier with $n^{\Omega_d(k)}$ at depth three for both orientations and for every fixed depth $d \geq 4$. All direct $k$-$\mathsf{XOR}$ bounds stated above concern odd $k$; a black-box odd-to-even lift transfers any such lower bound through a supplied admissible parameter decomposition. The $k$-$\mathsf{SUM}$ projection works for both parities. At the bit width $m = \Theta(k \log(\mathrm{e}n/k))$ used by our projection, a block-carry $\Sigma_3$ upper bound of size $(n/k)^{O(k)}$ matches the fixed-$k$ specialization of the top-disjunction depth-three lower bound $(n/k)^{\Omega(k)}$ up to constants in the exponent. The remaining upper-versus-lower-bound gaps concern depth two, top-conjunction depth three, and other width regimes.

*This work was supported by the National Research Foundation, Singapore, under its NRF Fellowship programme, award no. NRF-NRFF14-2022-0010.



ISSN 1433-8092

# Contents

# 1 Introduction

The problems studied in this paper have different algebraic forms, but they share one witness-selection task: choose $k$ objects and verify one joint relation. Informally, their accepting witnesses have the following forms:

$$\begin{aligned}
&k\text{-}\mathsf{OV}: && \exists\,(u_1,\dots,u_k)\in U_1\times\cdots\times U_k \quad \forall t\in[D],\quad \prod_{i=1}^{k}u_i(t)=0,\\
&k\text{-}\mathsf{XOR}: && \exists\,S\in\binom{[n]}{k} \quad \bigoplus_{i\in S}a_i=0^m,\\
&k\text{-}\mathsf{SUM}: && \exists\,S\in\binom{[n]}{k} \quad \sum_{i\in S}z_i\equiv 0 \pmod{2^m}.
\end{aligned}$$

For $k$-$\mathsf{OV}$, the input consists of $k$ arrays of $n$ pairwise-distinct $D$-dimensional binary vectors, and a witness chooses one vector from each array. For $k$-$\mathsf{XOR}$ and $k$-$\mathsf{SUM}$, the input is a single indexed list of size $n$ whose entries are $m$-dimensional binary vectors ($k$-$\mathsf{XOR}$) or $m$-bit integers ($k$-$\mathsf{SUM}$), and a witness chooses $k$ distinct indices; different selected indices may carry equal values. The formal definitions and input conventions appear in Section 3.1.

Fine-grained complexity refines coarse running-time classifications by asking for the correct exponent of the running time and by using reductions that preserve the significance of an exponent improvement [IP01, IPZ01, VW18]. We ask the analogous quantitative question for nonuniform constant-depth computation: how does the exponent of the required circuit size scale with $k$ and with the dimension, row count, or bit width of the instance? This is an analogy in granularity, not a transfer of a running-time hypothesis.

We answer this circuit analogue by projecting from colored subgraph isomorphism rather than by importing a time-complexity hypothesis. A common family of depth-zero projections yields fixed-$k$ lower bounds for all three targets and an unconditional depth-versus-$k$ frontier when $k$ grows. The exponent is linear in $k$ at depth two. A precise source-side conjecture would extend that exponent to depth three and to every fixed depth $d \geq 4$.

## 1.1 Problems, fine-grained complexity, and constant-depth circuits

**The three target problems.** The targets share a selection skeleton but use three different verification algebras. Orthogonality asks that every coordinate avoid the all-one pattern among the selected vectors. XOR asks that independent linear constraints over $\mathbb{F}_2$ vanish. Modular SUM asks that an integer sum vanish in $\mathbb{Z}_{2^m}$, where carries couple the bit positions. Orthogonal Vectors is a canonical hub of fine-grained complexity, and its two-vector form has a substantial equivalence class under truly subquadratic reductions [VW18, CW19]; the $k$-set formulation studied here exposes the number of selected vectors as an additional quantitative parameter. The $k$-$\mathsf{SUM}$ and $k$-$\mathsf{XOR}$ problems have their own algorithmic, average-case, and generalized-birthday lineages, discussed in Section 1.4. We do not place all three targets under one algorithmic conjecture. They are grouped here because the same source witness can be realized through each of their three algebras.

**Our sense of "fine-grained" in this paper.** Here *fine-grained* refers to the dependence of the circuit-size exponent on $k$ and to the preservation of that dependence under our projections. Theorems A–D in Section 1.2 are unconditional. Theorem E assumes only Pattern-Uniform LRR, a circuit lower-bound conjecture for colored subgraph isomorphism; it is neither SETH, OVC, nor any running-time hypothesis for the target problems. The fine-grained literature therefore motivates the quantitative question and the choice of targets, but it supplies no hardness assumption used in our unconditional proofs.

**Constant-depth circuits.** The class $\mathsf{AC}^0$ consists of nonuniform families of polynomial-size, constant-depth Boolean circuits with unbounded-fan-in AND and OR gates and negations at the inputs. To state quantitative lower bounds, we allow arbitrary size at each fixed depth and let $\mathrm{size}_d(f)$ denote the minimum number of non-input gates in a depth-at-most-$d$ circuit computing $f$, with negations normalized to input leaves. Throughout the paper, $\Omega(\cdot)$ hides an absolute positive constant, whereas $\Omega_d(\cdot)$ may hide a constant depending on the fixed depth $d$; in general, a subscript lists every parameter on which the hidden constant may depend. Foundational work of Ajtai, Furst, Saxe, Sipser, Yao, and Håstad established strong limitations of this model, most famously through lower bounds for PARITY and related explicit functions [Ajt83, FSS84, Yao85, Hås86].

Those classical results usually express complexity as a function of the total input length. Our question is parameter-sensitive: for structured witness-selection functions, how precisely can the circuit-size exponent scale with the number $k$ of selected objects and with the target's constraint budget, namely dimension, row count, or bit width?

**Time lower bounds do not answer the circuit question.** SETH- and OVC-based lower bounds concern the running time of uniform algorithms [IP01, IPZ01, VW18, CW19]. They do not by themselves rule out nonuniform constant-depth circuits, whose circuit may be chosen separately for each parameter tuple. Our route therefore starts with unconditional constant-depth lower bounds for a source Boolean function and transfers them by depth-zero projections. Such a projection replaces every input of a target circuit by a constant, a source input bit, or its negation; composition preserves depth and introduces no new gates. The resulting bounds are direct worst-case circuit lower bounds for the target functions.

**The resulting viewpoint.** This function-level bridge yields a modular methodology rather than three unrelated reductions. Three proved source statements and one conjecture feed a common projection interface and then branch into orthogonality, addition over $\mathbb{F}_2$, and modular integer addition. Quantitatively, the outcome depends jointly on circuit depth, the witness parameter $k$, the target budget (dimension for $k$-$\mathsf{OV}$, row count for $k$-$\mathsf{XOR}$, or bit width for $k$-$\mathsf{SUM}$), and the way the target universe packs the source candidates.

Structurally, the direct $k$-$\mathsf{XOR}$ qualification arises while enforcing exact selection over $\mathbb{F}_2$: odd $k$ rules out an anchor-free even-multiplicity branch that survives for even $k$. Signed integer selectors give $k$-$\mathsf{SUM}$ no analogous parity restriction. Both list targets nevertheless remain PARITY-hard after a simple restriction that fixes the $k$ selected indices. Quantitatively, for a fixed support $S \in \binom{[n]}{k}$, the remaining $k$-$\mathsf{XOR}$ predicate has a depth-two verifier of size $m \cdot 2^{O(k)}$, whereas the direct $k$-$\mathsf{SUM}$ verifier costs $2^{\Theta(km)}$; at the bit-width scale $m = \Theta(k \log(en/k))$ supplied by our projection, the block-carry depth-three circuit removes the extra factor of $m$ in the latter exponent. We next state the resulting depth-versus-$k$ frontier before turning to the proof architecture that produces it.

## 1.2 Main results and the depth-versus-$k$ frontier

We refer to the principal results as Theorems A–E; each paragraph heading below links to its formal statement. As a cue to the notation used below, $\gamma$ denotes a source-host exponent rate

| Regime and circuit class | Common displayed lower bound | Status |
|---|---|---|
| Sufficiently large fixed $k$, every fixed depth | $n^{\Omega(k)}$ for $k$-OV; $(n/k)^{\Omega(k)}$ for $k$-XOR and $k$-SUM | Unconditional; Theorem B |
| Growing $k = n^{o(1)}$, every fixed depth $d$ | $n^{\Omega_d(\min\{\sqrt{k}, \log n\})}$ | Unconditional; Theorem C |
| Growing $k = n^{o(1)}$, depth two, both orientations | $n^{\Omega(k)}$ | Unconditional; Theorem D |
| Growing $k = n^{o(1)}$, depth three with both orientations; every fixed depth $d \geq 4$ | $n^{\Omega_d(k)}$ | Conditional on Pattern-Uniform LRR; Theorem E |

Table 1: The depth-versus-$k$ frontier. In the growing-$k$ rows the common base-$n$ display uses $k = n^{o(1)}$; the exact natural base for $k$-XOR and $k$-SUM is $n/k$, as in Table 2. Here $\Omega(\cdot)$ hides an absolute constant and $\Omega_d(\cdot)$ a depth-dependent one. The direct $k$-XOR statements are for odd $k$.

and $\beta$ or $c$ a target-size rate; Section 2.1 gives the full convention and its exceptions. Throughout this subsection, the direct $k$-XOR statements concern odd $k$; the even-$k$ lift is summarized after Theorem E.

**Theorem A: one projection interface for three targets.** Let $P$ be a simple loopless pattern with exactly $k-1$ edges. In colored $P$-subgraph isomorphism at host size $N$, written $P\text{-SUB}_N$, the host has one color class $\{v\} \times [N]$ of $N$ vertices for every $v \in V(P)$, and the input specifies the possible host edges between the color classes corresponding to edges of $P$. The source accepts when one can choose one vertex from each color class so that every pattern edge is present; the coloring fixes which host vertex plays each pattern role. The projection represents one selected host edge for each of the $k-1$ pattern edges and adds one anchor to fill the one-object gap, producing a target witness of size $k$. Writing $\leq_{\text{proj}}$ for a depth-zero projection, we obtain $P\text{-SUB}_N \leq_{\text{proj}} k\text{-OV}$, $P\text{-SUB}_N \leq_{\text{proj}} k\text{-XOR}$ for odd $k$, and $P\text{-SUB}_N \leq_{\text{proj}} k\text{-SUM}$ for both parities, in each case without increasing circuit depth or size and while preserving gate orientation. The exact host capacities and $O(k \log n)$-scale budgets appear in Table 2. The $k$-OV construction stores each edge group in a separate class and therefore permits $N = \Theta(\sqrt{n})$, whereas the two list targets $k$-XOR and $k$-SUM store all $k-1$ groups together and permit only $N = \Theta(\sqrt{n/k})$; this packing difference produces the two natural lower-bound bases, $n$ for $k$-OV and $n/k$ for the list targets. Consequently, any lower bound for a suitable colored-subgraph source transfers through the same three target constructions, and source hardness and target realization can be selected independently.

Table 1 summarizes the resulting circuit frontier. Its growing-$k$ rows use the common simplification $k = n^{o(1)}$, under which $n/k = n^{1-o(1)}$ and the list-target lower bounds can also be displayed in base $n$. The exact target bases and constraint budgets appear in Table 2 and in the formal theorem statements.

| Target | Source host size | Target budget | Natural base and qualification |
|---|---|---|---|
| $k$-$\mathsf{OV}$ | $N = \lfloor \sqrt{n} \rfloor$ | $D \geq C_{\mathrm{OV}} k \log n$ | base $n$; both parities |
| $k$-$\mathsf{XOR}$ | $N = \left\lfloor \sqrt{\frac{n-1}{k-1}} \right\rfloor$ | $m \geq C_{\oplus} k \log(en/k)$ | base $n/k$; direct projection for odd $k$ |
| $k$-$\mathsf{SUM}$ | $N = \left\lfloor \sqrt{\frac{n-1}{k-1}} \right\rfloor$ | $m \geq C_{\Sigma} k \log(en/k)$ | base $n/k$; both parities; fixed-$k$ top-disjunction depth-three exponent-scale tight when $m = \Theta(k \log(en/k))$ |

Table 2: Target packing and principal constraint budgets. We call the displayed dimension, row-count, and bit-width thresholds the *principal budgets*: they are the $O(k \log n)$-scale budgets supplied directly by the projections of Theorem 10. The universal constants $C_{\mathrm{OV}}, C_{\oplus}, C_{\Sigma} > 0$ are fixed in Theorem 10 and lemma 11, and these budgets are used by Theorems 17 and 21, and Theorem 28. Theorem 19 instead uses the more demanding $k$-$\mathsf{SUM}$ width $m \geq C_{\Sigma} k \log n$, because $O(k \log(kN))$ is not uniformly $O(k \log(n/k))$ throughout its range $k \leq n^{1-\varepsilon}$.

The depth-two theorem is proved in the larger ranges $k \leq \xi_D n^{1/4}$ for $k$-$\mathsf{OV}$ and $k \leq \xi_D n^{1/5}$ for $k$-$\mathsf{XOR}$ and $k$-$\mathsf{SUM}$, where $\xi_D > 0$ is a universal range constant.

**Theorem B: a universal fixed-$k$ rate.** Let $k_0 \in \mathbb{N}$ be the universal threshold in Lemma 5, and for each $k \geq k_0$ let $P_k^{\mathrm{exp}}$ denote the padded expander pattern supplied there. Let $C_{\mathrm{OV}}, C_{\oplus}, C_{\Sigma}$ be the universal construction constants fixed by Theorem 10. There exists a universal target-side exponent rate $\beta > 0$, independent of $k$, the depth $d$, and the instance size $n$. For every fixed depth $d$ and every fixed $k \geq k_0$, once $n$ exceeds a threshold depending on $(d, k)$, every depth-$d$ circuit for $k$-$\mathsf{OV}$ has size at least $n^{\beta(k-1)}$, while every depth-$d$ circuit for $k$-$\mathsf{XOR}$ or $k$-$\mathsf{SUM}$ has size at least $(n/k)^{\beta(k-1)}$, at the budgets in Table 2. The exponent-rate constant is therefore uniform in both $d$ and $k$; only the onset threshold is not. At the principal budgets, the top-disjunction depth-three specializations for all three targets match elementary upper bounds at the exponent scale. This comparison makes no tightness claim at depth two or for the top-conjunction depth-three orientation.

**Theorem C: an unconditional growing-$k$ floor at every fixed depth.** When $k$ grows, the fixed-pattern source theorem provides no uniform control of the onset threshold, so we replace the padded expander source by a clique core padded with a matching. For every fixed depth $d$ and every subpolynomial $k = n^{o(1)}$ tending to infinity, the resulting lower bound for each target has the common scale

$$n^{\Omega_d(\min\{\sqrt{k}, \log n\})}.$$

More generally, the theorem holds throughout $k \leq n^{1-\varepsilon}$ with the exact base-$n$ and base-$(n/k)$ expressions in Theorem 19; its $k$-$\mathsf{SUM}$ line uses the larger width $m \geq C_{\Sigma} k \log n$ recorded in Table 2. The exponent first grows as $\sqrt{k}$ because a clique using at most $k-1$ pattern edges has only $\Theta(\sqrt{k})$ vertices. It then reaches a plateau whose hidden height constant may depend on $d$ when Beame's small-clique range becomes binding; the transition scale itself is $k = \Theta(\log^2 n)$, independent of $d$.

**Theorem D: both depth-two orientations.** At depth two, direct counting restores an exponent linear in $k$. The DNF branch is the standard minimal-positive-input count: every colored copy is a minimal positive input of the source and therefore forces a distinct accepting term. The source-specific CNF branch constructs an explicit exponentially large family of minimal transversals of the colored-copy hypergraph, each of which forces a clause; a single pattern vertex of degree at least two already generates the required family. Transferring the resulting source bound yields $n^{\Omega(k)}$ for $k$-$\mathsf{OV}$ when $k \leq \xi_D n^{1/4}$ and $(n/k)^{\Omega(k)}$ for the two list targets when $k \leq \xi_D n^{1/5}$. Thus both the top-conjunction and top-disjunction orientations are covered.

**Theorem E: a conditional completion.** Pattern-Uniform LRR asserts that, for each fixed depth $d$, there are constants $\gamma_d, c'_d > 0$ such that the padded expander family $(P_k^{\exp})_{k \geq k_0}$ satisfies $\mathrm{size}_d(P_k^{\exp}\text{-SUB}_N) \geq N^{\gamma_d k}$ for every $k \geq k_0$ and every $N \geq k^{c'_d}$. Assuming this source-side statement, the unchanged projections of Theorem A give $n^{\Omega_d(k)}$ lower bounds throughout the subpolynomial regime for all three targets. At depth three this supplies the full linear-in-$k$ exponent for both orientations, and for every fixed depth $d \geq 4$ it supplies the full linear-in-$k$ exponent. We use Pattern-Uniform LRR only as a sufficient condition and do not claim that it is necessary. It strengthens the fixed-pattern Li–Razborov–Rossman theorem by requiring one polynomial host threshold uniformly along the growing family, and it is not known to follow from that theorem.

Two target-specific qualifications complete the frontier. First, the direct $k$-$\mathsf{XOR}$ projection enforces exact selection through equations over $\mathbb{F}_2$ and is therefore clean for odd $k$. For an even target parameter $K$, Lemma 65 gives a black-box lift from any supplied odd parameter $r$ in an admissible decomposition $K = tr + s$; Corollary 67, and Corollary 68 record the corresponding quantitative consequences. Second, the $k$-$\mathsf{SUM}$ projection works for both parities because signed integer coordinates enforce exact multiplicities. Although the direct fixed-support depth-two verifier costs $2^{\Theta(km)}$, Proposition 71 gives a top-disjunction depth-three block-carry circuit of size $(n/k)^{O(k)}$ at the principal width $m = \Theta(k \log(en/k))$. At fixed $k$, this makes the top-disjunction depth-three specialization of Theorem 17 exponent-scale tight. This does not settle the optimal size at depth two or for the opposite depth-three orientation. Nor does it make fixed-support verification polynomial-size: Proposition 63 gives a two-point PARITY restriction for $k$-$\mathsf{SUM}$, and the same one-line restriction applies to $k$-$\mathsf{XOR}$. Rather, block carries remove the extra factor of $m$ in the exponent of the direct $k$-$\mathsf{SUM}$ verifier.

## 1.3 Proof architecture and technical ideas

Figure 1 records the proof dependencies. Four source statements feed two pattern families, each padded to exactly $k-1$ edges, and every resulting colored subgraph source passes through the same target interface. In particular, the conditional path changes only the source statement: it introduces no new reduction to any target.

**One witness skeleton, three verification algebras.** A source witness selects one host edge for each edge of the pattern. It is valid exactly when every selected edge is present and all edges incident to the same pattern vertex assign that vertex the same host label. The target instances represent each proposed host edge by a candidate object and add one anchor, while coordinates or rows enforce selection, presence, consistency, dummy exclusion, and, only for $k$-$\mathsf{OV}$, pairwise distinctness within each class. The algebra changes but the semantics do not: a $k$-$\mathsf{OV}$ witness already chooses one vector from each class, $k$-$\mathsf{XOR}$ uses equations over $\mathbb{F}_2$ to enforce the group pattern, and $k$-$\mathsf{SUM}$ uses exact signed coordinates that are packed into one residue modulo a power of two. Because the target constructions are depth-zero projections, all circuit lower-bound work remains on the colored-subgraph side.

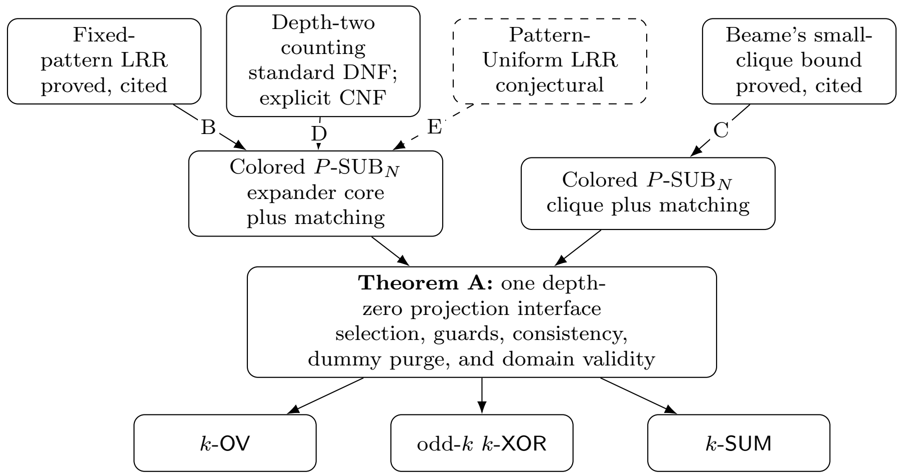


Figure 1: Proof architecture. Solid boxes and arrows denote proved ingredients; the dashed box and arrow denote Pattern-Uniform LRR. The expander family carries B, D, and E, while the clique family carries C; see Table 3. All four paths use the same target interface in Theorem A.

**Why two pattern families appear.** The strongest available source statement depends on the circuit regime. For the Li–Razborov–Rossman colored pattern parameter $\kappa(P)$, a treewidth-like graph parameter that controls the source exponent (Section 2.2), a bounded-degree expander core satisfies $\kappa(P) = \Omega(k)$, so the fixed-pattern theorem [LRR17] supplies an exponent linear in $k$, and the same exactly padded family also has no isolated vertices, has $\Theta(k)$ vertices, and contains a vertex of degree at least two, which are the only pattern properties used by the depth-two counting proof; neither expansion nor $\kappa$ enters that argument. A clique core supports Beame's lower bound [Bea90] uniformly while the clique size grows; the pattern-edge allowance limits the clique order to $\Theta(\sqrt{k})$, while Beame's depth-independent upper range is $r \le \log N$, together yielding the source scale $r = \Theta(\min\{\sqrt{k}, \log N\})$ used in Theorem C. Under the host substitutions above, $\log N = \Theta(\log n)$ for $k$-$\mathsf{OV}$ and $\log N = \Theta(\log(n/k))$ for the list targets; in the subpolynomial regime both are $\Theta(\log n)$, which is why the target statement is displayed with $\min\{\sqrt{k}, \log n\}$.

**Exact counting at depth two.** After flattening adjacent gates with the same connective, a depth-two circuit is either a DNF, an OR of AND-terms, or a CNF, an AND of OR-clauses. Here an edge variable is the Boolean source input recording one possible colored host edge. For the DNF orientation, consider the minimal positive input consisting exactly of the edge variables of one source witness, or colored copy. Deleting any selected variable removes the only present edge from one pattern-edge group, so the input becomes rejecting. Any DNF term accepting this input must therefore contain every selected edge variable positively. Because the pattern has no isolated vertices and has $\Theta(k)$ vertices, distinct source maps give distinct colored copies and force $N^{\Omega(k)}$ distinct terms. For the CNF orientation, monotonicity lets us remove negative literals, after which each clause is a set of edge variables meeting every colored copy; call such a set a transversal. For each inclusion-minimal transversal, any CNF for the function must contain a clause included in it, and minimality forces equality. To generate many of them, choose a pattern vertex $a$ of degree $\delta \ge 2$. Independently for each host label $i \in [N]$, choose one incident pattern edge $h(i)$ and include every variable on $h(i)$ that assigns label $i$ to $a$. Every colored copy assigns some label $i$ to $a$ and therefore meets this set. Conversely, for any included variable $x$, fixing the endpoint labels encoded by $x$ and choosing all other labels arbitrarily produces a colored copy whose unique intersection with the set is $x$, proving minimality. The $\delta^N \geq 2^N$ choices of $h$ give distinct minimal transversals, and $2^N \geq N^{\Omega(k)}$ in the theorem's range $N \geq k^2$. Thus both depth-two orientations require size $N^{\Omega(k)}$.

**Where parity and carries enter.** The two target effects arise at different logical stages. For $k$-$\mathsf{XOR}$, the obstruction appears while enforcing selection: equations over $\mathbb{F}_2$ see group multiplicities only modulo two, so they cannot by themselves exclude the branch in which the anchor is unselected and every group contributes an even number of candidates; an odd $k$ leaves that branch an odd number of slots to fill with dummies, which a single anti-dummy row rejects, whereas an even $k$ does not. For $k$-$\mathsf{SUM}$, signed integer coordinates enforce the desired support exactly for both parities, so the projection itself loses nothing. Once a support $S \in \binom{[n]}{k}$ is fixed, i.e., that is, once the $k$ selected indices have been chosen, the remaining $k$-$\mathsf{XOR}$ or $k$-$\mathsf{SUM}$ predicate checks only whether those entries satisfy the corresponding zero-XOR or zero-sum relation. Under a two-point restriction, either fixed-support predicate becomes the complement of PARITY, and hence remains PARITY-hard at every fixed depth as $k$ grows. The quantitative distinction is that $k$-$\mathsf{XOR}$ has a depth-two fixed-support verifier of size $m \cdot 2^{O(k)}$, whereas the direct $k$-$\mathsf{SUM}$ verifier costs $2^{\Theta(km)}$; the top-disjunction depth-three circuit of Proposition 71 guesses block carries and removes the extra factor of $m$ in the exponent at the principal width $m = \Theta(k \log(en/k))$. Thus the odd-$k$ loss is a selection phenomenon specific to $k$-$\mathsf{XOR}$, while the carry overhead is a verification-cost phenomenon specific to $k$-$\mathsf{SUM}$. Section 8 develops this distinction further after the formal proofs.

### 1.4 Related work

**Direct lower bounds for Orthogonal Vectors.** Kane and R. Ryan Williams prove lower bounds for Orthogonal Vectors in branching programs, Boolean formulas over bounded-fan-in complete bases, and formulas whose unbounded-fan-in gates compute arbitrary symmetric functions; in their main regimes these bounds are within $\widetilde{O}(D)$ factors of the natural upper bounds [KW19, Thms. 2, 3, and 5]. Choudhury, Limaye, Sreenivasaiah, and Srinivasan later sharpen the bounded-fan-in formula and branching-program bounds in the regime $D > c \log n$, where $c > 1$ is constant, obtaining $\Omega(n^2 D)$ for formulas and $\Omega(n^2 D/\log(nD))$ for branching programs [CLSS26, Thms. 6 and 25]. Kane and Williams's lower-bound argument uses a non-product restriction. Separately, for each fixed bias $p \in (0, 1)$, they construct $\mathsf{AC}^0$ formulas of size $n^{2-\varepsilon_p}$, for some $\varepsilon_p > 0$, that are correct on a $1 - o(1)$ fraction of instances under the $p$-biased product distribution [KW19, Thm. 6]. They also formulate a depth-three $\mathsf{AC}^0$ circuit lower bound for worst-case Orthogonal Vectors as a conjecture [KW19, Conj. 10]. These formula and branching-program models differ from general unbounded-fan-in $\mathsf{AC}^0$ circuits, so the results are precursors and motivation rather than statements subsumed by ours.

Choudhury and Sreenivasaiah study layered top-disjunction depth-three circuits through disjunctions of restricted bottom functions. They prove that, for $k \leq D$, a disjunction of $t$-CNFs computing the *unpromised* $k$-$\mathsf{OV}$ function, in which vectors may repeat within an array, has top fan-in, and hence size under our convention, $\Omega((n/t)^k)$; more generally, the bottom gates may be unate functions of unbounded fan-in provided that at most $t$ inputs have negative polarity [CS26, Thms. 1.1, 1.2, and 5.12]. They also prove a parameterized lower bound for the opposite depth-three orientation with no bottom-fan-in restriction, yielding a $2^{\Omega(n)}$ lower bound for the unpromised 2-OV function when $D = \Omega(n^2)$ [CS26, Thm. 1.3]. When $k = O(1)$ and $k \leq t = O(1)$, their main bound matches the $n^k$ exponent of the brute-force construction; for general $t$, their paper records a remaining gap in the top-/bottom-fan-in tradeoff. The promise obstruction differs between the two arguments. In the top-disjunction argument, every maxterm has at most one vector other than $\vec{1}$

in each array, so no maxterm satisfies pairwise distinctness once $n \geq 3$ [CS26, Prop. 4.4 and proof of Thm. 5.12]. In the opposite-orientation argument, the image of the projection contains arrays with repeated vectors, so a circuit required to be correct only on promised inputs need not decide the entire projected source function. Thus neither proof by itself lower-bounds $\mathrm{size}_3(k\text{-}\mathsf{OV}_{n,D,k})$ under the distinctness promise of Definition 7. These results concern circuit models and parameter regimes different from the unconditional lower bounds proved here.

The Choudhury–Limaye–Sreenivasaiah–Srinivasan work cited above also proves quantitatively stronger lower bounds for unrestricted fixed-depth circuits in a different dimension regime. Its main constant-depth theorem shows that, for fixed constants $k, d \geq 2$ and $\varepsilon > 0$, every depth-$d$ circuit computing the monotone complement of $k$-$\mathsf{OV}$ at dimension $D = n^{\varepsilon}$ has size at least $n^{k-\varepsilon}$; because the circuit model is nonmonotone, they observe that the same statement may be phrased directly for $k$-$\mathsf{OV}$ [CLSS26, Thm. 4 and Footnote 4]. They also prove the monotone-circuit analogue of OVC for the complement of the unpromised two-set Orthogonal Vectors function at logarithmic dimension; in the proof's 0-distribution, every unchosen position is filled with $1^D$, and Lemma 20 uses that filler directly [CLSS26, Thm. 5; construction of $\mathcal{D}_0$, Step 4; and Lem. 20]. Their 1-distribution is pairwise distinct with high probability, so the promise sensitivity enters specifically through the 0-distribution. Their transfer is projection-based: a split-and-list construction maps $\ell$-hyperclique in a $u$-uniform hypergraph on $v$ vertices to the target by listing all $\ell/k$-subsets and paying dimension $O(v^u)$ [CLSS26, Thm. 11]. The listed vectors are pairwise distinct within each array, so this transfer is compatible with the promise in Definition 7. This gives a near-maximal exponent at every fixed depth for fixed $k$, while their discussion records a barrier at $D = \Omega((\log n)^2)$ for the underlying reduction framework [CLSS26, Rem. 16]. Our results instead work at $O(k \log n)$-scale budgets, allow $k$ to grow, and cover $k$-$\mathsf{XOR}$ and $k$-$\mathsf{SUM}$ through the same interface.

**Broader Orthogonal Vectors–circuit interfaces.** Abboud, Bringmann, Dell, and Nederlof show that falsifying the moderate-dimensional Orthogonal Vectors Conjecture would yield unexpected speedups for weighted hypergraph clique and sparse $\mathsf{TC}^1$-circuit satisfiability [ABDN18]. R. Ryan Williams develops a different win–win connection between OVC and nonuniform lower bounds [RW25]: one branch gives lower bounds for exact-threshold and equality-matrix representations, while the other yields nearly linear algorithms for logarithmic-dimensional Orthogonal Vectors together with further nonuniform consequences. These works establish important interfaces between fine-grained complexity and circuit complexity, but they do not give direct worst-case lower bounds for the present target functions in standard $\mathsf{AC}^0$. Our route instead transfers unconditional source-function lower bounds through depth-zero projections and does not assume OVC.

**Constant-depth lower bounds for subgraph isomorphism.** The source side belongs to the line of constant-depth lower bounds for detecting small subgraphs: Beame's small-clique bound, Rossman's $k$-Clique theorem, Amano's lower bounds for uncolored general graph and hypergraph patterns (extending a weaker-exponent form of Rossman's method), and the structural theory of colored subgraph isomorphism developed by Li, Razborov, and Rossman [Bea90, Ros08, Ama10, LRR17]. Li, Razborov, and Rossman identify the colored fixed-pattern exponent within a logarithmic factor of treewidth and prove minor-monotonicity of $\kappa_{\mathrm{col}}$; on the function side, their graph-minor reductions for structured colored subgraph isomorphism are linear-size monotone projections. Rosenthal subsequently closes their factor-two gap in the average-case exponent [Ros21, Thm. 1.3], proves that the embedding parameter $\mathrm{emb}(G)$ underlying Marx's ETH-hardness result is $O(\kappa(G))$ [Ros21, Thm. 1.5], and separates $\kappa$ from treewidth: for the $t$-dimensional hypercube $Q_t$, one has $\kappa(Q_t) = \Theta\Big(\mathrm{tw}(Q_t)/\sqrt{\log \mathrm{tw}(Q_t)}\Big)$ [Ros21, Thm. 1.4 and the discussion following it]. Our source menu uses the fixed-pattern Li–Razborov–Rossman theorem for Theorem B and Beame's clique lower bound for Theorem C, while the depth-two source theorem is proved here. The fixed-pattern quantifiers are essential: Pattern-Uniform LRR strengthens the host-size uniformity across a growing pattern family and is not known to follow from the published theorem.

**Fine-grained algorithms and Orthogonal Vectors.** The ETH and SETH formulations of Impagliazzo and Paturi and the sparsification and reduction framework of Impagliazzo, Paturi, and Zane underlie the modern fine-grained program [IP01, IPZ01]. Vassilevska Williams surveys the resulting exponent-preserving methodology, and Chen and R. Ryan Williams identify a broad equivalence class around two-set Orthogonal Vectors under truly subquadratic reductions [VW18, CW19]. This literature motivates both the choice of Orthogonal Vectors and our insistence on preserving exponent dependence, but its conditional running-time lower bounds are logically separate from the nonuniform circuit lower bounds proved here.

**Algorithmic and average-case work on $k$-SUM and $k$-XOR.** Wagner's generalized-birthday algorithm initiated a central algorithmic line for finding short zero-sum and XOR relations in dense groups [Wag02]. Dinur, Keller, and Klein establish essentially tight conditional bounds for dense average-case $k$-$\mathsf{SUM}$ and $k$-$\mathsf{XOR}$ for $k \leq 5$, and in restricted parameter ranges for larger $k$ [DKK24], while Agrawal, Saha, Schwartzbach, Vanukuri, and Vasudevan study sparse and planted regimes, hardness amplification, reductions, and cryptographic applications [ASS+24]. Dalirrooyfard, Lincoln, Saha, and Vassilevska Williams establish conditional average-case hardness for parity-counting variants of $k$-$\mathsf{OV}$, $k$-$\mathsf{SUM}$, and $k$-$\mathsf{XOR}$ under explicit distributions [DLSV25]. This literature motivates the algebraic targets and their sensitivity to parameters, but it concerns uniform algorithms and distributional or counting problems with different success criteria and computational models. The present results are worst-case nonuniform $\mathsf{AC}^0$ lower bounds and do not imply security for any cryptographic construction.

**Comparison of regimes.** Existing direct results give strong Orthogonal-Vectors-related lower bounds in four distinct settings: structurally restricted top-disjunction depth-three circuits when $k \leq D$, the opposite depth-three orientation without a bottom-fan-in restriction at dimension $D = \Omega(n^2)$, unrestricted fixed-depth circuits for fixed $k$ at polynomial dimension, and monotone circuits for the unpromised two-set complement at logarithmic dimension. Our results occupy a complementary region: $O(k \log n)$-scale constraint budgets, growing $k$, three target functions, and a common depth-zero transfer, with an unconditional exponent linear in $k$ at depth two. The resource units in these comparisons are not uniform: Kane–Williams use formula and branching-program size in some results [KW19, Thms. 2 and 3] and count wires in their symmetric-gate theorem and depth-three conjecture [KW19, Thm. 5; Conj. 10]; Choudhury–Limaye–Sreenivasaiah–Srinivasan use formula or branching-program size [CLSS26]; and Choudhury–Sreenivasaiah count gates or middle CNFs [CS26], whereas $\mathrm{size}_d$ here counts non-input gates. The comparisons above are therefore model-and-regime comparisons, not numerical identifications across complexity measures. The depth-three and higher-depth linear-in-$k$ frontier is stated conditionally rather than folded into the unconditional claims.

### 1.5 Organization

Section 2 presents colored subgraph isomorphism, the source lower bounds, and the two pattern families. Section 3 isolates the depth-zero projection interface, and Section 4 realizes it for $k$-$\mathsf{OV}$, odd-$k$ $k$-XOR, and $k$-SUM. Section 5 derives the fixed-$k$ consequences. Section 6 proves the unconditional growing-$k$ frontier, including the depth-two result, and records the complementary row-rich PARITY route together with its projection-saturation limit. Section 7 states Pattern-Uniform LRR and derives the conditional completion, and Section 8 synthesizes the parity and carry phenomena and records the open problems. Appendices A to F contain the source formalities, pattern constructions, full projection proofs, parameter completions, supplementary $k$-XOR results,and elementary upper bounds.

## 2 Colored Subgraph Isomorphism and the Source Menu

Throughout, $k$ denotes the number of target objects selected by a witness, and every corresponding source pattern has exactly $k-1$ edges. The source problem is a structured colored form of subgraph isomorphism in which the color classes are built into the input coordinates.

### 2.1 The structured source and the circuit model

**The source function.** Let $P$ be a finite simple loopless undirected graph. Write $v(P) := |V(P)|$, $e(P) := |E(P)|$, and $\Delta(P)$ for its maximum degree, and fix an orientation $f = (a_f, b_f)$ of every edge $f \in E(P)$. The orientation is bookkeeping only: it names the two host indices in each input coordinate and does not change the undirected pattern.

**Definition 1** (Colored $P$-subgraph isomorphism)**.** For $N \geq 1$, the input to $P\text{-SUB}_N$ consists of variables

$$X_{f,u,w} \in \{0,1\}, \qquad f = (a_f, b_f) \in E(P), \qquad u, w \in [N]. \tag{1}$$

The variable $X_{f,u,w}$ records whether the colored host contains the edge between $(a_f, u)$ and $(b_f, w)$. The function accepts exactly when there is a map $\phi : V(P) \to [N]$ such that

$$X_{f,\phi(a_f),\phi(b_f)} = 1 \qquad \text{for every } f \in E(P). \tag{2}$$

Equivalently, for each pattern edge $f = (a_f, b_f)$, one may select a host pair $(u_f, w_f) \in [N]^2$ with $X_{f,u_f,w_f} = 1$. These selections define an accepting map precisely when all edges incident to the same non-isolated pattern vertex assign that vertex the same host index; any isolated pattern vertices may then be assigned arbitrary indices.

The host vertex set is $V(P) \times [N]$, with one color class $\{a\} \times [N]$ for each $a \in V(P)$. The map $\phi$ need not be injective as a map into $[N]$: if $a \neq b$, then $(a, \phi(a))$ and $(b, \phi(b))$ are distinct host vertices even when $\phi(a) = \phi(b)$. Appendix A proves that this function is exactly the structured problem $\text{SUBGRAPH}_{\text{col},N}(P)$ used by Li, Razborov, and Rossman [LRR17, Section 5, p. 960] under a bijection of input coordinates. Their host-size parameter is written $n$; throughout this paper it is renamed $N$, while $n$ is reserved for the target universe size.

The present-and-consistent one-edge-per-pattern-edge formulation in Definition 1 is the interface used by the generic framework and the three target instantiations in Sections 3 and 4.

Whenever a pattern $P$ is obtained from a core $F$ by adjoining disjoint matching edges, we first fix an orientation of $F$, then fix an orientation of $P$ whose restriction to $F$ is the chosen orientation of $F$, and orient the padding edges arbitrarily. This convention makes every later core-to-pattern projection coordinatewise unambiguous.

**Circuit conventions.** Throughout the paper, log denotes the base-two logarithm. We normalize circuits so that negations occur only at input leaves, and we count only non-input gates. Thus $\mathrm{size}_d(g)$ is the minimum number of non-input gates in an unbounded-fan-in AND/OR circuit of depth at most $d$ computing $g$. At depth three, write $\Sigma_3 := \mathsf{OR} \circ \mathsf{AND} \circ \mathsf{OR}$ and $\Pi_3 := \mathsf{AND} \circ \mathsf{OR} \circ \mathsf{AND}$, with

$$\mathrm{size}_3(g) = \min\{\mathrm{size}_{\Sigma_3}(g), \mathrm{size}_{\Pi_3}(g)\}. \tag{3}$$

After flattening adjacent equal gates, every depth-at-most-three circuit has one of these two orientations without increasing its number of non-input gates, which justifies Equation (3).

**Exponent rates, construction constants, and thresholds.** When a scalar denotes an exponent rate, we generally use $\gamma$, possibly with a subscript, for a rate measured in the source host size, and $\beta$ or $c$ for a rate measured in the target size. The inherited LRR edge weighting $\beta : E(P) \to [0, 2]$ in Appendix A, the structural constant $c_\kappa$ in Lemma 5, and Beame's clique rate $a_d$ in Fact 18 keep their own letters. A capital $C$ with one of the target subscripts OV, $\oplus$, or $\Sigma$ denotes a universal construction-budget constant; a $k$ with a subscript denotes an onset threshold on $k$; and symbols such as $n_1$, $N_0$, $L_\oplus$, and $L_\Sigma$ denote onset thresholds on the universe, host, or workable-width parameter. The symbols $c'_d$, $C_E(d)$ are exponents in polynomial host or universe thresholds such as $N, n \geq k^C$, not circuit-size rates.

### 2.2 Fixed-pattern hardness

The fixed-pattern source theorem and its expander corollary use the colored parameter $\kappa_{\mathrm{col}}(P)$ of Li, Razborov, and Rossman [LRR17, Def. 2.12(iii)]. We abbreviate it to $\kappa(P)$, following Rosenthal [Ros21, Footnote 1]; the uncolored parameter denoted by the same letter in parts of [LRR17] is never used in this paper. For this paper, the operational role of $\kappa(P)$ is as the source-host exponent in the fixed-pattern lower bound below; Theorem 4 supplies the structural estimates used to lower-bound it.

**Theorem 2** (Li–Razborov–Rossman fixed-pattern lower bound [LRR17])**.** *For every fixed simple loopless pattern $P$ with at least one edge and no isolated vertices, every fixed depth $d$, and every constant $\eta > 0$, there is a threshold $N_0(P, d, \eta)$ such that*

$$\mathrm{size}_d(P\text{-SUB}_N) + 2e(P)N^2 + 2 \geq N^{\kappa(P)-\eta} \tag{4}$$

*for every $N \geq N_0(P, d, \eta)$. If $\kappa(P) - \eta > 2$, then the threshold can be chosen so that the additive convention-bridge term is absorbed and* $\mathrm{size}_d(P\text{-SUB}_N) \geq N^{\kappa(P)-\eta}$.

The additive term in Equation (4) makes the import independent of whether the source's phrase "number of gates" includes variable, constant, or input-negation nodes; no result derived from Corollary 6 carries it, while the quantifier display in Section 7 restates the theorem in full. We state the import only for patterns without isolated vertices. Li–Razborov–Rossman do permit a single vertex as a base element of a union sequence [LRR17, Def. 2.11], so this is a conservative draft-side scope rather than an empty-sequence convention; it matches every application below and avoids relying on an unused isolated-vertex edge case in the $\alpha \equiv 1$ citation assembly. No connectedness hypothesis is imposed: the two padded pattern families are cores together with disjoint matchings, and [LRR17, Rem. 2.7] computes the relevant parameters for a disconnected pattern. The theorem is pointwise in the pattern: both the loss absorbed by $\eta$ and the onset threshold may depend on $P$. This distinction is harmless for fixed $k$, where the selected pattern is fixed as $N \to \infty$, but becomes the precise issue isolated by the pattern-uniform conjecture in Section 7. Appendix A gives the model, measure, notation, and citation assembly proving Theorem 2 for the structured function of Definition 1.

**Definition 3** (Edge expansion)**.** For a graph $P$ with at least two vertices, let

$$h(P) := \min_{\substack{\varnothing \neq S \subseteq V(P) \\ |S| \leq v(P)/2}} \frac{|E_P(S, V(P) \setminus S)|}{|S|}. \tag{5}$$

Equivalently, Equation (5) is the minimum of $|E_P(S, V(P) \setminus S)| / \min\{|S|, |V(P) \setminus S|\}$ over all nonempty proper sets $S \subsetneq V(P)$, which is the normalization used in [LRR17, Thm. 4.9].

**Theorem 4** ($\kappa$ from expansion, treewidth, and minors)**.** *For every simple loopless graph $P$ with at least one edge and no isolated vertices,*

$$\kappa(P) \geq \frac{v(P)h(P)}{3\Delta(P)}. \tag{6}$$

*Furthermore, $\kappa(P) \leq \mathrm{tw}(P) + 1$. Finally, $\kappa$ is minor-monotone: if $F$ is a minor of $P$, then $\kappa(F) \leq \kappa(P)$.*

*Proof.* The three assertions are [LRR17, Thm. 4.9], [LRR17, Prop. 4.3], and [LRR17, Thm. 5.1], respectively. None imposes a connectivity hypothesis. Although [LRR17, Def. 2.11] permits single-vertex bases, we adopt the no-isolated-vertices scope stated in the theorem; this is the only regime used below and is also the standing scope of Rosenthal's corresponding restatements [Ros21, Thm. 3.8(ii),(iii)]. Footnote 2 of [Ros21] identifies those restatements with the corresponding Li–Razborov–Rossman results. Every pattern used in this paper, i.e, the expander and clique core-plus-matching families, has no isolated vertices, as do the ambient padded graphs in every minor-monotonicity application. In particular, a bounded-degree family with $h(P) = \Omega(1)$ has $\kappa(P) = \Omega(v(P))$ [Ros21, Cor. 3.9(i)]. ☐

The theorem supplies all structural information about $\kappa$ needed below. On a bounded-degree expander core $F$, Equation (6) gives $\kappa(F) = \Omega(v(F))$. Adjoining a disjoint matching need not preserve expansion, but $F$ remains a minor of the resulting padded pattern, so minor-monotonicity transfers this lower bound. The treewidth upper bound in Theorem 4 situates $\kappa$ below the familiar treewidth exponent; Remark 39 records that the two parameters have the same linear scale on the expander cores used here.

**Lemma 5** (Padded expander patterns)**.** *There are universal constants $k_0 \in \mathbb{N}$ and $c_\kappa > 0$ such that, for every integer $k \geq k_0$, there is a simple loopless graph $P_k^{\mathrm{exp}}$ with exactly $k-1$ edges and maximum degree 7, obtained from a simple 7-regular expander core by adjoining a disjoint matching, for which*

$$\kappa(P_k^{\mathrm{exp}}) \geq c_\kappa(k-1). \tag{7}$$

*One may take $c_\kappa = 1/147$, and $k_0$ may be chosen so that $c_\kappa(k_0 - 1) > 4$.*

*Proof.* Appendix B.1 constructs the core by applying Alon's exact-size transformation [Alo21] to the simple near-Ramanujan source graphs of Mohanty, O'Donnell, and Paredes [MOP20], verifies that the transformed graph remains simple, combines the discrete Cheeger inequality in Fact 36 with Theorem 4, and pads to exactly $k-1$ edges by a matching. The degree-7 calculation gives the stated universal constant. ☐

**Corollary 6** (Universal fixed-$k$ source rate)**.** *Fix any constant $\gamma$ with $0 < \gamma < c_\kappa$. For every fixed depth $d$ and every fixed integer $k \geq k_0$, there is a threshold $N_0(d,k)$ such that*

$$\mathrm{size}_d(P_k^{\exp}\text{-SUB}_N) \geq N^{\gamma(k-1)} \tag{8}$$

*for every $N \geq N_0(d,k)$.*

*Proof.* The threshold fixed in the construction satisfies $c_\kappa(k_0 - 1) > 4$. Fix $d$ and $k \geq k_0$, put $\overline{\gamma} := (c_\kappa + \gamma)/2$, and set $\eta := (c_\kappa - \overline{\gamma})(k-1) > 0$. Then

$$\kappa(P_k^{\exp}) - \eta \geq \overline{\gamma}(k-1) \geq \frac{c_\kappa}{2}(k-1) > 2.$$

The pure non-input-gate consequence in Theorem 2 therefore gives, for every sufficiently large $N$,

$$\mathrm{size}_d(P_k^{\exp}\text{-SUB}_N) \geq N^{\kappa(P_k^{\exp})-\eta} \geq N^{\overline{\gamma}(k-1)} \geq N^{\gamma(k-1)}.$$

Absorbing all preceding thresholds into $N_0(d,k)$ proves the claim. $\square$

The threshold in Corollary 6 is a threshold on the host size $N$. A later target-side threshold $n_1(d,k)$ is obtained only after substituting a host size $N = N(n,k)$ that tends to infinity with the target universe; Lemma 11 records the target-side substitutions and estimates used for this step.

### 2.3 The source menu

The paper uses two source families because the strongest available source lower bound depends on the circuit regime; these are the two pattern-family branches in Figure 1. Table 3 records where each lower-bound statement or proof and each pattern construction appears.

Table 3: The source families used in the lower-bound transfers.

| Source family | Property used | Detailed locations | Results carried |
|---|---|---|---|
| bounded-degree expander core plus matching | $\kappa(P_k^{\exp}) = \Omega(k)$; also $v(P_k^{\exp}) = \Theta(k)$, no isolated vertices, and a vertex of degree at least 2 | Lemma 5; construction in Appendix B.1 | Theorems 17, 21 and 28 |
| $K_r$ plus matching | Beame's small-clique lower bound [Bea90] | Fact 18; construction and projections in Appendix B.2 | Theorem 19 |

Theorem 21 is attached to the expander family because that family is already available with exactly $k-1$ edges, has $\Theta(k)$ vertices, has no isolated vertices, and contains a vertex of degree at least two. Its depth-two proof uses the latter three structural properties but neither expansion nor $\kappa$. The clique family is not bounded-degree when $r$ grows, so the two rows do not share a degree hypothesis.

## 3 The Projection Framework

The source function asks for one present host edge for each edge of the pattern, with agreement at shared endpoints. This section isolates that anatomy from the algebra used to enforce it. The resulting interface has one common universe skeleton, four semantic roles, and one domain-validity role; Section 4 realizes them separately through orthogonality, addition over $\mathbb{F}_2$, and addition over the integers.

### 3.1 Targets and depth-zero projections

We first fix the input conventions for the three targets, including the pairwise-distinctness promise for $k$-$\mathsf{OV}$ and the indexed-list semantics used by $k$-$\mathsf{XOR}$ and $k$-$\mathsf{SUM}$.

**Definition 7** (The three target problems)**.** The target families are defined as follows.

(i) For $n \le 2^D$, an input to $k\text{-}\mathsf{OV}_{n,D,k}$ consists of $k$ ordered arrays, each containing $n$ vectors in $\{0,1\}^D$; this is a $knD$-bit encoding. Write $U_i = (u_{i,1}, \dots, u_{i,n})$, and impose the promise that the vectors within each array are pairwise distinct. The function accepts exactly when there are indices $j_1, \dots, j_k \in [n]$ such that $\prod_{i=1}^k u_{i,j_i}(t) = 0$ for every $t \in [D]$.

(ii) An input to $k\text{-}\mathsf{XOR}_{n,m,k}$ is an indexed list $(a_1, \dots, a_n) \in (\mathbb{F}_2^m)^n$. The function accepts exactly when there is a set $S \in \binom{[n]}{k}$ such that $\bigoplus_{i \in S} a_i = 0^m$.

(iii) An input to $k\text{-}\mathsf{SUM}_{n,m,k}$ is an indexed list $(z_1, \dots, z_n) \in (\mathbb{Z}_{2^m})^n$. The function accepts exactly when there is a set $S \in \binom{[n]}{k}$ such that $\sum_{i \in S} z_i \equiv 0 \pmod{2^m}$.

For the promised $k$-$\mathsf{OV}$ function, $\mathrm{size}_d$ denotes the minimum size of a circuit that is correct on every promised input.

The promise formulation of $k$-$\mathsf{OV}$ is equivalent to presenting each class as a set: the order of an array is irrelevant to the function value. A lower bound for this promised function automatically applies to the unrestricted array variant, because every circuit correct when repetitions are allowed is also correct on pairwise-distinct arrays. By contrast, the indices, rather than the values, are the objects selected in $k$-$\mathsf{XOR}$ and $k$-$\mathsf{SUM}$, so distinct indices may carry equal vectors or equal residues. This asymmetry is essential: the two list reductions use repeated dummy objects, whereas the $k$-$\mathsf{OV}$ construction must land inside the pairwise-distinct promise.

**Definition 8** (Projection)**.** For possibly promised Boolean functions $F$ and $G$, write $F \le_{\mathrm{proj}} G$ if there is a map $R$ from the promise domain of $F$ into the promise domain of $G$ such that $F(x) = G(R(x))$ for every promised input $x$ and every output bit of $R$ is a constant, an input bit, or the negation of an input bit.

We call such a map a *depth-zero projection*: it substitutes constants and literals for target inputs and therefore adds neither gates nor circuit depth.

**Lemma 9** (Projection monotonicity)**.** *If $F \le_{\mathrm{proj}} G$, then $\mathrm{size}_d(G) \ge \mathrm{size}_d(F)$ for every depth $d$. The same implication holds for each fixed circuit orientation, such as $\Sigma_3$ or $\Pi_3$.*

*Proof.* Substitute the constants and literals of the projection for the input leaves of a circuit computing $G$ on its promise domain. Because the projection maps every promised input of $F$ into that domain, the resulting circuit computes $F$ on its promise domain. The substitution adds no gates and no depth, and it preserves the orientation of every internal gate. □

### 3.2 The common universe skeleton

Fix an integer $k \ge 2$ and a simple loopless pattern $P$ with $e(P) = k-1$, together with the orientation $f = (a_f, b_f)$ of each edge fixed in Section 2.1. For every $f \in E(P)$ and $(u, w) \in [N]^2$, introduce a candidate object $c_{f,u,w}$ representing the proposal that the pattern edge $f$ is realized by the host edge from $(a_f, u)$ to $(b_f, w)$. We also introduce one anchor object $\alpha$. Thus the genuine objects have the form

$$\{\alpha\} \,\dot\cup \bigcup_{f \in E(P)} \{c_{f,u,w} : (u, w) \in [N]^2\}. \tag{9}$$

For $k$-XOR and $k$-SUM these objects occupy one indexed list, so their total number is $1 + e(P)N^2$; for $k$-OV, the anchor and the $e(P)$ edge groups become $k$ separate classes, each edge class containing $N^2$ genuine vectors. Dummies fill the remaining positions.

The anchor compensates for the one-object gap between the $k-1$ edge groups and a target witness of size $k$. In the additive targets it is also the pivot of the selector equations: comparing every group count with the anchor indicator forces one candidate per group rather than zero candidates per group. For $k$-OV, selection already chooses one vector from each class, so the anchor serves only as the additional class needed to reach $k$ classes.

For a pattern vertex $a$ incident to an oriented edge $f = (a_f, b_f)$, define the label proposed by a candidate by

$$\mathrm{lab}_a(f, u, w) := \begin{cases} u, & a = a_f, \\ w, & a = b_f. \end{cases} \tag{10}$$

Put $\ell_N := \lceil \log N \rceil$. We use the $\ell_N$-bit binary encoding of $x-1$ for each label $x \in [N]$, and write $\mathrm{bit}_t(x)$ for its $t$-th bit, where $t \in [\ell_N]$.

For each non-isolated vertex $a$, fix one reference incident edge $\rho(a)$, and let

$$\mathcal{I}(P) := \{(a, g) : a \in V(P),\ \deg_P(a) \geq 1,\ g \ni a,\ g \neq \rho(a)\}. \tag{11}$$

The set $\mathcal{I}(P)$ contains one comparison for every non-reference incidence, and

$$|\mathcal{I}(P)| = \sum_{a:\deg_P(a)\geq 1} (\deg_P(a) - 1) \leq \sum_{a \in V(P)} \deg_P(a) = 2e(P). \tag{12}$$

An implementation of the skeleton must enforce the following roles, summarized in Table 4.

(R1) **Selection rigidity.** The witness selects the anchor and exactly one candidate from each edge group.

(R2) **Guard.** A selected candidate $c_{f,u,w}$ is admissible only when $X_{f,u,w} = 1$.

(R3) **Consistency.** For each pattern vertex $a$, all selected candidates from edges incident to $a$ propose the same value under $\mathrm{lab}_a$.

(R4) **Purge.** No dummy belongs to an accepting witness.

(R5) **Promise validity for $k$-OV.** Within each $k$-OV class, all $n$ vectors are pairwise distinct, without changing which one-per-class selections are orthogonal.

The first four roles identify accepting witnesses with the present-and-consistent edge selections described in Definition 1. The fifth does not alter that witness semantics, but it is essential for the image of the $k$-OV map to lie in the promise domain of Definition 7. Obtaining it with only $O(\log n)$ additional coordinates is therefore a strength of the construction rather than a cosmetic representation choice.

Three target-side effects determine the final parameter statements. First, each edge group contains $N^2$ candidates. Since $k$-OV stores different groups in different classes, it permits $N^2 \leq n$ and later yields a base-$n$ bound; $k$-XOR and $k$-SUM store all groups in one list, require $1 + e(P)N^2 \leq n$, and later yield a base-$(n/k)$ bound. Second, the $\mathbb{F}_2$ selector sees cardinalities only modulo two, which creates the odd-$k$ restriction in the direct $k$-XOR projection. Third, the $k$-SUM construction packs $O(k)$ signed coordinates into one residue, producing the bit-width cost $O(k \log(kN))$. Constants such as $c_\kappa$ and the onset threshold in the source lower bound are inherited from Section 2 and are logically separate from these three effects.

Table 4: How the three target constructions realize the common witness roles.

| Target | Selection rigidity (R1) | Guard and purge (R2, R4) | Consistency (R3) | Domain condition (R5) | Constructed budget |
|---|---|---|---|---|---|
| $k$-OV | built into the one-vector-per-class witness | one coordinate per class | two coordinates per compared label bit | inert identifiers enforce pairwise distinctness | $D_0 = O(k \log(2n))$ |
| $k$-XOR | $e(P)$ selector rows, for odd $k$ | compressed separating labels and one anti-dummy row | one row per compared label bit | total indexed-list domain | $m_\oplus = O(k \log(2N))$ |
| $k$-SUM | exact signed group coordinates | one nonnegative guard and one dummy coordinate | one signed coordinate per comparison | total indexed-list domain | $m_\Sigma = O(k \log(2kN))$ |

## 3.3 Master projections and host substitutions

The next theorem records exactly what the three implementations provide. Its bounds are construction budgets, not asymptotic lower bounds; source hardness enters only after a pattern family and a host size have been chosen.

**Theorem 10** (A: master projections)**.** *There are universal constants $C_{\mathrm{OV}}, C_\oplus, C_\Sigma > 0$ such that the following holds. Let $k \geq 2$, let $P$ be a simple loopless pattern with $e(P) = k-1$, and fix an orientation of its edges. Then the following depth-zero projections exist.*

*(i) If $N^2 \leq n$ and $D \geq D_0(P,N,n)$, then $P\text{-SUB}_N \leq_{\mathrm{proj}} k\text{-}\mathsf{OV}_{n,D,k}$, where $D_0(P,N,n) \leq C_{\mathrm{OV}} k \log(2n)$. Moreover, $D_0(P,N,n) \geq \lceil \log n \rceil$, so the hypothesis on $D$ automatically ensures $n \leq 2^D$.*

*(ii) If $k$ is odd, $1 + e(P)N^2 \leq n$, and $m \geq m_\oplus(P,N)$, then $P\text{-SUB}_N \leq_{\mathrm{proj}} k\text{-}\mathsf{XOR}_{n,m,k}$, where $m_\oplus(P,N) \leq C_\oplus k \log(2N)$. The compressed guard labels are fixed nonuniformly, once for the pair $(P,N)$ and before the source input is read.*

*(iii) If $1 + e(P)N^2 \leq n$ and $m \geq m_\Sigma(P,N)$, then $P\text{-SUB}_N \leq_{\mathrm{proj}} k\text{-}\mathsf{SUM}_{n,m,k}$, where $m_\Sigma(P,N) \leq C_\Sigma k \log(2kN)$. This projection has no parity restriction.*

*Proof.* Part (i) is Theorem 13, part (ii) is Theorem 15, and part (iii) is Theorem 16. The exact definitions of $D_0(P,N,n)$, $m_\oplus(P,N)$, and $m_\Sigma(P,N)$ appear in the corresponding subsections, and Appendix C contains the complete correctness and projection proofs. The absolute estimates follow from Equations (12), (21), (22), (29), (31) and (32), after fixing the three displayed constants sufficiently large. □

The theorem deliberately leaves the host size $N$ free. In particular, it does not impose the common substitution $N = \Theta(\sqrt{n/k})$, because that would discard the stronger packing available for $k$-$\mathsf{OV}$.

**Lemma 11** (Standard host substitutions)**.** *Let $k \geq 2$ and $n \geq 16k$, and define the $k$-*$\mathsf{OV}$ *host size and the common list-target host size by*

$$N_{\mathrm{OV}} := \lfloor \sqrt{n} \rfloor, \qquad N_{\oplus,\Sigma} := \left\lfloor \sqrt{\frac{n-1}{k-1}} \right\rfloor. \tag{13}$$

*For every simple loopless pattern $P$ with $e(P) = k-1$, these choices satisfy*

$$N_{\mathrm{OV}}^2 \leq n, \qquad 1 + (k-1)N_{\oplus,\Sigma}^2 \leq n, \tag{14}$$

*and*

$$N_{\mathrm{OV}} \geq \frac{1}{2}\sqrt{n}, \qquad\qquad \log N_{\mathrm{OV}} \geq \frac{1}{4}\log n, \tag{15}$$

$$N_{\oplus,\Sigma} \geq \frac{1}{2}\sqrt{\frac{n}{k}}, \qquad\qquad \log N_{\oplus,\Sigma} \geq \frac{1}{4}\log\frac{n}{k}. \tag{16}$$

*The constants in Theorem 10 may be fixed so that, for the same substitutions,*

$$D_0(P, N_{\mathrm{OV}}, n) \leq C_{\mathrm{OV}} k \log n, \tag{17}$$

$$m_{\oplus}(P, N_{\oplus,\Sigma}) \leq C_{\oplus} k \log(\mathrm{e}n/k), \tag{18}$$

$$m_{\Sigma}(P, N_{\oplus,\Sigma}) \leq C_{\Sigma} k \log n. \tag{19}$$

*If in addition $n \geq k^3$, then the last estimate sharpens to*

$$m_{\Sigma}(P, N_{\oplus,\Sigma}) \leq C_{\Sigma} k \log(\mathrm{e}n/k). \tag{20}$$

*Proof.* The capacity inequalities are immediate from the definitions. Because $n/k \geq 16$, both quantities inside the floors are at least 4, and $\lfloor x \rfloor \geq x/2$ for $x \geq 2$. Moreover, $(n-1)/(k-1) \geq n/k$ when $n \geq k$, which gives the two lower bounds on the host sizes. Taking logarithms yields $\log N_{\mathrm{OV}} \geq \frac{1}{2}\log n - 1 \geq \frac{1}{4}\log n$ and $\log N_{\oplus,\Sigma} \geq \frac{1}{2}\log(n/k) - 1 \geq \frac{1}{4}\log(n/k)$.

For the budgets, Theorem 10 gives the native bounds in terms of $\log(2n)$, $\log(2N)$, and $\log(2kN)$. The first is $O(\log n)$. Also $N_{\oplus,\Sigma} \leq \sqrt{n/(k-1)} \leq \sqrt{2n/k}$, so $\log(2N_{\oplus,\Sigma}) = O(\log(\mathrm{e}n/k))$ and $\log(2kN_{\oplus,\Sigma}) = O(\log n)$ uniformly for $n \geq 16k$. If $n \geq k^3$, then $kN_{\oplus,\Sigma} \leq \sqrt{2kn} \leq \sqrt{2}\, n/k$, and hence $\log(2kN_{\oplus,\Sigma}) = O(\log(\mathrm{e}n/k))$. Enlarging the three universal constants once establishes all four displayed inequalities. ☐

The lemma is purely target-side: it packages the repeated floor and budget arithmetic but inserts no source lower bound. Each later theorem remains responsible for checking that its chosen host size lies beyond the onset required by its own source statement.

# 4 Three Instantiations

We now implement the roles of Section 3.2. The constructions deliberately use the same candidate labels and the same reference-edge comparisons, so that their differences are confined to the algebra of the target primitive.

### 4.1 $k$-Orthogonal Vectors

An orthogonality coordinate rejects a selected tuple exactly when every chosen vector has entry 1 there. Selection rigidity is therefore automatic: a witness already chooses one vector from each class. The remaining complication is that a two-class equality test must forbid the two ordered disagreement patterns separately.

Put $\ell_n := \lceil \log n \rceil$, and

$$s_{k,n} := \left\lceil \frac{k\ell_n}{k-1} \right\rceil, \qquad D_0(P, N, n) := k + 2|\mathcal{I}(P)|\ell_N + s_{k,n}. \tag{21}$$

Here $\ell_N$ counts label bits, whereas $\ell_n$ counts identifier bits. Since $k \geq 2$, one has $s_{k,n} \leq 2\ell_n$; together with Equation (12), the inequality $N^2 \leq n$ implies

$$D_0(P, N, n) = O(k \log(2N) + \log(2n)) = O(k \log(2n)). \tag{22}$$

The $k$ target classes, i.e., the $k$ input arrays of Definition 7, are an anchor class $U_\alpha$ and one edge class $U_f$ for every $f \in E(P)$. The anchor class contains one genuine vector $v_\alpha$, while $U_f$ contains the $N^2$ genuine vectors $v_{f,u,w}$ indexed by $(u, w) \in [N]^2$; each class is padded to cardinality $n$ with dummies. The structural coordinates are as follows.

**Guards (R2).** There is one coordinate $q_h$ for every class $h \in \{\alpha\} \cup E(P)$. On $q_\alpha$, the genuine anchor has entry 0 and every other vector has entry 1. On $q_f$, a genuine vector $v_{f,u,w}$ has entry $\overline{X}_{f,u,w}$, while every vector in every other class and every dummy in $U_f$ has entry 1. Thus a genuine edge vector satisfies its guard exactly when the proposed edge is present, and any dummy causes the guard of its own class to fail.

**Consistency (R3).** Fix $(a, g) \in \mathcal{I}(P)$, write $f := \rho(a)$, and let $t \in [\ell_N]$. On the coordinate $C^{10}_{a,g,t}$, a candidate in class $f$ carries $\mathrm{bit}_t(\mathrm{lab}_a(f, u, w))$, a candidate in class $g$ carries $1 - \mathrm{bit}_t(\mathrm{lab}_a(g, u, w))$, and every vector in every other class has entry 1. The coordinate $C^{01}_{a,g,t}$ complements the two active entries in the opposite way. For selected label bits $b_f, b_g \in \{0, 1\}$, the two coordinate products on the selected tuple are $b_f(1 - b_g)$ and $(1 - b_f)b_g$, so both vanish exactly when $b_f = b_g$. Ranging over all $t$ and all $(a, g) \in \mathcal{I}(P)$ enforces full-label agreement at every non-isolated pattern vertex.

**Dummies and identifiers (R4, R5).** Dummies are set to 1 on every guard and consistency coordinate. Zero-vector padding would instead make every selected tuple containing a dummy automatically orthogonal, so we use the all-ones structural choice; Fact 43 gives the one-line failure proof. The structural coordinates need not distinguish all vectors within a class, and simply appending unpinned binary identifiers need not preserve a genuine orthogonal witness, as Fact 44 records. We therefore use identifiers that are inert for every selected tuple.

**Lemma 12** (Inert identifiers). *There are $s_{k,n}$ identifier coordinates such that every coordinate is pinned to 0 throughout one owner class, while every class is unpinned on at least $\ell_n$ coordinates. The $n$ vectors of each class can consequently be assigned pairwise distinct identifiers, and the product over every selected tuple is identically zero on each identifier coordinate.*

The complete proof and an explicit balanced ownership assignment appear in Appendix C.1. Combining the structural coordinates with these identifiers gives genuine promised inputs with $n$ vectors in each class, without changing which selected tuples are orthogonal.

**Theorem 13** ($k$-$\mathsf{OV}$ projection)**.** *Let $k \geq 2$ and let $P$ be a simple loopless pattern with $e(P) = k-1$. For every $N, n$ with $N^2 \leq n$ and every $D \geq D_0(P, N, n)$, the construction above gives a depth-zero projection*

$$P\text{-SUB}_N \leq_{\text{proj}} k\text{-}\mathsf{OV}_{n,D,k}. \tag{23}$$

*Equivalently, the constructed $k$-$\mathsf{OV}$ instance has a one-vector-per-class orthogonal witness if and only if the source instance contains a colored copy of $P$. Since $s_{k,n} \geq \ell_n$, the hypothesis $D \geq D_0(P, N, n)$ also implies $n \leq 2^D$, so the projection lands in the promise domain of $k$-$\mathsf{OV}_{n,D,k}$.*

The proof in Appendix C.1 follows the five roles directly. A source embedding selects the anchor and one present, label-consistent candidate from each edge class; conversely, the class guards remove every dummy, the edge guards certify presence, and the two-coordinate comparisons recover one common host label at each pattern vertex. The inert identifiers place the output inside the pairwise-distinct promise. Every output bit is a constant or a negated source variable. Dimensions above $D_0(P, N, n)$ are obtained by appending all-zero coordinates.

## 4.2 Odd $k$-XOR

Retain $\ell_N$ and the binary label encoding fixed in Section 3.2. For $k$-$\mathsf{XOR}$, all objects lie in one indexed list, so selection rigidity must be enforced algebraically. The construction has one anchor column, one candidate column $c_{f,u,w}$ for each $f \in E(P)$ and $(u, w) \in [N]^2$, and dummy columns padding the list to length $n$.

For a selected support $S$, let $\zeta \in \{0, 1\}$ indicate whether the anchor is selected, let $c_f$ be the number of selected candidates from group $f$, and let $d$ be the number of selected dummies. A selector row for $f$ has entry 1 on the anchor and every group-$f$ candidate and entry 0 elsewhere, so a zero sum imposes

$$\zeta + c_f \equiv 0 \pmod 2. \tag{24}$$

The anti-dummy row has entry 1 on every dummy and 0 on every genuine column. Together with the selector equations, the support-size identity is

$$\zeta + \sum_{f \in E(P)} c_f + d = k = e(P) + 1. \tag{25}$$

These equations prove support rigidity when $k$ is odd. If $\zeta = 1$, every $c_f$ is a positive odd integer, and Equation (25) forces $c_f = 1$ for every $f$ and $d = 0$. If $\zeta = 0$, every $c_f$ is even and the anti-dummy row makes $d$ even, so the support size is even, contradicting that $k$ is odd. Thus every zero-sum $k$-support contains the anchor, exactly one candidate from each edge group, and no dummies.

The guard must reject every support containing at least one absent edge. Private guard rows would do so but would cost $e(P)N^2$ rows. Instead, a standard random-labelling argument with a union bound compresses them into

$$r_{\text{guard}}(P, N) := \lceil 2e(P) \log N + e(P) + 1 \rceil \tag{26}$$

rows.

**Lemma 14** (Separating guard labels)**.** *There are labels $\lambda_{f,u,w} \in \mathbb{F}_2^{r_{\text{guard}}(P,N)}$ such that, for every choice $(u_f, w_f) \in [N]^2$ for each $f \in E(P)$ and every nonempty $T \subseteq E(P)$,*

$$\bigoplus_{f \in T} \lambda_{f,u_f,w_f} \neq 0. \tag{27}$$

*The labels depend only on $(P, N)$ and may be fixed nonuniformly before the source input is read.*

The probabilistic proof is in Appendix C.2. At the integer value in Equation (26), its union bound is

$$N^{2e(P)}2^{e(P)}2^{-r_{\mathrm{guard}}(P,N)} \le \frac{1}{2}. \tag{28}$$

Using these labels, write $r_g := r_{\mathrm{guard}}(P, N)$ and define the remaining rows as follows.

**Compressed guards (R2).** For each $h \in [r_g]$, the entry of candidate $c_{f,u,w}$ is $\overline{X}_{f,u,w}\lambda_{f,u,w}(h)$, and the anchor and all dummies have entry 0. Present candidates contribute 0, while the selected absent candidates contribute the XOR of their labels, which is nonzero by Equation (27).

**Consistency (R3).** For every $(a, g) \in \mathcal{I}(P)$, with $f := \rho(a)$, and every $t \in [\ell_N]$, one row places $\mathrm{bit}_t(\mathrm{lab}_a(\cdot))$ on every candidate in groups $f$ and $g$ and places 0 elsewhere. Once the selectors have chosen one candidate from each group, the row sum is the XOR of the two proposed label bits and vanishes exactly when they agree. Unlike orthogonality, one $\mathbb{F}_2$ equation forbids both disagreement patterns.

The exact constructed row budget is

$$m_{\oplus}(P, N) := e(P) + r_{\mathrm{guard}}(P, N) + |\mathcal{I}(P)|\ell_N + 1 = O(k \log(2N)), \tag{29}$$

where the four terms are the selectors, compressed guards, consistency rows, and anti-dummy row, respectively.

**Theorem 15** ($k$-$\mathsf{XOR}$ projection for odd $k$)**.** *Let $k \ge 3$ be odd, and let $P$ be a simple loopless pattern with $e(P) = k - 1$. For every $N, n$ with $1 + e(P)N^2 \le n$ and every $m \ge m_{\oplus}(P, N)$, the construction above gives a depth-zero projection*

$$P\text{-}\mathrm{SUB}_N \le_{\mathrm{proj}} k\text{-}\mathsf{XOR}_{n,m,k}. \tag{30}$$

The complete proof is in Appendix C.2. It shows that a zero-sum support uses only present candidates and is label-consistent, and it checks that every matrix entry is a constant or a negated source variable. Larger row counts are reached by appending all-zero rows.

The oddness condition is an artifact of exact selection over $\mathbb{F}_2$, not of colored subgraph isomorphism. When $k$ is even, the branch $\zeta = 0$ makes every $c_f$ even and also leaves an even number of dummies, so the anti-dummy row no longer distinguishes it; whenever at least $k$ dummy indices are available, the all-dummy support already satisfies every row. The black-box lifting projection is Lemma 65; Corollary 67 gives the quantitative consequence for any supplied admissible odd source parameter. The body-level bound is Equation (43).

### 4.3 $k$-SUM

The $k$-$\mathsf{SUM}$ construction works natively over the integers. A black-box additive, that is, group-homomorphic, encoding of the $\mathbb{F}_2$ construction into $\mathbb{Z}_{2^m}$ cannot preserve all zero relations; Proposition 50 gives the formal obstruction. We instead encode selection, consistency, presence, and dummy rejection by exact signed coordinates and then pack those coordinates into one residue.

The indexed list again contains the anchor, all $e(P)N^2$ candidates, and repeated dummy residues. Associate with every index $j$ an integer vector $\mathrm{vec}(j) \in \mathbb{Z}^{R(P)}$, where

$$R(P) := e(P) + |\mathcal{I}(P)| + 2 \le 3e(P) + 2 = O(k). \tag{31}$$

For a selected support $S$, let $\zeta \in \{0, 1\}$ indicate whether the anchor is selected, let $c_f$ count selected candidates from group $f$, and let $d$ count selected dummies. The coordinates of $\mathrm{vec}(j)$ are the following.

**Group coordinates (R1).** For each $f \in E(P)$, the coordinate $G_f$ is $-1$ on the anchor, $+1$ on every group-$f$ candidate, and 0 elsewhere. On a selected support it equals $c_f - \zeta$, so vanishing enforces the exact equality $c_f = \zeta$ over $\mathbb{Z}$.

**Consistency coordinates (R3).** For $(a, g) \in \mathcal{I}(P)$, write $f := \rho(a)$. The coordinate $C_{a,g}$ assigns $+\mathrm{lab}_a(g, u, w)$ to a group-$g$ candidate, $-\mathrm{lab}_a(f, u, w)$ to a group-$f$ candidate, and 0 elsewhere. Once one candidate is selected from each group, it is the signed difference of the two complete labels and vanishes exactly when they agree. Thus one integer coordinate replaces the $\Theta(\log N)$ bitwise comparisons used by $k$-OV and $k$-XOR, although the carry-safe packing in Equation (32) later allocates $\Theta(\log(2kN))$ bits per integer coordinate.

**Guard and dummy coordinates (R2, R4).** The guard coordinate $Q$ assigns $\overline{X}_{f,u,w} \in \{0, 1\}$ to candidate $c_{f,u,w}$ and 0 to the anchor and dummies. Its selected sum is nonnegative and vanishes exactly when every selected edge is present. The dummy coordinate $Q_{\mathrm{dum}}$ is 1 on dummies and 0 on genuine objects, so it counts selected dummies exactly.

These exact coordinates already force the desired support shape. If all coordinate sums vanish, then the dummy coordinate gives $d = 0$ and every group coordinate gives $c_f = \zeta$, so the support-size identity becomes $k = \zeta + \sum_{f \in E(P)} c_f + d = k\zeta$. Hence $\zeta = 1$, every $c_f = 1$, and no dummy is selected.

To pack these signed vectors, we use the standard large-base positional-encoding device introduced in Karp's reduction from Exact Cover to Knapsack [Kar72], where the base is chosen to exceed the largest attainable digit so that no carry propagates between coordinates. We use it in signed form, with digits in $[-kN, kN]$ and a power-of-two base, and correct for the modular ambient group in Equation (35). Set

$$q := \lceil \log(2kN + 1) \rceil, \qquad B := 2^q, \qquad m_\Sigma(P, N) := qR(P). \tag{32}$$

Fix an ordering of the $R(P)$ coordinates and define

$$\Phi(z_0, \ldots, z_{R(P)-1}) := \sum_{i=0}^{R(P)-1} z_i B^i. \tag{33}$$

Every $k$-support sum $y_S := \sum_{j \in S} \mathrm{vec}(j)$ satisfies $\|y_S\|_\infty \le kN$, while $B > 2kN$. Consequently the balanced base-$B$ representation is faithful:

$$\Phi(y_S) \equiv 0 \pmod{2^{m_\Sigma(P,N)}} \iff y_S = 0. \tag{34}$$

The proof is a digit induction given in Lemma 53.

For each index $j$, let $\widehat{a}_j := \Phi(\mathrm{vec}(j)) \bmod 2^{m_\Sigma(P,N)}$ be the standard residue in $[0, 2^{m_\Sigma(P,N)})$. When the requested bit-width is $m \ge m_\Sigma(P, N)$, define

$$a_j := 2^{m - m_\Sigma(P,N)} \widehat{a}_j \in [0, 2^m). \tag{35}$$

Simply viewing $\widehat{a}_j$ as a low-bit $m$-bit integer is not sound: negative exact packed values wrap modulo $2^{m_\Sigma(P,N)}$, and a true witness can leave a nonzero multiple of that smaller modulus. The top-bit scaling in Equation (35) preserves divisibility exactly, because $2^m \mid 2^{m - m_\Sigma(P,N)} Z$ if and only if $2^{m_\Sigma(P,N)} \mid Z$.

**Theorem 16** ($k$-SUM projection). *Let $k \geq 2$ and let $P$ be a simple loopless pattern with $e(P) = k-1$. For every $N, n$ with $1 + e(P)N^2 \leq n$ and every $m \geq m_\Sigma(P, N)$, the construction above gives a depth-zero projection*

$$P\text{-SUB}_N \leq_{\text{proj}} k\text{-}\mathsf{SUM}_{n,m,k}. \tag{36}$$

*Moreover, $m_\Sigma(P, N) = O(k \log(2kN))$, and the projection holds for both parities of $k$.*

The complete proof is in Appendix C.3. The exact support argument above leaves one candidate from every group and no dummies; consistency and the nonnegative guard then recover a colored embedding. Although the packing uses ordinary integer carries, every packed candidate depends on only the single bit $X_{f,u,w}$, so each output bit is one of two constants as that bit varies and is therefore a constant, $X_{f,u,w}$, or $\overline{X}_{f,u,w}$. No parity condition appears anywhere in the argument.

## 5 Unconditional Lower Bounds for Fixed $k$

For fixed $k$, the strongest target consequences use the standard host substitutions of Lemma 11: $N_{\text{OV}} = \lfloor \sqrt{n} \rfloor$ for $k$-$\mathsf{OV}$ and $N_{\oplus,\Sigma} = \lfloor \sqrt{(n-1)/(k-1)} \rfloor$ for the two list targets. The first is available because every edge group occupies its own $k$-$\mathsf{OV}$ class, whereas the second is forced because all $k-1$ edge groups share one indexed list in $k$-$\mathsf{XOR}$ and $k$-$\mathsf{SUM}$. Thus the base-$n$ versus base-$(n/k)$ distinction below is a target-packing effect, not a difference in source hardness.

Although the depth-two result Theorem 21 already applies to sufficiently large fixed $k$, Theorem 17 is not subsumed by it. Its distinctive content is an exponent linear in $k$ at every fixed depth, with one target-side rate uniform in both $d$ and $k$.

**Theorem 17** (B: unconditional lower bounds for fixed $k$). *Let $k_0 \in \mathbb{N}$ be the universal threshold of Lemma 5, and let $C_{\text{OV}}, C_\oplus, C_\Sigma$ be the universal construction constants fixed in Theorem 10 and lemma 11. There is a universal constant $\beta > 0$, independent of $k$, $d$, and $n$, such that for every fixed depth $d$ and every fixed integer $k \geq k_0$ there is a threshold $n_1(d, k)$ for which the following hold for every $n \geq n_1(d, k)$:*

$$\text{size}_d(k\text{-}\mathsf{OV}_{n,D,k}) \geq n^{\beta(k-1)} \qquad \textit{for every } D \geq C_{\text{OV}} k \log n, \tag{37}$$

$$\text{size}_d(k\text{-}\mathsf{XOR}_{n,m,k}) \geq (n/k)^{\beta(k-1)} \qquad \textit{for odd } k \textit{ and every } m \geq C_\oplus k \log(en/k), \tag{38}$$

$$\text{size}_d(k\text{-}\mathsf{SUM}_{n,m,k}) \geq (n/k)^{\beta(k-1)} \qquad \textit{for every } m \geq C_\Sigma k \log(en/k). \tag{39}$$

*The same rate $\beta$ works simultaneously for every fixed $d$ and every fixed $k \geq k_0$; only the onset threshold depends on $(d, k)$.*

*Proof.* Let $c_\kappa$ be the constant of Lemma 5, and choose universal constants

$$0 < 2\beta < \gamma < c_\kappa. \tag{40}$$

Apply Corollary 6 with the source rate $\gamma$, so that for every fixed $(d, k)$ and all $N \geq N_0(d, k)$,

$$\text{size}_d(P_k^{\exp}\text{-SUB}_N) \geq N^{\gamma(k-1)}. \tag{41}$$

For $k$-$\mathsf{OV}$, put $N = N_{\text{OV}}$. Enlarge $n_1(d, k)$ so that $n \geq 16k$, $N \geq N_0(d, k)$, and $n^{\gamma/2-\beta} \geq 4^{\gamma/2}$. By Equations (14), (15) and (17), the $k$-$\mathsf{OV}$ projection is admissible at every $D \geq C_{\text{OV}} k \log n$, and Lemma 9 and eq. (41) give

$$\text{size}_d(k\text{-}\mathsf{OV}_{n,D,k}) \geq N^{\gamma(k-1)} \geq (n/4)^{\gamma(k-1)/2} \geq n^{\beta(k-1)}.$$

For $k$-XOR and $k$-SUM, put $N = N_{\oplus,\Sigma}$. Enlarge $n_1(d,k)$ further so that $n \geq \max\{16k, k^3\}$, $N \geq N_0(d,k)$, and $(n/k)^{\gamma/2-\beta} \geq 4^{\gamma/2}$. Then Equations (14), (16), (18) and (20) make the respective projections admissible at the displayed budgets. The odd-$k$ projection for $k$-XOR and the parity-free projection for $k$-SUM, followed by Equations (16) and (41), yield

$$\mathrm{size}_d(Q_{n,m,k}) \geq N^{\gamma(k-1)} \geq \left(\frac{n}{4k}\right)^{\gamma(k-1)/2} \geq (n/k)^{\beta(k-1)}, \qquad Q \in \{k\text{-XOR}, k\text{-SUM}\},$$

with the oddness qualification in the $k$-XOR case. Enlarging the single threshold $n_1(d,k)$ to satisfy all preceding requirements proves the theorem. $\square$

The substantive uniformity assertion in Theorem 17 is its quantifier order. Suppressing only the constraint parameters and retaining the odd-$k$ qualification for $k$-XOR, it is

$$\begin{gathered} \exists\, \beta > 0,\ k_0 \quad \forall\, d \quad \forall\, k \geq k_0 \quad \exists\, n_1(d,k) \quad \forall\, n \geq n_1(d,k): \\ \mathrm{size}_d(k\text{-OV}) \geq n^{\beta(k-1)}, \qquad \mathrm{size}_d(k\text{-SUM}) \geq (n/k)^{\beta(k-1)}, \\ k \text{ odd} \Longrightarrow \mathrm{size}_d(k\text{-XOR}) \geq (n/k)^{\beta(k-1)}. \end{gathered} \tag{42}$$

In particular, the constant hidden by the customary notation $n^{\Omega(k)}$ is not allowed to deteriorate with either $k$ or the depth. The proof obtains this target rate $\beta$ from the universal source rate $\gamma$ under the explicit slack condition $2\beta < \gamma$; Remark 40 records the corresponding source-side quantifier form. The factor e inside $\log(\mathrm{e}n/k)$ merely keeps the displayed budget positive in small boundary regimes; it has no asymptotic effect once $n/k \to \infty$.

The direct $k$-XOR projection, and hence Equation (38), is restricted to odd $k$. The odd-to-even projection in Lemma 65 applies whenever an even target parameter $K$ is written as

$$K = tr + s, \qquad t \geq 2, \qquad r \geq k_0 \text{ odd}, \qquad 0 \leq s < 2t, \qquad s = 0 \text{ or } t \nmid s.$$

For every such supplied decomposition, Corollary 67 gives a universal constant $C'_\oplus > 0$ such that every fixed depth $d$ admits a threshold $n'_1(d,K,t,r,s)$ for which

$$\mathrm{size}_d(k\text{-XOR}_{n',m',K}) \geq (n'/K)^{\beta(r-1)/2} \tag{43}$$

for all $n' \geq n'_1(d,K,t,r,s)$ and every $m' \geq C'_\oplus K \log n'$, where $\beta$ is the universal rate in Theorem 17.

Theorems 59 and 60 give the corresponding lower bounds away from the principal $O(k \log n)$-scale row and width budgets of Theorem 17. At the principal budgets, the elementary circuits of Propositions 69 to 71 give the comparison in Table 5.

Proposition 72 shows that the specific $\kappa$-based regular-core-plus-matching route used for Theorem 17 remains separated from the brute-force leading exponent by a factor greater than the core degree; Remark 73 delimits this as a limitation of that route rather than a general barrier.

For $k$-SUM, Proposition 71 retains the depth-two DNF of size $2^{\Theta(km)}$ but also gives a top-disjunction depth-three block-carry circuit. At the principal width $m = \Theta(k \log(\mathrm{e}n/k))$ and in the asymptotic fixed-$k$ regime, the block-carry circuit has size $(n/k)^{O(k)}$ and closes, for $\Sigma_3$, the exponent-scale gap created by the direct $2^{\Theta(km)}$ verifier. It does not provide a same-depth upper bound at depth two or for $\Pi_3$. The general-width estimates in Equations (183) and (184) separate the residual support-enumeration gap at smaller widths from the carry overhead at very large widths.

The parity and carry mechanisms underlying these comparisons are synthesized in Section 8.

Table 5: Same-depth exponent-scale comparisons at the principal fixed-$k$ budgets. Each lower bound is specialized to top-disjunction depth three, and all elementary upper bounds are $\Sigma_3$ circuits; the $k$-XOR row uses the direct odd-$k$ statement. No claim is made about leading constants in the exponent.

| Target | Transferred lower bound | Elementary $\Sigma_3$ upper bound | Exponent-scale verdict |
|---|---|---|---|
| $k$-OV | $n^{\beta(k-1)}$ | $n^{k+o(1)}$ | same-orientation match at $\Sigma_3$ and scale $n^{\Theta(k)}$ |
| $k$-XOR | $(n/k)^{\beta(k-1)}$ | $(n/k)^{k+o(1)}$ | same-orientation match at $\Sigma_3$ and scale $(n/k)^{\Theta(k)}$ |
| $k$-SUM | $(n/k)^{\beta(k-1)}$ | $(n/k)^{O(k)}$ | same-orientation match at $\Sigma_3$; scale $(n/k)^{\Theta(k)}$, with only $O(k)$ on the upper side |

# 6 Unconditional Lower Bounds for Growing $k$

The fixed-pattern theorem used in Section 5 does not control its onset threshold as the pattern grows. This section therefore changes the source lower bound while leaving every target projection unchanged. A padded clique pattern gives an unconditional floor at every fixed depth. Direct DNF-term and CNF-clause counting give an exponent linear in $k$ at depth two. The section closes by summarizing the unconditional frontier and comparing it with a complementary row-rich PARITY route.

## 6.1 A clique fallback at every fixed depth

A clique packs many pattern edges into few pattern vertices. This vertex deficiency weakens the exponent from linear in $k$ to order $\sqrt{k}$, but it also lets us invoke a source lower bound that is uniform while the clique size grows. The only other restriction is the small-clique range of Beame's theorem, which produces the plateau at $k = \Theta(\log^2 n)$.[1]

**The imported PRAM statement and notation.** Beame works with PRIORITY CRCW PRAMs on an $N$-node graph represented by $\binom{N}{2}$ Boolean input cells, one per unordered vertex pair; every non-input cell is initially 0, and the answer must occupy a designated cell $C_1$ after the final step. No computability condition is imposed on the transition functions, so the model is nonuniform. His function $\mathit{Clique}_r^N$ is the total monotone function accepting exactly the $N$-node graphs containing an $r$-clique, hence it is the function $K_r$-CLIQUE$_N$ of Definition 41. For a depth-$d$ circuit with $G$ non-input gates, the pointwise dictionary is

$$n_{\text{Bea90}} = N, \qquad m_{\text{Bea90}} = \binom{N}{2}, \qquad k_{\text{Bea90}} = r,$$
$$T_{\text{Bea90}} = T \le d+2, \quad c(n)_{\text{Bea90}} = G + \binom{N}{2} + O(1), \quad \mathit{Clique}_k^n = K_r\text{-CLIQUE}_N.$$

Throughout [Bea90, Sec. 2], $n$ is the number of graph vertices and $m = \binom{n}{2}$ is the number of input variables; the phrase "$n$ inputs" in Corollary 3.8 is therefore a notational slip. Theorem 3.1(b)

[1] The use of Beame's small-clique lower bound [Bea90] as the source statement for this section was suggested by the AI language model GPT-5.5; the authors independently verified its applicability and developed the resulting gate-count consequence (Fact 18) and Theorem 19.

of [Bea90] states the memory-cell bound $c(N) \geq N^{r/(43T^3)}$, even with infinitely many processors, for $r \leq \log N$, for $r$ above one absolute threshold, and for all sufficiently large $N$; its proof also uses $c(N) \geq N$. We quote this PRAM statement and, for the constant, the three terminal cases of its proof. We do not use [Bea90, Cor. 3.8]: that corollary does not define its circuit "size," and its one-sentence simulation does not resolve the gate-versus-wire convention.

**Fact 18** (Gate-count consequence of Beame's small-clique lower bound)**.** *For every fixed depth $d$, there are a constant $a_d > 0$ and integers $r_d, N_d \geq 1$ such that*

$$\mathrm{size}_d(K_r\text{-CLIQUE}_N) \geq N^{a_d r} \tag{44}$$

*where $K_r$-CLIQUE$_N$ is the total monotone function on $\binom{N}{2}$ edge variables that accepts exactly when the represented graph contains an $r$-clique; see Definition 41. The bound holds whenever $N \geq N_d$ and $r_d \leq r \leq \log N$. In particular, the upper cap $r \leq \log N$ is depth-independent; only the exponent rate and the lower onset may depend on $d$. The proof permits $a_d := 1/(2000(d+2)^3)$ and $r_d \geq 3000(d+2)^3$, after enlarging $r_d$ to absorb the source lower cutoff.*

*Proof.* Let $C$ be a depth-$d$ circuit for $K_r$-CLIQUE$_N$ with $G$ non-input gates. Propagate constant gates and flatten every edge joining gates of the same type, neither of which increases the depth or $G$. Give each of the $\binom{N}{2}$ input variables and each non-input gate one memory cell, together with one junk cell, and use one processor per circuit wire. The unrestricted processor count is legitimate because Beame's theorem explicitly permits infinitely many processors. Every non-input cell starts at 0, as required by his model. An OR-gate cell stores the gate value, whereas an AND-gate cell stores its complement. When evaluating a layer, a wire processor writes 1 to its gate cell exactly when its predecessor makes the stored disjunction true. Beame's model has every processor write somewhere at each step, so a nontriggered or idle processor writes 0 to the junk cell; writing 0 to the gate cell would destroy the PRIORITY implementation of OR. Thus every processor writing to a gate cell writes the same value 1, so PRIORITY resolves the concurrent write correctly; if no processor writes there, the initial 0 is the correct stored value. Gate-to-gate wires can test the required event from the predecessor cell because adjacent gate types alternate, while positive and negated input literals are handled by the processor's local transition rule. Beame's designated output cell $C_1$ is itself an input cell and therefore cannot serve as an accumulator during the simulation. Evaluating one circuit layer per PRAM step and then using one final step to copy the output, with a polarity flip when the output gate is an AND gate, into $C_1$ takes at most $T \leq d+2$ steps. Hence $C$ yields a PRIORITY CRCW PRAM with $c(N) := G + \binom{N}{2} + O(1)$ memory cells. Moreover, $c(N) \geq N$ for $N \geq 3$, as used in Beame's memory-cell argument.

Set $a := \log_N c(N)$. Beame states the exponent $r/(43T^3)$, but we use the weaker $r/(1000T^3)$ because it is what the three terminal cases in the proof of [Bea90, Thm. 3.1(b)] establish uniformly for all $T \geq 1$. If $a \geq r/6$, then $a \geq r/(1000T^3)$ because $T \geq 1$. If $T \geq (3/10)(r/a)^{1/3} - 2$, then

$$a \geq \frac{27r}{1000(T+2)^3} \geq \frac{r}{1000T^3};$$

where the second inequality uses $T \geq 1$. This branch reaches the published constant only once $T > 39$ (that is, $T \geq 40$ for integer $T$), whereas our $T = d + O(1)$ may be a small fixed integer. In the remaining terminal case, Beame's displayed inequality $343T^3a/(8r) \geq 343/344$ gives $a \geq r/(43T^3)$ and hence the weaker bound. Consequently, the common conclusion of all three cases is

$$c(N) \geq N^{r/(1000T^3)} \geq N^{b_d r}, \qquad b_d := \frac{1}{1000(d+2)^3},$$

throughout the range $r \le \log N$, once the absolute clique-order cutoff and the sufficiently-large-$N$ condition are met.

Let $r_\star$ be the absolute clique-order cutoff in Beame's theorem, set $a_d := b_d/2$, and choose

$$r_d := \max\left\{r_\star, \left\lceil \frac{3}{b_d} \right\rceil\right\} = \Theta(d^3).$$

After enlarging $N_d$ if necessary, for every $r \ge r_d$ the preceding memory bound and the definition of $c(N)$ give

$$G \ge N^{b_d r} - \binom{N}{2} - O(1) \ge \frac{1}{2} N^{b_d r} \ge N^{a_d r},$$

which proves Equation (44) under the paper's non-input-gate size convention. □

The explicit choices in Fact 18 permit $a_d = \Theta(d^{-3})$ and $r_d = \Theta(d^3)$. Hence the interval $r_d \le r \le \log N$ can be nonempty only when $d = O((\log N)^{1/3})$; a convenient sufficient asymptotic regime is $d = o((\log N)^{1/3})$, subject also to $N \ge N_d$. All results below keep $d$ fixed.

The upper range $r \le \log N$ is the feature needed below. Rossman's stronger exponent is proved for every fixed clique order $r$, whereas a superconstant-$r$ extension is presented only as a possibility [Ros08, Thm. 1.2; Sec. 6, final paragraph before "Open Questions"]. In that same paragraph, Rossman's phrase "as is the case with the lower bounds of Lynch and Beame" records Beame's result as already covering superconstant clique order. Rossman's theorem therefore supplies no uniform onset threshold for the choice $r = r(n)$ used here.

We combine Fact 18 with the padded clique pattern $P^{\mathrm{clq}}_{k,r}$ of Definition 41. By Lemma 42, ordinary clique projects to colored clique because completeness forces the color-respecting map to be injective, and colored clique projects to the padded pattern by setting every padding-edge variable to 1.

**Theorem 19** (C: growing $k$ at every fixed depth)**.** *Fix a constant $\varepsilon > 0$. For every fixed depth $d$, the following hold along every sequence $k = k(n)$ satisfying $k \to \infty$ and $k \le n^{1-\varepsilon}$, for all sufficiently large $n$. Define*

$$\rho_{\mathrm{OV}} := \min\{\sqrt{k-1}, \log n\}, \qquad \rho := \min\{\sqrt{k-1}, \log(n/k)\}. \tag{45}$$

*Then*

$$\begin{aligned}
\mathrm{size}_d(k\text{-}\mathsf{OV}_{n,D,k}) &\ge \exp\big(\Omega_d(\rho_{\mathrm{OV}} \log n)\big) && \textit{for every } D \ge C_{\mathrm{OV}} k \log n, && (46)\\
\mathrm{size}_d(k\text{-}\mathsf{XOR}_{n,m,k}) &\ge \exp\big(\Omega_d(\rho \log(n/k))\big) && \textit{for odd } k \textit{ and every } m \ge C_\oplus k \log(en/k), && (47)\\
\mathrm{size}_d(k\text{-}\mathsf{SUM}_{n,m,k}) &\ge \exp\big(\Omega_d(\rho \log(n/k))\big) && \textit{for every } m \ge C_\Sigma k \log n. && (48)
\end{aligned}$$

*The implied constants in the three lower bounds depend only on $d$.*

*Proof.* Fix $d$, and let $a_d, r_d, N_d$ be supplied by Fact 18. We use the same argument for the three targets, with base parameter

$$B := \begin{cases} n, & Q = k\text{-}\mathsf{OV}, \\ n/k, & Q \in \{k\text{-}\mathsf{XOR}, k\text{-}\mathsf{SUM}\}, \end{cases}$$

and host size $N = N_{\mathrm{OV}}$ or $N = N_{\oplus,\Sigma}$ from Equation (13), respectively. Since $k \le n^{1-\varepsilon}$, one has $B \to \infty$ in every case, and eventually $n \ge 16k$. The host estimates in Equations (15) and (16) therefore give

$$\log N \ge \frac{1}{4} \log B. \tag{49}$$

Let $\rho_Q$ denote $\rho_{\mathrm{OV}}$ for $Q = k\text{-}\mathsf{OV}$ and $\rho$ otherwise, and set

$$r := \left\lfloor \frac{\rho_Q}{4} \right\rfloor. \tag{50}$$

Because $k \to \infty$ and $B \to \infty$, we have $\rho_Q \to \infty$, so $r \geq r_d$, $N \geq N_d$, and $r \geq \rho_Q/8$ for all sufficiently large $n$. The pattern-edge allowance follows from $r \leq \sqrt{k-1}$:

$$\binom{r}{2} \leq \frac{r^2}{2} \leq k - 1.$$

Beame's upper-range condition also holds, since $\rho_Q \leq \log B$ and therefore $r \leq \rho_Q/4 \leq \frac{1}{4}\log B \leq \log N$ by Equation (49). Thus Lemma 42 and fact 18 imply

$$\mathrm{size}_d(P^{\mathrm{clq}}_{k,r}\text{-SUB}_N) \geq \mathrm{size}_d(K_r\text{-CLIQUE}_N) \geq N^{a_d r}. \tag{51}$$

The pattern $P^{\mathrm{clq}}_{k,r}$ has exactly $k-1$ edges, so the appropriate projection in Theorem 10 applies. Its maximum degree is $r-1$, but this causes no budget loss: by Equation (12), the consistency count is governed by $|\mathcal{I}(P)| \leq 2e(P) = 2(k-1)$ rather than by $\Delta(P)$. With the universal constants fixed in Theorem 10 and lemma 11, Equations (17) and (18) give the displayed $k$-$\mathsf{OV}$ and $k$-$\mathsf{XOR}$ budgets, while Equation (19) gives the $k$-$\mathsf{SUM}$ width $m \geq C_\Sigma k \log n$. This is why Equation (48) requires the larger width $C_\Sigma k \log n$ rather than the sharper fixed-$k$ budget.

Composing the target projection with Equation (51) and using $r \geq \rho_Q/8$ and Equation (49), we obtain

$$\log \mathrm{size}_d(Q) \geq a_d r \log N \geq \frac{a_d}{32}\rho_Q \log B.$$

This is exactly Equations (46) to (48), with the oddness condition inherited only by $k$-$\mathsf{XOR}$. □

The restriction $k \leq n^{1-\varepsilon}$ ensures that the list-target host size grows and that $\log(n/k)$ is a meaningful asymptotic base. The larger $k$-$\mathsf{SUM}$ width requirement in Equation (48) is also genuine: at $N = \Theta(\sqrt{n/k})$, the exact requirement $m_\Sigma(P, N) = O(k\log(kN))$ is not uniformly $O(k\log(n/k))$ when $k$ approaches $n$. The sharper estimate in Equation (20) applies whenever $n \geq k^3$, including the parameter ranges used in Theorems 17 and 21, and Theorem 28.

**Corollary 20** (The growing-$k$ frontier and its plateau)**.** *For every fixed depth $d$ and constant $\varepsilon > 0$, the budgets of Theorem 19 imply, along every sequence $k = k(n) \to \infty$ with $k \leq n^{1-\varepsilon}$,*

$$\log \mathrm{size}_d \geq \Omega_{d,\varepsilon}\big(\min\{\sqrt{k}, \log n\} \cdot \log n\big) \tag{52}$$

*for all three targets, with $k$ odd for $k$-$\mathsf{XOR}$. In the subpolynomial regime $k = n^{o(1)}$, this sharpens to the common form*

$$\mathrm{size}_d \geq n^{\Omega_d(\min\{\sqrt{k}, \log n\})}. \tag{53}$$

*Consequently the exponent in base $n$ grows as $\sqrt{k}$ until $k = \Theta(\log^2 n)$ and then plateaus at order $\log n$; at $k = \Theta(\log^2 n)$ the lower bound is $\exp(\Omega_d(\log^2 n))$.*

*Proof.* Since $k \to \infty$, one has $\sqrt{k-1} = \Theta(\sqrt{k})$. Under $k \leq n^{1-\varepsilon}$, one has $\log(n/k) \geq \varepsilon \log n$, so the list-target expressions in Theorem 19 are bounded below by the right-hand side of Equation (52) up to a constant depending on $\varepsilon$; the $k$-$\mathsf{OV}$ expression already has that form. If $k = n^{o(1)}$, then $\log(n/k) = (1 - o(1))\log n$, so the dependence on $\varepsilon$ disappears and exponentiating gives Equation (53). The two terms in the minimum balance when $\sqrt{k} = \Theta(\log n)$. □

The two branches have a simple source-side interpretation. The edge allowance permits a clique on only $\Theta(\sqrt{k})$ vertices, because $K_r$ uses $\binom{r}{2}$ of the available $k-1$ edges; in contrast, the expander source has $\Theta(k)$ vertices. The source exponent tracks the clique's vertices and therefore rises only as $\sqrt{k}$. Once $r$ reaches $\Theta(\log N)$, Beame's upper range becomes the binding cap, and the lower bound remains at $\exp(\Omega_d(\log^2 n))$ even as $k$ continues to grow.

### 6.2 Depth two: an exponent linear in $k$

At depth two, no switching argument is needed. The DNF orientation uses the standard minimal-positive-input principle: each minimal positive input forces a distinct accepting term. The source-specific CNF orientation constructs exponentially many minimal transversals of the hypergraph of colored copies, each of which must appear as a distinct clause. We use the padded expander family $P_k^{\exp}$ of Lemma 5, but only because it has no isolated vertices, has $\Theta(k)$ vertices, and contains a vertex of degree at least two; expansion and $\kappa$ play no role.

For a map $\phi : V(P) \to [N]$, let

$$E_\phi := \{X_{f,\phi(a_f),\phi(b_f)} : f = (a_f, b_f) \in E(P)\}. \tag{54}$$

The assignment with positive support exactly $E_\phi$ is a minimal positive input of $P$-SUB$_N$, and

$$P\text{-SUB}_N = \bigvee_{\phi:V(P)\to[N]} \ \bigwedge_{x\in E_\phi} x. \tag{55}$$

**Theorem 21** (D: depth two, both orientations)**.** *There are universal constants $k_D \geq k_0$, $\gamma_D > 0$, and $\xi_D > 0$ such that the following hold.*

*(i) For every $k \geq k_D$ and every $N \geq k^2$,*

$$\mathrm{size}_2(P_k^{\exp}\text{-SUB}_N) \geq N^{\gamma_D k}. \tag{56}$$

*(ii) For every $k \geq k_D$, the following target bounds hold whenever the indicated range condition is satisfied:*

*(a) if $k \leq \xi_D n^{1/4}$, then*

$$\mathrm{size}_2(k\text{-}\mathsf{OV}_{n,D,k}) \geq n^{\Omega(k)} \tag{57}$$

*for every $D \geq C_{\mathrm{OV}} k \log n$;*

*(b) if $k \leq \xi_D n^{1/5}$, then*

$$\mathrm{size}_2(k\text{-}\mathsf{XOR}_{n,m,k}) \geq (n/k)^{\Omega(k)} \qquad \textit{for odd } k \textit{ and every } m \geq C_\oplus k \log(\mathrm{e}n/k), \tag{58}$$

$$\mathrm{size}_2(k\text{-}\mathsf{SUM}_{n,m,k}) \geq (n/k)^{\Omega(k)} \qquad \textit{for every } m \geq C_\Sigma k \log(\mathrm{e}n/k). \tag{59}$$

*All implied constants are universal.*

*Proof.* Fix $P = P_k^{\exp}$. We first lower-bound both possible top-gate orientations of a depth-two source circuit.

**DNF orientation.** Let $\mathcal{D}$ be a DNF, with arbitrary input negations, computing $P$-$\mathrm{SUB}_N$. For every $\phi$, the minimal positive input $E_\phi$ satisfies some term $T_\phi$ of $\mathcal{D}$. Every positive literal of $T_\phi$ lies in $E_\phi$. If the positive part omitted an edge variable $x \in E_\phi$, then the assignment setting exactly the positive literals of $T_\phi$ to 1 and every other variable to 0 would still satisfy the term, including all its negative literals, but its positive support would be contained in $E_\phi \setminus \{x\}$.

The set $E_\phi \setminus \{x\}$ contains no variable from the pattern-edge group to which $x$ belongs, so it cannot support any colored copy. This contradicts correctness of $\mathcal{D}$, and therefore the positive part of $T_\phi$ is exactly $E_\phi$. Distinct maps give distinct colored edge sets: if $\phi' \neq \phi$, choose a vertex $a$ on which they differ; because $P$ has no isolated vertices, an edge incident to $a$ contributes different input coordinates to $E_\phi$ and $E_{\phi'}$. Hence the map $\phi \mapsto T_\phi$ is injective, so every such DNF has at least

$$N^{v(P)} = N^{\Omega(k)} \tag{60}$$

terms, where the maximum-degree bound gives $v(P) \geq 2e(P)/7 = 2(k-1)/7$.

**CNF orientation.** By Equation (55), the function $P$-$\mathrm{SUB}_N$ is monotone. Let $\mathcal{C}$ be a CNF computing it. First discard every tautological clause, and then remove negative literals without increasing the number of clauses. Write a clause as $C = P_C \vee \neg N_C$, where $P_C$ is its positive part. Every 1-input satisfies $P_C$: otherwise, raising all variables in $N_C$ to 1 would preserve acceptance by monotonicity while falsifying $C$. Every 0-input still falsifies some positive part, because any original clause falsified on that input already has all its positive literals equal to 0. Thus replacing each clause by its positive part gives an equivalent monotone CNF.

A monotone clause is a transversal of the hypergraph $\{E_\phi : \phi : V(P) \to [N]\}$. Moreover, every minimal transversal must occur as a clause in any monotone CNF computing the function. To see this, let $W$ be minimal and set the variables in $W$ to 0 and all others to 1. Since $W$ meets every colored copy, this is a 0-input, so some clause $C$ is falsified and hence satisfies $C \subseteq W$. The clause $C$ is itself a transversal, and minimality of $W$ forces $C = W$.

Choose a pattern vertex $a$ of degree $\delta \geq 2$, and let $E_P(a)$ be its incident pattern edges. For every function $h : [N] \to E_P(a)$, define

$$W_h := \{X_{f,u,w} : \text{there is } i \in [N] \text{ with } f = h(i) \text{ and } \mathrm{lab}_a(f,u,w) = i\}. \tag{61}$$

Every colored copy meets $W_h$: if $\phi(a) = i$, then its variable for the edge $h(i)$ belongs to $W_h$. The transversal is minimal. For a variable $x \in W_h$ belonging to edge $f = h(i) = \{a, b\}$ and assigning the opposite endpoint the label $j$, choose a map $\phi$ with $\phi(a) = i$, $\phi(b) = j$, and arbitrary labels elsewhere. Its copy meets $W_h$ exactly in $x$, so deleting $x$ destroys the transversal property. Distinct functions $h$ give distinct transversals, and therefore every CNF has at least

$$\delta^N \geq 2^N \tag{62}$$

clauses. The function $x/\log x$ is increasing for all sufficiently large $x$, so for $N \geq k^2$ one has $N/\log N \geq k^2/\log(k^2)$. After choosing a universal $\gamma_D > 0$ and then increasing $k_D$, this implies $N \geq \gamma_D k \log N$, or equivalently $2^N \geq N^{\gamma_D k}$.

The DNF bound in Equation (60) also has the form $N^{\gamma_D k}$ after decreasing $\gamma_D$ if necessary. Flattening every child gate that has the same connective as the output, treating literals as width-one terms or clauses, and deleting unsatisfiable terms or tautological clauses normalizes every depth-at-most-two circuit to a DNF or a CNF without increasing its size. Each counted term or clause has fan-in at least two once $k_D$ is large, and therefore contributes a distinct non-input gate. This proves Equation (56).

**Transfer to the targets.** Use the host substitutions in Equation (13). If $k \le \xi_D n^{1/4}$ and $\xi_D$ is sufficiently small, then Equation (15) gives $N_{\mathrm{OV}} \ge k^2$ after accounting for the floor. If $k \le \xi_D n^{1/5}$, then Equation (16) similarly gives $N_{\oplus,\Sigma} \ge k^2$. Thus the source bound applies in each case.

After increasing $k_D$ and decreasing $\xi_D$ if necessary, the range hypotheses imply $n \ge 16k$, and the list-target range also implies $n \ge k^3$. Hence Equations (17), (18) and (20) give exactly the displayed projection budgets. The same host estimates give $N_{\mathrm{OV}} \ge n^{1/4}$ and $N_{\oplus,\Sigma} \ge (n/k)^{1/4}$, so Equation (56) transfers to Equations (57) to (59). Every reduction in Theorem 10 is depth zero. In particular, the packed integer associated with a $k$-$\mathsf{SUM}$ candidate depends on a single source bit, so its internal carries add no circuit depth; the conclusion is genuinely at depth exactly two. $\square$

*Remark* 22 (Why a degree-2 vertex is necessary). The CNF argument fails for a matching pattern, and the hypothesis cannot be removed. If $P$ is a matching, then

$$P\text{-SUB}_N = \bigwedge_{f \in E(P)} \bigvee_{u,w \in [N]} X_{f,u,w}$$

is an explicit polynomial-size monotone CNF. The padded expander family contains a degree-7 core vertex, so the necessary degree condition is automatic in the application.

**Corollary 23** (Subpolynomial form of Theorem D)**.** *Along every sequence $k = k(n) \to \infty$ with $k = n^{o(1)}$, the range conditions of Theorem 21 eventually hold and all three target lower bounds simplify to*

$$\mathrm{size}_2 \ge n^{\Omega(k)} = \exp\big(\Omega(k \log n)\big), \tag{63}$$

*with $k$ odd for $k$-$\mathsf{XOR}$.*

*Proof.* One has $n/k = n^{1-o(1)}$, so the list-target base $(n/k)^{\Omega(k)}$ equals $n^{\Omega(k)}$. The polynomial range conditions follow from $k = n^{o(1)}$. $\square$

At $k = \Theta(\log^2 n)$, Equation (63) becomes $\exp(\Omega(\log^3 n))$. This is stronger than the all-depth clique fallback because depth two admits exact counting of the required DNF terms and CNF clauses; the argument does not use, and therefore does not advance, the higher-depth source machinery.

### 6.3 The unconditional depth-versus-$k$ frontier

The preceding subsections occupy two different parameter ranges and consume different structural features. Table 6 records those ranges together with the common subpolynomial-regime simplification; the exact target bases and constraint budgets remain those of Theorems 19 and 21.

At $k = \Theta(\log^2 n)$, the all-depth row gives $2^{\Omega_d(\log^2 n)}$, while the depth-two row gives $2^{\Omega(\log^3 n)}$. The strength of the displayed bounds does not vary monotonically with the depth label, because the rows consume different source structures and proof mechanisms. At depth two, both orientations yield to exact DNF-term and CNF-clause counting; at depth three and higher an exponent linear in $k$ is not known unconditionally. Thus the table records which structural feature each proof consumes, not a general principle that lower bounds become progressively weaker with depth.

Table 6: The unconditional growing-$k$ frontier, including the full theorem ranges and the common simplification for $k = n^{o(1)}$. The direct $k$-XOR statements require odd $k$.

| Circuit class | Range in which the theorem holds | Common subpolynomial-regime bound | Structural feature consumed |
|---|---|---|---|
| Every fixed depth $d$ | $k \to \infty$ and $k \le n^{1-\varepsilon}$ for fixed $\varepsilon > 0$ | $n^{\Omega_d(\min\{\sqrt{k}, \log n\})}$ | growing clique; edge allowance and Beame cap |
| Depth 2, both orientations | $k \ge k_D$; $k \le \xi_D n^{1/4}$ for $k$-$\mathsf{OV}$ and $k \le \xi_D n^{1/5}$ for the list targets | $n^{\Omega(k)}$ | exact DNF-term and CNF-clause counting |

### 6.4 The row-rich PARITY comparison

**The imported PARITY bound.** Håstad's fixed-depth theorem counts AND/OR gates and places negations at the input leaves, so its size measure agrees with our non-input-gate convention; his depth parameter counts the AND/OR layers and therefore equals our $d$. More explicitly, there is an absolute constant $\ell_0 > 1$ such that, for every $d \ge 2$ and every $\ell > \ell_0^d$, every depth-$d$ circuit for $\mathsf{PARITY}_\ell$ has at least

$$2^{(1/10)^{d/(d-1)}\ell^{1/(d-1)}} = \exp\bigl(\Omega_d(\ell^{1/(d-1)})\bigr)$$

AND/OR gates [Hås86]. Our circuits are already normalized to input literals, so no model conversion is needed. The range condition is depth-dependent and is absorbed only because every application fixes $d$ before sending the number $\ell$ of free variables to infinity; no growing-depth claim is made.

There is a complementary route for $k$-XOR through this bound. Write $\mathsf{PARITY}_\ell(x) := \bigoplus_{i=1}^{\ell} x_i$. The route operates at $m = \Theta(n)$ rows rather than at the principal $O(k \log n)$-scale budget, but it is useful for comparing the depth dependence of two qualitatively different anchors.

**Theorem 24** (Amplified row-rich PARITY projection)**.** *Let $k \ge 3$ be odd and let $n \ge 4k$. Put*

$$b := \left\lfloor \log \frac{n}{2k} \right\rfloor, \qquad B := (k-1)b + 1, \qquad \ell := (k-1)B. \tag{64}$$

*There is an integer $m_0 \le 2n$ and a projection*

$$\mathsf{PARITY}_\ell \le_{\text{proj}} k\text{-}\mathsf{XOR}_{n,m_0,k}. \tag{65}$$

*Consequently, for every fixed depth $d \ge 2$ and every $m \ge m_0$, once $\ell$ exceeds the depth-dependent onset in Håstad's theorem,*

$$\text{size}_d(k\text{-}\mathsf{XOR}_{n,m,k}) \ge \exp\Bigl(\Omega_d\Bigl((k^2 \log(n/k))^{1/(d-1)}\Bigr)\Bigr). \tag{66}$$

*In particular, the bound holds in the row-rich regime $m = \Theta(n)$ whenever the implicit constant is large enough.*

The construction in Theorem 24 matches the general projection upper bound of Proposition 25 up to constant factors and is therefore order-optimal among projections from PARITY. Thus the difference between the PARITY route and the subgraph route cannot be removed merely by packing a larger parity instance into the same $k$-XOR target.

Table 7: Depth-by-depth comparison of the PARITY and subgraph routes for $k$-XOR, with odd $k = \Theta(\log^2 n)$ and $m = \Theta(n)$.

| Circuit class | PARITY route | Subgraph route | Comparison |
|---|---|---|---|
| Depth 2 | $\exp(\Omega_2(\log^5 n))$ | $\exp(\Omega(\log^3 n))$ by Theorem 21 | PARITY stronger |
| $\Sigma_3$ | $\exp(\Omega_3(\log^{5/2} n))$ | $\exp(\Omega_3(\log^2 n))$ unconditionally by Theorem 19 | PARITY stronger unconditionally |
| $\Pi_3$ | $\exp(\Omega_3(\log^{5/2} n))$ | $\exp(\Omega_3(\log^2 n))$ unconditionally by Theorem 19 | PARITY stronger unconditionally |
| Fixed $d \geq 4$ | $\exp(\Omega_d(\log^{5/(d-1)} n))$ | $\exp(\Omega_d(\log^2 n))$ by Theorem 19 | PARITY weaker |

**Proposition 25** (Upper bound for projection-based PARITY reductions)**.** *Let $n \geq k \geq 1$, and suppose that a projection $R : \{0,1\}^\ell \to (\mathbb{F}_2^m)^n$ satisfies*

$$k\text{-}\mathsf{XOR}_{n,m,k}(R(x)) = \mathsf{PARITY}_\ell(x) \qquad \textit{for every } x \in \{0,1\}^\ell. \tag{67}$$

*Then*

$$\ell \leq k^2 \log(en/k) + k. \tag{68}$$

The proofs of Theorem 24 and proposition 25 appear in Appendix E.3. At $k = \Theta(\log^2 n)$, one has $\log(n/k) = \Theta(\log n)$, so Theorem 24 gives exponent $\Omega_d(\log^{5/(d-1)} n)$ in the logarithm of the circuit-size lower bound. Table 7 compares this with the subgraph route for the same circuit class at $m = \Theta(n)$.

The comparison is within one row-rich regime: the principal lower bounds hold for every row count above their displayed budgets and therefore remain valid at $m = \Theta(n)$. The PARITY route is complementary rather than superseded. Under Conjecture 26, the subgraph route gives $\exp(\Omega_d(\log^3 n))$ for both depth-three orientations and every fixed $d \geq 4$, and hence dominates the PARITY route in every unresolved row. The order-optimal embedded dimension $\ell = \Theta(k^2 \log(n/k))$ from Proposition 25 also explains why the PARITY route cannot reproduce the polynomial host parameter $N = \Theta(\sqrt{n/k})$ exploited by the subgraph projection.

## 7 The Pattern-Uniform Conjecture and the Conditional Completion

The fixed-pattern lower bound of Theorem 2 is pointwise in the pattern: once $P$ and the depth are fixed, its exponent loss vanishes as the host size tends to infinity, but both that loss and the onset threshold may depend arbitrarily on $P$. When the pattern is $P_k^{\exp}$ and grows with $k$, this quantifier order does not provide the polynomial host threshold needed by the target reductions. The following conjecture isolates exactly the uniform source statement used in this section.

**Conjecture 26** (Pattern-Uniform LRR, depth-by-depth form)**.** *For the padded expander family $(P_k^{\exp})_{k \geq k_0}$, for every fixed depth $d$ there are constants $\gamma_d > 0$ and $c'_d > 0$ such that*

$$\mathrm{size}_d(P_k^{\exp}\text{-}\mathrm{SUB}_N) \geq N^{\gamma_d k} \tag{69}$$

*for every $k \geq k_0$ and every $N \geq k^{c'_d}$.*

Equivalently, the conjecture asks for two forms of uniformity at once: a source exponent linear in $k$ and an onset host size polynomial in $k$, with constants allowed to depend on the fixed depth.

The fixed-pattern theorem of Theorem 2 has the quantifier order

$$\begin{aligned}\forall\,&\text{simple loopless } P \text{ with } e(P) \geq 1 \text{ and no isolated vertices } \forall d\ \forall \eta > 0\\ &\exists N_0(P,d,\eta)\ \forall N \geq N_0(P,d,\eta):\\ &\qquad \mathrm{size}_d(P\text{-SUB}_N) + 2e(P)N^2 + 2 \geq N^{\kappa(P)-\eta}.\end{aligned} \tag{70}$$

whereas Conjecture 26 asks for

$$\forall d\ \exists \gamma_d, c'_d > 0\ \forall k \geq k_0\ \forall N \geq k^{c'_d}: \qquad \mathrm{size}_d(P_k^{\exp}\text{-SUB}_N) \geq N^{\gamma_d k}. \tag{71}$$

When $\kappa(P)-\eta > 2$, Theorem 2 also gives the pure non-input-gate form $\mathrm{size}_d(P\text{-SUB}_N) \geq N^{\kappa(P)-\eta}$; this is the form used in Corollary 6. The threshold in Equation (70) may depend arbitrarily on $P_k^{\exp}$, and hence on $k$, so the conjecture is not obtained by exchanging two quantifiers.

Tracking the published switching estimate reveals the same obstruction. Even if its restriction parameter is a fixed constant $\delta > 0$ along the whole family and the desired source rate $\gamma > 0$ is fixed, Lemma 32 shows that the estimate becomes useful only when $\log N = \Omega_{d,\delta,\gamma}(k)$, rather than at the polynomial scale $N = k^{O_d(1)}$ required here. The published analysis also permits $d = d(N) = o(\log N/\log\log N)$ for each fixed pattern [LRR17, p. 938]; this is a growing-depth allowance on a different uniformity axis and does not control the growing family $P_k^{\exp}$. Remark 33 records the scope of this limitation.

The depth-two instance is already proved, up to the harmless choice of the universal starting threshold: Theorem 21(i) is Equation (69) with $\gamma_2 = \gamma_D$ and $c'_2 = 2$ after replacing $k_0$ by $\max\{k_0, k_D\}$.

At depth three, no polynomial-host source lower bound with exponent linear in $k$ is presently proved for the growing expander family. Thus the $d = 3$ case of Conjecture 26, and all cases $d \geq 4$, remain open.

*Remark* 27 (Universal-rate strengthening). A stronger form of Conjecture 26 asserts that the constants $\gamma_d$ may all be bounded below by one universal constant $\gamma_0 > 0$, independent of the depth. The depth-by-depth form is the minimal hypothesis needed below and yields depth-dependent constants in the target exponents. The universal-rate form would replace every $\Omega_d$ in Theorem 28 by a universal $\Omega$, paralleling the universal fixed-$k$ rate of Theorem 17. Both formulations are sufficient source-side statements; neither is claimed to be necessary for the target lower bounds.

**Theorem 28** (E: conditional all-depth completion)**.** *Assume Conjecture 26. For every fixed depth $d$ there are integers $k_E(d) \geq k_0$ and constants $C_E(d) > 1$ such that, for every $k \geq k_E(d)$ and every $n \geq k^{C_E(d)}$,*

$$\mathrm{size}_d(k\text{-}\mathsf{OV}_{n,D,k}) \geq \exp\big(\Omega_d(k\log n)\big) \qquad \textit{for every } D \geq C_{\mathrm{OV}}k\log n, \tag{72}$$

$$\mathrm{size}_d(k\text{-}\mathsf{XOR}_{n,m,k}) \geq \exp\big(\Omega_d(k\log n)\big) \qquad \textit{for odd } k \textit{ and every } m \geq C_{\oplus}k\log(en/k), \tag{73}$$

$$\mathrm{size}_d(k\text{-}\mathsf{SUM}_{n,m,k}) \geq \exp\big(\Omega_d(k\log n)\big) \qquad \textit{for every } m \geq C_{\Sigma}k\log(en/k). \tag{74}$$

*Consequently, the conclusion applies along every sequence $k = k(n) \to \infty$ with $k = n^{o(1)}$. No new target reduction is used: the projections are exactly those of Theorem 10.*

*Proof.* Fix the depth $d$, and let $\gamma_d, c'_d > 0$ be supplied by Conjecture 26. Choose $C_E(d)$ sufficiently large that

$$C_E(d) \geq \max\{2c'_d + 4, 4\}. \tag{75}$$

After increasing $k_E(d)$, every pair $k \geq k_E(d)$ and $n \geq k^{C_E(d)}$ satisfies $n \geq \max\{16k, k^3\}$, and both host sizes in Equation (13) are at least $k^{c'_d}$. Indeed, Equations (15) and (16) give

$$N_{\mathrm{OV}} \geq \frac{1}{2}k^{C_E(d)/2} \geq k^{c'_d}, \qquad N_{\oplus,\Sigma} \geq \frac{1}{2}k^{(C_E(d)-1)/2} \geq k^{c'_d} \tag{76}$$

for all sufficiently large $k$.

For $k$-$\mathsf{OV}$, the projection in Theorem 10, projection monotonicity, and Conjecture 26 give

$$\mathrm{size}_d(k\text{-}\mathsf{OV}_{n,D,k}) \geq N_{\mathrm{OV}}^{\gamma_d k} \tag{77}$$

whenever $D \geq C_{\mathrm{OV}} k \log n$, where admissibility follows from Equation (17). Since Equation (15) gives $\log N_{\mathrm{OV}} = \Omega(\log n)$, this proves Equation (72).

For $k$-$\mathsf{XOR}$ and $k$-$\mathsf{SUM}$, Conjecture 26, theorem 10, and lemma 9 yield

$$\mathrm{size}_d(k\text{-}\mathsf{XOR}_{n,m,k}) \geq N_{\oplus,\Sigma}^{\gamma_d k} \qquad \text{for odd } k \text{ and every } m \geq m_{\oplus}(P_k^{\exp}, N_{\oplus,\Sigma}), \tag{78}$$

$$\mathrm{size}_d(k\text{-}\mathsf{SUM}_{n,m,k}) \geq N_{\oplus,\Sigma}^{\gamma_d k} \qquad \text{for every } m \geq m_{\Sigma}(P_k^{\exp}, N_{\oplus,\Sigma}). \tag{79}$$

Because $C_E(d) \geq 4$, one has $\log(n/k) \geq (3/4)\log n$. Together with Equation (16), this gives $\log N_{\oplus,\Sigma} = \Omega(\log n)$, so both lower bounds are $\exp(\Omega_d(k \log n))$. Finally, Equations (18) and (20) make the displayed hypotheses $m \geq C_{\oplus} k \log(en/k)$ and $m \geq C_{\Sigma} k \log(en/k)$ admissible, completing the proof. □

Corollary 68 combines Theorem 28 with the even-$k$ lifting projection. For every fixed depth $d$ and every supplied decomposition $K = tr + s$ with $t \geq 2$, odd $r \geq k_E^{\oplus}(d)$, $0 \leq s < 2t$, and either $s = 0$ or $t \nmid s$, it gives an exponent $\Omega_d(r \log n')$ under its own polynomial threshold in $n'$. In particular, any family of decompositions with $r = \Theta(K)$ preserves the linear-in-$K$ exponent scale.

In the subpolynomial regime, the unconditional rows are those of Table 6, including the all-depth floor

$$n^{\Omega_d(\min\{\sqrt{k}, \log n\})}. \tag{80}$$

Assuming Conjecture 26, Theorem 28 supplies the only conditional row: $n^{\Omega_d(k)}$ for both depth-three orientations and for every fixed depth $d \geq 4$. This completes the three growing-$k$ rows summarized in Table 1.

# 8 Synthesis and Open Problems

This section distills three cross-target lessons from the preceding proofs, i.e., how the targets enforce selection rigidity, when lower and upper bounds match at the exponent scale, and how verification cost depends on depth, and then separates the remaining source-side and target-side frontiers.

## 8.1 Cross-target synthesis

The three targets share the same source and the same present-and-consistent edge-selection interface, but they differ in how selection rigidity is represented. Over $\mathbb{F}_2$, cardinality is visible only modulo two. The selector equations in Equation (24), together with the support-size identity in Equation (25), yield the odd-$k$ rigidity formalized in Lemma 47; when $k$ is even, the anchor-free all-even-multiplicity branch survives and can encode genuinely spurious witnesses. This is an algebraic obstruction specific to parity-based selection, not a property of the source pattern.

The $k$-SUM construction instead uses signed integer coordinates that count group multiplicities exactly; Proposition 50 shows that this mechanism cannot arise from a group-homomorphic encoding of the $\mathbb{F}_2$ primitive into $\mathbb{Z}_{2^m}$. The $k$-OV target builds one-vector-per-class selection into the witness semantics, as summarized in Table 4. These two selection mechanisms therefore work for both parities without an exponent loss.

For an even target parameter $K$ supplied with a decomposition $K = tr + s$ satisfying the hypotheses of Lemma 65, the black-box lift recovers the fixed-depth, and conditional lower bounds of Corollary 67, and Corollary 68. The inherited exponent is governed by the odd source parameter $r$.

At the principal fixed-$k$ budgets, specializing the lower bounds to the top-disjunction depth-three orientation and comparing them with the elementary circuits of Propositions 69 to 71 shows that the upper and lower exponents have the same asymptotic scale for all three targets; the $k$-XOR comparison uses the direct odd-$k$ statement. This makes no tightness claim at depth two or for top-conjunction depth three, and it does not identify the leading constant: Proposition 72 and remark 73 show that the specific degree-7 regular-core route remains separated from the brute-force leading exponent constant by a factor greater than 7.

A separate comparison concerns the cost of checking a fixed choice of candidate indices. For $k$-OV and $k$-XOR, the remaining depth-two predicates have size $O(D)$ and $m2^{O(k)}$, respectively. For $k$-SUM, the direct depth-two verifier costs $2^{\Theta(km)}$ at the principal width, whereas the top-disjunction depth-three block-carry construction reduces the additional exponent to the scale in Equation (183); Equation (184) records the remaining very-high-width overhead. The fixed-support restrictions in Equations (141) and (143) impose a size floor $\exp\bigl(\Omega_d(k^{1/(d-1)})\bigr)$ on both list targets for every fixed depth $d \geq 2$ as $k \to \infty$. The separation is therefore quantitative and depth-sensitive rather than the mere presence of a parity obstruction.

### 8.2 Open problems

(1) **The unresolved depth frontier.** Conjecture 26 is proved at $d = 2$ by Theorem 21(i), but remains open for every $d \geq 3$. The source-side goal is to prove the conjecture for the padded expander family at those depths. The target-side goal is weaker: without necessarily proving the conjecture, obtain the missing lower bounds for both depth-three orientations and for every fixed depth $d \geq 4$. Lemma 32 and remark 33 explain why the published switching estimate does not yield the conjecture at the required polynomial host size.

(2) **Even-$k$ XOR without an exponent loss.** The projection in Lemma 65 transfers an odd-parameter lower bound through any supplied admissible decomposition $K = tr + s$, but the resulting exponent is governed by the odd source parameter $r$ rather than directly by $K$. Can one design a different linear lift that, for every even $K$, starts from an odd parameter $r = \Omega(K)$, or a non-parity selection mechanism that enforces exact cardinalities without this potential loss?

(3) **The $k$-SUM depth-and-width frontier.** At fixed $k$, the block-carry circuit of Proposition 71 closes the same-orientation exponent-scale gap at the principal width for top-disjunction depth three, but the optimal bounds at depth two and the growing-$k$ depth-three frontier remain open. The upper-bound estimates in Equations (183) and (184) leave two width regimes unresolved: support enumeration can dominate when the lower bound is width-limited, and the square-root carry overhead can grow at very large width. Determine which of these depth and width overheads are necessary, or strengthen the lower bound by exploiting the coupled structure of modular addition.

Planted and average-case variants, positioned in Section 1.4, require distributional lower bounds that do not follow from the present worst-case statements and lie outside the scope of this paper. A systematic theory of which fine-grained $\mathsf{AC}^0$ reductions preserve the correct lower-bound exponent is likewise deferred to separate work.

## Acknowledgments

I am deeply grateful to my advisor, Prashant Nalini Vasudevan, who first suggested that I study average-case planted $k$-XOR lower bounds in $\mathsf{AC}^0$ and with whom I had many formative discussions throughout 2023, as well as a more recent discussion on the projection framework developed in this paper. His guidance, support, and encouragement have been the foundation of this work.

## AI Disclosure

Four specific technical contributions were aided by the AI language model GPT-5.5. We verified each of them independently before inclusion. GPT-5.5 pointed us to Beame's small-clique lower bound for CRCW PRAMs [Bea90] as a candidate unconditional source statement for the growing-$k$, every-fixed-depth regime; we verified its applicability and developed the resulting argument (Fact 18, Theorem 19) in Section 6.1. GPT-5.5 proposed and derived the Erdős–Ginzburg–Ziv degeneracy argument of Proposition 62 (Appendix D.4). GPT-5.5 proposed and derived the constant-factor floor argument of Proposition 72 (Appendix F.2). GPT-5.5 also discovered and derived the depth-sensitive exponent comparison for $k$-SUM in Appendix F.3, contrasting the depth-three block-carry construction against the direct depth-two verifier. In every case, the authors take full responsibility for the correctness of the final statements and proofs.

## References

[ABDN18] Amir Abboud, Karl Bringmann, Holger Dell, and Jesper Nederlof. More consequences of falsifying SETH and the orthogonal vectors conjecture. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2018)*, pages 253–266. Association for Computing Machinery, 2018.

[Ajt83] Miklós Ajtai. $\Sigma^1_1$-formulae on finite structures. *Annals of Pure and Applied Logic*, 24(1):1–48, 1983.

[Alo21] Noga Alon. Explicit expanders of every degree and size. *Combinatorica*, 41(4):447–463, 2021.

[Ama10] Kazuyuki Amano. $k$-subgraph isomorphism on $\mathsf{AC}^0$ circuits. *Computational Complexity*, 19(2):183–210, 2010. Preliminary version in CCC'09.

[ASS$^+$24] Shweta Agrawal, Sagnik Saha, Nikolaj I. Schwartzbach, Akhil Vanukuri, and Prashant Nalini Vasudevan. $k$-SUM in the sparse regime: Complexity and applications. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology—CRYPTO 2024, Part II*, volume 14921 of *Lecture Notes in Computer Science*, pages 315–351. Springer, 2024.

[Bea90] Paul Beame. Lower bounds for recognizing small cliques on CRCW PRAM's. *Discrete Applied Mathematics*, 29(1):3–20, 1990.

[CLSS26] Tameem Choudhury, Nutan Limaye, Karteek Sreenivasaiah, and Srikanth Srinivasan. New and improved concrete lower bounds for orthogonal vectors. Technical Report TR26-121, Electronic Colloquium on Computational Complexity, July 2026. Also available as arXiv:2607.23799.

[CS26] Tameem Choudhury and Karteek Sreenivasaiah. Depth-3 circuit lower bounds for $k$-OV. *ACM Transactions on Computation Theory*, 2026. Published online May 2026; preliminary version appeared in STACS 2024.

[CW19] Lijie Chen and R. Ryan Williams. An equivalence class for orthogonal vectors. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2019)*, pages 21–40. Society for Industrial and Applied Mathematics, 2019.

[DKK24] Itai Dinur, Nathan Keller, and Ohad Klein. Fine-grained cryptanalysis: Tight conditional bounds for dense $k$-SUM and $k$-XOR. *Journal of the ACM*, 71(3):23:1–23:41, 2024.

[DLSV25] Mina Dalirrooyfard, Andrea Lincoln, Barna Saha, and Virginia Vassilevska Williams. Average-case hardness of parity problems: Orthogonal vectors, $k$-SUM and more. In *Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2025)*, pages 4613–4643. Society for Industrial and Applied Mathematics, 2025.

[EGZ61] Paul Erdős, Abraham Ginzburg, and Abraham Ziv. Theorem in the additive number theory. *Bulletin of the Research Council of Israel, Section F: Mathematics and Physics*, 10F(1):41–43, 1961.

[FSS84] Merrick Furst, James B. Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. *Mathematical Systems Theory*, 17:13–27, 1984.

[Hås86] Johan Håstad. Almost optimal lower bounds for small depth circuits. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing (STOC 1986)*, pages 6–20, 1986.

[IP01] Russell Impagliazzo and Ramamohan Paturi. On the complexity of $k$-SAT. *Journal of Computer and System Sciences*, 62(2):367–375, 2001.

[IPZ01] Russell Impagliazzo, Ramamohan Paturi, and Francis Zane. Which problems have strongly exponential complexity? *Journal of Computer and System Sciences*, 63(4):512–530, 2001.

[Kar72] Richard M. Karp. Reducibility among combinatorial problems. In Raymond E. Miller and James W. Thatcher, editors, *Complexity of Computer Computations*, pages 85–103, New York, 1972. Plenum Press.

[KW19] Daniel M. Kane and R. Ryan Williams. The orthogonal vectors conjecture for branching programs and formulas. In *10th Innovations in Theoretical Computer Science Conference (ITCS 2019)*, volume 124 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 48:1–48:15. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2019.

[LRR17] Yuan Li, Alexander Razborov, and Benjamin Rossman. On the $AC^0$ complexity of subgraph isomorphism. *SIAM Journal on Computing*, 46(3):936–971, 2017.

[MOP20] Sidhanth Mohanty, Ryan O'Donnell, and Pedro Paredes. Explicit near-Ramanujan graphs of every degree. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2020, pages 510–523, New York, NY, USA, 2020. Association for Computing Machinery. Corrected full version: arXiv:1909.06988v3, 29 November 2022.

[Ros08] Benjamin Rossman. On the constant-depth complexity of k-clique. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, STOC 2008, pages 721–730, New York, NY, USA, 2008. Association for Computing Machinery.

[Ros21] Gregory Rosenthal. Beating treewidth for average-case subgraph isomorphism. *Algorithmica*, 83(8):2521–2551, 2021.

[RW25] R. Ryan Williams. The orthogonal vectors conjecture and nonuniform circuit lower bounds. *SIAM Journal on Computing*, pages FOCS24–1–FOCS24–28, 2025. Special Section FOCS 2024; published online 14 October 2025.

[VW18] Virginia Vassilevska Williams. On some fine-grained questions in algorithms and complexity. In *Proceedings of the International Congress of Mathematicians (ICM 2018)*, volume 3, pages 3447–3487, 2018.

[Wag02] David Wagner. A generalized birthday problem. In Moti Yung, editor, *Advances in Cryptology—CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 288–304. Springer, 2002.

[Yao85] Andrew Chi-Chih Yao. Separating the polynomial-time hierarchy by oracles. In *Proceedings of the 26th Annual IEEE Symposium on Foundations of Computer Science (FOCS 1985)*, pages 1–10, 1985.

# A Source Formalities

Throughout this appendix, $N$ denotes the host-size parameter that Li, Razborov, and Rossman write as $n$; our $n$ is reserved for the target universe size and never denotes a source host parameter. This appendix verifies that the structured source of Definition 1 is exactly the colored function to which their lower bound applies, matches their circuit model and gate measure with ours, assembles the cited ingredients of Theorem 2, and finally records the switching-scale obstruction of Lemma 32, which explains why the published estimate does not yield Conjecture 26 at the polynomial-in-$k$ host size required by the target reductions. No reduction or target-specific construction is used here.

## A.1 Coordinate equivalence with the LRR structured problem

**Proposition 29** (Coordinate-level equivalence)**.** *For every simple loopless graph $P$ with one fixed orientation $f = (a_f, b_f)$ of each edge and every $N \geq 1$, the function $P$-$\mathrm{SUB}_N$ of Definition 1 coincides, after a bijection of Boolean input coordinates, with $\mathrm{SUBGRAPH}_{\mathrm{col},N}(P)$ of [LRR17, Sec. 5, p. 960].*

*Proof.* The structured problem introduced in the unnumbered paragraph of [LRR17, Sec. 5, p. 960] uses the host vertex set $V(P) \times [N]$ and first-coordinate coloring $\chi(a, u) = a$; this is the same coordinate space as the random colored graph of [LRR17, Def. 2.8(v)] at vertex exponent $\alpha \equiv 1$. Its Boolean input coordinates are the possible host edges

$$\{(a, u), (b, w)\} \qquad \text{with } \{a, b\} \in E(P) \text{ and } u, w \in [N]. \tag{81}$$

Because $P$ is simple and every undirected edge is oriented exactly once, the map

$$\{(a_f, u), (b_f, w)\} \longmapsto X_{f,u,w} \tag{82}$$

is a bijection between the coordinates in Equation (81) and those in Equation (1).

A properly colored copy of $P$ in the structured host selects one vertex from each color class $\{a\} \times [N]$, and therefore has the form $\{(a, \phi(a)) : a \in V(P)\}$ for a map $\phi : V(P) \to [N]$. Vertices of distinct colors are automatically distinct, even if their second coordinates agree. The selected vertices span every required pattern edge exactly when, for each $f = (a_f, b_f) \in E(P)$, the host edge $\{(a_f, \phi(a_f)), (b_f, \phi(b_f))\}$ is present. Under Equation (82), this condition is $X_{f,\phi(a_f),\phi(b_f)} = 1$, which is precisely the acceptance condition in Equation (2). Hence the two Boolean functions agree under the coordinate bijection. □

*Remark* 30 (Why the structured form is used)*.* The structured form has a fixed Boolean input set, with the coloring encoded by coordinate names rather than supplied as part of the input. Consequently, the later maps to $k$-OV, $k$-XOR, and $k$-SUM are literal projections from a fixed source cube. Moreover, the hard distributions used in [LRR17] are supported on this structured host space, so passing from their notation to $P$-$\mathrm{SUB}_N$ loses neither instances nor hardness.

## A.2 Citation assembly for the fixed-pattern lower bound

*Proof of Theorem 2.* Fix a simple loopless pattern $P$ with at least one edge and no isolated vertices, and fix a depth $d$. By Proposition 29, it suffices to prove the lower bound for $\mathrm{SUBGRAPH}_{\mathrm{col},N}(P)$ on the structured host $V(P) \times [N]$. We use $\theta_{\mathrm{col}}(P)$, $\kappa_{\alpha,\beta}(P)$, and $G_{\alpha,\beta}(N)$ only as the names of the objects defined in [LRR17, Defs. 2.8 and 2.12]; no property of them beyond the statements cited below is used.

By [LRR17, Cor. 4.2], there is a function $\beta : E(P) \to [0, 2]$ such that $(\mathbf{1}, \beta) \in \theta_{\mathrm{col}}(P)$ and

$$\kappa_{\mathbf{1},\beta}(P) = \kappa_{\mathrm{col}}(P) = \kappa(P), \tag{83}$$

where $\kappa_{\mathrm{col}}(P)$ is the parameter defined in [LRR17, Def. 2.12(iii)]; the first equality is the conclusion of the cited corollary, and the second is the notation fixed in Section 2.2.

Consider the colored random graph $G_{\mathbf{1},\beta}(N)$ of [LRR17, Def. 2.8(v)]. The displays of [LRR17, Thms. 3.11 and 3.12] write $G_{\alpha,\beta}(P)$, but the definition and the surrounding proofs show that the argument is the host parameter; we therefore use the corrected notation $G_{\alpha,\beta}(N)$. Since the vertex exponent is identically one, its vertex set is

$$\{(a, u) : a \in V(P),\ 1 \le u \le \lfloor N^1 \rfloor\} = V(P) \times [N], \tag{84}$$

and its possible edges are exactly the coordinates of Equation (81), with the first-coordinate coloring. Thus every graph in the support of $G_{\mathbf{1},\beta}(N)$ is an input to the structured function of Proposition 29. Any circuit computing $P\text{-SUB}_N$ on every input has zero error under this distribution and therefore satisfies the average-case correctness hypothesis of the Li–Razborov–Rossman theorem.

Li, Razborov, and Rossman call the relevant model type-I in [LRR17, Sec. 3.2, p. 948]: constant-depth circuits over unbounded-fan-in AND and OR together with NOT gates. Their Theorem 3.11 is the type-II statement for fan-in two and $O(1)$ alternations and is not used for this import. Our circuits, whose negations are already normalized to input leaves, form a subclass of the type-I model. If their depth convention counts the input layer or a leaf-negation layer separately, we apply their theorem at depth $d + 2$; because the statement holds at every fixed depth, this conservative offset changes neither the conclusion nor any later quantifier.

Footnote 4 of [LRR17, p. 940] specifies that size is the number of gates, but the paper does not separately state whether variable nodes, constant nodes, or input NOT gates are included. Let $S := \mathrm{size}_d(P\text{-SUB}_N)$, and recall that $M_{\mathrm{src}} = e(P)N^2$. A normalized circuit with $S$ non-input AND/OR gates can be presented in their model using at most

$$S + 2M_{\mathrm{src}} + 2$$

gates under every reading of that omission: at most $M_{\mathrm{src}}$ variable nodes, at most one shared input-negation node per variable, plus at most two constant nodes. Thus the source's gate lower bound implies a lower bound on this quantity, without assuming that its word "gate" already means our non-input gate. This also avoids relying on the proof-internal estimate $w = O(g^2)$ on p. 949 to infer which nodes are included in $g$.

To invoke the theorem, suppose this additive quantity is smaller than $N^{\kappa(P)+1}$; otherwise the desired lower bound is immediate. Under this assumption the converted source-model circuit has polynomial size in $N$, as required by the definition of type-I $\mathsf{AC}^0$ used in [LRR17]. Fix any constant accuracy requirement in the average-case formulation. The circuit under consideration has zero error on the support of $G_{\mathbf{1},\beta}(N)$ and therefore satisfies that requirement. The type-I lower bound of [LRR17, Thm. 3.12] now gives

$$S + 2M_{\mathrm{src}} + 2 \ge N^{\kappa_{\mathbf{1},\beta}(P) - o_{P,d}(1)} = N^{\kappa(P) - o_{P,d}(1)}, \tag{85}$$

where the equality uses Equation (83). The asymptotic is taken with $P$, $(\mathbf{1}, \beta)$, the adjusted fixed depth, and the accuracy requirement fixed; in particular it is not uniform in $P$ or $d$, and $\beta$ is determined by $P$ through Equation (83). Choosing the $o_{P,d}(1)$ term to have magnitude at most

$\eta$ proves Equation (4). If $\kappa(P) - \eta > 2$, instead choose it to have magnitude at most $\eta/2$. Then $2e(P)N^2 + 2 = o(N^{\kappa(P)-\eta/2})$, and for all sufficiently large $N$,

$$S \geq N^{\kappa(P)-\eta/2} - 2e(P)N^2 - 2 \geq N^{\kappa(P)-\eta},$$

which proves the pure non-input-gate consequence in Theorem 2. □

*Remark* 31 (Alternative citation route). One may instead use the equivalence between the structured and unstructured colored functions established in [LRR17, Sec. 5, p. 960], together with their worst-case corollary. The argument above is more direct for the present paper because it identifies the hard distribution with the exact fixed input space of Definition 1 before invoking the average-case theorem.

### A.3 The switching-scale obstruction

The quantifier orders of the fixed-pattern theorem and the pattern-uniform conjecture are displayed side by side in Equations (70) and (71). In particular, the fixed-pattern threshold may depend arbitrarily on $P_k^{\exp}$, and hence on $k$; no bound of the form $N_0(P_k^{\exp}, d, \eta) \leq k^{O_d(1)}$ follows from Theorem 2. The published switching estimate exhibits a separate obstruction at the level of direct parameter tracking.

The relevant bad-event bound in [LRR17, Appendix C] has the form

$$B_{d,\delta}(S, N) := S\big(5N^{-\delta/d}\delta \log N\big)^{\delta \log N}. \tag{86}$$

Here and below, logarithms follow the paper's base-two convention; replacing another fixed logarithm base by base two changes only fixed $d$- and $\delta$-dependent constants in the scale estimates. The fixed-pattern analysis takes $S = N^{O(1)}$ and chooses the constant $\delta > 0$ after fixing the pattern. The next lemma grants the favorable assumption that one fixed positive $\delta$ is available along the whole family and shows that the same estimate nevertheless does not handle size $N^{\Theta(k)}$ at polynomial host size.

**Lemma 32** (Scale limitation of the published switching estimate)**.** *Fix constants $d \geq 1$, $\gamma > 0$, and $\delta > 0$. Along every sequence with $k \to \infty$ and $N \to \infty$,*

$$\log B_{d,\delta}(N^{\gamma k}, N) = \gamma k \log N - \Theta_{d,\delta}\big((\log N)^2\big) + O_\delta\big(\log N \log\log N\big). \tag{87}$$

*Consequently, for every fixed $C > 0$,*

$$B_{d,\delta}(N^{\gamma k}, N) \longrightarrow \infty \qquad \text{as } k \to \infty \text{ along } N = k^C. \tag{88}$$

*Moreover, along every sequence with $k \to \infty$ and $N \to \infty$ for which $B_{d,\delta}(N^{\gamma k}, N) = o(1)$, one necessarily has*

$$\log N = \Omega_{d,\delta,\gamma}(k). \tag{89}$$

*Proof.* Substituting $S = N^{\gamma k}$ into Equation (86) and taking logarithms gives

$$\begin{aligned}\log B_{d,\delta}(N^{\gamma k}, N) &= \gamma k \log N + \delta \log N \left(\log(5\delta) + \log\log N - \frac{\delta}{d}\log N\right) \\ &= \gamma k \log N - \frac{\delta^2}{d}(\log N)^2 + \delta \log N \log\log N + O_\delta(\log N),\end{aligned} \tag{90}$$

which proves Equation (87). If $N = k^C$, the first term in Equation (90) is $\Theta_{C,\gamma}(k \log k)$, whereas the negative quadratic term and the remaining positive terms have magnitude $O_{C,d,\delta}((\log k)^2)$ and $O_{C,\delta}(\log k \log\log k)$, respectively. The logarithm therefore tends to $+\infty$, proving Equation (88).

Now consider a sequence with $k \to \infty$, $N \to \infty$, and $B_{d,\delta}(N^{\gamma k}, N) = o(1)$. Writing $x := \log N$, Equation (90) and $\log B_{d,\delta}(N^{\gamma k}, N) < 0$ imply, after rearranging and dropping the nonpositive term $-\delta x \log x$, that for all sufficiently large terms of the sequence,

$$\gamma k x \leq \frac{\delta^2}{d} x^2 + O_\delta(x). \tag{91}$$

After dividing by $x > 0$, the right-hand side is $O_{d,\delta}(x)$ because $x \to \infty$. If $x = o(k)$, this is $o(k)$ and contradicts the left-hand side $\gamma k$. Hence $x = \Omega_{d,\delta,\gamma}(k)$, proving Equation (89). $\square$

*Remark* 33 (Scope of the switching-scale calculation). The lemma limits direct parameter tracking of the published estimate; it does not rule out a refinement of the Li–Razborov–Rossman method, a different restriction scheme, or another proof of Conjecture 26. At the host sizes used by the target reductions, the benchmark $k = \Theta(\log^2 n)$ gives $\log N = \Theta(\log n) = \Theta(\sqrt{k})$, whereas Equation (89) requires $\log N = \Omega_{d,\delta,\gamma}(k)$. Two additional pattern dependencies remain in the original argument: the auxiliary restriction parameter and the constants in the probabilistic estimates are chosen after the pattern is fixed and would also have to be controlled uniformly. By contrast, the hitting-set estimate $|\mathcal{H}| \leq 2^{|E(P)|}$ from the proof of [LRR17, Thm. 3.11] is not itself an obstruction at polynomial host size, because $2^{O(k)} = N^{O(k/\log N)} = N^{o(k)}$ whenever $\log N \to \infty$, and such a factor can be absorbed into an exponent $\gamma_d k$.

# B Pattern Constructions and Constants

For $t \geq 0$, let $J_t$ denote a matching of $t$ pairwise disjoint edges on fresh vertices, with $J_0$ empty. Every padded pattern below is a disjoint union $F \mathbin{\dot\cup} J_t$. All core and padding orientations follow the convention fixed in Section 2.1.

## B.1 The bounded-degree expander family

The bounded-degree expander core supplies $\kappa = \Omega(k)$, while a disjoint matching realizes every sufficiently large edge count exactly.

**Theorem 34** (Explicit simple near-Ramanujan graphs of every degree and size)**.** *For every fixed integer $\Delta \geq 3$ and every $\varepsilon > 0$, there is a finite threshold $n_{\mathrm{A}}(\Delta, \varepsilon)$ such that, for every $v \geq n_{\mathrm{A}}(\Delta, \varepsilon)$ with $v\Delta$ even, there is a simple $\Delta$-regular graph on $v$ vertices whose nontrivial adjacency eigenvalues, i.e., every adjacency eigenvalue other than the Perron eigenvalue $\Delta$, all have absolute value at most $2\sqrt{\Delta - 1} + \varepsilon$.*

*Proof. Cited conclusion.* Regularity, the exact vertex count, and the two-sided spectral bound are the conclusion of [Alo21, Thm. 1.3]. Simplicity is not part of Alon's $(n, d, \lambda)$-graph convention, so it is verified separately below rather than attributed to that theorem.

*Selected source graph.* Alon's exact-size proof invokes the near-Ramanujan, bicycle-free input of [Alo21, Thm. 3.3 and Sec. 3] for its intermediate graph $H$; from that point onward, the transformation uses only the regularity, vertex-count, spectral, and local-cycle properties stated there. Alon's restatement does not include simplicity, so we inspect the corrected full version underlying that input directly. Its lift-model branch constructs $G_0$ as a lift of the simple base graph $K_{\Delta+1}$ and then obtains $G_1, \ldots, G_t$ by successive 2-lifts [MOP20, full version, Def. 2.8 and Sec. 5, Steps 1–2].

The resulting lift-model output has all the properties required of $H$ and is therefore an admissible choice in Alon's transformation. Here $H$ is Alon's notation; Mohanty–O'Donnell–Paredes use the same letter in their overview for the smaller starting graph, not for the final lift output. Their construction produces a dense sequence of sizes, while Alon's transformation is the ingredient that reaches the prescribed exact size $v$.

*Simplicity of the lift chain.* Every lift of a simple base graph is simple. Indeed, a loop in the lift would project to a loop in the base. If two lifted edges had the same unordered pair of endpoints, simplicity of the base would force them to lie over the same base edge $\{u, v\}$. Orient that edge from $u$ to $v$; the two lifted edges share an endpoint $(u, i)$, and the permutation attached to $\{u, v\}$ sends $i$ to a unique fiber index $j$, so both have other endpoint $(v, j)$ and coincide. Thus $G_0$ is simple, and a 2-lift is a lift in the same sense, so induction makes every $G_i$, and hence $H$, simple.

*Simplicity of Alon's exact-size modification.* Set $r := \lceil 2/\varepsilon \rceil$. In the notation of [Alo21, Sec. 3], Alon deletes a set $U$ chosen as in [Alo21, Lem. 3.1] and restores regularity by adding a perfect matching on the deficient set $W := N_H(U)$. For every $u \in U$, [Alo21, Lem. 3.1(2)] makes the $(r+1)$-neighborhood of $u$ cycle-free, so $N_H(u)$ is independent. For distinct $u, u' \in U$, [Alo21, Lem. 3.1(3)] gives $d_H(u, u') \geq 2r + 3$, so the two neighborhoods are disjoint; moreover, for $x \in N_H(u)$ and $x' \in N_H(u')$ one has $d_H(x, x') \geq 2r + 1 > 1$, and hence no edge joins them. Thus $W$ is independent in the simple graph $H - U$, so every perfect matching on $W$ creates neither a loop nor an edge parallel to one already present. □

*Remark* 35 (The finite threshold). Alon's construction is deterministic polynomial-time for fixed $\Delta$ and $\varepsilon$, but we use only that $n_{\mathrm{A}}(\Delta, \varepsilon)$ is finite; no theorem in the paper depends on a closed numerical value of this threshold. The later reductions are nonuniform: for each parameter choice, the pattern and all literal substitutions are fixed before the source input is read, so no strongly explicit construction is required. Accordingly, the universal lower cutoff $k_0$ below is finite but intentionally unoptimized.

**Fact 36** (Discrete Cheeger inequality, adjacency form)**.** *Let $F$ be a $\Delta$-regular graph. With $h(F)$ normalized as in Definition 3 and $\lambda_2(F)$ denoting the second-largest eigenvalue of the adjacency matrix, one has*

$$h(F) \geq \frac{\Delta - \lambda_2(F)}{2}. \tag{92}$$

*Proof.* This is the discrete Cheeger inequality in the form recorded in [Ros21, Fact 2.4]. Rosenthal's $h(F)$ uses the same denominator $\min\{|S|, |V(F) \setminus S|\}$ as the equivalent form of Definition 3, and his $\lambda_2(F)$ is the second-largest adjacency-matrix eigenvalue [Ros21, p. 2525]. □

**Proposition 37** (Expander core padded to an arbitrary edge count)**.** *Fix an integer $\Delta \geq 3$ and a constant*

$$0 < \varepsilon < \Delta - 2\sqrt{\Delta - 1}. \tag{93}$$

*Set*

$$\lambda_0 := 2\sqrt{\Delta - 1} + \varepsilon, \qquad h_0 := \frac{\Delta - \lambda_0}{2}, \qquad c_\kappa(\Delta, \varepsilon) := \frac{\Delta - \lambda_0}{6\Delta^2}. \tag{94}$$

*Let*

$$n_0 := \max\{n_{\mathrm{A}}(\Delta, \varepsilon), \Delta + 1\}, \qquad k_0 := \Delta n_0 + 1. \tag{95}$$

*Then, for every integer $k \geq k_0$, there is a simple loopless pattern $P_k$ with exactly $k - 1$ edges and maximum degree $\Delta$, obtained from a simple $\Delta$-regular core $F_k$ by adjoining a disjoint matching, such that*

$$\kappa(P_k) \geq c_\kappa(\Delta, \varepsilon)(k - 1). \tag{96}$$

*Proof.* Fix $k \geq k_0$ and consider the interval

$$\mathcal{V}_k := \left[\frac{k-1}{\Delta}, \frac{2(k-1)}{\Delta}\right]. \tag{97}$$

Its left endpoint is at least $n_0$, and its length is $(k-1)/\Delta \geq n_0 \geq 2$. If $\Delta$ is even, every integer $v \in \mathcal{V}_k$ satisfies $v\Delta$ even. If $\Delta$ is odd, an interval of length at least two contains an even integer. Hence in either case there is an integer $v \in \mathcal{V}_k$ with $v \geq n_0$ and $v\Delta$ even.

By Theorem 34, there is a simple $\Delta$-regular graph $F_k$ on $v$ vertices with $\lambda_2(F_k) \leq \lambda_0$. The range in Equation (93) gives $\lambda_0 < \Delta$, so the top eigenvalue has multiplicity one and $F_k$ is connected; this observation guarantees $h_0 > 0$, although regularity is the only hypothesis needed for Fact 36. Since $e(F_k) = \Delta v/2$, the bounds defining $\mathcal{V}_k$ give

$$\frac{k-1}{2} \leq e(F_k) \leq k-1. \tag{98}$$

By Fact 36, $h(F_k) \geq h_0$, and Theorem 4 therefore gives

$$\begin{aligned}\kappa(F_k) &\geq \frac{vh(F_k)}{3\Delta} \geq \frac{vh_0}{3\Delta} && (99)\\ &\geq \frac{k-1}{\Delta} \cdot \frac{\Delta - \lambda_0}{6\Delta} = \frac{\Delta - \lambda_0}{6\Delta^2}(k-1) = c_\kappa(\Delta, \varepsilon)(k-1). && (100)\end{aligned}$$

Let $t := k - 1 - e(F_k) \geq 0$ and define $P_k := F_k \,\dot\cup\, J_t$. Then $P_k$ is simple and loopless, $e(P_k) = k-1$, and $\Delta(P_k) = \Delta$. Since $F_k$ is a subgraph and hence a minor of $P_k$, and both graphs have no isolated vertices, minor-monotonicity in Theorem 4 and Equation (100) imply

$$\kappa(P_k) \geq \kappa(F_k) \geq c_\kappa(\Delta, \varepsilon)(k-1),$$

which proves the proposition. ∎

**Corollary 38** (The degree-7 family)**.** *Set $\Delta := 7$ and $\varepsilon := 1/10$, let $k_0^{\mathrm{raw}}$ be the value of Equation (95) for these parameters, and put $k_0 := \max\{k_0^{\mathrm{raw}}, 600\}$. For every $k \geq k_0$, define $P_k^{\exp} := P_k$, where $P_k$ is supplied by Proposition 37. Then $P_k^{\exp}$ has maximum degree 7 and*

$$\kappa(P_k^{\exp}) \geq \frac{k-1}{147}. \tag{101}$$

*Proof.* By Proposition 37, it remains only to verify the displayed constant. Since $\sqrt{6} < 49/20$, one has

$$\lambda_0 = 2\sqrt{6} + \frac{1}{10} < \frac{49}{10} + \frac{1}{10} = 5,$$

so $\Delta - \lambda_0 > 2$ and

$$c_\kappa(7, 1/10) = \frac{7 - \lambda_0}{6 \cdot 7^2} > \frac{2}{294} = \frac{1}{147}.$$

Weakening the strict inequality proves Equation (101). In particular, Lemma 5 holds with this $k_0$ and with $c_\kappa = 1/147$, and the chosen threshold also satisfies $c_\kappa(k_0 - 1) > 4$. ∎

*Remark* 39 ($\kappa$ versus treewidth). The source lower bound is stated in terms of $\kappa$, not treewidth. For the bounded-degree expander cores used here, however, Equation (6) gives $\kappa(F_k) = \Omega(v(F_k))$, while Theorem 4 gives $\kappa(F_k) \leq \mathrm{tw}(F_k) + 1 \leq v(F_k)$, so $\kappa(F_k) = \Theta(\mathrm{tw}(F_k)) = \Theta(v(F_k))$. The distinction therefore does not affect the exponent scale of the present construction.

*Remark* 40 (Quantifier form of the fixed-$k$ source bound). Combining Corollaries 6 and 38, one may fix any universal $\gamma$ with $0 < \gamma < c_\kappa$, i.e.,in particular, any $0 < \gamma < 1/147$, apply Corollary 6 with source rate $\gamma$, and read the source statement as

$$\exists\, \gamma > 0,\ k_0 \quad \forall\, d \quad \forall\, k \geq k_0 \quad \exists\, N_0(d,k) \quad \forall\, N \geq N_0(d,k): \quad \mathrm{size}_d(P_k^{\mathrm{exp}}\text{-SUB}_N) \geq N^{\gamma(k-1)}. \tag{102}$$

The rate is universal in $d$ and $k$, whereas the host-size threshold is allowed to depend on the fixed pair $(d,k)$.

### B.2 The clique family

The clique core trades pattern vertices for a source bound that remains usable when the clique order grows, while a matching fills the remaining edge allowance.

**Definition 41** (Ordinary clique and clique core plus matching)**.** For integers $r \geq 2$ and $N \geq 1$, let $K_r$-CLIQUE$_N$ be the total monotone Boolean function on variables $y_{\{u,w\}}$, indexed by unordered pairs of distinct $u, w \in [N]$, that accepts exactly when the represented graph contains an $r$-clique.

For integers $k \geq 2$ and $r \geq 2$ with $\binom{r}{2} \leq k-1$, define

$$P_{k,r}^{\mathrm{clq}} := K_r \,\dot\cup\, J_{k-1-\binom{r}{2}}. \tag{103}$$

Then $e(P_{k,r}^{\mathrm{clq}}) = k-1$ and $\Delta(P_{k,r}^{\mathrm{clq}}) = r-1$.

**Lemma 42** (Clique hardness embeds into the padded pattern)**.** *For every admissible $k, r, N$,*

$$K_r\text{-CLIQUE}_N \leq_{\mathrm{proj}} K_r\text{-SUB}_N \leq_{\mathrm{proj}} P_{k,r}^{\mathrm{clq}}\text{-SUB}_N. \tag{104}$$

*Proof.* Let the ordinary clique input have variables $y_{\{u,w\}}$ for distinct $u, w \in [N]$. For an oriented edge $f = (a_f, b_f)$ of the colored $K_r$ pattern, project

$$X_{f,u,w} \longmapsto \begin{cases} y_{\{u,w\}}, & u \neq w, \\ 0, & u = w. \end{cases} \tag{105}$$

If the projected colored instance accepts via $\phi : [r] \to [N]$, then every pair of distinct pattern vertices is joined by an edge of $K_r$, and Equation (105) forces their images to be distinct. Hence $\phi$ is injective and its image is an ordinary $r$-clique. Conversely, every ordinary $r$-clique gives an injective accepting map after assigning its vertices to the colors. This proves the first projection.

For the second projection, preserve every variable belonging to the $K_r$ core and set every variable belonging to a padding edge to 1. Any accepting core map extends to the fresh matching colors by arbitrary host indices, and any accepting padded map restricts to an accepting core map. The orientation-extension convention recalled at the beginning of this appendix makes the preserved core coordinate unique, so the map is a projection. □

The clique family is not bounded-degree when $r$ grows. Its source lower bound in Section 6.1 is obtained by combining Fact 18 and lemma 42.

## C Full Projection Proofs

This appendix proves the three projection theorems of Section 4, together with their supporting lemmas, the two design facts motivating the $k$-OV dummy and identifier conventions, and the torsion obstruction motivating the native integer encoding for $k$-SUM. The proofs use only the common skeleton of Section 3.2; no property of the source pattern beyond simplicity, looplessness, the fixed orientation, and $e(P) = k-1$ is required.

## C.1 The $k$-OV projection

Call a choice of one vector from each of the $k$ target classes a selected tuple. Relative to the roles in Section 3.2, this one-vector-per-class semantics supplies selection rigidity (R1), the guard coordinates certify presence (R2), Lemma 46 establishes label consistency (R3), Lemma 45 purges dummies (R4), and Lemma 12 enforces the pairwise-distinctness promise (R5).

We first record the two elementary failures that motivate the dummy and identifier designs.

**Fact 43** (Zero-vector dummies are unsound)**.** *If a $k$-OV class contains the zero vector as a dummy, then every selected tuple using that dummy is orthogonal, independently of the remaining chosen vectors and independently of the source input.*

*Proof.* The selected zero vector contributes a zero factor on every coordinate, so the product of the selected entries is zero on every coordinate. ☐

**Fact 44** (Unpinned shared identifiers need not be inert)**.** *Appending classwise identifiers without pinning each coordinate to zero in some class can destroy a genuine orthogonal witness, even when the identifiers make every class pairwise distinct.*

*Proof.* Take any structural instance with an orthogonal witness. Append one shared coordinate that is 1 on the witness's selected vector in every class, and use further coordinates to assign pairwise distinct codes within each class. That witness then has product 1 on the shared coordinate and is no longer orthogonal. ☐

Pinning every identifier coordinate to zero throughout one owner class makes that coordinate inert for every selected tuple.

We next prove the identifier lemma. Recall that $\ell_n = \lceil \log n \rceil$ and $s_{k,n} = \lceil k\ell_n/(k-1) \rceil$.

*Proof of Lemma 12.* Create $s_{k,n}$ identifier coordinates and assign each coordinate to one owner class. Balance these assignments as evenly as possible, so every class owns at most $\lceil s_{k,n}/k \rceil$ coordinates. The defining inequality $(k-1)s_{k,n} \geq k\ell_n$ is equivalent to $s_{k,n} - \ell_n \geq s_{k,n}/k$; since the left-hand side is an integer, it follows that

$$\left\lceil \frac{s_{k,n}}{k} \right\rceil \leq s_{k,n} - \ell_n. \tag{106}$$

Hence every class is unpinned on at least $s_{k,n} - \lceil s_{k,n}/k \rceil \geq \ell_n$ coordinates. Pin every vector of a coordinate's owner class to zero on that coordinate. For each class $U_h$, choose an injection from its $n$ vectors into the bit strings on its unpinned coordinates; such an injection exists because there are at least $\ell_n$ unpinned coordinates and $2^{\ell_n} \geq n$. Assign those code bits on the unpinned coordinates and retain zero on the owned coordinates. The vectors within each class are then pairwise distinct. On every identifier coordinate, however, the owner class contributes zero to every selected tuple, so the product of the selected entries is identically zero. Finally,

$$s_{k,n} = \left\lceil \frac{k\ell_n}{k-1} \right\rceil \leq 2\ell_n \tag{107}$$

for $k \geq 2$. ☐

For completeness, we spell out the structural entries. On the anchor guard $q_\alpha$, set $v_\alpha(q_\alpha) = 0$ and set every other vector's entry to 1. On an edge guard $q_f$, set $v_{f,u,w}(q_f) = \overline{X}_{f,u,w}$ and set every other entry, including every dummy entry in $U_f$, to 1. For $(a,g) \in \mathcal{I}(P)$, with $f := \rho(a)$, and $t \in [\ell_N]$, define

$$v_{f,u,w}(C^{10}_{a,g,t}) := \mathrm{bit}_t(\mathrm{lab}_a(f,u,w)), \qquad v_{g,u',w'}(C^{10}_{a,g,t}) := 1 - \mathrm{bit}_t(\mathrm{lab}_a(g,u',w')), \tag{108}$$

$$v_{f,u,w}(C^{01}_{a,g,t}) := 1 - \mathrm{bit}_t(\mathrm{lab}_a(f,u,w)), \qquad v_{g,u',w'}(C^{01}_{a,g,t}) := \mathrm{bit}_t(\mathrm{lab}_a(g,u',w')), \tag{109}$$

and set every other entry on these coordinates to 1. Every dummy is therefore 1 on every structural coordinate; its identifier entries are supplied by Lemma 12.

**Lemma 45** (Dummy rejection for $k$-$\mathsf{OV}$)**.** *Every selected tuple containing a dummy vector is non-orthogonal.*

*Proof.* Suppose the selected vector in class $h \in \{\alpha\} \cup E(P)$ is a dummy. On the guard $q_h$, that dummy has entry 1, and every selected vector from every other class also has entry 1 by the guard definition. The product of the selected entries on $q_h$ is therefore 1. □

**Lemma 46** (The $k$-$\mathsf{OV}$ consistency test)**.** *Suppose a selected tuple uses genuine candidates from the reference group $f = \rho(a)$ and a non-reference group $g$ incident to $a$. For a fixed bit position $t$, the products on $C^{10}_{a,g,t}$ and $C^{01}_{a,g,t}$ both vanish if and only if the two proposed label bits agree.*

*Proof.* Let $x$ and $y$ be the two proposed bits. Every inactive class contributes 1, so the products are $x(1-y)$ and $(1-x)y$. The first is one only on $(x,y) = (1,0)$, and the second is one only on $(0,1)$; both vanish exactly when $x = y$. □

*Proof of Theorem 13.* We first take $D = D_0(P,N,n)$. The construction has one anchor class and one edge class for each of the $e(P) = k-1$ pattern edges, hence exactly $k$ classes. The condition $N^2 \le n$ permits every edge class to contain all $N^2$ genuine candidates and enough dummies to reach cardinality $n$, while the anchor class contains its one genuine vector and $n-1$ dummies. By Lemma 12, every class contains $n$ pairwise distinct vectors. Moreover, $s_{k,n} \ge \ell_n$, so $D \ge D_0(P,N,n) \ge \ell_n$ and therefore $n \le 2^{\ell_n} \le 2^D$; the constructed instance lies in the promised target family of Definition 7.

Assume first that $P\text{-SUB}_N(X) = 1$, and let $\phi : V(P) \to [N]$ satisfy Equation (2). Select the genuine anchor and, for every oriented edge $f = (a_f, b_f)$, the genuine vector $v_{f,\phi(a_f),\phi(b_f)}$. The anchor guard has product zero because the anchor contributes zero. On the guard $q_f$, the selected group-$f$ vector contributes $\overline{X}_{f,\phi(a_f),\phi(b_f)} = 0$, so that product also vanishes. Every pair of selected candidates incident to a vertex $a$ proposes the common label $\phi(a)$, and Lemma 46 therefore makes every consistency product zero. Finally, every identifier coordinate is zero in its owner class by Lemma 12. The selected tuple is an orthogonal witness.

Conversely, suppose the constructed instance has an orthogonal witness. By Lemma 45, every selected vector is genuine, so the witness consists of $v_\alpha$ and one candidate $v_{f,u_f,w_f}$ from every edge class. On $q_f$, all classes other than $U_f$ contribute one, and orthogonality therefore forces $\overline{X}_{f,u_f,w_f} = 0$; hence every selected candidate represents a present edge. For every non-isolated vertex $a$, Lemma 46 applied to every $(a,g) \in \mathcal{I}(P)$ and every bit position forces all incident candidates to propose the same label. Define $\phi(a)$ to be this common value; for an isolated vertex, choose any value in $[N]$. Then $X_{f,\phi(a_f),\phi(b_f)} = 1$ for every $f \in E(P)$, so $P\text{-SUB}_N(X) = 1$.

It remains to verify that the map is a projection. The only source-dependent entries are the edge-guard entries $\overline{X}_{f,u,w}$; every consistency bit, dummy bit, identifier bit, and inactive entry is a constant determined by $(P,N,n)$ and the candidate index. Thus every output bit is a constant or a negated input literal. For $D > D_0(P,N,n)$, append $D - D_0(P,N,n)$ all-zero coordinates. They preserve pairwise distinctness and make the product of every selected tuple zero on the new coordinates, so correctness and the projection property remain unchanged. □

## C.2 The odd-$k$ $k$-XOR projection

Here Lemma 47 establishes selection rigidity (R1) and dummy purge (R4), Lemma 48 certifies presence (R2), and Lemma 49 establishes label consistency (R3). Because the target is an indexed list in which repeated vector values are permitted, no separate promise-validity role is needed.

We begin with the nonuniform guard compression. Write $r := r_{\mathrm{guard}}(P, N)$.

*Proof of Lemma 14.* Choose every label $\lambda_{f,u,w} \in \mathbb{F}_2^r$ independently and uniformly. Fix one choice $(u_f, w_f) \in [N]^2$ for every $f \in E(P)$ and one nonempty set $T \subseteq E(P)$. Because the selected labels belong to distinct edge groups, they are independent uniform vectors, and their XOR is uniform on $\mathbb{F}_2^r$. Consequently,

$$\Pr\left[\bigoplus_{f\in T} \lambda_{f,u_f,w_f} = 0\right] = 2^{-r}. \tag{110}$$

There are $N^{2e(P)}$ choices of the candidate tuple and fewer than $2^{e(P)}$ nonempty choices of $T$. Since $r = \lceil 2e(P)\log N + e(P) + 1\rceil$, the union bound gives

$$\Pr[\text{some violation of Equation (27)}] \le N^{2e(P)} 2^{e(P)} 2^{-r} \le N^{2e(P)} 2^{e(P)} 2^{-(2e(P)\log N + e(P)+1)} = \frac{1}{2}. \tag{111}$$

Hence a deterministic labelling satisfying Equation (27) exists. Fix one such labelling for the parameter pair $(P, N)$; it is independent of the source input $X$. □

For the remaining proof, the matrix rows are exactly those described in Section 4.2: selector rows $S_f$, compressed guard rows $H_h$, consistency rows $C_{a,g,t}$, and one anti-dummy row $A_{\mathrm{dum}}$. All unspecified entries are zero, and each dummy column is zero except for its entry one on $A_{\mathrm{dum}}$.

**Lemma 47** (Support rigidity for odd $k$)**.** *Assume $k = e(P) + 1$ is odd. If a $k$-support has zero sum on every selector row and on the anti-dummy row, then it contains the anchor, exactly one candidate from every edge group, and no dummies.*

*Proof.* Let $\zeta \in \{0, 1\}$ indicate whether the anchor is selected, let $c_f$ count selected candidates from group $f$, and let $d$ count selected dummies. The selector equations give $c_f \equiv \zeta \pmod 2$ for every $f$, while the anti-dummy row gives $d \equiv 0 \pmod 2$. If $\zeta = 1$, then every $c_f$ is a positive odd integer, and the support-size identity

$$1 + \sum_{f\in E(P)} c_f + d = k = 1 + e(P)$$

forces $c_f = 1$ for every $f$ and $d = 0$. If $\zeta = 0$, then every $c_f$ and $d$ is even, so the support size is even, contradicting that $k$ is odd. □

**Lemma 48** (Compressed-guard correctness)**.** *Suppose a support contains exactly one candidate $c_{f,u_f,w_f}$ from each edge group. Its vector of compressed-guard row sums is zero if and only if every selected edge is present.*

*Proof.* A present candidate has $\overline{X}_{f,u_f,w_f} = 0$ and contributes the zero label, while an absent candidate contributes $\lambda_{f,u_f,w_f}$. Hence the vector of guard sums is

$$\bigoplus_{f\colon X_{f,u_f,w_f}=0} \lambda_{f,u_f,w_f}. \tag{112}$$

If every selected edge is present, this XOR is empty and therefore zero. If at least one edge is absent, the indexing set in Equation (112) is a nonempty subset of $E(P)$, and the XOR is nonzero by Equation (27). $\square$

**Lemma 49** ($k$-XOR consistency)**.** *Suppose a support contains exactly one candidate from each edge group. The consistency rows all sum to zero if and only if, at every non-isolated pattern vertex $a$, all incident selected candidates propose the same label under $\mathrm{lab}_a$.*

*Proof.* Fix $(a,g) \in \mathcal{I}(P)$, write $f := \rho(a)$, and fix a bit position $t$. Only the selected candidates from groups $f$ and $g$ can contribute to $C_{a,g,t}$, and its sum is

$$\mathrm{bit}_t(\mathrm{lab}_a(f,u_f,w_f)) \oplus \mathrm{bit}_t(\mathrm{lab}_a(g,u_g,w_g)). \tag{113}$$

This sum is zero exactly when the two bits agree. Ranging over all $t \in [\ell_N]$ forces equality of the complete binary encodings, and ranging over all $(a,g) \in \mathcal{I}(P)$ ties every non-reference incident group to the reference group at $a$. $\square$

*Proof of Theorem 15.* First take $m = m_\oplus(P,N)$. If $P\text{-SUB}_N(X) = 1$ via an accepting map $\phi$, select the anchor and the $e(P)$ candidates $c_{f,\phi(a_f),\phi(b_f)}$. Every selector row sees two ones, one from the anchor and one from its group, and therefore sums to zero. Every selected edge is present, so all compressed-guard contributions vanish. The selected candidates propose the common label $\phi(a)$ at every pattern vertex, so every consistency row sums to zero by Lemma 49. No dummy is selected, so the anti-dummy row also sums to zero. These $k = e(P)+1$ columns witness acceptance.

Conversely, let $S$ be a zero-sum support of size $k$. By Lemma 47, it contains the anchor, one candidate $c_{f,u_f,w_f}$ from every group, and no dummies. By Lemma 48, every selected edge is present. By Lemma 49, all candidates incident to a non-isolated vertex $a$ propose one common label; define this value to be $\phi(a)$, and assign an arbitrary value in $[N]$ to every isolated vertex. Then $X_{f,\phi(a_f),\phi(b_f)} = 1$ for every pattern edge, so $P\text{-SUB}_N(X) = 1$.

Every selector, consistency, anti-dummy, anchor, and dummy entry is constant. A compressed-guard entry is $\overline{X}_{f,u,w}\lambda_{f,u,w}(h)$, which is either the constant zero or the literal $\overline{X}_{f,u,w}$ because the label bit is fixed. Thus the map is a projection.

The column budget $1 + e(P)N^2 \le n$ permits padding with the required number of dummy indices; repeated dummy columns are allowed by the indexed-list convention of Definition 7. For $m > m_\oplus(P,N)$, append all-zero rows. Finally, Equations (12) and (26) give

$$m_\oplus(P,N) = e(P) + r_{\mathrm{guard}}(P,N) + |\mathcal{I}(P)|\ell_N + 1 = O(k\log(2N)) \tag{114}$$

for every $N \ge 1$. $\square$

### C.3 The $k$-SUM projection

Here Lemma 51 establishes selection rigidity (R1) and dummy purge (R4), while the guard and consistency coordinates certify presence (R2) and label consistency (R3) in the proof of Theorem 16. Lemma 57 reduces the target modular equation to the exact integer-vector condition used by those arguments. Repeated list values are permitted, so no analogue of (R5) is needed.

We first justify why the construction is native to integer addition rather than imported from $\mathbb{F}_2$. The signed packing below is the large-base positional device introduced in Section 4.3 and traced there to Karp's Exact Cover-to-Knapsack reduction [Kar72]; here we verify its range and modular faithfulness in full.

**Proposition 50** (2-torsion obstruction)**.** *Let $r \geq 2$, $m \geq 1$, and $k \geq 2$. There is no additive map $\psi : \mathbb{F}_2^r \to \mathbb{Z}_{2^m}$ such that, for every $k$-tuple $(v_1, \dots, v_k)$,*

$$\bigoplus_{i=1}^{k} v_i = 0 \quad \Longleftrightarrow \quad \sum_{i=1}^{k} \psi(v_i) = 0 \quad \text{in } \mathbb{Z}_{2^m}. \tag{115}$$

*Proof.* Additivity gives $2\psi(v) = \psi(v \oplus v) = \psi(0) = 0$ for every $v$. The only elements of $\mathbb{Z}_{2^m}$ annihilated by two are 0 and $2^{m-1}$, so the image of $\psi$ has $\mathbb{F}_2$-dimension at most one. Since $r \geq 2$, the kernel contains a nonzero vector $v$. The $k$-tuple $(v, 0, \dots, 0)$ has nonzero XOR but image sum zero, contradicting Equation (115). □

We now analyze the signed vector construction. For a $k$-support $S$, write

$$y_S := \sum_{j \in S} \mathrm{vec}(j) \in \mathbb{Z}^{R(P)}. \tag{116}$$

**Lemma 51** (Exact support structure)**.** *If $y_S = 0$, then $S$ contains the anchor, exactly one candidate from every edge group, and no dummies.*

*Proof.* Let $\zeta \in \{0, 1\}$ indicate whether the anchor is selected, let $c_f$ count selected candidates from group $f$, and let $d$ count selected dummies. Vanishing of the group coordinates gives $c_f = \zeta$ for every $f$, and vanishing of the dummy coordinate gives $d = 0$. Since $e(P) = k - 1$, the support-size identity becomes

$$k = \zeta + \sum_{f \in E(P)} c_f + d = k\zeta.$$

Hence $\zeta = 1$, every $c_f = 1$, and no dummy is selected. □

**Lemma 52** (Coordinate range)**.** *For every $k$-support $S$, one has $\|y_S\|_\infty \leq kN$.*

*Proof.* Every coordinate of every role vector has absolute value at most $N$: group, guard, and dummy entries lie in $\{-1, 0, 1\}$, while consistency entries lie in $[-N, N]$. Summing $k$ vectors gives the claimed bound. □

Recall that $B = 2^q > 2kN$, $R = R(P)$, $m_\Sigma(P, N) = qR$, and $2^{m_\Sigma(P,N)} = B^R$.

**Lemma 53** (Faithful balanced-digit packing)**.** *For every $y \in \mathbb{Z}^R$ with $\|y\|_\infty \leq kN$,*

$$\Phi(y) \equiv 0 \pmod{B^R} \quad \Longleftrightarrow \quad y = 0. \tag{117}$$

*Proof.* The reverse implication is immediate. For the forward implication, proceed by induction on $R$. When $R = 1$, divisibility by $B$ gives $B \mid y_0$, while $|y_0| \leq kN < B/2$, so $y_0 = 0$.

Assume $R > 1$. Reducing $\Phi(y) = y_0 + B \sum_{i=1}^{R-1} y_i B^{i-1}$ modulo $B$ shows that $B \mid y_0$, and the same balanced-range argument gives $y_0 = 0$. Dividing by $B$ then gives

$$B^{R-1} \mid \sum_{i=1}^{R-1} y_i B^{i-1}. \tag{118}$$

The remaining digits satisfy the same $\ell_\infty$ bound, so the induction hypothesis gives $y_1 = \cdots = y_{R-1} = 0$. □

**Lemma 54** (Single-column range)**.** *For every anchor, candidate, or dummy index $j$,*

$$|\Phi(\mathrm{vec}(j))| < B^R. \tag{119}$$

*Proof.* Every coordinate of $\mathrm{vec}(j)$ has absolute value at most $N$, and $B > 2kN \geq 2N$. Hence

$$|\Phi(\mathrm{vec}(j))| \leq N \sum_{i=0}^{R-1} B^i < \frac{B}{2} \cdot \frac{B^R - 1}{B - 1} < B^R, \tag{120}$$

where the last inequality uses $B > 2$. □

*Remark* 55 (Why low-bit modulus extension fails). Let $S$ be the support arising from an accepting source map, so $y_S = 0$. Put $t_j := \Phi(\mathrm{vec}(j))$ and let $w$ be the number of selected indices with $t_j < 0$. The anchor has negative exact packed value, so $1 \leq w \leq k$. By Lemma 54, reduction modulo $B^R$ wraps each negative $t_j$ exactly once and each nonnegative $t_j$ not at all; therefore

$$\sum_{j \in S} \widehat{a}_j = \sum_{j \in S} t_j + wB^R = wB^R. \tag{121}$$

If these residues are merely viewed as low-bit integers modulo $2^m$ and $2^{m - m_\Sigma(P,N)} > k$, then Equation (121) is nonzero modulo $2^m$, so the true witness is rejected. This is the reason for the top-bit scaling.

**Lemma 56** (Top-bit scaling)**.** *For every $m \geq m_\Sigma(P, N)$ and every integer $Z$,*

$$2^m \mid 2^{m - m_\Sigma(P,N)} Z \quad \Longleftrightarrow \quad 2^{m_\Sigma(P,N)} \mid Z. \tag{122}$$

*Consequently, for every support $S$,*

$$\sum_{j \in S} a_j \equiv 0 \pmod{2^m} \quad \Longleftrightarrow \quad \sum_{j \in S} \widehat{a}_j \equiv 0 \pmod{2^{m_\Sigma(P,N)}}. \tag{123}$$

*Proof.* The first equivalence follows by cancelling the common power of two $2^{m - m_\Sigma(P,N)}$ from the divisibility relation. Apply it to $Z = \sum_{j \in S} \widehat{a}_j$ to obtain the second equivalence. □

**Lemma 57** (Packed supports are exact)**.** *For every $k$-support $S$,*

$$\sum_{j \in S} a_j \equiv 0 \pmod{2^m} \quad \Longleftrightarrow \quad y_S = 0. \tag{124}$$

*Proof.* By Lemma 56, the modular equation on the left is equivalent to $\sum_{j \in S} \widehat{a}_j \equiv 0 \pmod{B^R}$. Since $\widehat{a}_j \equiv \Phi(\mathrm{vec}(j)) \pmod{B^R}$ and $\Phi$ is $\mathbb{Z}$-linear, this is equivalent to

$$\Phi\left(\sum_{j \in S} \mathrm{vec}(j)\right) = \Phi(y_S) \equiv 0 \pmod{B^R}. \tag{125}$$

By Lemma 52, $\|y_S\|_\infty \leq kN$, so Lemma 53 makes Equation (125) equivalent to $y_S = 0$. □

*Proof of Theorem 16.* Assume first that $P\text{-SUB}_N(X) = 1$ via an accepting map $\phi$, and select the support

$$S_\phi := \{\alpha\} \cup \{c_{f,\phi(a_f),\phi(b_f)} : f \in E(P)\}. \tag{126}$$

Every group coordinate of $y_{S_\phi}$ is $1-1=0$. Every consistency coordinate compares two occurrences of the common value $\phi(a)$ and is zero. Every selected edge is present, so every guard contribution is zero, and no dummy is selected. Hence $y_{S_\phi} = 0$, and Lemma 57 gives a zero-sum $k$-support modulo $2^m$.

Conversely, suppose the constructed $k$-SUM instance has a zero-sum support $S$ of size $k$. By Lemma 57, $y_S = 0$, and Lemma 51 forces the anchor, exactly one candidate $c_{f,u_f,w_f}$ from each group, and no dummies. The guard coordinate is the nonnegative sum $\sum_f \overline{X}_{f,u_f,w_f}$; since it is zero, every term is zero and every selected edge is present. Each consistency coordinate is the signed difference of the labels proposed by a non-reference group and the reference group at the same pattern vertex, so its vanishing makes those labels equal. Define $\phi(a)$ to be the common proposed label at each non-isolated vertex and choose an arbitrary value for every isolated vertex. Then $X_{f,\phi(a_f),\phi(b_f)} = 1$ for every $f$, and the source instance accepts.

The column budget permits all genuine indices and enough dummies to reach length $n$, with repeated dummy residues allowed by Definition 7. The anchor and dummy residues are constants.

For a candidate $c_{f,u,w}$, every coordinate of $\text{vec}(c_{f,u,w})$ is constant except the guard coordinate $\overline{X}_{f,u,w}$, so the packed-and-scaled integer $a_{f,u,w}(X)$ takes one of two fixed $m$-bit values according to the single bit $X_{f,u,w}$. At each output bit position, a Boolean function of one bit is either a constant, that bit, or its negation. Thus every target input bit is a constant, $X_{f,u,w}$, or $\overline{X}_{f,u,w}$, and the map is a projection.

Finally, Equations (31) and (32) give

$$m_\Sigma(P, N) = R(P) \lceil \log(2kN+1) \rceil = O(k \log(2kN)). \tag{127}$$

The support-rigidity proof used exact integer equalities and never the parity of $k$, so the construction applies to both odd and even $k$. ☐

# D Parameter Completions

This appendix completes the parameter picture left implicit in the main theorems. We first record how each projection extends beyond its constructed constraint budget and then optimize the source host size when the available row count or bit width is smaller than the principal $O(k \log n)$-scale budget used in Theorem 17.

We do not pursue an analogous $k$-OV dimension interpolation in the fixed-$k$ results below. Unlike the two list targets, whose construction floors depend only on $k$, the $k$-OV floor $k + s_{k,n} \geq k + \ell_n$ grows with the target universe: the identifier block enforcing the promise in Definition 7 is sized by $n$, not by the source host $N$. For fixed $k$, this floor and the principal budget $C_{\text{OV}} k \log n$ are both $\Theta(\log n)$, so varying $N$ trades one constant against another rather than opening a regime analogous to $m \ll k \log(n/k)$.

The final subsection records two boundary regimes outside this interpolation: a small-modulus degeneracy and a parity-hard restriction at the minimal universe $n = k$.

## D.1 Extension beyond the constructed budget

*Remark* 58 (Monotone extension of the constraint parameter). Let $P$ be a pattern with $e(P) = k-1$, and suppose one of the projections in Theorem 10 has been constructed at its native constraint parameter. Then the same source instance projects to every larger admissible target parameter: from $D_0 := D_0(P, N, n)$ to every $D \geq D_0$ for $k$-$\mathsf{OV}$, from $m_0 := m_\oplus(P, N)$ to every $m \geq m_0$ for odd-$k$ $k$-$\mathsf{XOR}$, and from $m_0 := m_\Sigma(P, N)$ to every $m \geq m_0$ for $k$-$\mathsf{SUM}$.

*Proof.* For $k$-$\mathsf{OV}$, append $D - D_0$ coordinates that are 0 on every vector; this preserves pairwise distinctness within each array and makes the product of every one-vector-per-class selection identically zero on the new coordinates. For $k$-$\mathsf{XOR}$, append $m - m_0$ all-zero rows, which do not change the sum of any support. For $k$-$\mathsf{SUM}$, let $\widehat{a}_j \in \mathbb{Z}_{2^{m_0}}$ be the residue produced at width $m_0$ and replace it at width $m$ by $a_j := 2^{m-m_0}\widehat{a}_j \in \mathbb{Z}_{2^m}$, as in Equation (35). For every support $S$,

$$\sum_{j\in S} a_j \equiv 0 \pmod{2^m} \iff 2^m \mid 2^{m-m_0}\sum_{j\in S}\widehat{a}_j \iff \sum_{j\in S}\widehat{a}_j \equiv 0 \pmod{2^{m_0}}.$$

Every added target bit is still a Boolean function of at most the single source bit on which the original residue depended, and is therefore a constant, that bit, or its negation. Thus all three extensions remain depth-zero projections; this remark consolidates operations already built into Theorems 13, 15 and 16 rather than adding a separate reduction. ☐

**Growing $k$ for $k$-$\mathsf{OV}$.** Although the identifier floor leaves no qualitatively new fixed-$k$ window, the explicit growing-pattern source bounds do yield a shifted interpolation above that floor. For every pattern $P$ with $e(P) = k - 1$, one has $|\mathcal{I}(P)| \leq 2e(P)$ and therefore

$$D_0(P, N, n) \leq 4k\ell_N + k + 2\ell_n.$$

Define

$$w_{\mathrm{OV}} := \left[\min\left\{\frac{1}{2}\log n, \frac{D - k - 2\ell_n}{4k}\right\}\right]_+.$$

If $w_{\mathrm{OV}} > 0$, put $N := 2^{\lfloor w_{\mathrm{OV}}\rfloor}$. Then $N^2 \leq n$ and $D_0(P, N, n) \leq D$. Hence Theorem 13 applied to $P_k^{\exp}$, followed by Theorem 21(i), gives

$$w_{\mathrm{OV}} \geq 2\log k + 1 \implies \log \mathrm{size}_2(k\text{-}\mathsf{OV}_{n,D,k}) \geq \frac{\gamma_D}{2} k w_{\mathrm{OV}}$$

for every $k \geq k_D$. In particular, once $D \geq 2(k + 2\ell_n)$ and the corresponding onset condition holds, this conclusion has exponent $\Omega(\min\{k \log n, D\})$.

## D.2 General row counts for odd $k$-XOR

The exact formula in Equation (29) yields a convenient absolute estimate. Since $e(P) = k - 1$, $|\mathcal{I}(P)| \leq 2e(P)$, and $r_{\mathrm{guard}}(P, N) = \lceil 2e(P)\log N + e(P) + 1\rceil$, for every $k \geq 2$ and $N \geq 1$,

$$m_\oplus(P, N) \leq 4(k-1)\log(2N) + 2(k-1) + 3 \leq 8k\log(2N). \tag{128}$$

The bound depends only on the edge count, so it applies uniformly to the expander pattern family used below.

**Theorem 59** (General row count for odd $k$-XOR)**.** *There is a universal constant $c_\oplus > 0$ with the following property. For every fixed depth $d$ and every fixed odd integer $k \geq k_0$, there is a threshold $L_\oplus(d, k)$ such that, whenever*

$$w_\oplus := \min\left\{\log\frac{n}{k}, \frac{m}{k}\right\} \geq L_\oplus(d, k), \tag{129}$$

*one has*

$$\log \operatorname{size}_d(k\text{-}\mathsf{XOR}_{n,m,k}) \ge c_\oplus \min\left\{k \log \frac{n}{k}, m\right\}. \tag{130}$$

*Equivalently,* $\operatorname{size}_d(k\text{-}\mathsf{XOR}_{n,m,k}) \ge \exp\bigl(\Omega(\min\{k\log(n/k), m\})\bigr)$*, with a universal implied constant; only the onset threshold depends on* $(d,k)$*.*

*Proof.* Fix a universal source rate $\gamma_\star$ with $0 < \gamma_\star < c_\kappa$, and let $N_0(d,k)$ be the threshold supplied by Corollary 6 for $P_k^{\exp}$ and $\gamma_\star$. Define

$$Y_\oplus := \min\left\{2^{m/(8k)-1}, \sqrt{\frac{n-1}{k-1}}\right\}, \qquad N := \lfloor Y_\oplus \rfloor. \tag{131}$$

The second term ensures $1 + (k-1)N^2 \le n$. The first gives $\log(2N) \le m/(8k)$, so Equation (128) implies $m_\oplus(P_k^{\exp}, N) \le m$. Thus Theorem 15 gives a projection from $P_k^{\exp}$-$\mathrm{SUB}_N$ to $k$-$\mathsf{XOR}_{n,m,k}$.

Set $x := w_\oplus$. Once $x$ is above an absolute constant, one has $n \ge k$ and $Y_\oplus \ge 2$. Using $(n-1)/(k-1) \ge n/k$ and $\lfloor Y_\oplus \rfloor \ge Y_\oplus/2$ gives

$$\begin{aligned}\log N &\ge \min\left\{\frac{m}{8k} - 1, \frac{1}{2}\log\frac{n-1}{k-1}\right\} - 1\\ &\ge \min\left\{\frac{x}{8} - 1, \frac{x}{2}\right\} - 1 \ge \frac{x}{16},\end{aligned} \tag{132}$$

where the last inequality holds after increasing the absolute lower bound on $x$. Choose $L_\oplus(d,k)$ large enough that Equation (132) also forces $N \ge N_0(d,k)$. Projection monotonicity and Corollary 6 then yield

$$\begin{aligned}\log \operatorname{size}_d(k\text{-}\mathsf{XOR}_{n,m,k}) &\ge \gamma_\star(k-1)\log N\\ &\ge \frac{\gamma_\star}{32} k w_\oplus = \frac{\gamma_\star}{32}\min\left\{k\log\frac{n}{k}, m\right\},\end{aligned}$$

using $k - 1 \ge k/2$. Taking $c_\oplus := \gamma_\star/32$ proves the theorem. □

### D.3 General bit widths for $k$-SUM

For this construction, the integer packing depends on $kN$, rather than on $N$ alone. Indeed, Equations (31) and (32) imply, for every $k \ge 2$ and $N \ge 1$,

$$m_\Sigma(P, N) = R(P)\lceil \log(2kN+1)\rceil \le 9k\log(2kN), \tag{133}$$

because $R(P) \le 3k$ and $\lceil \log(2kN+1)\rceil \le 3\log(2kN)$. The factor $k$ inside the logarithm produces the $-\log k$ term below.

**Theorem 60** (General bit width for $k$-SUM)**.** *There is a universal constant $c_\Sigma > 0$ with the following property. For every fixed depth $d$ and every fixed integer $k \ge k_0$, of either parity, there is a threshold $L_\Sigma(d,k)$ such that, with*

$$w_\Sigma := \left[\min\left\{\log\frac{n}{k}, \frac{m}{9k} - \log(2k)\right\}\right]_+, \qquad [x]_+ := \max\{x, 0\}, \tag{134}$$

*the implication*

$$w_\Sigma \ge L_\Sigma(d,k) \quad\Longrightarrow\quad \log \operatorname{size}_d(k\text{-}\mathsf{SUM}_{n,m,k}) \ge c_\Sigma k w_\Sigma \tag{135}$$

*holds. The constant $c_\Sigma$ is universal; only the onset threshold depends on $(d,k)$.*

*Proof.* Use the same universal $\gamma_\star$ as in the proof of Theorem 59, and let $N_0(d,k)$ be the corresponding source threshold. Define

$$Y_\Sigma := \min\left\{\frac{2^{m/(9k)}}{2k}, \sqrt{\frac{n-1}{k-1}}\right\}, \qquad N := \lfloor Y_\Sigma \rfloor. \tag{136}$$

The column budget again holds by the second term. The first term gives $\log(2kN) \le m/(9k)$, so Equation (133) implies $m_\Sigma(P_k^{\exp}, N) \le m$. Hence Theorem 16 gives a projection from $P_k^{\exp}$-SUB$_N$ to $k$-$\mathsf{SUM}_{n,m,k}$.

Write $x := w_\Sigma$. If $x > 0$, then both entries inside the minimum in Equation (134) are positive. Since $(n-1)/(k-1) \ge n/k$, one has

$$\log Y_\Sigma \ge \min\left\{\frac{m}{9k} - \log(2k), \frac{1}{2}\log\frac{n}{k}\right\} \ge \frac{x}{2}.$$

Once $x \ge 4$, this gives $Y_\Sigma \ge 2$ and therefore

$$\log N \ge \log Y_\Sigma - 1 \ge \frac{x}{4}. \tag{137}$$

Choose $L_\Sigma(d,k)$ large enough that Equation (137) forces $N \ge N_0(d,k)$. By projection monotonicity and Corollary 6,

$$\begin{aligned}\log \operatorname{size}_d(k\text{-}\mathsf{SUM}_{n,m,k}) &\ge \gamma_\star(k-1)\log N \\ &\ge \frac{\gamma_\star}{8} k w_\Sigma,\end{aligned}$$

where $k-1 \ge k/2$ is used in the last step. Taking $c_\Sigma := \gamma_\star/8$ proves the theorem. $\square$

**Growing $k$ at depth two.** The fixed-$k$ qualification in Theorems 59 and 60 enters only through Corollary 6. Replacing that source bound by Theorem 21(i), the same host choices give, for every $k \ge k_D$, the implications

$$\begin{aligned} w_\oplus \ge 32\log k \quad &\Longrightarrow \quad \log \operatorname{size}_2(k\text{-}\mathsf{XOR}_{n,m,k}) \ge \frac{\gamma_D}{16} k w_\oplus \qquad \text{for odd } k, \\ w_\Sigma \ge 8\log k \quad &\Longrightarrow \quad \log \operatorname{size}_2(k\text{-}\mathsf{SUM}_{n,m,k}) \ge \frac{\gamma_D}{4} k w_\Sigma. \end{aligned}$$

Indeed, Equations (132) and (137) then force $N \ge k^2$. Together with the preceding $k$-$\mathsf{OV}$ interpolation, the parameter completion is uniform for growing $k$ at depth two once the corresponding logarithmic host size $w_{\mathrm{OV}}$, $w_\oplus$, or $w_\Sigma$ is $\Omega(\log k)$. No analogous low-row consequence follows from the even-$K$ lift: its tag matrix and inert-column padding already cost $\Theta(K\log n')$ rows independently of the source host size.

The $[\cdot]_+$ and the subtraction of $\log(2k)$ are substantive. They keep the theorem silent whenever the available width does not permit a growing source host. Far above that boundary, the familiar minimum form is recovered.

**Corollary 61** (High-width minimum form for $k$-SUM)**.** *For every fixed depth $d$ and every fixed integer $k \ge k_0$, there is a threshold $L'_\Sigma(d,k)$ such that, whenever*

$$m \ge 18k\log(2k) \qquad \text{and} \qquad \min\left\{\log\frac{n}{k}, \frac{m}{k}\right\} \ge L'_\Sigma(d,k), \tag{138}$$

*one has*

$$\operatorname{size}_d(k\text{-}\mathsf{SUM}_{n,m,k}) \ge \exp\left(\Omega\left(\min\left\{k\log\frac{n}{k}, m\right\}\right)\right), \tag{139}$$

*with a universal implied constant.*

*Proof.* Put $u := \min\{\log(n/k), m/k\}$. The first hypothesis gives $m/(9k) - \log(2k) \geq m/(18k)$, and therefore

$$w_\Sigma \geq \min\left\{\log \frac{n}{k}, \frac{m}{18k}\right\} \geq \frac{u}{18}.$$

Choose $L'_\Sigma(d,k) := 18L_\Sigma(d,k)$. Then Theorem 60 applies and gives

$$\log \mathrm{size}_d \geq \Omega(ku) = \Omega\left(\min\left\{k \log \frac{n}{k}, m\right\}\right).$$

□

## D.4 Two boundary cases for $k$-SUM

The next two propositions show why no uniform lower bound can cover the silent regime: one boundary family is constant, while another contains PARITY under a restriction. The latter restriction also supplies the fixed-support verification floor used in the discussion following Equation (184) and in Section 8.1.

**Proposition 62** (Erdős–Ginzburg–Ziv degeneracy). *If $k = 2^m$ and $n \geq 2k-1$, then $k$-$\mathsf{SUM}_{n,m,k}$ is identically one.*[2]

*Proof.* Write $G = \mathbb{Z}_{2^m}$, a cyclic group of order $2^m = k$. Fix an arbitrary input $x = (x_1, \ldots, x_n) \in G^n$ and any $S \subseteq [n]$ with $|S| = 2k-1$, which exists since $n \geq 2k-1$. The Erdős–Ginzburg–Ziv theorem [EGZ61] asserts that every sequence of $2k-1$ elements of $G$, repetitions permitted, admits a subsequence of length exactly $k$ summing to 0;[3] applied to $(x_i)_{i \in S}$ it yields $I \subseteq S$ with $|I| = k$ and $\sum_{i \in I} x_i = 0$ in $G$. Since $I$ is a set of $k$ distinct indices of $[n]$, it witnesses $k$-$\mathsf{SUM}_{n,m,k}(x) = 1$; as $x$ was arbitrary, the function is identically one. □

**Proposition 63** (The parity corner at every bit width). *Under the convention that $\mathsf{PARITY}_k(x) = 1$ on odd Hamming weight, for every $m \geq 1$,*

$$k\text{-}\mathsf{SUM}_{k,m,k}(2^{m-1}x_1, \ldots, 2^{m-1}x_k) = 1 - \mathsf{PARITY}_k(x). \tag{140}$$

*Consequently, for every fixed depth $d \geq 2$ and every $m \geq 1$, once $k$ is sufficiently large as a function of $d$,*

$$\mathrm{size}_d(k\text{-}\mathsf{SUM}_{k,m,k}) \geq \exp\big(\Omega_d(k^{1/(d-1)})\big). \tag{141}$$

*Proof.* When $n = k$, the only size-$k$ support is all of $[k]$. On the displayed restriction, its sum is $2^{m-1}|x|$, which vanishes modulo $2^m$ exactly when $|x|$ is even; this proves Equation (140). For Equation (141), first observe that $\mathrm{size}_d(f) = \mathrm{size}_d(\neg f)$ exactly in our model because only non-input AND/OR gates are counted and complementing a leaf literal introduces no gate. Given a depth-$d$ circuit for $f$, swap every $\wedge$ with $\vee$, complement every input literal, and interchange constant leaves 0 and 1 if they occur. Induction on gate height shows that the transformed gate computes the complement of the original gate, so the transformed circuit has the same size and depth and computes $\neg f$; applying the same involution to a circuit for $\neg f$ gives the reverse inequality. The substitution in Equation (140) realizes $1 - \mathsf{PARITY}_k$ as a depth-zero restriction of the total indexed-list function $k$-$\mathsf{SUM}_{k,m,k}$. Therefore Lemma 9, the dualization equality, and the fixed-depth PARITY bound recorded in Section 6.4 imply Equation (141) once $k$ exceeds the depth-dependent onset. □

[2]This proposition and its proof were proposed by the AI language model GPT-5.5; the authors independently verified the argument before inclusion.

[3][EGZ61] phrases this for a set of $2k-1$ integers and a subset of $k$ of them. The sequence form is what the proof there establishes, and the two are equivalent: given $g_1, \ldots, g_{2k-1} \in \mathbb{Z}_k$ with representatives $\tilde{g}_i \in [0,k)$, the integers $z_i := \tilde{g}_i + ki$ are pairwise distinct, since $z_i \in [ki, ki+k)$ and these intervals are disjoint, and satisfy $z_i \equiv g_i \pmod{k}$.

The same fixed-support floor is shared by $k$-XOR. For every $m \geq 1$, set rows $2, \ldots, m$ to zero and leave the first-row bits $x_1, \ldots, x_k$ free. Since $n = k$, the only candidate support is $[k]$, and hence

$$k\text{-}\mathsf{XOR}_{k,m,k}\big((x_1, 0^{m-1}), \ldots, (x_k, 0^{m-1})\big) = 1 - \mathsf{PARITY}_k(x). \tag{142}$$

This is a genuine depth-zero restriction of the total indexed-list function in Definition 7, not a promise-sensitive map. All $k$ first-row bits remain free, and the substitution uses only literals and constants. By Lemma 9, the preceding dualization equality, and the fixed-depth PARITY bound recorded in Section 6.4, for every fixed depth $d \geq 2$ and every $m \geq 1$, once $k$ is sufficiently large as a function of $d$,

$$\mathrm{size}_d(k\text{-}\mathsf{XOR}_{k,m,k}) \geq \exp\big(\Omega_d(k^{1/(d-1)})\big). \tag{143}$$

Consequently, no fixed depth yields a polynomial-size per-support verifier uniformly in $k$ for either list target. As Propositions 70 and 71 make explicit, the later comparison instead distinguishes the $m\,2^{k-1}$-clause CNF for a fixed $k$-XOR support from the $2^{(k-1)m}$-term direct DNF for a fixed $k$-SUM support, and then from the block-carry $\Sigma_3$ verifier.

The two propositions concern different boundary phenomena. At $k = 2^m$ and $n \geq 2k-1$, the function is trivial by additive combinatorics, whereas at $n = k$ every bit width contains a parity-hard two-point restriction. Neither contradicts Theorem 60: in both cases the host-size parameter $w_\Sigma$ is below the theorem's onset threshold. The hypothesis $n \geq 2k-1$ is optimal: at $n = 2k-2$ the input consisting of $k-1$ zeros and $k-1$ ones has no zero-sum witness, since any $k$ of its coordinates contain $j$ ones with $1 \leq j \leq k-1$, and $j \not\equiv 0 \pmod{k}$.

# E Supplementary Results for $k$-XOR

This appendix contains two black-box extensions of the principal odd-$k$ $k$-XOR results. The first is a projection from an odd source parameter to an even target parameter, parameterized by a supplied admissible decomposition of the target parameter. The second is the amplified PARITY projection stated in Theorem 24, together with a matching limitation for every projection-based PARITY reduction.

## E.1 The even-$K$ lifting projection

The threshold $k_0$ fixed in Corollary 38 already satisfies $k_0 \geq 3$. The lift uses a nonuniformly fixed tag matrix to force every target witness of weight at most $K$ to lie in the image of a repetition code. The $t$-fold repetition makes an odd-weight source witness of weight $r$ occupy $tr$ positions, while the $s$ auxiliary copies of the parity bit $p(\xi)$ raise that weight to $tr + s = K$; even-weight vectors remain at weights divisible by $t$, so the condition $t \nmid s$ eliminates that branch, with the case $s = 0$ handled by the opposite parities of $r$ and an even weight.

The next lemma is the standard probabilistic parity-check-matrix argument; we include it to fix the nonuniform tag construction and its exact row count.

**Lemma 64** (Separating tag matrix)**.** *Let $n' \geq 2$ and $K \geq 1$, and let $U \subseteq \mathbb{F}_2^{n'}$ be a linear subspace. Put*

$$q := (K+1)\lceil \log n' \rceil + 1. \tag{144}$$

*There is a matrix $\Pi \in \mathbb{F}_2^{q \times n'}$ such that $U \subseteq \ker \Pi$ and every $y \in \ker \Pi$ with $|y| \leq K$ belongs to $U$.*

*Proof.* Let $\pi : \mathbb{F}_2^{n'} \to \mathbb{F}_2^{n'}/U$ be the quotient map. Choose $q$ independent uniformly random linear functionals $\varphi_1, \ldots, \varphi_q$ on $\mathbb{F}_2^{n'}/U$, and let $\Pi$ be the matrix representing $(\varphi_1 \circ \pi, \ldots, \varphi_q \circ \pi)$. Then

$U \subseteq \ker \Pi$ deterministically. For each fixed $y \notin U$, the class $\pi(y)$ is nonzero, so every $\varphi_h$ annihilates it with probability $1/2$, independently, and therefore

$$\Pr[\Pi y = 0^q] = 2^{-q}. \tag{145}$$

The number of vectors of weight at most $K$ is at most

$$\sum_{j=0}^{K} \binom{n'}{j} \le \sum_{j=0}^{K} (n')^j \le 2(n')^K. \tag{146}$$

By Equation (144), the expected number of vectors $y \notin U$ with $|y| \le K$ and $\Pi y = 0^q$ is at most

$$2(n')^K 2^{-q} \le (n')^{-1} < 1.$$

Hence some fixed choice of the functionals leaves no such vector, and the corresponding matrix has the required property. □

**Lemma 65** (Odd-to-even lifting projection)**.** *Let $r \ge 1$ be odd, let $t \ge 2$ and $s \ge 0$ be integers, put $K := tr + s$, and assume that $K$ is even and that either $s = 0$ or $t \nmid s$. Then, for all $n, m \ge 1$, there is a projection*

$$k\text{-}\mathsf{XOR}_{n,m,r} \le_{\text{proj}} k\text{-}\mathsf{XOR}_{tn+s,m+q,K}, \qquad q = (K+1)\lceil \log(tn+s) \rceil + 1. \tag{147}$$

*Proof.* For $\xi \in \mathbb{F}_2^n$, write $p(\xi) := \bigoplus_{i=1}^n \xi_i$ and define the linear repetition map $\mathrm{rep} : \mathbb{F}_2^n \to \mathbb{F}_2^{tn+s}$ by

$$\mathrm{rep}(\xi) := \big(\underbrace{\xi_1, \ldots, \xi_1}_{t}, \ldots, \underbrace{\xi_n, \ldots, \xi_n}_{t}, \underbrace{p(\xi), \ldots, p(\xi)}_{s}\big). \tag{148}$$

Put $U := \operatorname{im} \mathrm{rep}$. The map is injective because $\xi_i$ is recovered from the first copy of the $i$th block, and its Hamming weight satisfies

$$|\mathrm{rep}(\xi)| = t|\xi| + s\big(|\xi| \bmod 2\big). \tag{149}$$

Let $n'' := tn + s$, and let $\Pi \in \mathbb{F}_2^{q \times n''}$ be supplied by Lemma 64 for $U$ and $K$, with columns $\Pi_1, \ldots, \Pi_{n''}$. The target universe contains $t$ copies of every source index followed by $s$ auxiliary indices. For each target position $j$ corresponding to the first copy of source index $i$, the target column is the concatenation of the source column $a_i \in \mathbb{F}_2^m$ with that position's tag $\Pi_j$; every remaining copy and every auxiliary position $j$ has payload $0^m$ and tag $\Pi_j$. Every target bit is therefore a constant or a source bit, so this map is a projection.

Suppose first that $\xi$ is the indicator of a source witness. Then $|\xi| = r$ and the selected source payloads sum to zero. Since $r$ is odd, Equation (149) gives $|\mathrm{rep}(\xi)| = tr + s = K$; moreover, $\mathrm{rep}(\xi) \in U \subseteq \ker \Pi$, and the selected target payloads are exactly the selected source payloads. Thus $\mathrm{rep}(\xi)$ is a target witness.

Conversely, let $y \in \mathbb{F}_2^{n''}$ indicate a target witness. Its tag sum is zero and $|y| = K$, so Lemma 64 gives $y \in U$. Write $y = \mathrm{rep}(\xi)$ for the unique $\xi \in \mathbb{F}_2^n$. If $|\xi|$ is odd, then Equation (149) and $|y| = K = tr + s$ imply $|\xi| = r$. If $|\xi|$ is even, then the same equations give $t|\xi| = tr + s$, so $t \mid s$. When $s > 0$ this contradicts the hypothesis, and when $s = 0$ it gives $|\xi| = r$, contradicting the opposite parities of $|\xi|$ and $r$. Hence $|\xi| = r$. Finally, the target payload sum is the XOR of the source columns indexed by $\mathrm{supp}(\xi)$, so its vanishing makes $\xi$ a source witness. □

*Remark* 66 (Nonuniformity and arbitrary target universes). The matrix $\Pi$ is chosen by the probabilistic method and fixed once for each parameter tuple before the input is read, which is legitimate for the nonuniform circuit lower bounds considered here. To reach an arbitrary target universe size $n' \geq t+s$, let $n := \lfloor (n'-s)/t \rfloor$ and $\rho := n' - (tn+s) < t$. Apply Lemma 65 to the first $tn+s$ columns and append $\rho$ columns that are zero on every existing row, giving each one a private guard row equal to 1 on that column and 0 elsewhere. No zero-sum support uses any appended column, and the additional row count is less than $t$. Appending all-zero rows then reaches every larger target row count without changing the function.

## E.2 Consequences of the lift

The lift is independent of the source of the odd-$k$ lower bound. We first recover the fixed-$k$ statement quoted in Section 5 and then apply the same projection to the conditional all-depth theorem.

Call a tuple $(t, r, s)$ admissible for an even integer $K$ when $t \geq 2$, $r \geq 1$ is odd, $0 \leq s < 2t$, $K = tr + s$, and either $s = 0$ or $t \nmid s$. By Lemma 65, every admissible tuple gives an odd-to-even projection. We use the same elementary estimates in the consequences below. Let $(t, r, s)$ be admissible for $K$, assume $r \geq 3$, and for a target universe size $n'$ put $n := \lfloor (n'-s)/t \rfloor$. Since $tn + s \leq n' < t(n+1) + s < t(n+3)$ and $tr \leq K < t(r+2)$, whenever $n \geq 3$ and $n'/K \geq 4$ one has

$$\frac{n}{r} \geq \frac{n'}{2K} \geq \left(\frac{n'}{K}\right)^{1/2}. \tag{150}$$

Moreover, the tag matrix and the inert-column padding add $O(K \log n')$ rows in total. More explicitly, let $q$ be the tag-row count in Equation (147) and let $\rho < t$ be the number of inert columns in Remark 66. There is a universal constant $C'_{\oplus} > 0$ such that, given a target budget $m' \geq C'_{\oplus} K \log n'$, the quantity $\widetilde{m} := m' - q - \rho$ exceeds each source row budget used below. Applying the source theorem at row count $\widetilde{m}$, then adding the $q$ tag rows and the $\rho$ private guard rows, fits within $m'$, and all-zero padding reaches the budget exactly.

**Corollary 67** (Fixed even $K$ from an admissible odd parameter)**.** *Let $K$ be even, and let $(t, r, s)$ be admissible for $K$ with $r \geq k_0$. For every fixed depth $d$ there is a threshold $n'_1(d, K, t, r, s)$ such that, for every $n' \geq n'_1(d, K, t, r, s)$ and every $m' \geq C'_{\oplus} K \log n'$,*

$$\mathrm{size}_d(k\text{-}\mathsf{XOR}_{n',m',K}) \geq (n'/K)^{\beta(r-1)/2}, \tag{151}$$

*where $\beta$ is the universal target-rate constant of Theorem 17.*

*Proof.* Put $n := \lfloor (n'-s)/t \rfloor$ and use the arbitrary-universe version of the lift from Remark 66. For $n'$ above a threshold depending on $(d, K, t, r, s)$, the source universe satisfies the onset condition in Theorem 17, the source theorem applies at row count $\widetilde{m}$, and the common row estimate above fits the lifted instance within every $m' \geq C'_{\oplus} K \log n'$. Projection monotonicity therefore gives

$$\mathrm{size}_d(k\text{-}\mathsf{XOR}_{n',m',K}) \geq \mathrm{size}_d(k\text{-}\mathsf{XOR}_{n,\widetilde{m},r}) \geq (n/r)^{\beta(r-1)}. \tag{152}$$

After enlarging the threshold so that Equation (150) applies, substituting that estimate into Equation (152) proves Equation (151). $\square$

**Corollary 68** (Conditional all-depth bound for even $K$ from an admissible odd parameter)**.** *Assume Conjecture 26, and fix a depth $d$. There are $k_E^{\oplus}(d) \in \mathbb{N}$ and $C_E^{\oplus}(d) > 1$ such that the following holds. Let $K$ be even, and let $(t, r, s)$ be admissible for $K$ with $r \geq k_E^{\oplus}(d)$. If $n' \geq K^{C_E^{\oplus}(d)}$ and $m' \geq C'_{\oplus} K \log n'$, then*

$$\mathrm{size}_d(k\text{-}\mathsf{XOR}_{n',m',K}) \geq \exp\bigl(\Omega_d\bigl(r \log n'\bigr)\bigr). \tag{153}$$

*Proof.* Let $k_E^{\oplus}(d)$ be at least $k_E(d)$ from Theorem 28 and at least $k_0$. Choose $C_E^{\oplus}(d) \geq \max\{C_E(d)+3, 4\}$, and put $n := \lfloor (n'-s)/t \rfloor$. Since $r \leq K$ and $t \leq K$, the relation $n' \geq K^{C_E^{\oplus}(d)}$ makes $n \geq r^{C_E(d)}$ after increasing $k_E^{\oplus}(d)$ if necessary, so Theorem 28 applies to the odd-$r$ source instance at row count $\widetilde{m}$. The common row estimate above fits the lift within $C'_{\oplus} K \log n'$. Thus

$$\mathrm{size}_d(k\text{-}\mathsf{XOR}_{n',m',K}) \geq \exp\bigl(\Omega_d(r \log n)\bigr). \tag{154}$$

Moreover, $s < 2t$, $t \leq K$, and $n' \geq K^4$ imply

$$n = \left\lfloor \frac{n'-s}{t} \right\rfloor > \frac{n'}{K} - 3 \geq \sqrt{n'},$$

for every $K \geq 2$, and hence $\log n \geq \frac{1}{2} \log n'$. Substituting this estimate into Equation (154) proves Equation (153). ☐

### E.3 The row-rich PARITY route

We now prove the two statements from Section 6.4. The construction embeds a parity instance of length $\Theta(k^2 \log(n/k))$ while using only $O(n)$ target rows.

*Proof of Theorem 24.* Let $b, B, \ell$ be as in Equation (64), and put $q := 2^b$. The input variables are

$$x = (x_{r,t})_{r \in [B],\, t \in [k-1]} \in \{0,1\}^{\ell}. \tag{155}$$

The target universe contains one anchor column $a_\star$ and, for every $t \in [k-1]$, a block of $q$ columns $(t, u)$ indexed by $u \in \{0,1\}^b$. Since $q \leq n/(2k)$,

$$n_0 := 1 + (k-1)q < n, \tag{156}$$

and the remaining $n - n_0$ positions are dummies, each equipped with one private guard row. All dummy entries on the selector and data rows introduced below are set to 0. Thus no zero-sum support contains a dummy.

For each $t \in [k-1]$, add a selector row that is 1 on the anchor and on every column of block $t$, and 0 elsewhere. Let $\zeta$ indicate whether a support contains the anchor, and let $c_t$ be the number of selected columns from block $t$. Vanishing of the selector rows gives $\zeta + c_t \equiv 0 \pmod 2$ for every $t$. If $\zeta = 0$, every $c_t$ is even and the support size $\sum_t c_t = k$ is even, contradicting odd $k$. Hence $\zeta = 1$, every $c_t$ is odd, and

$$1 + \sum_{t=1}^{k-1} c_t = k.$$

Because there are $k-1$ positive odd integers in the sum, each $c_t = 1$. Every zero-sum support therefore has the form

$$\{a_\star\} \cup \{(t, u_t) : t \in [k-1]\} \tag{157}$$

for a unique tuple $u = (u_1, \ldots, u_{k-1}) \in (\{0,1\}^b)^{k-1}$.

Define $y : (\{0,1\}^b)^{k-1} \to \{0,1\}^B$ by

$$y(u)_{(t-1)b+j} := u_{t,j} \qquad \text{for } t \in [k-1],\ j \in [b], \tag{158}$$

$$y(u)_B := 1 \oplus \bigoplus_{t \in [k-1]} \bigoplus_{j \in [b]} u_{t,j}. \tag{159}$$

The image of $y$ is exactly the set of odd-parity strings in $\{0,1\}^B$. We add $B$ data rows. For a row $r = (t_r - 1)b + j_r \le (k-1)b$, put 0 on the anchor, and put the literal

$$x_{r,t} \oplus \mathbf{1}[t = t_r] u_{j_r} \tag{160}$$

on the column $(t, u)$. On the last row $B$, put 1 on the anchor and put

$$x_{B,t} \oplus \bigoplus_{j \in [b]} u_j \tag{161}$$

on the column $(t, u)$. Since $u$ is part of the column index, every expression in Equations (160) and (161) is either an input variable or its negation, and the construction is a projection.

For the support in Equation (157), data row $r$ has parity zero exactly when

$$\bigoplus_{t \in [k-1]} x_{r,t} = y(u)_r. \tag{162}$$

Such a tuple $u$ exists if and only if the vector $(\bigoplus_t x_{r,t})_{r \in [B]}$ has odd parity, which is equivalent to

$$\bigoplus_{r \in [B]} \bigoplus_{t \in [k-1]} x_{r,t} = 1. \tag{163}$$

Thus the target accepts exactly the odd-parity inputs, proving Equation (65).

The number of rows before zero padding is

$$m_0 = (k-1) + B + (n - n_0). \tag{164}$$

For $n \ge 4k$, one has $k - 1 \le n/4$ and $B \le k \log(n/k) + 1 \le n/2 + 1$, where the last inequality uses $\log x \le x/2$ for $x \ge 4$. Hence $m_0 \le 2n$. Also, $k - 1 = \Theta(k)$ and $b = \Theta(\log(n/k))$, so

$$\ell = (k-1)B = \Theta(k^2 \log(n/k)). \tag{165}$$

Appending zero rows extends the projection to every $m \ge m_0$. Every variable in Equation (155) remains free, every target bit is a constant or a possibly negated source literal, and $k$-XOR is a total function, so Equation (65) is an ordinary projection with no promise-side obligation. For fixed $d$, once $\ell$ exceeds the depth-dependent onset, the PARITY bound recorded in Section 6.4 gives size $\exp(\Omega_d(\ell^{1/(d-1)}))$, and Equation (165) yields Equation (66). $\square$

*Proof of Proposition 25.* Write $R(x) = (A_1(x), \ldots, A_n(x))$. For each support $S \in \binom{[n]}{k}$, define

$$V_S := \left\{ x \in \{0,1\}^\ell : \bigoplus_{j \in S} A_j(x) = 0^m \right\}. \tag{166}$$

Every output entry of a projection is a constant or one possibly negated input bit, hence an affine function over $\mathbb{F}_2$ involving at most one variable. Each row equation in Equation (166) is therefore affine and involves at most $k$ input variables. Thus $V_S$ is either empty or an affine subspace cut out by $k$-sparse equations.

Suppose $V_S$ is nonempty. Choose a maximal linearly independent subset of the coefficient rows defining it, and write the resulting equivalent system as $M_S x = \eta_S$, where $M_S$ has rank $r_S$ and every row has Hamming weight at most $k$. For every $x \in V_S$, the support $S$ witnesses acceptance of

$k$-$\mathsf{XOR}(R(x))$, so Equation (67) implies that the all-ones linear functional has value 1 throughout $V_S$. Writing $V_S = x_0 + \ker M_S$, this means that the all-ones vector belongs to $(\ker M_S)^{\perp}$, which is the row space of $M_S$. It is therefore the XOR of at most $r_S$ rows of $M_S$. The union of their supports has size at most $r_S k$, and consequently

$$\ell \leq r_S k. \tag{167}$$

It follows that

$$|V_S| = 2^{\ell - r_S} \leq 2^{\ell - \ell/k}. \tag{168}$$

Every odd-parity input is accepted and hence lies in $V_S$ for at least one support $S$. The $2^{\ell-1}$ odd inputs are therefore covered by at most $\binom{n}{k}$ affine spaces satisfying Equation (168). Hence

$$2^{\ell-1} \leq \binom{n}{k} 2^{\ell - \ell/k}. \tag{169}$$

Cancelling the common factor, taking logarithms, and using $\binom{n}{k} \leq (\mathrm{e}n/k)^k$ gives

$$\frac{\ell}{k} - 1 \leq \log \binom{n}{k} \leq k \log(\mathrm{e}n/k),$$

which rearranges to Equation (68). ☐

# F Elementary Upper Bounds and Quantitative Tightness

This appendix supplies the elementary circuits used to calibrate the lower bounds. Circuit size counts non-input gates, as fixed in Section 2.1; fan-in therefore affects the depth and the formula semantics but not the gate count directly.

## F.1 Brute-force circuits

**Proposition 69** (Brute-force circuit for $k$-OV)**.** *For all $n, D, k$,*

$$\mathrm{size}_{\Sigma_3}(k\text{-}\mathsf{OV}_{n,D,k}) \leq 1 + n^k(D+1). \tag{170}$$

*In particular, if $D = O(k \log n)$ and $k$ is fixed, then*

$$\mathrm{size}_{\Sigma_3}(k\text{-}\mathsf{OV}_{n,D,k}) \leq n^{k+o(1)}. \tag{171}$$

*The fixed-$k$ hypothesis is unnecessary for the sharper conclusion whenever $D = n^{o(1)}$: if $\log D = o(\log n)$, then*

$$\mathrm{size}_{\Sigma_3}(k\text{-}\mathsf{OV}_{n,D,k}) \leq n^{k+o(1)}.$$

*More generally, if $k \to \infty$ and $\log D = o(k \log n)$, then the same circuit has size $n^{k+o(k)}$.*

*Proof.* For a tuple $(i_1, \ldots, i_k) \in [n]^k$, orthogonality is the conjunction, over all coordinates $t \in [D]$, of the clause asserting that not all selected vectors have a 1 in coordinate $t$. Thus

$$k\text{-}\mathsf{OV}_{n,D,k} = \bigvee_{(i_1,\ldots,i_k)\in[n]^k} \ \bigwedge_{t\in[D]} \ \bigvee_{\ell\in[k]} \neg u_{\ell,i_\ell}(t). \tag{172}$$

The formula has one top OR gate, one middle AND gate for each of the $n^k$ tuples, and one bottom OR gate for each pair of a tuple and a coordinate $t \in [D]$, proving Equation (170). If $D = O(k \log n)$ and $k$ is fixed, then $1 + n^k(D+1) = n^{k+o(1)}$. More generally,

$$\log \mathrm{size}_{\Sigma_3}(k\text{-}\mathsf{OV}_{n,D,k}) \le k \log n + O(\log(D+1)),$$

so $\log D = o(\log n)$ gives the $n^{k+o(1)}$ estimate, while $\log D = o(k \log n)$ gives $n^{k+o(k)}$ when $k \to \infty$. $\square$

**Proposition 70** (Brute-force circuit for $k$-XOR)**.** *For all $n, m, k$,*

$$\mathrm{size}_{\Sigma_3}(k\text{-}\mathsf{XOR}_{n,m,k}) \le 1 + \binom{n}{k}\left(1 + m2^{k-1}\right) = O\left(\binom{n}{k} m 2^k\right). \tag{173}$$

*If $k$ is fixed, $n/k \to \infty$, and $\log m = o(\log(n/k))$, then*

$$\mathrm{size}_{\Sigma_3}(k\text{-}\mathsf{XOR}_{n,m,k}) \le (n/k)^{k+o(1)}. \tag{174}$$

*More generally, if $k \to \infty$, $\log(n/k) \to \infty$, and $\log m = o(k \log(n/k))$, then*

$$\mathrm{size}_{\Sigma_3}(k\text{-}\mathsf{XOR}_{n,m,k}) \le (n/k)^{k+o(k)}.$$

*Proof.* Fix a support $S \in \binom{[n]}{k}$ and a row $r \in [m]$. The condition $\bigoplus_{j \in S} A_{r,j} = 0$ is an even-parity predicate on $k$ bits and has a CNF with exactly $2^{k-1}$ clauses, one excluding each odd-parity assignment. Conjoining these clauses over all $m$ rows computes that $S$ is a zero-sum support, and taking the OR over all supports computes $k$-XOR. This gives an $\mathsf{OR} \circ \mathsf{AND} \circ \mathsf{OR}$ circuit with one top OR gate, one middle AND gate per support, and $m2^{k-1}$ bottom clause gates per support, proving Equation (173). Finally, $\binom{n}{k} \le (\mathrm{e}n/k)^k$, so

$$\log \mathrm{size}_{\Sigma_3}(k\text{-}\mathsf{XOR}_{n,m,k}) \le k \log(n/k) + O(k) + \log m = (k + o(1)) \log(n/k)$$

under the stated fixed-$k$ hypotheses. In particular, this condition holds at the principal $O(k \log n)$-scale row budgets used in Theorem 17. Without fixing $k$, the same estimate has error term $O(k) + \log m$; the growing-$k$ hypotheses in the proposition make this $o(k \log(n/k))$, proving that bound. $\square$

**Proposition 71** (Elementary circuits for $k$-SUM)**.** *For all $n \ge k \ge 2$ and $m \ge 1$,*

$$\mathrm{size}_2(k\text{-}\mathsf{SUM}_{n,m,k}) \le 1 + \binom{n}{k} 2^{(k-1)m}. \tag{175}$$

*Consequently,*

$$\log \mathrm{size}_2(k\text{-}\mathsf{SUM}_{n,m,k}) \le (k-1)m + k \log(\mathrm{e}n/k) + O(1), \tag{176}$$

*and the displayed depth-two circuit has size $2^{\Theta(km)}$ whenever $m \ge \log(\mathrm{e}n/k)$. There is also a top-disjunction depth-three block-carry circuit: for every integer $b \in [m]$, with $t := \lceil m/b \rceil$,*

$$\mathrm{size}_{\Sigma_3}(k\text{-}\mathsf{SUM}_{n,m,k}) \le 1 + \binom{n}{k} k^{t-1}\left(1 + t2^{kb}\right). \tag{177}$$

*In particular,*

$$\log \mathrm{size}_{\Sigma_3}(k\text{-}\mathsf{SUM}_{n,m,k}) \le k \log(\mathrm{e}n/k) + O\left(\sqrt{km \log k} + k + \log m\right). \tag{178}$$

*If $n \ge k^2$ and $m = \Theta(k \log(\mathrm{e}n/k))$, then*

$$\mathrm{size}_{\Sigma_3}(k\text{-}\mathsf{SUM}_{n,m,k}) \le (n/k)^{O(k)}. \tag{179}$$

*Proof.* Fix a support $S \in \binom{[n]}{k}$. Choosing arbitrary values for any $k-1$ of its residues uniquely determines the remaining residue that makes the sum zero modulo $2^m$. Hence exactly $2^{(k-1)m}$ assignments to the $km$ selected input bits satisfy the support equation. A conjunction of literals recognizes each such assignment, so the support predicate has a DNF with $2^{(k-1)m}$ terms. Taking the OR of these terms over every support gives one depth-two DNF with the gate count in Equation (175). The binomial estimate $\binom{n}{k} \leq (\mathrm{e}n/k)^k$ gives Equation (176). When $m \geq \log(\mathrm{e}n/k)$, the upper bound is $O(km)$ in the logarithm, while the construction contains $2^{(k-1)m}$ term gates for every fixed support, proving the stated $2^{\Theta(km)}$ size.

For the block-carry circuit, partition the $m$ bit positions, from least to most significant, into $t = \lceil m/b \rceil$ consecutive blocks of width at most $b$. For a fixed support, the carry into the first block is zero, and every later carry lies in $\{0, \dots, k-1\}$: the sum of $k$ $b$-bit chunks and an incoming carry at most $k-1$ is at most $k2^b - 1$. Guess the $t-1$ intermediate carries. For each nonfinal block, require that the sum of its $k$ chunks and its incoming carry equal $2^b$ times the guessed outgoing carry; for the final, possibly shorter block, require only that this sum vanish modulo the corresponding power of two. Every block predicate is a Boolean function of at most $kb$ input bits and therefore has a CNF with at most $2^{kb}$ clauses, one excluding each falsifying assignment. For a fixed support and carry guess, flatten the conjunctions of all block CNFs into one middle AND gate; then take the OR over all supports and carry guesses. This gives an $\mathsf{OR} \circ \mathsf{AND} \circ \mathsf{OR}$ circuit. The true arithmetic carries give a satisfying branch whenever the modular sum is zero, and conversely any satisfying branch certifies zero in every block, so the circuit is correct. Its gate count is bounded by Equation (177).

Taking logarithms in Equation (177), using $\binom{n}{k} \leq (\mathrm{e}n/k)^k$, gives

$$\log \mathrm{size}_{\Sigma_3}(k\text{-}\mathsf{SUM}_{n,m,k}) \leq k \log(\mathrm{e}n/k) + t \log k + kb + O(\log m). \tag{180}$$

Choose $b := \lceil \sqrt{m \log k/k} \rceil$. Since $k \geq 2$ and $m \geq 1$, this choice lies in $[m]$, and $t \leq m/b + 1$. Hence both $t \log k$ and $kb$ are $O(\sqrt{km \log k} + k)$, proving Equation (178). Finally, if $n \geq k^2$ and $m = \Theta(k \log(\mathrm{e}n/k))$, then $\log k = O(\log(n/k))$, so every term on the right of Equation (178) is $O(k \log(n/k))$, which proves Equation (179). ☐

## F.2 The structural constant floor for the expander route

The preceding circuits show that the natural brute-force exponent is $k$ for $k$-$\mathsf{OV}$ in base $n$ and for $k$-$\mathsf{XOR}$ in base $n/k$. The lower bounds of Theorem 17 have the same linear scale, but the particular $\kappa$-based expander route cannot match the leading constant.

**Proposition 72** (A constant-factor floor for regular-core padding)**.** *Let $P = F \mathbin{\dot\cup} J_t$, where $F$ is a nonempty $\Delta$-regular core with $\Delta \geq 2$, $J_t$ is a disjoint matching, and $e(P) = k-1$. If one idealizes the LRR exponent $\kappa(P) - o(1)$ to $\kappa(P)$ and then applies a quadratic host substitution $N^2 = \Theta(n)$ or $N^2 = \Theta(n/k)$, the resulting target-base exponent is at most $(k-1)/\Delta$. Consequently, compared with the brute-force exponent $k$, the ratio between the upper exponent and this ceiling for the $\kappa$-based route is strictly greater than $\Delta$.*[4]

*Proof.* By Theorem 4, $\kappa(P) \leq \mathrm{tw}(P) + 1$. Treewidth is the maximum over connected components; moreover, $\mathrm{tw}(J_t) \leq 1$, while the minimum-degree condition on $F$ forces a cycle, whose treewidth is 2, and treewidth is minor-monotone. Hence $\mathrm{tw}(F) \geq 2$, while trivially $\mathrm{tw}(F) \leq v(F) - 1$, and therefore

$$\kappa(P) \leq \mathrm{tw}(P) + 1 = \max\{\mathrm{tw}(F), 1\} + 1 \leq v(F). \tag{181}$$

[4] This proposition and its proof were proposed and derived by the AI language model GPT-5.5; the authors independently verified the argument before inclusion.

Since $F$ is $\Delta$-regular,

$$v(F) = \frac{2e(F)}{\Delta} \le \frac{2(k-1)}{\Delta}. \tag{182}$$

The idealized LRR exponent $\kappa(P)$ in base $N$ becomes $\kappa(P)/2$ in the corresponding target base after either quadratic host substitution. Combining Equations (181) and (182) gives the ceiling $(k-1)/\Delta$. The brute-force exponent $k$ divided by this ceiling is $\Delta k/(k-1) > \Delta$. □

*Remark* 73 (Scope of the floor). The proposition is a limitation of this specific $\kappa$-based regular-core-plus-matching route, not an upper bound on what other source families or other lower-bound methods could prove. For the degree-7 family used in Theorem 17, it already forces a ratio greater than 7, even before accounting for slack in the expansion estimate or in the LRR exponent.

## F.3 The depth-sensitive comparison for $k$-SUM

In the nondegenerate high-width regime of Corollary 61, the transferred lower exponent has scale $\min\{k\log(n/k), m\}$. By Proposition 71, a top-disjunction depth-three upper exponent is controlled by

$$U_\Sigma(n,m,k) := k\log(en/k) + \sqrt{km\log k} + k + \log m. \tag{183}$$

At the principal width $m = \Theta(k\log(en/k))$ and under $n \ge k^2$, which holds throughout the polynomial-host regimes of Theorem 21, and Theorem 28, one has $U_\Sigma(n,m,k) = \Theta(k\log(n/k))$. Thus, after specializing the fixed-$k$ lower bound of Theorem 17 to top-disjunction depth three, the lower and upper bounds match at exponent scale there.[5]

Away from the principal width, two different gaps may remain. When $m \le k\log(n/k)$, the lower exponent can be width-limited while the elementary circuit still enumerates all supports, contributing $k\log(en/k)$. When $m \ge k\log(n/k)$, the ratio between the displayed depth-three upper scale and the saturated lower scale satisfies

$$\frac{U_\Sigma(n,m,k)}{k\log(n/k)} = O\left(1 + \frac{\sqrt{m\log k/k}}{\log(n/k)} + \frac{k+\log m}{k\log(n/k)}\right). \tag{184}$$

The carry contribution in Equation (184) becomes superconstant only beyond $m = \omega(k\log^2(n/k)/\log k)$. The resulting overhead is much smaller than the $\Theta(m/\log(n/k))$ gap suggested by the depth-two DNF, but it need not be constant at arbitrarily large width.

The block-carry improvement is depth-sensitive. The direct depth-two circuit resolves complete assignments to a support, whereas the top-disjunction depth-three circuit guesses intermediate block carries and verifies the blocks in parallel. No fixed depth yields a polynomial-size verifier for the fixed-support predicate uniformly in $k$: by Proposition 63, restricting each selected residue to $\{0, 2^{m-1}\}$ turns that predicate into the complement of PARITY, so every fixed depth still requires size $\exp(\Omega_d(k^{1/(d-1)}))$. The matching restriction in Equations (142) and (143) shows that this parity floor is shared by $k$-$\mathsf{XOR}$. Hence the PARITY obstruction itself does not distinguish the two list targets. The quantitative distinction is in the available upper bounds: the fixed-support $k$-$\mathsf{XOR}$ predicate has an $m\,2^{k-1}$-clause CNF, the direct fixed-support $k$-$\mathsf{SUM}$ predicate has a $2^{(k-1)m}$-term DNF, and the block-carry $\Sigma_3$ construction replaces the latter dependence by the square-root carry overhead.

[5]The depth-sensitive comparison in this section, including the block-carry width choice underlying the exponent bound $U_\Sigma(n,m,k)$ of Equation (183) and the resulting ratio estimate of Equation (184), was discovered and derived by the AI language model GPT-5.5; the authors independently verified the argument before inclusion.



ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il